ESET Internet Security

Kullanıcı Kılavuzu

Bu belgenin yardım sürümünü görüntülemek için burayı tıklayın

Digital Security
Progress. Protected.

ESET Internet Security, ESET, spol. s r.o. tarafından geliştirildi

Daha fazla bilgi için https://www.eset.com adresini ziyaret edin.

Teknik Destek: https://support.eset.com

REVİZE. 12.04.2024

ADVANCED SECURITY

ESET Internet Security

ESET Internet Security tamamen tümleşik bilgisayar güvenliğinde yepyeni bir yaklaşımın temsilcisidir. ESET LiveGrid® tarama altyapısının en yeni sürümü, özel Güvenlik duvarı ve Antispam modülleriyle birlikte bilgisayarınızın güvenliğini korumak için hızlı ve son derece hassastır. Sonuç olarak ortaya, bilgisayarınızı tehlikeye sokabilecek saldırı ve kötü amaçlı yazılımlara karşı sürekli tetikte olan akıllı bir sistem çıkmıştır.

ESET Internet Security, maksimum korumayı ve sistem kaynaklarının en az seviyede kullanımını bir araya getiren tam bir güvenlik çözümüdür. Gelişmiş teknolojilerimiz virüsler, casus yazılımlar, truva atları, solucanlar, reklam yazılımları, kök setleri ve diğer tehditler tarafından gerçekleştirilebilecek sızıntıları sistem performansını düşürmeden veya bilgisayarınızı kesintiye uğratmadan önlemek için yapay zeka kullanır.

Özellikler ve avantajlar

Yeniden tasarlanan kullanıcı arabirimi	Bu sürümdeki kullanıcı arabirimi, kullanışlılık testlerinin sonuçlarına göre önemli ölçüde yeniden tasarlandı ve basitleştirildi. Tüm GUI ifade ve bildirimleri titizlikle gözden geçirildi ve arabirim İbranice ve Arapça gibi sağdan sola dilleri destekleyecek şekilde değiştirildi. Çevrimiçi yardım artık ESET Internet Security ürünü içinde de yer alıyor ve dinamik olarak güncellenen destek içerikleri sağlıyor.
Koyu Mod	Ekranı hızlı bir şekilde koyu bir temaya dönüştürmenize yardımcı olan bir uzantı. Kullanıcı arabirimi öğelerinde tercih ettiğiniz renk düzenini seçebilirsiniz.
Antivirus ve antispyware	Daha çok sayıda bilinen ve bilinmeyen virüsleri, solucanları, truva atlarını ve kök setlerini proaktif bir şekilde algılar ve temizler. Gelişmiş sezgisel tarama teknolojisi, daha önce hiçbir yerde görülmemiş kötü amaçlı yazılımları bile bayraklayarak sizi bilinmeyen tehditlerden korur ve bunları, size zarar vermeden önce etkisiz duruma getirir. Web erişimi koruması ve Kimlik Avı koruması, web tarayıcıları ile uzak sunucular (SSL dahil) arasındaki iletişimi izleyerek çalışır. E-posta istemci koruması POP3(S) ve IMAP(S) protokolleri üzerinden alınan e-posta iletişiminin denetimini sağlar.
Düzenli güncellemeler	Algılama altyapısının (önceki adıyla "virüs imza veri tabanını") ve program modüllerinin düzenli olarak güncellenmesi, bilgisayarınızda maksimum güvenlik düzeyi sağlamak için en iyi yöntemdir.
ESET LiveGrid® (Bulut-tabanlı Bilinirlik)	Çalışan işlemlerin ve dosyaların bilinirliğini doğrudan ESET Internet Security içinde kontrol edebilirsiniz.
Aygıt denetimi	Tüm USB flash sürücülerini, bellek kartlarını ve CD'leri/DVD'leri otomatik olarak tarar. Medya türüne, üreticiye, boyuta ve diğer niteliklere göre çıkarılabilir medyayı engeller.
HIPS işlevselliği	Sistemin davranışını daha ayrıntılı biçimde özelleştirebilirsiniz; sistem kayıt defteri, etkin işlemler ve programlar için kurallar belirleyebilir ve güvenlik tutumunuzda ince ayarlar yapabilirsiniz.
Oyun modu	Sistem kaynaklarını oyunlar veya diğer tam ekranlı aktiviteler için korumak üzere tüm açılır pencereleri, güncellemeleri veya sistemi yoğun bir şekilde kullanan diğer aktiviteleri erteler.

ESET Internet Security özellikleri

Bankacılık ve Ödeme Sistemleri Koruması	Bankacılık ve Ödeme Sistemleri Koruması, tüm çevrim içi işlemlerin güvenilir ve emniyetli bir ortamda gerçekleşmesini sağlamak için çevrim içi bankacılık veya çevrim içi ödeme ağ geçitlerine erişilirken kullanılmak üzere bir güvenli tarayıcı sunar.
Ağ imzaları için destek	Ağ imzaları hızlı tanımlamaya izin verir ve bot ya da exploit paketleri gibi, kullanıcı aygıtlarından gelen veya bu aygıtlara giden kötü amaçlı trafiği engeller. Bu özellik Botnet Koruması'nın geliştirilmiş hali olarak düşünülebilir.
Akıllı Güvenlik Duvarı	Yetkisiz kullanıcıların bilgisayarınıza erişip kişisel verilerinizden faydalanmasını engeller.
ESET Antispam	İstenmeyen posta, tüm e-posta iletişiminin yüzde 50'ini oluşturuyor. Antispam Koruması, bu sorundan koruma hizmeti sunar.
Anti-Theft	Anti-Theft, bilgisayarın kaybolması veya çalınması durumunda kullanıcı düzeyindeki güvenliği artırır. ESET Internet Security ve Anti-Theft ürünlerini yükledikten sonra cihazınız web arabiriminde listelenir. Web arabirimi, cihazınızda Anti-Theft yapılandırmasını ve Anti-Theft özelliklerini yönetmenize olanak sağlar.
Ebeveyn kontrolü	Çeşitli web sitesi kategorilerini engelleyerek ailenizi rahatsız edici olabilecek web içeriğinden korur.

ESET Internet Security Özelliklerinin çalışması için bir lisansın etkin olması gerekmektedir. ESET Internet Security lisansının süresi dolmadan birkaç hafta önce lisansınızı yenilemeniz önerilir.

Yenilikler

ESET Internet Security 16 sürümündeki yenilikler

Geliştirilmiş Bankacılık ve Ödeme Sistemleri Koruması

"Tüm tarayıcıların güvenliğini sağla" modu, favori tarayıcınızı kullandığınız her seferinde ödemelerinizi, bankacılık işlemlerinizi ve hassas verilerinizi korumanıza yardımcı olmak için desteklenen tarayıcılarda varsayılan olarak etkinleştirilir.

Intel® Threat Detection Technology

Bellekte tespiti önlemeye çalışan bir fidye yazılımını ortaya çıkartan donanım tabanlı teknoloji. Entegrasyonu, genel sistem performansını yüksek düzeyde tutarken fidye yazılımı korumasını güçlendirir.

Koyu Mod

Bu özellik, ESET Internet Security Grafik kullanıcı arabirimi için açık veya koyu renk düzeni seçmenize olanak sağlar. Kullanıcı arabirimi öğelerinde tercih ettiğiniz renk düzenini seçebilirsiniz.

> **Yenilikler ile ilgili bildirimleri** devre dışı bırakmak için **Gelişmiş ayarlar** > **Bildirimler** > **Masaüstü bildirimleri**'ni tıklayın. **Masaüstü bildirimleri**'nin yanındaki **Düzenle**'yi tıklayıp **Yenilikler ile ilgili bildirimleri göster** onay kutusunun işaretini kaldırın ve **Tamam**'ı tıklayın. Daha fazla bilgi için Bildirimler bölümüne bakın.

Benim ürünüm hangisi?

ESET güçlü ve hızlı antivirus çözümlerinden minimum düzeyde sistem ayak izine sahip tümü bir arada çözümlerine kadar çeşitli güvenlik katmanlarında yeni ürünler sunar:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

Hangi ürünü yüklediğinizi öğrenmek için ana program penceresini açtığınızda pencerenin üst bölümünde ürünün adını göreceksiniz (Bilgi Bankası makalesine bakın).

Aşağıdaki tabloda her spesifik üründe bulunan özelliklerin detayları verilmektedir.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Algılama altyapısı	✔	✔	✔
Gelişmiş Makine Öğrenimi	✔	✔	✔
Exploit Engelleyici	✔	✔	✔
Komut Dosyası Tabanlı Saldırı Koruması	✔	✔	✔
Kimlik Avı Koruması	✔	✔	✔
Web erişimi koruması	✔	✔	✔
HIPS (Fidye Yazılımı koruması dahil)	✔	✔	✔
Antispam		✔	✔
Güvenlik Duvarı		✔	✔
Ağ Denetçisi		✔	✔
Web Kamerası Koruması		✔	✔
Ağ Saldırısına Karşı Koruma		✔	✔
Botnet Koruması		✔	✔
Bankacılık ve Ödeme Sistemleri Koruması		✔	✔
Ebeveyn Kontrolü		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Yukarıdaki ürünlerdne bazıları sizin dilinizde / bölgenizde mevcut olmayabilir.

Sistem gereksinimleri

ESET Internet Security ürününün optimal şekilde performans göstermesi için sisteminiz aşağıdaki donanım ve yazılım gerekliliklerini karşılamalıdır:

Desteklenen İşlemciler

Intel veya AMD işlemci, 32 bit (x86) ve SSE2 talimat kümesi veya 64 bit (x64), 1 GHz veya üzeri
ARM64 tabanlı işlemci, 1 GHz veya üzeri

Desteklenen İşletim Sistemleri

Microsoft® Windows® 11
Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7 SP1 (en son Windows güncellemeleri ile birlikte)

Microsoft® Windows® Home Server 2011 64-bit

> Teknik sınırlamalar nedeniyle, ESET Internet Security sürüm 16.0; Windows 7, Windows 8 (8.1) ve Windows Home Server 2011'i destekleyen en son sürümdür. Korunmaya devam etmek ve ESET Internet Security için en son güncellemeleri almak üzere işletim sisteminizi Windows 10 veya üzeri sürüme yükseltin. Daha fazla bilgi için Microsoft Windows'un güncel olmayan sürümleri'ne bakın.

Anti-Theft, Microsoft Windows Home Server'ı desteklemiyor.

ESET Internet Security özellik gereksinimleri

Aşağıdaki tabloda belirli ESET Internet Security özellikleri için sistem gereksinimlerine bakın:

Özellik	Gereklilikler
Intel® Threat Detection Technology	Desteklenen işleyicilere bakın.
Bankacılık ve Ödeme Sistemleri Koruması	Desteklenen web tarayıcılarına bakın.
Saydam arka plan	Windows 10 sürümü RS4 ve üzeri.
Özelleştirilmiş temizleyici	ARM64 tabanlı olmayan işleyici.
Sistem temizleyici	ARM64 tabanlı olmayan işleyici.
Exploit Engelleyici	ARM64 tabanlı olmayan işleyici.
Derin Davranışsal İnceleme	ARM64 tabanlı olmayan işleyici.
Bankacılık ve Ödeme Sistemleri Koruması - web sitesi yönlendirmesi	ARM64 tabanlı olmayan işleyici.

Diğer

Etkinleştirme işlemi ve ESET Internet Security güncellemelerinin doğru şekilde çalışması için internet bağlantısı gereklidir.

Tek bir cihazda eş zamanlı olarak çalışan iki antivirus programı, sistemi kullanılamaz hale getirecek şekilde yavaşlatma gibi kaçınılmaz sistem kaynağı çakışmalarına neden olur.

Microsoft Windows'un eski sürümü

Sorun

- ESET Internet Security ürününü Windows 7, Windows 8 (8.1) veya Windows Home Server 2011'e sahip bir bilgisayara yüklemek istiyorsunuz
- ESET Internet Security yükleme sırasında veya ana program penceresinde bir **Güncel olmayan işletim sistemi** bildirimi görüntüler

Ayrıntılar

Microsoft'un en son bilgilerine dayalı olarak, Windows 8.1 desteği Ocak 2023'te sona erecek. Windows 7 desteği 14 Ocak 2020'de sona ermişti. Daha fazla bilgi için Windows 7 ve Windows 8.1 destek ömrü sonu'na bakın.

Teknik sınırlamalar nedeniyle, ESET Internet Security sürüm 16.0; Windows 7, Windows 8 (8.1) ve Windows Home Server 2011'i destekleyen en son sürümdür. Aşağıdaki bilgiler ESET Internet Security sürüm 16.0 için geçerlidir:

- ESET Internet Security sürüm 16.0 desteklenecek ve Kullanım Ömrü Sonu politikamıza uygun olarak Windows 7, Windows 8 (8.1) ve Windows Home Server 2011 ile ilgili güncellemeleri alacak.
- Windows 7, Windows 8 (8.1) ve Windows Home Server 2011'de ESET Internet Security 16.0 sürümünü 16.1 ve üzeri sürümlere yükseltemezsiniz.
- İşletim sisteminizi yükseltmek, yalnızca ESET Internet Security ürününün bilgisayarınızda çalışması için değil, aynı zamanda genel olarak güvenliğiniz için de önemlidir.

Çözüm

Aşağıdaki çözümler mevcuttur:

Windows 10 veya Windows 11'e yükseltin

Yükseltme işlemi nispeten kolaydır ve birçok durumda, dosyalarınızı kaybetmeden yapabilirsiniz. Windows 10'a yükseltmeden önce:

1. Önemli verileri yedekleme.
2. Microsoft'un Windows 10'a Yükseltme ile ilgili SSS'ler veya Windows 11'e Yükseltme ile ilgili SSS'ler bölümünü okuyun ve Windows işletim sisteminizi güncelleyin.

Yeni bir bilgisayara taşıyın ve ESET ürününü aktarın

Yeni bir bilgisayar veya cihaz alıyorsanız ya da aldıysanız - mevcut ESET ürününüzü yeni bir cihaza nasıl aktaracağınızı öğrenin.

Güncel olmayan işletim sistemi bildirimini gizleyin ve Windows 7, Windows 8 veya Windows 8.1 sürümünü kullanmaya devam edin (önerilmez)

Windows 7, Windows 8 veya Windows 8.1'i kullanmayı sürdürürseniz bilgisayarınız çalışmaya devam edecektir,

ancak güvenlik risklerine ve virüslere karşı daha savunmasız hale gelebilir. Bilgisayarınız artık Windows güncellemelerini (güvenlik güncellemeleri dahil) almayacak ve en son ESET Internet Security sürümünü yüklemeniz mümkün olmayacak. Bildirimi devre dışı bırakmak için:

1. Ana program penceresi > **Ayarlar** > **Gelişmiş Ayarlar** (F5) > **Bildirimler**'i açın ve **Uygulama durumları**'nın yanındaki **Düzenle**'yi tıklayın.

2. **Genel** grubunda, **İşletim sisteminiz güncel değil** seçeneğinin yanındaki onay kutusunun işaretini kaldırın. **Tamam** > **Tamam**'ı tıklayın.

Windows 7 sürümünüz güncel değil

Sorun

Güncel olmayan bir işletim sistemi sürümü kullanıyorsunuz. Korunmaya devam etmek için işletim sisteminizi daima güncel tutmaya çalışın.

Çözüm

{GET_OSNAME} {GET_BITNESS} üzerinde çalışan bir ESET Internet Security yüklediniz.

En son Windows güncellemelerini içeren (en azından KB4474419 ve KB4490628) Windows 7 Service Pack 1 (SP1) paketini yüklediğinizi doğrulayın.

Windows 7 otomatik olarak güncellenecek şekilde yapılandırılmamışsa **Başlat menüsü** > **Kontrol Paneli** > **Sistem ve Güvenlik** > **Windows Update** > **Güncellemeleri denetle** seçeneğini ve ardından **Güncellemeleri yükle**'yi tıklayın.

Engelleme

Bilgisayarınızda çalışırken ve özellikle internette gezinirken, dünyadaki hiçbir antivirus sisteminin algılama ve uzaktan saldırı risklerini tam olarak ortadan kaldıramadığını lütfen unutmayın. Maksimum koruma ve rahatlık sağlamak için antivirus çözümünüzü doğru şekilde kullanmanız ve birkaç faydalı kurala uymanız çok önemlidir:

Düzenli güncelleme

ESET LiveGrid® Kaynaklı istatistik verilerine göre, her gün, var olan güvenlik önlemlerini aşmak ve yazanlara kazanç sağlamak amacıyla (bedelini diğer kullanıcıların ödeyeceği şekilde) binlerce yeni ve benzersiz sızıntı yöntemi oluşturulmaktadır. ESET Araştırma Laboratuvarı'ndaki uzmanlar bu tehditleri günlük olarak çözümler ve kullanıcılarımıza sağlanan koruma düzeyini sürekli olarak artırmak için güncellemeler hazırlayıp yayınlar. Bu güncellemelerin maksimum etki sağladığından emin olmak için bu güncellemelerin sisteminizde düzgün bir şekilde yapılandırılması çok önemlidir. Güncellemeleri yapılandırma konusunda daha fazla bilgi için Güncelleme ayarları bölümüne bakın.

Güvenlik eklerini karşıdan yükleme

Kötü niyetli yazılım yazarları, kötü amaçlı kodun etki alanını genişletmek amacıyla genellikle çeşitli sistem açıklarından yararlanırlar. Yazılım şirketleri bunu göz önünde bulundurarak uygulamalarında ortaya çıkan güvenlik açıklarını yakından izler ve olası tehditleri ortadan kaldırmak üzere düzenli olarak güvenlik güncellemeleri yayımlar. Bu güvenlik güncellemelerini yayımlanır yayımlanmaz karşıdan yüklemek önemlidir. Microsoft Windows ve Internet Explorer gibi web tarayıcıları düzenli olarak güvenlik güncellemeleri yayınlayan programlara verilebilecek iki örnektir.

Önemli verileri yedekleme

Kötü niyetli kod yazanlar genellikle kullanıcıların ihtiyaçlarına aldırmaz ve kötü amaçlı programların çalışması sıklıkla işletim sisteminin tamamen çalışmaz hale gelmesine ve önemli verilerin kaybolmasına neden olur. Bu nedenle önemli ve gizli verilerinizi düzenli olarak DVD veya harici sabit sürücü gibi bir dış kaynağa yedeklemeniz büyük önem taşır. Bu şekilde sisteminizde bir arıza olduğunda verilerinizi çok daha kolay ve hızlı biçimde kurtarabilirsiniz.

Bilgisayarınızda düzenli olarak virüs taraması yapma

Diğer bilinen veya bilinmeyen virüslerin, solucanların, truva atlarının ve kök setlerinin algılanması Gerçek zamanlı dosya sistemi koruma modülü tarafından gerçekleştirilir. Bu, her dosyaya erişim sağladığınızda veya dosya açtığınızda, dosyanın kötü amaçlı etkinlik için tarandığı anlamına gelir. Kötü amaçlı yazılımlar çok çeşitli olduğundan ve algılama altyapısı her gün kendini yenilediğinden en az ayda bir kere tam bir Bilgisayar taraması gerçekleştirmenizi öneririz.

Temel güvenlik kurallarını uygulama

En yararlı ve en etkili kural şudur: Her zaman dikkatli olun. Günümüzde birçok sızıntı türü yürütülmek veya dağıtılmak için kullanıcı müdahalesi gerektirir. Yeni dosyaları açarken dikkatli davranırsanız, sızıntıları temizlemek için harcayacağınız önemli ölçüdeki zamandan ve çabadan tasarruf edersiniz. Aşağıda bazı faydalı yönergeler verilmiştir:

- Birçok açılır pencere ve gösterişli reklam içeren şüpheli web sitelerini ziyaret etmeyin.
- Ücretsiz programları, codec paketlerini ve benzerlerini yüklerken dikkatli olun. Yalnızca güvenli programları kullanın ve yalnızca güvenli Internet web sitelerini ziyaret edin.
- E-posta eklerini, özellikle yığın postalar olarak gelen iletilerin ve bilinmeyen kişilerden gelen iletilerin eklerini açarken dikkatli olun.
- Bilgisayarda gündelik işler yaparken Yönetici hesabı kullanmayın.

Yardım sayfaları

ESET Internet Security kullanım kılavuzuna hoş geldiniz. Burada sağlanan bilgiler, ürününüzü tanımanızı ve bilgisayarınızı daha güvenli hale getirmenizi sağlayacaktır.

Başlarken

ESET Internet Security aracını kullanmaya başlamadan önce, bilgisayarınızı kullanırken karşılaşabileceğiniz çeşitli tespit türleri ve uzaktan saldırılar hakkında bilgi edinebilirsiniz. Ayrıca ESET Internet Security ürününde sunulan yeni özelliklerin bir listesini de derledik.

Önce ESET Internet Security aracını yükleyin. Zaten ESET Internet Security uygulamasını yüklediyseniz ESET Internet Security ile çalışma bölümüne bakın.

ESET Internet Security Yardım sayfalarını kullanma

Online Yardım, çeşitli bölümlere ve alt bölümlere ayrılmıştır. Halihazırda açılan pencereyle ilgili bilgileri görüntülemek için ESET Internet Security ürünündeki **F1** seçeneğine basın.

Program, bir yardım başlığını anahtar sözcükler kullanarak aramanıza veya sözcük ya da ifadeler girerek içerikte arama yapmanıza olanak tanır. Bu iki yöntem arasındaki fark; anahtar sözcüğün bu anahtar sözcüğü metninde bulundurmayan yardım sayfalarıyla mantıksal olarak ilişkilendirilmiş olabilmesidir. Sözcükler ve sözcük gruplarıyla arama ise, tüm sayfaların içeriğini arar ve yalnızca aranan sözcüğü veya sözcük grubunu metninde içeren sayfaları görüntüler.

Tutarlılık sağlamak ve karışıklığı önlemek için bu kılavuzda kullanılan terminoloji, ESET Internet Security kullanıcı arabirimine dayanmaktadır. Ayrıca, belirli ilgi veya öneme sahip konuları vurgulamak için de tek tip bir semboller dizisi de kullanılmaktadır.

Not, kısa bir gözlem aktarır. Not kısımları atlanabilir ancak bazen bu bölümlerde belirli özellikler veya diğer ilgili başlıklara yönelik bir bağlantı gibi değerli bilgiler sunulur.

Bu, atlamamanızı önerdiğimiz konulara dikkatinizi çekmeyi amaçlar. Genellikle kritik olmayan ancak önemli bilgiler sağlar.

Bu, ekstra dikkat ve önlem gerektiren bilgidir. Uyarılar, zarar getirebilecek olası hatalar yapmanızı engellemek için özellikle belirtilir. Son derece hassas sistem ayarlarına veya riskli bir şeye referans içerdiğinden metni okuyup iyice anlamanızı öneririz.

Belirli bir işlev veya özelliğin nasıl kullanılacağını anlamanıza yardımcı olan kullanıma veya uygulamaya yönelik bir örnektir.

Kural	Anlam
Kalın yazı tipi	Kutular ve seçenek düğmeleri gibi arabirim öğesi adları.
İtalik yazı tipi	Sağlamak istediğiniz bilgiler için yer tutucular. Örneğin, dosya adı veya yolu, bir dosyanın gerçek yolunu veya adını girdiğiniz anlamına gelir.
`Courier New`	Kod örnekleri veya komutlar.
Köprü	Çapraz referanslı konulara veya harici web konumlarına hızlı ve kolay erişim sağlar. Köprüler mavi renkte vurgulanır ve altı çizili olabilir.
%ProgramFiles%	Windows'ta yüklenen programların depolandığı Windows sistem dizini.

Çevrimiçi yardım, yardım içeriğinin başlıca kaynağıdır. En son Online Yardım sürümü, çalışan bir internet bağlantınız olduğunda otomatik olarak görüntülenir.

Yükleme

ESET Internet Security ürününü bilgisayarınıza yüklemenin birkaç yöntemi vardır. Yükleme yöntemleri, ülkeye ve dağıtım şekline göre değişebilir:

- Live installer - ESET web sitesinden veya CD/DVD'den indirildi. Yükleme paketi tüm diller için evrenseldir (uygun dili seçin). Live installer küçük bir dosyadır ve ESET Internet Security ürününü yüklemek için gereken ek dosyalar otomatik olarak indirilir.

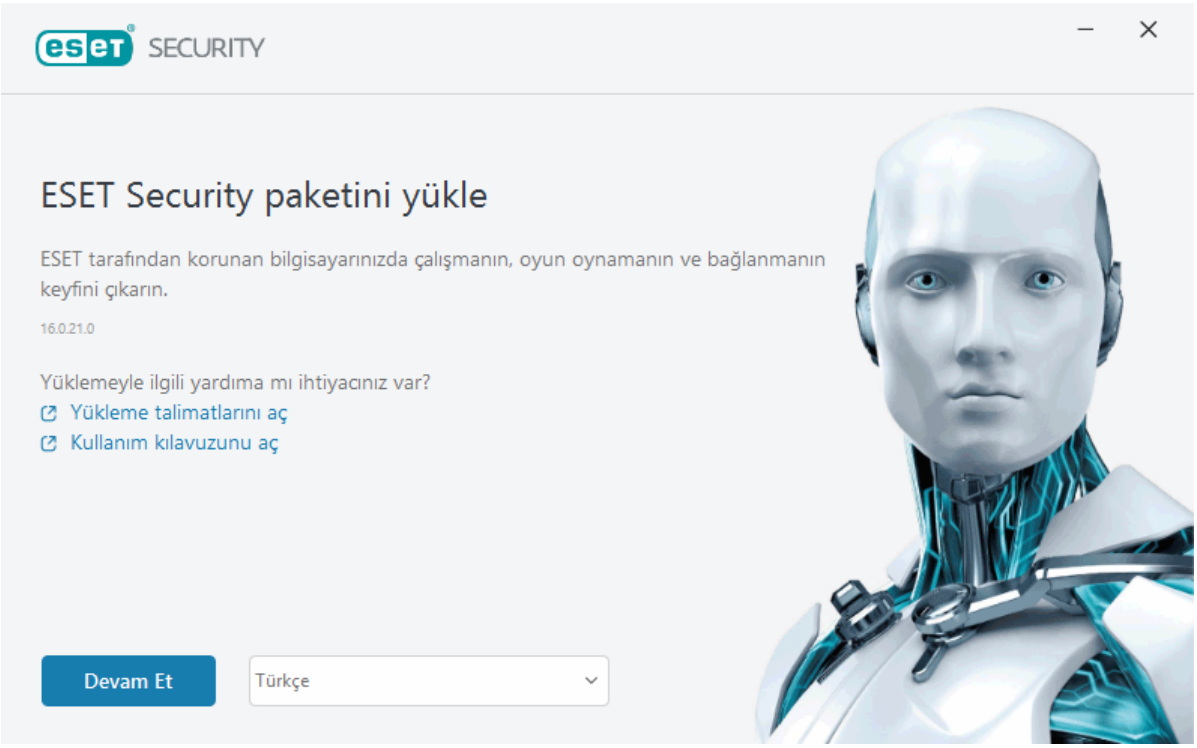
- Çevrim dışı yükleme - Live installer dosyasından daha büyük bir .exe dosyası kullanır ve yükleme işleminin tamamlanması için internet bağlantısı veya ek dosyalar gerektirmez.

ESET Internet Security Ürününü yüklemeden önce, bilgisayarınızda başka antivirüs programları yüklü olmadığından emin olun. Tek bir bilgisayarda iki veya daha fazla antivirüs çözümü yüklüyse, bu ürünler birbiriyle çakışabilir. Sisteminizdeki diğer antivirüs programlarını kaldırmanızı öneririz. Genel antivirüs yazılımına yönelik kaldırıcı araçlarının bir listesi için bkz.ESET Bilgi Bankası makalesi (İngilizce ve diğer birkaç dilde mevcuttur).

Canlı yükleyici

Önce Live installer yükleme paketiaracını indirin, ardından yükleme dosyasını çift tıklayın ve Yükleyici Sihirbazı'ndaki adım adım talimatları uygulayın.

Bu tür yükleme için Internet'e bağlı olmanız gerekir.



1. Açılır menüden uygun dili seçip **Devam**'ı tıklayın.

Parola korumalı ayarlara sahip önceki sürüm üzerine daha yeni bir sürüm yüklüyorsanız parolanızı yazın. Erişim ayarlarında ayarlar parolasını yapılandırabilirsiniz.

2. Aşağıdaki özellikler için tercihinizi yapın, Son Kullanıcı Lisans Sözleşmesi ve Gizlilik Politikası'nı okuyun ve **Devam**'ı tıklayın veya tüm özellikleri etkinleştirmek için **İzin ver**'i tıklayın:

- ESET LiveGrid® geri bildirim sistemi
- İstenmeyen türden olabilecek uygulamalar
- Müşteri Deneyimini İyileştirme Programı

> **Devam** veya **Tüm izin ver ve devam et**'i tıklayarak Son Kullanıcı Lisans Sözleşmesi'ni kabul eder ve Gizlilik Politikası'nı onaylarsınız.

3. ESET HOME Kullanarak cihazın güvenliğini etkinleştirmek, yönetmek ve görüntülemek için cihazınızı ESET HOME hesabına bağlayın. ESET HOME hesabına bağlamadan devam etmek için **Girişi atla**'yı tıklayın. Daha sonra cihazınızı ESET HOME hesabınıza bağlayabilirsiniz.

4. ESET HOME portalına bağlanmadan devam ederseniz bir etkinleştirme seçeneği belirleyin. Daha eski bir sürümün üzerine yeni bir sürümü yüklüyorsanız Lisans Anahtarınız otomatik olarak girilir.

5. Yükleme Sihirbazı, lisansınıza bağlı olarak hangi ESET ürününün yüklenmiş olduğunu belirler. En fazla güvenlik özelliğine sahip sürüm her zaman önceden seçilidir. ESET ürününün farklı bir sürümünü yüklemek istiyorsanız **Ürünü değiştir**'i tıklayın. Yükleme işlemini başlatmak için **Devam**'ı tıklayın. Bu, birkaç dakika sürebilir.

> Geçmişte kaldırılmış olan ESET ürünlerinden kalanlar (dosyalar veya klasörler) varsa bunların kaldırılmasına izin vermeniz istenir. Devam etmek için **Yükle**'yi tıklayın.

6. Yükleme Sihirbazı'ndan çıkmak için **Bitti**'yi tıklayın.

Yükleme sorun gidericisi.

> Ürün yüklenip etkinleştirildikten sonra modüller indirilmeye başlar. Koruma başlatılır ve indirme işlemi tamamlanmadığı takdirde bazı özellikler tam olarak işlevsel olmayabilir.

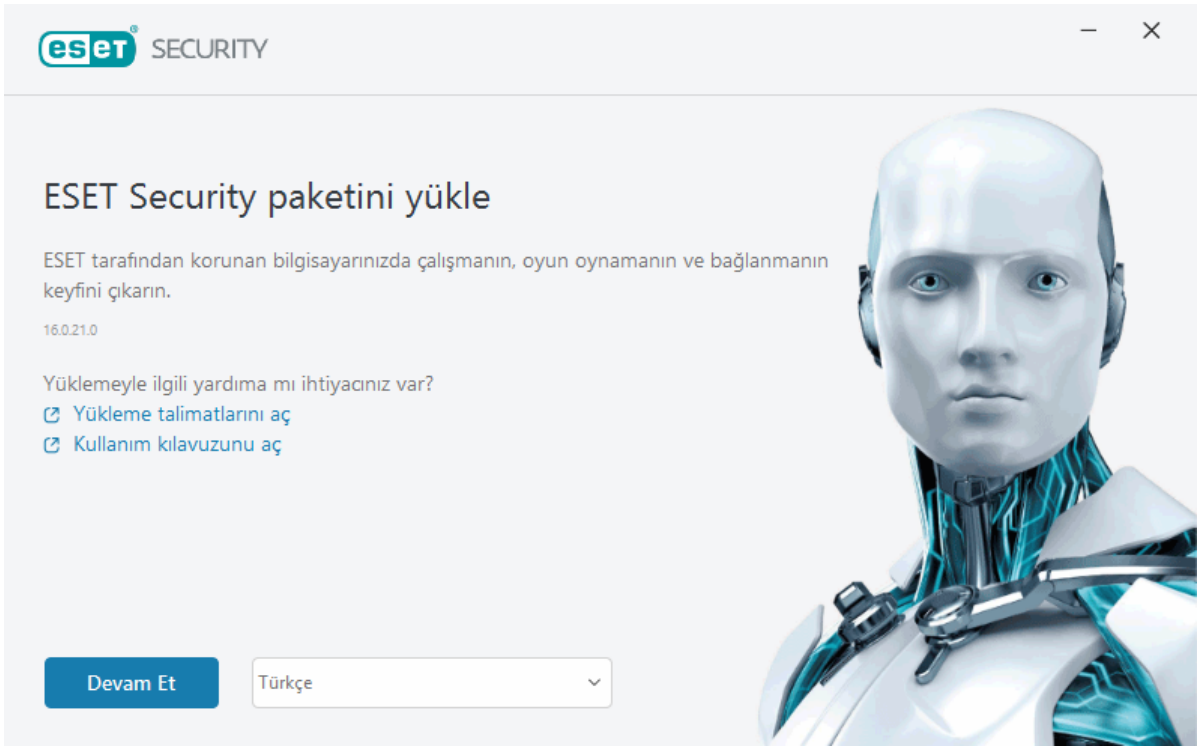
Çevrimdışı yükleme

Aşağıdaki çevrim dışı yükleyiciyi (.exe) kullanarak ESET Windows ev ürününüzü indirip yükleyin. İndirilecek ESET ev ürününün sürümünü seçin (32 bit, 64 bit veya ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
64 bit indir 32 bit indir ARM İndirme	64 bit indir 32 bit indir ARM İndirme	64 bit indir 32 bit indir ARM İndirme

> Etkin bir internet bağlantınız varsa ESET ürününüzü bir Live installer kullanarak yükleyin.

Çevrim dışı yükleyiciyi (.exe) başlattığınızda Yükleme Sihirbazı kurulum sürecinde size yol gösterecektir.



1. Açılır menüden uygun dili seçip **Devam**'ı tıklayın.

> Parola korumalı ayarlara sahip önceki sürüm üzerine daha yeni bir sürüm yüklüyorsanız parolanızı yazın. Erişim ayarlarında ayarlar parolasını yapılandırabilirsiniz.

2. Aşağıdaki özellikler için tercihinizi yapın, Son Kullanıcı Lisans Sözleşmesi ve Gizlilik Politikası'nı okuyun ve **Devam**'ı tıklayın veya tüm özellikleri etkinleştirmek için **İzin ver**'i tıklayın:

- ESET LiveGrid® geri bildirim sistemi
- İstenmeyen türden olabilecek uygulamalar
- Müşteri Deneyimini İyileştirme Programı

> **Devam** veya **Tüm izin ver ve devam et**'i tıklayarak Son Kullanıcı Lisans Sözleşmesi'ni kabul eder ve Gizlilik Politikası'nı onaylarsınız.

3. **Girişi atla**'yı tıklayın. İnternet bağlantınız olduğunda cihazınızı ESET HOME hesabınıza bağlayabilirsiniz.

4. **Etkinleştirmeyi atla**'yı tıklayın. ESET Internet Security ürününün tam işlevsel olması için yüklemeden sonra etkinleştirilmesi gerekir. Ürün etkinleştirme için etkin bir internet bağlantısı gereklidir.

5. Yükleme Sihirbazı, indirilen çevrim dışı yükleyiciye dayalı olarak hangi ESET ürününün yükleneceğini gösterir. Yükleme işlemini başlatmak için **Devam**'ı tıklayın. Bu, birkaç dakika sürebilir.

> Geçmişte kaldırılmış olan ESET ürünlerinden kalanlar (dosyalar veya klasörler) varsa bunların kaldırılmasına izin vermeniz istenir. Devam etmek için **Yükle**'yi tıklayın.

6. Yükleme Sihirbazı'ndan çıkmak için **Bitti**'yi tıklayın.

⚠ Yükleme sorun gidericisi.

Ürün etkinleştirme

Ürününüzü etkinleştirmeye yönelik birkaç yöntem bulunmaktadır. Etkinleştirme penceresindeki belirli bir etkinleştirme senaryosunun kullanılabilirliği, ülkeye ve dağıtım şekline (CD/DVD, ESET web sayfası vb.) bağlı olarak değişiklik gösterebilir:

- Ürünün perakende kutulu bir sürümünü satın aldıysanız veya lisans bilgilerini içeren bir e-posta aldıysanız **Satın alınmış bir Lisans Anahtarı kullan**'ı tıklayarak ürününüzü etkinleştirin. Lisans Anahtarı genellikle ürün paketinin içinde veya arka tarafında bulunur. Etkinleştirmenin başarılı olabilmesi için Lisans Anahtarı sağlandığı şekilde girilmelidir. Lisans Anahtarı –Lisans sahibinin tanımlanması ve lisansın etkinleştirilmesi için kullanılan XXXX-XXXX-XXXX-XXXX-XXXX veya XXXX-XXXXXXXX biçimindeki benzersiz bir dizidir.

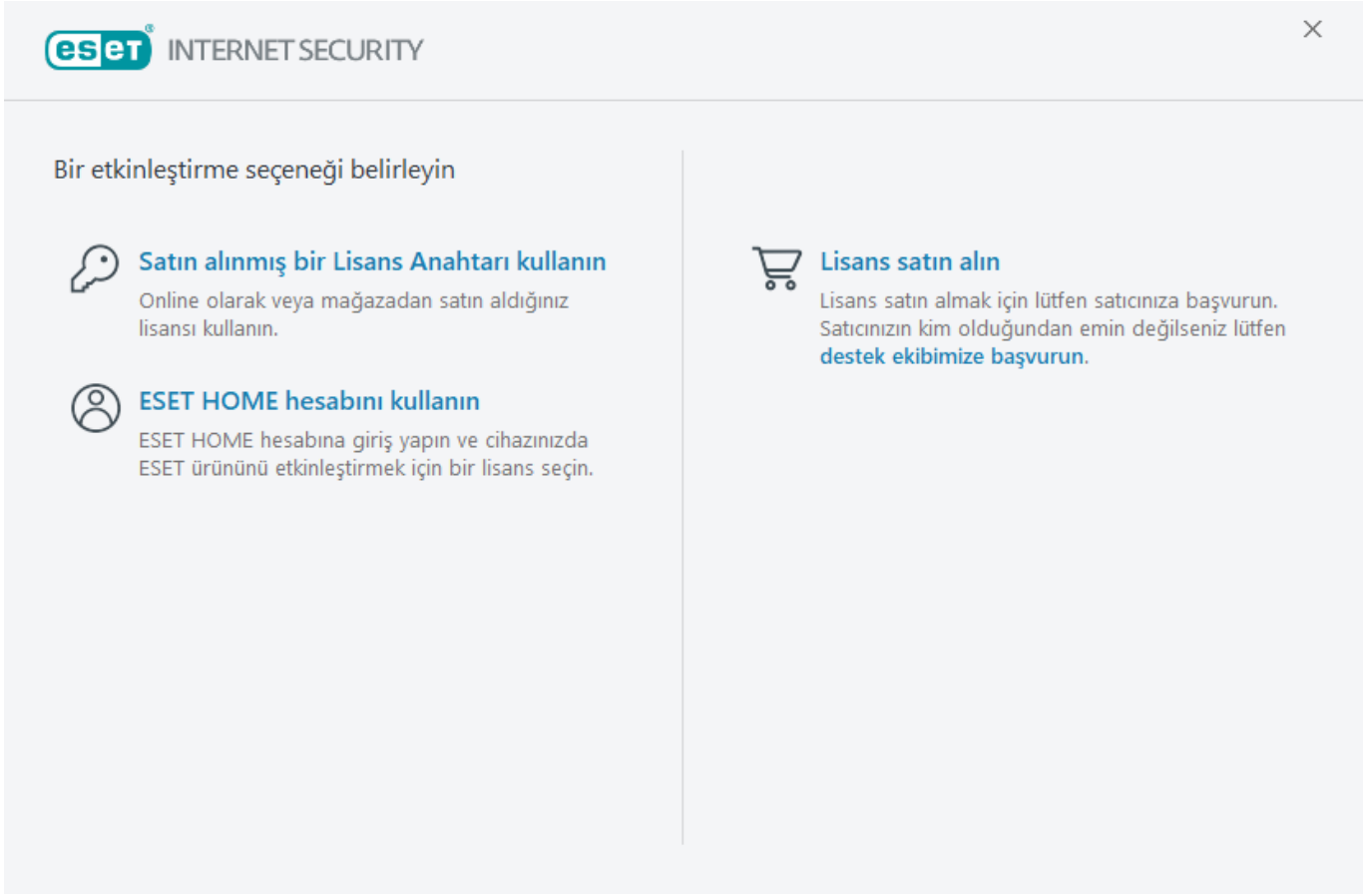
- ESET HOME hesabını kullan'ı seçtikten sonra ESET HOME hesabınıza giriş yapmanız istenir.

- Satın alma işlemini gerçekleştirmeden önce ESET Internet Security ürününü değerlendirmek istiyorsanız Ücretsiz deneme sürümü seçeneğini belirleyin. ESET Internet Security Ürününü sınırlı bir süre için etkinleştirmek üzere e-posta adresinizi ve ülkenizi girin. Deneme lisansınız size e-posta ile gönderilecektir. Deneme lisansları yalnızca her bir müşteri için etkinleştirilebilir.

- Lisansınız yoksa ve satın almak istiyorsanız **Lisans satın al** seçeneğini tıklayın. Bu, sizi yerel ESET dağıtımcısının web sitesine yönlendirir. ESET Windows ev ürünü tam lisansları ücretsiz değildir.

Ürün lisansınızı dilediğiniz zaman değiştirebilirsiniz. Bunun için, ana program penceresinde **Yardım ve Destek** > **Lisansı değiştir**'i tıklayın. Lisansınızı ESET Destek bölümüne tanıtmak için kullanılan genel lisans kimliğinizi görürsünüz.

Ürün etkinleştirme işlemi başarısız mı oldu?



Etkinleştirme sırasında Lisans anahtarınızı girme

Otomatik güncellemeler, güvenliğiniz için önemlidir. ESET Internet Security yalnızca etkinleştirildikten sonra güncellemeleri alır.

Lisans anahtarınızı girerken tam olarak yazıldığı gibi girilmesi önemlidir:

- Lisans Anahtarınız, lisans sahibinin tanımlanması ve lisans etkinleştirmesi için kullanılan XXXX-XXXX-XXXX-XXXX-XXXX biçiminde benzersiz bir dizidir.

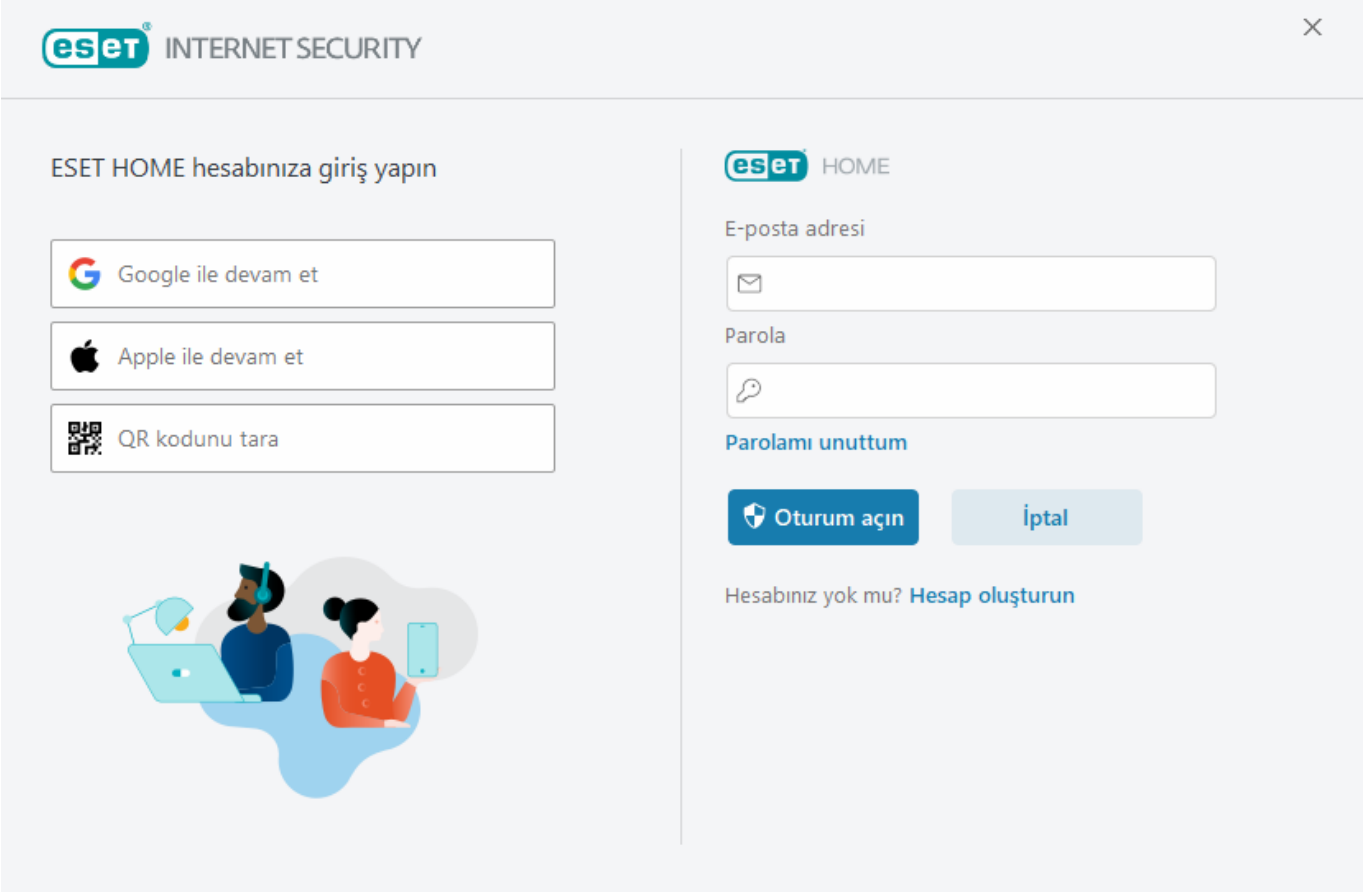
Doğruluğunu garantilemek adına Lisans Anahtarınızı kayıt e-postanızdan kopyalayıp yapıştırmanızı öneririz.

Yüklemenin ardından Lisans Anahtarınızı girmediyseniz ürününüz etkinleştirilmez. Ana program penceresinde **Yardım ve Destek** > **Lisansı Etkinleştir** seçeneğini kullanarak ESET Internet Security ürününü etkinleştirebilirsiniz.

ESET Windows ev ürünü tam lisansları ücretsiz değildir.

ESET HOME hesabını kullanma

Etkinleştirilen tüm ESET lisanslarınızı ve cihazlarınızı görüntülemek ve yönetmek için cihazınızı ESET HOME hesabına bağlayın. Lisansınızı yenileyebilir, yükseltebilir veya uzatabilir ve önemli lisans ayrıntılarını görüntüleyebilirsiniz. ESET HOME yönetim portalında veya mobil uygulamada farklı lisanslar ekleyebilir, ürünleri cihazlarınıza indirebilir, ürün güvenlik durumunu kontrol edebilir veya lisansları e-posta üzerinden paylaşabilirsiniz. Daha fazla bilgi için ESET HOME Online Yardım'ı ziyaret edin.



Etkinleştirme yöntemi olarak veya yükleme sırasında ESET HOME hesabına bağlanırken **ESET HOME hesabını**

kullan'ı seçtikten sonra:

1. ESET HOME hesabınıza giriş yapın.

> ESET HOME hesabınız yoksa kaydolmak için **Hesap oluştur**'u tıklayın veya ESET HOME Online Yardım bölümündeki talimatlara bakın.
> Parolanızı unuttuysanız **Parolamı unuttum** seçeneğini tıklayın ve ekrandaki adımları uygulayın veya ESET HOME Online Yardım bölümüne bakın.

2. Tüm ESET HOME hizmetlerinde kullanılacak olan cihazınız için bir **Cihaz adı** belirleyip **Devam**'ı tıklayın.

3. Etkinleştirme için bir lisans seçin veya yeni bir lisans ekleyin. ESET Internet Security ürününü etkinleştirmek için **Devam'ı** tıklayın.

Deneme Lisansını etkinleştir

ESET Internet Security Deneme sürümünüzü etkinleştirmek için **E-posta adresi** ve **E-posta adresini onaylayın** alanına geçerli bir e-posta adresi girin. Etkinleştirmeden sonra, ESET lisansı oluşturulur ve e-posta adresinize gönderilir. Bu e-posta adresi aynı zamanda ürün kullanım süresinin dolmasına yönelik bildirimler ve ESET ile olan diğer iletişimler için kullanılacaktır. Deneme sürümü yalnızca bir kez etkinleştirilebilir.

ESET Internet Security ürününü, teknik destek sağlayacak olan yerel dağıtımcınıza kaydettirmek için **Ülke** açılır menüsünden ülkenizi seçin.

Ücretsiz ESET Lisans anahtarı

ESET Internet Security için tam lisans ücretsiz değildir.

ESET lisans anahtarı, ESET Internet Security ürününün Son Kullanıcı Lisans Sözleşmesi gereğince yasal olarak kullanılmasını sağlamak için ESET tarafından sağlanan, harf ve rakamlardan oluşan ve kısa çizgiyle ayrılan benzersiz bir dizidir. Her Son Kullanıcı, Lisans anahtarını ESET tarafından verilen lisans sayısına göre ESET Internet Security ürününü kullanma hakkının kapsamıyla sınırlı olacak şekilde kullanabilecektir. Lisans anahtarı gizli kabul edilir ve paylaşılamaz, ancak lisans altındaki cihaz lisanslarını ESET HOME portalını kullanarak paylaşabilirsiniz.

İnternette size "ücretsiz" ESET lisans anahtarları sağlayabilecek kaynaklar vardır, ancak şunları unutmayın:

- Bir "Ücretsiz ESET lisansı" reklamını tıklamak, bilgisayarınızı veya cihazınızı tehlikeye düşürebilir ve zararlı yazılımların saldırısına uğramanıza neden olabilir. Zararlı yazılım resmi olmayan sosyal medya içeriklerinde (ör. videolarda), ziyaretlerinize vs. bağlı olarak para kazanmak için reklam gösteren web sitelerinde gizlenebilir. Bunlar genellikle tuzaktır.
- ESET, korsan lisanları devre dışı bırakabilir ve bırakır.
- Korsan bir lisans anahtarına sahip olmak, ESET Internet Security ürününü yüklemek için kabul etmeniz gereken Son Kullanıcı Lisans Sözleşmesi'ne uygun değildir.
- ESET lisanslarını yalnızca www.eset.com, ESET dağıtıcıları veya bayileri gibi resmi kanallardan satın alın (eBay gibi resmi olmayan üçüncü taraf web sitelerinden lisans satın almayın veya üçüncü taraflara ait ortak lisansları kullanmayın).

- ESET Internet Security ürünü ücretsiz olarak indirilir, ancak yükleme sırasında etkinleştirme işlemi, geçerli bir ESET lisans anahtarı gerektirir (ürünü indirip yükleyebilirsiniz, ancak etkinleştirmeden kullanamazsınız)
- Lisansınızı internette veya sosyal medyada paylaşmayın (yayılabilir).

Korsan bir ESET lisansını tespit edip bildirmek için talimatları uygulamak amacıyla Bilgi Bankası makalemizi ziyaret edin.

\Bir ESET güvenlik ürününü alma konusunda kararsızsanız karar vermek için deneme sürümünü kullanabilirsiniz:

1. ESET Internet Security ürününü ücretsiz deneme lisansıyla etkinleştirme
2. ESET Beta Programına katılım
3. Android mobil cihaz kullanıyorsanız ESET Mobile Security uygulamasını yükleyin, bu "freemium" (ücretsiz premium) bir uygulamadır.

Lisansınız için indirim kazanmak veya lisans süresini uzatmak için ESET ürününüzü yenileyin.

Etkinleştirme başarısız - sık karşılaşılan durumlar

ESET Internet Security ürününün etkinleştirilmesi başarılı olmadıysa en yaygın nedenler şu şekildedir:

- Lisans anahtarı zaten kullanımdadır.
- Geçersiz bir lisans anahtarı girdiniz.
- Etkinleştirme formundaki bilgiler eksik veya geçersiz.
- Etkinleştirme sunucusuyla iletişim kurulamadı.
- ESET etkinleştirme sunucularına bağlantı yok veya bağlantı devre dışı.

Doğru lisans anahtarını girdiğinizi ve internet bağlantınızın etkin olduğunu doğrulayın. ESET Internet Security ürününü yeniden etkinleştirmeyi deneyin. Etkinleştirme için ESET HOME hesabı kullanıyorsanız ESET HOME Lisans Yönetimi - Çevrimiçi Yardım'a bakın.

> Belirli bir hata alırsanız (örneğin, Askıya alınan lisans veya Lisans aşırı kullanılmış), Lisans durumuyla ilgili talimatları uygulayın.

Yine de etkinleştiremiyorsanız ESET Etkinleştirme Sorun Gidericisi etkinleştirme ve lisanslarla ilgili sık sorulan sorular, hatalar ve sorunlar hakkında size yol gösterir (İngilizce ve diğer bazı dillerde mevcuttur).

Lisans durumu

Lisansınız farklı durumlara sahip olabilir. Lisans durumunuzu ESET HOME portalında bulabilirsiniz. Lisansınızı ESET HOME hesabınıza eklemek için Lisans ekleme bölümüne bakın.

ESET HOME hesabınız yoksa Yeni bir ESET HOME hesabı oluşturabilirsiniz.

Lisans durumu **Aktif** haricindeki bir durumsa etkinleştirme sırasında bir hata veya ana program penceresinde bir bildirim alırsınız.

Lisans durumu bildirimlerini devre dışı bırakmak için **Gelişmiş ayarlar** (F5) > **Bildirimler** > **Uygulama durumları**'nı açın. **Uygulama durumlarının** yanındaki **Düzenle**'yi tıklayın, **Lisans**'ı genişletin ve devre dışı bırakmak istediğiniz bildirimin yanındaki onay kutusunun işaretini kaldırın. Bildirimi devre dışı bırakmak sorunu çözmez.

Farklı lisans durumları için açıklamaları ve önerilen çözümleri aşağıdaki tabloda görebilirsiniz:

Lisans durumu	Açıklama	Çözüm
Etkin	Lisans geçerli. Herhangi bir etkileşimde bulunmanıza gerek yok. ESET Internet Security etkinleştirilebilir ve lisans ayrıntılarını ana program penceresi > **Yardım ve destek** bölümünde bulabilirsiniz.	
Aşırı kullanıldı	Bu lisansı izin verilenden daha fazla cihaz kullanıyor. Bir etkinleştirme hatası alırsınız.	Daha fazla bilgi için Lisans aşırı kullanım nedeniyle etkinleştirilemedi bölümüne bakın.
Askıya alındı	Lisansınız ödeme sorunları nedeniyle askıya alındı. Lisansı kullanmak için ESET HOME portalındaki ödeme bilgilerinizin güncel olduğundan emin olun veya lisans satıcınıza başvurun. Bu hatayı etkinleştirme sırasında veya ana program penceresinden alabilirsiniz.	Yüklü ürün - ESET HOME hesabınız varsa ana program penceresinde gösterilen bildirimde **Lisansınızı ESET HOME portalından yönetin**'i tıklayın ve ödeme ayrıntılarınızı gözden geçirin. Aksi halde, lisans satıcınıza başvurun. Etkinleştirme hatası - ESET HOME hesabınız varsa etkinleştirme hatası penceresinde **ESET HOME portalını aç**'ı tıklayın ve ödeme bilgilerinizi gözden geçirin. Aksi halde, lisans satıcınıza başvurun.
Sona erdi	Lisansınız sona erdi ve ESET Internet Security ürününü etkinleştirmek için bu lisansı kullanamazsınız. Bu hatayı etkinleştirme sırasında veya ana program penceresinden alabilirsiniz. Zaten ESET Internet Security ürününü yüklediyseniz bilgisayarınız korunmuyor.	Yüklenmiş ürün - Ana program penceresinde görüntülenen bildirimde, **Lisansı yenile**'yi tıklayın ve Lisansımı nasıl yenilerim? bölümündeki talimatları uygulayın veya **Ürünü etkinleştir**'i tıklayın ve etkinleştirme yönteminizi seçin. Etkinleştirme hatası - Etkinleştirme hatası penceresinde **Lisansınızı yenile**'yi tıklayın ve Lisansımı nasıl yenilerim? bölümündeki talimatları uygulayın veya yeni ya da yenilenen bir lisans anahtarı yazıp **Lisansı yenile**'yi tıklayın.

Lisans aşırı kullanım nedeniyle etkinleştirilemedi

Sorun

- Lisansınız aşırı kullanılmış ya da kötüye kullanılmış olabilir
- Lisans aşırı kullanım nedeniyle etkinleştirilemedi

Çözüm

Bu lisans, izin verilenden daha çok cihaz tarafından kullanılıyor. Yazılım korsanlığı veya sahteciliğine maruz kalmış olabilirsiniz. Lisans başka bir ESET ürününü etkinleştirmek için kullanılamaz. Lisansı yönetme izniniz varsa veya yasal bir kaynaktan satın aldıysanız bu sorunu doğrudan ESET HOME hesabınızdan çözebilirsiniz. Henüz hesabınız yoksa bir hesap oluşturun.

Lisans sahibiyseniz ve e-posta adresinizi girmeniz istenmemişse:

1. ESET lisansınızı yönetmek için bir web tarayıcısını açıp https://home.eset.com sayfasına gidin. Cihaz lisanslarını devre dışı bırakmak için ESET License Manager aracına erişin. Daha fazla bilgi için Lisans aşırı kullanıldığında ne olur? bölümüne bakın.

2. Korsan saldırısına uğramış bir ESET lisansını tespit edip bildirmek için talimatları uygulamak amacıyla Korsan saldırıya uğramış ESET lisanslarını tespit etme ve bildirme makalemizi ziyaret edin.

3. Emin değilseniz **Geri** tuşunu tıklayıp ESET Teknik Destek ekibine e-posta gönderin.

Lisans sahibi değilseniz bu lisansın sahibiyle, lisansın aşırı kullanımından dolayı ESET ürününü etkinleştiremediğinizi bildirmek üzere iletişime geçin. Lisans sahibi sorunu ESET HOME portalında çözebilir.

E-posta adresinizi girmeniz istenirse (yalnızca birkaç kez istenir), ESET Internet Security ürününüzü satın almak veya etkinleştirmek için kullandığınız e-posta adresini girin.

Lisansı yükseltme

Bu bildirim penceresi, ESET ürününüzü etkinleştirmek için kullanılan lisans değiştirildiğinde görüntülenir. Değiştirilen lisansınız, daha fazla güvenlik özelliğine sahip bir ürünü etkinleştirmenize olanak tanır. Hiçbir değişiklik yapılmamışsa ESET Internet Security, bir kez **Daha fazla özelliğe sahip bir ürüne geçiş yapın** başlıklı bir uyarı penceresi gösterir.

Evet (önerilir) - Otomatik olarak daha fazla güvenlik özelliğine sahip ürünü yükler.

Hayır, teşekkürler - Değişiklik yapılmaz ve bildirim kalıcı olarak kaybolur.

Ürünü daha sonra değiştirmek için ESET Bilgi Bankası makalemize bakın. ESET lisansları hakkında daha fazla bilgi için Lisansla ilgili SSS'ler bölümüne bakın.

Aşağıdaki tabloda her spesifik üründe bulunan özelliklerin detayları verilmektedir.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Algılama altyapısı	✔	✔	✔
Gelişmiş Makine Öğrenimi	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Exploit Engelleyici	✔	✔	✔
Komut Dosyası Tabanlı Saldırı Koruması	✔	✔	✔
Kimlik Avı Koruması	✔	✔	✔
Web erişimi koruması	✔	✔	✔
HIPS (Fidye Yazılımı koruması dahil)	✔	✔	✔
Antispam		✔	✔
Güvenlik Duvarı		✔	✔
Ağ Denetçisi		✔	✔
Web Kamerası Koruması		✔	✔
Ağ Saldırısına Karşı Koruma		✔	✔
Botnet Koruması		✔	✔
Bankacılık ve Ödeme Sistemleri Koruması		✔	✔
Ebeveyn Kontrolü		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Ürün yükseltme

Varsayılan bir yükleyici indirdiniz ve etkinleştirilecek ürünü değiştirmeye karar verdiniz veya yüklenmiş ürününüzü daha fazla güvenlik özelliğine sahip bir ürünle değiştirmek istiyorsunuz.

Yükleme sırasında ürünü değiştirin.

Aşağıdaki tabloda her spesifik üründe bulunan özelliklerin detayları verilmektedir.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Algılama altyapısı	✔	✔	✔
Gelişmiş Makine Öğrenimi	✔	✔	✔
Exploit Engelleyici	✔	✔	✔
Komut Dosyası Tabanlı Saldırı Koruması	✔	✔	✔
Kimlik Avı Koruması	✔	✔	✔
Web erişimi koruması	✔	✔	✔
HIPS (Fidye Yazılımı koruması dahil)	✔	✔	✔
Antispam		✔	✔
Güvenlik Duvarı		✔	✔
Ağ Denetçisi		✔	✔
Web Kamerası Koruması		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Ağ Saldırısına Karşı Koruma		✔	✔
Botnet Koruması		✔	✔
Bankacılık ve Ödeme Sistemleri Koruması		✔	✔
Ebeveyn Kontrolü		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Lisans eski sürüme düşürme

Bu iletişim penceresi, ESET ürününüzü etkinleştirmek için kullanılan lisans değiştirildiğinde görüntülenir. Değiştirilen lisansınız yalnızca daha az güvenlik özelliklerine sahip farklı bir ESET ürünüyle kullanılabilir. Ürün, korumanın kaybedilmesini önlemek için otomatik olarak değiştirilmiştir.

ESET lisansları hakkında daha fazla bilgi için Lisansla ilgili SSS'ler bölümüne bakın.

Aşağıdaki tabloda her spesifik üründe bulunan özelliklerin detayları verilmektedir.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Algılama altyapısı	✔	✔	✔
Gelişmiş Makine Öğrenimi	✔	✔	✔
Exploit Engelleyici	✔	✔	✔
Komut Dosyası Tabanlı Saldırı Koruması	✔	✔	✔
Kimlik Avı Koruması	✔	✔	✔
Web erişimi koruması	✔	✔	✔
HIPS (Fidye Yazılımı koruması dahil)	✔	✔	✔
Antispam		✔	✔
Güvenlik Duvarı		✔	✔
Ağ Denetçisi		✔	✔
Web Kamerası Koruması		✔	✔
Ağ Saldırısına Karşı Koruma		✔	✔
Botnet Koruması		✔	✔
Bankacılık ve Ödeme Sistemleri Koruması		✔	✔
Ebeveyn Kontrolü		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Ürünü eski sürüme düşürme

Şu anda yüklü olan ürün, etkinleştirmek üzere olduğunuz üründen daha fazla güvenlik özelliğine sahip. Hırsızlığa karşı korumayı ve ESET HOME içinde depolanan ilgili verilere erişimi kaybedersiniz.

Aşağıdaki tabloda her spesifik üründe bulunan özelliklerin detayları verilmektedir.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Algılama altyapısı	✔	✔	✔
Gelişmiş Makine Öğrenimi	✔	✔	✔
Exploit Engelleyici	✔	✔	✔
Komut Dosyası Tabanlı Saldırı Koruması	✔	✔	✔
Kimlik Avı Koruması	✔	✔	✔
Web erişimi koruması	✔	✔	✔
HIPS (Fidye Yazılımı koruması dahil)	✔	✔	✔
Antispam		✔	✔
Güvenlik Duvarı		✔	✔
Ağ Denetçisi		✔	✔
Web Kamerası Koruması		✔	✔
Ağ Saldırısına Karşı Koruma		✔	✔
Botnet Koruması		✔	✔
Bankacılık ve Ödeme Sistemleri Koruması		✔	✔
Ebeveyn Kontrolü		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Yükleme sorun giderici

Yükleme sırasında sorunlar oluşursa Yükleme Sihirbazı, mümkünse sorunu çözen bir sorun giderici sağlar.

Sorun gidericiyi başlatmak için **Sorun gidericiyi çalıştır**'ı tıklayın. Sorun giderici sona erdiğinde önerilen çözümü izleyin.

Sorun devam ederse genel yükleme hataları ve çözüm listesine bakın.

Ek ESET güvenlik araçlarının kurulumu

ESET Internet Security ürününü kullanmaya başlamadan önce korumanızı en üst düzeye çıkarmak için ek güvenlik araçları da ayarlayabilirsiniz:

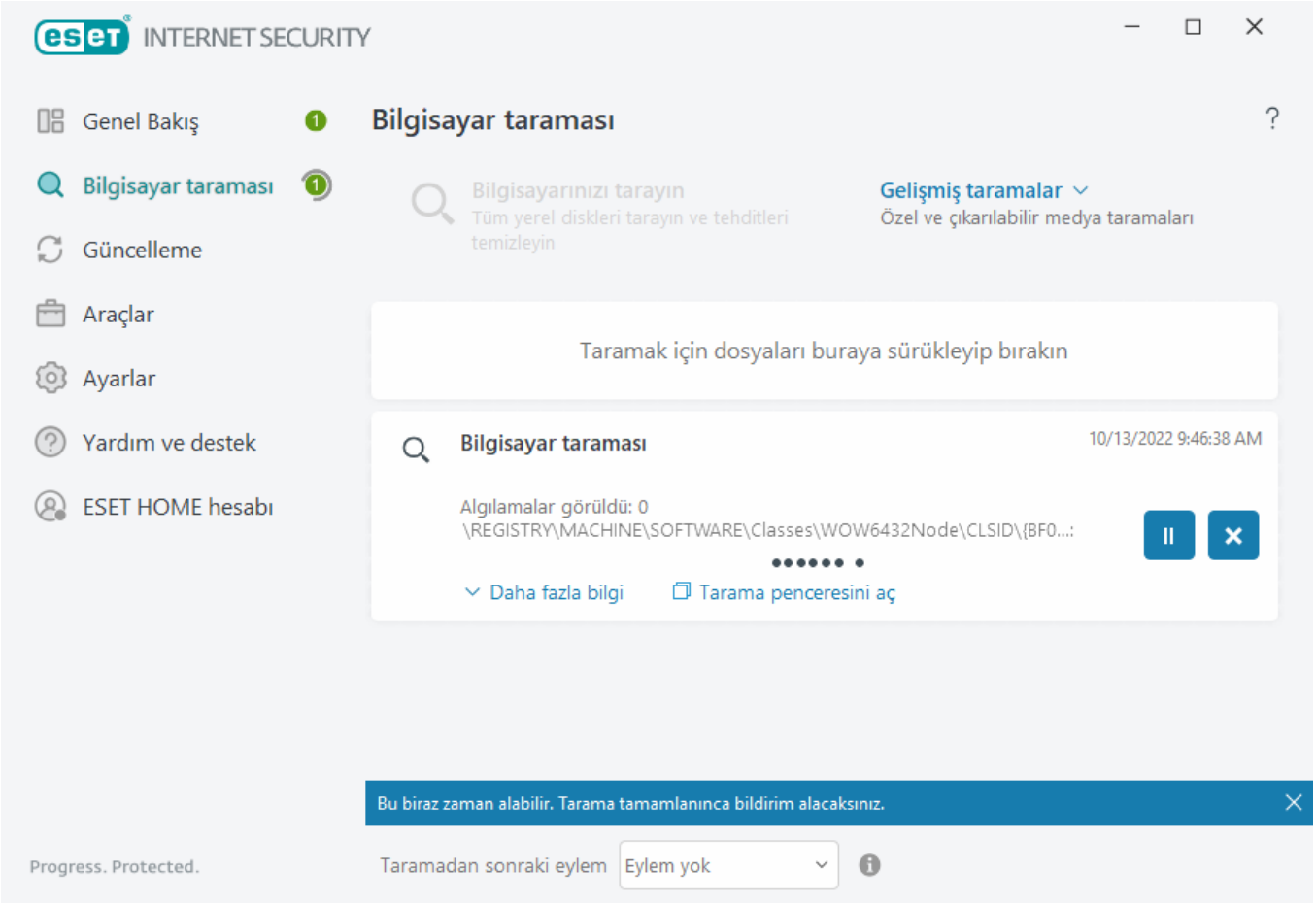
- Ebeveyn Kontrolü
- Anti-Theft

ESET Internet Security ürününde ek güvenlik araçları ayarlama hakkında daha fazla bilgi için aşağıdaki ESET Bilgi Bankası makalesini okuyun.

Yüklemeden sonra ilk tarama

ESET Internet Security Yüklendikten sonra, kötü amaçlı kod denetimi için ilk başarılı güncellemenin ardından bir bilgisayar taraması otomatik olarak başlar.

Ayrıca **Bilgisayar taraması** > **Bilgisayarınızı tarayın** seçeneğini tıklatarak ana program penceresinden manuel olarak bilgisayar taraması da başlatabilirsiniz. Bilgisayar taramaları hakkında daha fazla bilgi için bkz. Bilgisayar taraması.



Daha yeni bir sürüme yükseltme

ESET Internet Security ürününün yeni sürümleri, iyileştirmeleri uygulamak veya program modüllerinin otomatik güncellemeleriyle çözülemeyen sorunları gidermek için yayımlanır. Daha yeni bir sürüme yükseltme işlemi çeşitli şekillerde gerçekleştirilebilir:

1. Bir program güncellemesi ile otomatik olarak.
Program yükseltmesi tüm kullanıcılara dağıtıldığından ve belirli sistem yapılandırmalarına etki edebildiğinden, tüm olası sistem yapılandırmalarında çalışması için uzun bir sınama süresinden sonra yayımlanır. Yeni bir

sürüm yayımlandıktan hemen sonra bu sürüme yükseltme yapmanız gerekiyorsa, aşağıdaki yöntemlerden birini kullanın.
Gelişmiş ayarlar (F5) > **Güncelleme** > **Profiller** > **Güncellemeler** bölümünde **Uygulama özellik güncellemeleri**'ni etkinleştirdiğinizden emin olun.

2. Manuel olarak, ana program penceresinde, **Güncelleme** bölümündeki **Güncellemeleri kontrol et** seçeneğini tıklayarak.

3. Daha yeni bir sürümü indirip eskisinin üzerine yükleyerek manuel olarak.

Ek bilgi ve resimli talimatlar için şuraya bakın:

- ESET Ürünlerini güncelleme—en son ürün modüllerini kontrol etme
- Farklı ESET ürün güncellemesi ve sürüm türleri nelerdir?

Eski ürün için otomatik yükseltme işlemi

ESET ürün sürümünüz artık desteklenmiyor ve ürününüz en son sürüme yükseltildi.

Genel yükleme sorunları

ESET ürünlerinin her yeni sürümünde birçok hata düzeltmesi ve iyileştirme bulunmaktadır. Bir ESET ürünü için geçerli bir lisansa sahip mevcut müşteriler, aynı ürünün en son sürümüne ücretsiz olarak yükseltme yapabilir.

Yüklemeyi tamamlamak için:

1. Son Kullanıcı Lisansı Sözleşmesi'ni kabul etmek için **Devam et ve kabul et**'i tıklayın ve Gizlilik Politikası'nı onaylayın. Son Kullanıcı Lisans Sözleşmesi'ni kabul etmiyorsanız **Kaldır**'ı tıklayın. Önceki sürüme geri dönemezsiniz.

2. **Tümüne izin ver ve devam et**'i tıklayarak hem ESET LiveGrid® geri bildirim sistemine hem de Müşteri Deneyimi Geliştirme Programına izin verin veya katılmak istemiyorsanız **Devam**'ı tıklayın.

3. Yeni ESET ürününüzü Lisans Anahtarınızla etkinleştirdikten sonra Genel bakış sayfası görüntülenir. Lisans bilgileriniz bulunmuyorsa yeni bir deneme lisansıyla devam edin. Önceki üründe kullanılan lisansınız geçerli değilse ESET ürününüzü etkinleştirin.

4. Yüklemeyi tamamlamak için cihazın yeniden başlatılması gerekir.

ESET Internet Security yüklenecek

Şu iletişim penceresi görüntülenebilir:

- Yükleme işlemi sırasında - ESET Internet Security ürününü yüklemek için **Devam**'ı tıklayın.
- ESET Internet Security Ürününde bir lisansı değiştirirken - Lisansı değiştirmek ESET Internet Security ürününü etkinleştirmek için **Etkinleştir**'i tıklayın.

Ürünü değiştir seçeneği, ESET lisansınıza göre ESET Windows ev ürünleri arasında geçiş yapmanıza olanak tanır.

Daha fazla bilgi için Benim ürünüm hangisi? bölümüne bakın.

Farklı bir ürüne geçiş yapma

ESET lisansınıza göre farklı ESET Windows ev ürünleri arasında geçiş yapabilirsiniz. Daha fazla bilgi için Benim ürünüm hangisi? bölümüne bakın.

Kayıt

Lütfen kayıt formundaki alanları tamamlayıp Etkinleştir seçeneğini tıklatarak lisansınızı kaydedin. Parantez içinde gerekli olarak işaretlenen alanlar zorunludur. Bu bilgiler yalnızca ESET lisansınızla ilgili konularda kullanılacaktır.

Etkinleştirme ilerlemesi

Etkinleştirme işleminin tamamlanması için birkaç saniye bekleyin (gereken süre internet bağlantınızın veya bilgisayarınızın hızına göre farklılık gösterebilir).

Etkinleştirme başarılı

Etkinleştirme işlemi tamamlandı. ESET Internet Security ürününün kurulumunu tamamlamak için yükleme sonrası sihirbazını takip edin.

Birkaç saniye içinde modül güncellemesi başlatılır. ESET Internet Security için düzenli güncellemeler hemen başlar.

Modül güncellemesinin ardından 20 dakika içinde birinci tarama otomatik olarak başlar.

Yeni Başlayanlara yönelik kılavuz

ESET Internet Security ve temel ayarları hakkında genel bir ilk bakış sağlar.

Ana program penceresi

ESET Internet Security ana program penceresi iki bölüme ayrılır. Sağdaki birincil pencere, soldaki ana menüden seçilen seçeneğe karşılık gelen bilgileri görüntüler.

> **Resimli talimatlar**
> İngilizce ve diğer çeşitli dillerde mevcut olan resimli talimatlar için ESET Windows ürünlerinin ana program penceresini açın bölümüne bakın.

Ana menü seçenekleri:

Genel bakış – ESET Internet Security ürününün koruma durumu hakkında bilgiler sağlar.

Bilgisayar taraması – Bilgisayarınızın taramasını yapılandırın ve başlatın ya da özel bir tarama oluşturun.

Güncelleme - Modül ve tespit altyapısı güncellemeleriyle ilgili bilgileri görüntüler.

Araçlar - Şuna erişim sağlar: Ağ Denetçisi, Bankacılık ve Ödeme Sistemleri Koruması, Anti-Theft ve program yönetimini basitleştirmeye yardımcı olan ve ileri düzey kullanıcılar için ek seçenekler sunan diğer özellikler.

Ayarlar - ESET Internet Security koruma özellikleri için yapılandırma seçenekleri (Bilgisayar koruması, İnternet koruması, Ağ koruması ve Güvenlik araçları) ve Gelişmiş ayarlara erişim sağlar.

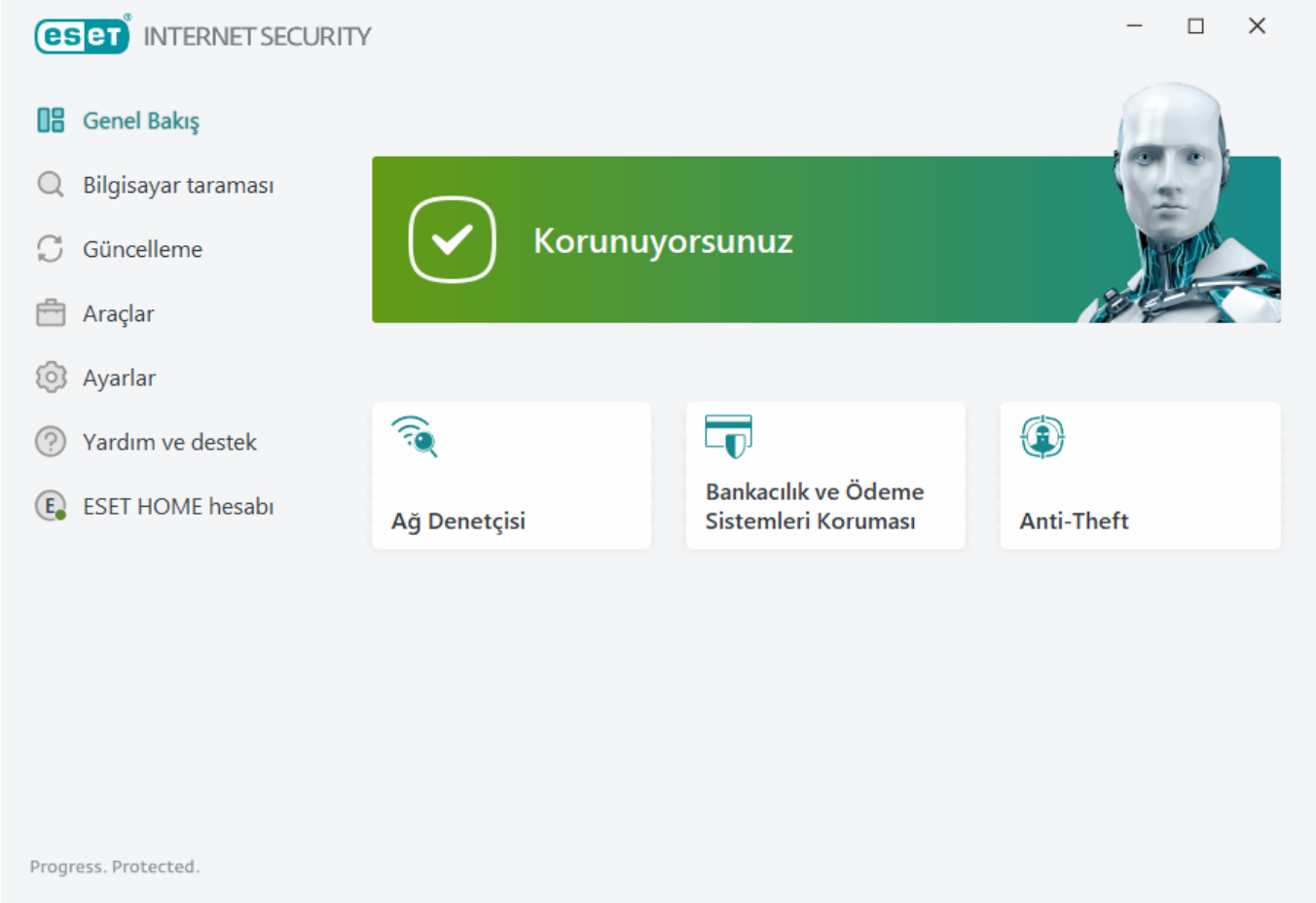
Yardım ve destek - Lisansınız ve yüklenmiş ESET ürünüyle ilgili bilgilerin yanı sıra Online Yardım, ESET Bilgi Bankası ve Teknik Destek ile ilgili bağlantıları görüntüler.

ESET HOME hesabı - Cihazınızı ESET HOME portalına bağlayın veya ESET HOME hesabının bağlantı durumunu inceleyin. ESET HOME yönetim portalını kullanarak Anti-Theft ayarlarınızın yanı sıra etkin ESET lisanslarını ve cihazlarını görüntüleyip yönetebilirsiniz.

ESET Internet Security grafik kullanıcı arabiriminin renk düzenini değiştirmek için Kullanıcı arabirimi öğelerine bakın.

Genel Bakış penceresi, bilgisayarınızın mevcut korumasıyla ilgili bilgilerin yanı sıra ESET Internet Security ürünündeki güvenlik özelliklerine hızlı bağlantıları gösterir.

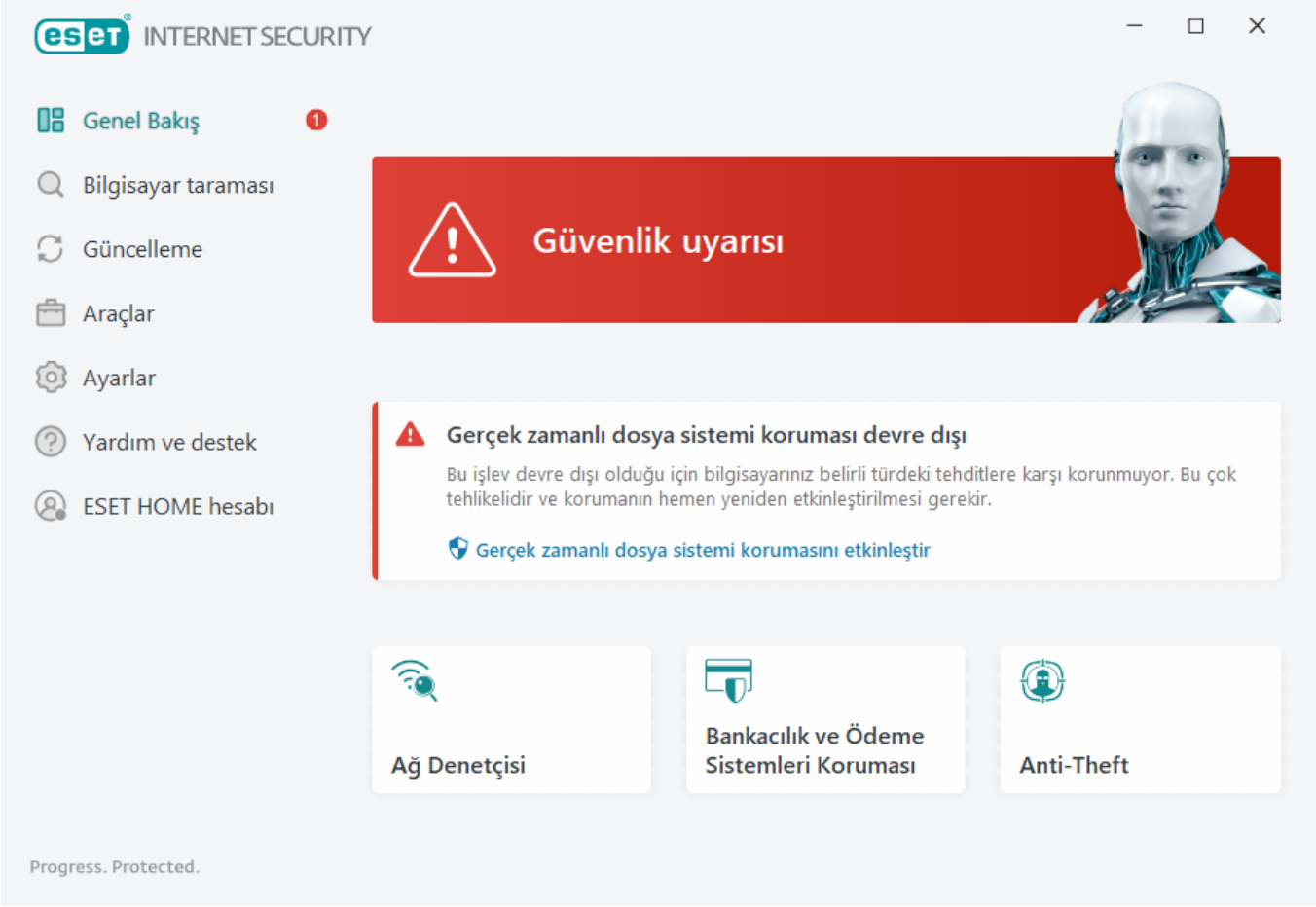
Genel Bakış penceresinde, ESET Internet Security güvenliğini iyileştirmek, ek özellikleri açmak veya maksimum koruma sağlamak için önerilen çözümlerle birlikte ayrıntılı bilgiler içeren bildirimler gösterilir. Daha fazla bildirim varsa tüm bildirimleri genişletmek için **X daha fazla bildirim**'i tıklayın.



Yeşil simge ve yeşil **Korunuyorsunuz** durumu maksimum korumanın sağlandığını gösterir.

Program düzgün çalışmadığında yapılacaklar

Etkin bir koruma modülü düzgün bir şekilde çalışıyorsa koruma durumu simgesi yeşil olur. Kırmızı bir ünlem işareti veya turuncu bildirim simgesi en yüksek koruma düzeyinin garantilenmediğini gösterir. Her bir modülün koruma durumuyla ilgili ek bilgilerin yanı sıra tam korumayı geri yüklemek için önerilen çözümler **Genel bakış** penceresinde bildirim olarak gösterilir. Ayrı ayrı modüllerin durumunu değiştirmek için **Ayarlar**'ı tıklatın ve istenilen modülü seçin.



Kırmızı simge ve kırmızı **Güvenlik uyarısı** durumu kritik sorunlar olduğunu gösterir. Bu durumun görüntülenmesinin birkaç nedeni olabilir, örneğin:

- **Ürün etkinleştirilmedi** veya **Lisans süresi doldu** – Bu durum kırmızı koruma durumu simgesiyle belirtilir. Lisans süresi dolduktan sonra program güncellenemez. Lisansınızı yenilemek için uyarı penceresindeki talimatları uygulayın.
- **Algılama altyapısı güncel değil** – Bu hata, algılama altyapısını güncellemeye yönelik birkaç başarısız girişimden sonra görüntülenir. Güncelleme ayarlarını denetlemenizi öneririz. Bu hatanın en yaygın nedeni yanlış girilmiş kimlik doğrulama verileri veya yanlış yapılandırılmış bağlantı ayarlarıdır.
- **Gerçek zamanlı dosya sistemi koruması devre dışı bırakıldı** – Gerçek zamanlı koruma, kullanıcı tarafından devre dışı bırakıldı. Bilgisayarınız tehditlere karşı korunmuyor. Bu işlevi yeniden etkinleştirmek için **Gerçek zamanlı dosya sistemi korumasını etkinleştir** seçeneğini tıklayın.
- **Antivirus ve antispyware koruması devre dışı – Antivirus ve antispyware korumasını etkinleştir**

seçeneğini tıklatarak antivirus ve antispyware korumasını yeniden etkinleştirebilirsiniz.

- **ESET Kişisel güvenlik duvarı devre dışı** – Bu sorun, masaüstünüzde bulunan **Ağ** öğesinin yanındaki bir güvenlik bildirimi ile de gösterilir. **Güvenlik duvarını etkinleştir** seçeneğine tıklatarak ağ korumasını yeniden etkinleştirebilirsiniz.

 Turuncu simge sınırlı koruma anlamına gelir. Örneğin, program güncellenirken bir sorun oluşmuştur veya lisansınızın süresi yakında dolacaktır.
Bu durumun görüntülenmesinin birkaç nedeni olabilir, örneğin:

- **Anti-Theft iyileştirme uyarısı** – Bu aygıt Anti-Theft için optimize edilmemiştir. Örneğin Sahte hesap (bir aygıtı kayıp olarak işaretlediğinizde otomatik olarak tetiklenen güvenlik özelliği) bilgisayarınızda oluşturulamaz. Anti-Theft web arabirimindeki Optimizasyon özelliğini kullanarak bir Sahte hesap oluşturabilirsiniz.
- **Oyun modu etkin** – Oyun modunun etkinleştirilmesi olası bir güvenlik riskidir. Bu özellik etkinleştirildiğinde tüm açılır pencereler devre dışı kalır ve zamanlanan tüm görevler durur.
- **Lisansınız kısa bir süre içinde sona erecek** – Bu durum koruma durumu simgesinin sistem saatinin yanında ünlem işareti görüntülemesiyle belirtilir. Lisansınızın süresi dolduktan sonra program güncellenemeyecek ve Koruma durumu simgesi kırmızı renk olacaktır.

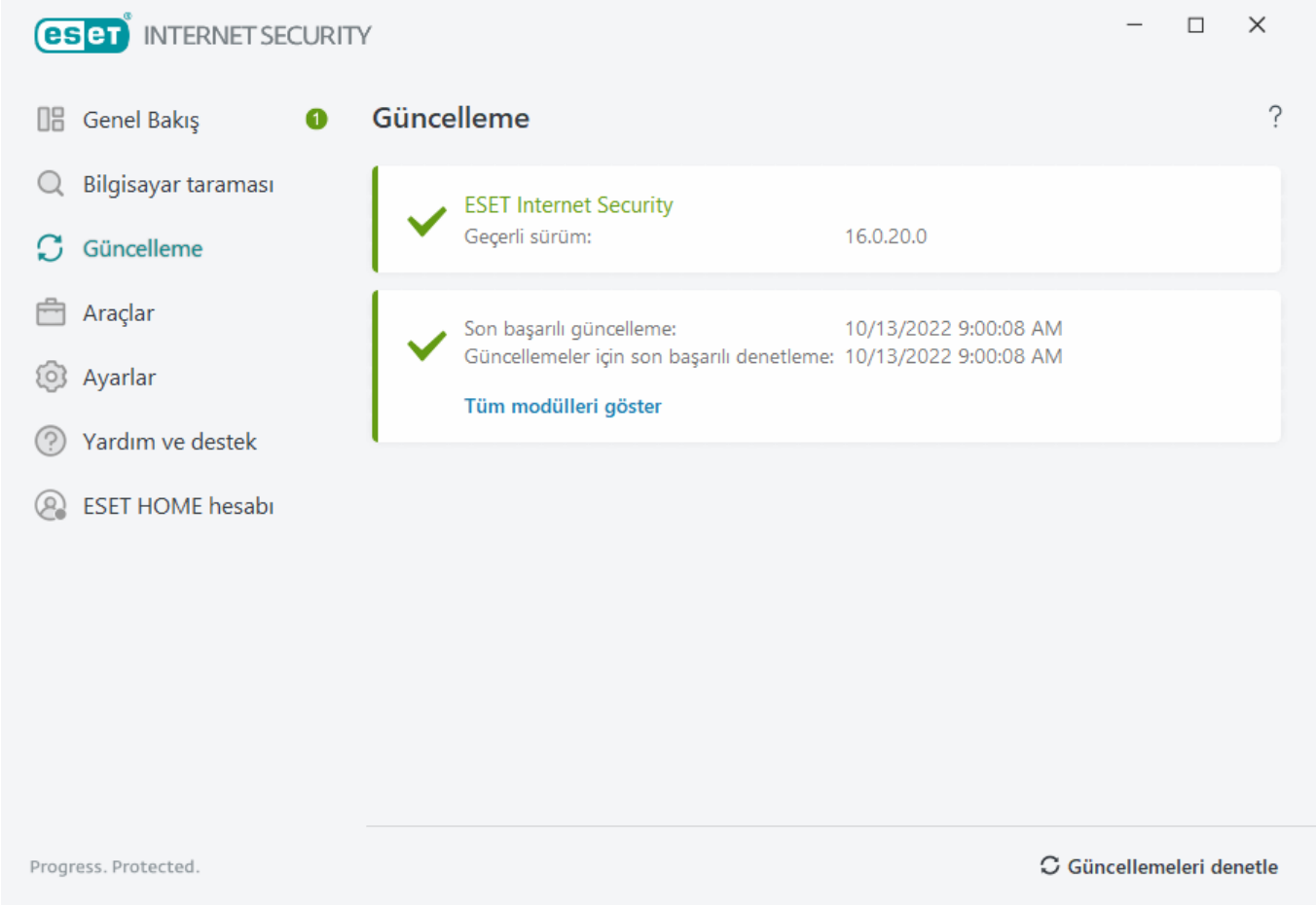
Önerilen çözümleri kullanarak sorunu çözemiyorsanız yardım dosyalarına erişmek için **Yardım ve destek** öğesini tıklayın veya ESET Bilgi Bankası'nda arama yapın. Hâlâ yardıma ihtiyacınız varsa destek isteği gönderebilirsiniz. ESET Teknik Destek ekibi sorularınızı hızla yanıtlar ve çözüm yolu bulunmasına yardımcı olur.

Güncellemeler

ESET Internet Security Ürününün düzenli olarak güncellenmesi, bilgisayarınızda maksimum güvenlik düzeyini sağlamak için en iyi yöntemdir. Güncelleme modülü hem program modüllerini hem de sistem bileşenlerini her zaman güncel tutmanıza olanak tanır.

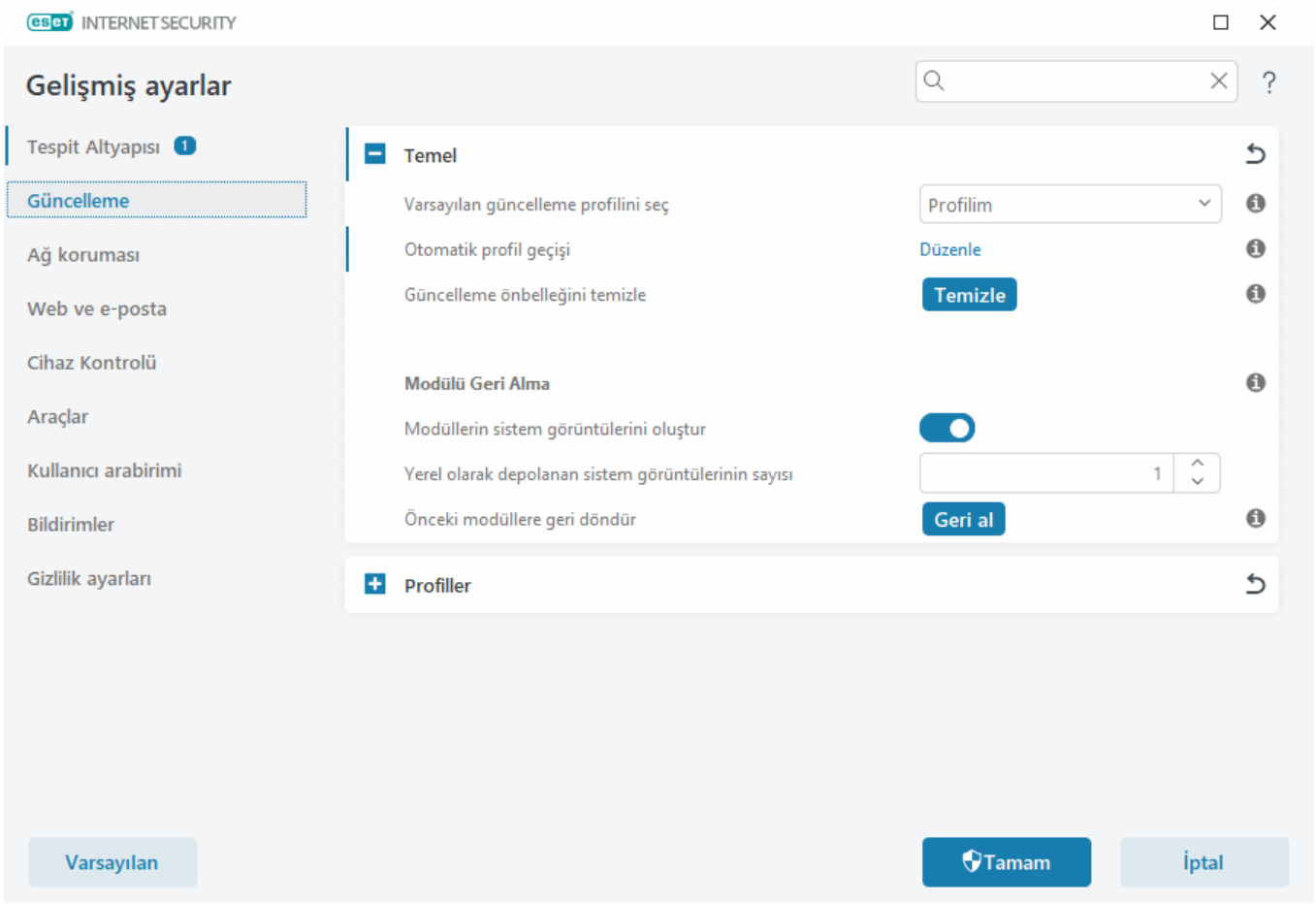
Ana program penceresinde **Güncelle** seçeneğini tıklatarak, son başarılı güncellemenin tarih ve saati ile güncelleme gerekip gerekmediği de dahil olmak üzere geçerli güncelleme durumunu görüntüleyebilirsiniz.

Otomatik güncellemelerin yanı sıra bir manuel güncellemeyi başlatmak için **Güncellemeleri kontrol edin** seçeneğini tıklayabilirsiniz.



Gelişmiş ayarlar penceresi (Ana menüden **Ayarlar**'ı, ardından **Gelişmiş ayarlar**'ı tıklayın veya klavyenizde **F5** tuşuna basın) ek güncelleme seçenekleri içerir. Güncelleme modu, proxy sunucu erişimi, LAN bağlantıları gibi gelişmiş güncelleme seçeneklerini yapılandırmak için Gelişmiş ayarlar ağacında **Güncelle**'yi tıklayın.

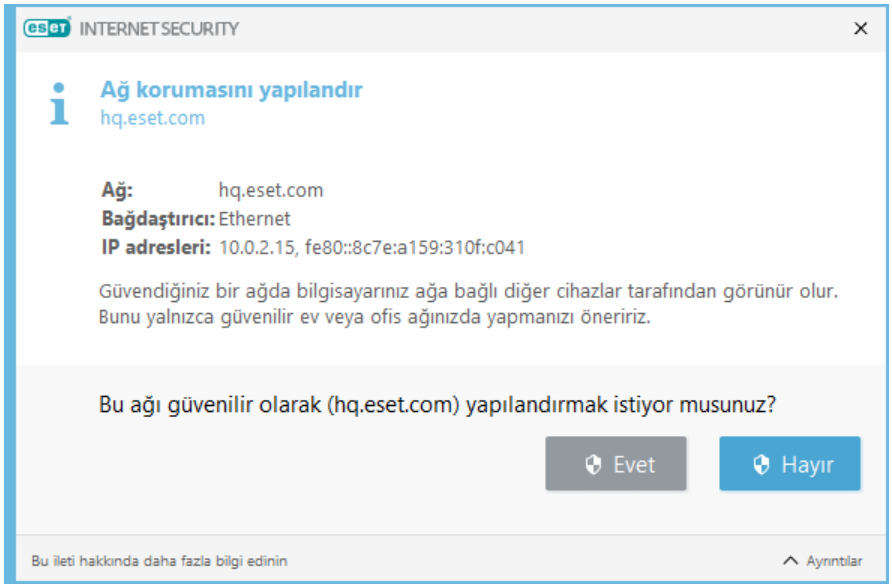
Güncellemeyle ilgili sorunlarla karşılaşırsanız güncelleme ön belleğini temizlemek için **Temizle**'yi tıklayın. Program modüllerini hala güncelleyemiyorsanız "Modül güncellemesi başarısız oldu" iletisi için sorun giderme bölümüne bakın.



Ağ korumasını yapılandır

Bir ağ ortamında bilgisayarınızın korunması için bağlı ağların yapılandırılması gerekmektedir. Paylaşıma izin vermek için ağ korumasını yapılandırarak diğer kullanıcıların bilgisayarınıza erişmesine izin verebilirsiniz. **Ayarlar** > **Ağ koruması** > **Bağlı ağlar** seçeneğine, ardından bağlı ağın altındaki bağlantıyı tıklayın. Seçilen ağı güvenilir olarak yapılandırmanıza olanak tanıyan seçeneklerin yer aldığı bir pencere gösterilir.

Varsayılan olarak, ESET Internet Security yeni bir ağ tespit edildiğinde Windows ayarlarını kullanır. Yeni bir ağ tespit edildiğinde iletişim penceresi görüntülemek için kullanıcıya sormak üzere Bilinen ağlar'da yeni ağların koruma türünü değiştirin. Bilgisayarınız yeni bir ağa her bağlandığında Ağ koruması yapılandırması gerçekleşir. Bu nedenle, genellikle Güvenilir bölgeleri tanımlamaya gerek yoktur.



Yapılandırma ağ koruması penceresinden seçebileceğiniz iki ağ koruma modu vardır:

- **Evet** - Güvenilir ağ (ev veya ofis ağı) için. Bilgisayarınız ve bilgisayarınızda depolanan paylaşılan dosyalar diğer ağ kullanıcıları tarafından görülür ve ağdaki diğer kullanıcılar sistem kaynaklarına erişilebilir. Güvenli bir yerel ağa erişirken bu ayarın kullanılması önerilir.

- **Hayır** - Güvenilir olmayan ağ (ortak ağ) için. Sisteminizdeki dosyalar ve klasörler ağdaki diğer kullanıcılarla paylaşılmaz veya bu kullanıcılar tarafından görülmez ve sistem kaynaklarının paylaşımı devre dışı bırakılır. Kablosuz ağlara erişirken bu ayarın kullanılması önerilir.

Hatalı bir ağ yapılandırması bilgisayarınız için güvenlik riski oluşturabilir.

Varsayılan olarak, güvenilir bir ağdaki iş istasyonlarına paylaşılan dosya ve yazıcılara erişim izni verilir, gelen RPC iletişimi etkinleştirilir ve uzak masaüstü paylaşımı kullanılabilir hale gelir.

Bu özellik hakkında daha fazla bilgi için şu ESET Bilgi Bankası makalesini okuyun:

- ESET Windows ev ürünlerinde ağ bağlantısı güvenlik duvarı ayarını değiştirme

Etkinleştir Anti-Theft

Evden işe veya başka kamusal alanlara yaptığımız günlük seyahatlerimizde kişisel cihazlarımız sürekli kaybolma veya çalınma riski altındadır. Anti-Theft cihazın kaybolması veya çalınması durumunda kullanıcı düzeyi güvenliği artıran bir özelliktir. Anti-Theft, ESET HOME portalındaki IP adresi ile yerini tespit etme özelliğini kullanarak kayıp cihazın kullanımını izlemenize ve cihazı takip etmenize olanak tanır, böylece cihazınızı geri alıp kişisel verilerinizi korumanıza yardımcı olur.

Anti-Theft, coğrafi IP adresi arama, web kamerası görüntüsü yakalama, kullanıcı hesabı koruması ve aygıt izleme gibi modern teknolojileri kullanarak, size ve bir emniyet kuruluşuna kaybolması veya çalınması durumunda bilgisayarınızı ya da aygıtınızı bulma konusunda yardımcı olabilir. ESET HOME portalında, bilgisayarınızda veya cihazınızda hangi etkinliklerin olduğunu görebilirsiniz.

ESET HOME portalında Anti-Theft ile ilgili daha fazla bilgi edinmek için ESET HOME Online Yardım'a bakın.

Anti-Theft, kullanıcı hesapları yönetimindeki kısıtlamalar nedeniyle etki alanlarındaki bilgisayarlarda düzgün çalışmayabilir.

Anti-Theft ürününü etkinleştirmek ve kaybolması veya çalınması durumunda cihazınızı korumak için aşağıdaki seçeneklerden birini belirleyin:

- Ürün yüklemesinin ardından, **Ek ESET güvenlik araçları ayarları** penceresinde, Anti-Theft aracını etkinleştirmek için **Anti-Theft** seçeneğinin yanındaki **Etkinleştir**'i tıklayın.
- Ana program penceresinde > **Genel bakış** ekranında "Anti-Theft kullanılabilir" mesajını görüyorsanız **Anti-Theft ürününü etkinleştir**'i tıklayın.
- Ana program penceresinden **Araçlar** > **Anti-Theft**'i tıklayın.
- Ana program penceresinden **Ayarlar** > **Güvenlik araçları**'nı tıklayın. Kaydırma çubuğu simgesi  **Anti-Theft**'i tıklayın ve ekrandaki talimatları uygulayın.

Cihazınız ESET HOME portalına bağlı değilse şunları yapmanız gerekir:
1. Anti-Theft ürününü etkinleştirirken ESET HOME hesabınıza giriş yapın.
2. Cihaz adı belirleyin.

Anti-Theft, Microsoft Windows Home Server'ı desteklemiyor.

Anti-Theft ürününü etkinleştirdikten sonra ana program penceresinde > **Araçlar** > **Anti-Theft** bölümünde cihazınızın güvenliğini optimize edebilirsiniz.

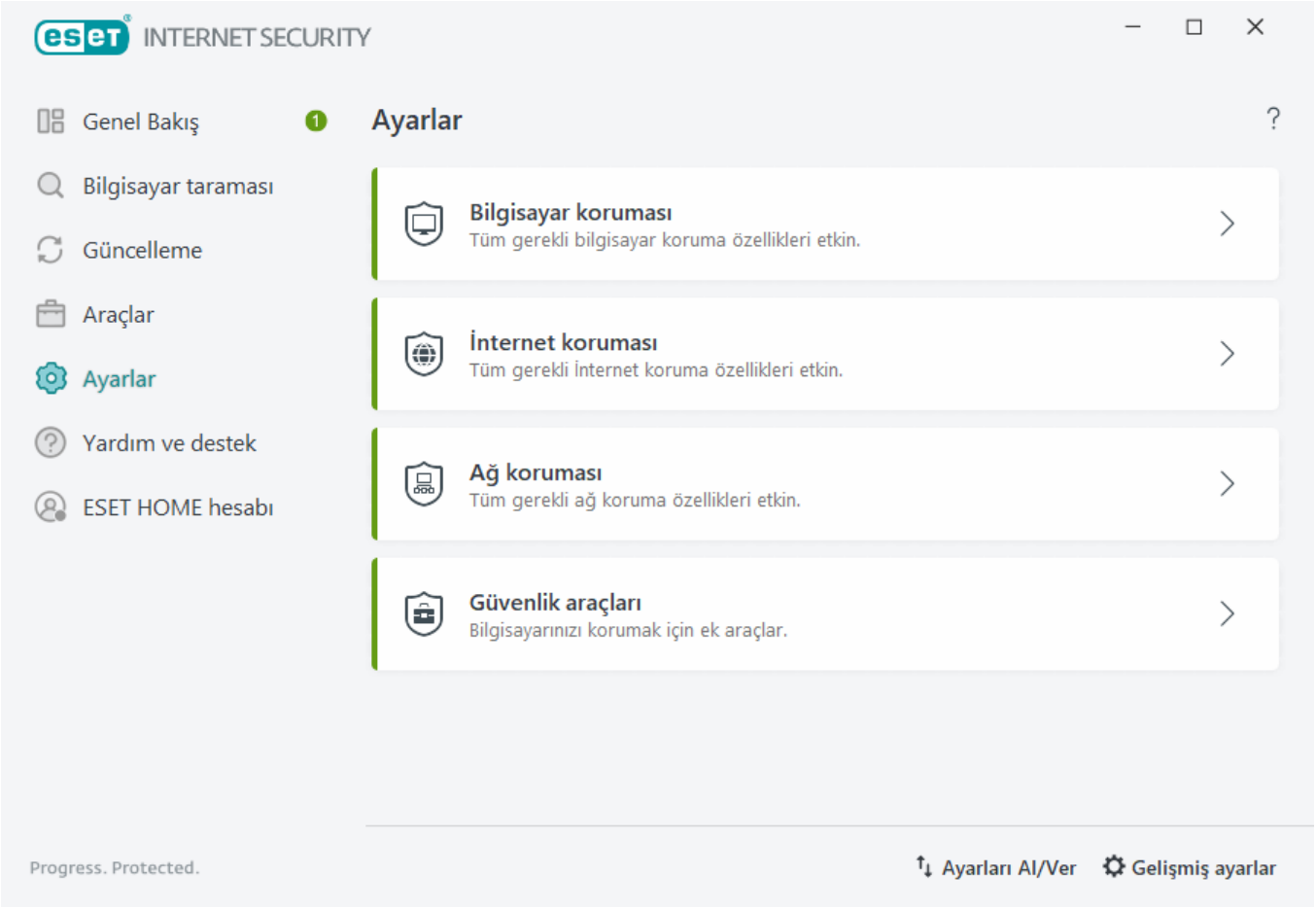
Ebeveyn kontrolü araçları

ESET Internet Security ürününde Ebeveyn kontrolünü zaten etkinleştirdiyseniz düzgün çalışması için Ebeveyn kontrolünü, ilgili tüm kullanıcı hesaplarına yönelik olarak da yapılandırabilirsiniz.

Ebeveyn kontrolü etkin olduğunda ve kullanıcı hesapları yapılandırılmamışsa ESET Internet Security, **Genel Bakış** ekranında "Ebeveyn kontrolü ayarlanmadı" bildirimi görüntüler. **Kuralları oluştur**'u tıklayın ve daha fazla bilgi için Ebeveyn kontrolü bölümüne bakın.

ESET Internet Security İle çalışma

ESET Internet Security ayar seçenekleri, bilgisayarınızın ve ağınızın koruma düzeylerini ayarlamanıza olanak verir.



Ayarlar menüsünde aşağıdaki bölümler bulunur:

Bilgisayar koruması

İnternet koruması

Ağ koruması

Güvenlik araçları

Bir bileşeni tıklatarak ilgili koruma modülünün gelişmiş ayarlarını yapılandırın.

Bilgisayar koruması ayarları, şu bileşenleri etkinleştirmenize veya devre dışı bırakmanıza olanak sağlar:

- **Gerçek zamanlı dosya sistemi koruması** – Tüm dosyalar açıldığında, oluşturulduğunda ve çalıştırıldığında kötü amaçlı koda karşı taranır.

- **Aygıt denetimi** – Bu modül, genişletilmiş filtreleri/izinleri taramanıza, engellemenize veya ayarlamanıza ve kullanıcının belirli bir aygıta (CD/DVD/USB...) nasıl erişim sağlayabileceğini ve aygıtı nasıl kullanabileceğini belirlemenize olanak sağlar.

- **Host Tabanlı Saldırı Önleme Sistemi (HIPS)** – HIPS sistemi işletim sistemindeki olayları izler ve bunlara özelleştirilmiş bir kurallar kümesine göre yanıt verir.

- **Oyun modu** – Oyun modunu etkinleştirir veya devre dışı bırakır. Oyun modunu etkinleştirdikten sonra bir uyarı iletisi (olası güvenlik riski) alırsınız ve ana pencere turuncuya döner.

- **Web Kamerası Koruması** – Bilgisayara bağlı kameraya erişimi olan işlem ve uygulamaları denetler.

İnternet koruması ayarları, şu bileşenleri etkinleştirmenize veya devre dışı bırakmanıza olanak sağlar:

- **Web erişimi koruması** – Etkinleştirilirse, HTTP veya HTTPS üzerinden iletilen tüm trafik kötü amaçlı yazılım için taranır.

- **E-posta istemci koruması** – POP3(S) ve IMAP(S) protokolü üzerinden alınan iletişimi izler.

- **Antispam koruması** – İstenmeyen (spam olan) e-postaları tarar.

- **Kimlik Avı Koruması** - Kullanıcıları gizli bilgilerini göndermeleri için kandırmaya yönelik içerik dağıttığından şüphelenilen web sitelerini filtreler.

Ağ koruması bölümü, Güvenlik duvarını, Ağ Saldırısı Koruması (IDS) ve Botnet korumasını etkinleştirmenize veya devre dışı bırakmanıza izin verir.

Güvenlik araçları ayarları, aşağıdaki modülleri ayarlamanıza olanak sağlar:

- **Bankacılık ve Ödeme Sistemleri Koruması** - Çevrim içi işlemler sırasında finansal verilerinizi korumak için tasarlanmış ek bir tarayıcı koruması katmanı sunar. Desteklenen tüm web tarayıcılarını güvenli modda başlatmak için **Tüm tarayıcıları güvenli hale getir**'i etkinleştirin. Daha fazla bilgi için Bankacılık ve Ödeme Sistemleri Koruması'na bakın.

- **Anti-Theft** - Kayıp veya hırsızlık durumunda bilgisayarınızı korumak için Anti-Theft özelliğini etkinleştirin.

Ebeveyn kontrolü, olası saldırgan materyaller içerebilecek web sayfalarını engellemenize izin verir. Ayrıca ebeveynler 40'tan fazla önceden tanımlanmış web sitesi kategorisine ve 140'ın üstünde alt kategoriye erişimi yasaklayabilir.

Devre dışı bırakılan bir güvenlik bileşenini tekrar etkinleştirmek için kaydırıcıyı  tıklatın, Etkinleştirilen güvenlik bileşeni yeşil bir anahtar simgesi  içerir.

Ayarlar penceresinin alt kısmında ek seçenekler bulunur. Her bir modül için daha ayrıntılı parametreler ayarlamak üzere **Gelişmiş ayarlar** bağlantısını kullanın. .xml yapılandırma dosyası kullanan ayar parametrelerini yüklemek veya yapılandırma dosyasına geçerli ayar parametrelerinizi kaydetmek için Ayarları Al/Ver öğesini kullanın.

Bilgisayar koruması

Tüm koruma modüllerinin genel görünümüne erişmek için **Ayarlar** penceresinden **Bilgisayar Koruması**'nı tıklayın:

- Gerçek zamanlı dosya sistemi koruması

- Aygıt denetimi

- HIPS

- Oyun modu

- Web kamerası koruması

Koruma modüllerini tek tek duraklatmak veya devre dışı bırakmak için kaydırma çubuğunu tıklayın.

Koruma modüllerini kapatmak, bilgisayarınızın koruma düzeyini düşürebilir.

Koruma modülünün yanındaki dişli simgesini tıklayarak bu modülün gelişmiş ayarlarına erişebilirsiniz.

Gerçek zamanlı dosya sistemi koruması için dişli simgesini tıklayın ve aşağıdaki seçeneklerden birini belirleyin:

- **Yapılandır** - Gerçek zamanlı dosya sistemi koruması Gelişmiş ayarları açılır.
- **Tarama dışı öğeleri düzenle** - Dosya ve klasörleri tarama dışında bırakmanız için Tarama dışı bırakma ayarları penceresi açılır.

Webcam koruması için dişli simgesini tıklayın ve aşağıdaki seçeneklerden birini belirleyin:

- **Yapılandır** - Webcam koruması Gelişmiş ayarları açılır.
- **Yeniden başlatmaya kadar tüm erişimi engelle** - Bilgisayar yeniden başlatana kadar Web kamerasına tüm erişim engellenir.
- **Tüm erişimi kalıcı olarak engelle** - Bu ayar devre dışı bırakılana kadar Web Kamerasına tüm erişim engellenir.
- **Tüm erişimi engellemeyi durdur** - Web kamerası erişiminin engellemesi devre dışı bırakılır. Bu seçenek yalnızca Web kamerası erişimi engellenmişse kullanılabilir.

Antivirus ve antispyware korumasını duraklat - Tüm antivirus ve antispyware koruma modüllerini devre dışı bırakır. Korumayı devre dışı bıraktığınızda açılan pencerede **Zaman aralığı** açılır menüsünü kullanarak korumanın ne kadar süre boyunca devre dışı olacağını belirleyebilirsiniz. Yalnızca deneyimli bir kullanıcıysanız veya ESET Teknik Destek ekibi tarafından talimat aldıysanız bunu kullanın.

Algılama altyapısı

Algılama altyapısı dosyayı, e-postayı ve internet iletişimini kontrol ederek kötü amaçlı sistem saldırılarına karşı koruma sağlar. Örneğin zararlı yazılım olarak sınıflandırılan bir nesne algılandığında düzeltme işlemi başlatılır. Algılama altyapısı bu nesneyi önce engelleyerek, ardından temizleyerek, silerek veya karantinaya alarak bertaraf edebilir.

Algılama altyapısı ayarlarını ayrıntılı olarak yapılandırmak için **Gelişmiş Ayarlar**'ı tıklayın veya **F5** tuşuna basın.

Algılama altyapısı ayarlarındaki değişiklikler yalnızca deneyimli bir kullanıcı tarafından yapılmalıdır. Ayarların yanlış yapılandırılması, koruma düzeyinin düşmesine neden olabilir.

Bu bölümde:

- Gerçek zamanlı ve makine öğrenimi koruması kategorileri
- Kötü amaçlı yazılım taramaları
- Raporlama ayarları
- Koruma ayarları

Gerçek zamanlı ve makine öğrenimi koruması kategorileri

Tüm koruma modülleri için **Gerçek zamanlı ve makine öğrenimi koruması** (örneğin, Gerçek zamanlı dosya sistemi koruması, Web erişimi koruması, ...) aşağıdaki kategorilerin raporlama ve koruma düzeylerini yapılandırmanıza olanak tanır.

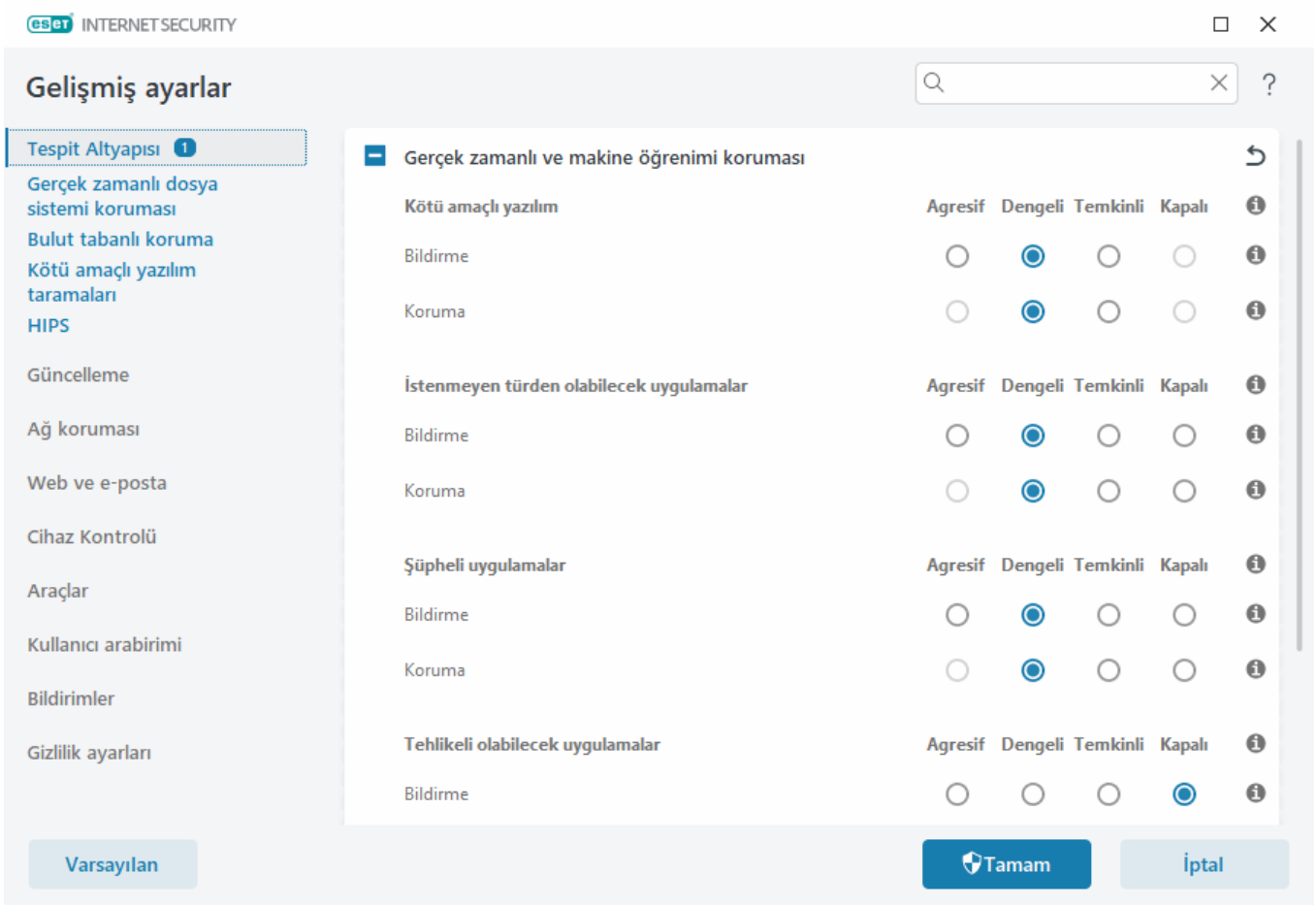
- **Kötü amaçlı yazılım** – Bilgisayar virüsü bilgisayarınızda bulunan dosyaların önüne veya arkasına eklenen kötü amaçlı bir kod parçasıdır. Ancak, "virüs" terimi çoğu zaman yanlış kullanılır. "Kötü amaçlı yazılım" (zararlı yazılım) daha doğru bir terimdir. Kötü amaçlı yazılım algılaması, makine öğrenimi bileşeniyle birlikte algılama altyapısı modülü tarafından gerçekleştirilir. Bu uygulama türleriyle ilgili daha fazla bilgi için Sözlüğe başvurabilirsiniz.

- **İstenmeyen türden olabilecek uygulamalar** – Grayware veya istenmeyen türden olabilecek uygulamalar (PUA'lar), niyeti virüs veya truva atları gibi diğer kötü amaçlı yazılım türleri kadar kesin şekilde kötü olmayan geniş bir yazılım kategorisidir. Ancak bu yazılımlar istenmeyen ek yazılımları indirebilir, dijital aygıtın davranışını değiştirebilir veya kullanıcı tarafından onaylanmayan veya beklenmeyen işlemleri gerçekleştirebilir. Bu uygulama türleriyle ilgili daha fazla bilgi için Sözlüğe başvurabilirsiniz.

- **Şüpheli uygulamalar** - Şüpheli uygulamalara paketleyiciler veya koruyucularla sıkıştırılmış programlar dahildir. Bu tür koruyuculardan genellikle kötü amaçlı program yazarları, algılanmadan kaçınmak için faydalanır.

- **Tehlikeli olabilecek uygulamalar** – Kötü amaçlı olarak yanlış bir şekilde kullanılabilme olasılığına sahip yasal

ticari yazılım anlamına gelir. Tehlikeli olabilecek uygulamalara (PUA'lara) uzaktan erişim araçları, parola kırma uygulamaları ve tuş kaydeden uygulamalar (kullanıcı tarafından yazılan her tuş vuruşunu kaydeden programlar) örnek olarak verilebilir. Bu uygulama türleriyle ilgili daha fazla bilgi için Sözlüğe başvurabilirsiniz.



İyileştirilmiş koruma

Gelişmiş makine öğrenimi, makine öğrenimine dayalı olarak algılamayı iyileştiren gelişmiş bir koruma katmanı olarak algılama altyapısının bir parçası olarak sunulmaktadır. Bu koruma türüyle ilgili daha fazla bilgi için Sözlüğe başvurun.

Kötü amaçlı yazılım taramaları

Tarayıcı ayarları gerçek zamanlı tarama ve isteğe bağlı tarama için ayrı ayrı yapılandırılabilir. Varsayılan olarak, **Gerçek zamanlı koruma ayarlarını kullan** ayarı etkindir. Etkinleştirildiğinde alakalı İsteğe bağlı tarama ayarları **Gerçek zamanlı ve makine öğrenimi koruması** bölümünden alınır. Daha fazla bilgi için zararlı yazılım taramaları'na bakın.

Raporlama ayarları

Bir algılama görüldüğünde (ör. bir tehdit bulunduğunda ve kötü amaçlı yazılım olarak sınıflandırıldığında), bilgiler Algılama günlüğüne kaydedilir ve ESET Internet Security ürününde yapılandırılmış olması halinde Masaüstü bildirimleri gösterilir.

Raporlama eşiği her kategori için yapılandırılır (bunlara "KATEGORİ" adı verilir):

1.Zararlı yazılım

2.İstenmeyen türden olabilecek uygulamalar

3.Tehlikeli olabilecek uygulamalar

4.Şüpheli uygulamalar

Raporlama, makine öğrenimi bileşeniyle birlikte algılama altyapısında gerçekleştirilir. Mevcut koruma eşiğinden daha yüksek bir raporlama eşiği ayarlayabilirsiniz. Bu raporlama ayarları nesneleri engellemeyi, temizlemeyi veya silmeyi etkilemez.

KATEGORİ raporlaması için bir eşiği (veya düzeyi) değiştirmeden önce aşağıdakileri okuyun:

Eşik	Açıklama
Saldırgan	KATEGORİ raporlaması maksimum hassasiyet düzeyine ayarlanır. Daha fazla algılama bildirilir. **Agresif** ayar, nesneleri hatalı bir şekilde KATEGORİ olarak tanımlayabilir.
Dengeli	KATEGORİ raporlaması dengeli olarak ayarlanır. Bu ayar, performansı dengelemek ve algılama oranlarını ve hatalı bir şekilde bildirilen nesnelerin sayısını doğru bildirecek şekilde optimize edilir.
Temkinli	KATEGORİ raporlaması, yeterli bir koruma düzeyi sunarken hatalı bir şekilde bildirilen nesnelerin sayısını en düşük düzeye indirecek şekilde yapılandırılır. Nesneler yalnızca çok yüksek bir olasılık olduğunda ve KATEGORİ davranışıyla eşleştiğinde bildirilir.
Kapalı	CATEGORY için raporlama düzeyi etkin değildir ve bu türden algılamalar bulunmaz, bildirilmez veya temizlenmez. Bunun sonucunda bu ayar, korumayı bu algılama türü için devre dışı bırakır. Kapalı modu zararlı yazılım raporlaması için mevcut değildir ve tehlikeli olabilecek uygulamalar için varsayılan değerdir.

ESET Internet Security koruma modüllerinin kullanılabilirliği

Belirli bir KATEGORİ eşiği için koruma modülünün (etkin veya devre dışı) kullanılabilirliği aşağıdaki gibidir:

	Saldırgan	Dengeli	Temkinli	Kapalı**
Gelişmiş makine öğrenimi modülü*	✓ (agresif mod)	✓ (temkinli mod)	X	X
Algılama altyapısı modülü	✓	✓	✓	X
Diğer koruma modülleri	✓	✓	✓	X

* ESET Internet Security sürüm 13.1 ve üzeri yazılımlarda mevcuttur.
** Önerilmez

Ürün sürümü, program modülü sürümleri ve yapı tarihlerini belirleyin

1. **Yardım ve destek** > **ESET Internet Security Hakkında**'yı tıklayın.
2. **Hakkında** bölümünde metnin ilk satırı ESET ürününüzün sürüm numarasını gösterir.
3. Belirli modüllerle ilgili bilgilere erişmek için **Yüklenen bileşenler**'i tıklayın.

Önemli noktalar

Ortamınız için uygun bir eşik değer ayarlarken göz önüne alınacak önemli noktalar:

- **Dengeli** eşik ayarların çoğu için önerilir.

• **Temkinli** eşik, önceki ESET Internet Security sürümlerine (13.0 ve aşağısı) benzer bir koruma düzeyini temsil eder. Bu, güvenlik yazılımı tarafından hatalı şekilde tanımlanan nesnelerin sayısını en düşük düzeye indirmeye öncelik verilen ortamlar için önerilir.

• Yüksek raporlama eşiği daha yüksek bir algılama oranı sunsa da hatalı bir şekilde tanımlanan nesnelerin sayısını artırabilir.

• Gerçek dünya perspektifinden bakıldığında temiz nesnelerin zararlı yazılım olarak yanlış bir şekilde sınıflandırılmasını tamamen önlemek mümkün olmadığı gibi algılama oranının %100 olması da garanti edilemez.

• ESET Internet Security Vve modüllerini güncel halde tutarak performans ve algılama oranlarının doğruluğu arasındaki dengeyi en üst düzeye çıkarırken hatalı bildirilen nesnelerin sayısını en düşük düzeye indirin.

Koruma ayarları

CATEGORY olarak sınıflandırılan bir nesne bildirildiğinde program nesneyi engeller ve ardından temizler, siler ya da Karantinaya alır.

KATEGORİ koruması için bir eşiği (veya düzeyi) değiştirmeden önce aşağıdakileri okuyun:

Eşik	Açıklama
Saldırgan	Bildirilen agresif (veya daha düşük) düzeydeki algılamalar engellenir ve otomatik düzeltme (örneğin temizleme) başlatılır. Bu ayar, tüm uç noktalar agresif ayarlarla tarandığında ve hatalı olarak bildirilen nesneler algılama istisnalarına eklendiğinde önerilir.
Dengeli	Bildirilen dengeli (veya düşük) seviyedeki algılamalar engellenir ve otomatik düzeltme (örneğin temizleme) başlatılır.
Temkinli	Bildirilen temkinli algılamalar engellenir ve otomatik düzeltme (örneğin temizleme) başlatılır.
Kapalı	Yanlışlıkla bildirilen nesnelerin tespit edilmesi ve tarama dışı bırakılması için kullanılabilir. Kapalı modu zararlı yazılım koruması için mevcut değildir ve tehlikeli olabilecek uygulamalar için varsayılan değerdir.

ESET Internet Security 13.0 ve aşağı sürümler için dönüşüm tablosu

13.0 ve aşağı sürümlerden 13.1 ve üzeri sürümlere yükseltirken yeni eşik durumu aşağıdaki gibidir:

Yükseltme öncesi kategori anahtarı		
Yükseltme sonrası yeni KATEGORİ eşiği	Dengeli	Kapalı

Algılama altyapısı gelişmiş seçenekleri

Anti-Stealth teknolojisi kendini işletim sisteminden gizleyebilen kök setleri gibi tehlikeli programları algılamayı sağlayan gelişmiş bir sistemdir. Bu, antivirus uygulamasının standart test tekniklerini kullanarak bunları algılayamadığı anlamına gelir.

AMSI üzerinden gelişmiş taramayı etkinleştir; PowerShell komut dosyalarının, Windows Script Host tarafından yürütülen komut dosyalarının ve AMSI SDK'sı (yalnızca Windows 10'da) kullanılarak taranan verilerin taranmasını

sağlayan Microsoft Antimalware Scan Arabirimi aracıdır.

Sızıntı algılandı

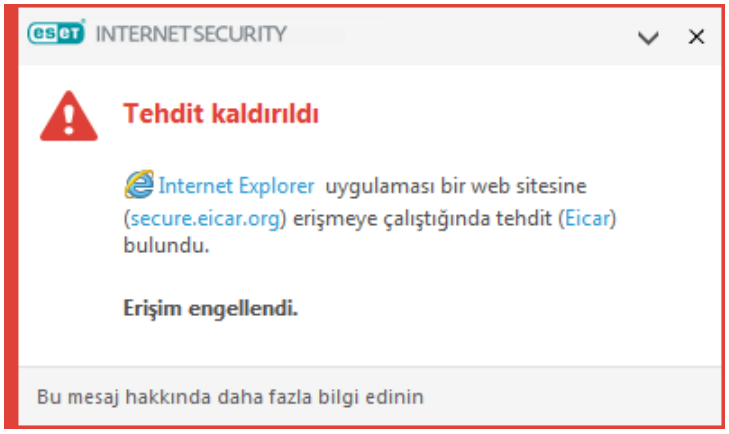
Sızıntılar sisteme web sayfaları, paylaşılan klasörler, e-posta veya çıkarılabilir aygıtlar (USB, harici diskler, CD, DVD, vb.) gibi çeşitli giriş noktalarından ulaşabilir.

Standart davranış

Sızıntıların, ESET Internet Security tarafından nasıl işlendiğine dair genel bir örnek olarak, sızıntılar şunların kullanımıyla algılanabilir:

- Gerçek zamanlı dosya sistemi koruması
- Web erişimi koruması
- E-posta istemci koruması
- İsteğe bağlı bilgisayar taraması

Bunların her biri standart temizleme düzeyini kullanır ve dosyayı temizleyip Karantinaya taşımaya veya bağlantıyı sonlandırmaya çalışır. Ekranın sağ alt köşesindeki bildirim alanında bir bildirim penceresi görüntülenir. Tespit edilen/temizlenen nesnelerle ilgili ayrıntılı bilgiler için Günlük dosyaları bölümüne bakın. Temizleme düzeyleri ve davranışı ile ilgili daha fazla bilgi için Temizleme bölümüne bakın.



Enfekte olan dosyalar için bilgisayarı tarama

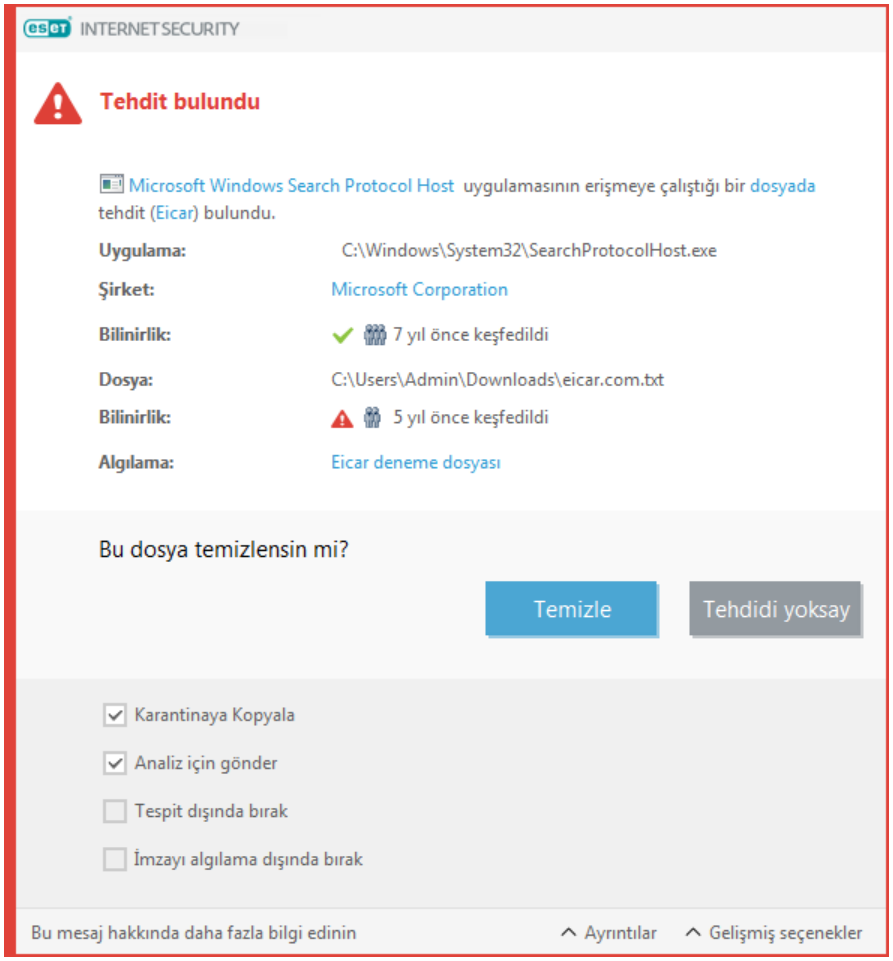
Bilgisayarınız yavaşlama, sık sık donup kalma gibi kötü amaçlı yazılımdan etkilenme işaretleri gösteriyorsa, şunları yapmanızı öneririz:

1. ESET Internet Security uygulamasını açıp **Bilgisayar taraması**'nı tıklatın.
2. **Bilgisayarınızı tarayın**'ı tıklatın (daha fazla bilgi için Bilgisayar taraması bölümüne bakın).
3. Tarama bittikten sonra taranan, etkilenen ve temizlenen dosyaların sayısını görmek için günlüğü inceleyin.

Diskinizin yalnızca belirli bir bölümünü taramak istiyorsanız **Özel tarama**'yı tıklatın ve virüs taraması yapılacak hedefleri belirleyin.

Temizleme ve silme

Gerçek zamanlı dosya sistemi korumasının gerçekleştireceği önceden tanımlı bir eylem yoksa, uyarı penceresinde bir seçenek belirlemeniz istenir. Genellikle, **Temizle**, **Sil** ve **Eylem yok** seçenekleri kullanılabilir. Etkilenen dosyaları temizlenmemiş olarak bırakacağından **Eylem yok** seçeneğinin belirlenmesi önerilmez. Burada geçerli olan özel durum, dosyanın zararsız olduğundan ve yanlışlıkla algılandığından emin olduğunuz durumdur.



Bir dosya, kendisine kötü amaçlı kod ekleyen bir virüsün saldırısına uğradıysa temizleme işlemi uygulayın. Durum buysa, öncelikle etkilenen dosyayı özgün durumuna geri yüklemek için temizlemeyi deneyin. Dosya tümüyle kötü amaçlı kod içeriyorsa silinir.

Etkilenen dosya bir sistem işlemi tarafından "kilitlendiyse" veya kullanılıyorsa, genellikle ancak serbest bırakıldıktan sonra silinir (normalde sistem yeniden başlatıldıktan sonra).

Karantinadan geri yükleme

Karantinaya ESET Internet Security ana program penceresinden **Araçlar** > **Diğer araçlar** > **Karantina** öğeleri tıklanarak erişilebilir.

Karantinaya alınan dosyalar da orijinal konumlarına geri yüklenebilir:

- Bunun için, Karantinadaki belirli bir dosyayı sağ tıklayarak içerik menüsünden **Geri Yükle** özelliğini kullanın.
- Bir dosya istenmeyen türden olabilecek uygulama olarak işaretlenmişse, **Geri yükle ve tarama dışı bırak** seçeneği etkinleştirilir. Ayrıca Tarama dışı bırakma bölümüne de bakın.

• İçerik menüsü **Şuna geri yükle** seçeneğini de sunar. Bu seçenek, bir dosyayı silindiği konumdan başka bir konuma geri yüklemenize olanak tanır.

• Geri yükleme işlevi bazı durumlarda (örneğin, salt okunur ağ paylaşımında bulunan dosyalar için) kullanılamaz.

Birden çok tehdit

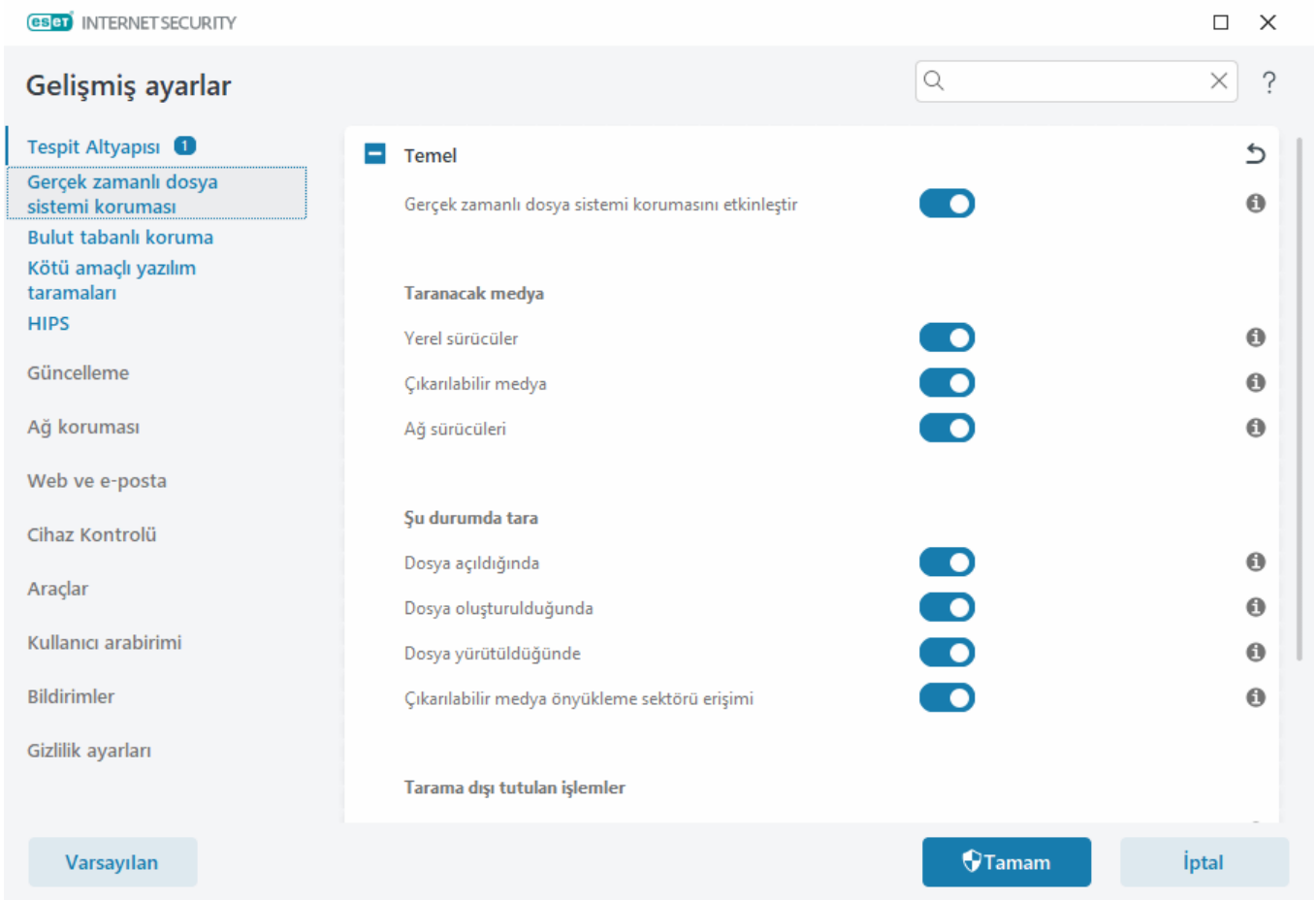
Etkilenen dosyalar Bilgisayar taraması sırasında temizlenmediyse (veya Temizleme düzeyi **Temizleme Yok** olarak ayarlandıysa), bir uyarı penceresi, görüntülenen dosyalar için eylem seçmenizi ister. Dosyalar için eylemleri seçin (eylemler listedeki her dosya için ayrı ayrı belirlenir) ve sonra **Son** seçeneğini tıklatın.

Arşivlerdeki dosyaları silme

Varsayılan temizleme modunda, arşiv ancak yalnızca etkilenen dosyalar içeriyor ve temiz dosya içermiyorsa tümüyle silinir. Başka bir deyişle, arşivler zararsız temiz dosyalar da içeriyorsa silinmez. Katı kurallı temizleme taraması gerçekleştirirken dikkatli olun; Katı kurallı temizleme etkinken arşivde tek bir etkilenen dosya bulunsa bile, arşivdeki diğer dosyaların durumuna bakılmaksızın arşiv tümüyle silinir.

Gerçek zamanlı dosya sistemi koruması

Gerçek zamanlı dosya sistemi koruması, sistemde açılan, oluşturulan veya çalıştırılan tüm dosyaları kötü amaçlı kodlara karşı kontrol eder.



Varsayılan olarak, Gerçek zamanlı dosya sistemi koruması sistem başlatılırken başlatılır ve kesintisiz tarama sağlar.

Algılama altyapısı > **Gerçek zamanlı dosya sistemi koruması** > **Temel** altındaki **Gelişmiş ayarlar** içinde **Gerçek zamanlı dosya sistemi koruması** seçeneğinin devre dışı bırakılmasını önermeyiz.

Taranacak medya

Varsayılan olarak tüm medya türleri olası tehditlere karşı denetlenir:

- **Yerel sürücüler** – Tüm sistemi ve kalıcı sabit sürücüleri tarar (örnek: *C:*\, *D:*\).
- **Çıkarılabilir medya** – CD/DVD'leri, USB depolamasını, bellek kartlarını vs. tarar.
- **Ağ sürücüleri** – İşaretlenen tüm ağ sürücülerini (örnek: *store04* olarak *H:*\ sürücüsünü) veya doğrudan erişilen ağ sürücülerini (örnek: *store08* sürücüsünü) tarar.

Varsayılan ayarları kullanmanızı ve yalnızca belirli durumlarda (örneğin belirli medya türlerini denetlerken veri aktarımı önemli ölçüde yavaşladığında) değiştirmenizi öneririz.

Şu durumda tara

Varsayılan olarak tüm dosyalar açıldığında, oluşturulduğunda veya yürütülürken taranır. Bilgisayarınız için en üst düzeyde gerçek zamanlı koruma sağladığından, şu varsayılan ayarları korumanızı öneririz:

- **Dosya açıldığında** – Bir dosya açıldığında tarar.
- **Dosya oluşturulduğunda** – Oluşturulan veya değiştirilen bir dosyayı tarar.
- **Dosya yürütüldüğünde** – Bir dosya yürütüldüğünde veya çalıştırıldığında tarar.
- **Çıkarılabilir medya önyükleme kesimi erişimi** – Önyükleme kesimi içeren bir çıkarılabilir medya cihaza takıldığında önyükleme kesimi hemen taranır. Bu seçenek, çıkarılabilir medya dosyası taramasını etkinleştirmez. Çıkarılabilir medya dosyası taraması **Taranacak medya** > **Çıkarılabilir medya** bölümünde bulunur. **Çıkarılabilir medya önyükleme kesimi erişiminin** düzgün çalışması için ThreatSense parametrelerinde **Önyükleme kesimleri/UEFI**'yi etkin halde bırakın.

Gerçek zamanlı sistem koruması her medya türünü kontrol eder ve bir dosyaya erişme gibi çeşitli sistem olayları tarafından tetiklenir. ThreatSense teknolojisi algılama yöntemleri kullanıldığında (ThreatSense motoru parametre ayarları bölümünde açıklandığı gibi), Gerçek zamanlı dosya sistemi koruması, yeni oluşturulmuş dosyalarda, mevcut olanlardan daha farklı işlem uygulayacak şekilde yapılandırılabilir. Örneğin, Gerçek zamanlı dosya sistemi korumasını yeni oluşturulmuş dosyaları daha yakından izleyecek şekilde yapılandırabilirsiniz.

Gerçek zamanlı koruma kullanılırken sistem kaynaklarının minimum düzeyde kullanılmasını sağlamak için, zaten taranmış olan dosyalar sürekli olarak taranmaz (değiştirilmedikleri sürece). Her algılama altyapısı güncellemesinden sonra dosyalar hemen tekrar taranır. Bu davranış**Akıllı optimizasyon** kullanılarak denetlenir. Bu **Akıllı optimizasyon** devre dışı bırakılırsa tüm dosyalar her erişildiğinde taranır. Bu seçeneği değiştirmek isterseniz, **F5** tuşuna basarak **Gelişmiş ayarları** açın ve **Algılama altyapısı** > **Gerçek zamanlı dosya sistemi koruması** seçeneğini genişletin. **ThreatSense parametresi** > **Diğer** öğesine tıklatın ve **Akıllı optimizasyonu etkinleştir** seçeneğinin işaretini seçin veya seçimini kaldırın.

Temizleme düzeyleri

İstenen bir koruma modülü için temizleme düzeyi ayarlarına erişmek üzere **ThreatSense parametreleri**'ni (örneğin, **Gerçek zamanlı dosya sistemi koruması**)genişletin ve **Temizleme > Temizleme düzeyi**'ni bulun.

ThreatSense parametreleri aşağıdaki düzeltme (yani temizlik) düzeylerine sahiptir.

ESET Internet Security Ürününde Düzeltme

Temizleme düzeyi	Açıklama
Algılamayı her zaman düzelt	Herhangi bir son kullanıcı müdahalesi olmadan, nesneler temizlenirken algılamayı düzeltme girişimi. Bazı nadir durumlarda (örneğin sistem dosyaları), tespit düzeltilemezse bildirilen nesne orijinal konumunda bırakılır.
Güvenliyse algılamayı düzelt, değilse olduğu gibi bırak	Herhangi bir son kullanıcı müdahalesi olmadan nesneler temizlenirken algılamayı düzeltme girişimi. Bazı durumlarda (örneğin, sistem dosyaları veya hem temiz hem de etkilenmiş dosyalar bulunan arşivler), algılama düzeltilemezse bildirilen nesne orijinal konumunda bırakılır.
Güvenliyse algılamayı düzelt, değilse sor	Nesneler temizlenirken algılamayı düzeltme girişimi. Bazı durumlarda hiçbir işlem gerçekleştirilmezse son kullanıcı interaktif bir uyarı alır ve bir düzeltme işlemi seçmelidir (örneğin, silme veya yoksayma gibi). Bu ayar çoğu durum için önerilir.
Her zaman son kullanıcıya sor	Son kullanıcı, nesneler temizlenirken interaktif bir pencere görüntüler ve bu pencerede bir uyumlulaştırma işlemi seçmeleri gerekir (örneğin silme veya yoksayma). Bu düzey, bir algılama durumunda atılacak adımları bilen daha ileri seviye kullanıcılar için tasarlanmıştır.

Gerçek zamanlı koruma yapılandırması ne zaman değiştirilir

Gerçek zamanlı koruma, güvenli bir sistemi korumanın en temel bileşenidir. Parametrelerini değiştirirken dikkatli olun. Bu parametrelerin yalnızca özel durumlarda değiştirilmesi önerilir.

ESET Internet Security Yüklendikten sonra, kullanıcılara en üst düzeyde sistem güvenliği sağlamak için tüm ayarlar en iyi duruma getirilir. Varsayılan ayarları geri yüklemek için penceredeki her sekmenin yanında bulunan simgesini tıklayın (**Gelişmiş ayarlar** > **Algılama altyapısı** > **Gerçek zamanlı dosya sistemi koruması**).

Gerçek zamanlı korumayı denetleme

Gerçek zamanlı korumanın çalıştığını ve virüsleri algıladığını doğrulamak için *www.eicar.com* tarafından sağlanan sınama dosyasını kullanın. Bu sınama dosyası tüm antivirus programları tarafından algılanabilen, zararsız bir dosyadır. Dosya, EICAR şirketi (European Institute for Computer Antivirus Research) tarafından antivirus programlarının işlevselliğini sınamak için oluşturulmuştur.

Dosya şuradan indirilebilir: http://www.eicar.org/download/eicar.com
Bu URL'yi tarayıcınıza girdikten sonra tehdidin kaldırıldığını bildiren bir mesaj alırsınız.

Gerçek zamanlı koruma çalışmıyorsa neler yapılabilir

Bu bölümde, gerçek zamanlı koruma kullanılırken oluşabilecek sorunları ve bu sorunları nasıl gidereceğinizi açıklıyoruz.

Gerçek zamanlı koruma devre dışı bırakılmış

Gerçek zamanlı koruma kullanıcı tarafından yanlışlıkla devre dışı bırakıldıysa özelliği yeniden etkinleştirmeniz gerekir. Gerçek zamanlı korumayı yeniden etkinleştirmek için ana program penceresinde **Ayarlar**'a gidin ve **Bilgisayar koruması** > **Gerçek zamanlı dosya sistemi koruması** öğesini tıklayın.

Gerçek zamanlı koruma sistem başlangıcında başlatılmıyorsa bunun nedeni genellikle **Gerçek zamanlı dosya sistemi korumasını etkinleştir** seçeneğinin devre dışı bırakılmış olmasıdır. Bu seçeneğin etkinleştirildiğinden emin olmak için **Gelişmiş Ayarlar**'a gidin (**F5**) ve **Algılama altyapısı** > **Gerçek zamanlı dosya sistemi koruması** seçeneğini tıklayın.

Gerçek zamanlı koruma sızıntıları algılamıyor ve temizlemiyorsa

Bilgisayarınızda başka antivirüs programları yüklü olmadığından emin olun. İki antivirus programı aynı anda yüklüyse birbirleriyle çakışabilir. ESET'i kurmadan önce sisteminizdeki diğer antivirüs programlarını kaldırmanızı öneririz.

Gerçek zamanlı koruma başlamıyor

Gerçek zamanlı koruma, sistem başlatılırken başlamıyorsa (ve **Gerçek zamanlı dosya sistemi korumasını etkinleştir** seçeneği etkinse), bunun nedeni diğer programlarla çakışmalar olabilir. Bu sorunu çözmek için ESET SysInspector günlüğü oluşturun ve bunu analiz için ESET Teknik Destek birimine gönderin.

Tarama dışı tutulan işlemler

Tarama dışı bırakılan süreçler özelliği, uygulama süreçlerini Gerçek zamanlı dosya sistemi korumasından hariç tutmanıza olanak tanır. Yedekleme hızını, işlem bütünlüğünü ve hizmet sunumunu iyileştirmek amacıyla, yedekleme sırasında dosya düzeyi koruma ile çakıştığı bilinen bazı teknikler kullanılır. Her iki durumu önlemenin etkili tek yolu, Anti-malware yazılımını devre dışı bırakmaktır. Belirli süreçleri hariç tutarak (örneğin yedekleme çözümleri süreçlerini), hariç tutulan bu süreçlerle ilişkili tüm dosya işlemleri yoksayılır ve güvenli olarak algılanarak yedekleme süreciyle çakışma en düşük düzeye indirilir. Tarama dışı bırakılan öğeleri oluştururken dikkatli olmanızı öneririz - tarama dışı bırakılan bir yedekleme aracı uyarı tetiklemeden etkilenen dosyalara erişebilir. Bu nedenle, genişletilen izinlere yalnızca gerçek zamanlı koruma modülünde izin verilmektedir.

> Tarama dışı bırakılan dosya uzantıları, HIPS taraması dışında bırakılan öğeler, Algılamayla ilgili tarama dışı bırakma işlemleri veya Performansla ilgili tarama dışı bırakma işlemleri ile karıştırmayın.

Tarama dışı bırakılan işlemler, potansiyel çakışma riskini en düşük düzeye indirir ve tarama dışı bırakılan uygulamaların performansını iyileştirir. Bu, genel performans ve işletim sisteminin istikrarı üzerinde olumlu bir etkide bulunur. Bir işlemin/uygulamanın tarama dışı bırakılması, yürütülebilir dosyasının (*.exe*) tarama dışında bırakılması anlamına gelir.

Yürütülebilir dosyaları **Gelişmiş ayarlar** (F5) > **Algılama altyapısı** > **Gerçek zamanlı dosya sistemi koruması** >

Tarama dışı bırakılan işlemler üzerinden tarama dışı bırakılacak işlemler listesine ekleyebilirsiniz.

Bu özellik, yedekleme araçlarını tarama dışında bırakmak için tasarlanmıştır. Yedekleme aracının sürecini tarama dışında bırakmak sadece sistem istikrarını sağlamakla kalmaz, aynı zamanda yedekleme işlemi çalışırken yavaşlatılmayacağı için yedekleme performansını da iyileştirir.

Düzenle'yi tıklayarak **Tarama dışı bırakılan süreçler** yönetim penceresini açın. Burada, tarama dışı öğeler Ekleyebilir ve tarama dışı bırakılacak olan yürütülebilir dosyayı bulabilirsiniz (örneğin *Backup-tool.exe*). *.exe* dosyası tarama dışı öğelere eklendiğinde, bu sürecin işlemi ESET Internet Security tarafından izlenmez ve bu süreç tarafından gerçekleştirilen hiçbir dosya işlemi taranmaz.

Yürütülebilir süreç dosyasını seçerken göz atma işlevini kullanmıyorsanız, söz konusu yürütülebilir dosyanın tam yolunu manuel olarak girmeniz gerekir. Aksi halde, yürütülebilir dosya düzgün çalışmaz ve HIPS hata bildirebilir.

Ayrıca mevcut süreçleri **Düzenleyebilir** veya onları tarama dışı öğelerden **Silebilirsiniz**.

Web erişimi koruması bu tarama dışı bırakma işlemini dikkate almadığı için web tarayıcınızın yürütülebilir dosyasını tarama dışı bırakırsanız, indirilen dosyalar taranmaya devam eder. Bu sayede olası bir sızıntı algılanabilir. Bu senaryo sadece bir örnektir. Web tarayıcıları için tarama dışı öğe oluşturmanızı önermeyiz.

Tarama dışı bırakılan işlem ekleme veya düzenleme

Bu iletişim kutusu algılama altyapısının dışında tutulan işlemleri **eklemenize** olanak tanır. Tarama dışı bırakılan işlemler, potansiyel çakışma riskini en düşük düzeye indirir ve tarama dışı bırakılan uygulamaların performansını iyileştirir. Bu, genel performans ve işletim sisteminin istikrarı üzerinde olumlu bir etkide bulunur. Bir işlemin/uygulamanın tarama dışı bırakılması, yürütülebilir dosyasının (*.exe*) tarama dışında bırakılması anlamına gelir.

... öğesini tıklayarak beklenen bir uygulamanın dosya yolunu seçin (örneğin *C:\Program Files\Firefox\Firefox.exe*). Uygulamanın adını GİRMEYİN.
.exe dosyası tarama dışı öğelere eklendiğinde, bu sürecin işlemi ESET Internet Security tarafından izlenmez ve bu süreç tarafından gerçekleştirilen hiçbir dosya işlemi taranmaz.

Yürütülebilir süreç dosyasını seçerken göz atma işlevini kullanmıyorsanız, söz konusu yürütülebilir dosyanın tam yolunu manuel olarak girmeniz gerekir. Aksi halde, yürütülebilir dosya düzgün çalışmaz ve HIPS hata bildirebilir.

Ayrıca mevcut süreçleri **Düzenleyebilir** veya onları tarama dışı öğelerden **Silebilirsiniz**.

Bulut tabanlı koruma

ESET LiveGrid® (ESET ThreatSense.Net gelişmiş erken uyarı sistemi üzerine kurulmuştur), dünya genelindeki ESET kullanıcılarının gönderdiği verilerden yararlanır ve bunları ESET Araştırma Laboratuvarı'na gönderir. Şüpheli örnekleri ve meta verileri sağlayan ESET LiveGrid®, müşterilerimizin ihtiyaçları doğrultusunda hemen harekete geçmemizi ve en son tehditler hakkında ESET'in tepki verebilmesini sağlar.

Aşağıdaki seçenekler kullanılabilir:

ESET LiveGrid® bilinirlik sistemini etkinleştirebilirsiniz

ESET LiveGrid® bilinirlik sistemi bulut tabanlı beyaz ve kara liste özelliği sunar.

Doğrudan programın arabiriminden veya ESET LiveGrid® ürünündeki ek bilgileri içeren bağlam menüsünden Çalışan işlemlerin ve dosyaların bilinirliğini kontrol edebilirsiniz.

ESET LiveGrid® Geri bildirim sistemini etkinleştirebilirsiniz

ESET LiveGrid® bilinirlik sistemine ek olarak, ESET LiveGrid® geri bildirim sistemi yeni tespit edilen tehditlerle ilişkili olarak bilgisayarınız hakkındaki bilgileri toplar. Bu bilgiler şunları içerebilir:

- Tehdidin ortaya çıkmış olduğu dosyanın örneği veya kopyası
- Dosyanın yolu
- Dosya adı
- Tarih ve saat
- Tehdidin bilgisayarınızda ortaya çıktığı işlem
- Bilgisayarınızın işletim sistemi ile ilgili bilgiler

Varsayılan olarak ESET Internet Security, şüpheli dosyaları ayrıntılı analiz için ESET Virüs Laboratuvarı'na gönderecek şekilde yapılandırılmıştır. *.doc* veya *.xls* gibi uzantılara sahip dosyalar daima hariç tutulur. Siz veya şirketinizin göndermek istemediği belirli dosyalar varsa, onların uzantılarını da ekleyebilirsiniz.

Alakalı verileri gönderme ile ilgili daha fazla bilgi için Gizlilik Politikası'na başvurun.

ESET LiveGrid® aracını etkinleştirmemeyi seçebilirsiniz

Yazılımdaki işlevlerin hiçbirini kaybetmezsiniz, ancak bazı durumlarda ESET Internet Security ürünü, ESET LiveGrid® etkinleştirildiğinde yeni tehditlere daha hızlı yanıt verebilir. Daha önce ESET LiveGrid® kullandıysanız ve devre dışı bıraktıysanız, gönderilecek veri paketleri kalmış olabilir. Devre dışı bıraktıktan sonra bile bu paketler ESET'e gönderilir. Mevcut tüm bilgiler gönderildikten sonra başka paket oluşturulmaz.

ESET LiveGrid® İle ilgili daha fazla bilgi sözlükten edinilebilir.
ESET Internet Security ürününde ESET LiveGrid® aracının etkinleştirilmesi veya devre dışı bırakılması için İngilizce ve diğer çeşitli dillerde sunulan resimli talimatlarımıza bakın.

Gelişmiş ayarlarda bulut tabanlı koruma yapılandırması

ESET LiveGrid® ayarlarına erişmek için, **Gelişmiş ayarlar** (F5) > **Tespit Altyapısı** > **Bulut Tabanlı Koruma**'yı açın.

- **ESET LiveGrid® Bilinirlik sistemini etkinleştir (önerilir)** – ESET LiveGrid® bilinirlik sistemi, taranan dosyaları buluttaki beyaz ve kara listelerde yer alan öğelerden oluşan veri tabanıyla karşılaştırarak ESET anti-malware çözümlerinin etkisini artırır.

• **ESET LiveGrid® Geri bildirim sistemini etkinleştir** – Alakalı gönderim verilerini (aşağıdaki **Örneklerin gönderimi** bölümünde açıklanmaktadır), kilitlenme raporları ve istatistiklerle birlikte daha fazla analiz için ESET Araştırma laboratuvarına gönderir.

• **Kilitlenme raporlarını ve tanılama verilerini gönder** – Kilitlenme raporları ve modül belleği döküm dosyaları gibi ESET LiveGrid® ile ilgili tanılama verilerini gönderin. ESET'in sorunları tespit etmesine, ürünleri iyileştirmesine ve son kullanıcı korumasını daha iyi hale getirmesine yardımcı olmak için bu özelliği etkin halde bırakmanızı öneririz.

• **Anonim istatistikleri gönder** – ESET'in yeni tespit edilen tehditler hakkında tehdit adı, algılama tarihi ve saati, algılama yöntemi ve ilgili meta veriler, ürün sürümü ve yapılandırması gibi bilgilerin yanı sıra sisteminiz hakkındaki bilgileri toplamasına izin verir.

• **İletişim e-posta adresi (isteğe bağlı)** – Şüpheli dosyalar içine iletişim e-posta adresiniz de dahil edilebilir ve analiz için daha fazla bilgiye ihtiyaç duyulursa sizinle iletişim kurmak için kullanılabilir. Daha fazla bilgi gerekmedikçe ESET'ten herhangi bir yanıt almayacağınızı unutmayın.

Örneklerin gönderimi

Örneklerin manuel olarak gönderilmesi - Örnekleri, içerik menüsündeki Karantina veya Araçlar bölümünden manuel olarak ESET'e gönderme seçeneğini etkinleştirir.

Algılanan örneklerin otomatik gönderimi

Gelecekte tespit düzeyini iyileştirmemize yardımcı olmak amacıyla analiz için ESET'e ne tür örnekler gönderileceğini seçin (varsayılan maksimum örnek boyutu 64 MB'dir). Aşağıdaki seçenekler kullanılabilir:

• **Algılanan tüm örnekler** – Algılama altyapısı tarafından algılanan tüm nesneler (tarayıcı ayarlarında etkinleştirildiğinde istenmeyen türden olabilecek uygulamalar da dahil).

• **Belgeler dışındaki tüm örnekler** – **Belgeler** dışında algılanan nesnelerin tümü (aşağıya bakın).

• **Gönderme** – Algılanan nesneler, ESET'e gönderilmez.

Şüpheli örneklerin otomatik gönderimi

Bu örnekler, tespit altyapısı tarafından tespit edilmezse yine de ESET'e gönderilir. Örneğin, tespitten neredeyse kaçmış olan örnekler veya ESET Internet Security koruma modüllerinden biri tarafından şüpheli olarak değerlendirilen veya anlaşılmaz davranış gösterdiği belirtilen örnekler (varsayılan maksimum örnek boyutu 64 MB'dir).

• **Yürütülebilir dosyalar** – .exe, .dll, .sys gibi yürütülebilir dosyaları içerir.

• **Arşivler** – Şunun gibi arşiv dosyası türlerini içerir: .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.

• **Komut dosyaları** – .bat, .cmd, .hta, .js, .vbs, .ps1 gibi komut dosyası türlerini içerir.

• **Diğer** – Şunlar gibi dosya biçimlerini içerir: .jar, .reg, .msi, .sfw, .lnk.

• **İstenmeyen türde olabilecek e-postalar** – Bu, daha ayrıntılı analiz için olası spam bölümlerini veya spam e-postalarının tamamını ESET'e gönderir. Bu seçeneğin etkinleştirilmesi, sizin için gelecekteki spam algılamasına yönelik iyileştirmeler dahil olmak üzere Genel spam algılamasını geliştirir.

- **Belgeler** – Etkin içeriği olan veya olmayan Microsoft Office ya da PDF belgelerini içerir.

Dahil edilen tüm belge dosyası türlerinin listesi için genişlet

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Tarama dışı bırakma

Tarama dışı bırakma filtresi, belirli dosyaları/klasörleri gönderimden hariç tutmanıza olanak tanır (örneğin belgeler veya elektronik tablolar gibi gizli bilgiler içerebilecek dosyaları hariç tutmak için faydalı olabilir). Listelenen dosyalar, şüpheli kod içerse bile hiçbir zaman analiz için ESET laboratuvarına gönderilmez. En yaygın kullanılan dosya türleri (.doc, vs.) varsayılan olarak tarama dışı bırakılır. İstendiğinde tarama dışında bırakılan dosyalar listesine ekleyebilirsiniz.

`Download.domain.com` üzerinden indirilen dosyaları tarama dışı bırakmak için **Gelişmiş ayarlar** > **Tespit Altyapısı** > **Bulut tabanlı koruma** > **Örnek gönderme**'ye gidin ve **Tarama dışı öğeler**'in yanındaki **Düzenle**'ye tıklayın. `.download.domain.com` adresini tarama dışı öğe olarak ekleyin.

Örneklerin maksimum boyutu (MB) – Örneklerin maksimum boyutunu (1-64 MB) tanımlar.

Bulut tabanlı koruma için özel durum filtresi

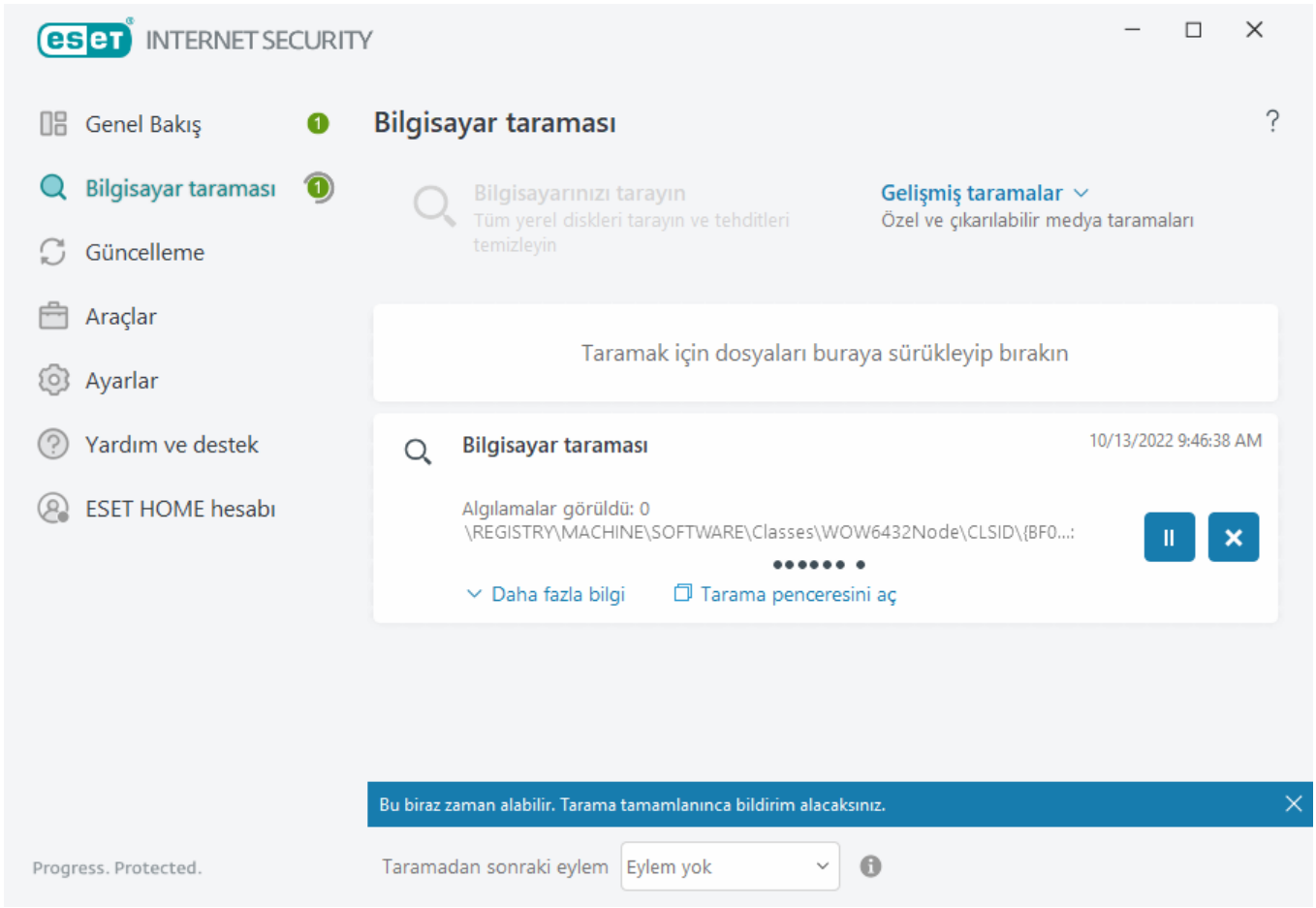
Tarama dışı bırakma filtresi, belirli dosyaları veya klasörleri örnek gönderiminin dışında bırakmanıza olanak tanır. Listelenen dosyalar, şüpheli kod içerse bile hiçbir zaman analiz için ESET laboratuvarına gönderilmez. Genel dosya türleri (.doc gibi) varsayılan olarak tarama dışıdır.

Bu özellik, belgeler veya elektronik tablolar gibi, gizli bilgiler içerebilecek dosyaları tarama dışında bırakmak için kullanılır.

Download.domain.com'dan indirilen dosyaları hariç tutmak için **Gelişmiş ayarlar** > **Tespit Altyapısı** > **Bulut tabanlı koruma** > **Örneklerin gönderimi** > **Tarama dışı öğeler**'i tıklayın ve *download.domain.com* adresini tarama dışı öğe olarak ekleyin.

Bilgisayar taraması

İsteğe bağlı tarayıcı antivirüs çözümünüzün önemli bir parçasıdır. Bilgisayarınızdaki dosyalarda ve klasörlerde tarama işlemi gerçekleştirmek için kullanılır. Güvenlik açısından, güvenlik taramalarının yalnızca enfeksiyondan şüphelenildiğinde değil, rutin güvenlik önlemlerinin parçası olarak düzenli şekilde yapılması önemlidir. Diske yazıldıklarında Gerçek zamanlı dosya sistemi koruması tarafından yakalanmayan virüsleri algılamak için sisteminizde düzenli olarak kapsamlı tarama gerçekleştirmenizi öneririz. Gerçek zamanlı dosya sistemi koruması o anda devre dışıysa, algılama altyapısı eskiyse veya dosya diske kaydedildiğinde virüs olarak algılanmadıysa bu gerçekleşebilir.



İki tür **Bilgisayar taraması** mevcuttur. **Bilgisayarınızı tarayın** seçeneği, tarama parametreleri belirtmeye gerek olmadan sistemi hızlıca tarar. **Özel tarama** (Gelişmiş taramalar altında) belirli konumları hedeflemenizi sağlamak üzere tasarlanmış önceden tanımlanmış tarama profilleri arasından seçim yapmanıza ve spesifik tarama hedefleri belirlemenize izin verir.

Tarama işlemi hakkında daha fazla bilgi için Tarama ilerleme durumu bölümüne bakın.

Varsayılan olarak, ESET Internet Security bilgisayar taraması sırasında bulunan tespitleri otomatik olarak temizlemeye veya silmeye çalışır. Bazı durumlarda, hiçbir işlem gerçekleştirilemezse interaktif bir uyarı alırsınız ve bir temizleme işlemi seçmeniz gerekir (örneğin, silme veya yoksayma gibi). Temizleme düzeyini değiştirmek ve daha ayrıntılı bilgi edinmek için Temizleme bölümüne bakın. Önceki taramaları gözden geçirmek için Günlük dosyaları'na bakın.

Bilgisayarınızı tarayın

Bilgisayarınızı tarayın seçeneği, hızlı bir şekilde bilgisayar taraması başlatmanıza ve etkilenen dosyaları kullanıcı müdahalesine gerek kalmadan temizlemenize olanak verir. **Bilgisayarınızı tarayın** seçeneğinin avantajı, kullanımının kolay olması ve ayrıntılı tarama yapılandırması gerektirmemesidir. Bu tarama, yerel sürücülerdeki tüm dosyaları denetler ve algılanan sızıntıları otomatik olarak temizler veya siler. Temizleme düzeyi otomatik olarak varsayılan değere ayarlanır. Temizleme türleri hakkında ayrıntılı bilgi için bkz. Temizleme.

Ayrıca bir dosya veya klasörü taramak için **Sürükle-Bırak taramasını** da kullanabilirsiniz. Bunun için söz konusu dosya veya klasörü tıklayın, fare düğmesini basılı tutarken imleci işaretli alana taşıyıp bırakın. Bunun ardından, uygulama ön plana taşınır.

Gelişmiş taramalar altında şu tarama seçenekleri yer alır:

Özel tarama

Özel tarama, tarama hedefleri ve yöntemleri gibi tarama parametreleri belirtmenize izin verir. **Özel taramanın** avantajı, parametreleri ayrıntılı bir şekilde yapılandırabilmenizdir. Yapılandırmalar, kullanıcı tanımlı tarama profillerine kaydedilebilir; bu da taramanın aynı parametrelerle yinelenerek gerçekleştirildiği durumlarda kullanışlı olabilir.

Çıkarılabilir medya taraması

Bilgisayarınızı tarayın seçeneğine benzer. Bilgisayara bağlı olan çıkarılabilir medyanın (CD/DVD/USB gibi) hızlı taramasını başlatır. Bu, bir bilgisayara USB flash sürücü bağladığınızda ve bu medyanın içeriklerini kötü amaçlı yazılım ve diğer olası tehditlere karşı taramak istediğinizde faydalıdır.

Bu tür tarama **Özel tarama** öğesini tıklatıp **Tarama hedefleri** açılır menüsünden **Çıkarılabilir medya** ve **Tara** seçeneklerini tıklatarak da başlatılabilir.

Son taramayı tekrarla

Bu seçenek, daha önce gerçekleştirilen tarama işlemini aynı ayarları koruyarak hızlıca başlatmanıza olanak sağlar.

Taramadan sonraki işlem açılır menüsü, taramanın tamamlanmasının ardından otomatik olarak gerçekleştirilecek işlemi belirlemenize olanak tanır:

- **Eylem yok** - Tarama tamamlandıktan sonra hiçbir eylem gerçekleştirilmez.
- **Kapat** – Bilgisayar, tarama tamamlandıktan sonra kapatılır.
- **Gerekirse yeniden başlat** - Bilgisayar yalnızca tespit edilen tehditlerin temizlenmesi işlemini tamamlamak için gerekirse yeniden başlatılır.
- **Yeniden başlat** – Taramanın ardından tüm açık programları kapatır ve bilgisayarı yeniden başlatır.
- **Gerekirse yeniden başlatmayı zorla** - Bilgisayar yalnızca tespit edilen tehditlerin temizlenmesi işlemini tamamlamak için gerekirse yeniden başlamaya zorlanır.
- **Yeniden başlatmayı zorla** - Kullanıcı etkileşimini beklemeden tüm açık programların kapatılmasını zorlar ve tarama tamamlandıktan sonra bilgisayarı yeniden başlatır.
- **Uykuya geç** – Oturumunuzu korur ve bilgisayarı düşük güç moduna getirir ve bu sayede işinize hızlı bir şekilde devam edebilirsiniz.
- **Hazırda beklet** – RAM'de çalışan her şeyi alıp sabit sürücünüzde özel bir dosyaya taşır. Bilgisayarınız kapanır, ancak daha sonra başlattığınızda önceki durumundan devam eder.

> **Uyku** veya **Hazırda Beklet** işlemleri bilgisayarınızın Güç ve uyku işletim sistemi ayarlarına veya bilgisayar/dizüstü bilgisayar özelliklerine dayalı olarak kullanılabilir. Uyuyan bir bilgisayarın hâlâ çalışan bir bilgisayar olduğunu lütfen unutmayın. Bilgisayarınız pil gücü ile çalıştığı sırada temel işlevleri çalıştırmaya ve elektrik kullanmaya devam eder. Örneğin ofis dışında seyahat ederken pil ömrünü korumak için Hazırda Beklet seçeneğini kullanmanızı öneririz.

Seçilen eylem, çalışan tüm taramaların tamamlanmasının ardından başlatılacak. **Kapat** veya **Yeniden Başlat**'ı

seçtiğinizde onay iletişim penceresinde 30 saniyelik bir geri sayım görüntülenir (istenen işlemi devre dışı bırakmak için **İptal**'i tıklayın).

> Ayda en az bir defa bilgisayar taraması çalıştırmanızı öneririz. Tarama, **Araçlar** > **Diğer araçlar** > **Zamanlayıcı**'dan zamanlanan görev olarak yapılandırılabilir. Haftalık bilgisayar taramasını nasıl zamanlayabilirim?

Özel tarama başlatıcı

İşletim belleğini, ağı veya bir diskin tamamı yerine belirli bölümlerini taramak için Özel Tarama özelliğini kullanabilirsiniz. Bunun için **Gelişmiş taramalar** > **Özel tarama**'yı tıklayıp klasör (ağaç) yapısından belirli hedefleri seçin.

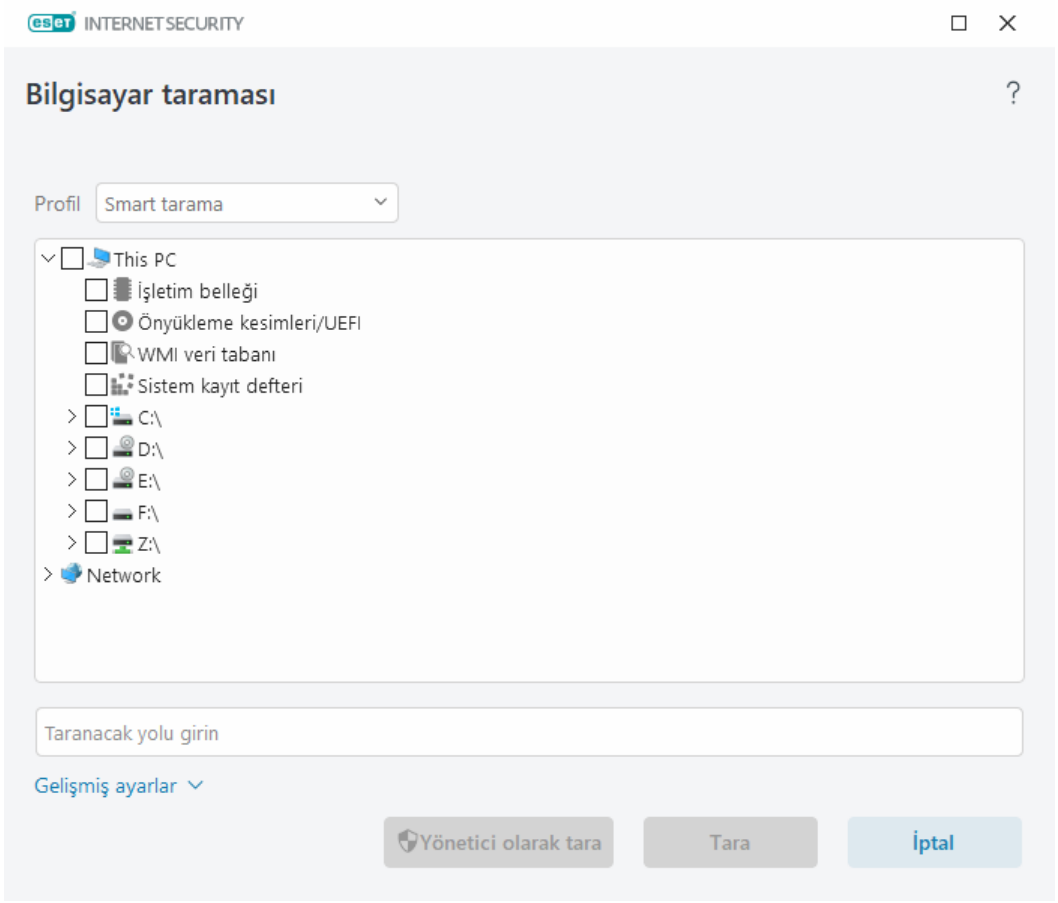
Belirli hedefler taranırken kullanılmak üzere **Profili** açılır menüsünden bir profil seçebilirsiniz. Varsayılan profil **Smart tarama** profilidir. **Kapsamlı tarama**, **İçerik menüsü taraması** ve **Bilgisayar taraması** olmak üzere üç adet önceden tanımlanmış tarama profili daha bulunmaktadır. Bu tarama profilleri farklı ThreatSense parametreleri kullanır. Kullanılabilir seçenekler **Gelişmiş ayarlar** (F5) > **Tespit altyapısı** > **Zararlı yazılım taramaları** > **İsteğe bağlı tarama** > ThreatSense parametreleri bölümünde açıklanmaktadır.

Klasör (ağaç) yapısı, belirli tarama hedefleri de içerir.

- **İşletim belleği** - İşletim belleği tarafından halihazırda kullanılan tüm işlemleri ve verileri tarar.
- **Önyükleme kesimleri/UEFI** - Önyükleme kesimlerini ve UEFI'yi zararlı yazılımlara karşı tarar. UEFI tarayıcı ile ilgili daha fazla bilgi için sözlükten yararlanın.
- **WMI veri tabanı** - Tüm Windows Management Instrumentation (WMI) veri tabanını, tüm ad alanlarını, tüm sınıf örneklerini ve tüm özelliklerini tarar. Enfekte olan dosyalara veya veri olarak katıştırılmış zararlı yazılımlara referans arar.
- **Sistem kayıt defteri** - Tüm sistem kayıt defterini, tüm anahtarları ve alt anahtarları tarar. Enfekte olan dosyalara veya veri olarak katıştırılmış zararlı yazılımlara referans arar. Tespitleri temizlerken önemli verilerin kaybolmadığından emin olmak için referans kayıt defterinde kalır.

Hızlı bir şekilde bir tarama hedefine (dosya veya klasöre) gitmek için yolu ağaç yapısının altındaki metin alanına yazın. Yol büyük/küçük harfe duyarlıdır. Hedefi taramaya dahil etmek için ağaç yapısındaki onay kutusunu işaretleyin.

> Haftalık bir bilgisayar taraması zamanlama
> Normal bir görev zamanlamak için Haftalık bilgisayar taraması planlama bölümünü okuyun.



Gelişmiş ayarlar (F5) > **Tespit altyapısı** > **İsteğe bağlı tarama** > **ThreatSense parametreleri** > **Temizleme** altında tarama için temizleme parametrelerini yapılandırabilirsiniz. Temizleme işlemi olmadan bir taramayı çalıştırmak için **Gelişmiş ayarlar**'ı tıklayıp **Temizleme olmadan tara**'yı seçin. Tarama geçmişi tarama günlüğüne kaydedilir.

Özel durumları yoksay seçildiğinde, daha önce tarama dışında bırakılan uzantılara sahip dosyalar özel durum olmadan taranır.

Taramayı ayarladığınız özel parametreleri kullanarak yürütmek için **Tara** seçeneğini tıklatın.

Yönetici olarak tara seçeneği, taramayı Yönetici hesabı altında yürütmenize izin verir. Geçerli kullanıcının taramak istediğiniz dosyalara erişme izinleri yoksa bunu kullanın. Bu düğme, geçerli kullanıcı Yönetici olarak UAC işlemlerini çağıramıyorsa kullanılamaz.

Günlüğü göster'i tıklatarak bir tarama tamamlandığında bilgisayar tarama günlüğünü görüntüleyebilirsiniz.

Tarama ilerleme durumu

Tarama ilerleme durumu penceresi taramanın geçerli durumunu ve kötü amaçlı kod içerdiği belirlenen dosya sayısı hakkında bilgileri gösterir.

Parolayla korunan dosyalar ve özel olarak sistem tarafından kullanılan dosyalar (tipik olarak *pagefile.sys* ve belirli günlük dosyaları) gibi bazı dosyaların taranamaması normaldir. Daha fazla bilgi için bu bilgi bankası makalesine bakabilirsiniz.

Haftalık bir bilgisayar taraması zamanlama

Normal bir görev zamanlamak için Haftalık bilgisayar taraması planlama bölümünü okuyun.

Tarama ilerlemesi – İlerleme çubuğu taranmış olan nesnelerin taranmayı bekleyen nesnelere kıyasla durumunu gösterir. Tarama ilerleme durumu, taramaya dahil edilen toplam nesne sayısından elde edilir.

Hedef – Taranmakta olan nesnenin ve konumunun adı.

Bulunan tehditler – Taranan dosyaların, bulunan tehditlerin ve tarama sırasında temizlenen tehditlerin toplam sayısını gösterir.

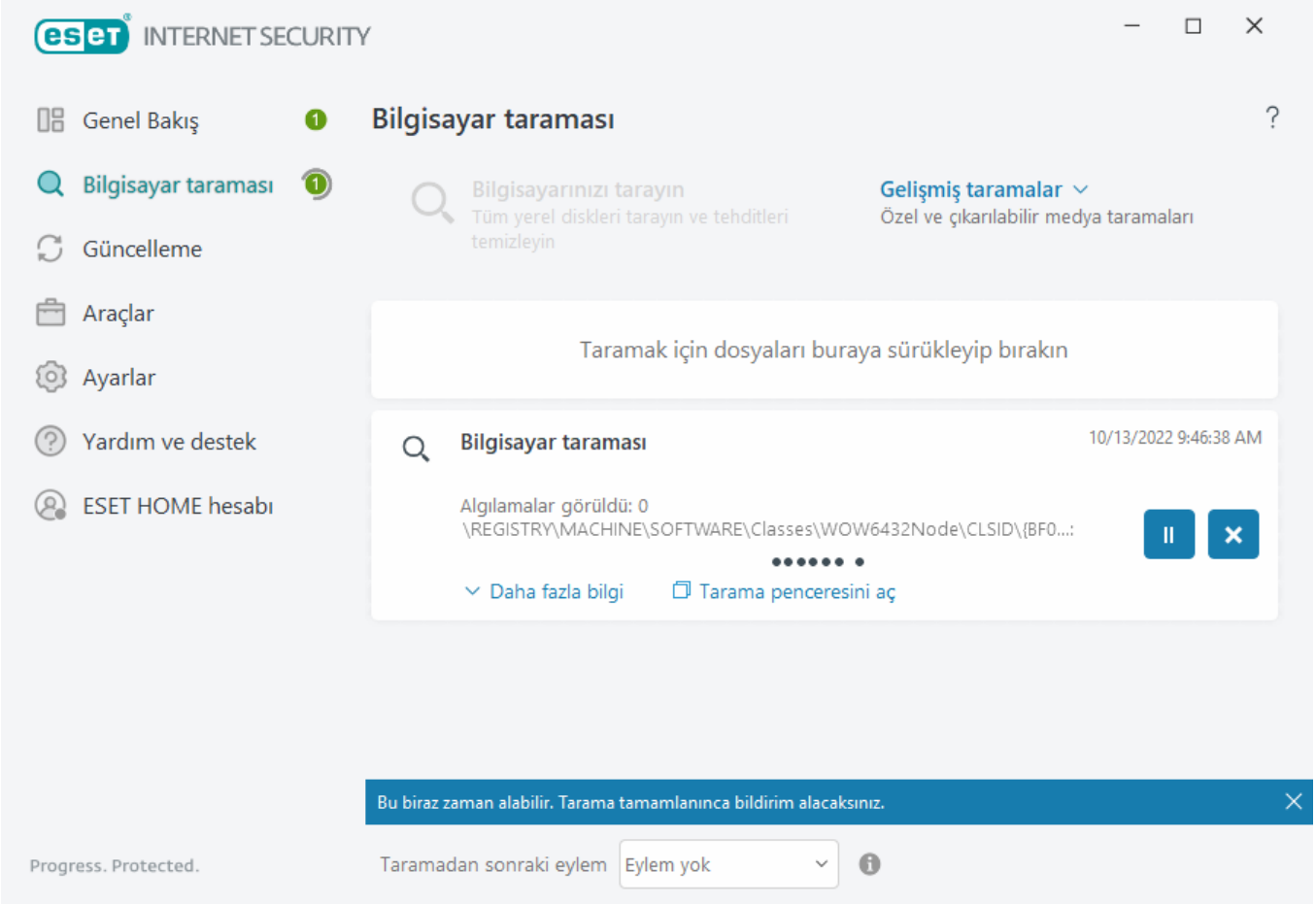
Duraklat – Taramayı duraklatır.

Sürdür – Tarama ilerlemesi duraklatıldığında bu seçenek görünür. Taramaya devam etmek için **Devam et** öğesini tıklatın.

Durdur – Taramayı sonlandırır.

Tarama günlüğünü kaydır - Etkinse, en yeni girişlerin görünür olması için yeni girişler eklendikçe tarama günlüğü otomatik olarak aşağı doğru kaydırılır.

Halihazırda çalışmakta olan taramayla ilgili ayrıntıları görüntülemek için büyüteci veya oku tıklayın. **Bilgisayarınızı tarayın** veya **Gelişmiş taramalar** > **Özel tarama**'yı tıklayarak başka bir paralel tarama çalıştırabilirsiniz.



Taramadan sonraki işlem açılır menüsü, taramanın tamamlanmasının ardından otomatik olarak gerçekleştirilecek işlemi belirlemenize olanak tanır:

- **Eylem yok** - Tarama tamamlandıktan sonra hiçbir eylem gerçekleştirilmez.

- **Kapat** – Bilgisayar, tarama tamamlandıktan sonra kapatılır.
- **Gerekirse yeniden başlat** - Bilgisayar yalnızca tespit edilen tehditlerin temizlenmesi işlemini tamamlamak için gerekirse yeniden başlatılır.
- **Yeniden başlat** – Taramanın ardından tüm açık programları kapatır ve bilgisayarı yeniden başlatır.
- **Gerekirse yeniden başlatmayı zorla** - Bilgisayar yalnızca tespit edilen tehditlerin temizlenmesi işlemini tamamlamak için gerekirse yeniden başlamaya zorlanır.
- **Yeniden başlatmayı zorla** - Kullanıcı etkileşimini beklemeden tüm açık programların kapatılmasını zorlar ve tarama tamamlandıktan sonra bilgisayarı yeniden başlatır.
- **Uykuya geç** – Oturumunuzu korur ve bilgisayarı düşük güç moduna getirir ve bu sayede işinize hızlı bir şekilde devam edebilirsiniz.
- **Hazırda beklet** – RAM'de çalışan her şeyi alıp sabit sürücünüzde özel bir dosyaya taşır. Bilgisayarınız kapanır, ancak daha sonra başlattığınızda önceki durumundan devam eder.

Uyku veya **Hazırda Beklet** işlemleri bilgisayarınızın Güç ve uyku işletim sistemi ayarlarına veya bilgisayar/dizüstü bilgisayar özelliklerine dayalı olarak kullanılabilir. Uyuyan bir bilgisayarın hâlâ çalışan bir bilgisayar olduğunu lütfen unutmayın. Bilgisayarınız pil gücü ile çalıştığı sırada temel işlevleri çalıştırmaya ve elektrik kullanmaya devam eder. Örneğin ofis dışında seyahat ederken pil ömrünü korumak için Hazırda Beklet seçeneğini kullanmanızı öneririz.

Seçilen eylem, çalışan tüm taramaların tamamlanmasının ardından başlatılacak. **Kapat** veya **Yeniden Başlat**'ı seçtiğinizde onay iletişim penceresinde 30 saniyelik bir geri sayım görüntülenir (istenen işlemi devre dışı bırakmak için **İptal**'i tıklayın).

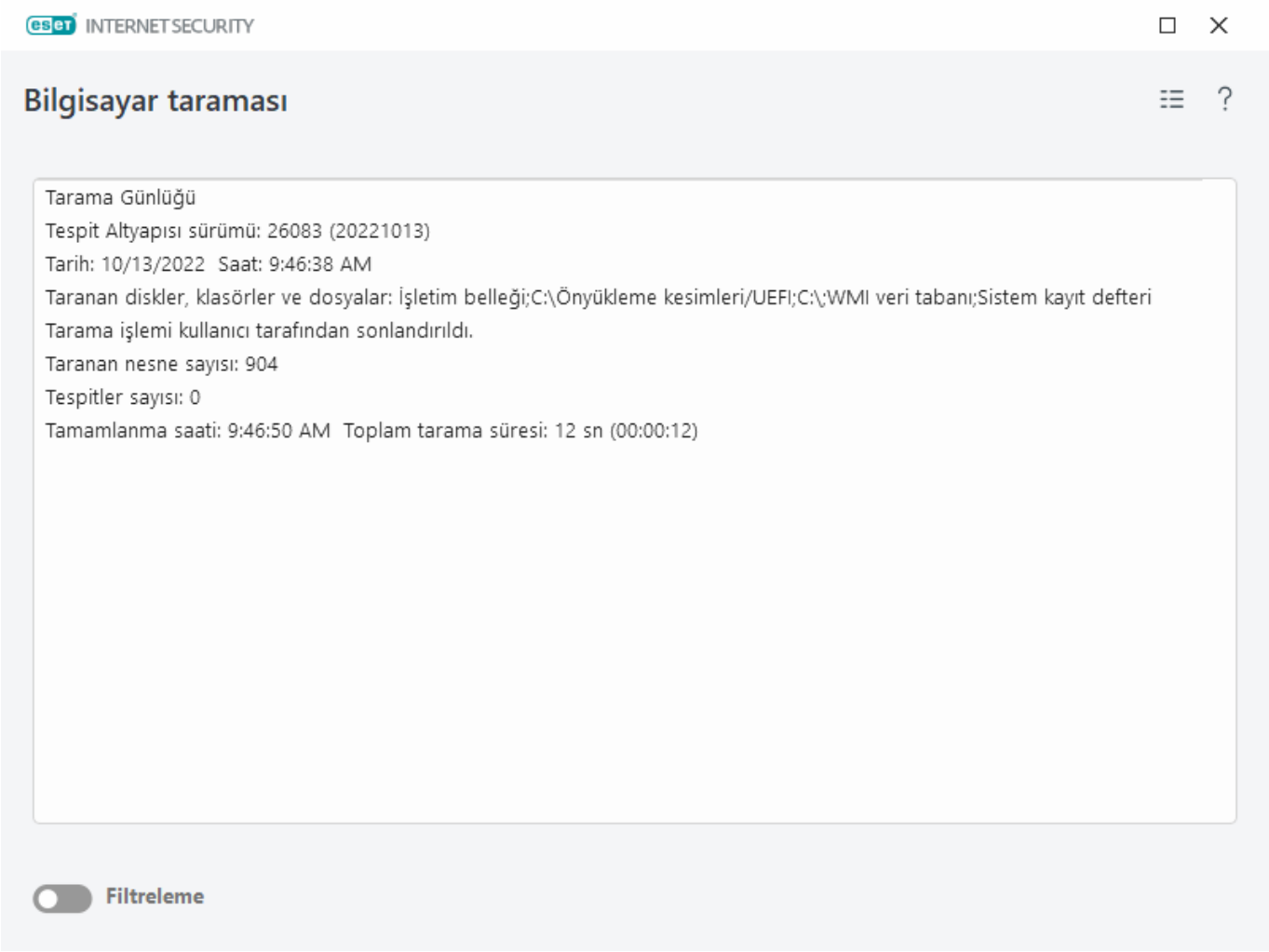
Bilgisayar tarama günlüğü

Tarama sona erdiğinde Bilgisayar tarama günlüğü, söz konusu taramayla ilgili tüm bilgileri açar. Tarama günlüğü size aşağıdaki gibi bilgileri verir:

- Algılama altyapısı sürümü
- Başlama tarihi ve saati
- Taranan diskler, klasörler ve dosyalar
- Zamanlanan tarama adı (yalnızca zamanlanan tarama)
- Tarama durumu
- Taranan nesne sayısı
- Bulunan algılama sayısı
- Tamamlanma zamanı
- Toplam tarama süresi

Daha önce yürütülen zamanlanan görevin aynısı çalışmaya devam ediyorsa zamanlanan bilgisayar tarama görevi için yeni bir başlatma işlemi atlanır. Atlanan zamanlanan tarama görevi, 0 taranan nesneye sahip bir Bilgisayar tarama günlüğü oluşturur ve **Önceki tarama çalışmaya devam ettiği için tarama başlatılamadı** durumu gösterilir.

Önceki tarama günlüklerini bulmak için ana program penceresinde **Araçlar** > **Diğer araçlar** > **Günlük dosyaları**'nı seçin. Açılır menüde **Bilgisayar taraması**'nı seçip istediğini kaydı çift tıklayın.



"Açılamıyor", "açılırken hata oluştu" ve/veya "arşiv zarar görmüş" kayıtları hakkında daha fazla bilgi edinmek için ESET Bilgi Bankası makalemize bakın.

Günlük filtreleme penceresini açmak için **Filtreleme** kaydırma çubuğunu tıklayın. Bu pencerede aramanızı özel kriterlere göre daraltabilirsiniz. İçerik menüsünü görmek için belirli bir günlük girişini sağ tıklayın:

Eylem	Kullanım
Aynı kayıtları filtrele	Günlük filtreleme özelliğini etkinleştirir. Günlük, yalnızca seçilenle aynı türdeki kayıtları gösterir.
Filtrele...	Bu seçenek, Günlük filtreleme penceresini açar ve belirli günlük girişleri için kriterleri tanımlamanıza olanak tanır. Kısayol: `Ctrl+Shift+F`
Filtreyi etkinleştir	Filtre ayarlarını etkinleştirir. Filtreyi ilk kez etkinleştiriyorsanız ayarları tanımlamanız gerekir. Günlük filtreleme penceresi açılır.
Filtreyi devre dışı bırak	Filtreyi kapatır (alt taraftaki açma/kapama düğmesini tıklamak da aynı işlevi görür).
Kopyala	Vurgulanan kayıtları panoya kopyalar. Kısayol: `Ctrl+C`

Eylem	Kullanım
Tümünü kopyala	Penceredeki tüm kayıtları kopyalar.
Dışa aktar	Panoda vurgulanan kayıtları XML dosyasına aktarır.
Tümünü ver	Bu seçenek, penceredeki tüm kayıtları XML dosyasına aktarır.
Tespit açıklaması	Kaydedilen sızıntının tehlikeleri ve belirtileri ile ilgili ayrıntılı bilgiler içeren ESET Tehdit Ansiklopedisi açılır.

Kötü amaçlı yazılım taramaları

Zararlı yazılım taramaları bölümüne **Gelişmiş ayarlar** (F5) > **Algılama altyapısı** > **Zararlı yazılım taramaları**'ndan ulaşılabilir ve burada tarama parametrelerini seçmeniz için seçenekler sunulur. Bu bölümde aşağıdaki öğeler bulunur:

Seçilen profil – İsteğe bağlı tarayıcı tarafından kullanılan belirli parametre kümesi. Yeni bir profil oluşturmak için **Profil listesi** öğesinin yanındaki **Düzenle**'yi tıklayın. Daha fazla bilgi için Tarama profilleri'ne bakın.

Tarama hedefleri – Yalnızca özel bir hedefi taramak isterseniz **Tarama hedefleri** öğesinin yanındaki **Düzenle**'yi tıklayabilir, açılır menüden bir seçenek belirleyebilir ya da klasör (ağaç) yapısından belirli bir hedefi seçebilirsiniz. Daha fazla bilgi için Tarama hedefleri'ne bakın.

ThreatSense parametreleri – Denetlemek istediğiniz dosya uzantıları, kullanılan algılama yöntemleri vb. gibi gelişmiş ayar seçenekleri bu bölümde bulunabilir. Gelişmiş tarayıcı seçeneklerinin bulunduğu bir sekmeyi açmak için tıklayın.

Boşta durumu taraması

Gelişmiş ayarlar'da, **Algılama altyapısı** > **Kötü amaçlı yazılım taramaları** > **Boşta durumu taraması** altında **boşta durumu tarayıcısını** etkinleştirebilirsiniz.

Boşta durumu taraması

Bu özelliği etkinleştirmek için **Boşta durum taramasını etkinleştir** seçeneğinin yanındaki kaydırma çubuğunu etkinleştirin. Bilgisayar boşta durumundayken, sessiz bilgisayar taraması tüm yerel sürücülerde gerçekleştirilir.

Bilgisayar (dizüstü bilgisayar) pil ile çalışırken boşta durumu tarayıcı varsayılan olarak çalışmaz. Bu ayarı, Gelişmiş ayarlar içinde **Bilgisayar pil gücüyle çalışıyor olsa da çalıştır** seçeneğinin yanındaki kaydırma çubuğunu etkinleştirerek geçersiz kılabilirsiniz.

Günlük dosyaları bölümünde bilgisayar taramasının sonucunu kaydetmek için **Günlük kaydını etkinleştir** seçeneğinin yanındaki kaydırma çubuğunu açık konuma getirin (ana program penceresinden **Araçlar** > **Diğer araçlar** > **Günlük dosyaları**'nı tıklayıp **Günlük** açılır menüsünden **Bilgisayar taraması**).

Boşta durumunun algılanması

Boşta durumu tarayıcısının tetiklenebilmesi için karşılanması gereken koşulların tam listesi için Boşta durumu algılama tetiklemeleri'ne bakın.

Boşta durumu tarayıcısı için tarama parametrelerini (örneğin, algılama yöntemi) değiştirmek için ThreatSense altyapısı parametre ayarları öğesini tıklatın.

Tarama profilleri

ESET Internet Security ürününde önceden tanımlanmış 4 tarama profili bulunmaktadır:

- **Smart tarama** – Bu varsayılan gelişmiş tarama profilidir. Smart tarama profili, önceki bir taramada temiz olduğu tespit edilen ve bu taramadan beri değiştirilmemiş dosyaları hariç tutan Smart Optimizasyon teknolojisini kullanır. Bu, sistem güvenliğine en az etkiyle daha kısa tarama süreleri sağlar.

- **İçerik menüsü taraması** – İçerik menüsünden herhangi bir dosyanın isteğe bağlı taramasını başlatabilirsiniz. İçerik menüsü tarama profili, taramayı bu şekilde tetiklediğinizde kullanılacak bir tarama yapılandırması tanımlamanıza olanak tanır.

- **Kapsamlı tarama** – Kapsamlı tarama profili varsayılan olarak Akıllı optimizasyonu kullanmadığından bu profil kullanıldığında hiçbir dosya taramadan hariç tutulmaz.

- **Bilgisayar taraması** – Standart bilgisayar taramasında kullanılan varsayılan profildir.

Tercih edilen tarama parametreleriniz daha sonraki taramalar için kaydedilebilir. Düzenli olarak kullanılan her tarama için farklı bir profil (çeşitli tarama hedefleriyle, tarama yöntemleriyle ve diğer parametrelerle) oluşturmanızı öneririz.

Yeni bir profil oluşturmak için Gelişmiş ayarlar penceresini (F5) açın ve **Algılama altyapısı** > **Kötü amaçlı yazılım taramaları** > **İsteğe bağlı tarama** > **Profil listesi**'ni tıklayın. **Profil yöneticisi** penceresi, mevcut tarama profillerini listeleyen bir **Seçilen profil** açılır menüsü ve yeni bir profil oluşturma seçeneği içerir. İhtiyaçlarınıza uygun bir tarama profili oluşturmanıza yardımcı olması için, tarama ayarlarının her bir parametresine yönelik bir açıklama içeren ThreatSense altyapısı parametre ayarları bölümüne bakın.

> Kendi tarama profilinizi oluşturmak istediğinizi ve **Bilgisayarınızı tarayın** yapılandırmasının kısmi olarak uygun olduğunu, ancak tarama çalışma zamanı paketleyicileri veya tehlikeli olabilecek uygulamaları istemezken, **Algılamayı her zaman düzelt** uygulamak istediğinizi varsayalım. **Profil yöneticisi** penceresinde yeni profilinizin adını girin ve **Ekle** seçeneğini tıklayın. **Seçilen profil** açılır menüsünden yeni profilinizi seçip kalan parametreleri gereksinimlerinize göre ayarladıktan sonra yeni profilinizi kaydetmek için **Tamam**'ı tıklayın.

Tarama hedefleri

Tarama hedefleri açılır menüsü, önceden tanımlı tarama hedefleri seçmenizi sağlar.

- **Profil ayarlarına göre** – Seçili tarama profili tarafından belirtilen hedefleri seçer.
- **Çıkarılabilir sürücü** – Disketi, USB depolama aygıtını, CD/DVD'yi seçer.

- **Yerel sürücüler** – Sistem sabit sürücülerinin tümünü seçer.

- **Ağ sürücüleri** – Tüm eşlenen sürücüleri seçer.

- **Özel seçim** - Önceki tüm seçimleri iptal eder.

Klasör (ağaç) yapısı, belirli tarama hedefleri de içerir.

- **İşletim belleği** - İşletim belleği tarafından halihazırda kullanılan tüm işlemleri ve verileri tarar.
- **Önyükleme kesimleri/UEFI** - Önyükleme kesimlerini ve UEFI'yi zararlı yazılımlara karşı tarar. UEFI tarayıcı ile ilgili daha fazla bilgi için sözlükten yararlanın.
- **WMI veri tabanı** - Tüm Windows Management Instrumentation (WMI) veri tabanını, tüm ad alanlarını, tüm sınıf örneklerini ve tüm özelliklerini tarar. Enfekte olan dosyalara veya veri olarak katıştırılmış zararlı yazılımlara referans arar.
- **Sistem kayıt defteri** - Tüm sistem kayıt defterini, tüm anahtarları ve alt anahtarları tarar. Enfekte olan dosyalara veya veri olarak katıştırılmış zararlı yazılımlara referans arar. Tespitleri temizlerken önemli verilerin kaybolmadığından emin olmak için referans kayıt defterinde kalır.

Hızlı bir şekilde bir tarama hedefine (dosya veya klasöre) gitmek için yolu ağaç yapısının altındaki metin alanına yazın. Yol büyük/küçük harfe duyarlıdır. Hedefi taramaya dahil etmek için ağaç yapısındaki onay kutusunu işaretleyin.

Aygıt denetimi

ESET Internet Security, otomatik aygıt (CD/DVD/USB/...) denetimi sağlar. Bu modül genişletilmiş filtreleri/izinleri engellemenize veya ayarlamanıza ve bir kullanıcının belirli bir aygıta erişip erişemeyeceğini ve bu aygıtla çalışıp çalışamayacağını tanımlamanıza olanak tanır. Bilgisayar yöneticisi, istenmeyen içerik bulunduran aygıtların kullanımını engellemek istiyorsa bu özellik faydalı olabilir.

Desteklenen harici aygıtlar:

- Disk Depolama (HDD, USB çıkarılabilir disk)
- CD/DVD
- USB Yazıcı
- FireWire Depolama alanı
- Bluetooth Aygıt
- Akıllı kart okuyucu
- Görüntüleme Aygıtı
- Modem
- LPT/COM bağlantı noktası
- Taşınabilir Aygıt
- Tüm aygıt türleri

Aygıt denetimi ayarları seçenekleri **Gelişmiş ayarlar** (F5) > **Aygıt denetimi** içinde değiştirilebilir.

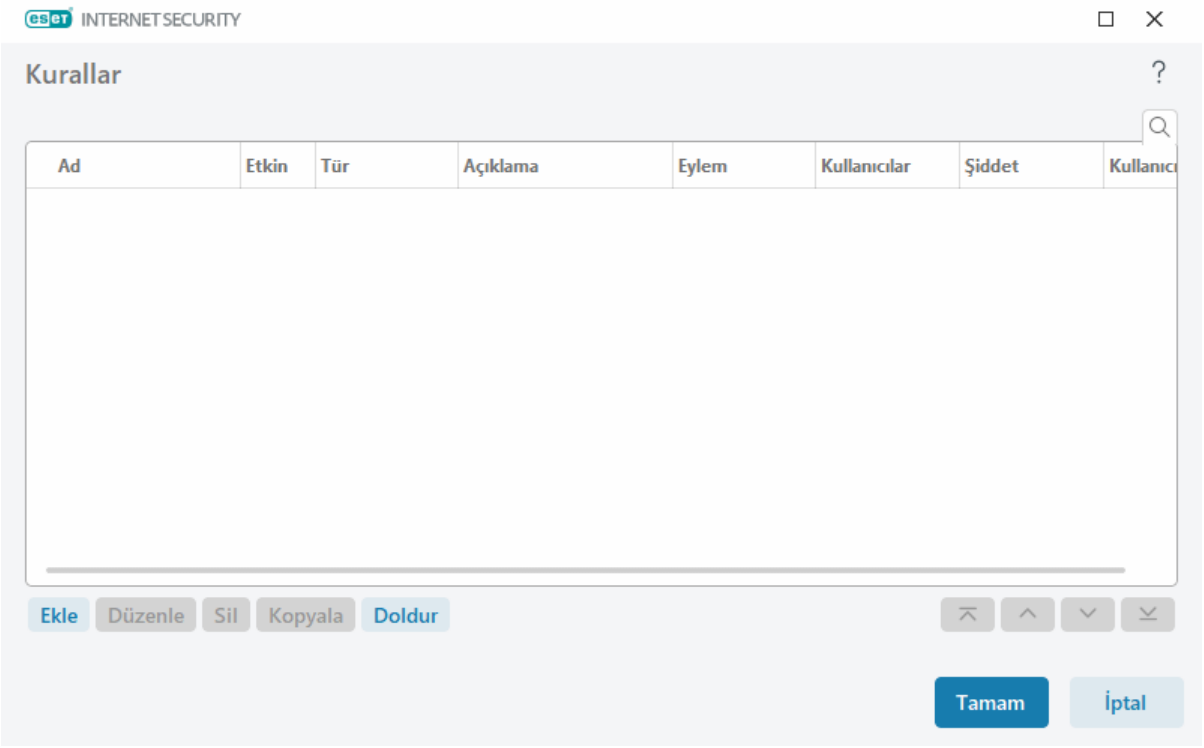
Cihaz kontrolünü etkinleştir öğesinin yanındaki kaydırma çubuğunu açık konuma getirerek ESET Internet Security ürünündeki Cihaz kontrolü özelliğini etkinleştirebilirsiniz. Bu değişikliğin geçerli olması için bilgisayarınızı yeniden başlatmanız gerekir. Cihaz Kontrolü etkinleştirildikten sonra Kurallar düzenleyicisi penceresinde **Kurallar**'ı tanımlayabilirsiniz.

> Farklı kuralların uygulanacağı aygıtlardan oluşan farklı gruplar oluşturabilirsiniz. Ayrıca **İzin ver** veya **Yazma Engeli** eylemine sahip kuralın uygulanacağı tek bir cihaz grubu oluşturabilirsiniz. Bu, tanınmayan aygıtlar bilgisayarınıza bağlandığında Aygıt denetimi tarafından engellenmelerini sağlar.

Mevcut bir kural ile engellenen bir aygıt takılırsa, bir bildirim penceresi görüntülenir ve aygıta erişim verilmez.

Aygıt denetimi kural düzenleyicisi

Cihaz kontrolü kuralları düzenleyicisi penceresi, mevcut kuralları görüntüler ve kullanıcıların bilgisayara bağladığı harici cihazların hassas denetimine izin verir.



Kullanıcı veya kullanıcı grubu başına ve kural yapılandırmasında belirlenebilen ek cihaz parametrelerine göre belirli cihazlara izin verilebilir ya da bu cihazlar engellenebilir. Kural listesi, bir kuralın çeşitli açıklamalarını içerir: ad, harici cihaz türü, bir harici cihazın bilgisayarınıza bağlanmasının ardından gerçekleştirilecek işlem ve günlük düzeyi. Ayrıca Cihaz kontrolü kurallarını ekleme bölümüne de bakın.

Bir kuralı yönetmek için **Ekle** veya **Düzenle** seçeneğini tıklayın. Seçili başka bir kural için kullanılan önceden tanımlı seçeneklere sahip yeni bir kural oluşturmak için **Kopyala** seçeneğini tıklatın. Bir kural tıklatıldığında görüntülenen XML dizileri, sistem yöneticilerinin bu verileri vermesine/almasına ve kullanmasına yardımcı olma amacıyla, örneğin, içine kopyalanabilir.

CTRL tuşuna basıp tıklatarak birden fazla kural seçebilirsiniz ve bunları silme, listenin yukarısına veya aşağısına taşıma gibi eylemleri seçili tüm kurallara uygulayabilirsiniz. **Etkinleştirildi** onay kutusu bir kuralı devre dışı bırakmak veya etkinleştirmek için kullanılabilir; kuralı tutmak istediğinizde bu özellik yararlı olabilir.

Denetim, yüksek öncelikli kurallar üstte olacak şekilde önceliklerini belirleyen sırada sıralanan kurallar tarafından gerçekleştirilir.

Günlük girişleri ESET Internet Security ürününün ana penceresinde **Araçlar** > **Diğer araçlar** > **Günlük dosyaları** tıklatılarak görüntülenebilir.

Aygıt denetim günlüğü, Aygıt denetiminin tetiklendiği tüm olayları kaydeder.

Algılanan aygıtlar

Doldur düğmesi, bağlı olan tüm aygıtlar için bir genel bakış şunar ve şunlar hakkındaki bilgileri sağlar: aygıt türü, aygıt satıcısı, modeli ve seri numarası (varsa).

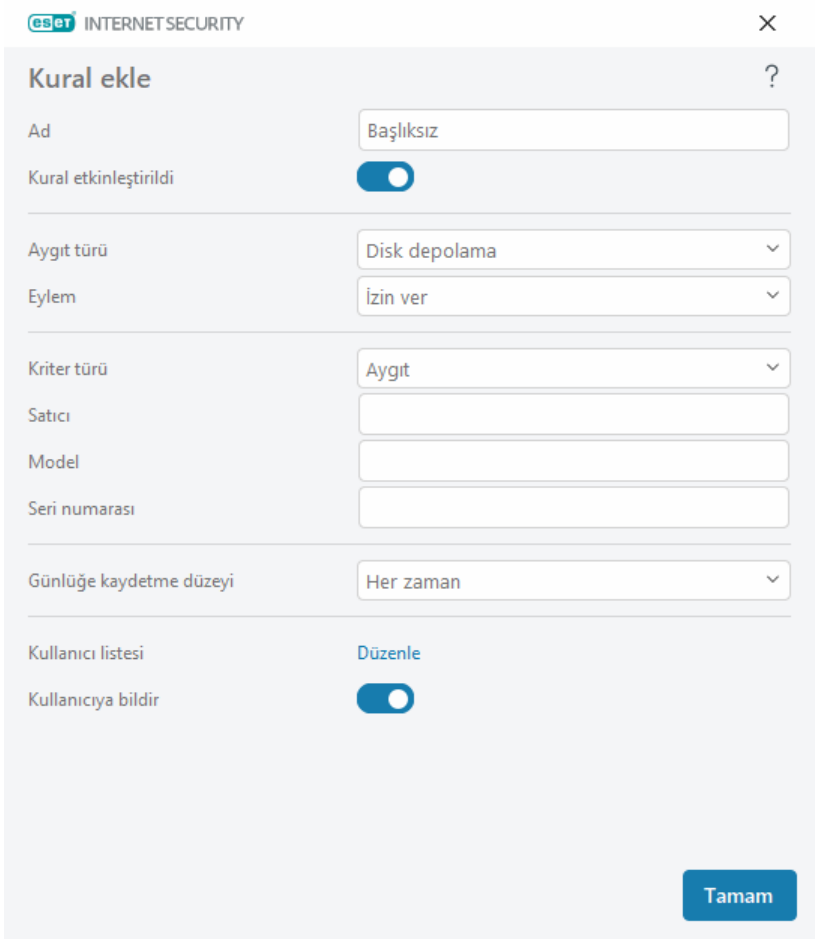
Algılanan cihazlar listesinden bir cihaz seçin ve önceden tanımlı bilgilere sahip bir cihaz kontrolü kuralı eklemek için **Tamam**'ı tıklayın (tüm ayarlar yapılabilir).

Düşük güç (uyku) modundaki cihazlar bir uyarı simgesiyle işaretlenir. **Tamam** düğmesini etkinleştirmek ve bu cihaz için bir kural eklemek üzere:

- Cihazı yeniden bağlayın
- Cihazı kullanın (örneğin, bir web kamerasını uyandırmak için Windows'da Kamera uygulamasını başlatın)

Aygıt denetimi kuralları ekleme

Cihaz Kontrolü kuralı, kural ölçütlerini karşılayan bir cihaz bilgisayara bağlandığında gerçekleştirilecek eylemi tanımlar.



Daha iyi tanımlama için **Ad** alanına bir açıklamasını girin. Bu kuralı devre dışı bırakmak veya etkinleştirmek için **Kural etkin** seçeneğinin yanındaki kaydırma çubuğunu tıklayın. Bu, kuralı kalıcı olarak silmek istemediğinizde kullanılabilecek yararlı bir özelliktir.

Aygıt türü

Aşağı açılır menüden harici aygıt türünü seçin (Disk depolama/Taşınabilir aygıt/Bluetooth/FireWire/...). Aygıt türü bilgileri, işletim sisteminden devralınır ve aygıtın bilgisayara bağlı olması şartıyla Sistem aygıt yöneticisinde görülebilir. Depolama aygıtları USB veya FireWire ile bağlanan harici diskleri veya geleneksel bellek kart okuyucularını içerir. Akıllı kart okuyucuları SIM kartlar veya kimlik doğrulama kartları gibi katıştırılmış tümleşik devreye sahip tüm akıllı kart okuyucularını içerir. Görüntüleme aygıtları örnekleri tarayıcılar ve kameralardır. Bu aygıtlar sadece eylemleri hakkında bilgi verdiği ve kullanıcılar hakkında bilgi sağlamadığı için yalnızca genel olarak engellenebilir.

Eylem

Depolama özelliği olmayan aygıtlara erişime izin verilebilir veya erişim engellenebilir. Buna karşın, depolama aygıtlarına yönelik kurallar, aşağıdaki haklara ilişkin ayarlardan birini seçebilmenize olanak tanır:

- **Izin ver** – Aygıta tam erişime izin verilir.
- **Engelle** – Aygıta erişim engellenir.
- **Yazma Engeli** – Aygıt için yalnızca okuma erişimine izin verilir.
- **Uyarı** – Bir aygıtın her bağlanışında kullanıcı, izin verildiği/engellendiği konusunda bilgilendirilir ve bir günlük girişi yapılır. Cihazlar hatırlanmaz ve aynı cihazın sonraki bağlanışlarında bildirim gösterilmeye devam eder.

Tüm Eylemlerin (izinler) tüm aygıt türleri için kullanılabilir olmadığını unutmayın. Depolama türünde bir cihaz için dört Eylemin tümü kullanılabilir. Depolama özelliği olmayan aygıtlar için yalnızca üç eylem bulunur (örneğin, **Yazma Engeli** eylemi Bluetooth için kullanılamaz; bu nedenle, Bluetooth aygıtları için yalnızca izin vermek, engellemek veya uyarmak eylemleri mevcuttur).

Kriter türü

Aygıt grubu veya **Aygıt**'ı seçin.

Aşağıda gösterilen ek parametreler, farklı cihazlar için kurallarda hassas ayarlar yapmak için kullanılabilir. Tüm parametreler büyük/küçük harfe duyarlıdır ve joker karakterleri destekler (*, ?):

- **Satıcı** – Satıcı adı veya kimliğine göre filtreler.
- **Model** – Aygıtın adı.
- **Seri numarası** – Harici aygıtların genellikle kendi seri numaraları vardır. CD/DVD'lerde bu, CD sürücünün değil, belirli bir medyanın seri numarasıdır.

Bu parametreler tanımsızsa kural eşleşse dahi bu alanları yoksayar. Tüm metin alanlarındaki filtreleme parametreleri büyük/küçük harfe duyarlıdır ve özel karakterleri destekler (Soru işareti ? tek bir karakteri, yıldız işareti * sıfır veya daha çok karakter içeren bir dizeyi temsil eder).

Bir aygıt hakkındaki bilgileri görüntülemek üzere aygıtın türü için kural oluşturun, aygıtı bilgisayarınıza bağlayın ve Aygıt denetim günlüğünde aygıt detaylarını kontrol edin.

Günlüğe kaydetme şiddeti

ESET Internet Security tüm önemli olayları ana menüden doğrudan görüntülenebilen bir günlük dosyasına kaydeder. **Araçlar** > **Diğer araçlar** > **Günlük dosyaları**'nı tıklayıp **Günlük** açılır menüsünden **Aygıt denetimi**'ni seçin.

- **Her zaman** – Tüm olayları günlüğe kaydeder.
- **Tanılama** – Programda hassas ayarlama yapmak için gereken bilgileri günlüğe kaydeder.
- **Bilgiler** – Başarılı güncelleme iletileri dahil olmak üzere bilgilendirici iletileri ve yukarıdaki tüm kayıtları kaydeder.
- **Uyarı** – Kritik hataları ve uyarı iletilerini kaydeder.
- **Yok** – Günlüğe herhangi bir şey kaydedilmez.

Kullanıcı listesi

Kurallar, **Kullanıcı listesi** yanındaki **Düzenle** seçeneğini tıklayarak Kullanıcı listesine eklemek yoluyla belirli kullanıcılarla veya kullanıcı gruplarıyla sınırlandırılabilir.

- **Ekle** – İstenen kullanıcıları seçmenize olanak tanıyan **Nesne türleri: Kullanıcılar veya Gruplar** iletişim penceresini açar.
- **Kaldır** - Seçili kullanıcıyı filtreden kaldırır.

Kullanıcı listesi sınırlamaları

Kullanıcı listesi belirli Cihaz türlerinesahip kurallar için tanımlanamaz:

- USB Yazıcı
- Bluetooth aygıtı
- Akıllı kart okuyucu
- Görüntüleme aygıtı
- Modem
- LPT/COM bağlantı noktası

Kullanıcıya bildir - Mevcut bir kural tarafından engellenen bir cihaz takılırsa bildirim penceresi görüntülenir.

Aygıt grupları

Bilgisayarınıza bağlanan aygıt, bir güvenlik riski oluşturabilir.

Aygıt grupları penceresi iki bölüme ayrılır. Pencerenin sağındaki bölüm, söz konusu gruba ait aygıtların listesini verir; sol tarafındaki bölümse oluşturulan grupları içerir. Sağ bölmede cihazları görüntülemek için bir grup seçin.

Aygıt grupları penceresini açıp bir grup seçtiğinizde listeden aygıtları ekleyip çıkarabilirsiniz. Gruba aygıt eklemenin diğer bir yolu, onları bir dosyadan aktarmaktır. Alternatif olarak, **Doldur** düğmesini tıklayabilirsiniz; bunun üzerine, bilgisayarınıza bağlanan tüm aygıtlar **Algılanan aygıtlar** penceresinde listelenir. Doldurulan listeden cihazları seçip **Tamam**'ı tıklayarak gruba ekleyin.

Denetim öğeleri

Ekle - Bir grubu adını tıklayarak veya bir cihazı pencerenin hangi bölümünde düğmeyi tıklamış olduğunuza bağlı olarak mevcut bir gruba ekleyebilirsiniz.

Düzenle – Seçilen grubun adını veya aygıt parametrelerini (satıcı, model, seri numarası) değiştirmenize olanak sağlar.

Sil – Pencerenin hangi tarafında düğmeyi tıkladığınıza bağlı olarak seçili grubu veya aygıtı siler.

İçe aktar - Bir metin dosyasından cihazların listesini içe aktarır. Cihazları metin dosyasından içe aktarma işlemi için doğru biçimlendirme gerekir:

- Her cihaz yeni bir satırda başlar.
- **Satıcı**, **Model** ve **Seri numarası** her cihaz için mevcut olmalı ve virgülle ayrılmalıdır.

Metin dosyası içeriğine örnek:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Dışa aktar - Cihaz listesini bir dosyaya aktarır.

Doldur düğmesi, bağlı olan tüm aygıtlar için bir genel bakış şunar ve şunlar hakkındaki bilgileri sağlar: aygıt türü, aygıt satıcısı, modeli ve seri numarası (varsa).

Cihaz ekle

Bir cihazı mevcut bir gruba eklemek için sağ pencerede **Ekle**'yi tıklayın. Aşağıda gösterilen ek parametreler, farklı cihazlar için kurallarda hassas ayarlar yapmak için kullanılabilir. Tüm parametreler büyük/küçük harfe duyarlıdır ve joker karakterleri destekler (*, ?):

- **Satıcı** – Satıcı adı veya ID kimliğine göre filtreler.
- **Model** – Aygıtın adı.
- **Seri numarası** – Harici aygıtların genellikle kendi seri numaraları vardır. CD/DVD'lerde bu, CD sürücünün değil, belirli bir medyanın seri numarasıdır.
- **Açıklama** - Daha iyi bir düzen için cihazla ilgili açıklamanız.

> Bu parametreler tanımsızsa kural eşleşse dahi bu alanları yoksayar. Tüm metin alanlarındaki filtreleme parametreleri büyük/küçük harfe duyarlıdır ve joker karakterleri destekler (Soru işareti "?" tek bir karakteri, yıldız işareti "*" sıfır veya daha çok karakter içeren bir dizeyi temsil eder).

Değişiklikleri kaydetmek için **Tamam**'ı tıklatın. Değişiklikleri kaydetmeden **Cihaz grupları** penceresinden ayrılmak için **İptal** seçeneğini tıklayın.

> Bir cihaz grubu oluşturduktan sonra, oluşturulan cihaz grubu için yeni bir cihaz denetimi kuralı eklemeniz ve yapılacak eylemi seçmeniz gerekir.

Tüm Eylemlerin (izinler) tüm aygıt türleri için kullanılabilir olmadığını unutmayın. Depolama türü bir cihazsa dört eylemin tümü kullanılabilir. Depolama özelliği olmayan cihazlar için yalnızca üç eylem kullanılabilir (örneğin, **Yazma Engeli** Bluetooth için kullanılamaz; bu nedenle, Bluetooth cihazlar için yalnızca izin verilebilir, engellenebilir veya uyarılabilir).

Web kamerası koruması

Web Kamerası Koruması bilgisayarınızın web kamerasına erişen işlem ve uygulamalar hakkında sizi bilgilendirir. Bir uygulama kameranıza erişmeye çalıştığında bir bildirim penceresi görüntülenir. Bu pencerede erişime **izin verebilir** veya **engelleyebilirsiniz**. Uyarı penceresinin rengi uygulamanın bilinirliğine dayalıdır.

Webcam koruması kurulum seçenekleri, ana program penceresi > **Ayarlar** > **Gelişmiş ayarlar** (F5) > **Cihaz kontrolü** > **Webcam koruması**'nda değiştirilebilir.

ESET Internet Security ürününde Webcam koruması özelliğini etkinleştirmek için **Webcam korumasını etkinleştir**'in yanındaki kaydırma çubuğunu etkinleştirin.

Webcam koruması etkinleştirildiğinde, **Kurallar** etkin hale gelir ve Kurallar düzenleyicisi penceresini açmanıza olanak tanır.

Değiştirilen ancak hâlâ geçerli bir dijital imzaya sahip (örneğin, uygulama güncellemesi), kuralı olan uygulamalar için uyarıları kapatmak üzere **Değiştirilen uygulamalar için web kamerası erişim uyarılarını devre dışı bırak** özelliğinin yanındaki kaydırma çubuğunu etkinleştirin.

Web kamerası koruması kural düzenleyici

Bu pencere, mevcut kuralları görüntüler ve seçtiğiniz eyleme göre bilgisayarınızın web kamerasına erişen uygulama ve işlemlerin denetimine izin verir.

Kullanılabilir eylemler şunlardır:

- **Erişime izin ver**
- **Erişimi engelle**

- **Sor** (Bir uygulama web kamerasına her erişmeye çalıştığında kullanıcıya sorar)

Bir uygulama web kamerasına eriştiğinde bildirim almayı durdurmak için **Bildir** sütunundaki onay kutusunun işaretini kaldırın.

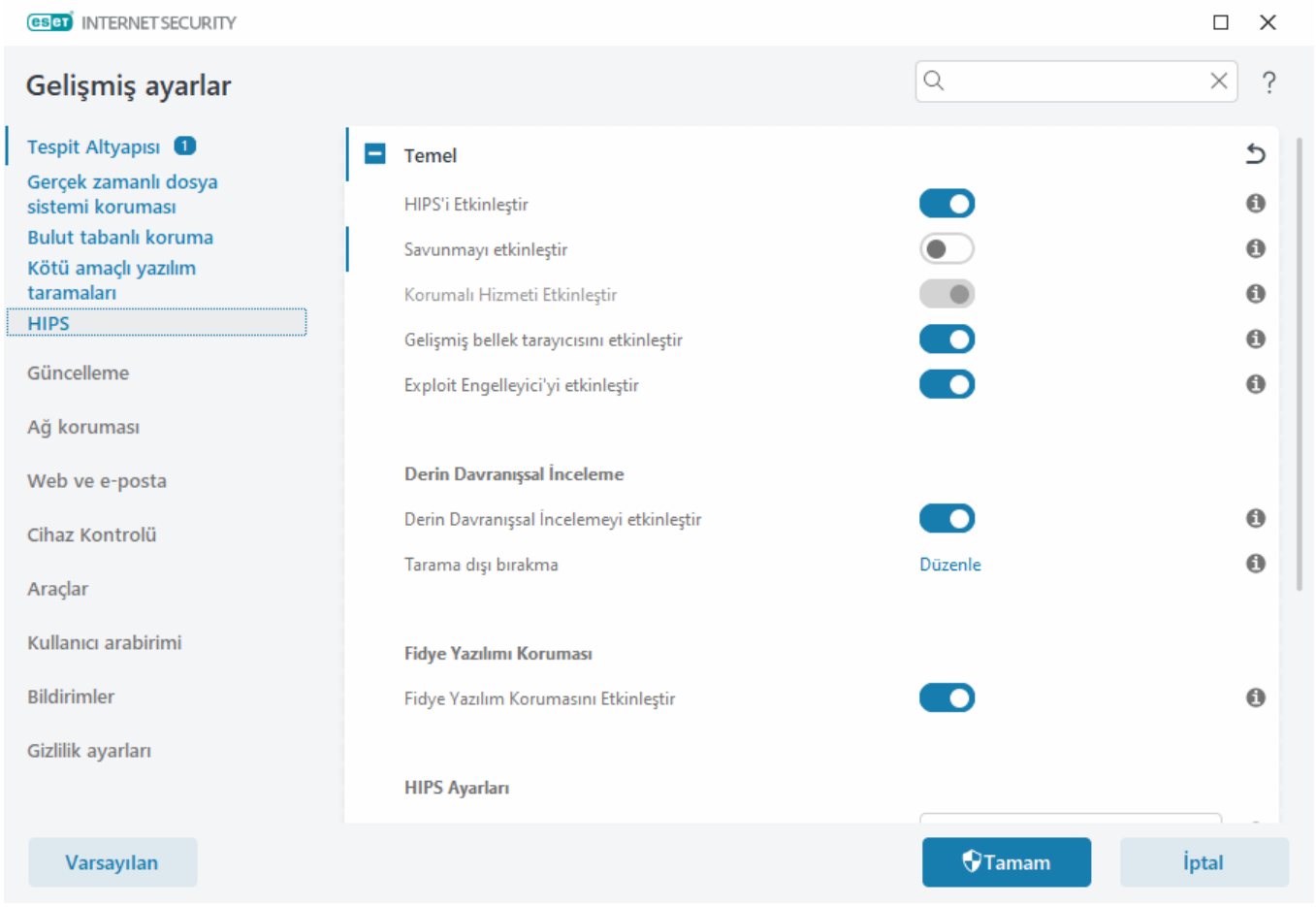
> **Resimli talimatlar**
> ESET Internet Security ürününde web kamerası kuralları oluşturma ve düzenleme.

HIPS

> HIPS ayarlarında yapılan değişiklikler yalnızca deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. HIPS ayarlarında yanlış bir yapılandırma, sistemde istikrarsızlığa neden olabilir.

Host Tabanlı Saldırı Önleme Sistemi (HIPS) sisteminizi, bilgisayarınızı olumsuz yönde etkilemeyi hedefleyen kötü amaçlı yazılımlardan ve istenmeyen etkinliklerden korur. HIPS; çalışan işlemleri, dosyaları ve kayıt defteri anahtarlarını izlemek için ağ filtrelemenin algılama özellikleriyle birlikte gelişmiş davranışsal analizi kullanır. HIPS Gerçek zamanlı dosya sistemi korumasından ayrıdır ve bir güvenlik duvarı değildir.

HIPS ayarlarına **Gelişmiş ayarlar**(F5) > **Algılama altyapısı** > **HIPS** > **Temel** menüsünden ulaşabilirsiniz. HIPS durumu (etkin/devre dışı), ESET Internet Security ana program penceresinde **Ayarlar** > **Bilgisayar koruması** içinde gösterilir.



Temel

HIPS'i etkinleştir – HIPS, ESET Internet Security ürününde varsayılan olarak etkindir. HIPS'i kapatmak Exploit Engelleyici gibi diğer HIPS özelliklerini devre dışı bırakır.

Kendini Korumayı etkinleştir – ESET Internet Security, kötü amaçlı yazılımların antivirus veya casus yazılım karşıtı korumanızı bozmasını veya devre dışı bırakmasını engellemek için HIPS'in bir parçası olarak tümleşik **Kendini koruma** teknolojisini kullanır. Kendini koruma, hayati önemdeki sistemi ve ESET'in işlemlerini, kayıt defteri anahtarlarını ve dosyaları kurcalanmaya karşı korur.

Korumalı Hizmeti Etkinleştir – ESET Hizmeti (ekrn.exe) için korumayı etkinleştirir. Bu etkinleştirildiğinde, hizmet kötü amaçlı yazılım tarafından gelen saldırılara karşı savunmak için korumalı bir Windows işlemi olarak başlatılır. Bu seçenek Windows 8.1 ve sürümlerinde vardır.

Gelişmiş bellek tarayıcısını etkinleştir, Exploit Engelleyici ile birlikte çalışarak gizlenme veya şifreleme yoluyla kötü amaçlı yazılımlara karşı koruma ürünlerinin algılamasından kaçan tehditlere karşı korumayı güçlendirir Gelişmiş bellek tarayıcı varsayılan olarak etkindir. Bu koruma türüyle ilgili daha fazla bilgi için sözlüğe başvurun.

Exploit Engelleyici'yi etkinleştir – Web tarayıcıları, PDF okuyucuları, e-posta istemcileri ve MS Office bileşenleri gibi yaygın olarak açıklarından yararlanılan uygulama türlerini desteklemek üzere tasarlanmıştır. Exploit Engelleyici varsayılan olarak etkindir. Bu koruma türüyle ilgili daha fazla bilgi için sözlüğe başvurun.

Derin Davranışsal İnceleme

Derin Davranışsal İnceleme'yi etkinleştir – HIPS özelliğinin parçası olarak çalışan başka bir koruma katmanıdır. Bu HIPS uzantısı, bilgisayarda çalışan tüm programların davranışını analiz eder ve işlem davranışının kötü amaçlı

olması halinde sizi uyarır.

Derin Davranışsal İnceleme dışında bırakılan HIPS tarama dışı öğeleri, işlemleri analiz dışında bırakmanızı sağlar. Tüm işlemlerin olası tehditlere karşı tarandığından emin olmak için, hariç tutulan öğelerin yalnızca kesinlikle gerekli olduğunda oluşturulmasını öneririz.

Ransomware koruması

Fidye yazılımı korumasını etkinleştir – HIPS özelliğinin bir parçası olarak çalışan başka bir koruma katmanıdır. Fidye yazılımı korumasının çalışması için ESET LiveGrid® bilinirlik sistemini etkinleştirmeniz gerekir. Bu koruma türü hakkında daha fazla bilgi edinin.

Intel® Threat Detection Technology Aracını etkinleştir - Tespit etkililiğini artırmak, yanlış tespit uyarılarını azaltmak ve gelişmiş kaçınma tekniklerini yakalamak amacıyla görünürlüğü genişletmek için benzersiz Intel CPU telemetrisini kullanarak fidye yazılımı saldırılarının tespit edilmesine yardımcı olur. Desteklenen işleyicilere bakın.

HIPS Ayarları

Filtreleme modu, aşağıdaki modlardan birinde gerçekleştirilebilir:

Filtreleme modu	Açıklama
Otomatik mod	Sisteminizi koruyan önceden tanımlı kurallar tarafından engellenenler dışında, işlemler etkinleştirilir.
Akıllı mod	Kullanıcıya yalnızca çok şüpheli olaylarla ilgili bildirim gönderilir.
Etkileşimli mod	Kullanıcının işlemleri onaylaması istenir.
İlke tabanlı mod	Kendilerine izin veren belirli bir kural tarafından tanımlanmamış tüm işlemleri engeller.
Öğrenme modu	İşlemler etkinleştirilir ve her işlemin ardından bir kural oluşturulur. Bu modda oluşturulan kurallar, **HIPS kuralları** düzenleyicisinde görüntülenebilir, ancak bunların önceliği manuel olarak veya otomatik modda oluşturulan kurallardan daha düşüktür. **Filtreleme modu** açılır menüsünden **Öğrenme modunu** seçerseniz **Öğrenme modu şu sürenin ardından sona erecek** ayarı kullanılabilir hale gelir. Öğrenme modunda kalmak istediğiniz süreyi seçin, maksimum süre 14 gündür. Belirtilen süre geçtiğinde öğrenme modundayken HIPS tarafından oluşturulan kuralları düzenlemeniz istenir. Ayrıca başka bir filtreleme modu seçebilir veya kararı erteleyebilir ve öğrenme modunu kullanmaya devam edebilirsiniz.

Öğrenme modunun süresi dolduktan sonra ayarlanan mod – Öğrenme modunun süresi dolduktan sonra kullanılacak filtreleme modunu seçin. Süre dolduktan sonra **Kullanıcıya sor** seçeneği, HIPS filtreleme moduna geçiş işlemini gerçekleştirmek için yönetici izinleri gerektirir.

HIPS sistemi, işletim sistemi içindeki olayları izler ve Güvenlik duvarı tarafından kullanılan kurallara benzer kurallara dayanarak uygun şekilde yanıt verir. **HIPS kuralları** düzenleyicisini açmak için **Kurallar**'ın yanındaki **Düzenle** seçeneğini tıklayın. HIPS kuralları penceresinde kuralları seçebilir, düzenleyebilir veya kaldırabilirsiniz. Kural oluşturma ve HIPS işlemlerine ilişkin daha fazla ayrıntı HIPS kuralı düzenle bölümünde bulunabilir.

HIPS interaktif penceresi

HIPS bildirimi penceresi, HIPS'in algıladığı yeni eylemlere göre kural oluşturmanıza ve ardından eyleme izin verileceği veya eylemin reddedileceği koşulları tanımlamanıza izin verir.

Bildirim penceresinden oluşturulan kuralların, manuel olarak oluşturulan kurallara eşit olduğu düşünülür. Bu nedenle bir bildirim penceresinden oluşturulan kural, söz konusu iletişim penceresini tetikleyen kuraldan daha az spesifik olabilir. Bu; iletişim kutusunda bir kural oluşturulduktan sonra aynı işlemin aynı pencereyi tetikleyebileceği anlamına gelir. HIPS kuralları için öncelik.

Bir kural için varsayılan eylem **Her defasında sor** olarak belirlenmişse, kuralın her tetiklenişinde bir iletişim penceresi görüntülenir. İşlem için **Reddet** veya **İzin Ver** seçeneklerini belirleyebilirsiniz. Belirtilen sürede bir eylem seçmezseniz yeni eylem kurallara göre seçilir.

Uygulamadan çıkılana kadar anımsa seçeneği; kural veya filtreleme modu değişikliği, HIPS modülü güncellemesi veya sistem yeniden başlatma işlemi gerçekleşinceye kadar eylemin (**İzin ver/Reddet**) kullanılmasına neden olur. Bu üç eylemden herhangi biri gerçekleştiğinde geçici kurallar silinir.

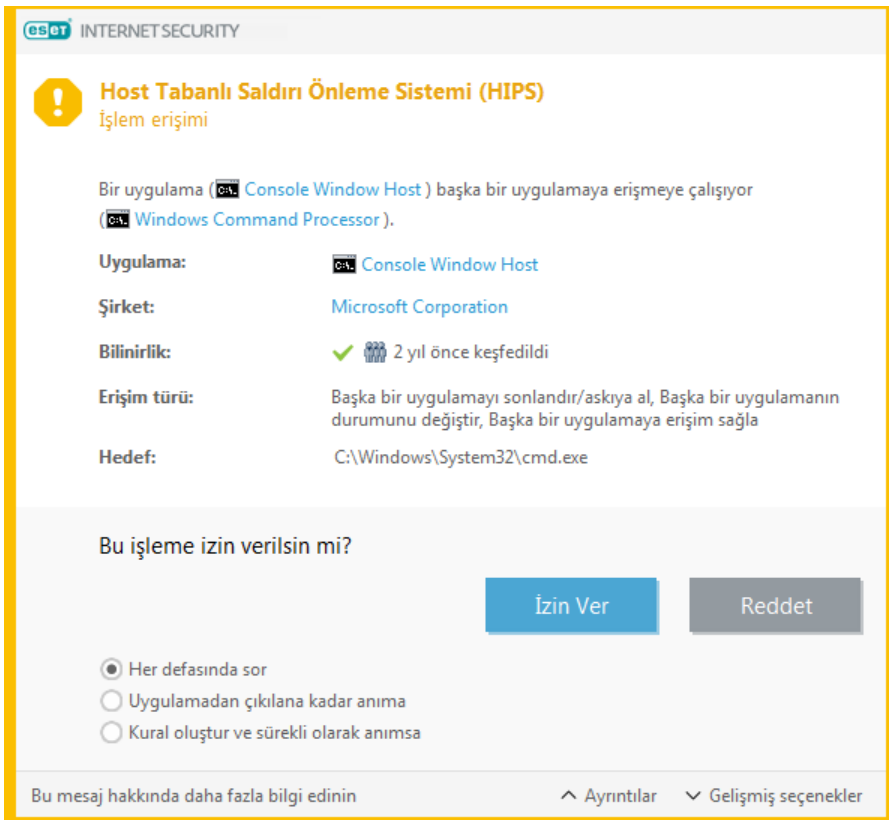
Kural oluştur ve sürekli olarak anımsa seçeneği yeni bir HIPS kuralı oluşturur ve bu kural daha sonra HIPS kuralı yönetimi bölümünde değiştirilebilir (yönetici hakları gerektirir).

İşlemi hangi uygulamanın tetiklediğini, dosyanın bilinirliğini veya ne tür bir işleme izin vermeniz ya da reddetmeniz istendiğini görmek için aşağıdaki **Ayrıntılar**'ı tıklayın.

Daha ayrıntılı kural parametreleri için ayarlara **Gelişmiş seçenekler** tıklanarak erişilebilir. **Kural oluştur ve sürekli olarak anımsa** seçeneğini işaretlerseniz aşağıdaki seçenekler sunulur:

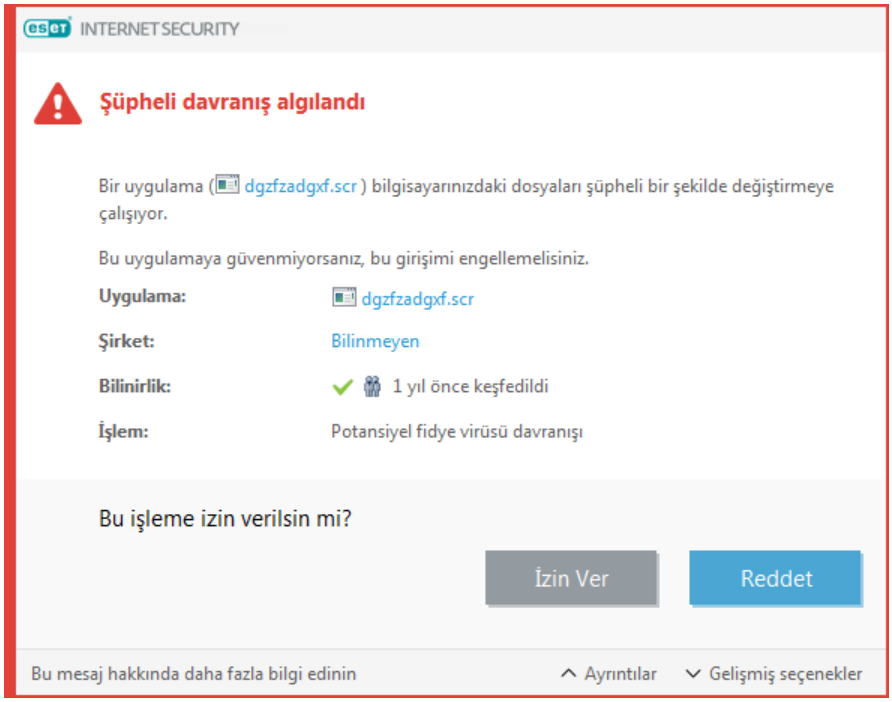
- **Yalnızca bu uygulama için geçerli bir kural oluştur** – Bu onay kutusunun işaretini kaldırırsanız kural tüm kaynak uygulamaları için oluşturulur.
- **Sadece şu işlem için** – Kural dosyası/uygulaması/kayıt defteri işlemleri seçin. Tüm HIPS işlemleri için açıklamalara bakın.
- **Yalnızca şu hedef için** – Kural dosyası/uygulaması/kayıt defteri hedefleri seçin.

> **Çok fazla HIPS bildirimi mi alıyorsunuz?**
> Bildirimlerin gösterilmesini durdurmak için **Gelişmiş ayarlar** (F5) > **Algılama altyapısı** > **HIPS** > **Temel** bölümünde filtreleme modunu **Otomatik mod** olarak ayarlayın.



Potansiyel fidye virüsü davranışı algılandı

Potansiyel ransomware davranışı algılandığında bu interaktif pencere görüntülenir. İşlem için **Reddet** veya **İzin Ver** seçeneklerini belirleyebilirsiniz.



Belirli algılama parametrelerini görmek için **Ayrıntılar**'ı tıklayın. İletişim penceresi dosyayı **analiz için göndermenize** veya **Algılama dışında bırakmanıza** olanak sağlar.

Ransomware korumasının düzgün çalışması için ESET LiveGrid® etkinleştirilmelidir.

HIPS kuralı yönetimi

HIPS sistemine ait kullanıcı tanımlı ve otomatik olarak eklenmiş kuralların listesi. Kural oluşturma ve HIPS işlemleriyle ilgili daha fazla ayrıntı HIPS kural ayarları bölümünde bulunabilir. Ayrıca Genel HIPS prensibi bölümüne de bakın.

Sütunlar

Kural – Kullanıcı tanımlı veya otomatik olarak seçilen kural adı.

Etkin - Kuralı listede tutmak istiyor ancak kullanmak istemiyorsanız kaydırma çubuğunu devre dışı bırakın.

Eylem – Koşulların doğru olması durumunda gerçekleştirilmesi gereken bir eylemi (**İzin ver**, **Engelle** veya **Sor**) belirtir.

Kaynaklar – Kural, yalnızca olayın bu uygulama(lar) tarafından tetiklenmesi durumunda kullanılır.

Hedefler – Kural, sadece işlemin belirli bir dosyayla, uygulamayla ya da kayıt defteri girişiyle ilgili olması halinde kullanılır.

Günlüğe kaydetme şiddeti – Bu seçeneği etkinleştirirseniz bu kuralla ilgili bilgiler HIPS günlüğüne yazılır.

Kullanıcıya bildir – Bir olay tetiklenirse, sağ alt köşede küçük bir açılır pencere görüntülenir.

Denetim öğeleri

Ekle – Yeni bir kural oluşturur.

Düzenle – Seçili girişleri düzenlemenize olanak tanır.

Sil - Seçilen girişleri kaldırır.

HIPS kuralları için öncelik

Üst/alt düğmeler kullanılarak HIPS kurallarının öncelik düzeyini ayarlama seçeneği yoktur (Güvenlik duvarı kuralları için kurallar yukarıdan aşağı yürütülür).

- Oluşturduğunuz tüm kurallar aynı önceliğe sahiptir
- Kural ne kadar belirliyse öncelik o kadar yüksek olur (örneğin, belirli bir uygulamanın kuralı, tüm uygulamalar için oluşturulmuş kuraldan daha yüksek önceliğe sahip olur)
- Dahili olarak, HIPS, sizin erişiminize açık olmayan daha yüksek öncelikli kurallar içerir (örneğin, Kendini koruma tarafından tanımlanmış kuralların üzerine yazamazsınız)
- İşletim sisteminizi dondurabilecek olan, sizin tarafınızdan oluşturulan bir kural uygulanmayacaktır (en düşük önceliğe sahip olacaktır)

Bir HIPS kuralını düzenleme

Önce HIPS kural yönetimine bakın.

Kural adı – Kullanıcı tanımlı veya otomatik olarak seçilen kural adı.

Eylem – Koşulların doğru olması durumunda gerçekleştirilmesi gereken bir eylemi (**İzin ver**, **Engelle** veya **Sor**) belirtir.

Etkilenen işlemler – Kuralın uygulanacağı işlem türünü seçmelisiniz. Kural, yalnızca bu tür işlem ve seçili hedef için kullanılır.

Etkin - Kuralı listede tutmak istiyor ancak uygulamak istemiyorsanız kaydırma çubuğunu devre dışı bırakın.

Günlüğe kaydetme şiddeti – Bu seçeneği etkinleştirirseniz bu kuralla ilgili bilgiler HIPS günlüğüne yazılır.

Kullanıcıya bildir – Bir olay tetiklenirse, sağ alt köşede küçük bir açılır pencere görünür.

Kural, bu kuralı tetikleyen koşulları açıklayan bölümlerden oluşur:

Kaynak uygulamalar– Kural, yalnızca olayın bu uygulamalar tarafından tetiklenmesi durumunda kullanılır. Açılır menüden **Belirli uygulamalar**'ı seçin ve **Ekle** öğesine tıklatarak yeni dosyaları ekleyin veya tüm uygulamaları eklemek için açılır menüden **Tüm uygulamalar** seçeneğini de belirleyebilirsiniz.

Hedef dosyalar – Kural, yalnızca işlemin bu hedefle ilgili olması durumunda kullanılır. Açılır menüden **Belirli dosyalar**'ı seçin ve **Ekle** öğesini tıklayarak yeni dosya veya klasörleri ekleyin ya da tüm uygulamaları eklemek için açılır menüden **Tüm dosyalar** seçeneğini belirleyin.

Uygulamalar – Kural, yalnızca işlemin bu hedefle ilgili olması durumunda kullanılır. Açılır menüden **Belirli uygulamalar**'ı seçin ve **Ekle** öğesini tıklatarak yeni dosya veya klasörleri ekleyin veya tüm uygulamaları eklemek için açılır menüden **Tüm uygulamalar** öğesini de seçebilirsiniz.

Kayıt defteri girişleri – Kural, yalnızca işlemin bu hedefle ilgili olması durumunda kullanılır. Açılır menüden **Belirli girişler**'i seçip manuel olarak yazmak için **Ekle** seçeneğini tıklatın veya Kayıt Defterinden anahtar seçmek için **Kayıt Defteri Düzenleyicisini Aç** seçeneğini tıklatabilirsiniz. Ayrıca tüm uygulamaları eklemek için açılır menüden **Tüm girişler** seçeneğini de belirleyebilirsiniz.

> HIPS Tarafından önceden tanımlanan belirli kuralların bazı işlemleri engellenemez ve varsayılan olarak izin verilir. Ek olarak, HIPS tarafından tüm sistem işlemleri izlenmez. HIPS tehlikeli olarak değerlendirilebilecek işlemleri izler.

Önemli işlemlerin açıklaması:

Dosya işlemleri

- **Dosyayı sil** – Uygulama hedef dosyayı silmek için izin istiyor.
- **Dosyaya yaz** – Uygulama hedef dosyaya yazmak için izin istiyor.
- **Diske doğrudan erişim** – Uygulama sıradan Windows prosedürlerini atlatan, standart olmayan bir şekilde diskten okumaya veya diske yazmaya çalışıyor. Bu, dosyaların ilgili kuralları uygulamaksızın değiştirilmesiyle

sonuçlanabilir. Bu işlem, algılamadan kurtulmaya çalışan bir kötü amaçlı yazılımdan, diskin tam kopyasını yapmaya çalışan bir yedekleme yazılımından veya disk birimlerini yeniden düzenlemeye çalışan bir bölüm yöneticisinden kaynaklanıyor olabilir.

- **Genel hook yükle** – MSDN kitaplığından SetWindowsHookEx işlevini çağırmayı ifade eder.

- **Sürücü yükle** - Sisteme sürücülerin kurulması ve yüklenmesi.

Uygulama işlemleri

- **Başka bir uygulamanın hatalarını ayıkla** – İşleme bir hata ayıklayıcı ekler. Bir uygulamanın hataları ayıklanırken davranışının birçok ayrıntısı görüntülenebilir, değiştirilebilir ve verilerine erişilebilir.

- **Başka bir uygulamanın olaylarını durdur** – Kaynak uygulama belirli bir uygulamaya hedeflenen olayları yakalamaya çalışır (örneğin tuş kaydedicinin tarayıcı olaylarını yakalamaya çalışması gibi).

- **Başka bir uygulamayı sonlandır/askıya al** – Bir işlemi askıya alır, sürdürür veya sonlandırır (doğrudan İşlem Gezgininden veya İşlemler bölmesinden erişilebilir).

- **Yeni uygulama başlat** – Yeni uygulamaları veya işlemleri başlatır.

- **Başka bir uygulamanın durumunu değiştir** – Kaynak uygulama hedef uygulamaların belleğine yazmaya çalışır veya onun adına kod çalıştırır. Bu işlev, bu işlemin kullanımını engelleyen bir kuralda hedef bir uygulama olarak yapılandırmak yoluyla önemli bir uygulamayı korumak için kullanışlı olabilir.

Kayıt defteri işlemleri

- **Başlatma ayarlarını değiştir** – Ayarlardaki, Windows açılışında çalıştırılacak uygulamaları tanımlayan tüm değişikliklerdir. Bunlar Windows Kayıt Defteri'nde örneğin Run anahtarı aranarak bulunabilir.

- **Kayıt defterinden sil** – Kayıt defteri anahtarını veya değerini siler.

- **Kayıt defteri anahtarını yeniden adlandır** – Kayıt defteri anahtarlarını yeniden adlandırma.

- **Kayıt defteri değiştiriliyor** - Kayıt defteri anahtarlarının yeni değerlerini oluşturma, mevcut değerleri değiştirme, veri tabanı ağacından veri taşıma veya kayıt defteri anahtarı için kullanıcı veya grup hakları ayarlama.

Bir hedef girerken, belirli kısıtlamalarla joker karakterler kullanabilirsiniz. Belirli bir anahtarın yerine * (yıldız işareti) simgesi kayıt defteri yollarında kullanılabilir. Örneğin *HKEY_USERS***software* ifadesi *HKEY_USER**.default**software* anlamına gelebilir, ancak *HKEY_USERS**S-1-2-21-2928335913-73762274-491795397-7895**.default**software* anlamına gelemez. *HKEY_LOCAL_MACHINE**system**ControlSet** geçerli bir kayıt defteri anahtarı yolu değil. * içeren bir kayıt defteri anahtarı yolu, "bu yol veya bu sembolden sonraki herhangi bir düzeydeki herhangi bir yol" olarak tanımlar. Dosya hedefleri için joker karakter kullanmanın tek yolu budur. Öncelikle, bir yolun belirli bir parçası, ardından joker karakter simgesini (*) izleyen yol değerlendirilir.

Çok genel bir kural oluşturursanız, bu kural türüyle ilgili uyarı gösterilir.

Aşağıdaki örnekte, belirli bir uygulamanın istenmeyen davranışlarını kısıtlamayı göstereceğiz:

1. Kuralı adlandırın ve **Eylem** açılır menüsünden **Engelle** seçeneğini belirleyin (veya daha sonra seçmeyi tercih

ederseniz **Sor**'u belirleyin).

2. Bir kuralın uygulandığı her defasında bildirim görüntülemek için **Kullanıcıya bildir** öğesinin yanındaki kaydırma çubuğunu seçin.

3. **Etkileyen işlemler** bölümünde kural için uygulanacak en az bir işlem seçin.

4. **İleri**'yi tıklayın.

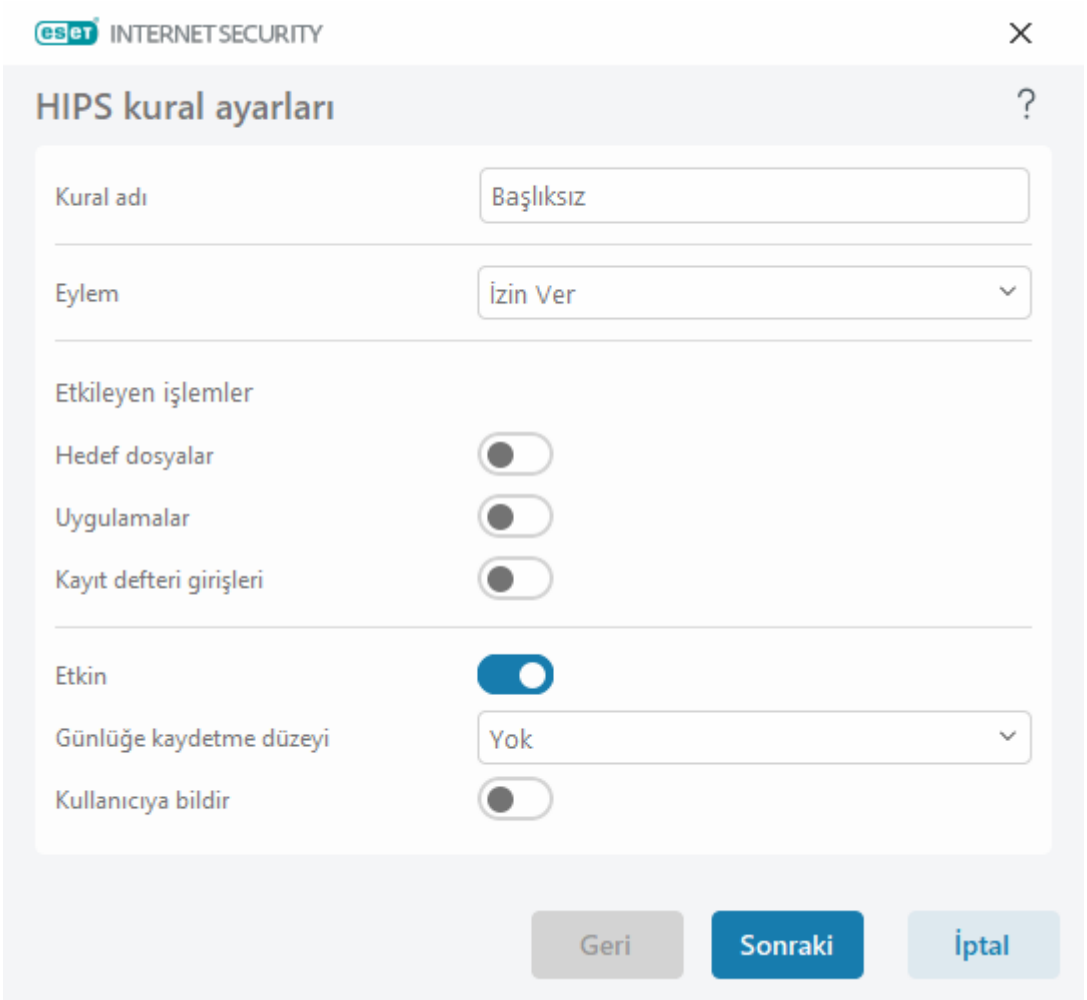
5. Yeni kuralınızı belirlediğiniz uygulamalar üzerinde, seçili uygulama işlemlerinden herhangi birini gerçekleştirmeye çalışan tüm uygulamalar için geçerli kılmak üzere **Kaynak uygulamaları** penceresinde, açılır menüden **Belirli uygulamalar**'ı seçin.

6. **Ekle**'yi, ardından **...** simgesini tıklayıp belirli bir uygulamanın yolunu seçin ve **Tamam**'a basın. Tercih etmeniz halinde daha fazla uygulama ekleyin.
Örneğin: *C:\Program Files (x86)\Untrusted application\application.exe*

7. **Dosyaya yaz** işlemini seçin.

8. Açılır menüden **Tüm dosyalar**'ı seçin. Bu, önceki adımda seçilmiş olan uygulamalar tarafından herhangi bir dosyaya yazma girişimini engeller.

9. Yeni kuralı kaydetmek için **Bitir**'ı tıklatın.



HIPS için uygulama/kayıt defteri yolu ekleme

... seçeneğini tıklatarak bir dosya uygulaması yolu seçin. Bir klasör seçildiğinde, bu konumda bulunan tüm uygulamalar dahil edilir.

Kayıt Defteri Düzenleyicisini aç seçeneği, Windows kayıt defteri düzenleyicisini (regedit) başlatır. Bir kayıt defteri yolu eklerken, **Değer** alanına doğru konumu girin.

Dosya veya kayıt defteri yolu örnekleri:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

HIPS gelişmiş ayarları

Aşağıda verilen seçenekler, hata ayıklamak ve uygulamanın davranışını analiz etmek için kullanışlıdır:

Yüklenmesine her zaman izin verilen sürücüler – Seçili sürücüler, kullanıcı kuralı tarafından açıkça engellenmediği takdirde yapılandırılan filtreleme modundan bağımsız olarak her zaman yüklenebilir.

Engellenen tüm işlemleri günlüğe kaydet - Engellenen tüm işlemler Host Tabanlı Saldırı Önleme Sistemi (HIPS) günlüğüne yazılır. Çok büyük bir günlük dosyası oluşturabileceği ve bilgisayarınızı yavaşlatabileceği için bu özelliği yalnızca sorun giderirken veya ESET Teknik Destek ekibi tarafından talep edildiğinde kullanın.

Başlangıç uygulamalarında değişiklik meydana geldiğinde bildir – Sistem başlangıcına her uygulama eklenişinde veya buradan her uygulama kaldırılışında bir masaüstü bildirimi görüntüler.

Sürücüler her zaman yüklenebilir

Bu listede görünen sürücülerin, kullanıcı kuralı tarafından açıkça engellenmemesi halinde, HIPS filtreleme modundan bağımsız olarak yüklenmesine her zaman izin verilir.

Ekle – Yeni bir sürücü ekler.

Düzenle – Seçili bir sürücüyü düzenler.

Kaldır – Sürücüyü listeden kaldırır.

Sıfırla - Sistem sürücülerinden oluşan bir grubu yeniden yükler.

> Manuel olarak eklediğiniz sürücülerin dahil edilmesini istemiyorsanız **Sıfırla** öğesini tıklatın. Bu seçenek, birçok sürücü eklediyseniz ve bunları listeden manuel olarak silemiyorsanız kullanılabilir.

Oyun modu

Oyun modu; yazılımlarını kesintisiz olarak kullanabilmeyi talep eden, açılır pencerelerle rahatsız edilmek istemeyen ve CPU kullanımının en aza inmesini isteyen kullanıcılara yönelik bir özelliktir. Oyun modu ayrıca

antivirüs etkinliği tarafından kesilmemesi gereken sunumlar sırasında da kullanılabilir. Bu özellik etkinleştirildiğinde tüm açılır pencereler devre dışı bırakılır ve zamanlayıcının etkinlikleri tamamen durdurulur. Sistem koruması arka planda çalışmaya devam eder ancak kullanıcıdan herhangi bir etkileşim talebi olmaz.

Oyun modunu ana program penceresinde **Ayarlar** > **Bilgisayar koruması**'nda  simgesini tıklayarak veya **Oyun modunun** yanındaki  simgesini tıklayarak etkinleştirebilir ya da devre dışı bırakabilirsiniz. Oyun modunu etkinleştirmek olası bir güvenlik riskidir, bu nedenle görev çubuğundaki koruma durumu simgesi turuncu renge döner ve bir uyarı gösterir. Ayrıca, bu uyarıyı turuncu renkli **Oyun modu etkin** mesajının gösterildiği ana program penceresinde de görürsünüz.

Tam ekran uygulama başlattığınız her seferinde Oyun modunun devreye girmesi ve uygulamadan çıktığınızda modun durdurulması için **Gelişmiş ayarlar** (F5) > **Araçlar** > **Oyun modu** altında **Uygulamaları tam ekran modunda çalıştırırken Oyun modunu otomatik olarak etkinleştir** seçeneğini etkinleştirin.

Oyun modunun ne kadar süre geçtikten sonra devre dışı bırakılacağını tanımlamak için **Şu sürenin sonunda Oyun modunu otomatik olarak devre dışı bırak** seçeneğini etkinleştirin.

> Güvenlik duvarı Etkileşimli moddaysa ve Oyun modu etkinleştirilirse, İnternet bağlantısı kurulurken sorun yaşayabilirsiniz. Bu durum Internet'e bağlantısı olan bir oyunu başlattığınızda sorun yaratabilir. Normal koşullarda bu eylemi onaylamanız istenir (iletişim kuralları veya özel durumlar tanımlanmamışsa) ancak Oyun modunda kullanıcıyla etkileşim devre dışıdır. İletişime izin vermek üzere bu sorunla karşılaşabilecek herhangi bir uygulama için bir iletişim kuralı tanımlayın veya Güvenlik duvarında farklı bir Filtreleme modu kullanın. Oyun modu etkinleştirildiğinde, güvenlik riski taşıyabilecek bir web sayfasına veya uygulamaya girdiğinizde bunların engelleneceğini ancak kullanıcı etkileşimi devre dışı olduğundan herhangi bir açıklama veya uyarı görmeyeceğinizi unutmayın.

Başlangıç taraması

Varsayılan olarak, başlangıçta otomatik dosya denetimi, sistem başlatılırken ve algılama altyapısı güncellemeleri sırasında gerçekleştirilir. Bu tarama, Zamanlayıcı yapılandırması ve görevlerine bağlıdır.

Başlangıç taraması seçenekleri, **Sistem başlangıcında dosya denetimi** zamanlayıcı görevinin bir parçasıdır. Ayarlarını değiştirmek için **Araçlar** > **Diğer araçlar** > **Zamanlayıcı** bölümüne gidin, **Başlangıçta otomatik dosya denetimi**'ni ve **Düzenle**'yi tıklatın. Son adımda Başlangıçta otomatik dosya denetimi penceresi görünür (daha fazla ayrıntı için aşağıdaki bölüme bakın).

Zamanlayıcı görevi oluşturma ve yönetme ile ilgili ayrıntılı talimatlar için bkz.Yeni görev oluşturma.

Başlangıçta otomatik dosya denetimi

Sistem başlangıç dosyası denetimi zamanlanmış görevi oluştururken aşağıdaki parametreleri ayarlamak için birkaç seçeneğiniz vardır:

Tarama hedefi açılır menüsü, gizli karmaşık algoritma temelinde sistem başlatma esnasında çalıştırılan dosyalar için tarama derinliğini belirler. Dosyalar aşağıdaki ölçütlere göre azalan sırada düzenlenir:

- **Kayıtlı tüm dosyalar** (birçok dosya taranır)

- **Az kullanılan dosyalar**
- **Yaygın olarak kullanılan dosyalar**
- **Sık kullanılan dosyalar**
- **Yalnızca en sık kullanılan dosyalar** (az sayıda dosya taranır)

İki belirli grup da eklenir:

- **Kullanıcı oturum açmadan önce çalışan dosyalar** – Kullanıcı oturum açmadan erişilebilen konumlardaki dosyaları içerir (hizmetler, tarayıcı yardımcı nesneleri, winlogon bildirimi, Windows zamanlayıcı girdileri, bilinen dll'ler gibi neredeyse tüm başlangıç konumlarını içerir).
- **Kullanıcı oturum açtıktan sonra çalışan dosyalar** - Yalnızca kullanıcı oturum açtıktan sonra erişilebilen konumlardaki dosyaları içerir (yalnızca belirli kullanıcı tarafından çalıştırılan dosyaları, özellikle *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* içindeki dosyaları içerir).

Yukarıda belirtilen her grup için taranacak dosya listeleri sabittir. Sistem başlatılırken çalıştırılan dosyalar için daha düşük bir tarama derinliği seçerseniz taranmayan dosyalar açma veya yürütme işlemi sırasında taranır.

Tarama önceliği – Bir taramanın ne zaman başlayacağını belirlemek için kullanılan öncelik düzeyi:

- **Boştayken** – Görev yalnızca sistem boştayken gerçekleştirilir,
- **En düşük** – sistem yüklemesi olası en düşük düzeyde olduğunda,
- **Düşük** – düşük sistem yüklemesinde,
- **Normal** – ortalama sistem yüklemesinde.

Belge koruması

Belge koruması özelliği, Microsoft Office belgelerini ve Microsoft ActiveX öğeleri gibi Internet Explorer tarafından otomatik olarak karşıdan yüklenen dosyaları açılmadan önce tarar. Belge koruması Gerçek zamanlı dosya sistemi korumasına ek olarak bir koruma katmanı sağlar ve fazla sayıda Microsoft Office belgesi işlemeyen sistemlerde performansı artırmak için devre dışı bırakılabilir.

Belge korumasını etkinleştirmek için **Gelişmiş ayarlar** (F5) > **Tespit altyapısı** > **Zararlı yazılım taramaları** > **Belge koruması**'na gidin ve **Belge korumasını etkinleştir**'in yanındaki kaydırma çubuğunu tıklayın.

> Bu özellik, Microsoft Antivirus API kullanan uygulamalar (ör. Microsoft Office 2000 ve üzeri veya Microsoft Internet Explorer 5.0 ve üzeri) tarafından etkinleştirilir.

Tarama dışı bırakma

Tarama dışı öğeler, nesneleri algılama altyapısı taramasının dışında bırakmanızı sağlar. Tüm nesnelerin tarandığından emin olmak için, tarama dışı öğelerin yalnızca kesinlikle gerekli olduğunda oluşturulmasını öneririz. Bir nesneyi tarama dışında bırakmanızı gerektirecek durumlar, tarama sırasında bilgisayarınızı yavaşlatan büyük veri tabanı girişlerini taramayı veya taramayla çakışan yazılımı içerebilir.

Performansla ilgili tarama dışı bırakma işlemleri - Dosya ve klasörler tarama dışı bırakılır. Performansla ilgili tarama dışı bırakma işlemleri, oyun uygulamalarını dosya düzeyinde tarama dışı bırakmak için veya anormal sistem davranışı ya da artan performans söz konusu olduğunda yararlıdır.

Algılamayla ilgili tarama dışı bırakma işlemleri, nesneleri algılama adı, yol veya hash kullanarak temizleme kapsamının dışında bırakmanıza olanak tanır. Algılamayla ilgili tarama dışı bırakma işlemlerinde dosya ve klasörler performansla ilgili tarama dışı bırakma işlemlerindeki gibi tarama dışında bırakılmaz. Algılamayla ilgili tarama dışı bırakma işlemleri nesneleri yalnızca algılama altyapısı tarafından algılandıklarında ve tarama dışı öğe listesinde uygun bir kural mevcut olduğunda tarama dışında bırakır.

Diğer tarama dışı öğe türleriyle karıştırılmamalıdır:

- Süreç özel durumları – Tarama dışı bırakılan uygulama süreçleriyle ilişkili tüm dosya işlemleri tarama dışında bırakılır (yedekleme hızını ve hizmetlerin sunulmasını iyileştirmek için gerekli olabilir).
- Tarama dışı bırakılan dosya uzantıları
- HIPS özel durumları
- Bulut tabanlı koruma için özel durum filtresi

Performansla ilgili tarama dışı bırakma işlemleri

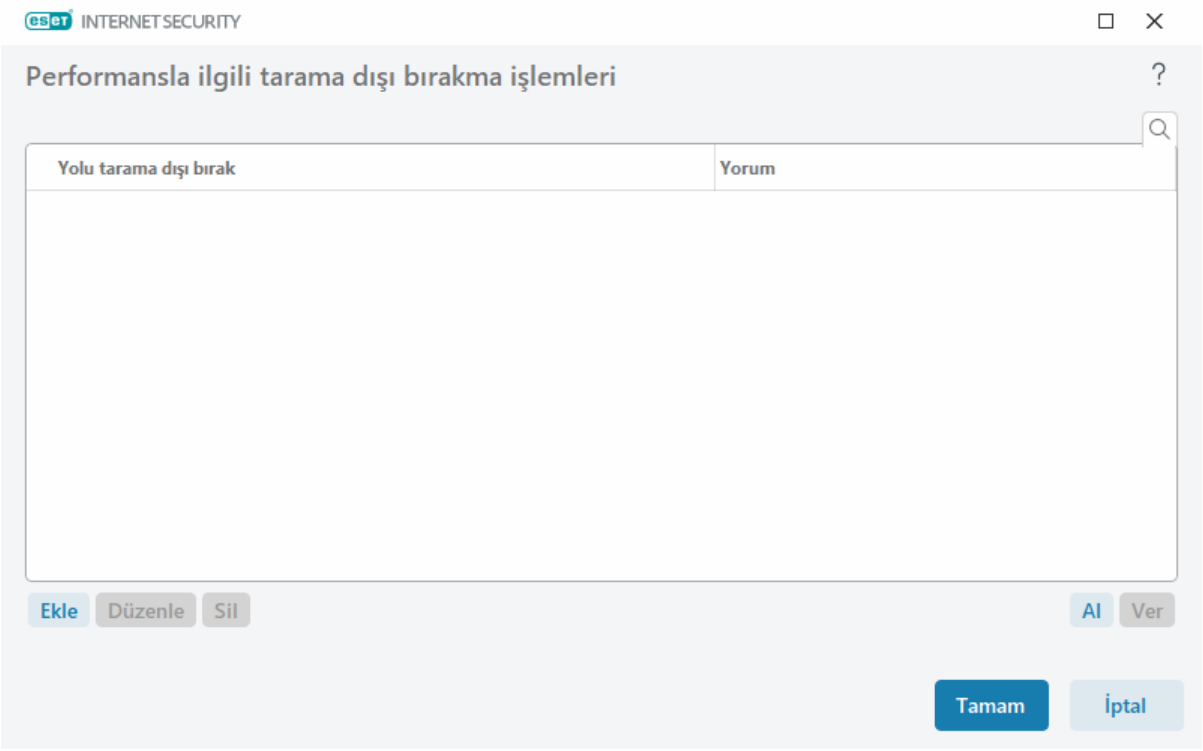
Performansla ilgili tarama dışı bırakma işlemleri, dosya ve klasörleri tarama dışı bırakmanıza olanak tanır.

Tüm nesnelerin tehditlere karşı tarandığından emin olmak için, tarama dışı öğelerin yalnızca kesinlikle gerekli olduğunda oluşturulmasını öneririz. Ancak, bir nesneyi tarama dışında bırakmanızı gerektirebilecek durumlar vardır (ör. tarama sırasında bilgisayarınızı yavaşlatan büyük veri tabanı girişleri veya taramayla çakışan yazılımlar).

Tarama dışında bırakılacak dosya ve klasörleri, **Gelişmiş ayarlar** (F5) > **Algılama altyapısı** > **Tarama dışı bırakma** > **Performansla ilgili tarama dışı bırakma işlemleri** > **Düzenle** üzerinden özel durum listesine ekleyebilirsiniz.

> Bunları Algılamayla ilgili tarama dışı bırakma işlemleri, Tarama dışı bırakılan dosya uzantıları, HIPS taraması dışında bırakılan öğeler veya Tarama dışı bırakılan işlemler ile karıştırmayın.

Bir nesneyi (yol: dosya veya klasör) tarama dışında bırakmak için **Ekle**'yi tıklayıp geçerli yolu girin veya ağaç yapısından söz konusu nesneyi seçin.



Bir dosya içindeki tehdit, söz konusu dosya tarama dışında bırakılma ölçütünü karşılıyorsa, **Gerçek zamanlı dosya sistemi koruması** modülü ya da **Bilgisayar taraması** modülü tarafından algılanmaz.

Denetim öğeleri

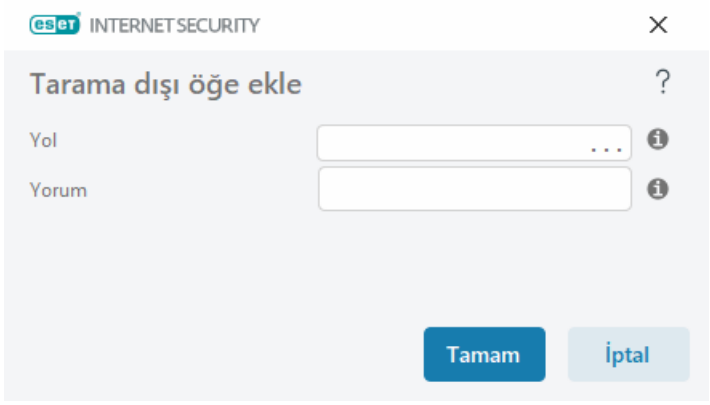
- **Ekle** – Nesneleri algılama dışında bırakır.
- **Düzenle** – Seçili girişleri düzenlemenize olanak tanır.
- **Sil** - Seçilen girişleri kaldırır (birden çok giriş seçmek için CTRL tuşuna basıp tıklayın).

Performansla ilgili tarama dışı bırakma işlemi ekleme veya düzenleme

Bu iletişim penceresi, bu bilgisayar için belirli bir yolu (dosya veya klasörü) tarama dışı bırakır.

Yolu seçin veya manuel olarak girin

Uygun bir yol seçmek için **Yol** alanında **...** seçeneğini tıklayın.
Manuel olarak yazarken aşağıda tarama dışı öğe biçimiyle ilgili daha fazla örnek bulabilirsiniz.



Bir dosya grubunu tarama dışı bırakmak için joker karakterler kullanabilirsiniz. Soru işareti (*?*) tek bir karakteri, yıldız işareti (***) ise sıfır veya daha çok karakter içeren bir dizeyi gösterir.

Tarama dışı öğelerin biçimi

• Bir klasördeki tüm dosyaları tarama dışı bırakmak istiyorsanız söz konusu klasörün yolunu yazın ve şu maskeyi kullanın: ***
• Yalnızca doc uzantılı dosyaları tarama dışında bırakmak istiyorsanız, şu maskeyi kullanın: **.doc*
• Bir yürütülebilir dosyanın adında belirli sayıda karakter varsa (ve karakterler farklılık gösteriyorsa) ve yalnızca ilk karakteri kesin olarak biliyorsanız (örneğin "D"), aşağıdaki biçimi kullanın:
D????.exe (soru işaretleri eksik/bilinmeyen karakterlerin yerine kullanılır)
Örnekler:
• *C:\Tools** - Bir klasör olduğunu ve tüm klasör içeriğinin (dosyalar ve alt klasörler) hariç tutulacağını belirtmek için yolun ters eğik çizgi (\) ve yıldız işaretiyle (*) bitmesi gerekir.
• *C:\Tools*.** - *C:\Tools** ile aynı davranış
• *C:\Tools* – *Tools* klasörü tarama dışı bırakılmaz. Tarayıcı için *Tools* bir dosya adı da olabilir.
• *C:\Tools*.dat* – Bu, *Tools* klasöründeki .dat dosyalarını tarama dışı bırakır.
• *C:\Tools\sg.dat* – Tam olarak bu yolda bulunan belirli dosya tarama dışı bırakılır.

Tarama dışı bırakılan öğelerdeki sistem değişkenleri

Tarama dışı bırakılan öğeler tanımlamak için %PROGRAMFILES% gibi sistem değişkenlerini kullanabilirsiniz.
• Bu sistem değişkenini kullanarak Program Dosyaları klasörünü tarama dışı bırakmak için klasörü tarama dışı öğelere eklerken *%PROGRAMFILES%** yolunu kullanın (yolun sonuna ters bölü çizgisi ve yıldız işareti eklemeyi unutmayın).
• Bir *%PROGRAMFILES%* alt klasöründeki tüm dosyaları ve klasörleri tarama dışı bırakmak istiyorsanız *%PROGRAMFILES%\Excluded_Directory** yolunu kullanın

Desteklenen sistem değişkenlerinin tam listesi

Tarama dışı tutulan yol biçiminde aşağıdaki değişkenler kullanılabilir:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*
Kullanıcı tarafından tanımlanan sistem değişkenleri (*%TEMP%* veya *%USERPROFILE%* gibi) ya da ortam değişkenleri (*%PATH%* gibi) desteklenmemektedir.

Yolun ortasındaki joker karakterler desteklenmez

Bir yolun ortasında joker karakter kullanmak (örneğin *C:\Tools*\Data\file.dat*) işe yarayabilir ancak performans tarama dışı bırakma işlemlerini resmi olarak desteklemez.
Algılamayla ilgili tarama dışı bırakma işlemleri kullanırken bir yolun ortasında özel karakter kullanmayla ilgili herhangi bir kısıtlama yoktur.

Tarama dışı bırakılan öğelerin sıralaması

- Yukarı/aşağı düğmeler kullanılarak Tarama dışı bırakılan öğelerin öncelik düzeyini ayarlama seçeneği yoktur (Güvenlik duvarı kuralları için kurallar yukarıdan aşağı yürütülür).
- Uygulanabilir ilk kural tarayıcı ile eşleştiğinde ikinci uygulanabilir kural değerlendirilmez.
- Ne kadar az kural olursa tarama performansı o kadar iyi olur.
- Eş zamanlı kurallar oluşturmaktan kaçının.

Tarama dışı bırakılan yol biçimi

Bir dosya grubunu tarama dışı bırakmak için joker karakterler kullanabilirsiniz. Soru işareti (*?*) tek bir karakteri, yıldız işareti (***) ise sıfır veya daha çok karakter içeren bir dizeyi gösterir.

Tarama dışı öğelerin biçimi

- Bir klasördeki tüm dosyaları tarama dışı bırakmak istiyorsanız söz konusu klasörün yolunu yazın ve şu maskeyi kullanın: *
- Yalnızca doc uzantılı dosyaları tarama dışında bırakmak istiyorsanız, şu maskeyi kullanın: **.doc*
- Bir yürütülebilir dosyanın adında belirli sayıda karakter varsa (ve karakterler farklılık gösteriyorsa) ve yalnızca ilk karakteri kesin olarak biliyorsanız (örneğin "D"), aşağıdaki biçimi kullanın: *D????.exe* (soru işaretleri eksik/bilinmeyen karakterlerin yerine kullanılır)

Örnekler:

- *C:\Tools** - Bir klasör olduğunu ve tüm klasör içeriğinin (dosyalar ve alt klasörler) hariç tutulacağını belirtmek için yolun ters eğik çizgi (\) ve yıldız işaretiyle (*) bitmesi gerekir.
- *C:\Tools*.** - *C:\Tools** ile aynı davranış
- *C:\Tools* – *Tools* klasörü tarama dışı bırakılmaz. Tarayıcı için *Tools* bir dosya adı da olabilir.
- *C:\Tools*.dat* – Bu, *Tools* klasöründeki .dat dosyalarını tarama dışı bırakır.
- *C:\Tools\sg.dat* – Tam olarak bu yolda bulunan belirli dosya tarama dışı bırakılır.

Tarama dışı bırakılan öğelerdeki sistem değişkenleri

Tarama dışı bırakılan öğeler tanımlamak için %PROGRAMFILES% gibi sistem değişkenlerini kullanabilirsiniz.

- Bu sistem değişkenini kullanarak Program Dosyaları klasörünü tarama dışı bırakmak için klasörü tarama dışı öğelere eklerken *%PROGRAMFILES%** yolunu kullanın (yolun sonuna ters bölü çizgisi ve yıldız işareti eklemeyi unutmayın).
- Bir *%PROGRAMFILES%* alt klasöründeki tüm dosyaları ve klasörleri tarama dışı bırakmak istiyorsanız *%PROGRAMFILES%\Excluded_Directory** yolunu kullanın

Desteklenen sistem değişkenlerinin tam listesi

Tarama dışı tutulan yol biçiminde aşağıdaki değişkenler kullanılabilir:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Kullanıcı tarafından tanımlanan sistem değişkenleri (*%TEMP%* veya *%USERPROFILE%* gibi) ya da ortam değişkenleri (*%PATH%* gibi) desteklenmemektedir.

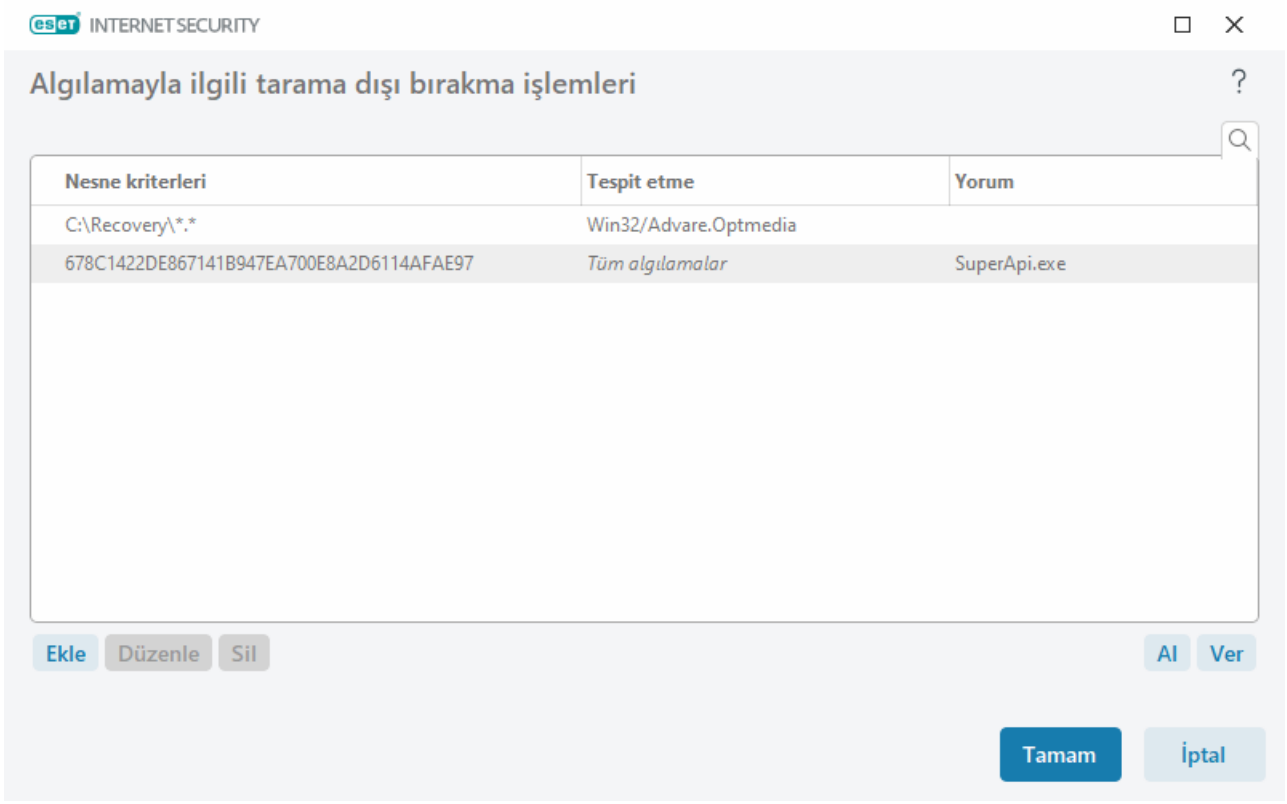
Algılamayla ilgili tarama dışı bırakma işlemleri

Tespitle ilgili tarama dışı bırakma işlemleri, tespit adını, nesne yolunu veya hash'ini filtreleyerek nesneleri temizleme işleminin dışında bırakmanıza olanak tanır.

Algılamayla ilgili tarama dışı bırakma işlemlerinin işleyiş şekli

Algılamayla ilgili tarama dışı bırakma işlemlerinde dosya ve klasörler Performansla ilgili tarama dışı bırakma işlemlerindeki gibi tarama dışında bırakılmaz. Algılamayla ilgili tarama dışı bırakma işlemleri nesneleri yalnızca algılama altyapısı tarafından algılandıklarında ve tarama dışı öğe listesinde uygun bir kural mevcut olduğunda tarama dışında bırakır.

Örneğin (aşağıdaki resmin ilk satırına bakın), bir nesne Win32/Adware.Optmedia olarak algılandığında ve algılanan dosya *C:\Recovery\file.exe* dosyası olduğunda. İkinci satırda uygun SHA-1 hash'ine sahip her bir dosya algılama adına rağmen her zaman tarama dışında bırakılır.



Tüm tehditlerin algılandığından emin olmak için yalnızca mutlaka gerekli olduğunda algılamaların tarama dışı bırakılmasını öneririz.

Dosya ve klasörleri özel durumlar listesine eklemek için **Gelişmiş ayarlar** (F5) > **Algılama altyapısı** > **Tarama dışı bırakma** > **Algılamayla ilgili tarama dışı bırakma işlemleri** > **Düzenle**'ye gidin.

> Bunları Performansla ilgili tarama dışı bırakma işlemleri, Tarama dışı bırakılan dosya uzantıları, HIPS taraması dışında bırakılan öğeler veya Tarama dışı bırakılan işlemler ile karıştırmayın.

Bir nesneyi (algılama adına veya hash'ine göre) algılama altyapısı dışında bırakmak için **Ekle**'yi tıklayın.

İstenmeyen türden olabilecek uygulamalar ve Tehlikeli olabilecek uygulamalar için tespit adına göre tarama dışı bırakma da oluşturulabilir:

- Tespitin bildirildiği uyarı penceresinde (**Gelişmiş seçenekleri göster**'i ve ardından **Tespit dışında bırak**'ı seçin).
- Tespiti tarama dışı bırakma sihirbazını kullanarak Günlük Dosyaları içerik menüsünden.
- **Araçlar** > **Diğer araçlar** > **Karantina**'yı tıkladıktan sonra karantinaya alınan dosyayı çift tıklayarak ve içerik menüsünden **Geri yükle ve tarama dışında bırak**'ı seçerek oluşturulabilir.

Algılamayla ilgili tarama dışı bırakma işlemlerinde nesne kriterleri

- **Yol** – Belirli bir yol (veya herhangi bir yol) için algılamayla ilgili tarama dışı bırakma işlemini sınırlandırın.
- **Tespit adı** - Tarama dışı bırakılan bir dosyanın yanında bir tespit adı varsa bu, dosyanın yalnızca söz konusu tespit için tarama dışı bırakıldığı, ancak tamamen dışarıda bırakılmadığı anlamına gelir. Dosya daha sonra başka bir zararlı yazılımdan etkilenirse tespit edilecektir.
- **Hash** – Bir dosyayı; dosya türü, konumu, adı veya uzantısı ne olursa olsun belirtilen hash'e SHA-1 göre

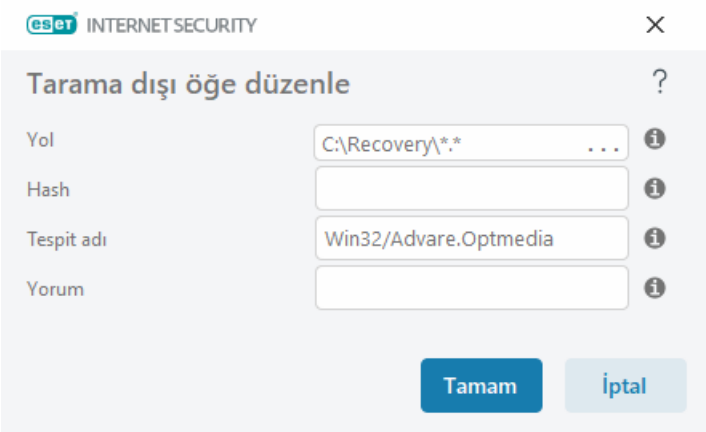
hariç tutar.

Algılamayla ilgili tarama dışı bırakma işlemi ekleme veya düzenleme

Tespit etme

Geçerli bir ESET algılaması adı sağlanmalıdır. Geçerli algılama adı için Günlük dosyaları'na bakın ve Günlük dosyaları açılır menüsünden **Algılamalar**'ı seçin. ESET Internet Security ürününde hatalı pozitif bir örnek algılandığında bu seçenek kullanılır. Gerçek sızıntılar için tarama dışı öğeler çok tehlikeli olduğundan, **Yol maskesi** alanındaki **...** simgesini tıklayarak yalnızca etkilenen dosyaları/klasörleri ve/veya yalnızca geçici bir süreliğine tarama dışı bırakmanız önerilir. Tarama dışı bırakma İstenmeyen türden olabilecek uygulamalar, tehlikeli olabilecek uygulamalar ve şüpheli uygulamalar için de geçerlidir.

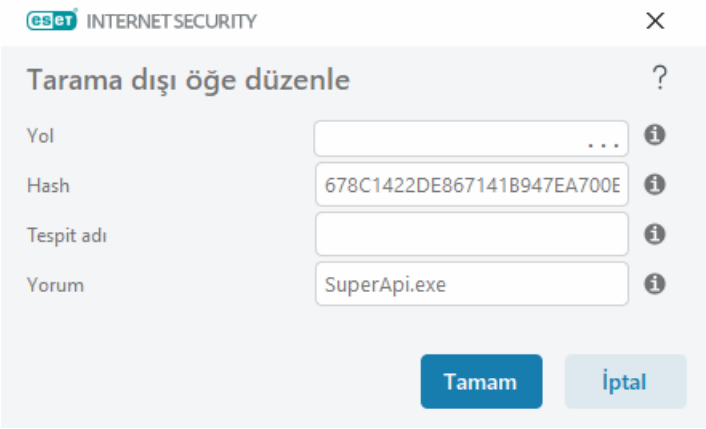
Tarama dışı bırakılan yol biçimi bölümüne de bakın.



Aşağıdaki Algılamayla ilgili tarama dışı bırakma işlemleri için örneğe bakın.

Karmayı hariç tut

Bir dosyayı; dosya türü, konumu, adı veya uzantısı ne olursa olsun belirtilen hash'e SHA-1 göre hariç tutar.



Algılama adına göre tarama dışı bırakma
Belirli bir algılamayı adına göre tarama dışında bırakmak için geçerli algılama adını girin: Win32/Adware.Optmedia
Ayrıca, bir algılamayı ESET Internet Security uyarı penceresinden hariç tuttuğunuzda aşağıdaki biçimi de kullanabilirsiniz:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Denetim öğeleri

- **Ekle** – Nesneleri algılama dışında bırakır.
- **Düzenle** – Seçili girişleri düzenlemenize olanak tanır.
- **Sil** - Seçilen girişleri kaldırır (birden çok giriş seçmek için CTRL tuşuna basıp tıklayın).

Algılama özel durum sihirbazı oluşturma

Algılamayla ilgili tarama dışı bırakma işlemi Günlük dosyaları içerik menüsünden de oluşturulabilir (zararlı yazılım algılamaları için kullanılamaz):

1. Ana program penceresinde şu yolu izleyin: **Araçlar** > **Diğer araçlar** > **Günlük dosyaları**.
2. **Algılamalar günlüğünde** bir algılamayı sağ tıklayın.
3. **Tarama dışı öğe oluştur**'u tıklayın.

Tarama dışı bırakma kriterlerine dayalı olarak en az bir algılamayı tarama dışı bırakmak için **Kriteri değiştir**'i tıklayın:

- **Kesin dosyalar** – Her dosyayı SHA-1 hash'ine göre tarama dışı bırakın.
- **Algılama** – Her dosyayı algılama adına göre tarama dışı bırakın.
- **Yol ve Algılama** – Her dosyayı dosya adı da dahil olmak üzere (ör. *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*) algılama adına ve yoluna göre tarama dışı bırakın.

Önerilen seçenek algılama türüne göre önceden seçilidir.

İsteğe bağlı olarak, **Tarama dışı öğe oluştur**'u tıklamadan önce **Yorum** ekleyebilirsiniz.

HIPS taraması dışında bırakılan öğeler

Tarama dışı bırakılan öğeler, işlemleri HIPS Derin Davranışsal İnceleme'den hariç tutmanıza olanak tanır.

HIPS tarama dışı bırakma işlemlerini düzenlemek için **Gelişmiş ayarlar** (F5) **Tespit altyapısı** > **HIPS** > **Temel** > **Tarama Dışı Bırakma İşlemleri** > **Düzenle**'ye gidin.

Tarama dışı bırakılan dosya uzantıları, Algılamayla ilgili tarama dışı bırakma işlemleri, Performansla ilgili tarama dışı bırakma işlemleri veya Tarama dışı bırakılan işlemler ile karıştırmayın.

Bir nesneyi tarama dışında bırakmak için **Ekle**'yi tıklayın ve nesnenin yolunu girin veya ağaç yapısından söz konusu nesneyi seçin. Ayrıca seçilen girişleri Düzenleyebilir veya Kaldır.

ThreatSense parametreleri

ThreatSense, birçok karmaşık tehdit algılama yönteminden oluşur. Bu teknoloji proaktiftir; yani, yeni bir tehdidin ilk yayılmaya başladığı zamanlarda da koruma sağlar. Sistem güvenliğini önemli ölçüde yükseltmek üzere birlikte çalışan kod analizinin, kod öykünmesinin, genel imzaların ve virüs imzalarının bir bileşimini kullanır. Tarama altyapısı birkaç veri akışını aynı anda denetleme, böylece verimliliği ve algılama hızını azamiye çıkarma yeteneğindedir. ThreatSense teknolojisi ayrıca kök setlerini de başarıyla ortadan kaldırır.

ThreatSense teknolojisi ayar seçenekleri, birkaç tarama parametresi belirtmenize olanak sağlar:

- Taranacak dosya türleri ve uzantılar
- Çeşitli algılama yöntemlerinin bileşimi
- Temizleme düzeyleri, vb.

Ayarlar penceresine girmek için ThreatSense teknolojisini kullanan herhangi bir modülün Gelişmiş ayarlar penceresinde **ThreatSense parametrelerini** tıklatın. Farklı güvenlik senaryoları farklı yapılandırmalar gerektirebilir. Bu göz önüne alınarak, ThreatSense aşağıdaki koruma modülleri için ayrı ayrı yapılandırılabilir nitelikte hazırlanmıştır:

- Gerçek zamanlı dosya sistemi koruması
- Boşta durumu taraması
- Başlangıç taraması
- Belge koruması
- E-posta istemci koruması
- Web erişimi koruması
- Bilgisayar taraması

ThreatSense parametreleri her modül için optimize edilmiştir ve bu parametrelerin değiştirilmesi sistemin çalışmasını önemli ölçüde etkileyebilir. Örneğin, parametreleri çalışma zamanı paketleyicilerini her zaman tarayacak şekilde değiştirmek veya Gerçek zamanlı dosya sistemi koruması modülünde gelişmiş sezgisel taramayı etkinleştirmek sistemin yavaşlamasına neden olabilir (normalde, bu yöntemler kullanılarak yalnızca yeni oluşturulmuş dosyalar taranır). Bilgisayar taraması dışındaki tüm modüller için varsayılan ThreatSense parametrelerini değiştirmeden bırakmanızı öneririz.

Taranacak nesneler

Bu bölüm, hangi bilgisayar bileşenlerinin ve dosyaların sızıntılara karşı taranacağını tanımlamanıza olanak tanır.

İşletim belleği – Sistemin işletim belleğine saldırıda bulunan tehditler için tarama yapar.

Önyükleme kesimleri/UEFI – Önyükleme kesimlerini ana önyükleme kaydında zararlı yazılım olup olmadığını algılamak için tarar. UEFI hakkında sözlükten daha fazla bilgi edinin.

E-posta dosyaları – Program aşağıdaki uzantıları destekler: DBX (Outlook Express) ve EML.

Arşivler – Program aşağıdaki uzantıları ve diğer birçok uzantıyı destekler: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE.

Kendi kendini ayıklayan arşivler – Kendi kendini ayıklayan arşivler (SFX) kendilerini ayıklayabilen arşivlerdir.

Çalışma zamanı paketleyicileri – Çalışma zamanı paketleyicileri, yürütüldükten sonra (standart arşiv türlerinin aksine) bellekte açılır. Standart statik paketleyicilere ek olarak (UPX, yoda, ASPack, FSG vb.) tarayıcı, kod öykünmesini kullanarak başka birçok paketleyici türünü tanıyabilir.

Tarama seçenekleri

Sistemi sızıntılara karşı tararken kullanılacak yöntemleri seçin. Aşağıdaki seçenekler kullanılabilir:

Sezgisel tarama – Sezgisel tarama, programların etkinliğini (kötü amaçlı) analiz eden bir algoritmadır. Bu teknolojinin en temel getirisi, var olmayan veya önceki algılama altyapıları tarafından bilinmeyen kötü amaçlı yazılımları tanıma özelliğine sahip olmasıdır. Olumsuz tarafıysa az da olsa yanlış uyarı verme olasılığıdır.

Gelişmiş sezgisel tarama/DNA/Akıllı imzalar – Gelişmiş sezgisel tarama ESET tarafından geliştirilen benzersiz bir sezgisel tarama algoritmasıdır. Bilgisayar solucanlarını ve truva atlarını algılamak için optimize edilmiş ve yüksek düzeyli programlama dillerinde yazılmıştır. Gelişmiş sezgisel tarama kullanımı ESET ürünlerinin tehdit algılama özelliklerini büyük oranda artırır. İmzalar, virüsleri güvenilir bir şekilde algılayabilir ve belirleyebilir. Otomatik güncelleme sistemini kullanarak, tehdidin tespitinden sonraki birkaç saat içinde yeni imzalar kullanılabilir. İmzaların tek olumsuz tarafı, yalnızca bildikleri virüsleri (veya bu virüslerin çok az değiştirilmiş sürümlerini) algılamalarıdır.

Temizleme

Temizleme ayarları, nesneleri temizlerken ESET Internet Security aracının davranışını belirler. 4 temizleme düzeyi vardır:

ThreatSense parametreleri aşağıdaki düzeltme (yani temizlik) düzeylerine sahiptir.

ESET Internet Security Ürününde Düzeltme

Temizleme düzeyi	Açıklama
Algılamayı her zaman düzelt	Herhangi bir son kullanıcı müdahalesi olmadan, nesneler temizlenirken algılamayı düzeltme girişimi. Bazı nadir durumlarda (örneğin sistem dosyaları), tespit düzeltilemezse bildirilen nesne orijinal konumunda bırakılır.
Güvenliyse algılamayı düzelt, değilse olduğu gibi bırak	Herhangi bir son kullanıcı müdahalesi olmadan nesneler temizlenirken algılamayı düzeltme girişimi. Bazı durumlarda (örneğin, sistem dosyaları veya hem temiz hem de etkilenmiş dosyalar bulunan arşivler), algılama düzeltilemezse bildirilen nesne orijinal konumunda bırakılır.

Temizleme düzeyi	Açıklama
Güvenliyse algılamayı düzelt, değilse sor	Nesneler temizlenirken algılamayı düzeltme girişimi. Bazı durumlarda hiçbir işlem gerçekleştirilmezse son kullanıcı interaktif bir uyarı alır ve bir düzeltme işlemi seçmelidir (örneğin, silme veya yoksayma gibi). Bu ayar çoğu durum için önerilir.
Her zaman son kullanıcıya sor	Son kullanıcı, nesneler temizlenirken interaktif bir pencere görüntüler ve bu pencerede bir uyumlulaştırma işlemi seçmeleri gerekir (örneğin silme veya yoksayma). Bu düzey, bir algılama durumunda atılacak adımları bilen daha ileri seviye kullanıcılar için tasarlanmıştır.

Tarama dışı bırakma

Uzantı, dosya adının nokta ile ayrılmış olan parçasıdır. Uzantı bir dosyanın türünü ve içeriğini tanımlar. ThreatSense parametre ayarlarının bu bölümü, taranacak dosyaların türlerini tanımlamanızı sağlar.

Diğer

İsteğe bağlı bilgisayar taraması için ThreatSense altyapısı parametre ayarlarını yapılandırırken **Diğer** bölümünde bulunan aşağıdaki seçenekler de kullanılabilir:

Alternatif veri akışlarını (ADS) tara – NTFS dosya sistemi tarafından kullanılan alternatif veri akışları (ADS), normal tarama teknikleriyle görülemeyen dosya ve klasör ilişkilendirmeleridir. Pek çok sızıntı, kendisini alternatif veri akışları olarak göstererek algılanmamaya çalışır.

Arka plan taramalarını düşük öncelikle çalıştır – Her tarama dizisi belirli miktarda sistem kaynağı tüketir. Sistem kaynaklarını aşırı yükleyen programlarla çalışıyorsanız, düşük öncelikli arka plan taramasını etkinleştirebilir ve uygulamalarınız için kaynak tasarrufu yapabilirsiniz.

Tüm nesneleri günlüğe kaydet – Tarama günlüğü kendi kendine ayıklanan arşivlerde, etkilenmemiş olanlar da dahil olmak üzere taranan tüm dosyaları gösterir (bu işlem çok sayıda tarama günlüğü verisi üreterek tarama günlüğü dosya boyutunu artırabilir).

Akıllı optimizasyonu etkinleştir – Akıllı Optimizasyon etkin durumdayken en yüksek tarama hızları korunur ve en etkili tarama düzeyinin sağlanması için en uygun ayarlar kullanılır. Çeşitli koruma modülleri, farklı tarama yöntemlerinden faydalanarak ve bunları belirli dosya türlerine uygulayarak smart tarama yapabilir. Akıllı Optimizasyon devre dışı bırakılırsa tarama yaparken belirli modüllerin ThreatSense çekirdeğinde yalnızca kullanıcı tarafından tanımlanan ayarlar uygulanır.

Son erişim zaman damgasını koru - Taranan dosyaların erişim zamanını güncellemek yerine özgün erişim zamanını tutmak için bu seçeneği belirleyin (örneğin, veri yedekleme sistemleri ile kullanmak için).

Sınırlar

Sınırlar bölümü, taranacak nesnelerin maksimum boyutunu ve taranacak arşivlerin iç içe geçme düzeylerini belirtmenize olanak sağlar.

Nesne ayarları

Maksimum nesne boyutu – Taranacak nesnelerin maksimum boyutunu tanımlar. Belirli bir antivirüs modülü yalnızca belirtilen boyuttan küçük olan nesneleri tarayacaktır. Bu seçenek yalnızca büyük nesneleri tarama dışında tutmaya yönelik belirli gerekçeleri olabilecek ileri düzey kullanıcılar tarafından değiştirilmelidir. Varsayılan değer:

sınırsız.

Nesne için maksimum tarama süresi (sn.) - Kapsayıcı nesnede (RAR/ZIP arşivi veya birden çok eki olan bir e-posta gibi) dosyaların taranması için maksimum süre değerini tanımlar. Bu ayar bağımsız dosyalar için geçerli değildir. Kullanıcı tanımlı bir değer girilirse ve bu süre sona ererse kapsayıcı nesnede her bir dosyanın taraması bitmiş olsun veya olmasın tarama en kısa sürede sona erer.
Büyük dosyalar içeren bir arşiv olması durumunda, arşivden bir dosya ayıklandığında tarama sonlanır (örneğin, kullanıcı tanımlı bir değişken 3 saniye olduğunda, ancak dosyanın ayıklanması 5 saniye sürdüğünde). Arşivdeki diğer dosyalar, bu süre dolduğunda taranmaz.
Daha büyük arşivler de dahil olmak üzere tarama süresini sınırlamak için **Maksimum nesne boyutu** ve **Arşivdeki dosyanın maksimum boyutu** ayarlarını kullanın (güvenlik risklerinden dolayı önerilmez).
Varsayılan değer: sınırsız.

Arşiv tarama ayarları

Arşiv iç içe geçme düzeyi – Arşiv taramanın maksimum derinliğini belirtir. Varsayılan değer: 10.

Arşivdeki dosyanın maksimum boyutu - Bu seçenek, taranacak arşivlerde bulunan dosyalar için (ayıklandıklarında) maksimum dosya boyutunu belirtmenize olanak sağlar. Maksimum değer **3 GB**'dir.

> Varsayılan değerlerin değiştirilmesi önerilmez; normal koşullarda bunları değiştirmenize neden olacak bir durumla karşılaşmazsınız.

Tarama dışında bırakılan dosya uzantıları

Tarama dışı bırakılan dosya uzantıları, ThreatSense parametrelerinin bir parçasıdır. Tarama dışı bırakılan dosya uzantılarını yapılandırmak için ThreatSense teknolojisini kullanan herhangi bir modül için Gelişmiş ayarlar penceresinde **ThreatSense parametreleri**'ni tıklayın.

Uzantı, dosya adının nokta ile ayrılmış olan parçasıdır. Uzantı bir dosyanın türünü ve içeriğini tanımlar. ThreatSense parametre ayarlarının bu bölümü, taranacak dosyaların türlerini tanımlamanızı sağlar.

> Tarama dışı bırakılan işlemler, HIPS taraması dışında bırakılan öğeler veya Tarama dışı bırakılan dosyalar/klasörler ile karıştırmayın.

Varsayılan olarak tüm dosyalar taranır. Tarama dışında bırakılan dosyaların listesine herhangi bir uzantı eklenebilir.

Belirli dosya türlerinin taranması, belirli uzantıları kullanan programın düzgün şekilde çalışmasını engelliyorsa, dosyaların bunun dışında tutulması gerekebilir. Örneğin MS Exchange sunucuları kullanılıyorsa `.edb`, `.eml` ve `.tmp` uzantılarının tarama dışında bırakılması önerilebilir.

> Listeye yeni bir uzantı eklemek için **Ekle**'yi tıklayın. Boş alana uzantıyı yazıp (örneğin tmp) **Tamam**'ı tıklayın. **Birden fazla değer gir** öğesini seçtiğinizde çizgiler, virgüller veya noktalı virgüller ile ayrılmış birden fazla dosya uzantısı ekleyebilirsiniz (örneğin açılır menüden ayırıcı olarak **Noktalı virgül** öğesini seçin ve `edb;eml;tmp` yazın:
> Özel simge ? (soru işareti) kullanabilirsiniz. Soru işareti herhangi bir simgeyi temsil eder (örneğin `?db`).

Windows işletim sistemindeki bir dosyanın varsa tam uzantısını görmek için **Denetim Masası** > **Klasör Seçenekleri** > **Görünüm** sekmesinde bulunan **Bilinen dosya türleri için uzantıları gizle** seçeneğinin işaretini kaldırın ve bu değişikliği uygulayın.

Ek ThreatSense parametreleri

Bu ayarları düzenlemek için **Gelişmiş Ayarlar** (F5) > **Tespit altyapısı** > **Gerçek zamanlı dosya sistemi koruması** > **Ek ThreatSense parametreleri**'ne gidin.

Yeni oluşturulan ve değiştirilen dosyalar için ek ThreatSense parametreleri

Yeni oluşturulan veya değiştirilen dosyalarda virüs bulaşma olasılığı, mevcut dosyalara kıyasla daha yüksektir. Bu nedenle program, bu dosyaları ek tarama parametreleriyle denetler. ESET Internet Security, imza tabanlı tarama yöntemleriyle birlikte yayınlanan tespit altyapısı güncellemesinden önce yeni tehditleri algılayabilen gelişmiş sezgisel taramayı kullanır.

Yeni oluşturulan dosyalara ek olarak tarama, **Kendiliğinden ayıklanan arşivlerde** (.sfx) ve **Çalışma Zamanı paketleyicilerinde** (dahili olarak sıkıştırılmış yürütülebilir dosyalar) gerçekleştirilir. Varsayılan olarak, arşivler 10. iç içe yerleştirme düzeyine kadar taranır ve gerçek boyutlarından bağımsız olarak denetlenir. Arşiv taraması ayarlarını değiştirmek için **Varsayılan arşiv taraması ayarları**'nın işaretini kaldırın.

Yürütülen dosyalar için ek ThreatSense parametreleri

Dosya yürütmesinde gelişmiş sezgisel tarama – Varsayılan olarak, dosyalar yürütüldüğünde Gelişmiş sezgisel tarama kullanılır. Etkinleştirildiğinde, sistem performansı üzerindeki etkiyi azaltmak için Akıllı optimizasyon ve ESET LiveGrid® uygulamasının etkin olmasını kesinlikle öneririz.

Dosyalar çıkarılabilir medyadan yürütülürken gelişmiş sezgisel tarama - Gelişmiş sezgisel tarama, sanal ortamda kod taklidi yaparak çıkarılabilir medyadan çalıştırılmasına izin verilmeden önce kodun davranışını değerlendirir.

İnternet koruması

İnternet korumasını (Web ve e-posta) yapılandırmak için **Ayarlar** penceresinde **İnternet koruması**'nı tıklayın. Buradan daha ayrıntılı program ayarlarına erişebilirsiniz.

Koruma modüllerini tek tek duraklatmak veya devre dışı bırakmak için  kaydırma çubuğunu tıklayın.

Koruma modüllerini kapatmak, bilgisayarınızın koruma düzeyini düşürebilir.

Koruma modülünün yanındaki dişli simgesini tıklayarak bu modülün gelişmiş ayarlarına erişebilirsiniz.

Ebeveyn Kontrolü modülü internetteki uygunsuz veya zararlı içeriği engelleyerek çocuklarınızı korur.

Internet'e bağlanabilirlik kişisel bilgisayarlardaki standart özelliktir. Ne yazık ki Internet, kötü amaçlı kodun dağıtımının gerçekleştirildiği başlıca ortam haline gelmiştir. Bu nedenle, Web erişimi koruması ayarlarınızı ciddiye almanız büyük önem taşır.

Kimlik Avı koruması, kimlik avı amaçlı içeriği yaydığı bilinen web sayfalarını engellemenizi sağlar. Kesinlikle Kimlik Avı Koruması'nı etkin şekilde bırakmanızı öneririz.

E-posta istemci koruması POP3(S) ve IMAP(S) protokolleri üzerinden alınan e-posta iletişiminin denetimini sağlar. ESET Internet Security, e-posta istemcinize yönelik olan eklenti programını kullanarak e-posta istemcisinden yapılan tüm iletişimler üzerinde denetim sağlar.

Antispam koruması, istenmeyen e-posta iletilerini filtreler.

Antispam Koruması için dişli simgesini tıklayın ve aşağıdaki seçeneklerden birini belirleyin:

- **Yapılandır** – E-posta istemci antispam koruması için gelişmiş ayarları açar.

- **Kullanıcının adres listesi** (etkinleştirilirse) - Antispam kurallarını tanımlamak için adresleri ekleyebileceğiniz, düzenleyebileceğiniz veya silebileceğiniz bir iletişim penceresi açar. Bu listedeki kurallar, geçerli kullanıcıya uygulanır.

- **Genel adres listesi** (etkinleştirilirse) - Antispam kurallarını tanımlamak için adresleri ekleyebileceğiniz, düzenleyebileceğiniz veya silebileceğiniz bir iletişim penceresi açar. Bu listedeki kurallar, tüm kullanıcılara uygulanır.

Protokol filtreleme

Uygulama protokolleri için antivirus koruması, tüm gelişmiş zararlı yazılım tarama tekniklerini sorunsuz bir şekilde bütünleştiren ThreatSense tarama altyapısı tarafından sağlanır. Protokol filtreleme, kullanılan İnternet tarayıcısından veya e-posta istemcisinden bağımsız olarak otomatik çalışır. Şifreli (SSL/TLS) ayarlarını düzenlemek için **Gelişmiş Ayarlar** (F5) > **Web ve e-posta** > **SSL/TLS**'ye gidin.

Uygulama protokolü içerik filtresini etkinleştir – Protokol filtrelemeyi devre dışı bırakmak için kullanılabilir. Birçok ESET Internet Security bileşeninin (Web erişim koruması, E-posta protokolleri koruması, Kimlik Avı, Ebeveyn kontrolü) bu seçeneğe bağlı olduğunu ve bu seçenek olmadan çalışmayacağını unutmayın.

Dışarıda bırakılan uygulamalar – Belirli uygulamaları protokol filtrelemesinin dışında bırakmanıza olanak tanır. Protokol filtrelemenin uyumluluk sorunlarına neden olması durumunda bu yararlıdır.

Tarama dışında bırakılan IP adresleri – Belirli uzak adresleri protokol filtrelemesinin dışında bırakmanıza olanak tanır. Protokol filtrelemenin uyumluluk sorunlarına neden olması durumunda bu yararlıdır.

Şunu ekler: (örneğin *2001:718:1c01:16:214:22ff:fec9:ca5*).

Alt ağ – IP adresi ve maske tarafından tanımlanan alt ağ (bilgisayar grubu) (örneğin: *2002:c0a8:6301:1::1/64*).

Dışarıda bırakılan IP adresi örneği

IPv4 adresleri maske:

- *192.168.0.10* – Kuralın uygulanacağı tek bir bilgisayarın IP adresini ekler.
- *192.168.0.1* ila *192.168.0.99* – Kuralın uygulanacağı IP aralığını (birkaç bilgisayarı kapsayan aralık) belirtmek için başlangıç ve bitiş IP adresleri.
- Bir IP adresi ve maske tarafından tanımlanan alt grup (bilgisayar grubu). Örneğin *255.255.255.0*, *192.168.1.0/24* önekinin ağ maskesidir. Bu da *192.168.1.1* - 192.168.1.254 adres aralığı anlamına gelir.

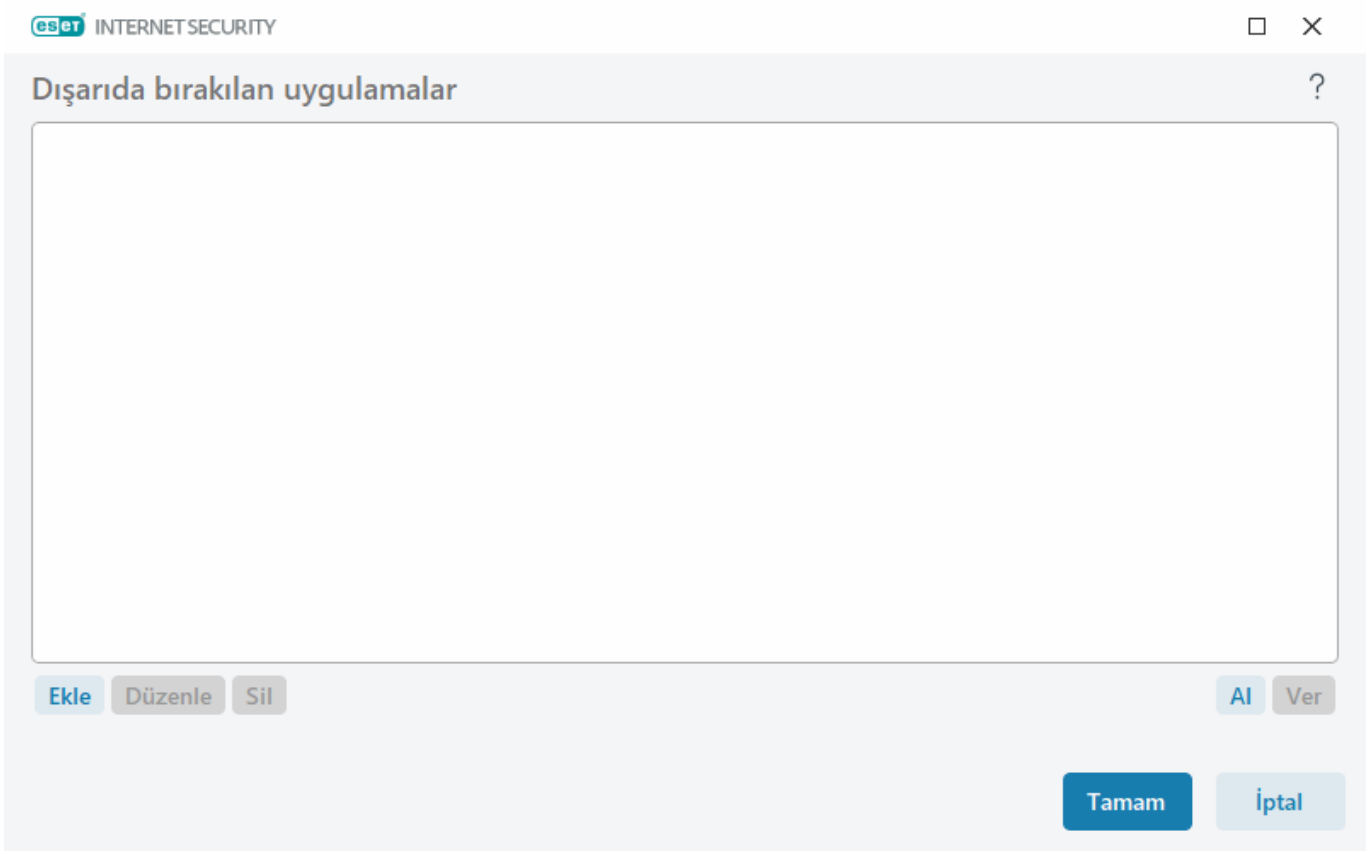
IPv6 adresi ve maske:

- *2001:718:1c01:16:214:22ff:fec9:ca5* – Kuralın uygulanacağı bilgisayarın IPv6 adresi
- *2002:c0a8:6301:1::1/64* – 64 bit ön ek uzunluğuna sahip IPv6 adresi, örneğin *2002:c0a8:6301:0001:0000:0000:0000:0000 to 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

Dışarıda bırakılan uygulamalar

Ağı algılayan belirli uygulamaları içerik filtreleme dışında bırakmak için bu uygulamaları listeden seçin. Seçili uygulamaların HTTP/POP3/IMAP iletişimi tehditlere karşı denetlenmeyecektir. Bu seçeneğin yalnızca, iletişimleri denetlendiğinde düzgün şekilde çalışmayan uygulamalar için kullanılmasını öneririz.

Çalışan uygulama ve hizmetler otomatik olarak burada olacaktır. Protokol filtreleme listesinde gösterilmeyen bir uygulamayı manuel olarak eklemek için **Ekle** seçeneğine tıklatın.

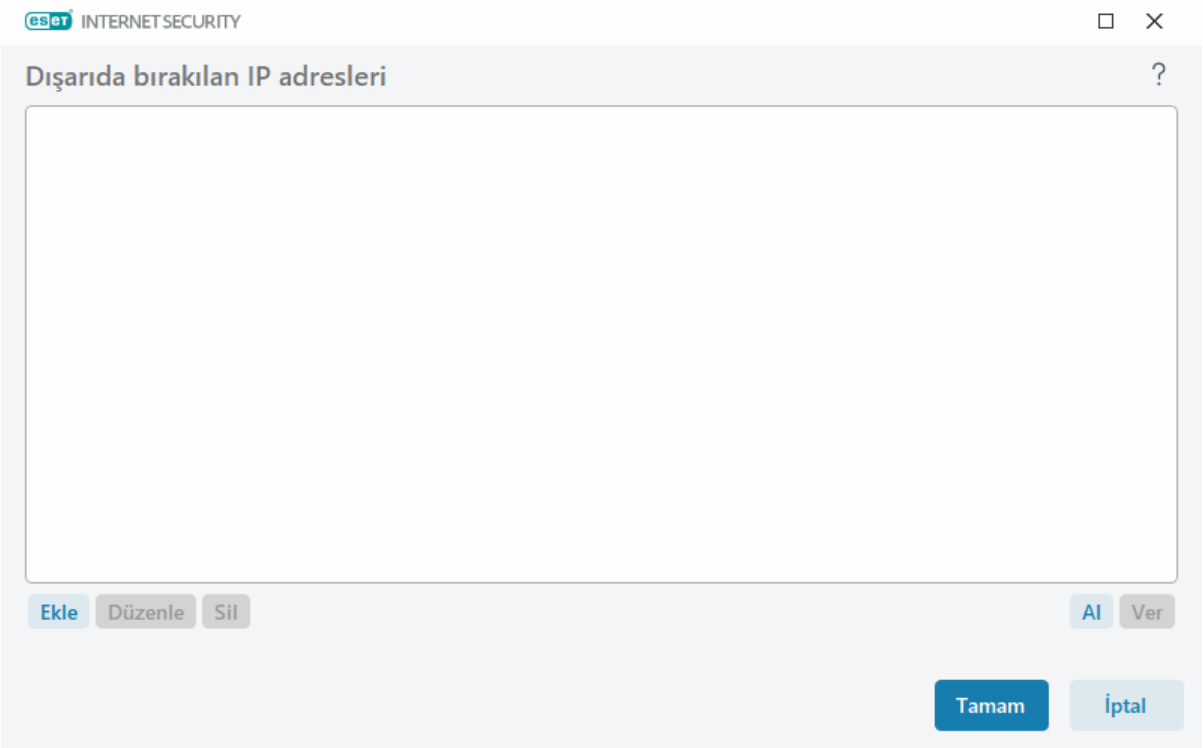


Dışarıda bırakılan IP adresleri

Listedeki girişler protokol içeriği filtreleme dışında bırakılır. Seçili adreslerden/adreslere HTTP/POP3/IMAP iletişimi tehditlere karşı denetlenmez. Bu seçeneği yalnızca güvenilir olduğu bilinen adresler için kullanmanızı öneririz.

Protokol filtreleme listesinde gösterilmeyen bir IP adresi/adres aralığı/uzak nokta alt ağını hariç bırakmak için **Ekle** seçeneğine tıklatın.

Seçili girişleri listeden kaldırmak için **Sil** seçeneğini tıklayın.



IPv4 adresi ekle

Bu, bir kuralın uygulandığı uzak noktanın IP adresini/adres aralığını/alt ağını eklemenize olanak sağlar. Internet Protokolü sürüm 4 eski sürümdür ancak hâlâ yaygın olarak kullanılmaktadır.

Tek adres – Kuralın uygulanacağı bilgisayarın IP adresini ekler (örneğin: *192.168.0.10*).

Adres aralığı – Kuralın uygulanacağı IP aralığını (birkaç bilgisayarın) belirtmek için başlangıç ve bitiş IP adresini girin (örneğin *192.168.0.1*'den *192.168.0.99*'a).

Alt ağ - IP adresi ve maske tarafından tanımlanan alt ağ (bilgisayar grubu).

Örneğin *255.255.255.0*, *192.168.1.0/24* önekinin ağ maskesidir. Bu da *192.168.1.1* - 192.168.1.254 adres aralığı anlamına gelir.

IPv6 adresi ekle

Bu, kuralın uygulandığı uzak noktanın IPv6 adresini/alt ağını eklemenize olanak sağlar. Bu, en yeni internet protokolü sürümüdür ve önceki 4 sürümünün yerini alır.

Tek adres – Kuralın uygulanacağı tek bir bilgisayarın IP adresini ekler (örneğin, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Alt ağ – IP adresi ve maske tarafından tanımlanan alt ağ (bilgisayar grubu) (örneğin: *2002:c0a8:6301:1::1/64*).

SSL/TLS

ESET Internet Security SSL protokolü kullanan iletişimlerde tehditleri denetleyebilir. Güvenilir sertifikaları, bilinmeyen sertifikaları veya SSL korumalı iletişim denetimi dışında tutulan sertifikaları kullanan SSL korumalı iletişimleri incelemek için çeşitli filtreleme modlarını kullanabilirsiniz.

SSL/TLS Protokolü filtrelemesini etkinleştir – Protokol filtrelemesi devre dışıysa program iletişimleri SSL üzerinden taramaz.

SSL/TLS protokolü filtreleme modu aşağıdaki seçeneklerde kullanılabilir:

Filtreleme modu	Açıklama
Otomatik mod	Varsayılan mod sadece, web tarayıcıları ve e-posta istemcileri gibi ilgili uygulamaları tarar. İletişimlerinin taranmasını istediğiniz uygulamaları seçerek bu modu geçersiz kılabilirsiniz.
Etkileşimli mod	Yeni bir SSL korumalı site girerseniz (bilinmeyen sertifikaya sahip), eylem seçimi iletişim kutusu görüntülenir. Bu mod tarama dışında tutulacak SSL sertifikaları / uygulamalar listesi hazırlayabilmenizi sağlar.
İlke modu	Otomatik mod – Denetim dışında bırakılan sertifikalar tarafından korunan iletişimler hariç tüm SSL korumalı iletişimleri taramak için bu seçeneği belirleyin. Bilinmeyen, imzalı bir sertifika kullanan yeni bir iletişim kurulduğunda, bilgilendirilmezsiniz ve iletişim otomatik olarak filtrelenir. Güvenilir olmayan sertifika sahibi olduğu halde güvenilir olarak işaretlenmiş (güvenilir sertifikalar listesindedir) bir sunucuya erişim sağladığınızda sunucuyla iletişime izin verilir ve iletişim kanalı içeriği filtrelenir.

Filtrelenmiş SSL/TLS uygulamalarının listesi – Belirli uygulamalar için ESET Internet Security davranışını özelleştirmenizi sağlar.

Bilinen sertifikalar listesi – Belirli SSL sertifikaları için ESET Internet Security davranışını özelleştirmenizi sağlar.

Güvenilir etki alanlarıyla iletişimi hariç tut – Etkinleştirildiğinde, güvenilir etki alanlarıyla iletişimler denetim dışı bırakılır. Etki alanı güvenilirliği tümleşik beyaz liste tarafından belirlenir.

Eski SSL v2 protokolünü kullanarak şifrelenmiş iletişimi engelle – SSL protokolünün önceki sürümü kullanılarak gerçekleştirilen iletişim otomatik olarak engellenir.

Kök sertifika

Kök sertifikayı bilinen tarayıcılara ekle – SSL iletişiminin tarayıcılarınızda/e-posta istemcilerinizde düzgün bir şekilde çalışması için ESET kök sertifikasının bilinen kök sertifikalar (yayımcılar) listesine eklenmesi gerekir. Etkinleştirildiğinde ESET Internet Security, ESET SSL Filter CA sertifikasını bilinen tarayıcılara (örneğin, Opera) otomatik olarak ekler. Sistem sertifika deposunu kullanan tarayıcılar için sertifika otomatik olarak eklenir. Örneğin Firefox, sistem sertifika mağazasındaki Kök yetkililerine güvenecek şekilde otomatik olarak yapılandırılır.

Sertifikayı desteklenmeyen tarayıcılara uygulamak için **Sertifikayı Görüntüle** > **Ayrıntılar** > **Dosyaya Kopyala** öğelerini tıklatın ve sonra el ile tarayıcıya alın.

Sertifika geçerliliği

Sertifika güvenilirliği onaylanmazsa - Bazı durumlarda bir web sitesi sertifikası Güvenilir Kök Sertifika Yetkilileri

(TRCA) deposu kullanılarak doğrulanamaz. Bu, sertifikanın birisi (örneğin, bir web sunucusunun veya küçük ölçekli bir şirketin yöneticisi) tarafından imzalandığı anlamına gelir ve bu sertifikanın güvenilir olduğunu düşünmek her zaman risk oluşturmaz. Çoğu büyük ölçekli şirketler (örneğin bankalar) TRCA tarafından imzalanmış sertifika kullanır. **Sertifika geçerliliğini sor** seçeneği (varsayılan olarak seçilidir) işaretlenirse şifreli bir iletişim kurulduğunda kullanıcıdan yapılacak işlemi seçmesi istenir. Doğrulanamayan sertifikalara sahip sitelere şifreli bağlantıları her zaman sonlandırmak için **Sertifikayı kullanan iletişimi engelle** seçeneğini işaretleyebilirsiniz.

Sertifika bozuksa - Bu, sertifikanın hatalı bir şekilde imzalanmış veya hasarlı olduğu anlamına gelir. Bu durumda ESET, **Sertifikayı kullanan iletişimi engelle** seçeneğini işaretli halde bırakmanızı önerir. **Sertifika geçerliliğini sor** seçeneği işaretliyse kullanıcıdan şifreli iletişim kurulduğunda yapılacak işlemi seçmesi istenir.

> **Çizimli örnekler**
>
> Aşağıdaki ESET Bilgi Bankası makaleleri sadece İngilizce dilinde mevcuttur:
> - ESET Windows ev ürünlerindeki sertifika bildirimleri
> - "Şifrelenmiş ağ trafiği: Web sayfalarını ziyaret ederken güvenilir olmayan sertifika"

Sertifikalar

SSL iletişiminin tarayıcılarınızda/e-posta istemcilerinizde düzgün şekilde çalışması için, ESET kök sertifikasının bilinen kök sertifikalar (yayımcılar) listesine eklenmesi önemlidir. **Kök sertifikayı bilinen tarayıcılara ekle** seçeneğinin etkinleştirilmesi gerekir. ESET kök sertifikasını bilinen tarayıcılara (örneğin, Opera ve Firefox) otomatik olarak eklemek için bu seçeneği belirleyin. Sistem sertifika deposunu kullanan tarayıcılar için sertifika otomatik olarak eklenir (ör. Internet Explorer). Sertifikayı desteklenmeyen tarayıcılara uygulamak için **Sertifikayı Görüntüle** > **Ayrıntılar** > **Dosyaya Kopyala** öğelerini tıklatın ve sonra el ile tarayıcıya alın.

Kimi durumlarda, Güvenilen Kök Sertifika Yetkilileri depolama alanı (örn. VeriSign) kullanılarak sertifika doğrulanamayabilir. Bu, sertifikanın birisi tarafından otomatik olarak imzalandığı (örn. bir web sunucusu yöneticisi veya küçük ölçekli bir şirket) anlamına gelir ve bu sertifikanın güvenilir olduğunu kabul etmek her zaman bir risk oluşturmaz.

Çoğu büyük ölçekli şirketler (örneğin, bankalar) TRCA tarafından imzalanmış sertifika kullanır. **Sertifika geçerliliğini sor** seçeneği (varsayılan olarak seçilir) belirlendiyse şifreli bir iletişim kurulduğunda kullanıcıdan yürütülecek eylemi seçmesi istenecektir. Sertifikayı güvenilir olarak veya dışarıda bırakmak üzere işaretleyebileceğiniz bir eylem seçimi iletişim penceresi görüntülenir. Sertifikanın TRCA listesinde olmaması halinde pencere kırmızı renkte olur. Sertifikanın TRCA listesinde olması halinde pencere yeşil renkte olacaktır.

Sertifikayı kullanan iletişimi engelle seçeneğini belirterek, doğrulanmamış sertifikayı kullanan siteyle olan şifreli bağlantıyı her zaman sonlandırabilirsiniz.

Sertifika geçersiz veya bozuksa, bu sertifika süresinin dolduğu veya hatalı bir şekilde otomatik olarak imzalandığı anlamına gelir. Bu durumda sertifikayı kullanan iletişimi engellemenizi öneririz.

Şifrelenmiş ağ trafiği

Sisteminiz SSL protokol taraması kullanmak üzere yapılandırıldıysa aşağıdaki iki durumda sizden bir eylem seçmenizi isteyen iletişim penceresi görüntülenir:

İlk olarak, bir web sitesi doğrulanamayan veya geçersiz bir sertifika kullanıyorsa ve ESET Internet Security bu gibi durumlarda kullanıcıya bunu sormak üzere yapılandırıldıysa (varsayılan olarak doğrulanamaz sertifika için evet,

geçersiz olanlar için hayır), bir iletişim kutusunda bağlantı için **İzin ver** veya **Engelle** seçeneklerinden birini belirlemeniz istenir. Trusted Root Certification Authorities store (TRCA) içinde bulunmayan bir sertifikanın güvenilir olmadığı düşünülür.

İkincisi, **SSL protokolü filtreleme modu Etkileşimli mod** olarak ayarlandıysa bir iletişim kutusunda her web sitesi için trafiği **Tara** veya **Yoksay** seçeneklerinden birini belirlemeniz istenir. Bazı uygulamalar kendi SSL trafiğinin değiştirilmediğini ya da herhangi biri tarafından denetlenmediğini doğrular; bu durumlarda ESET Internet Security ürününün, uygulamanın çalışmaya devam etmesi için bu trafiği **Yoksayması** gerekir.

> **Çizimli örnekler**
>
> Aşağıdaki ESET Bilgi Bankası makaleleri sadece İngilizce dilinde mevcuttur:
> - ESET Windows ev ürünlerindeki sertifika bildirimleri
> - "Şifrelenmiş ağ trafiği: Web sayfalarını ziyaret ederken güvenilir olmayan sertifika"

Her iki durumda da kullanıcı seçilen eylemin hatırlanmasını seçebilir. Kaydedilen eylemler Bilinen sertifikalar listesi içinde depolanır.

Bilinen sertifikalar listesi

Bilinen sertifikalar listesi; belirli SSL sertifikaları için ESET Internet Security davranışını özelleştirmek ve **SSL/TLS protokolü filtreleme modunda Etkileşimli modun** seçilmesi durumunda belirlenecek eylemleri hatırlamak için kullanılabilir. Listeyi **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **SSL/TLS** > **Bilinen sertifikalar listesi** menüsünde görüntüleyebilir ve düzenleyebilirsiniz.

Bilinen sertifikalar listesi penceresinde aşağıdakiler yer alır:

Sütunlar

Ad – Sertifikanın adı.

Sertifika sağlayıcı – Sertifikayı oluşturanın adı.

Sertifikanın konusu – Konu alanı, konu ortak anahtarı alanına kaydedilen ortak anahtarla ilişkili bir bölümü tanımlar.

Erişim – Güvenilirliğine bakılmaksızın, bu sertifika tarafından güvence altına alınan iletişimlere izin vermek/bunları engellemek üzere **Erişim eylemi** için **İzin ver** veya **Engelle** seçeneğini belirleyin. Güvenilen sertifikalara izin vermek ve güvenilmeyenlere ilişkin izin istemek için **Otomatik**seçeneğini belirleyin. Kullanıcıya her zaman ne yapılacağını sormak için **Sor** seçeneğini belirleyin.

Tara – Bu sertifika tarafından güvence altına alınan iletişimleri taramak veya yoksaymak üzere **Tarama eylemi** için **Tara** veya **Yoksay** seçeneğini belirleyin. Otomatik modda taramak ve interaktif modda sormak için **Otomatik** seçeneğini belirleyin. Kullanıcıya her zaman ne yapılacağını sormak için **Sor** seçeneğini belirleyin.

Denetim öğeleri

Ekle – Yeni bir sertifika ekleyin, erişim ve tarama seçenekleriyle ilgili ayarlarını yapın.

Düzenle – Yapılandırmak istediğiniz sertifikayı belirleyip **Düzenle** öğesine tıklatın.

Sil – Silmek istediğiniz sertifikayı seçip **Kaldır** öğesini tıklayın.

Tamam/İptal – Değişiklikleri kaydetmek isterseniz **Tamam**'ı, değişiklikleri kabul etmeden ayrılmak için **İptal**'i tıklatın.

SSL/TLS filtrelenmiş uygulamaların listesi

SSL/TLS filtreli uygulamalar listesi; belirli uygulamalar için ESET Internet Security davranışını özelleştirmek ve **SSL/TLS protokol filtreleme modu Etkileşimli modda** olduğunda belirlenecek işlemleri hatırlamak için kullanılabilir. Listeyi **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **SSL/TLS** > **SSL/TLS filtrelenmiş uygulamalar listesi** bölümünde görüntüleyebilir ve düzenleyebilirsiniz.

SSL/TLS filtrelenmiş uygulamalar listesi penceresinde şunlar yer alır:

Sütunlar

Uygulama – Dizin ağacından bir çalıştırılabilir dosya seçin, **...** seçeneğini tıklatın veya yolu el ile girin.

Tarama eylemi – İletişimi taramak veya yoksaymak için **Tara** veya **Yoksay** seçeneklerinden birini belirleyin. Otomatik modda taramak ve interaktif modda sormak için **Otomatik** seçeneğini belirleyin. Kullanıcıya her zaman ne yapılacağını sormak için **Sor** seçeneğini belirleyin.

Denetim öğeleri

Ekle – Filtrelenen uygulamayı ekler.

Düzenle - Yapılandırmak istediğiniz uygulamayı seçip **Düzenle**'ye tıklayın.

Sil - Silmek istediğiniz uygulamayı seçip **Sil**'e tıklayın.

İçe AktarmaDışa Aktarma - Uygulamaları bir dosyadan içe aktarın veya geçerli uygulama listenizi bir dosyaya kaydedin.

Tamam/İptal – Değişiklikleri kaydetmek isterseniz **Tamam**'ı, değişiklikleri kabul etmeden ayrılmak için **İptal**'i tıklatın.

E-posta istemcisi koruması

Entegrasyonu yapılandırmak için ESET Internet Security ile e-posta istemcinizin entegrasyonu bölümüne bakın.

E-posta istemcisi ayarları **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **E-posta istemci koruması** > **E-posta istemcileri** altında bulunur.

E-posta istemcileri

İstemci eklentileri ile e-posta korumasını etkinleştir – Devre dışı bırakıldığında e-posta istemcisi eklentileriyle koruma özelliği kapanır.

Taranacak e-posta

Taranan e-postaları seçin:

- **Alınan e-posta**
- **Gönderilen e-posta**
- **Okunan e-posta**
- **Değiştirilen e-posta**

> **İstemci eklentileri ile e-posta korumasını etkinleştir** ayarını etkin halde bırakmanızı öneririz. Tümleştirme etkin veya işlevsel olmasa bile, e-posta iletişimleri Protokol filtreleme (IMAP/IMAPS ve POP3/POP3S) ile korunmaya devam eder.

Etkilenen e-postada gerçekleştirilecek eylem

Eylem yok – Etkinleştirilirse, program etkilenen ekleri belirler, ancak e-postaları hiçbir işlem yapmadan olduğu gibi bırakır.

E-postayı sil – Program kullanıcıyı sızıntıyla/sızıntılarla ilgili olarak uyarır ve iletiyi siler.

E-postayı Silinmiş öğeler klasörüne taşı – Etkilenen e-postalar Silinmiş öğeler klasörüne otomatik olarak taşınır.

E-postayı klasöre taşı (varsayılan eylem) – Etkilenen e-postalar belirtilen klasöre otomatik olarak taşınır.

Klasör – Etkilenen e-postalar algılandığında bunları taşımak isteyeceğiniz özel bir klasör belirtin.

E-posta istemcisiyle tümleştirme

ESET Internet Security Uygulamasının e-posta istemcilerinizle entegre edilmesi, e-posta iletilerindeki kötü amaçlı kodlara karşı gerçekleştirilen etkin koruma düzeyini artırır. E-posta istemciniz destekleniyorsa ESET Internet Security aracında entegrasyonu etkinleştirebilirsiniz. E-posta istemcinizle entegre edildiğinde, ESET Internet Security araç çubuğu, daha etkili e-posta koruması için doğrudan e-posta istemcisine eklenir. Tümleştirme ayarları **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **E-posta istemci koruması** > **E-posta istemcisiyle tümleştirme** altında bulunur.

Microsoft Outlook şu anda desteklenen tek e-posta istemcisidir. E-posta koruması bir eklenti olarak çalışır. Eklentinin en temel getirisi, kullanılan protokolden bağımsız olmasıdır. E-posta istemcisi şifreli bir ileti aldığında, bu iletinin şifresi çözülür ve ileti virüs tarayıcıya gönderilir. Desteklenen Microsoft Outlook sürümlerinin tam listesi için bu ESET Bilgi Bankası makalesine bakın.

Ek işleme optimizasyonu - Optimizasyon devre dışı bırakılırsa tüm ekler hemen taranır. E-posta istemci performansında bir yavaşlama olabilir.

Gelişmiş e-posta istemcisi işleme - E-posta istemcinizle çalışırken sistemde yavaşlama oluyorsa bu seçeneği devre dışı bırakın.

Microsoft Outlook araç çubuğu

Microsoft Outlook koruması bir eklenti modülü olarak çalışır. ESET Internet Security yüklendikten sonra, antivirüs/antispam koruma seçeneklerini içeren bu araç çubuğu Microsoft Outlook'a eklenir:

İstenmeyen posta – Seçilen iletileri istenmeyen posta olarak işaretler. İşaretleme işleminden sonra iletinin "parmak izi", istenmeyen posta imzalarını depolayan merkezi sunucuya gönderilir. Sunucu birkaç kullanıcıdan daha benzer "parmak izleri" alırsa, ileti ileride istenmeyen posta olarak sınıflandırılır.

İstenmeyen posta değil – Seçilen iletileri istenmeyen posta değil olarak işaretler.

Spam adres (Engellendi, spam adresleri listesi) - Yeni bir gönderici adresini Adres listesine Engellendi olarak ekler. Listedeki adreslerden alınan tüm iletiler otomatik olarak istenmeyen posta olarak sınıflandırılır.

Sahtekarlık girişimlerine karşı dikkatli olun – E-posta alıcılarını yanıltarak iletiyi okumaya ve yanıtlamaya yönlendirmek için kullanılan e-posta iletilerindeki çalıntı gönderen adresi.

Güvenilen adres (İzin verilen) - Yeni bir gönderici adresini Adres listesine İzin Verilen olarak ekler. İzin verilen adreslerden alınan tüm mesajlar hiçbir zaman otomatik olarak spam şeklinde sınıflandırılmaz.

ESET Internet Security - ESET Internet Security ana penceresini açmak için simgeyi çift tıklayın.

İletileri yeniden tara – E-posta denetlemesini manuel olarak başlatmanıza olanak sağlar. Denetlenecek iletileri belirtebilir ve alınan postanın yeniden taranmasını etkinleştirebilirsiniz. Daha fazla bilgi için, bkz. E-posta istemci koruması.

Tarayıcı ayarları – E-posta istemci koruması ayar seçeneklerini görüntüler.

Antispam ayarları – Antispam koruması ayar seçeneklerini görüntüler.

Adres defterleri - Dışarıda bırakılan adresler, güvenilen adresler ve istenmeyen posta adresleri listelerine erişebileceğiniz antispam koruması penceresini açar.

Onay iletişim penceresi

Bu uyarı, kullanıcının seçilen eylemi gerçekten yapmak isteyip istemediğini doğrulamasını sağlayarak olası hataları ortadan kaldıracaktır.

İletişim penceresi aynı zamanda onayları devre dışı bırakma seçeneği de sunar.

İletileri yeniden tara

E-posta istemcileriyle tümleşik olan ESET Internet Security araç çubuğu, kullanıcıların e-posta denetimi için birçok seçenek belirtmesini sağlar. **İletileri yeniden tara** seçeneği, iki tarama modu sunar:

Geçerli klasördeki tüm iletiler – Geçerli olarak görüntülenen klasördeki iletileri tarar.

Yalnızca seçili iletiler – Yalnızca kullanıcı tarafından işaretlenen iletileri tarar.

Önceden taranmış iletileri yeniden tara onay kurusu, kullanıcıya önceden taranmış iletiler üzerinde bir tarama daha çalıştırma seçeneğini sunar.

E-posta protokolleri

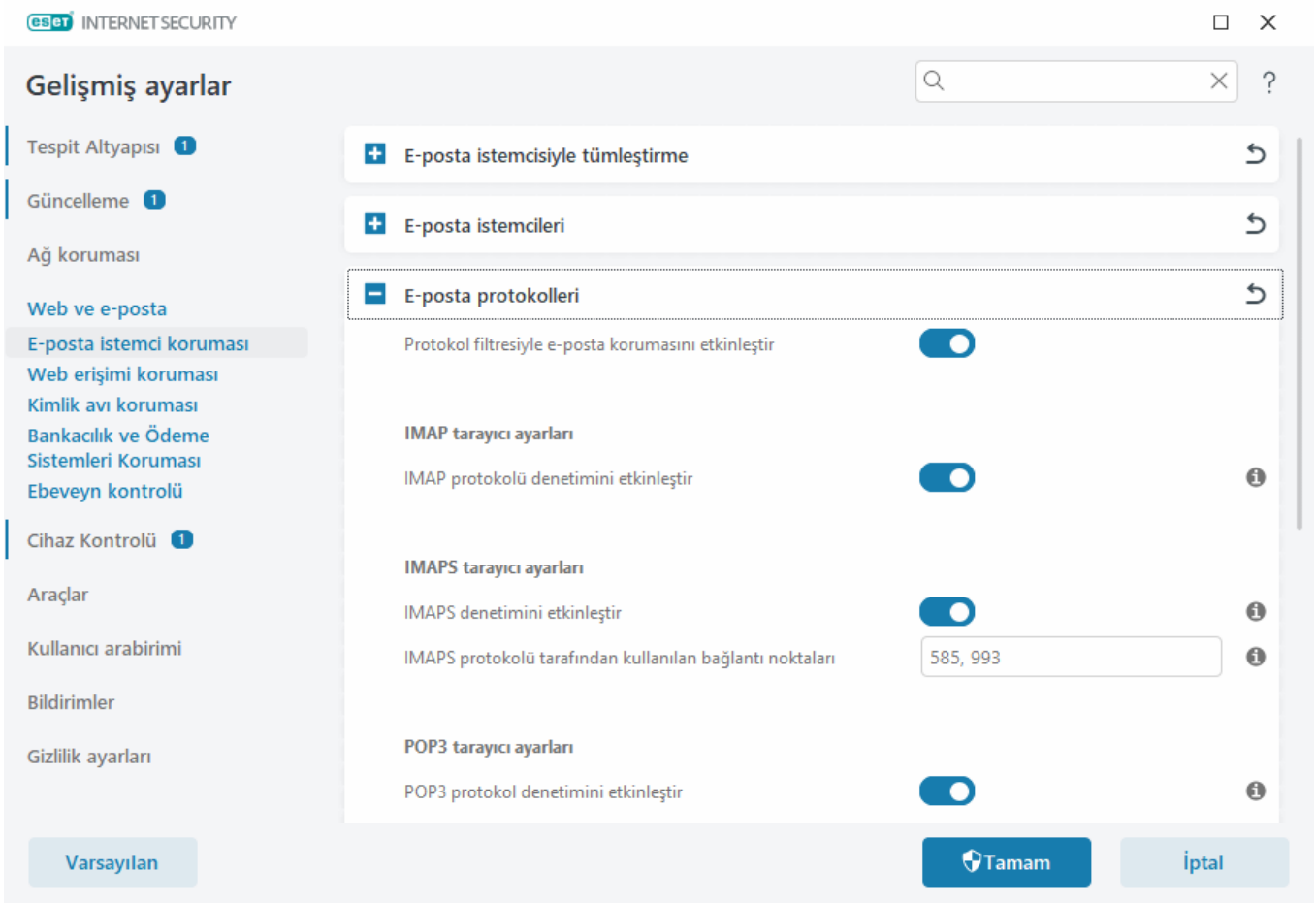
IMAP ve POP3 protokolleri, e-posta istemci uygulamasında e-posta iletişimlerini almak için kullanılan en yaygın protokollerdir. İnternet İleti Erişim Protokolü (IMAP) e-posta alımı için kullanılan başka bir internet protokolüdür. IMAP, POP3'le kıyasla bazı avantajlar sunar; örneğin, birden fazla istemci aynı anda aynı posta kutusuna bağlanabilir ve iletinin okunup okunmadığı, yanıtlanıp yanıtlanmadığı ya da silinip silinmediği gibi ileti durumu bilgilerini koruyabilir. Bu denetimi sağlayan koruma modülü, sistem başlatıldığında otomatik olarak başlatılır ve bellekte etkin halde kalır.

ESET Internet Security, kullanılan e-posta istemcisinden bağımsız olarak bu protokoller için koruma sağlar ve e-posta istemcisinin yeniden yapılandırılmasını gerektirmez. Varsayılan olarak, POP3 ve IMAP protokolleri üzerinden gerçekleşen iletişimlerin tamamı, varsayılan POP3/IMAP bağlantı noktaları ne olursa olsun taranır.
IMAP protokolü taranmaz. Ancak, Microsoft Exchange sunucusuyla iletişim Microsoft Outlook gibi e-posta istemcilerinde entegrasyon modülü tarafından taranabilir.

Protokol filtresiyle e-posta korumasını etkinleştir seçeneğini etkin halde bırakmanızı öneririz. IMAP/IMAPS ve POP3/POP3S protokol denetimini yapılandırmak için **Gelişmiş ayarlar** > **Web ve e-posta** > **E-posta istemci koruması** > **E-posta protokolleri**'ne gidin.

ESET Internet Security, IMAPS (585, 993) ve POP3S (995) protokolleri taramasını da destekler. Bu protokoller sunucu ve istemci arasında bilgilerin aktarılması için şifreli kanal kullanılır. ESET Internet Security, iletişimi SSL (Güvenli Yuva Katmanı) ve TLS (Aktarım Katmanı Güvenliği) protokollerini kullanarak denetler. Program, işletim sistemi sürümü fark etmeksizin, yalnızca **IMAPS/POP3S protokolü tarafından kullanılan bağlantı noktaları** içinde tanımlı bağlantı noktalarında trafiği tarar. Gerekirse diğer iletişim bağlantı noktaları eklenebilir. Birden fazla bağlantı noktası numaraları virgülle ayrılmalıdır.

Şifreli iletişim varsayılan olarak taranır. Tarayıcı kurulumunu görüntülemek için Gelişmiş ayarlar > **Web ve e-posta** > **SSL/TLS**'yi açın.



POP3, POP3S filtresi

POP3 protokolü, bir e-posta istemcisi uygulamasındaki e-posta iletişimini almak için kullanılan en yaygın protokoldür. ESET Internet Security, kullanılan e-posta istemcisi dikkate alınmaksızın bu protokol için koruma sağlar.

Bu denetimi sağlayan koruma modülü, sistem başlatıldığında otomatik olarak başlatılır ve bellekte etkin halde kalır. Modülün doğru çalışması için lütfen etkinleştirildiğinden emin olun – POP3 protokol denetimi e-posta istemcisini yeniden yapılandırmaya ihtiyaç duymadan otomatik olarak gerçekleştirilir. Varsayılan olarak, 110 numaralı bağlantı noktasındaki tüm iletişim taranır, ancak gerekirse başka iletişim bağlantı noktaları eklenebilir. Birden fazla bağlantı noktası numaraları virgülle ayrılmalıdır.

Şifreli iletişim varsayılan olarak taranır. Tarayıcı kurulumunu görüntülemek için Gelişmiş ayarlar > **Web ve e-posta** > **SSL/TLS**'yi açın.

Bu bölümde, POP3 ve POP3S protokolü denetimini yapılandırabilirsiniz.

POP3 protokolü denetimini etkinleştir – Bu seçenek etkinleştirilirse, POP3 üzerinden geçen tüm trafik kötü amaçlı yazılım açısından izlenir.

POP3 protokolü tarafından kullanılan bağlantı noktaları – POP3 protokolü tarafından kullanılan bağlantı noktalarının listesi (varsayılan olarak 110).

ESET Internet Security POP3S protokolü denetimini de destekler. Bu iletişim türü, sunucu ile istemci arasında bilgi aktarmak için şifreli bir kanal kullanır. ESET Internet Security, SSL (Güvenli Yuva Katmanı) ve TLS (Aktarım Katmanı Güvenliği) şifreleme yöntemlerini kullanarak iletişimleri denetler.

POP3S protokolü denetimini kullanma – Şifreli iletişim denetlenmez.

Seçili bağlantı noktaları için POP3S protokolü denetimini kullan – Yalnızca **POP3S protokolü tarafından kullanılan bağlantı noktaları** içinde tanımlanan bağlantı noktalarına yönelik POP3S denetimini etkinleştirmek için bu seçeneği işaretleyin.

POP3S protokolü tarafından kullanılan bağlantı noktaları - Denetlenecek POP3S bağlantı noktalarının listesi (varsayılan olarak 995).

E-posta etiketleri

Bu işlevselliğe ilişkin seçenekleri **Web ve e-posta** > **E-posta istemci koruması** > **Uyarılar ve bildirimler** alanında **Gelişmiş ayarlar** içinde bulabilirsiniz.

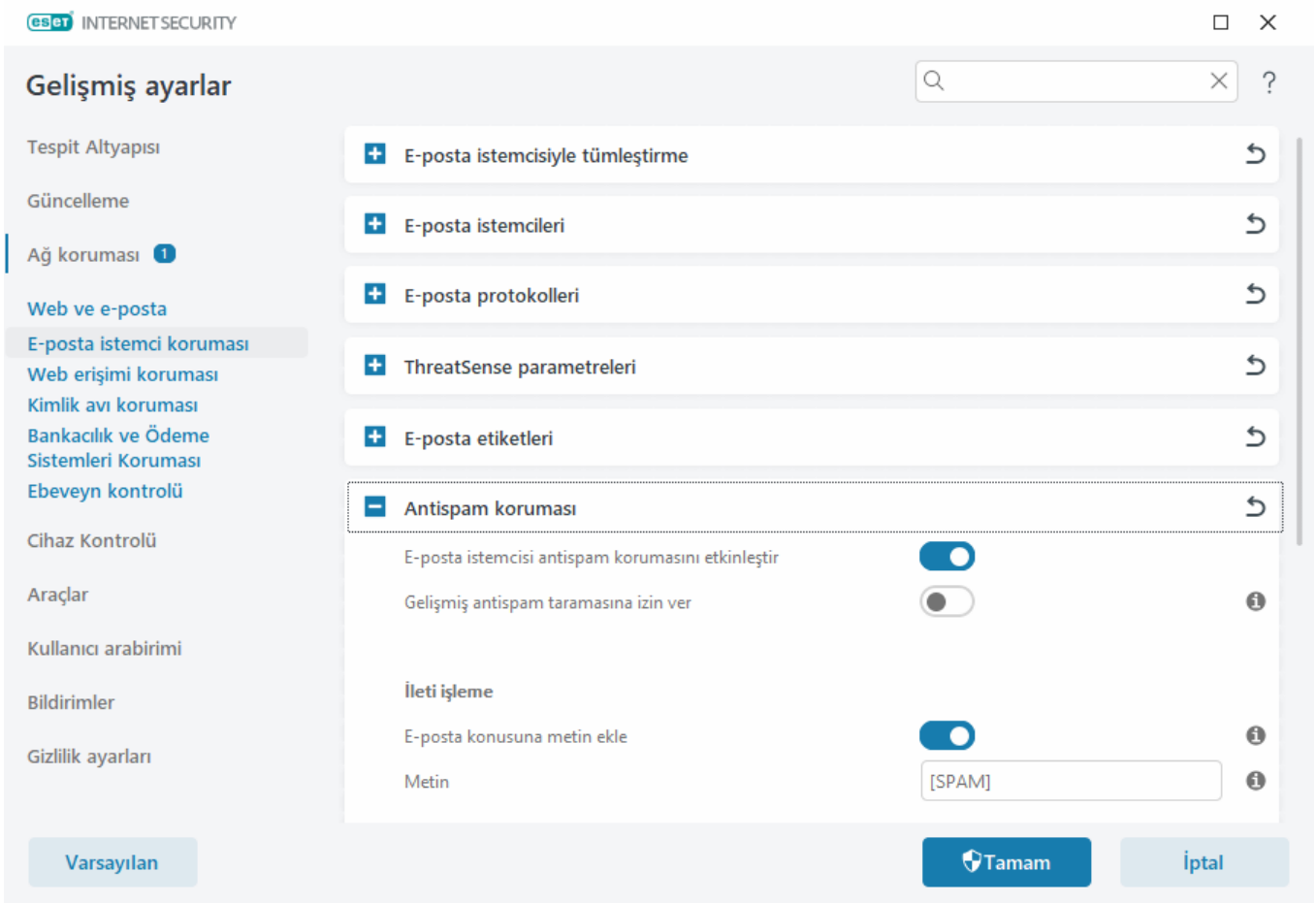
E-posta denetlendikten sonra, iletiye tarama sonucuyla birlikte bir bildirim eklenebilir. **Alınan ve okunan e-postaya etiket mesajları ekle** veya **Gönderilen e-postaya etiket mesajları ekle** seçeneklerinden birini belirleyebilirsiniz. Etiket mesajlarının nadir olarak, sorunlu HTML mesajlarında veya mesajların kötü amaçlı yazılımlar tarafından taklit edilebileceği hallerde atlanabileceğini unutmayın. Etiket mesajları alınan ve okunan e-postaya, giden e-postaya veya her ikisine eklenebilir. Aşağıdaki seçenekler kullanılabilir:

- **Hiçbir zaman** – Hiçbir etiket iletisi eklenmez.
- **Algılama gerçekleştiğinde** – Yalnızca kötü amaçlı yazılım içeren iletiler, "denetlendi" olarak işaretlenir (varsayılan).
- **Taranan tüm e-postalara** – Program taranan tüm e-postalara ileti ekler.

Algılanan e-postanın konusuna eklenecek metin – Etkilenen bir e-postanın konu ön eki biçimini değiştirmek isterseniz bu şablonu düzenleyin. Bu işlev, iletinin "Hello" şeklindeki konusunu şu biçimle değiştirir: "[tespit DETECTION NAME] Hello". %DETECTIONNAME% değişkeni algılamayı temsil eder.

Antispam koruması

Spam adı verilen yetkisiz e-postalar, elektronik iletişimin en büyük sorunlarından biri arasındadır. İstenmeyen posta, tüm e-posta iletişiminin yüzde 30'ini oluşturuyor. Antispam Koruması, bu sorundan koruma hizmeti sunar. Antispam modülü birkaç e-posta güvenliği ilkesini birleştirerek gelen kutusunu temiz tutmak için mükemmel bir filtre özelliği sağlar. Antispam korumasını yapılandırmak için **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **E-posta istemci koruması** > **Antispam koruması**'nı açın.



Spam tespiti için önemli ilkelerden biri, önceden tanımlı güvenilir adreslere (izin verilen) ve spam adreslerine (engellenen) dayalı olarak yetkisiz e-postaları tanımaktır.

Spam olan postaları algılamak için kullanılan birincil yöntem e-posta mesajı özelliklerini taramaktır. Alınan iletiler temel Antispam ölçütüne göre (ileti tanımları, istatistik sezgisel tarama, tanıma algoritmaları ve diğer benzersiz yöntemler) taranır ve bunun sonucunda oluşan indeks değeri iletinin istenmeyen posta olup olmadığını belirler.

E-posta istemcisi antispam korumasını etkinleştir - Bu etkinleştirildiğinde antispam koruması sistem başlangıcında otomatik olarak etkinleştirilir.

Gelişmiş antispam taramasına izin ver - Antispam özelliklerini artırmak ve daha iyi sonuçlar elde edilmesini sağlamak için düzenli aralıklarla ek antispam verileri karşıdan yüklenir.

ESET Internet Security ürünündeki antispam koruması, mesajlar için farklı parametreler ayarlamanıza olanak tanır.

İleti işleme

E-posta konusuna metin ekle – İstenmeyen posta olarak sınıflandırılmış iletilerin konu satırına özel bir önek dizesi eklemenizi sağlar. Varsayılan "[SPAM]" metnidir.

İletileri istenmeyen posta klasörüne taşı – Etkinleştirildiğinde, istenmeyen posta iletileri varsayılan önemsiz e-posta klasörüne taşınır; ayrıca istenmeyen posta değil olarak tekrar sınıflandırılan iletiler de gelen kutusuna taşınır. Bir e-posta iletisini sağ tıklatıp bağlam menüsünden ESET Internet Security öğesini seçtiğinizde geçerli seçenekler arasından tercih yapabilirsiniz.

Klasörü kullan – Etkilenen e-postalar algılandığında bunların taşınmasını isteyeceğiniz özel klasörü belirtin.

İstenmeyen posta iletilerini okundu olarak işaretle – İstenmeyen postaları okundu olarak otomatik işaretlemek

için bu seçeneği etkinleştirin. Bu, dikkatinizi "temiz" iletilere vermenize yardımcı olur.

Yeniden sınıflandırılan iletiyi okunmadı olarak işaretle - Başlangıçta istenmeyen posta olarak sınıflandırılan, ancak daha sonra “temiz" olarak işaretlenen iletiler okunmadı olarak görüntülenir.

Spam puanı günlük kaydı – ESET Internet Security Antispam motoru, taranan her iletiye bir istenmeyen posta puanı atar. İleti antispam günlüğüne (Ana program penceresi > **Araçlar** > **Diğer araçlar** > **Günlük dosyaları** > **Antispam koruması**) kaydedilir.

- **Yok** – Antispam taramasındaki puan günlüğe kaydedilmez.
- **İstenmeyen posta olarak tekrar sınıflandırıldı ve işaretlendi** – SPAM olarak işaretlenen iletiler için istenmeyen posta puanının kaydedilmesini istiyorsanız bu seçeneği belirleyin.
- **Tümü** - Tüm iletiler, günlüğe istenmeyen posta puanıyla kaydedilir.

Önemsiz e-posta klasöründe bir iletiyi tıklattığınızda **Seçili iletileri İSTENMEYEN POSTA DEĞİL olarak tekrar sınıflandır** öğesini seçebilirsiniz; böylece ileti gelen kutusuna taşınır. Gelen kutusunda isyenmeyen posta olduğunu düşündüğünüz bir iletiyi tıklattığınızda **Seçili iletileri İSTENMEYEN POSTA olarak tekrar sınıflandır** öğesini seçebilirsiniz; böylece ileti önemsiz e-posta klasörüne taşınır. Birden çok mesaj seçip bunların hepsi üzerinde aynı anda işlem yapabilirsiniz.

ESET Internet Security; Microsoft Outlook, Outlook Express, Windows Mail ve Windows Live Mail için Antispam korumasını destekler.

Adres işleme sonucu

Yeni adresler eklerken veya e-posta adresi için yapılan işlem değiştirildiğinde ESET Internet Security bildirim mesajları görüntüler. Bildirim iletilerinin içeriği, gerçekleştirmeyi denediğiniz eyleme göre değişiklik gösterir.

Bir dahaki sefere mesajı görüntülemeden işlemi otomatik olarak gerçekleştirmek için **Tekrar sorma** alanını işaretleyin.

Antispam adres listeleri

ESET Internet Security İçindeki Antispam özelliği, adres listeleri için çeşitli parametreler yapılandırmanızı sağlar.

Kullanıcının adres listesini etkinleştir - Kullanıcının adres listesini etkinleştirmek için bu seçeneği etkinleştirin.

Kullanıcının adres listesi - Antispam kurallarını tanımlamak için adresleri ekleyebileceğiniz, düzenleyebileceğiniz veya silebileceğiniz e-posta adresleri listesi. Bu listedeki kurallar, geçerli kullanıcıya uygulanır.

Genel adres listesini etkinleştir - Bu cihazdaki tüm kullanıcılar tarafından paylaşılan genel adres listesini etkinleştirmek için bu seçeneği etkinleştirin.

Genel adres listesi - Antispam kurallarını tanımlamak için adresleri ekleyebileceğiniz, düzenleyebileceğiniz veya silebileceğiniz e-posta adresleri listesi. Bu listedeki kurallar, tüm kullanıcılara uygulanır.

Otomatik olarak izin verin ve kullanıcının adres listesine ekleyin

Adres defterindeki adresleri güvenilir olarak kabul et – Kişi listenizdeki adresler kullanıcının adres listesine eklenmeden güvenilir olarak kabul edilir.

Giden mesajlardaki alıcı adreslerini ekle - Gönderilen mesajlardaki alıcı adreslerini kullanıcının adres listesine izin verilen şekilde ekleyin.

Spam DEĞİL biçiminde yeniden sınıflandırılan mesajlardaki adresleri ekle - Spam DEĞİL biçiminde yeniden sınıflandırılan mesajlardaki gönderen adreslerini kullanıcının adres listesine izin verilen şekilde ekleyin.

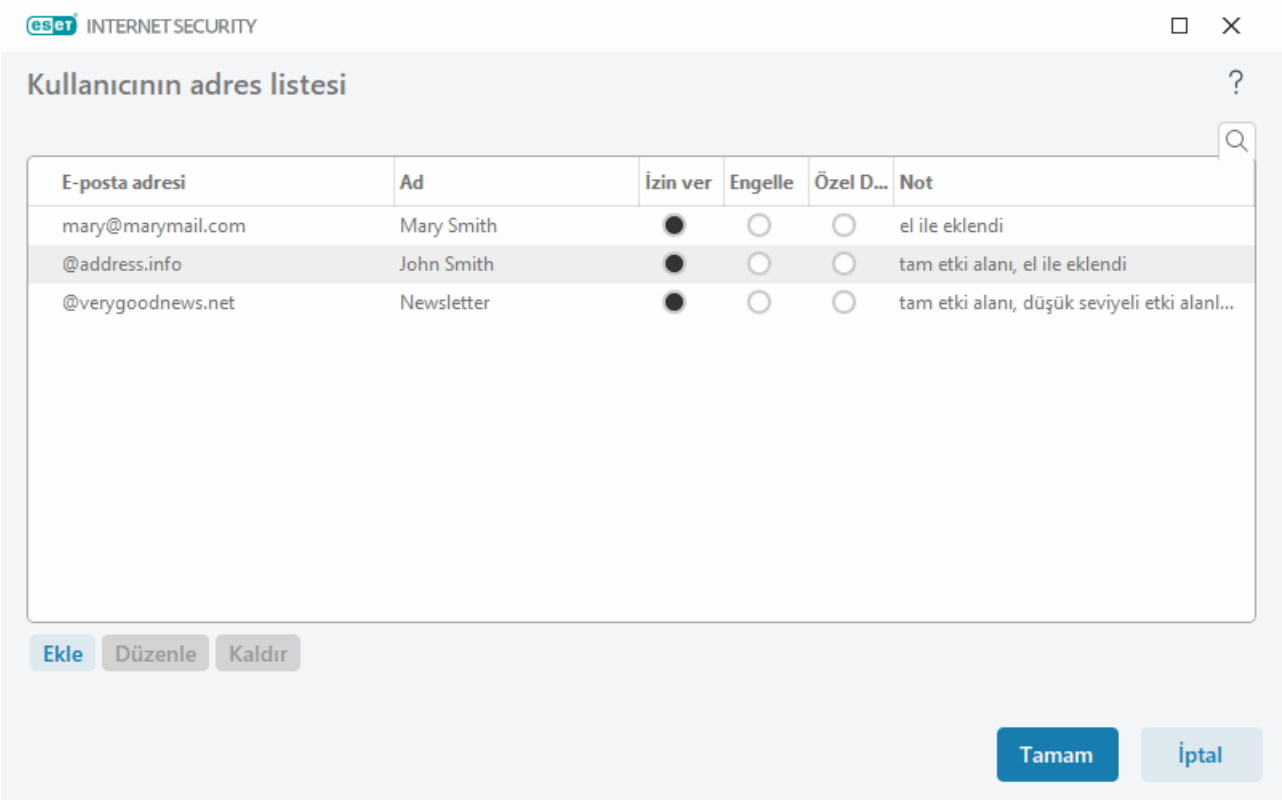
Kullanıcının adres listesine otomatik olarak özel durum şeklinde ekleyin

Kendi hesaplarından adresleri ekle - Mevcut e-posta istemcisi hesaplarındaki adreslerinizi kullanıcının adres listesine özel durum olarak ekleyin.

Adres listeleri

Yetkisiz e-postalara karşı koruma için, ESET Internet Security adres listelerindeki e-posta adreslerini sınıflandırmanıza olanak tanır.

Adres listelerini düzenlemek için **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **E-posta istemci koruması** > **Antispam adres listeleri**'ni açın ve **Kullanıcının adres listesi**'nin veya **Genel adres listesi**'nin yanındaki **Düzenle**'yi tıklayın.



Sütunlar

E-posta adresi - Kuralın uygulanacağı adres.

Ad – Özel kural adı.

İzin Ver/Engelle/Özel Durum - E-posta adresi için hangi işlemin gerçekleştirileceğini belirlemek üzere kullanılan radyo düğmeleri (işlemi hızlı bir şekilde değiştirmek için tercih edilen sütundaki radyo düğmesini tıklayın):

- **İzin ver** - Güvenli olarak kabul edilen ve mesaj almak istediğiniz adresler.
- **Engelle** - Tehlikeli/spam olarak kabul edilen ve mesaj almak istemeyebileceğiniz adresler.
- **Özel durum** - Spam için her zaman kontrol edilen ve kimlik sahtekarlığı yapılarak spam göndermek için kullanılıyor olabilecek adresler.

Not - Kuralın nasıl oluşturulacağı ve etki alanının tamamına/alt düzeydeki etki alanlarına uygulanıp uygulanmayacağı ile ilgili bilgiler.

Adresleri yönetme

- **Ekle** - Yeni adres için kural eklemek üzere tıklayın.
- **Düzenle** - Mevcut bir kuralı düzenlemek için seçin ve tıklayın.
- **Kaldır** - Adres listesinden bir kuralı silmek için seçin ve tıklayın.

Adres ekle/düzenle

Bu pencere, antispam adres listesine adres eklemenize veya bir adresi düzenlemenize ve gerçekleştirilen işlemi yapılandırmanıza olanak sağlar:

E-posta adresi - Kuralın uygulanacağı adres.

Ad – Özel kural adı.

İşlem - Kişinin e-posta adresi **E-posta adresi** alanında belirtilen adresle eşleşirse yapılan işlem:

- **İzin ver** - Güvenli olarak kabul edilen ve mesaj almak istediğiniz adresler.
- **Engelle** - Tehlikeli/spam olarak kabul edilen ve mesaj almak istemeyebileceğiniz adresler.
- **Özel durum** - Spam için her zaman kontrol edilen ve kimlik sahtekarlığı yapılarak spam göndermek için kullanılıyor olabilecek adresler.

Tam etki alanı - Kuralın, kişinin etki alanının tamamına (yalnızca **E-posta adresi** alanında belirtilen adrese değil, *address.info* etki alanındaki tüm e-posta adreslerine) uygulanması için bu seçeneği belirleyin.

Düşük seviyeli etki alanları - Kuralın, kişinin daha düşük düzeyli etki alanlarına uygulanması için bu seçeneği belirleyin (*adres.info*, etki alanını temsil eder; *my.address.info* ise alt etki alanını temsil eder).

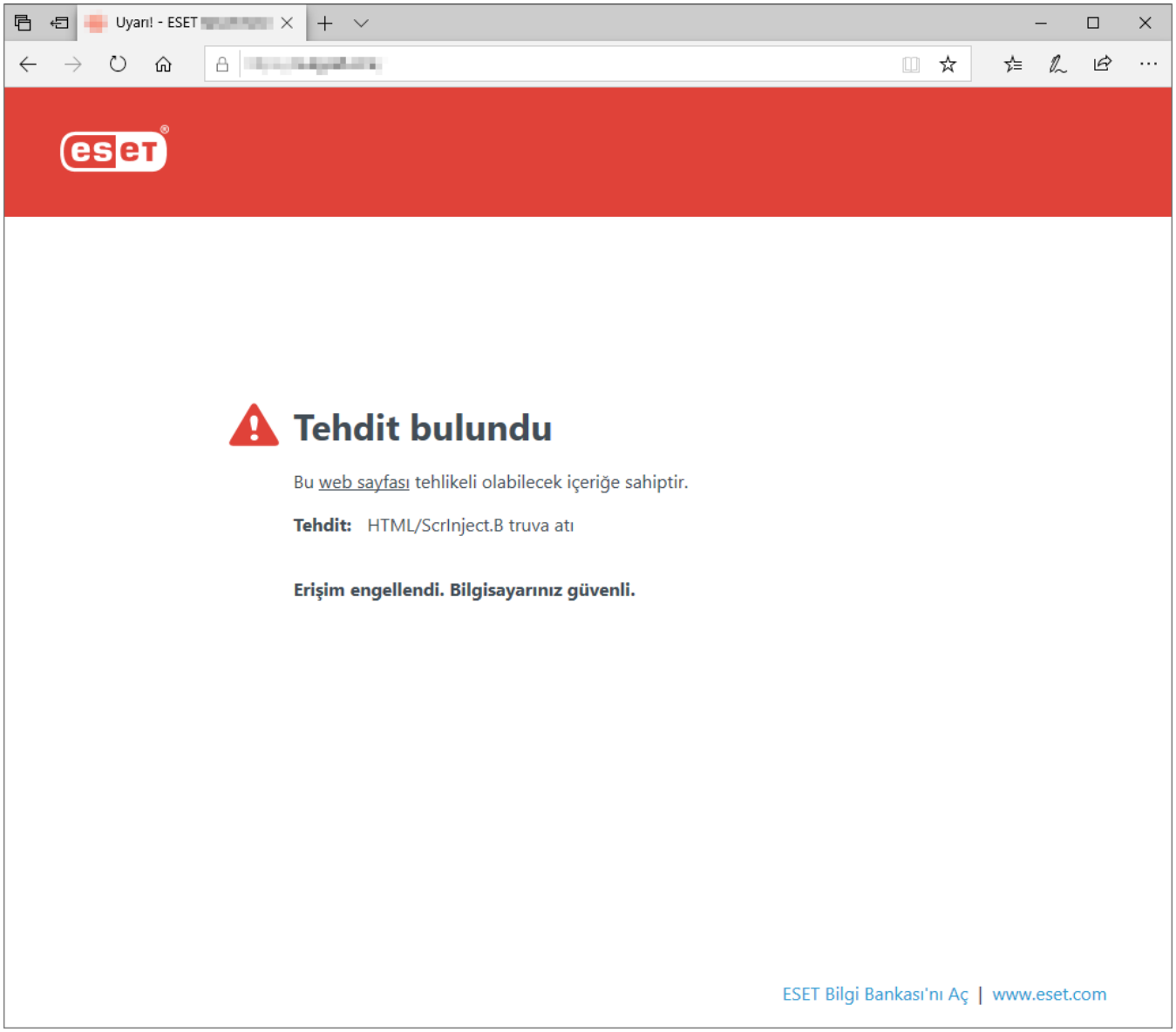
Web erişimi koruması

Internet'e bağlanabilirlik bir kişisel bilgisayardaki standart özelliktir. Ne yazık ki aynı zamanda kötü amaçlı kod aktarımının gerçekleştirildiği ana ortam haline gelmiştir. Web erişimi koruması, web tarayıcıları ile uzak sunucular arasındaki HTTP (Köprü Metni Aktarım Protokolü) ve HTTPS (şifreli iletişim) iletişimlerini tarar.

Kötü amaçlı içeriğe sahip olduğu bilinen web sayfalarına erişim, içerik indirilmeden önce engellenir. Tüm diğer web sayfaları, yüklenirken ThreatSense tarama motoru tarafından taranır ve kötü amaçlı içerik tespit edilmesi durumunda engellenir. Web erişimi koruması, URL adreslerine erişimi engellemenize veya bunlara izin vermenize ve adresleri tarama dışında bırakmanıza olanak sağlar.

Web erişiminin etkinleştirilmesini kesinlikle öneririz. Bu seçeneğe, **ana program penceresi** > **Ayarlar** > **İnternet koruması** > Web erişimi koruması üzerinden erişilebilir.

Web sitesi engellendiğinde web erişimi koruması tarayıcınızda aşağıdaki mesajı gösterir:



Resimli talimatlar

Aşağıdaki ESET Bilgi Bankası makaleleri sadece İngilizce dilinde mevcuttur:

- Güvenilir bir web sitesini Web Erişimi Koruması'nın engelleme işlevinin dışında bırakma
- Bir web sitesini ESET Internet Security aracını kullanarak engelleme

---

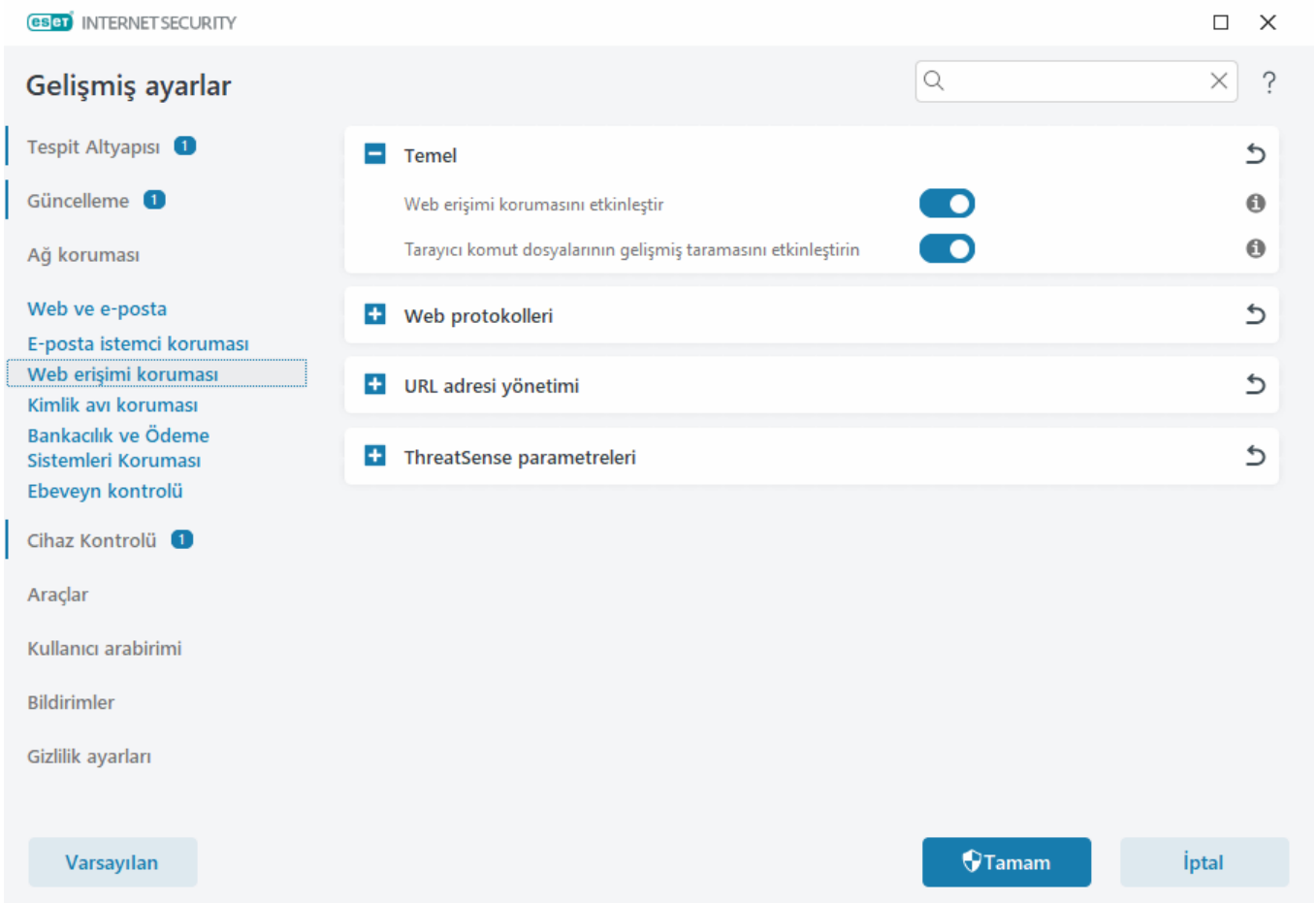
Aşağıdaki seçenekler **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **Web erişim koruması** içinde bulunabilir:

Temel – Bu özelliği Gelişmiş ayarlar'da etkinleştirmek veya devre dışı bırakmak için.

Web protokolleri – Çoğu İnternet tarayıcısı tarafından kullanılan bu standart protokolleri izlemeyi yapılandırmanızı sağlar.

URL adresi yönetimi – Engellenecek, izin verilecek veya denetim dışında bırakılacak URL adreslerini belirtmenizi sağlar.

ThreatSense parametreleri - Gelişmiş virüs tarayıcısı ayarları, taranacak nesne türleri (e-postalar, arşivler vb.), Web erişim koruması için algılama yöntemleri gibi ayarları yapılandırmanıza olanak tanır.



Web erişimi koruması gelişmiş ayarları

Aşağıdaki seçenekler şurada bulunabilir: **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **Web erişim koruması** > **Temel** içinde bulunabilir:

Web erişimi korumasını etkinleştir - Bu seçenek devre dışı bırakıldığında Web erişimi koruması ve Kimlik avı koruması çalışmaz. Bu seçenek yalnızca SSL/TLS protokol filtrelemesi etkin olduğunda kullanılabilir.

Tarayıcı komut dosyaları için gelişmiş taramayı etkinleştir - Bu seçenek etkinleştirildiğinde, İnternet tarayıcıları tarafından yürütülen tüm JavaScript programları algılama altyapısı tarafından denetlenir.

Web erişimi korumasını etkin durumda bırakmanızı kesinlikle öneririz.

Web protokolleri

Varsayılan olarak ESET Internet Security birçok İnternet tarayıcısı tarafından kullanılan HTTP protokolünü izlemek için yapılandırılmıştır.

HTTP Tarayıcı ayarları

HTTP trafiği, tüm uygulamalar için tüm bağlantı noktalarında her zaman izlenir.

HTTPS Tarayıcı ayarları

ESET Internet Security HTTPS protokol denetimini de destekler. HTTPS iletişimi, sunucu ile istemci arasında bilgi aktarmak için şifreli bir kanal kullanır. ESET Internet Security, SSL (Güvenli Yuva Katmanı) ve TLS (Aktarım Katmanı Güvenliği) protokollerini kullanarak iletişimleri denetler. Program, işletim sistemi sürümü fark etmeksizin, yalnızca **HTTPS protokolü tarafından kullanılan bağlantı noktaları** içinde tanımlı bağlantı noktalarındaki (443, 0-65535) trafiği tarar.

Şifreli iletişim varsayılan olarak taranır. Tarayıcı kurulumunu görüntülemek için Gelişmiş ayarlar > **Web ve e-posta** > **SSL/TLS**'yi açın.

URL adresi yönetimi

URL adresi yönetimi bölümü engellenecek, izin verilecek veya içerik taraması dışında bırakılacak HTTP adreslerini belirtmenize olanak sağlar.

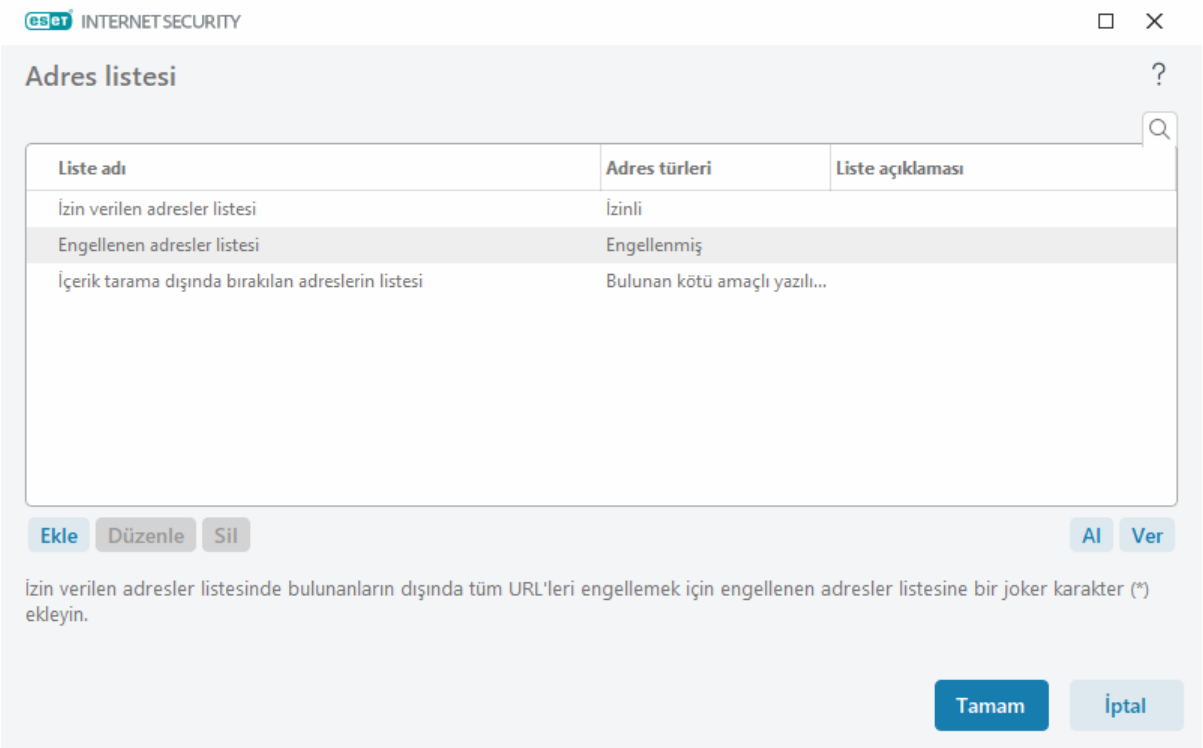
HTTP web sayfalarına ek olarak HTTPS adreslerini filtrelemek isterseniz SSL/TLS protokol filtrelemesini etkinleştir seçeneğini belirlemeniz gerekir. Aksi takdirde yalnızca ziyaret ettiğiniz HTTPS sitelerinin etki alanları eklenir, tam URL eklenmez.

Engellenen adresler listesindeki web siteleri **İzin verilen adresler listesine** dahil edilmedikçe bunlara erişilemez. **İçerik taraması dışında bırakılan adresler listesindeki** web sitelerine erişildiğinde bunlar üzerinde kötü amaçlı kod taraması yapılmaz.

Etkin **İzin verilen adresler listesi** içindeki adresler hariç tüm HTTP adreslerini engellemek isterseniz etkin **Engellenen adresler listesi**'ne * simgesini ekleyin.

* (yıldız işareti) ve ? (soru işareti) özel simgeleri listelerde kullanılabilir. Yıldız işareti herhangi bir karakter dizesinin, soru işaretiyse herhangi bir simgenin yerine geçer. Hariç bırakılan adresler listesinin yalnızca güvenilir ve güvenli adresleri içermesi gerektiğinden, hariç bırakılan adresleri belirlerken çok dikkatli olmak gerekir. Aynı şekilde * ve ? simgelerinin de bu listede doğru kullanıldığından emin olunmalıdır. Tüm alt etki alanlarını içeren bir etki alanının tamamının nasıl güvenli bir şekilde eşleştirilebileceğini öğrenmek için HTTP adresi / etki alanı maskesi ekle bölümüne bakın. Bir listeyi etkinleştirmek için **Liste etkin** öğesini seçin. Geçerli listedeki bir adrese girilirken bildirim almak istiyorsanız **Uygulanırken bildir** seçeneğini etkinleştirin.

> **Güvenilir etki alanları**
> **Web ve e-posta** > **SSL/TLS** > **Güvenilir etki alanlarıyla iletişimi tarama dışı bırak** ayarı etkinleştirilmişse ve etki alanı güvenilir olarak kabul ediliyorsa adresler filtrelenmez.



Denetim öğeleri

Ekle – Önceden tanımlı olanlara ek olarak yeni bir liste oluşturur. Adresleri mantıksal olarak farklı gruplara ayırmak isterseniz bu yararlıdır. Örneğin, engellenen adresler listelerinden biri harici bir genel kara listeden adresler içerirken diğeri kendi kara listenizden adresler içerebilir; böylece kendi kara listenizi bozulmadan korurken harici listeyi kolayca güncelleyebilirsiniz.

Düzenle – Mevcut listeleri düzenler. Adresleri eklemek veya kaldırmak için bunu kullanın.

Sil – Mevcut listeleri siler. Yalnızca **Ekle** ile oluşturulan listeler için mümkündür, varsayılanlar listeler için geçerli değildir.

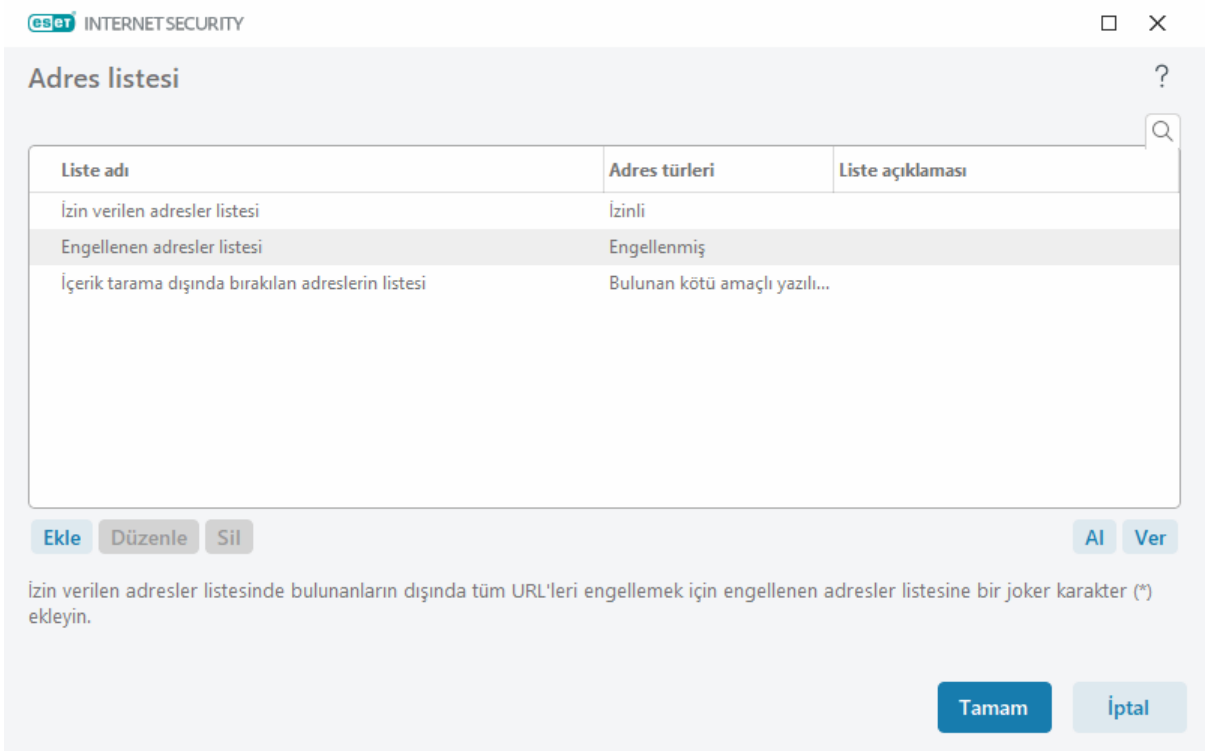
URL adresleri listesi

Bu bölümde; engellenecek, izin verilecek veya denetleme dışında bırakılacak HTTP adreslerinin listelerini belirleyebilirsiniz.

Varsayılan olarak aşağıdaki üç liste kullanılabilir:

- **İçerik taraması dışında bırakılan adreslerin listesi** – Bu listeye eklenen adresler için kötü amaçlı kod denetlemesi gerçekleştirilmez.
- **İzin verilen adresler listesi** – Yalnızca izin verilen adresler listesindeki HTTP adreslerine erişim izni ver seçeneği etkinleştirilirse ve engellenen adresler listesinde * simgesi (her şeyle eşleş) yer alıyorsa, kullanıcının yalnızca bu listede belirtilen adreslere erişmesine izin verilir. Engellenen adresler listesinde yer alsalar bile bu listedeki adreslere izin verilir.
- **Engellenen adresler listesi** - Ayrıca izin verilen adresler listesinde yer almadıkça kullanıcının bu listede belirtilen adreslere erişmesine izin verilmez.

Yeni bir liste oluşturmak için **Ekle**'yi tıklayın. Seçili listeleri silmek için **Sil**'i tıklayın.



> **Resimli talimatlar**
> Aşağıdaki ESET Bilgi Bankası makaleleri sadece İngilizce dilinde mevcuttur:
> - Güvenilir bir web sitesini Web Erişimi Koruması'nın engelleme işlevinin dışında bırakma
> - ESET Windows ev ürünlerini kullanarak bir web sitesini engelleyin

Daha fazla bilgi için URL adres yönetimine bakın.

Yeni URL adresleri listesi oluşturma

Bu iletişim penceresi engel olacak, kontrol kapsamında engellenecek, izin verilecek veya hariç bırakılacak yeni bir URL adresi/maske listesi yapılandırmanıza olanak sağlar.

Aşağıdaki seçenekleri yapılandırabilirsiniz:

Adres listesi türü – Üç liste türü mevcuttur:

- **Bulunan kötü amaçlı yazılım yoksayıldı** – Bu listeye eklenen adresler için kötü amaçlı kod denetlemesi gerçekleştirilmez.
- **Engellendi** - Bu listede belirtilen adreslere erişim engellenir.
- **İzin verildi** - Bu listede belirtilen adreslere erişime izin verilir. Engellenmiş adresler listesinde yer alsalar bile bu listedeki adreslere izin verilir.

Liste adı – Listenin adını belirtin. Bu alan, önceden tanımlı listelerden biri düzenlenirken kullanılamaz.

Liste açıklaması – Liste için kısa bir açıklama yazın (isteğe bağlı). Önceden tanımlı listelerden biri düzenlerken kullanılamaz.

Bir listeyi etkinleştirmek için bu listenin yanındaki **Liste etkin** öğesini seçin. Web sitelerine erişim esnasında belirli

bir liste kullanılırken bildirim almak istiyorsanız **Uygularken bildir**'i seçin. Örneğin, bir web sitesi engellenen veya izin verilen adresler listesine dahil edildiği için engellenir ya da izin verilirse bildirim alırsınız. Bildirim, listenin adını içerir.

Günlüğe kaydetme düzeyi - Web sitelerine erişilirken kullanılan belirli listeyle ilgili bilgiler Günlük dosyalarına yazılabilir.

Denetim öğeleri

Ekle – Listeye yeni bir URL adresi ekleyin (ayırıcı ile birden fazla değer girin).

Düzenle – Listede mevcut adresi değiştirir. Yalnızca **Ekle** ile oluşturulan adresler için kullanılabilir.

Kaldır – Listedeki mevcut adresleri siler. Yalnızca **Ekle** ile oluşturulan adresler için kullanılabilir.

Aktar - URL adresleri içeren bir dosyayı aktarın (değerleri satır sonuyla ayırın, örneğin UTF-8 kodlamasını kullanan *.txt).

Yeni URL maskesi nasıl eklenir?

İstenen adres/etki alanı maskesini girmeden önce lütfen bu iletişim kutusundaki talimatlara başvurun.

ESET Internet Security, kullanıcıların belirtilen web sitelerine erişimi engellemesini ve Internet tarayıcısının bu sitelerin içeriğini görüntülemesini önlemesini sağlar. Ek olarak, kullanıcının denetim dışında bırakılması gereken adresleri belirtmesine de olanak verir. Uzak sunucunun tam adı bilinmiyorsa veya kullanıcı tam bir uzak sunucular grubu belirtmek istiyorsa, böyle bir grubu tanımlamak için maskeler kullanılabilir. Maskelerde "?" ve "*" simgeleri bulunur:

- simgenin yerine ? kullanın
- metnin yerine * kullanın.

Örneğin, *.c?m son bölümü c harfi ile başlayan, sonu m harfi ile biten ve bunların arasında bilinmeyen bir simge bulunan bütün adreslere yöneliktir (.com, .cam ve bu gibi.)

Etki alanı adının başında kullanılırsa başa gelen "*." dizisi özel olarak ele alınır. Öncelikle, * joker karakteri bu durumda eğik çizgi karakteriyle ('/') eşleşmez. Bunun amacı maskeyi aşmaktan kaçınmaktır. Örneğin, **.domain.com* maskesi *http://anydomain.com/anypath#.domain.com* ile eşleşmez (bu tür bir sonek, indirme işlemini etkilemeden herhangi bir URL'ye eklenebilir). İkinci olarak "*." aynı zamanda bu özel durumda boş bir dize ile eşleşir. Bunun amacı, tüm alt etki alanlarını içeren etki alanının tümünü tek bir maske kullanarak eşleştirmektir. Örneğin **.domain.com* maskesi *http://domain.com* ile de eşleşir. Aynı zamanda *http://anotherdomain.com* ile de eşleşeceğinden, **domain.com*'u kullanmak yanlış olur.

Kimlik Avı koruması

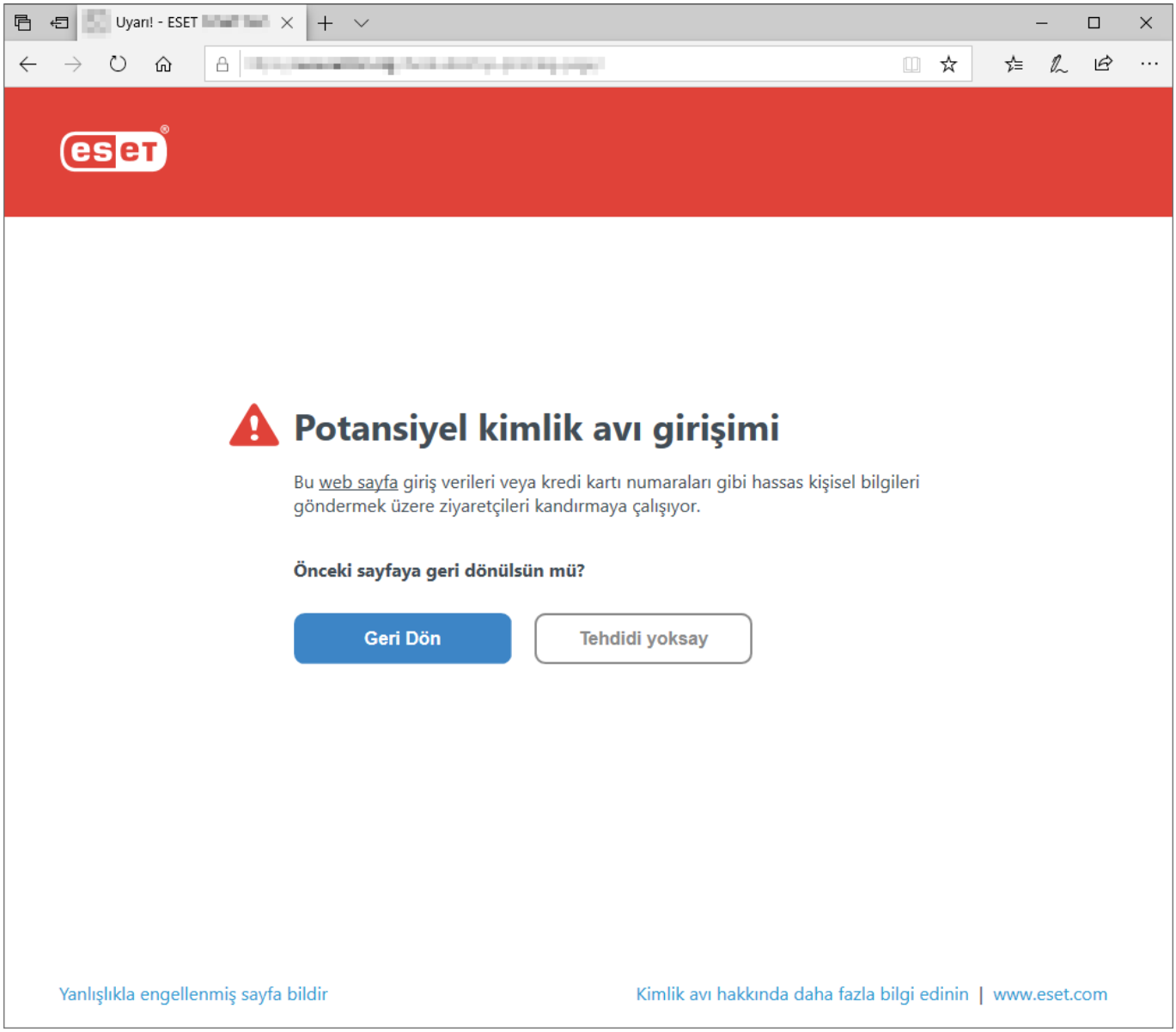
Kimlik avı, sosyal mühendisliği (kullanıcıları gizli bilgilerini elde etmek için manipüle etmek) kullanan bir suç faaliyetidir. Kimlik avı; banka hesap numaraları, PIN kodları gibi hassas verilere erişmek için kullanılır. Daha fazla bilgi için sözlüğe bakabilirsiniz. ESET Internet Security, bu tür içeriği dağıttığı bilinen web sayfalarını engelleyen kimlik avı koruması sağlar.

Kimlik Avı koruması varsayılan olarak etkindir. Bu ayara ana program penceresi > **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **Kimlik Avı koruması**'ndan erişilebilir.

ESET Internet Security ürününde Kimlik Avı koruması hakkında daha fazla bilgi edinmek için Bilgi bankası makalemize bakın.

Bir kimlik avı web sitesine erişme

Tespit edilen bir kimlik avı web sitesine eriştiğinizde web tarayıcınız aşağıdaki iletişim kutusunu görüntüler. Web sitesine yine de erişmek istiyorsanız **Tehdidi yoksay** (önerilmez) seçeneğine tıklatın.



Beyaz listeye eklenen potansiyel kimlik avı web sitelerinin süreleri varsayılan olarak birkaç saatten sonra dolar. Bir web sitesine kalıcı olarak izin vermek için URL adresi yönetimi aracını kullanabilirsiniz. **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **Web erişim koruması** > **URL adres yönetimi** > **Adres listesi** > **Düzenle** seçeneğini tıklatın ve düzenlemek istediğiniz web sitesini listeye ekleyin.

Kimlik avı sitesi bildir

Bildir bağlantısı bir kimlik avı/kötü amaçlı web sitesini analiz için ESET'e bildirmenizi sağlar.

> Bir web sitesini ESET'e göndermeden önce aşağıdaki ölçütlerden birine veya birden fazlasına uyduğundan emin olun:
> • Web sitesi algılanmamış.
> • Web sitesi tehdit olarak yanlış algılanmış. Böylece Yanlışlıkla engellenen bir sayfayı bildirebilirsiniz.

Alternatif olarak web sitesini e-posta ile de gönderebilirsiniz. E-postanızı samples@eset.com adresine gönderin. Açıklayıcı bir konu kullanmayı ve web sitesiyle ilgili mümkün olduğunca fazla bilgi (örneğin, hangi web sitesinden bu web sitesine geldiğiniz, web sitesini nasıl duyduğunuz vs.) eklemeyi unutmayın.

Ebeveyn kontrolü

Ebeveyn kontrolü modülü, ebeveynlerin çocuklarını korumalarına ve aygıtlar ile hizmetlerin kullanımına yönelik kısıtlamaları belirlemelerine yardımcı olmak üzere ebeveyn kontrolü ayarlarını yapılandırmanıza olanak tanır. Amaç, çocukların ve gençlerin uygunsuz veya zararlı içeriğe erişimini engellemektir.

Ebeveyn kontrolü, olası saldırgan materyaller içerebilecek web sayfalarını engellemenize izin verir. Ayrıca ebeveynler 40'tan fazla önceden tanımlanmış web sitesi kategorisine ve 140'ın üstünde alt kategoriye erişimi yasaklayabilir.

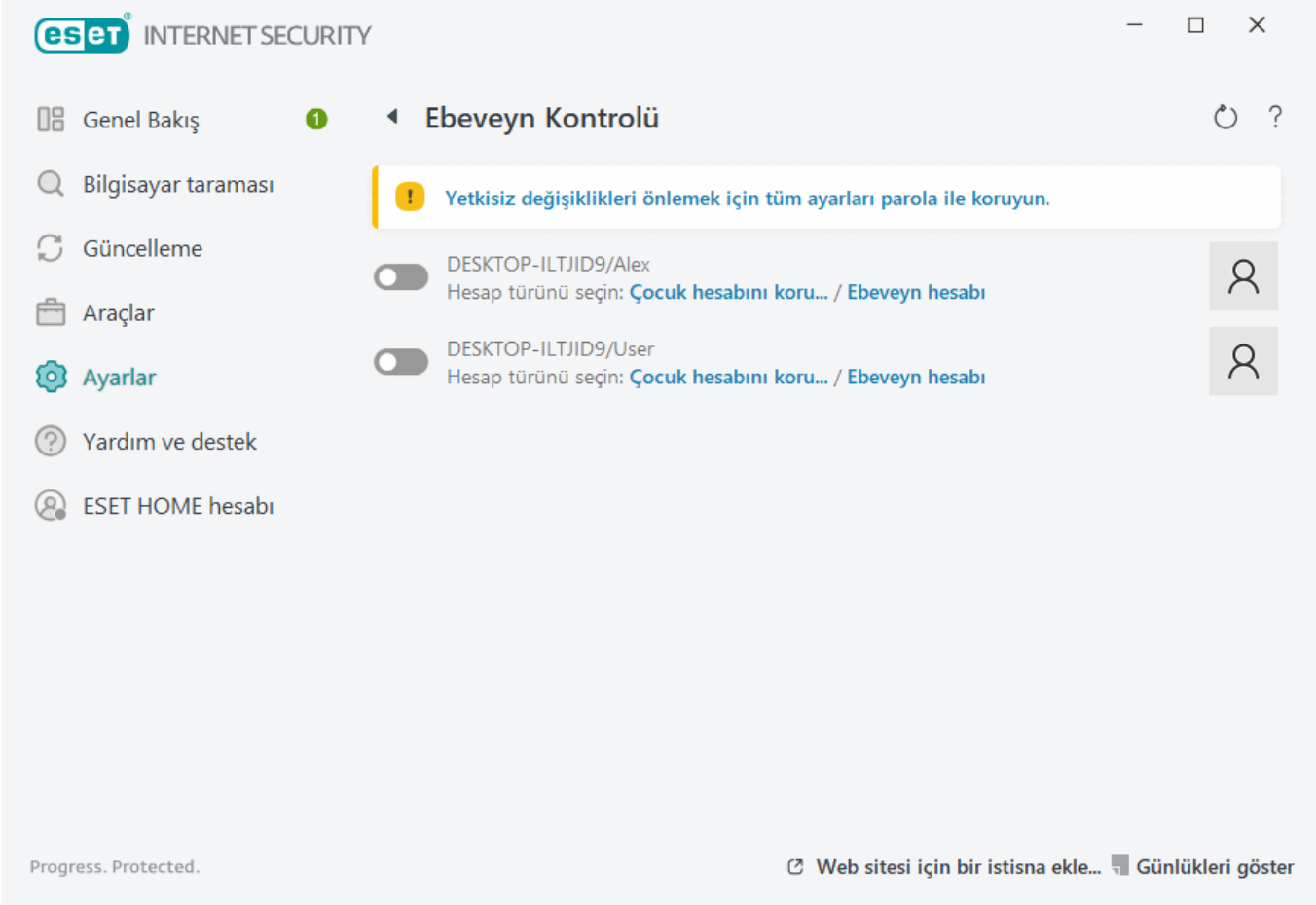
Belirli bir kullanıcı hesabı için Ebeveyn kontrolünü etkinleştirmek üzere aşağıdaki adımları uygulayın:

1. Varsayılan olarak, Ebeveyn kontrolleri ESET Internet Security içinde devre dışıdır. Ebeveyn kontrolünün etkinleştirilmesine yönelik iki yöntem bulunur:

   • Ana program penceresinde **Ayarlar** > **İnternet koruması** > **Ebeveyn Kontrolü** bölümünde simgesine tıklatın ve Ebeveyn kontrolü durumunu etkin olarak değiştirin.

   • F5 tuşuna basarak **Gelişmiş Ayarlar** ağacına erişin, **Web ve e-posta** > **Ebeveyn Kontrolü**'ne gidin ve **Ebeveyn Kontrolü'nü etkinleştir** seçeneğinin yanındaki kaydırma çubuğunu etkinleştirin.

2. Ana program penceresinden **Ayarlar** > **İnternet koruması** > **Ebeveyn kontrolü**'nü tıklayın. **Ebeveyn kontrolü** öğesinin yanında **Etkin** durumu görünse bile, ok simgesini tıklayarak istenen hesap için Ebeveyn Kontrolünü yapılandırmanız gerekir. Bunun ardından bir sonraki pencerede **Alt hesabı koru** veya **Üst hesap** seçeneğini tıklayın. Sonraki penceredeyse, erişim düzeyini ve yaşa uygun önerilen web sayfalarını belirlemek için bir doğum tarihi girin. Ebeveyn kontrolü artık belirtilen kullanıcı hesabı için etkinleşmiştir. Kategoriler sekmesinde izin vermek veya engellemek istediğiniz kategorileri özelleştirmek için hesap adının altındaki **Engellenen içerik ve ayarlar** öğesini tıklayın. Bir kategoriyle eşleşmeyen özel web sayfalarına izin vermek veya bunları engellemek için Özel Durumlar sekmesini tıklayın.



ESET Internet Security Ana ürün penceresinde **Ayarlar** > **İnternet koruması** > **Ebeveyn denetimi** öğesini tıklatırsanız ana pencerede şunların yer aldığını görürsünüz:

Windows kullanıcı hesapları

Mevcut bir hesap için rol oluşturduysanız burada gösterilir. Kaydırıcıyı tıklatırsanız hesap için Ebeveyn kontrolünün yanında yeşil bir onay işareti görüntülenir. Etkin hesap altında Engellenen içerik ve ayarlar seçeneğini tıklatarak söz konusu hesaba yönelik izin verilen web sayfası kategorilerinin listesini ve engellenen ve izin verilen web sayfalarını görüntüleyin.

Yeni bir hesap oluşturmak için (örneğin, bir çocuk için) Windows 7 veya Windows Vista için şu adım adım talimatları uygulayın:
1.**Başlat** düğmesini (masaüstünüzün sol alt tarafında bulunur) tıklatıp **Denetim Masası** öğesini tıklattıktan sonra **Kullanıcı Hesapları** öğesini tıklatarak **Kullanıcı Hesapları** bölümünü açın.
2.**Kullanıcı Hesabını Yönet** öğesini tıklatın. Sizden yönetici parolası veya onayı istenirse parolayı girin veya onayı sağlayın.
3.**Yeni Hesap Oluştur** öğesini tıklatın.
4.Kullanıcı hesabına vermek istediğiniz adı girin, hesap türünü tıklatın ve ardından **Hesap Oluştur** öğesini tıklatın.
5.ESET Internet Security Ana program penceresinden **Ayarlar** > **İnternet koruması** > **Ebeveyn kontrolü**'nü tekrar tıklayarak Ebeveyn kontrolü bölmesini yeniden açın ve ok simgesini tıklayın.

Pencerenin alt bölümünde şunlar yer alır:

Web sitesi için özel durum ekle – Belirli bir web sitesi, tercihlerinize bağlı olarak her bir ebeveyn hesabı için ayrı ayrı izinli veya engelli olarak ayarlanabilir.

Günlükleri göster – Bu, Ebeveyn kontrolü etkinliğinin ayrıntılı günlüğünü (engellenen sayfalar, sayfanın engellendiği hesap, kategori vb.) gösterir. Ayrıca bu günlüğü **Filtreleme** öğesini tıklatarak seçtiğiniz ölçütlere göre de filtreleyebilirsiniz.

Ebeveyn kontrolü

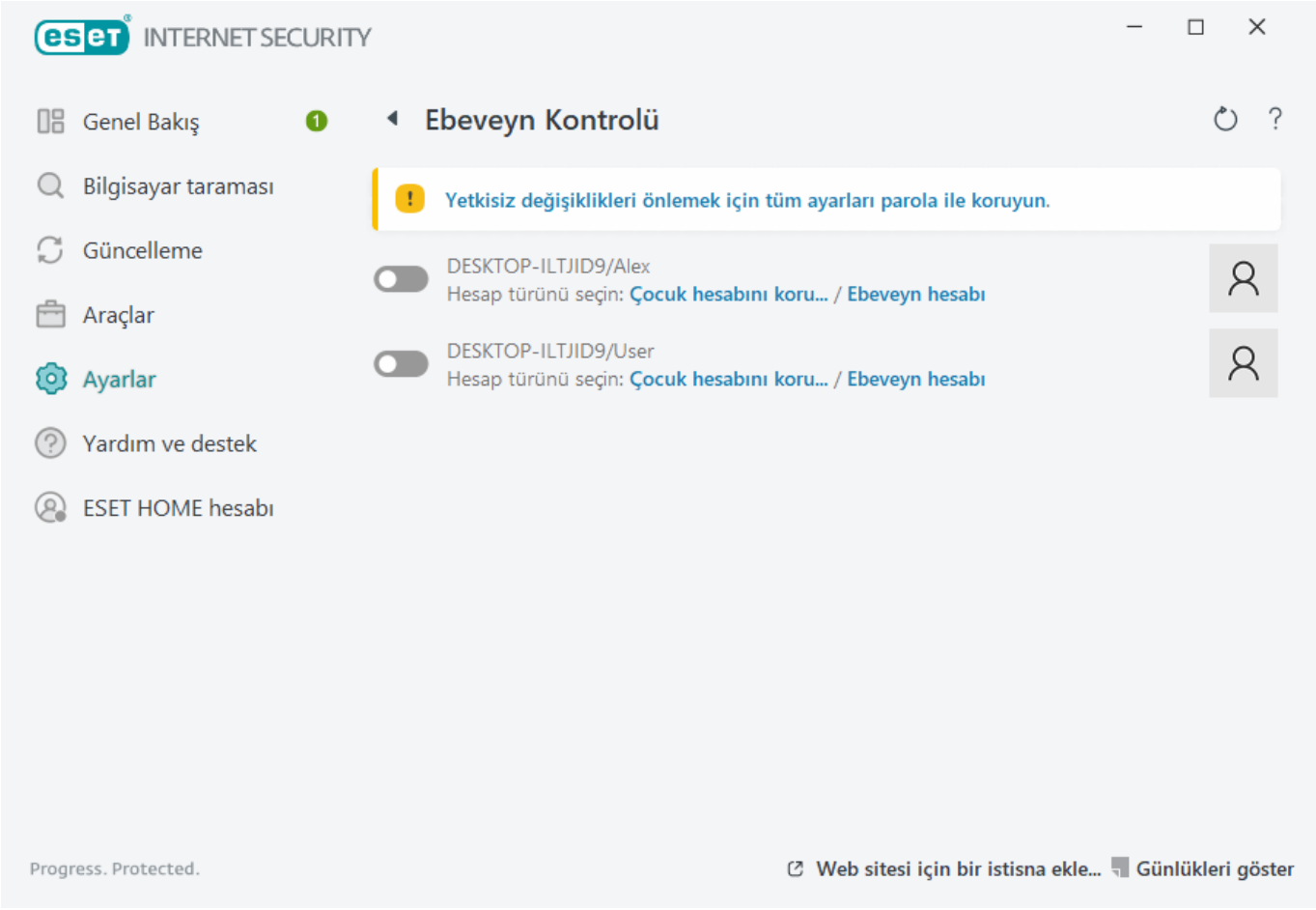
Ebeveyn kontrolünü devre dışı bıraktıktan sonra **Ebeveyn kontrolünü devre dışı bırak** penceresi görüntülenir. Burada korumanın devre dışı bırakılacağı zaman aralığını ayarlayabilirsiniz. Bu seçenek, **Duraklatıldı** veya **Kalıcı olarak devre dışı bırakıldı** şeklinde ayarlanabilir.

ESET Internet Security içindeki ayarları parolayla korumak önemlidir. Parola, Erişim ayarları bölümünde ayarlanabilir. Parola ayarlanmazsa şu uyarı görüntülenir - Yetkisiz değişiklikleri engellemek için **Tüm ayarları parolayla koruyun**. Ebeveyn kontrolü içinde ayarlanan kısıtlamalar yalnızca standart kullanıcı hesaplarını etkiler. Yönetici herhangi bir kısıtlamayı geçersiz kılabildiğinden kısıtlamaların etkisi olmaz.

Ebeveyn kontrolünün düzgün bir şekilde çalışması için Uygulama protokolü içerik filtreleme, HTTP protokolü denetimi ve Güvenlik duvarı işlevleri etkin olmalıdır. Bu işlevlerin hepsi varsayılan olarak etkindir.

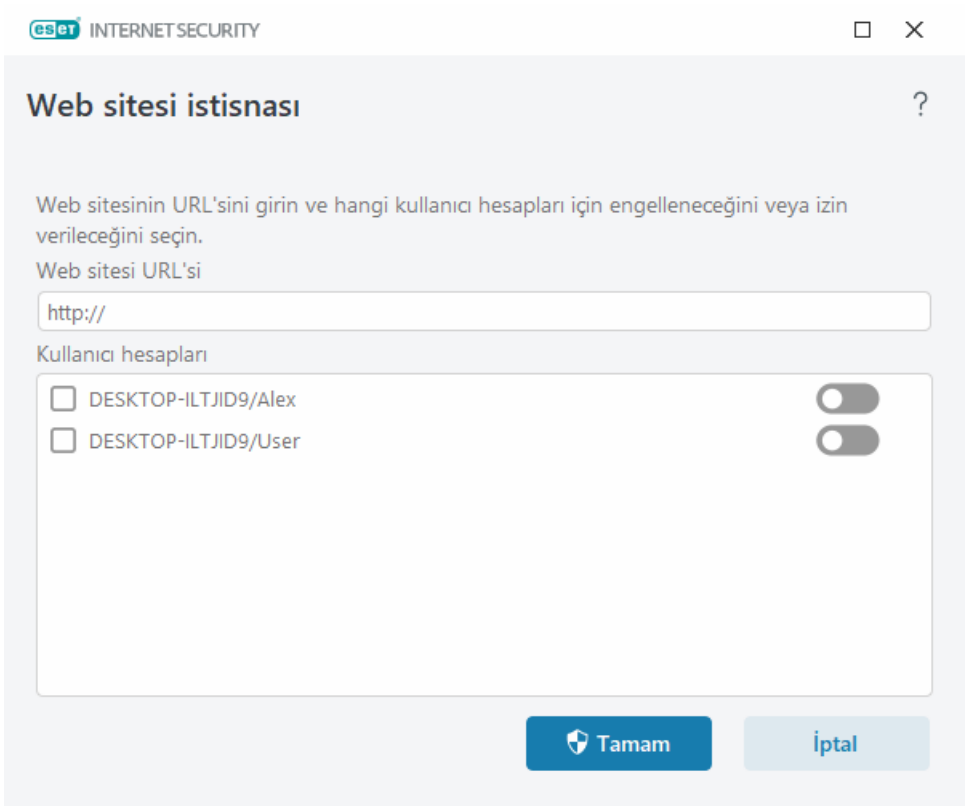
Web sitesi özel durumları

Bir web sitesi için özel durum eklemek üzere **Ayarlar** > **İnternet koruması** > **Ebeveyn kontrolü**ve ardından **Bir web sitesi için özel durum ekle**'yi seçin.

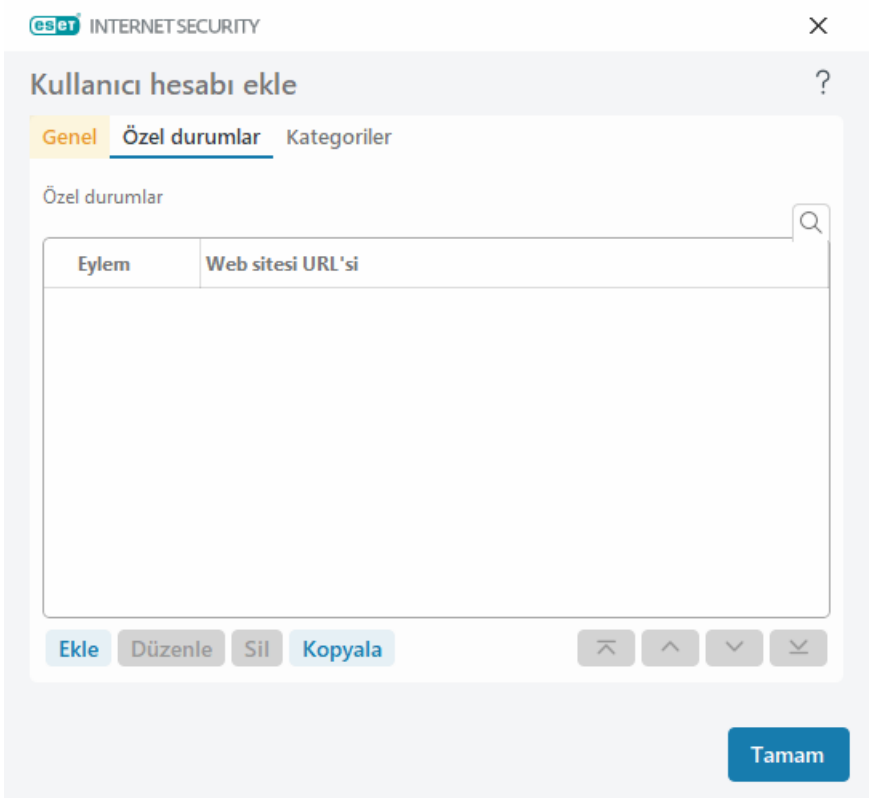


Web sitesi URL'si alanına URL'yi girdikten sonra her spesifik kullanıcı hesabı için ✔ (izin verildi) veya ⊘

(engellendi) simgelerinden birini seçip özel durumu listeye eklemek için **Tamam**'ı tıklayın.



Bir URL adresini listeden silmek için istenen kullanıcı hesabı altındaki **Ayarlar** > **İnternet koruması** > **Ebeveyn kontrolü** > **Engellenen içerikler ve ayarlar**'ı tıklatın. **Özel durumlar** sekmesini tıklattıktan sonra özel durumu seçip **Kaldır**'ı tıklatın.



URL adres listesinde, * (yıldız işareti) ve ? (soru işareti) özel sembolleri kullanılamaz. Örneğin, birden çok TLD'ye (Üst Düzey Etki Alanı) sahip web sayfası adresleri el ile girilmelidir (*examplepage.com*, *examplepage.sk*, vb.).

Listeye etki alanı eklediğinizde, bu etki alanında ve tüm alt etki alanlarında (örneğin *sub.examplepage.com*) bulunan tüm içerikler URL tabanlı eylem seçiminize bağlı olarak engellenir veya bunlara izin verilir.

> Belirli bir web sayfasının engellenmesi veya sayfaya izin verilmesi, bir web sayfası kategorisinin engellenmesi veya kategoriye izin verilmesinden daha doğru sonuç verebilir. Bu ayarları değiştirirken ve listeye bir kategori/web sayfası eklerken dikkatli olun.

Kullanıcı hesapları

Bu ayar **Gelişmiş kurulum** (F5) > **Web ve e-posta** > **Ebeveyn kontrolü** > **Kullanıcı hesapları** > **Düzenle** bölümünde bulunmaktadır.

Bu bölümde, belirli kullanıcıların İnternet'te bulunan uygunsuz veya zararlı içeriğe erişimini kısıtlamak amacıyla söz konusu kullanıcılarla Ebeveyn kontrolü tarafından kullanılan Windows kullanıcı hesaplarını ilişkilendirebilirsiniz.

Sütunlar

Windows hesabı – Kullanıcının adı.

Etkin – Etkinleştirildiğinde belirli bir kullanıcı için Ebeveyn kontrolleri etkinleştirilir.

Etki alanı – Bir kullanıcının ait olduğu etki alanı adı.

Doğum günü – Bu hesabın ait olduğu kişinin yaşı.

Denetim öğeleri

Ekle – Kullanıcı hesaplarıyla çalışma iletişim kutusu görüntülenir.

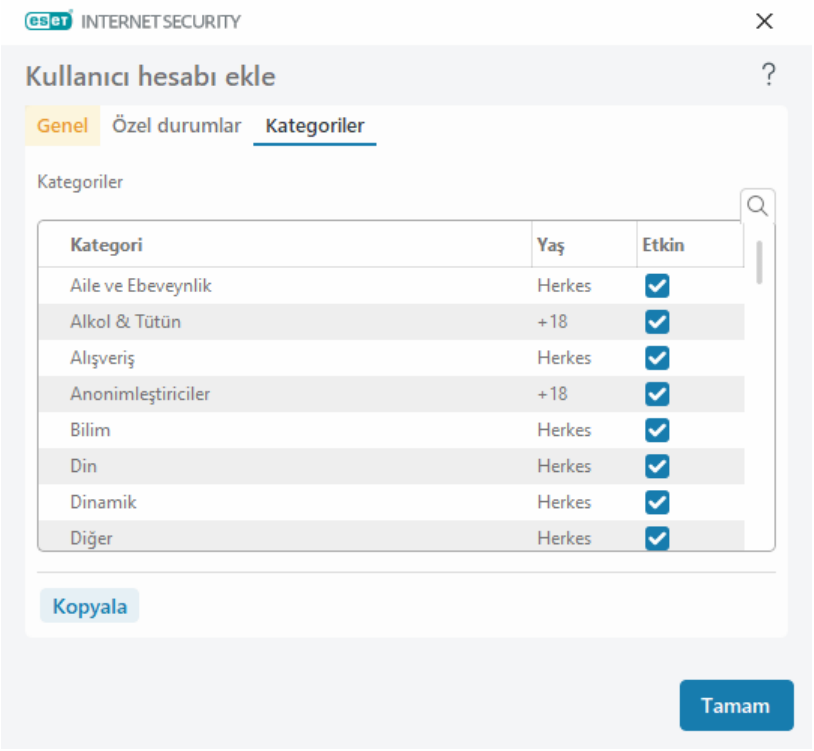
Düzenle – Bu seçenek seçili hesapları düzenlemenize izin verir.

Sil – Seçili hesabı siler.

Yenile - Bir kullanıcı hesabı eklediyseniz ESET Internet Security, bu pencereyi tekrar açmaya gerek kalmadan kullanıcı hesapları listesini yenileyebilir.

Kategoriler

İzin vermek için bir kategorinin yanındaki **Etkin** sütunundaki onay kutusunu işaretleyin. Onay kutusunu boş bırakırsanız bu hesap için kategoriye izin verilmez.



Aşağıda kullanıcılara bilindik gelmeyebilecek kategorilere (gruplara) bazı örnekler verilmiştir:

- **Çeşitli** – Genellikle intranet, 127.0.0.0/8, 192.168.0.0/16 vb. gibi özel (yerel) IP adresleri. Bir 403 veya 404 hata kodu aldığınızda bu web sitesi de bu kategoriyle eşleşir.
- **Çözümlenmeyenler** – Bu kategori Ebeveyn kontrolü veri tabanı altyapısına bağlanırken oluşan bir hata nedeniyle çözülemeyen web sayfalarını içerir.
- **Kategorize edilemeyenler** – Henüz Ebeveyn kontrolü veri tabanında bulunmayan bilinmeyen web sayfaları.
- **Dinamik** – Diğer web sitelerindeki sayfalara yönlendiren web sayfaları.

Kullanıcı hesaplarıyla çalışma

Pencerede üç sekme yer alır:

Genel

Aşağıda seçilen Windows hesabı için Ebeveyn Kontrolünü açmak üzere **Etkin** seçeneğinin yanındaki kaydırma çubuğunu tıklayın.

İlk olarak bilgisayarınızdan bir Windows hesabı **seçin**. Ebeveyn kontrolü içinde ayarlanan kısıtlamalar yalnızca standart Windows hesaplarını etkiler. Yönetici hesapları, kısıtlamaları geçersiz kılabilir.

Hesap ebeveyn tarafından kullanılıyorsa **Ebeveyn hesabını** seçin.

Hesap için **Çocuğun doğum günü** bilgisini girerek erişim düzeyini belirleyin ve yaşa uygun web sayfaları için erişim kuralları oluşturun.

Günlüğe kaydetme şiddeti

ESET Internet Security tüm önemli olayları ana menüden doğrudan görüntülenebilen bir günlük dosyasına kaydeder. **Araçlar** > **Diğer araçlar** > **Günlük dosyaları**'nı tıklayıp **Günlük** açılır menüsünden **Ebeveyn kontrolü**'ni seçin.

- **Tanılama** – Programda hassas ayarlama yapmak için gereken bilgileri günlüğe kaydeder.
- **Bilgi** – İzin verilen ve engellenen özel durumlar da dahil olmak üzere bilgilendirici iletileri ve yukarıdaki tüm kayıtları kaydeder.
- **Uyarı** – Kritik hataları ve uyarı iletilerini kaydeder.
- **Yok** – Günlüğe herhangi bir şey kaydedilmez.

Özel Durumlar

Özel durum oluşturularak bir kullanıcının özel durumlar listesinde yer almayan web sitelerine erişimine izin verilebilir veya erişimi engellenebilir. Kategorileri kullanmadan belirli web sitelerine erişimi denetlemek istediğinizde bu özellik kullanılabilir. Bir hesap için oluşturulan özel durumlar, başka hesap için kopyalanıp kullanılabilir. Birbirine yakın yaşlardaki çocuklar için aynı kuralları oluşturmak istediğinizde bu özellik kullanılabilir.

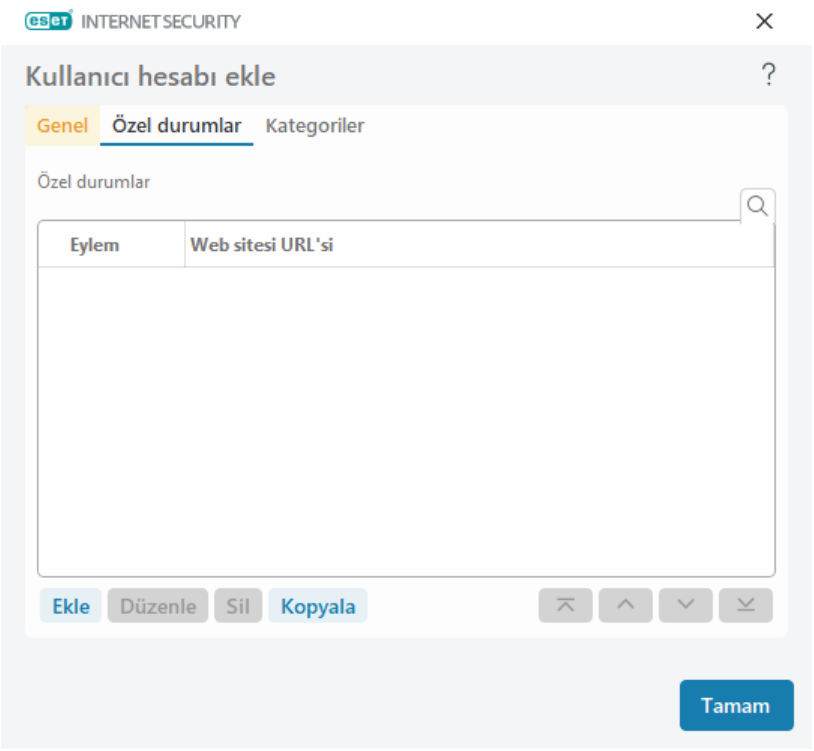
Yeni bir özel olay oluşturmak için **Ekle**'ye tıklatın. **Eylem** belirleyin (örneğin, **Engelle**); bunun için açılır menüyü kullanın, söz konusu özel durumun uygulanacağı **Web sitesi URL'si**'ni yazıp **Tamam**'a tıklatın. Özel durum gösterilen durumuyla birlikte, mevcut özel durumların yer aldığı listeye eklenir.

Ekle – Yeni bir özel durum oluşturur.

Düzenle – Seçilen özel durumun **Web Sitesi URL'sini** veya **Eylemini** düzenleyebilirsiniz.

Sil – Seçilen özel durumu kaldırır.

Kopyala - Oluşturulan özel durumu kopyalamak istediğiniz açılır menüden bir kullanıcı seçin.

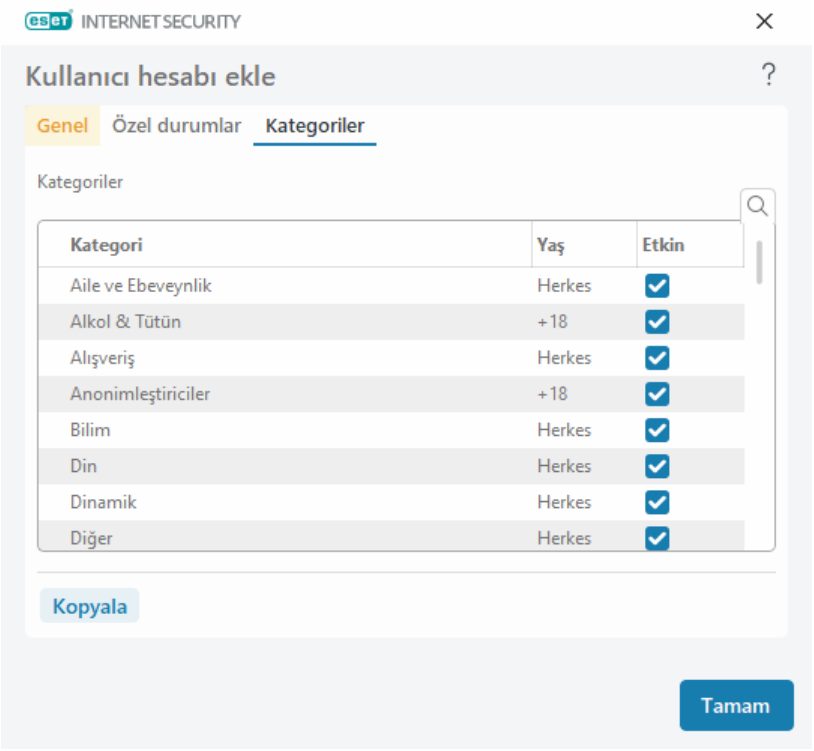


Tanımlanan özel durumlar, seçilen hesap(lar) için tanımlanan kategorileri geçersiz kılar. Örneğin hesapta **Haberler** kategorisi engellenmişse, ancak özel durum olarak izin verilecek bir haber web sayfası tanımladıysanız hesap izin verilen web sayfasına erişebilir. Burada yapılan tüm değişiklikleri Özel durumlar bölümünde görebilirsiniz.

Kategoriler

Kategoriler sekmesinde, her hesap için engellemek veya izin vermek istediğiniz web sayfalarının genel kategorilerini tanımlayabilirsiniz. Bir kategorinin yanındaki onay kutusunu işaretleyerek izin verebilirsiniz. Onay kutusunu boş bırakırsanız söz konusu hesap için kategoriye izin verilmez.

Kopyala - Değiştirilen mevcut bir hesaptaki engellenen veya izin verilen kategorilerin listesini kopyalamanıza olanak tanır.



Özel durumu kullanıcıdan kopyala

Oluşturulan özel durumu kopyalamak istediğiniz açılır menüden bir kullanıcı seçin.

Kategorileri hesaptan kopyala

Değiştirilen mevcut bir hesaptaki engellenen veya izin verilen kategorilerin listesini kopyalamanıza olanak tanır.

Ebeveyn Kontrolünü etkinleştir

Ebeveyn kontrolünü etkinleştir seçeneği, Ebeveyn kontrolünü ESET Internet Security aracına entegre eder.

Ağ koruması

Ağ koruması yapılandırması **Ağ koruması** altındaki **Ayarlar** bölmesinde bulunabilir.

Koruma modüllerini tek tek duraklatmak veya devre dışı bırakmak için kaydırma çubuğunu tıklayın.

⚠ Koruma modüllerini kapatmak, bilgisayarınızın koruma düzeyini düşürebilir.

Güvenlik duvarı – Buradan ESET Güvenlik duvarı için filtreleme modunu ayarlayabilirsiniz. Daha ayrıntılı ayarlara erişmek için **Güvenlik duvarı**'nın yanındaki dişli simgesini ⚙ > Yapılandır'ı tıklayın veya Gelişmiş ayarlar'a erişmek için **F5'e** basın.

Yapılandır – Güvenlik duvarının ağ iletişimlerini nasıl işleyeceğini belirtebileceğiniz, Gelişmiş ayarlar içinde yer alan Güvenlik duvarı penceresini açar.

Güvenlik duvarını duraklat (tüm trafiğe izin ver) – Tüm ağ trafiğinin engellenmesinin tam tersi. Seçilirse, tüm Güvenlik duvarı filtre seçenekleri kapatılıp gelen ve giden bağlantıların tümüne izin verilir. Ağ trafiği filtrelemesi bu moddayken güvenlik duvarını yeniden etkinleştirmek için **Güvenlik duvarını etkinleştir** öğesine tıklatın.

Tüm trafiği engelle – Tüm gelen ve giden iletişimler Güvenlik duvarı tarafından engellenir. Bu seçeneği yalnızca sistemin ağ ile bağlantısının kesilmesini gerektiren kritik bir güvenlik riskinden şüphelenirseniz kullanın. Ağ trafiği filtresi **Tüm trafiği engelle** modundayken güvenlik duvarını normal çalışmasına döndürmek için **Tüm trafiği engellemeyi durdur** seçeneğini tıklatın.

Otomatik mod – (başka bir filtreleme modu etkinleştirildiğinde) Filtreleme modunu otomatik filtreleme moduna (kullanıcı tanımlı kurallarla) değiştirmek için tıklatın.

Etkileşimli mod - (başka bir filtreleme modu etkinleştirildiğinde) - Filtreleme modunu etkileşimli filtreleme moduna değiştirmek için tıklatın.

Ağ Saldırısı Koruması (IDS) – Ağ trafiğinin içeriğini analiz eder ve ağ saldırılarına karşı korur. Zararlı olduğu düşünülen trafiğin tümü engellenir. ESET Internet Security korunmayan bir kablosuz ağa veya zayıf koruması olan bir ağa bağlandığınızda sizi bilgilendirir.

Botnet koruması – Sistemdeki kötü amaçlı yazılımları hızlı ve doğru bir şekilde bulur.

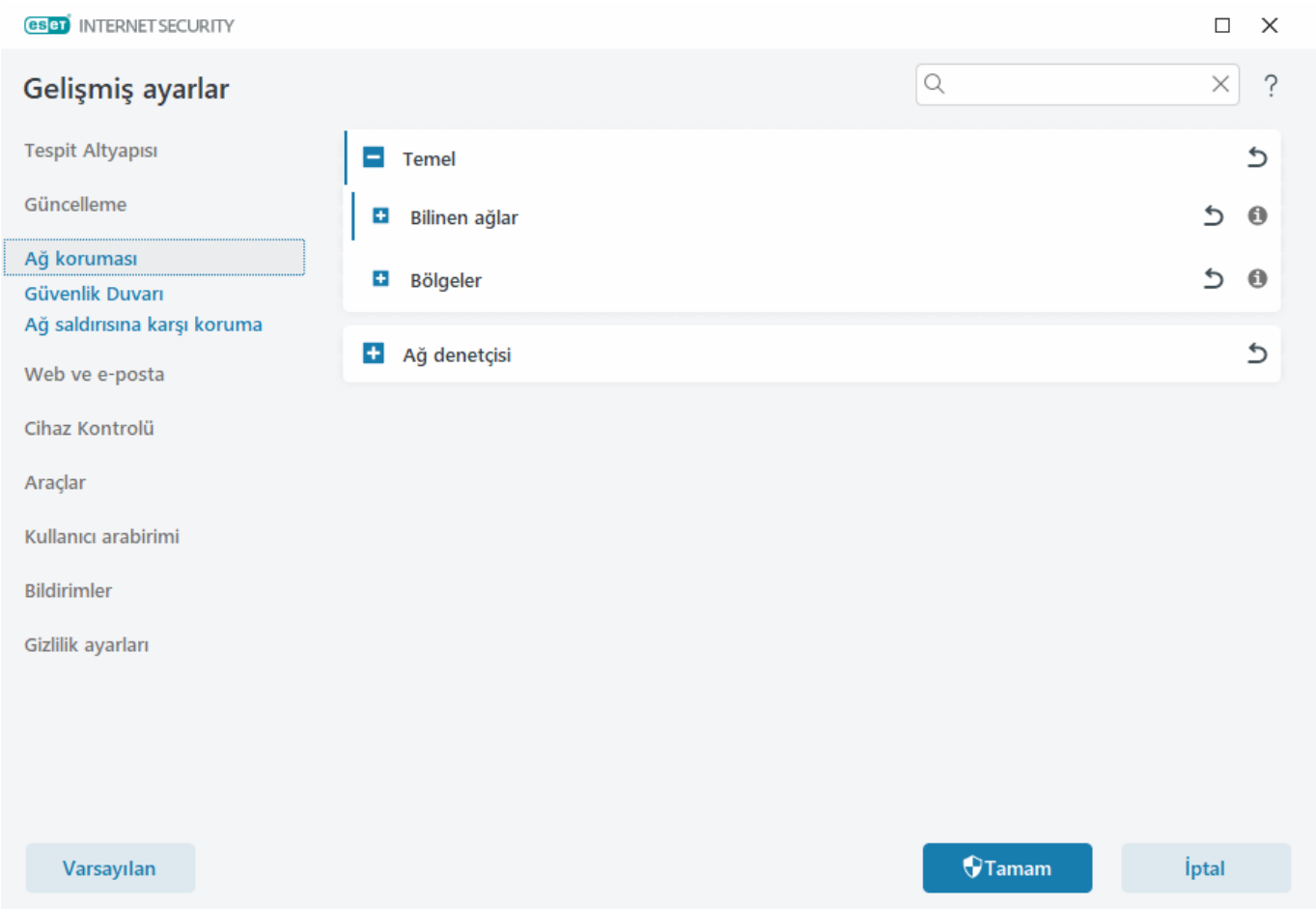
Bağlı ağlar – Ağ bağdaştırıcılarının bağlı olduğu ağları gösterir. Ağ adının altındaki bağlantıyı tıklamanızın ardından açılır pencere ağı güvenli olarak yapılandırmanıza olanak sağlar.

Geçici IP adresi kara listesi – Saldırıların kaynağı olarak algılanan, belirli bir süre boyunca bağlantıyı engellemek üzere kara listeye eklenen IP adreslerinin bir listesini görüntüleyebilirsiniz. Daha fazla bilgi için bu seçeneği tıklatın ve ardından F1 tuşuna basın.

Sorun giderme sihirbazı – ESET Güvenlik duvarından kaynaklanan bağlantı sorunlarını çözmenize yardımcı olur. Daha ayrıntılı bilgi için bkz. Sorun giderme sihirbazı.

Ağ koruması gelişmiş ayarlar

Ana program penceresinde **Ayarlar** > **Gelişmiş ayarlar** (F5) > **Ağ koruması** seçeneğini tıklayın.



Temel

Bilinen ağlar

Daha fazla bilgi için Bilinen ağlar'a bakın.

Bölgeler

Bölge, bir mantıksal grup oluşturan ağ adreslerinin toplamını temsil eder. Daha fazla bilgi için Bölgeleri yapılandırma bölümüne bakın.

Ağ Denetçisi

Ağ Denetçisi'ni etkinleştir

Ağ Denetçisi, ev ağında bulunan açık bağlantı noktaları veya zayıf yönlendirici parolası gibi güvenlik açıklarını belirlemeye yardımcı olur. Ayrıca, cihaz türüne göre sınıflandırılan bağlı cihazların listesini de sağlar.

Yeni keşfedilen ağ aygıtları hakkında bilgilendir

Ağınızda yeni bir aygıt algılandığında sizi bilgilendirir.

Bilinen ağlar

Güvenilir olmayan ağlara veya güvenilir (ev ya da iş yeri) ağınızın dışındaki ağlara sık sık bağlanan bir bilgisayar kullanırken bağlandığınız yeni ağların ağ güvenilirliğini doğrulamanızı öneririz. Ağlar tanımlandıktan sonra ESET Internet Security, **Ağ Kimliği**'nde yapılandırılan ağ parametrelerini kullanarak güvenilir (Ev veya iş yeri) ağlarını tanıyabilir. Bilgisayarlar genellikle güvenilir ağlara benzeyen IP adreslerine sahip ağlara girer. Böyle durumlarda ESET Internet Security, bilinmeyen bir ağı güvenilir (Ev veya iş yeri ağı) olarak kabul edebilir. Bu tür bir durumu önlemek için **Ağ kimlik doğrulaması** kullanmanızı öneririz. Bilinen ağ ayarlarına erişmek için **Gelişmiş ayarlar** (F5) > **Ağ Koruması** > **Temel** > **Bilinen ağlar**'a gidin.

Ağ bağdaştırıcı bir ağa bağlandığında veya bağdaştırıcının ağ ayarları yeniden yapılandırıldığında ESET Internet Security, bilinen ağ listesinde yeni ağ ile eşleşen bir kayıt arar. **Ağ kimliği** ve **Ağ kimlik doğrulaması** (isteğe bağlı) eşleşirse ağ, bu arabirimde bağlı olarak işaretlenir. Bilinen bir ağ bulunamadığında ağ kimliği yapılandırması bir sonraki bağlanışınızda ağı tanımak için yeni bir ağ bağlantısı oluşturur. Varsayılan olarak, yeni ağ bağlantısı Windows ayarlarında tanımlanan koruma türünü kullanır. **Yeni Ağ Bağlantısı Algılandı** iletişim kutusu, **güvenilir ağ**, **güvenilir olmayan ağ** ya da **Windows ayarını kullan** koruma türü arasında seçim yapmanızı ister. Ağ bağdaştırıcısı bilinen bir ağa bağlanırsa ve bu ağ **Güvenilir ağ** olarak işaretlenmişse bağdaştırıcının yerel alt ağları Güvenilir bölgeye eklenir.

Yeni ağların koruma türü - Aşağıdaki seçeneklerden birini belirleyin: **Windows ayarını kullan**, **Kullanıcıya sor** veya **Güvenilir değil olarak işaretle** seçenekleri, yeni ağlar için varsayılan olarak kullanılır.

Bilinen ağlar ağ adı, ağ kimliği, koruma türü gibi ayarları yapılandırmanıza olanak tanır. Bilinen ağ düzenleyicisine erişmek için **Düzenle**'yi tıklayın.

> **Windows ayarını kullan** seçeneğini belirlerseniz, bir iletişim kutusu görüntülenmez ve bağlandığınız ağ Windows ayarlarınıza göre otomatik olarak işaretlenir. Bu, belirli özelliklerin (dosya paylaşımı ve uzak masaüstü gibi) yeni ağlardan erişilebilir olmasına neden olur.

Bilinen ağ düzenleyicisi

Bilinen ağlar, **Gelişmiş ayarlar** > **Ağ koruması** > **Temel** > **Bilinen Ağlar**'da **Düzenle**'yi tıklayarak manuel olarak yapılandırılabilir.

Sütunlar

Ad - Bilinen bir ağın adı.

Koruma türü - Ağın **güvenilir**, **güvenilir olmayan** veya **Windows ayarını kullan** seçeneklerinden birine ayarlanıp ayarlanmadığını gösterir.

Güvenlik duvarı profili - Profil kuralları filtresini görüntülemek üzere **Profilde kullanılan kuralları görüntüle** aşağı açılır menüsünden bir profil seçin.

Güncelleme profili – Bu ağa bağlanıldığında oluşturulan güncelleme profilini uygulamanıza olanak sağlar.

Denetim öğeleri

Ekle – Yeni bir bilinen ağ oluşturur.

Düzenle – Mevcut bilinen ağı düzenlemek için tıklatın.

Kaldır – Bir ağ seçin ve bilinen ağlar listesinden bu ağı kaldırmak için **Kaldır** öğesini tıklatın.

Üst/Yukarı/Aşağı/Alt - Bilinen ağların öncelik düzeyini ayarlamanıza olanak tanır (ağlar baştan aşağı değerlendirilir).

Ağ yapılandırma ayarları aşağıdaki sekmelerde yapılır:

Ağ

Burada **Ağ adını** belirleyebilir ve ağ için **Koruma türünü** (güvenilir, güvenilir olmayan ya da Windows ayarını kullan) seçebilirsiniz. Bu ağ için profil seçmek üzere **Güvenlik duvarı profili** aşağı açılır menüsünü kullanın. Ağ, **güvenilir** koruma türünü kullanıyorsa doğrudan bağlı olan tüm alt ağlar güvenilir olarak kabul edilir. Örneğin, ağ bağdaştırıcısı bu ağa 192.168.1.5 IP adresi ve 255.255.255.0 alt ağ maskesi ile bağlıysa 192.168.1.0/24 alt ağı, bağdaştırıcının güvenilen bölgesine eklenir. Bağdaştırıcı daha fazla adrese/alt ağa sahipse bilinen ağın **Ağ tanımı** yapılandırması fark etmeksizin tümü güvenilir olur.

Ayrıca **Ek güvenilir adresler** altında eklenen adresler (ağın koruma türü fark etmeksizin) her zaman bu ağa bağlı bağdaştırıcıların güvenilen bölgesine eklenir.

Zayıf WiFi şifrelemesi hakkında uyar – ESET Internet Security, korunmayan bir kablosuz ağa veya zayıf korumalı bir ağa bağlandığınızda sizi bilgilendirir.

Güvenlik duvarı profili - Bu ağa bağlanırken kullanılan güvenlik duvarı profilini seçin.

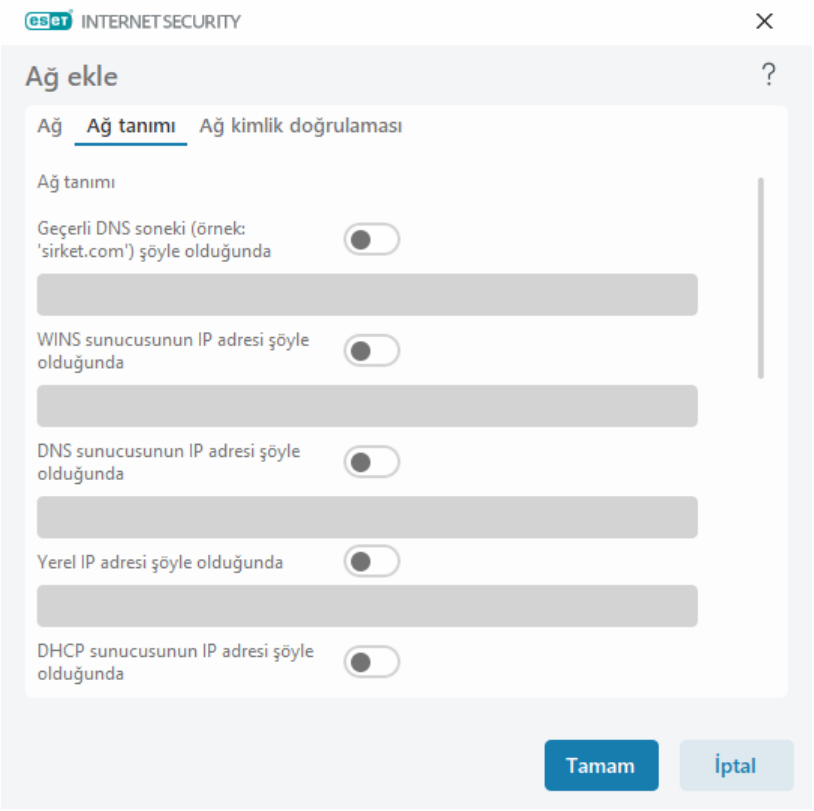
Güncelleme profili - Bu ağa bağlanırken kullanılan güncelleme profilini seçin.

Bir ağın bağlı ağlar listesinde bağlandı olarak işaretlenmesi için aşağıdaki koşulları yerine getirmesi gerekir:

- **Ağ tanımı** – Tüm doldurulan parametrelerin etkin bağlantı parametreleriyle eşleşmesi gerekir.
- **Ağ kimlik doğrulaması** – Kimlik doğrulama sunucusu seçilirse, ESET Kimlik Doğrulama Sunucusu ile başarılı bir şekilde kimlik doğrulaması yapılmalıdır.

Ağ tanımı

Ağ tanımı, yerel ağ bağdaştırıcısı parametreleri temelinde gerçekleştirilir. Tüm seçilen parametreler, etkin ağ bağlantılarının gerçek parametreleriyle karşılaştırılır. IPv4 ve IPv6 adreslerine izin verilir.



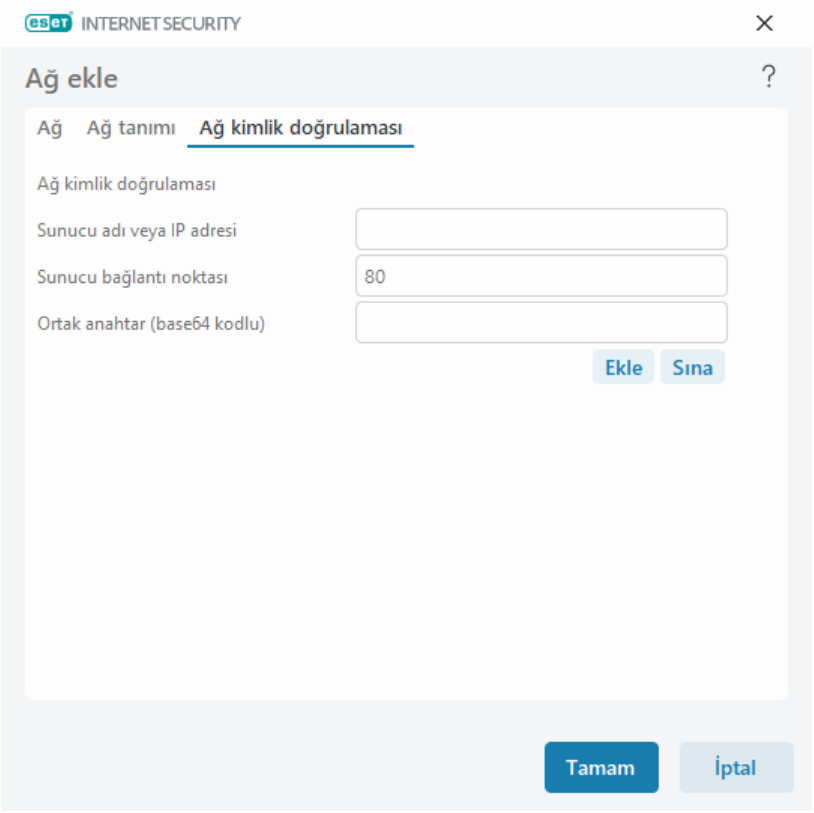
Ağ kimlik doğrulaması

Ağ kimlik doğrulaması ağdaki belirli bir sunucuyu arar ve bu sunucunun kimliğini doğrulamak için asimetrik şifrelemeyi (RSA) kullanır. Kimlik doğrulaması yapılan ağın adı kimlik doğrulama sunucu ayarlarında belirlenen bölge adıyla eşleşmelidir. Ad büyük/küçük harfe duyarlıdır. Özel sunucu anahtarına karşılık gelen bir sunucu adı, sunucu dinleme bağlantı noktası ve ortak anahtar belirleyin (bkz. Ağ kimlik doğrulaması - Sunucu yapılandırması). Sunucu adı IP adresi, DNS veya NetBios adı biçiminde girilebilir ve ardından anahtarın sunucudaki konumunu belirten bir yol gelebilir (örneğin, sunucu_adi_/dizin1/dizin2/kimlikdogrulamasi). Kullanılacak alternatif sunucuları, noktalı virgülle ayırarak yola ekleme suretiyle belirleyebilirsiniz.

ESET Authentication Server indirin.

Ortak anahtar aşağıdaki dosya türlerinden herhangi biri kullanılarak alınabilir:

- PEM şifrelenmiş ortak anahtarı (.pem), bu anahtar ESET Kimlik Doğrulama Sunucusu kullanılarak oluşturulabilir (Ağ kimlik doğrulaması - Sunucu yapılandırması bölümüne bakın).
- Şifrelenmiş ortak anahtar
- Ortak anahtar sertifikası (.crt)



Ayarlarınızı sınamak için **Sına** seçeneğini tıklatın. Kimlik doğrulama başarılı olursa Sunucu kimlik doğrulaması başarılı oldu bildirimi görüntülenir. Kimlik doğrulama düzgün biçimde yapılandırılmamışsa aşağıdaki hata iletilerinden biri görüntülenir:

Sunucu kimlik doğrulaması başarısız oldu. Geçersiz veya eşleşmeyen imza.
Sunucu imzası, girilen ortak anahtar ile eşleşmez.

Sunucu kimlik doğrulaması başarısız oldu. Ağ adı eşleşmiyor.
Yapılandırılan ağ adı, kimlik doğrulama sunucusu bölge adına karşılık gelmiyor. Her iki adı da inceleyin ve aynı olduğundan emin olun.

Sunucu kimlik doğrulaması başarısız oldu. Sunucudan gelen yanıt yok ya da geçersiz.
Sunucu çalışmıyorsa veya sunucuya erişilemiyorsa yanıt alınmaz. Başka bir HTTP sunucusu belirlenen adreste çalışıyorsa geçersiz bir yanıt alınabilir.

Geçersiz ortak anahtar girildi.
Girdiğiniz ortak anahtar dosyasının bozuk olmadığından emin olun.

Ağ kimlik doğrulaması - Sunucu yapılandırması

Kimlik doğrulama süreci, kimlik doğrulaması yapılacak ağa bağlı olan herhangi bir bilgisayar/sunucu tarafından yürütülebilir. Bir istemci ağa bağlanmak üzere her girişimde bulunduğunda kimlik doğrulaması için her zaman erişilebilir durumda olan bir bilgisayara/sunucuya ESET Authentication Server uygulamasının yüklenmesi gerekir. ESET Authentication Server uygulamasının yükleme dosyası ESET'in web sitesinden indirilebilir.

ESET Authentication Server uygulamasını yükledikten sonra, bir iletişim penceresi görüntülenir (**Başlat** > **Programlar** > **ESET** > **ESET Authentication Server** öğelerini tıklatarak uygulamaya erişebilirsiniz).

Kimlik doğrulama sunucusunu yapılandırmak için kimlik doğrulama bölgesi adını, sunucu dinleme bağlantı noktasını (varsayılan 80'dir), ortak ve özel anahtar çiftinin depolanacağı konumu girin. Ardından, kimlik doğrulama

işleminde kullanılacak ortak ve özel anahtarı oluşturun. Özel anahtar sunucuda kalırken; ortak anahtarın, güvenlik duvarı ayarlarında bölge ayarlama sırasında istemci tarafında Bölge kimlik doğrulama bölümünde alınması gerekir.

Daha fazla bilgi için şu ESET Bilgi Bankası makalesini okuyun.

Bölge yapılandırma

Bölge, IP adreslerini içeren mantıksal bir grup oluşturan ağ adresleri topluluğudur. Birden fazla kuralda aynı adres kümesini tekrar kullanırken yararlıdır. Verilen gruptaki her bir adrese tüm grup için merkezi olarak tanımlanmış benzer kurallar atanır. Böyle bir grup için **Güvenilir bölge** örnek olarak gösterilebilir. Güvenilir bölge, Güvenlik duvarı tarafından herhangi bir şekilde engellenmeyen ağ adresleri grubunu temsil eder.

Güvenilir bölge eklemek için:

1. **Gelişmiş ayarlar** (F5) > **Ağ koruması** > **Temel** > **Bölgeler**'i açın.
2. **Bölgeler**'in yanındaki **Düzenle**'yi tıklayın.
3. **Ekle**'yi tıklayın, bölge için bir **Ad** ve **Açıklama** yazın ve **Uzak bilgisayar adresi (IPv4/IPv6, aralık, maske)** alanına uzak IP adresini girin.
4. **Tamam**'ı tıklayın.

Daha fazla bilgi için Güvenlik duvarı bölgeleri'ne bakın.

Güvenlik duvarı bölgeleri

Bölgeler hakkında daha fazla bilgi için Bölgelerin yapılandırılması bölümüne bakın.

Sütunlar

Ad – Uzak bilgisayarlar grubunun adı.

IP adresleri - Bir bölgeye ait olan uzak IP adresleri.

Denetim öğeleri

Bir bölge için **ekle** veya **düzenle** eylemlerinden birini seçtiğinizde şu alanlar kullanılır:

Ad – Uzak bilgisayarlar grubunun adı.

Açıklama – Grubun genel açıklaması.

Uzak bilgisayar adresi (IPv4, IPv6, aralık, maske) – Uzak adres, adres aralığı veya alt ağ eklemenize olanak tanır.

Sil – Bölgeyi listeden kaldırır.

> Önceden tanımlı bölgeler kaldırılamaz.

Güvenlik Duvarı

Güvenlik duvarı, sisteme gelen ve giden tüm ağ trafiğini denetler. Bu, her bir ağ bağlantısına belirtilen filtre kurallarına göre izin vererek veya engelleyerek yapılır. Uzak cihazlardan gelen saldırılara karşı koruma sağlar ve tehlikeli olabilecek bazı hizmetleri engelleyebilir.

Temel

Güvenlik Duvarını etkinleştir

Sisteminizin güvenliğini sağlamak için bu özelliği etkin halde bırakmanızı öneririz. Etkin haldeki güvenlik duvarıyla, ağ trafiği her iki yönde taranır.

Windows Güvenlik Duvarı'ndaki kuralları da değerlendir

Otomatik modda, ESET kuralları tarafından engellenmemesi halinde, Windows Firewall'daki kurallar tarafından izin verilen gelen trafiğe de izin verin.

Filtreleme modu

Güvenlik duvarının davranışı filtreleme moduna göre değişir. Filtreleme modları aynı zamanda gerekli kullanıcı müdahalesi düzeyini de etkiler.

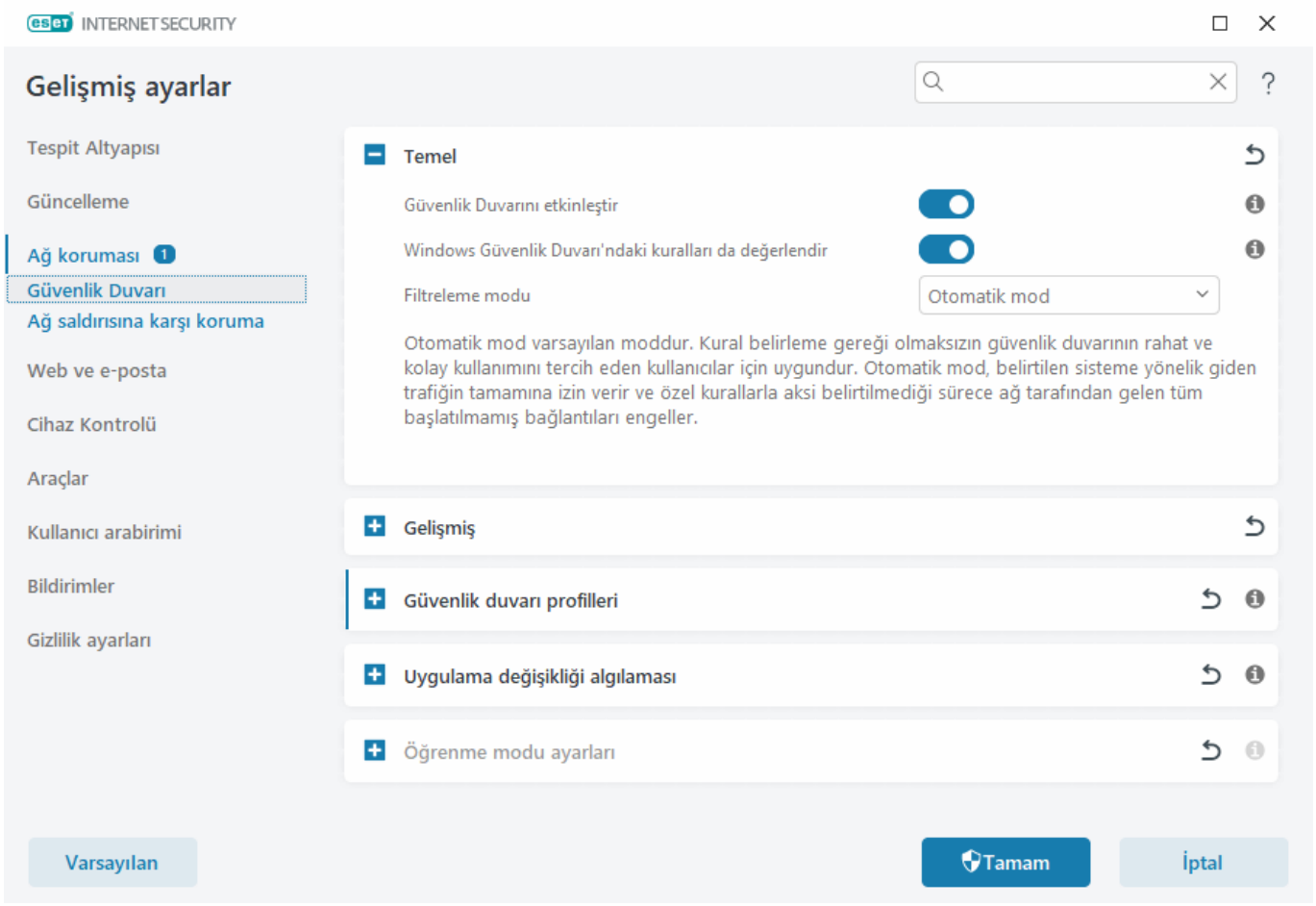
ESET Internet Security Güvenlik Duvarı için şu filtreleme modları kullanılabilir:

Filtreleme modu	Açıklama
Otomatik mod	Varsayılan mod. Bu mod güvenlik duvarını kural tanımlamaya gerek duymadan, kolay ve rahat bir şekilde kullanmayı tercih eden kullanıcılar için uygundur. Özel, kullanıcı tanımlı kurallar oluşturulabilir, ancak bunlar **Otomatik modda** gerekli değildir. Otomatik mod belirli bir sistem için tüm giden trafiğe izin verirken (IDS ve gelişmiş seçenek/İzin verilen hizmetler seçeneğinde belirtildiği şekilde) Güvenilir Bölgeden bazı trafikler ve yakın zamandaki giden iletişimlere verilen yanıtlar hariç gelen trafiğin çoğunu engeller.
Etkileşimli mod	Güvenlik duvarı için özel bir yapılandırma oluşturmanıza olanak sağlar. Bir iletişim algılandığında ve söz konusu iletişime ilişkin uygulanan herhangi bir kural yoksa bilinmeyen bağlantıyı bildiren bir iletişim penceresi görüntülenir. Bu iletişim penceresi iletişim için izin verme veya engelleme seçeneği sunar ve izin verme veya engelleme kararı Güvenlik duvarının yeni bir kuralı olarak kaydedilebilir. Yeni bir kural oluşturmayı seçerseniz ileride yapılacak bu türdeki tüm bağlantılara o kurala göre izin verilir veya bağlantılar engellenir.
İlke tabanlı mod	Kendilerine izin veren belirli bir kural tarafından tanımlanmamış tüm bağlantılar engellenir. Bu mod, ileri düzey kullanıcıların yalnızca istenen ve güvenli bağlantılara izin veren kurallar tanımlamasına olanak tanır. Belirtilmemiş diğer tüm bağlantılar Güvenlik duvarı tarafından engellenir.
Öğrenme modu	Kuralları otomatik olarak oluşturur ve kaydeder. Bu mod, Güvenlik duvarının ilk yapılandırılması için çok uygundur, ancak uzun süre boyunca etkin halde bırakılmamalıdır. ESET Internet Security kuralları önceden tanımlı parametrelere göre kaydettiği için herhangi bir kullanıcı müdahalesi gerekmez. Öğrenme modu güvenlik risklerini ortadan kaldırmak amacıyla sadece gerekli iletişimler için tüm kurallar oluşturulana kadar kullanılmalıdır.

Gelişmiş

Kurallar

Kurallar ayarları, güvenilen bölgelerdeki ve Internet'teki ayrı uygulamalar tarafından oluşturulan trafiğe uygulanan tüm kuralları görüntülemenize izin verir.



Bilgisayarınıza Botnet saldırısı olduğunda IDS kuralı oluşturabilirsiniz. Kural, **Gelişmiş ayarlar** (F5) > **Ağ koruması** > **Ağ saldırısı koruması** > **IDS kuralları** seçeneğinde **Düzenle**'yi tıklayarak değiştirilebilir.

İzin verilen hizmetler

Bilgisayarınızda çalışan ortak ağ hizmetlerine erişimi yapılandırın. Daha fazla bilgi için izin verilen hizmetler'e bakın.

Güvenlik duvarı profilleri

Güvenlik duvarı profilleri farklı durumlarda farklı kural kümeleri belirleyerek ESET Internet Security Kişisel güvenlik duvarının davranışını özelleştirmek için kullanılabilir.

Uygulama değişikliği algılaması

Uygulama değişikliği tespiti özelliği, güvenlik duvarı kuralının bulunduğu değiştirilmiş uygulamalar bağlantı kurmaya çalışırsa bildirimleri görüntüler.

Güvenlik duvarı profilleri

Profiller, ESET Internet Security Güvenlik duvarı davranışını denetlemek için kullanılabilir. Güvenlik duvarı kuralı oluştururken veya düzenlerken söz konusu kuralı belirli bir profile atayabilir veya her profile uygulayabilirsiniz. Bir profil ağ arabiriminde etkin olduğunda, yalnızca genel kurallar (profil belirtilmemiş kurallar) ve söz konusu profile atanmış kurallar uygulanır. Güvenlik duvarı davranışını kolayca değiştirmek için ağ bağdaştırıcılarına atanmış veya ağlara atanmış farklı kurallara sahip birden fazla profil oluşturabilirsiniz.

Profilleri düzenleyebileceğiniz **Güvenlik Duvarı Profilleri** penceresini açmak için Profil Listesi'nin yanındaki **Düzenle** öğesini tıklatın.

Ağ bağdaştırıcısı, belirli bir ağ için yapılandırılan profilin bu ağa bağlanıldığında kullanılması için ayarlanabilir. **Gelişmiş ayarlar** (F5) > **Ağ koruması** > **Bilinen Ağlar** > **Düzenle** içinde belirtilen ağda kullanılacak özel bir profil de atayabilirsiniz. **Bilinen ağlar** listesinden bir ağ seçin ve **Güvenlik duvarı profili** açılır menüsünden belirli bir ağa güvenlik duvarı profili atamak için Düzenle seçeneğine tıklatın.

Bu ağa atanmış bir profil yoksa bağdaştırıcının varsayılan profili kullanılır. Bağdaştırıcı, ağ profilini kullanmamak üzere ayarlandıysa hangi ağa bağlandığı dikkate alınmaksızın varsayılan profili kullanılır. Ağ için veya bağdaştırıcı yapılandırması için profil yoksa genel varsayılan profil kullanılır. Ağ bağdaştırıcısına bir profil atamak için ağ bağdaştırıcısını seçin, **Ağ bağdaştırıcılarına atanan profiller** öğesinin yanındaki **Düzenle** seçeneğini tıklatın, **Varsayılan güvenlik duvarı profili** açılır menüsünden profili seçin.

Güvenlik duvarı başka bir profile geçiş yaptığında, ekranınızın sağ alt köşesinde bir bildirim görüntülenir.

İletişim penceresi - Güvenlik duvarı profillerini düzenle

Buradan profillerle ilgili **Ekle**, **Düzenle** veya **Kaldır** eylemlerini gerçekleştirebilirsiniz. Bir profille ilgili olarak **Düzenle** veya **Kaldır** eylemini gerçekleştirmek için profilin **Güvenlik Duvarı Profiller** penceresindeki listeden seçilmesi gerektiğini unutmayın.

Daha fazla bilgi için Güvenlik Duvarı Profilleri başlığına bakın.

Profiller ağ bağdaştırıcılarına atanır

Profilleri değiştirerek güvenlik duvarı davranışlarında hızlı bir şekilde birden fazla değişiklik yapabilirsiniz. Profil - Belirli profiller için özel kurallar ayarlanıp uygulanabilir. Makinede bulunan tüm bağdaştırıcılar için ağ bağdaştırıcı girişleri **Ağ bağdaştırıcıları** listesine otomatik olarak eklenir.

Sütunlar

Ad – Ağ bağdaştırıcısının adı.

Varsayılan güvenlik duvarı profili – Varsayılan profil, bağlı olduğunuz ağ yapılandırılmış bir profile sahip değilse

veya ağ bağdaştırıcınız ağ profili kullanmak üzere ayarlanmadıysa kullanılır.

Ağ profilini tercih et – **Bağlı ağın güvenlik duvarı profilini** tercih et etkinleştirildiğinde ağ bağdaştırıcısı her fırsatta, bağlı ağa atanan güvenlik duvarı profilini kullanır.

Denetim öğeleri

Ekle – Yeni ağ bağdaştırıcısı ekler.

Düzenle – Mevcut ağ bağdaştırıcısını düzenlemenize olanak sağlar.

Kaldır – Bir ağ bağdaştırıcısını listeden kaldırmak istiyorsanız bir ağ bağdaştırıcısı seçin ve **Kaldır** öğesini tıklatın.

Tamam/İptal - Değişiklikleri kaydetmek isterseniz **Tamam**'ı, değişiklikleri kabul etmeden ayrılmak için **İptal**'i tıklatın.

Kuralları yapılandırma ve kullanma

Kurallar, tüm ağ bağlantılarını anlamlı olarak sınamak amacıyla kullanılan koşullar kümesini ve bu koşullara atanmış tüm eylemleri temsil eder. Güvenlik duvarı kurallarını kullanarak, farklı türlerde ağ bağlantıları kurulduğunda hangi eylemin gerçekleştirileceğini tanımlayabilirsiniz. Kural filtreleme ayarlarına erişmek için **Gelişmiş ayarlar** (F5) > **Güvenlik duvarı** > **Gelişmiş** öğesine gidin. Önceden tanımlı bazı kurallar **izin verilen hizmetler** (IDS ve gelişmiş seçenekler) içindeki onay kutularına bağlıdır ve doğrudan kapatılamaz, bunun yerine bu ilgili onay kutularını kullanabilirsiniz.

ESET Internet Security ürününün önceki sürümünden farklı olarak kurallar baştan sona değerlendirilir. Eşleşen ilk kuralın eylemi değerlendirilmekte olan ağ bağlantılarından her biri için kullanılır. Bu, kuralların önceliğinin otomatik olduğu ve daha özel kuralların genel olanlardan daha öncelikli olduğu önceki sürümden farklı olan önemli bir davranış değişikliğidir.

Bağlantılar gelen ve giden bağlantılar olarak ikiye ayrılabilir. Gelen bağlantılar, yerel sistemle bağlantı kurmaya çalışan uzak bir cihaz tarafından başlatılır. Giden bağlantılar ise tersi yönde çalışır; yerel sistem uzak cihazla bağlantı kurar.

Yeni bir bilinmeyen iletişim algılanırsa, buna izin vermek veya bunu reddetmek konusunda dikkatlice düşünmelisiniz. İstenmeden gelen, güvenli olmayan veya bilinmeyen bağlantılar sistem için bir güvenlik riski oluşturur. Böyle bir bağlantı kurulursa uzak cihaza ve bilgisayarınıza bağlanmaya çalışan uygulamaya dikkat etmenizi öneririz. Birçok sızıntı, özel verileri elde etmeye ve göndermeye veya ana bilgisayar iş istasyonlarına kötü amaçlı uygulamalar yüklemeye çalışır. Güvenlik duvarı, bu tür bağlantıları algılayıp sonlandırmanıza olanak sağlar.

Güvenlik duvarı kuralları listesi

Güvenlik Duvarı kurallarını içeren liste **Gelişmiş ayarlar** (F5) > **Ağ koruması** > **Güvenlik duvarı** > **Gelişmiş** bölümünde, **Kurallar**'ın yanındaki **Düzenle**'yi tıklayarak bulunabilir.

Sütunlar

Ad – Kuralın adı.

Etkin – Kuralların etkin veya devre dışı olma durumunu gösterir. Bir kuralın etkinleştirilmesi için ilgili onay kutusunun seçilmesi gerekir.

Protokol – Bu kuralın geçerli olduğu protokolü gösterir.

Profil – Bu kuralın geçerli olduğu güvenlik duvarı profilini gösterir.

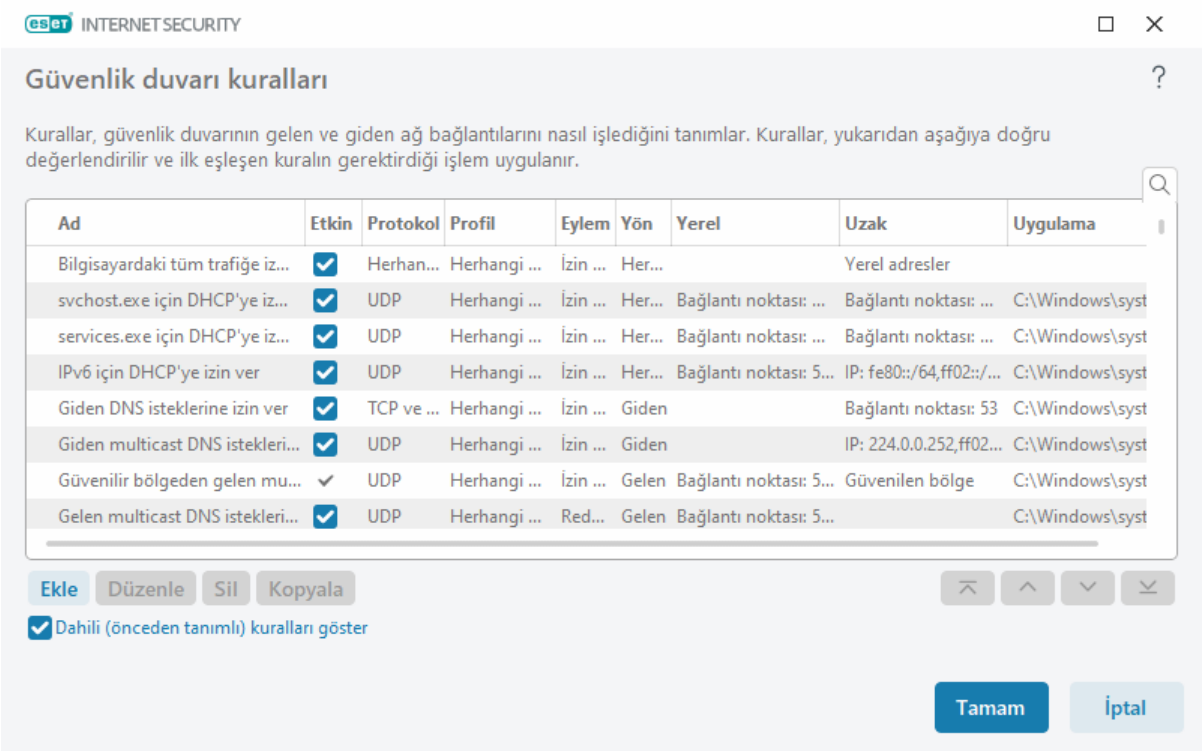
Eylem – İletişim durumunu gösterir (engelle/izin ver/sor).

Yön – İletişim yönü (gelen/giden/her ikisi).

Yerel – Yerel bilgisayarın uzak Ipv4 veya Ipv6 adresi / aralığı / alt ağı ve bağlantı noktası.

Uzak - Uzak cihazın uzak Ipv4 veya Ipv6 adresi/aralığı/alt ağı ve bağlantı noktası.

Uygulamala - Kuralın geçerli olduğu uygulamayı belirtir.



Denetim öğeleri

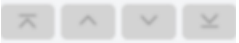
Ekle – Yeni bir kural oluşturur.

Düzenle – Mevcut bir kuralı düzenleyin.

Sil – Mevcut bir kuralı kaldırın.

Kopyala - Seçilen bir kuralın kopyasını oluşturun.

Dahili (önceden tanımlı) kuralları göster – Belirli iletişimlere izin veren veya bunları reddeden ESET Internet Security tarafından önceden tanımlanmış kurallar. Bu kuralları devre dışı bırakabilirsiniz, ancak önceden tanımlı bir kuralı silemezsiniz.

 **Üst/Yukarı/Aşağı/Alt** - Kuralların öncelik düzeyini ayarlamanıza olanak tanır (kurallar baştan aşağı yürütülür).

Kuralları ada, protokole veya bağlantı noktasına göre aramak için sağ üst taraftaki arama simgesini tıklayın.

Güvenlik duvarı kuralları ekleme veya düzenleme

Bir kuraldan etkilenen bir uygulamanın doğru şekilde çalışması için ağ ayarları değiştiğinde (örneğin, uzak taraf için ağ adresi veya bağlantı noktası numarası değiştirildiğinde) Güvenlik duvarı kurallarını düzenlemek veya eklemek gerekebilir.

Resimli talimatlar

Aşağıdaki ESET Bilgi Bankası makaleleri sadece İngilizce dilinde mevcuttur:

- ESET güvenlik duvarındaki belirli bir bağlantı noktasını açın veya kapatın (izin verin veya reddedin)
- ESET Internet Security günlük dosyalarından bir güvenlik duvarı kuralı oluşturun

Pencerenin üst tarafında üç sekme vardır:

- **Genel** – Kural adı, bağlantı yönü, eylem (**İzin ver**, **Reddet**, **Sor**), protokol ve kuralın uygulanacağı profil belirtin.

- **Yerel** – Yerel bağlantı noktasının numarası veya bağlantı noktası aralığı ve iletişim kuran uygulamanın adı da dahil olmak üzere, bağlantının yerel tarafı hakkındaki bilgileri görüntüler. **Ekle'ye** tıklayarak burada IP adresleri aralığıyla önceden tanımlı veya oluşturulan bir bölge eklemenize olanak sağlar.

- **Uzak** – Bu sekme uzak bağlantı noktasıyla (bağlantı noktası aralığıyla) ilgili bilgiler içerir. Belirli bir kural için uzak IP adresi veya bölge listesi tanımlamanıza izin verir. **Ekle'ye** tıklayarak burada IP adresleri aralığıyla önceden tanımlı veya oluşturulan bir bölge eklemenize olanak sağlar.

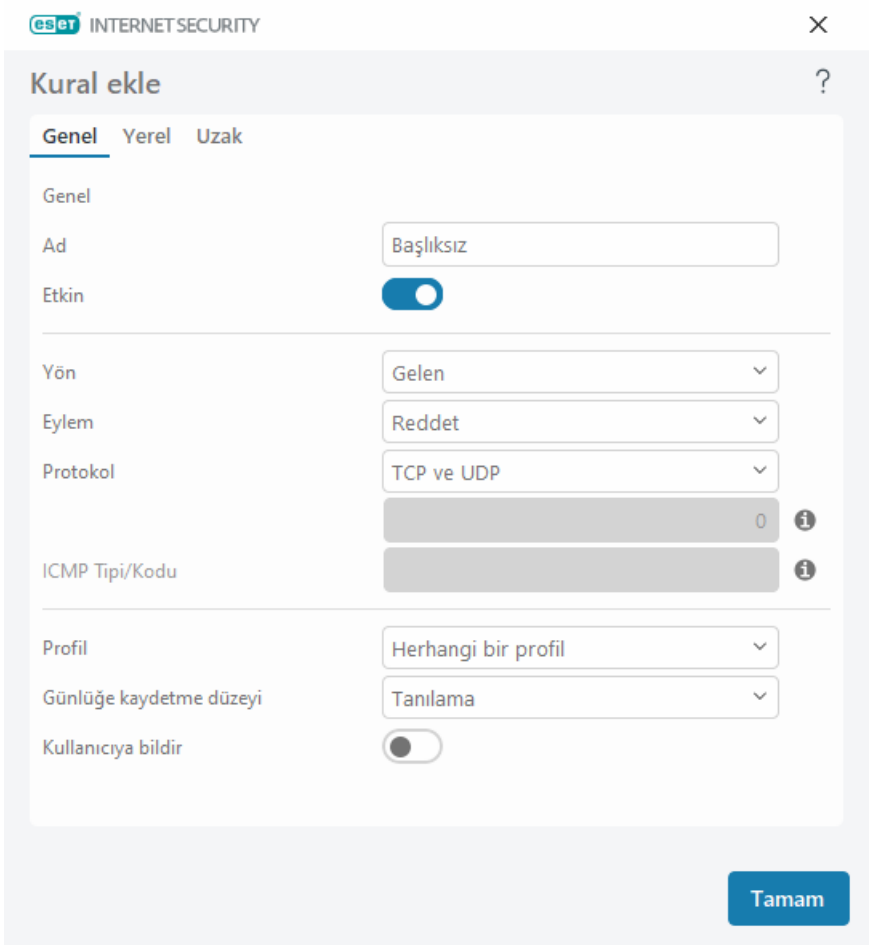
Yeni bir kural oluştururken **Ad** alanına kural için bir ad girmeniz gerekir. Bir iletişim, **Eylem** açılır menüsünden bir kurala karşılaştığında **Dizin** açılır menüsünden kuralın uygulanacağı dizini ve yürütülecek eylemi seçin.

Protokol kural için kullanılan aktarma protokolünü temsil eder. Açılır menüden belirlenen kural için kullanılacak protokolü seçin.

ICMP Türü/Kodu Bir sayıyla tanımlanan ICMP iletisini ifade eder (örneğin; 0, "Yankı Yanıtı"nı ifade eder).

Tüm kurallar varsayılan olarak **Herhangi bir profil** için etkindir. Alternatif olarak **Profiller** açılır menüsünü kullanarak özel bir güvenlik duvarı profili seçebilirsiniz.

Günlüğe kaydetme düzeyi öğesini etkinleştirirseniz kuralla ilişkili etkinlik bir günlüğe kaydedilir. **Kullanıcıya bildir** seçeneği kural uygulandığında bir bildirim görüntüler.



Firefox Web tarayıcısı uygulamasının Internet / yerel ağ web sitelerine erişmesine olanak tanıyacak yeni bir kural oluştururuz.
1.**Genel** sekmesinde, TCP ve UDP protokolü aracılığıyla giden iletişimi etkinleştirin.
2.**Yerel** sekmesini tıklayın.
3.**...** öğesini tıklayarak kullandığınız web tarayıcısının dosya yolunu seçin (örneğin *C:\Program Files\Firefox\Firefox.exe*). Uygulamanın adını GİRMEYİN.
4.**Uzak** sekmesinde, standart Internet taramasına izin vermek istiyorsanız 80 VE 443 bağlantı noktalarını etkinleştirin.

Önceden tanımlı kurallar sınırlı bir şekilde değiştirilebilir.

Güvenlik duvarı kuralı - Yerel

Kuralın uygulanacağı yerel uygulamanın adını ve yerel bağlantı noktasını/bağlantı noktalarını ekleyin.

Bağlantı noktası - Uzak bağlantı noktası numaraları. Numara belirtilmezse kural tüm bağlantı noktalarına uygulanır. Tek bir iletişim bağlantı noktası veya iletişim bağlantı noktaları aralığı ekleyin.

IP - Kuralın uygulanacağı yerel adres/adresler, adres aralığı veya alt ağ eklemenize olanak tanır. Herhangi bir değer belirtilmezse kural, tüm iletişim için uygulanır.

Bölgeler – Eklenen bölgelerin listesi.

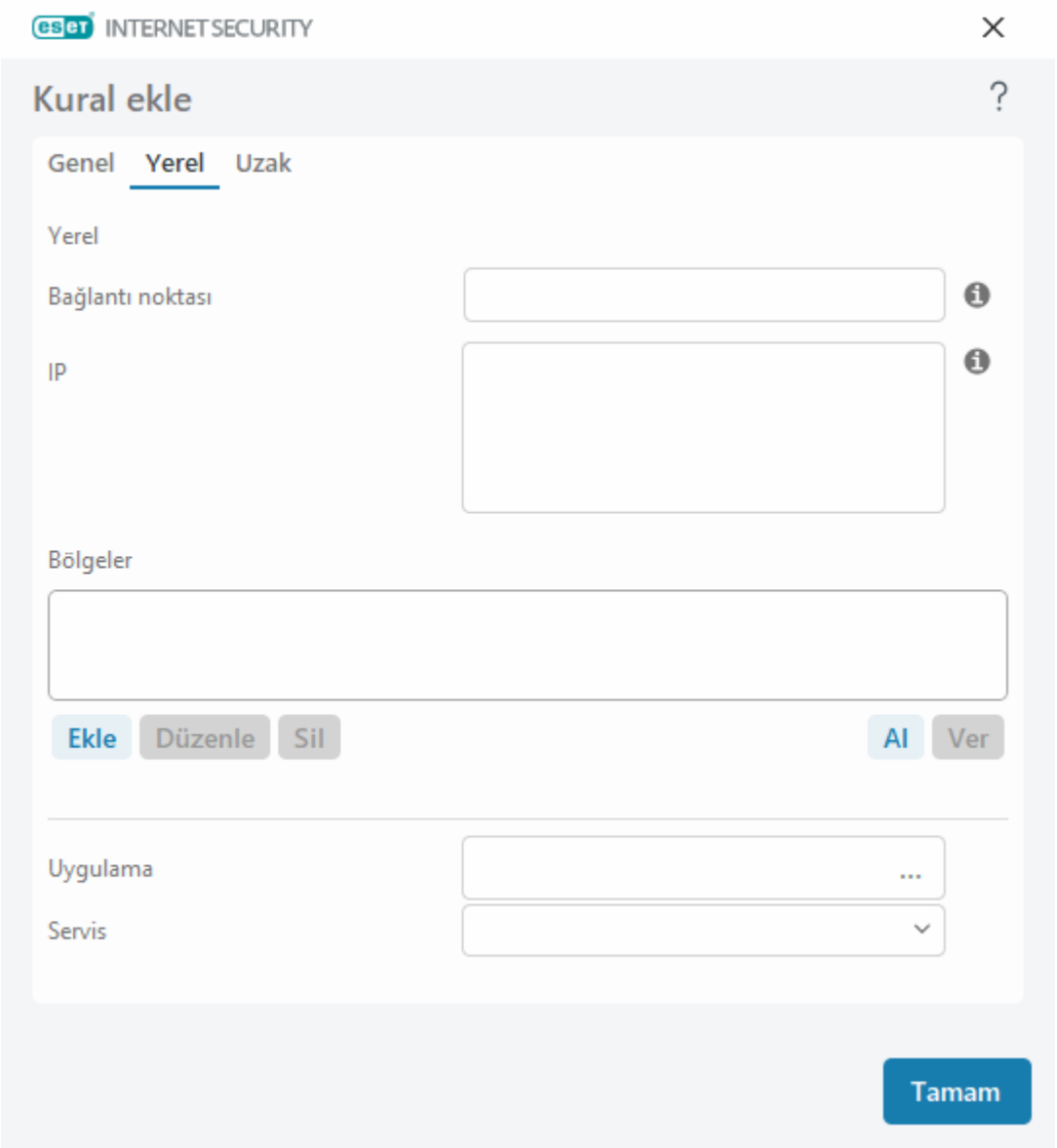
Ekle – Açılır menüden oluşturulan bölgeyi ekler. Bölge oluşturmak için Bölge ayarları sekmesini kullanın.

Kaldır – Bölgeleri listeden kaldırır.

Uygulama – Kuralın geçerli olduğu uygulamanın adı. Kuralın uygulanacağı uygulamanın konumunu ekleyin.

Servis – Açılır menü, sistem servislerini gösterir.

> Açılır menüdeki iletişim için EHttpSrv servisi kullanarak 2221 bağlantı noktasından güncellemeler sağlayan Yansıtmanızda uygulanacak bir kural oluşturmak isteyebilirsiniz.



Güvenlik duvarı kuralı - Uzak

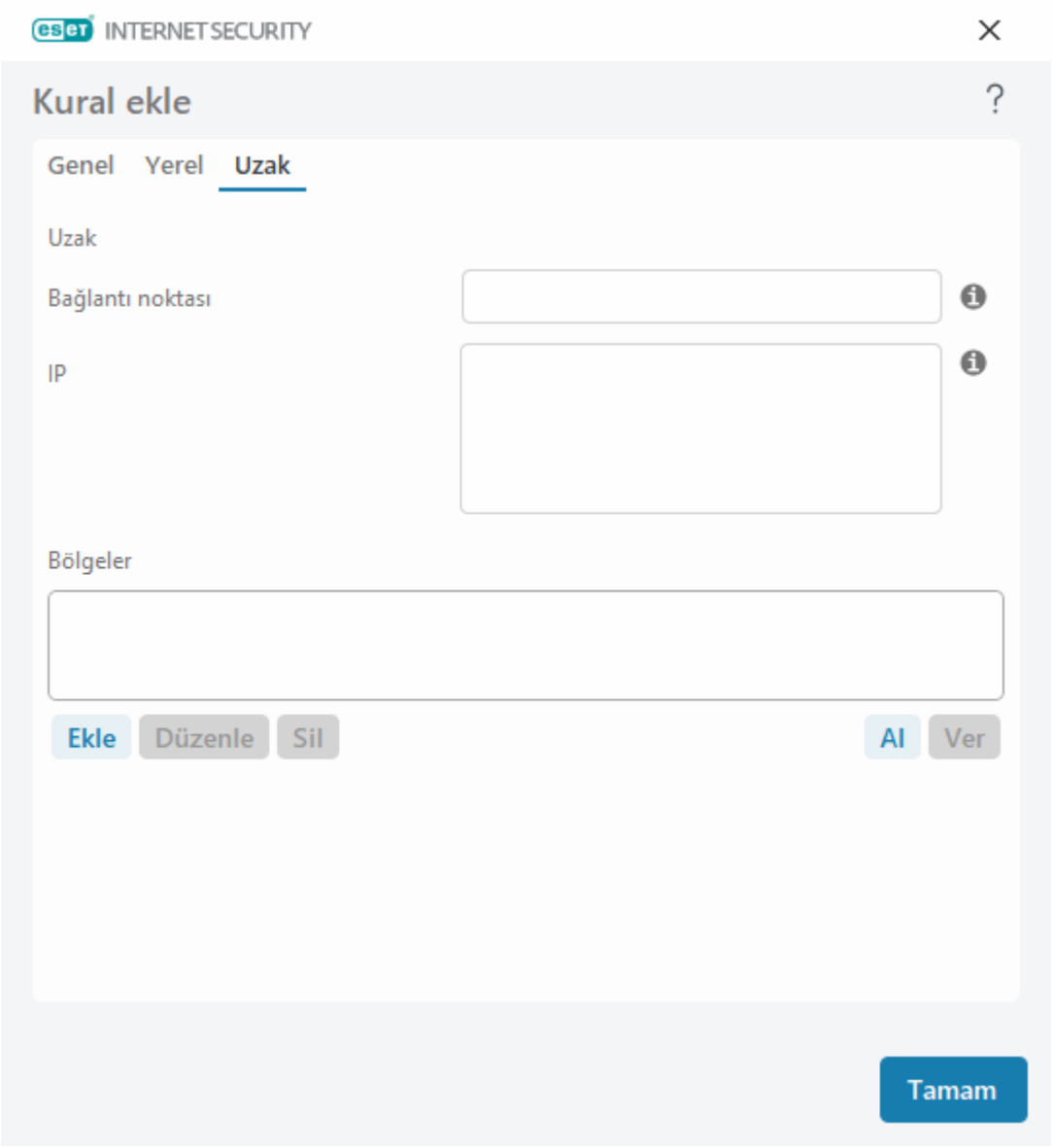
Bağlantı noktası - Uzak bağlantı noktası numaraları. Numara belirtilmezse kural tüm bağlantı noktalarına uygulanır. Tek bir iletişim bağlantı noktası veya iletişim bağlantı noktaları aralığı ekleyin.

IP – Uzak adres, adres aralığı veya alt ağ eklemenize olanak tanır. Kuralın uygulanacağı adres, aralık/alt ağ veya uzak bölge. Değer belirtilmezse, kural tüm iletişime uygulanır.

Bölgeler – Eklenen bölgelerin listesi.

Ekle – Açılır menüden seçerek bir bölge ekleyebilirsiniz. Bölge oluşturmak için Bölge ayarları sekmesini kullanın.

Kaldır – Bölgeleri listeden kaldırır.



Uygulama değişikliği algılaması

Uygulama değişikliği algılama özelliği, güvenlik duvarı kuralının bulunduğu değiştirilmiş uygulamalar bağlantı kurmaya çalışırsa bildirim görüntüler. Uygulama değişikliği, orijinal bir uygulamayı farklı bir yürütülebilir tarafından gerçekleştirilen başka bir uygulama ile geçici veya kalıcı olarak değiştirme mekanizmasıdır (güvenlik duvarı kurallarının kötüye kullanılmasına karşı korur).

Bu özelliğin genel olarak herhangi bir uygulamada yapılan değişiklikleri algılama amaçlı olmadığını lütfen unutmayın. Amacı güvenliği tehdit edici varolan güvenlik duvarı kurallarını engellemek ve yalnızca belirli güvenlik duvarı kurallarının var olduğu uygulamaların izlenmesini sağlamaktır.

Uygulama değişikliklerini algılamayı etkinleştir – Seçilirse, program uygulamalardaki değişiklikleri (güncellemeler, virüsten etkilenme, diğer değişiklikler) izler. Değiştirilen bir uygulama bağlantı kurmaya çalıştığında, Güvenlik duvarı tarafından bilgilendirilirsiniz.

İmzalı (güvenilir) uygulamalarda değişikliğe izin ver – Uygulama, değişiklikten önce ve sonra aynı geçerli dijital imzaya sahipse bildirmez.

Tespit dışında bırakılan uygulamaların listesi - Bu pencere, bildirim olmaksızın değişikliğe izin verilen uygulamaları tek tek eklemenize veya kaldırmanıza izin verir.

Algılama dışı bırakılan uygulamaların listesi

ESET Internet Security içindeki güvenlik duvarı kuralların mevcut olduğu uygulamalarda yapılan değişiklikleri algılar (Uygulama değişikliği algılaması bölümüne bakın).

Bazı durumlarda, güvenlik duvarının denetlemesinin dışında tutmak istediğinizde bu işlevselliği bazı uygulamalarda kullanmak istemeyebilirsiniz.

Ekle - Değişiklik tespiti dışında bırakılan uygulamalar listesine eklemek için bir uygulama seçebileceğiniz bir pencere açılır. Açık ağ iletişimi olan, güvenlik duvarı kuralının var olduğu çalışan uygulamalar listesinden seçim yapabilir veya belirli bir uygulama ekleyebilirsiniz.

Düzenle - Değişiklik tespiti dışında bırakılan uygulamalar listesinde yer alan bir uygulamanın konumunu değiştirebileceğiniz bir pencere açılır. Açık ağ iletişimi olan, güvenlik duvarı kuralının bulunduğu çalışan uygulamalar listesinden seçim yapabilir veya konumu manuel olarak değiştirebilirsiniz.

Kaldır - Değişiklik algılaması dışında bırakılan uygulamalar listesinden girişleri kaldırır.

Öğrenme modu ayarları

Öğrenme modu, sistemde kurulmuş her bir iletişim için otomatik olarak bir kural oluşturur ve kaydeder. ESET Internet Security Kuralları önceden tanımlı parametrelere göre kaydettiği için herhangi bir kullanıcı müdahalesi gerekmez.

Bu mod sisteminiz için riskli olabilir ve yalnızca Güvenlik duvarının ilk yapılandırmasında kullanılması önerilir.

Öğrenme modu seçenekleri'ni etkinleştirmek için **Gelişmiş ayarlar** (F5) > **Güvenlik Duvarı** > **Temel** > **Filtreleme modu**'ndaki açılır menüden **Öğrenme modu**'nu seçin. Bu bölümde aşağıdaki öğeler bulunur:

> ⚠ Öğrenme modundayken, Güvenlik duvarı iletişime filtre uygulamaz. Tüm giden ve gelen iletişimlere izin verilir. Bu modda, bilgisayarınız Güvenlik duvarı tarafından tam olarak korunmaz.

Öğrenme modunun süresi dolduktan sonra mod ayarlama – Öğrenme modu süresinin sona ermesinin ardından ESET Internet Security Güvenlik duvarının hangi filtreleme moduna geçeceğini belirtin. Filtreleme modları hakkında daha fazla bilgi edinin. Süre sona erdikten sonra **Kullanıcıya sor** seçeneği, güvenlik duvarı filtre moduna değişimi gerçekleştirmek için yönetici izinleri gerektirir.

İletişim türü – Her iletişim türü için özel kural oluşturma parametreleri seçin. Dört tür iletişim vardır:

Güvenilen bölgeden gelen trafik - Güvenilen bölge içerisindeki bir gelen bağlantıya örnek olarak, bilgisayarınızda çalıştırılan yerel bir uygulamayla iletişim kurmaya çalışan, güvenilen bölgedeki bir uzak cihaz verilebilir.

Güvenilen bölgeden giden trafik - Yerel ağda veya güvenilen bölgedeki bir ağda bulunan başka bir cihazla

bağlantı kurmaya çalışan yerel bir uygulama.

Gelen İnternet trafiği - Bilgisayarda çalışan bir uygulamayla iletişim kurmaya çalışan uzak cihaz.

Giden İnternet trafiği - Başka bir bilgisayarla bağlantı kurmaya çalışan yerel uygulama.

Her bölüm, yeni oluşturulan kurallara eklenecek parametreleri tanımlamanıza olanak tanır:

Yerel bağlantı noktası ekle – Ağ iletişiminin yerel bağlantı noktası numarasını içerir. Giden iletişimler için genellikle rastgele sayılar oluşturulur. Bu nedenle, bu seçeneğin yalnızca gelen iletişimler için etkinleştirilmesini öneririz.

Uygulama ekle – Yerel uygulamanın adını içerir. Bu seçenek, gelecekteki uygulama düzeyindeki kurallar (bir uygulamanın tamamı için iletişimi tanımlayan kurallar) için uygundur. Örneğin, yalnızca bir web tarayıcısı veya e-posta istemcisi için iletişimi etkinleştirebilirsiniz.

Uzak bağlantı noktası ekle – Ağ iletişiminin uzak bağlantı noktası numarasını içerir. Örneğin, standart bir bağlantı noktası numarasıyla ilişkilendirilmiş belirli bir hizmete (HTTP – 80, POP3 – 110, vb.) izin verebilir veya bu hizmeti reddedebilirsiniz.

Uzak IP adresi/Güvenilen bölge ekle – Uzak bir IP adresi veya bölge, yerel sistem ile o uzak adres / bölge arasındaki tüm ağ iletişimlerini tanımlayan yeni kurallar için bir parametre olarak kullanılabilir. Belirli bir cihaz veya ağ iletişimi olan bir cihaz grubu için eylemleri tanımlamak istiyorsanız bu seçenek uygundur.

Bir uygulama için maksimum farklı kural sayısı – Bir uygulama farklı bağlantı noktaları üzerinden çeşitli IP adresleri, vb. ile iletişim kuruyorsa, öğrenme modundaki güvenlik duvarı bu uygulama için uygun sayıda kural oluşturur. Bu seçenek, tek bir uygulama için oluşturulabilen kural sayısını sınırlandırmanıza olanak sağlar.

Ağ saldırısına karşı koruma (IDS)

Ağ saldırısına karşı koruma (IDS), bilinen güvenlik açıklarının tespitini iyileştirir. Sözlük'te Ağ saldırısına karşı koruma hakkında daha fazla bilgi edinin.

Ağ Saldırısına Karşı Korumayı etkinleştir (IDS) – Ağ trafiğinin içeriğini analiz eder ve ağ saldırılarına karşı koruma sağlar. Zararlı olduğu düşünülen tüm trafikler engellenir.

Botnet korumasını etkinleştir – Bilgisayara virüs bulaştığında ve bir bot iletişim kurma girişiminde bulunduğunda tipik modellere göre kötü amaçlı komutlar ve kontrol sunucuları içeren iletişimleri algılar ve engeller. Botnet korumasıyla ilgili sözlükte daha fazla bilgi edinin.

IDS kuralları - Bu seçenek, bilgisayarınıza zarar vermek için kullanılabilen çeşitli saldırı türlerini ve açıklardan yararlanma uygulamalarını algılamak üzere gelişmiş filtreleme seçeneklerini yapılandırmanıza izin verir.

> **Resimli talimatlar**
> Aşağıdaki ESET Bilgi Bankası makaleleri sadece İngilizce dilinde mevcuttur:
> - ESET Internet Security ürününde bir IP adresini IDS'den hariç tut

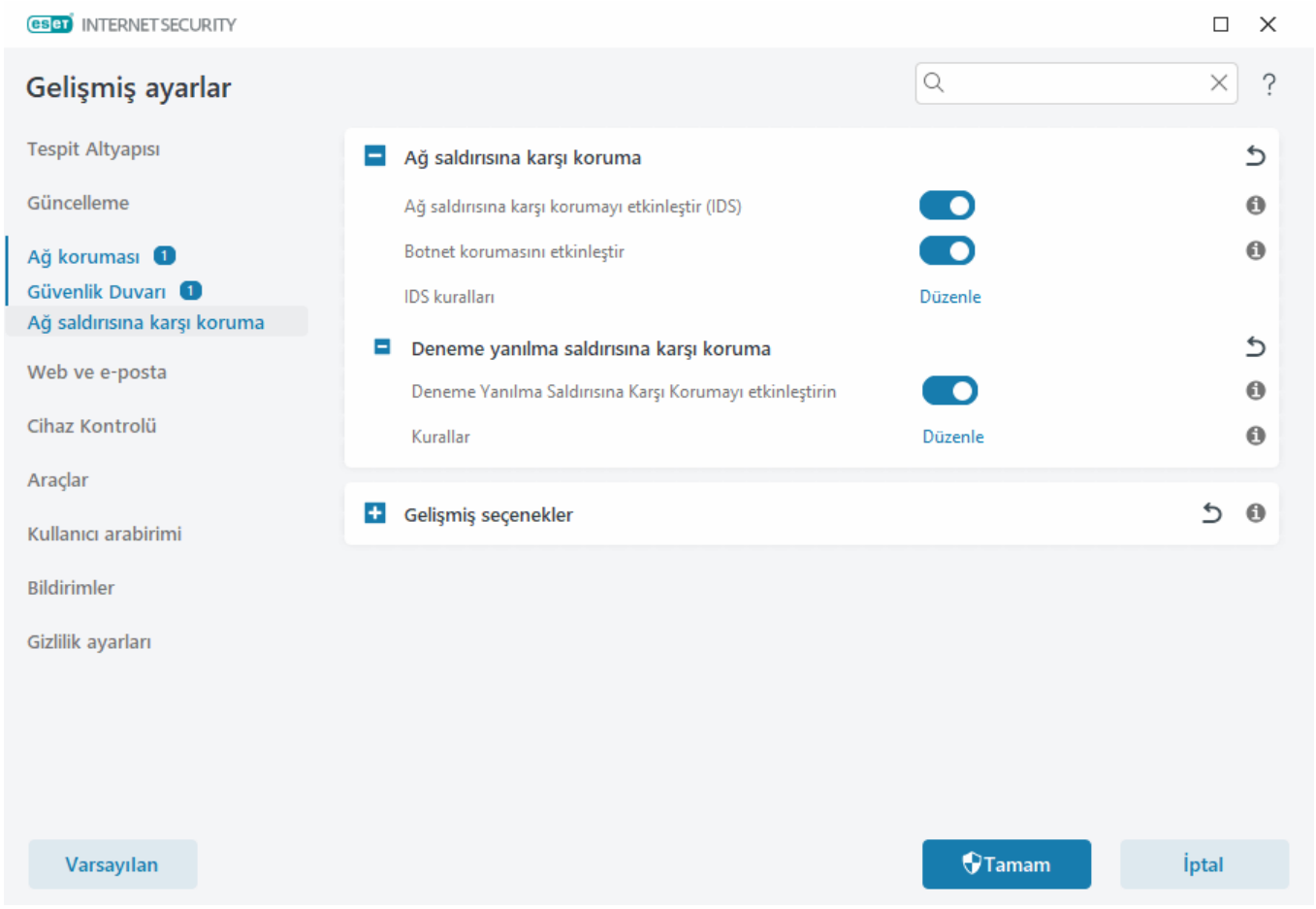
Ağ koruması tarafından tespit edilen tüm önemli olaylar bir günlük dosyasına kaydedilir. Daha fazla bilgi için ağ koruması günlüğüne bakın.

Deneme yanılma saldırısına karşı koruma

Deneme yanılma saldırısına karşı koruma, RDP ve SMB hizmetleri için parola tahmin saldırılarını engeller. Deneme yanılma saldırısı tüm harf, sayı ve sembol kombinasyonlarını sistemli bir şekilde deneyerek hedeflenen bir parolayı keşfetme yöntemidir. Deneme yanılma saldırısına karşı korumayı yapılandırmak için ana program penceresinde, **Ayarlar** > **Gelişmiş ayarlar** (F5) > **Ağ koruması** > **Ağ saldırısına karşı koruma** > **Deneme yanılma saldırısına karşı koruma**'yı tıklayın.

Deneme yanılma saldırısına karşı korumayı etkinleştir - ESET Internet Security ağ trafiği içeriğini inceler ve parola tahmin saldırılarına yönelik girişimleri engeller.

Kurallar - Gelen ve giden ağ bağlantıları için kurallar oluşturmanızı, düzenlemenizi ve görüntülemenizi sağlar. Daha fazla bilgi için Kurallar bölümüne bakın.



Kurallar

Deneme yanılma saldırılarına karşı koruma kuralları, gelen ve giden ağ bağlantıları için kurallar oluşturmanızı, düzenlemenizi ve görüntülemenizi sağlar. Önceden tanımlı kurallar düzenlenemez veya silinemez.

Deneme yanılma saldırısına karşı koruma kurallarını yönetme

Ekle – Yeni bir kural oluşturur.

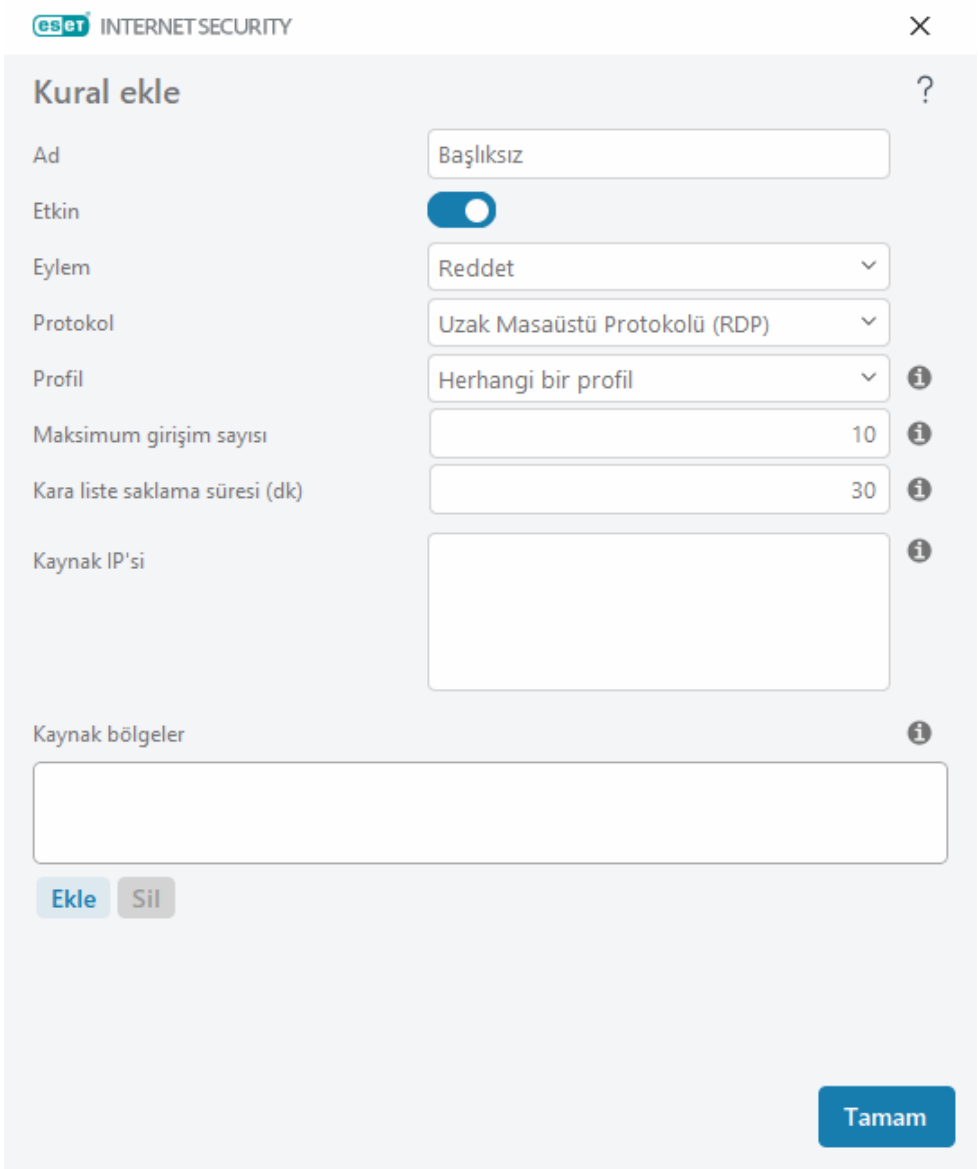
Düzenle – Mevcut bir kuralı düzenleyin.

Sil - Mevcut bir kuralı kurallar listesinden kaldırır.

 **Üst/Yukarı/Aşağı/Alt** - Kuralların öncelik düzeyini ayarlar.

> Mümkün olan en yüksek korumayı sağlamak için en düşük **Maks. deneme** değerine sahip engelleme kuralı uygulanır. Birden çok engelleme kuralı tespit koşullarıyla eşleştiğinde kural Kurallar listesinde daha düşük bir konumda olsa bile bu uygulama geçerli olur.

Kural düzenleyicisi



Ad - Kural adı.

Etkin - Kuralı listede tutmak istiyor ancak uygulamak istemiyorsanız kaydırma çubuğunu devre dışı bırakın.

İşlem - Kural ayarları yerine getirilirse **Reddet** veya **Bağlantıya izin ver** seçeneklerinden birini belirleyin.

Protokol - Bu kuralın inceleyeceği iletişim protokolü.

Profil - Belirli profiller için özel kurallar ayarlanıp uygulanabilir.

Maksimum girişim sayısı - IP adresi engellenene ve kara listeye eklenene kadar saldırı tekrarı girişimlerinin maksimum sayısı.

Kara listede kalma süresi (dk.) - Kara listede adres süresinin dolma zamanını ayarlar.

Kaynak IP'si - IP adresleri, aralıklar veya alt ağların listesi. Birden çok adres virgülle ayrılmalıdır.

Kaynak bölgeler - **Ekle**'yi tıklayarak burada IP adresleri aralığıyla önceden tanımlı veya oluşturulan bir bölge eklemenize olanak sağlar.

IDS kuralları

Bazı durumlarda, Yetkisiz Giriş Algılama Hizmeti (IDS), yönlendiriciler veya diğer dahili ağ cihazları arasındaki iletişimi potansiyel saldırı olarak algılayabilir. Örneğin, IDS'nin kapsamı dışında kalmak için güvenli olduğu bilinen adresleri IDS alanı dışında tutulan Adreslere ekleyebilirsiniz.

> **Resimli talimatlar**
> Aşağıdaki ESET Bilgi Bankası makaleleri sadece İngilizce dilinde mevcuttur:
> - ESET Internet Security ürününde bir IP adresini IDS'den hariç tut

Sütunlar

- **Tespit** - Tespit türü.

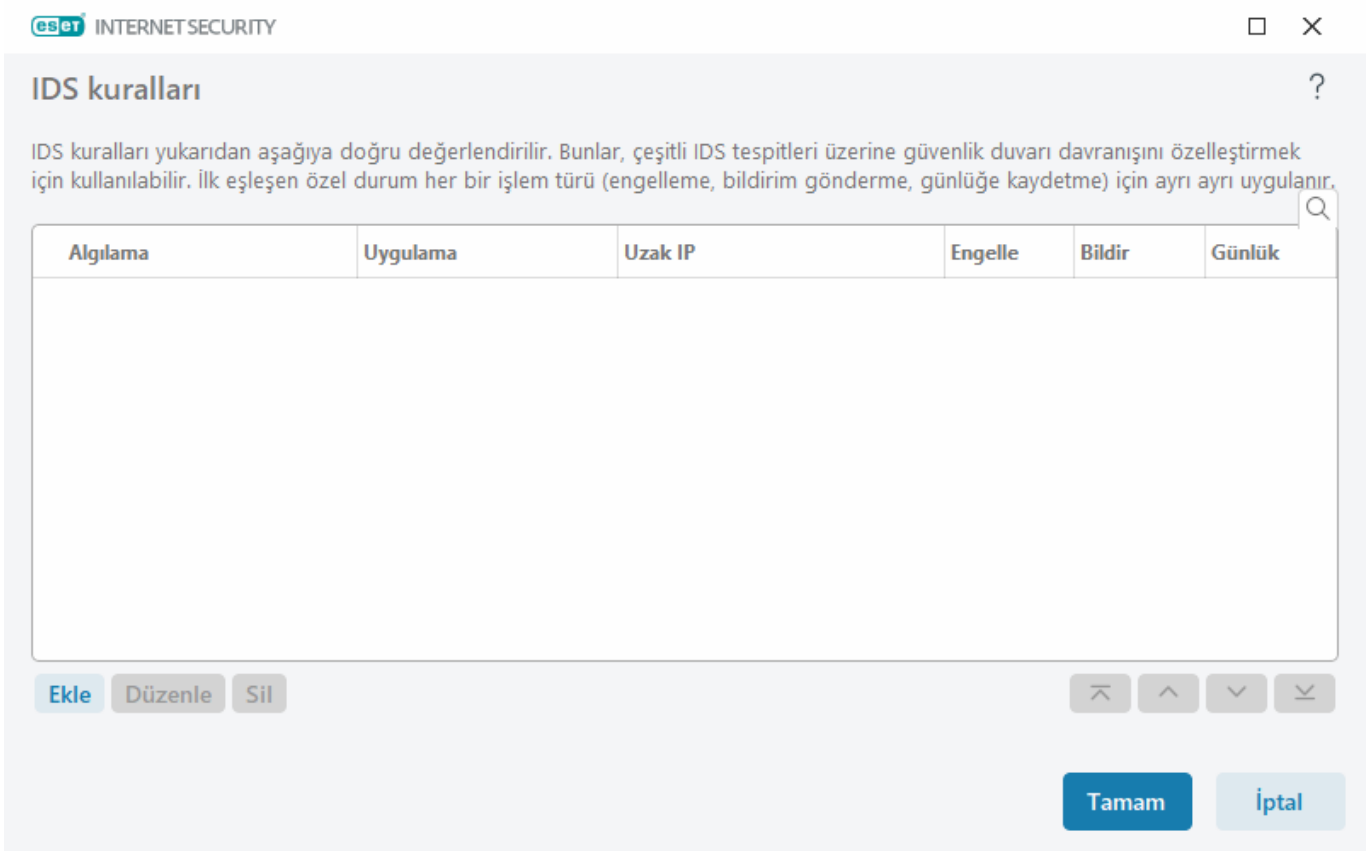
- **Uygulama** – ... öğesini tıklayarak beklenen bir uygulamanın dosya yolunu seçin (örneğin C:\Program Files\Firefox\Firefox.exe). Uygulamanın adını GİRMEYİN.

- **Uzak IP** – Uzak IPv4 veya IPv6 adreslerinin / aralıklarının / alt ağların listesi. Birden çok adres virgülle ayrılmalıdır.

- **Engelle** – Her sistem işlemi kendi varsayılan davranışına ve atanan eyleme (engelle veya izin ver) sahiptir. ESET Internet Security için varsayılan davranışı geçersiz kılmak amacıyla açılır menüyü kullanarak engellemeyi veya izin vermeyi seçebilirsiniz.

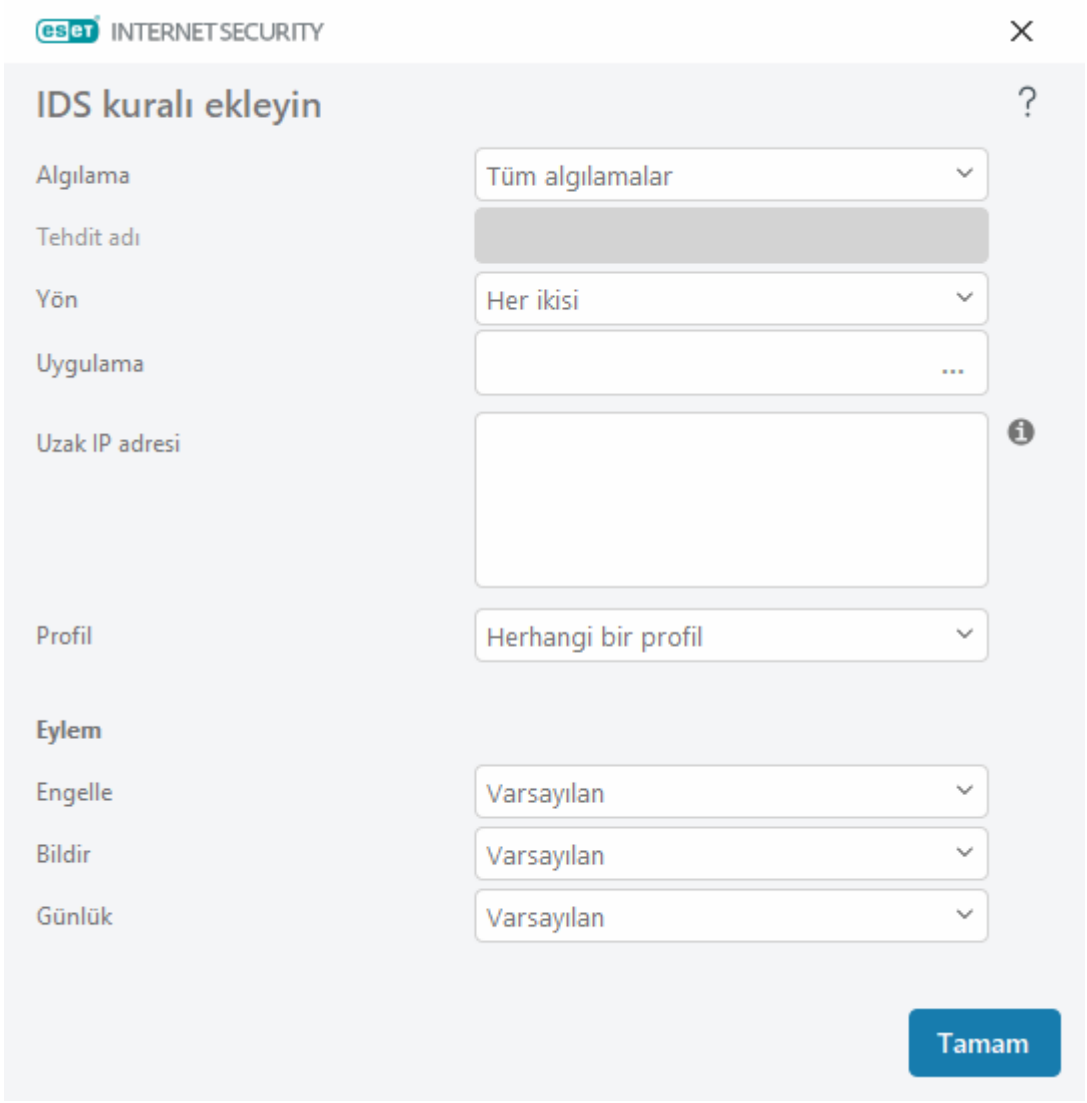
- **Bildir** – Bilgisayarınızda Masaüstü bildirimlerinin gösterilip gösterilmeyeceğini seçin. **Varsayılan**/**Evet**/**Hayır** değerlerinden birini seçin.

- **Günlüğe kaydet** – ESET Internet Security günlük dosyalarına olayları kaydeder. **Varsayılan**/**Evet**/**Hayır** değerlerinden birini seçin.



IDS kurallarını yönetme

- **Ekle** – Yeni bir IDS kuralı oluşturmak için tıklayın.
- **Düzenle** – Mevcut IDS kuralını düzenlemek için tıklayın.
- **Sil** - Bir kuralı, IDS kuralları listesinden kaldırmak istiyorsanız seçin ve tıklayın.
- **Üst/Yukarı/Aşağı/Alt** - Kuralların öncelik düzeyini ayarlamanıza olanak tanır (kurallar yukarıdan aşağı değerlendirilir).



Bir bildirim göstermek ve olay gerçekleştiğinde günlük kaydı oluşturmak isterseniz:
1.Yeni bir IDS kuralı eklemek için **Ekle**'yi tıklayın.
2.**Tespit** açılır menüsünden ilgili tespiti seçin.
3.Bu bildirimin uygulanmasını istediğiniz uygulama yolunu seçmek için **...** simgesini tıklayın.
4.**Varsayılan** değerini (**Engelle** açılır menüsünde) olduğu gibi bırakın. Böylece, ESET Internet Security tarafından uygulanan varsayılan eylem devralınır.
5.**Bildir** ve **Günlük** açılır menülerinin ikisini de **Evet** olarak ayarlayın.
6.Bu bildirimi kaydetmek için **Tamam**'ı tıklayın.

Belirli bir tür **Tespit**'nın tehdit olmadığını düşünüyor ve yinelenen bildirimler gösterilmesini istemiyorsanız:
1.Yeni bir IDS kuralı eklemek için **Ekle**'yi tıklayın.
2.**Tespit** açılır menüsünden belirli tespiti seçin, örneğin **güvenlik uzantıları olmayan SMB oturumu TCP Bağlantı Noktası Tarama saldırısı**.
3.Gelen bir iletişime aitse yönlendirme açılır menüsünden **Gelen**'i seçin.
4.**Bildir** açılır menüsünü **Hayır** olarak ayarlayın.
5.**Günlük** açılır menüsünü **Evet** olarak ayarlayın.
6.**Uygulama**'yı boş bırakın.
7.İletişim belirli bir IP adresinden gelmiyorsa **Uzak IP adreslerini** boş bırakın.
8.Bu bildirimi kaydetmek için **Tamam**'ı tıklayın.

Şüpheli tehdit engellendi

Bu durum, bilgisayarınızdaki uygulamanın bir güvenlik boşluğundan faydalanarak ağdaki başka bir cihaza kötü amaçlı trafik aktarmaya çalışması veya sisteminizde bağlantı noktası tarama girişiminin tespit edilmesi durumunda ortaya çıkabilir.

Tehdit – Tehdidin adı.

Uzak adres - Uzak IP adresi.

İzin ver - Her bir işlem türü için (engelleme, bildirme, günlüğe kaydetme) önceden tanımlı bir işlem olmaksızın Yetkisiz Giriş Tespit Hizmeti (IDS) kuralı oluşturur.

Engellemeye devam et - Algılanan tehdidi engeller. Bu tehdit için IDS kuralı oluşturmak amacıyla **Beni tekrar bilgilendirme** onay kutusunu işaretleyin; bunun üzerine kural herhangi bir bildirim ve günlük kaydı olmaksızın eklenir.

> Bu bildirim penceresinde gösterilen bilgiler, algılanan tehdidin türüne bağlı olarak değişiklik gösterebilir. Tehditler ve diğer ilgili terimler hakkında daha fazla bilgi için lütfen Uzaktan saldırı türleri veya Algılama türleri'ne bakın.
> **Ağda yinelenen IP adresleri yineleniyor** olayını çözümlemek için ESET Bilgi Bankası makalemize bakın.

Ağ koruması sorunlarını giderme

Sorun giderme sihirbazı ESET Güvenlik duvarından kaynaklanan bağlantı sorunlarını çözmenize yardımcı olur. Açılır menüden iletişim engellendiği süreyi seçin. Yakın zamanda engellenen iletişimler listesi; uygulama veya aygıtın türü, söz konusu süre boyunca engellenen uygulama ve aygıtların bilinirliği ve toplam sayısı hakkında size genel bakış sunar. Engellenen iletişim hakkında daha fazla bilgi için **Ayrıntılar**'ı tıklatın. Sonraki adım, bağlantı sorunları yaşadığınız uygulama veya aygıtın engellemesini kaldırmaktır.

Engellemeyi kaldır seçeneğini tıklattığınızda daha önce engellenmiş olan iletişime izin verilir. Bir uygulamayla ilgili sorun yaşamaya devam ederseniz veya aygıtınız beklendiği şekilde çalışmazsa **Uygulama hala çalışmıyor** seçeneğini tıklatın; böylece söz konusu aygıt için daha önce engellenen tüm iletişimlere artık izin verilir. Sorun devam ederse bilgisayarı yeniden başlatın.

Sihirbaz tarafından oluşturulan kuralları görmek için **Değişiklikleri göster**'i tıklayın. Ayrıca sihirbaz tarafından oluşturulan kuralları şuradan da görebilirsiniz: **Gelişmiş ayarlar** > **Ağ koruması** >**Güvenlik duvarı** > **Gelişmiş** > **Kurallar**.

Farklı bir aygıt veya uygulama ile ilgili iletişim sorunlarını gidermek için **Başka birinin engellemesini kaldır** seçeneğini tıklatın.

İzin verilen hizmetler ve gelişmiş seçenekler

Güvenlik Duvarı ve Ağ saldırısına karşı koruma bölümlerindeki gelişmiş seçenekler, Güvenilir bölgeden bilgisayarınızda çalışan hizmetlerden bazılarına erişimi yapılandırmanıza olanak sağlar.

Bilgisayarınıza zarar verebilecek çeşitli saldırı ve güvenlik açığı türlerinin tespit edilmesini etkinleştirebilirsiniz veya devre dışı bırakabilirsiniz.

Bazı durumlarda, engellenen iletişimlerle ilgili tehdit bildirimi almazsınız. Güvenlik duvarı günlüğünde engellenen tüm iletişimleri görüntülemeye ilişkin talimatlar için Günlüğe kaydetme ve günlükten kurallar ve özel durumlar oluşturma bağlantısına başvurun.

Bu penceredeki belirli seçeneklerin kullanılabilirliği, ESET ürününüzün türüne veya sürümüne ve Güvenlik duvarı modülünün yanı sıra işletim sisteminizin sürümüne bağlı olarak değişiklik gösterebilir.

İzin verilen hizmetler

Bu gruptaki ayarlar, güvenilen bölgeden bu bilgisayarın hizmetlerine erişimin yapılandırılmasını kolaylaştırmaya yöneliktir. Bu ayarların birçoğu önceden tanımlı güvenlik duvarı kurallarını etkinleştirir/devre dışı bırakır. İzin verilen hizmetleri **Gelişmiş ayarlar** (F5) > **Ağ koruması** > **Güvenlik Duvarı** > **Gelişmiş** > **İzin verilen hizmetler** bölümünde düzenleyebilirsiniz.

- **Güvenilen bölgede dosya ve yazıcı paylaşımına izin ver** – Güvenilen bölgede uzak bilgisayarların paylaşılan dosya ve yazıcılarınıza erişmesine izin verir.

- **Güvenilir bölgede sistem hizmetleri için UPNP'ye izin ver** – Sistem hizmetleri için UPnP protokollerinin gelen ve giden isteklerine izin verir. UPnP (Microsoft Network Discovery olarak da bilinen Evrensel Tak ve Kullan) Windows Vista'da ve sonraki işletim sistemlerinde kullanılır.

- **Güvenilen bölgede gelen RPC iletişimine izin ver** – Güvenilir bölgeden gelen TCP bağlantılarını etkinleştirir ve Microsoft RPC Portmapper ile RPC/DCOM hizmetlerine erişime izin verir.

- **Güvenilir bölgede uzak masaüstüne izin ver** – Microsoft Uzak Masaüstü Protokolü (RDP) aracılığıyla bağlantıları etkinleştirir ve Güvenilir bölgedeki bilgisayarların RDP kullanan bir programı (örneğin, Uzak Masaüstü Bağlantısı) kullanarak bilgisayarınıza erişmesine izin verir.

- **IGMP İle multicast gruplarında oturum açmayı etkinleştir** – Gelen/giden IGMP ve gelen UDP multicast akışlarına (örneğin, IGMP protokolünü (İnternet Grup Yönetimi Protokolü) kullanan uygulamalar tarafından oluşturulan video akışları) izin verir.

- **Köprülü bağlantılar için iletişime izin ver** – Köprülü bağlantıların sonlandırılmasını önlemek için bu seçeneği kullanın. Köprülü ağ, ana bilgisayarın Ethernet bağdaştırıcısını kullanarak sanal makineyi ağa bağlar. Köprülü ağ kullanıyorsanız sanal makine ağdaki diğer cihazlara erişebilir ve ağdaki fiziksel bir bilgisayarmış gibi bunun tersi de gerçekleşebilir.

- **Güvenilir bölgede sistem hizmetleri için otomatik Web Services Discovery'ye (WSD) izin ver** – Güvenilir bölgeden güvenlik duvarı yoluyla gelen Web Services Discovery isteklerine izin verir. WSD, hizmetlerin yerel bir ağda bulunması için kullanılan protokoldür.

- **Güvenilir bölgede multicast adres çözümlemeye izin ver (LLMNR)** – LLMNR (Yerel Bağlantı Multicast Ad Çözümlemesi) hem IPv4 hem de IPv6 ana bilgisayarlarının, bir DNS sunucusuna veya DNS istemci yapılandırmasına gerek duyulmadan aynı yerel bağlantıdaki ana bilgisayarlar için ad çözümlemelerini gerçekleştirebilmelerini sağlayan, DNS paketi tabanlı bir protokoldür. Bu seçenek, güvenlik duvarı üzerinden Güvenli bölgeden gelen çok noktaya yayın yapan DNS isteklerine izin verir.

- **Windows Ev Grubu desteği** – Windows 7 ve daha sonraki işletim sistemleri için Ev Grubu desteğini etkinleştirir. Ana Grup, bir ev ağı üzerindeki dosya ve yazıcıları paylaşabilir. Bir Ev Grubu'nu yapılandırmak için **Başlat** > **Denetim Masası** > **Ağ ve Internet** > **Ev Grubu** öğelerine gidin.

Yetkisiz giriş algılama

Yetkisiz giriş algılama, kötü amaçlı etkinlik için cihaz ağı iletişimini izler. Bu ayarları **Gelişmiş ayarlar** (F5) > **Ağ koruması** > **Ağ saldırısına karşı koruma** > **Gelişmiş seçenekler** > **Sızıntı tespiti** olarak düzenleyebilirsiniz.

- SMB **Protokolü – SMB** protokolündeki çeşitli güvenlik sorunlarını algılar ve engeller.

- **RPC Protokolü** – Dağıtılmış Bilgi İşlem Ortamı (DCE) için geliştirilen uzaktan prosedür arama sistemindeki çeşitli CVE'leri algılar ve engeller.

- **RDP Protokolü** – RDP protokolündeki çeşitli CVE'leri algılar ve engeller (yukarıya bakın).

- **ARP Zehirleme saldırısı tespiti** - Ortadaki adam (Man-in-the-middle) saldırıları veya ağ anahtarındaki sniffing tespiti tarafından tetiklenen ARP zehirleme saldırılarının algılanmasıdır. ARP (Adres Çözümleme Protokolü), Ethernet adresinin belirlenmesi için ağ uygulaması veya aygıt tarafından kullanılır.

- **TCP/UDP Bağlantı Noktası Tarama saldırısı algılama** – Bağlantı noktası tarama yazılımının (çeşitli bağlantı noktası adreslerine, etkin bağlantı noktaları bulmak ve hizmetin güvenlik açığından yararlanmak amacıyla istemci istekleri göndererek açık bağlantı noktaları için bir ana bilgisayarın incelenmesine yönelik olarak tasarlanmış uygulama) saldırılarını algılar. Bu saldırı türüyle ilgili daha fazla bilgi sözlük'ten edinilebilir.

- **Saldırının algılanmasından sonra güvenli olmayan adresi engelle** – Saldırıların kaynağı olarak algılanan IP adresleri, belirli bir süreliğine bağlantının önlenmesi için Kara Liste'ye eklenir.

- **Saldırı tespitini bildir** - Ekranın sağ alt köşesindeki Windows bildirim alanındaki bildirimi açar.

- **Güvenlik boşluklarına yönelik saldırılar için bildirimleri göster** – Güvenlik boşluklarına yönelik saldırılar algılanırsa veya bir tehdit bu şekilde sisteme girmek için girişimde bulunursa sizi uyarır.

Paket denetleme

Ağ üzerinden aktarılan verileri filtreleyen bir paket analizi türü. Bu ayarları **Gelişmiş ayarlar** (F5) > **Ağ koruması** > **Ağ saldırısına karşı koruma** > **Gelişmiş seçenekler** > **Paket denetleme** bölümünde düzenleyebilirsiniz.

- **SMB Protokolündeki yönetici paylaşımlarına gelen bağlantıya izin ver** - Yönetici paylaşımları, sistem klasörüyle (*ADMIN$*) birlikte sistemde sabit sürücü bölümlerini (*C$*, *D$*, ...) paylaşan varsayılan ağ paylaşımlarıdır. Yönetici paylaşımlarına gelen bağlantının devre dışı bırakılması birçok güvenlik riskini azaltacaktır. Örneğin, Conficker solucanı yönetici paylaşımlarıyla bağlantı kurmak için sözlük saldırılarında bulunur.

- **Eski (desteklenmeyen) SMB lehçelerini reddet** – IDS tarafından desteklenmeyen eski bir SMB lehçesi kullanan SMB oturumlarını reddeder. Modern Windows işletim sistemleri Windows 95 gibi eski işletim sistemleriyle geriye dönük uyumluluk nedeniyle eski SMB diyalektlerini destekler. Saldırgan, trafik denetlemesinden kaçınmak için SMB oturumunda eski bir diyalekti kullanabilir. Bilgisayarınızın, dosyaları eski bir Windows sürümüne sahip bir bilgisayarla paylaşması gerekmiyorsa (veya genellikle SMB iletişimi kullanıyorsa) eski SMB diyalektlerini reddedin.

- **Genişletilmiş güvenlik olmadan SMB oturumlarını reddet** – Genişletilmiş güvenlik, LAN Manager Sınama/Yanıt (LM) kimlik doğrulamasından daha güvenli kimlik doğrulama mekanizması sağlamak için SMB oturumu anlaşması sırasında kullanılabilir. LM şeması zayıf olarak değerlendirilir ve kullanım için önerilmez.

- **SMB Protokolünde Güvenilir bölgenin dışındaki bir sunucuda yürütülebilir dosyaların açılmasını reddet** –

Güvenlik duvarında Güvenilir Bölgeye ait olmayan, sunucuda paylaşılan bir klasördeki yürütülebilir dosyayı (.exe, .dll, ...) açmayı denediğinizde bağlantı kesilir. Yürütülebilir dosyaları güvenilir kaynaklardan kopyalamanın yasal olduğunu unutmayın. Güvenilir kaynaklardan yürütülebilir dosyaları kopyalamak yasal olabilir, ancak bu algılamanın kötü amaçlı bir sunucuda bir dosyanın istenmeyen bir şekilde açılması risklerini azaltması gerektiğini unutmayın (örneğin, paylaşılan kötü amaçlı bir yürütülebilir dosyaya giden köprü tıklatılarak açılan dosya).

- **Güvenilir bölge içindeki/dışındaki bir sunucuya bağlanmak için SMB protokolünde NTLM kimlik doğrulamasını reddet** – NTLM (her iki sürüm) kimlik doğrulama şemalarını kullanan protokoller, kimlik bilgileri iletme saldırısına (SMB protokolü durumunda SMB Geçişi saldırısı olarak bilinen) maruz kalır. Güvenilir bölgenin dışındaki bir sunucuyla olan NTLM kimlik doğrulamasının reddedilmesi, kimlik bilgilerinin Güvenilir bölge dışındaki kötü amaçlı bir sunucu tarafından iletilmesi risklerini azaltacaktır. Aynı şekilde, Güvenilir bölge içindeki sunucularla NTLM kimlik doğrulamasını reddedebilirsiniz.

- **Güvenlik Hesabı Yöneticisi hizmeti ile iletişime izin ver** – Bu hizmet hakkında daha fazla bilgi için [MS-SAMR] bölümüne bakın.

- **Yerel Güvenlik Yetkilisi hizmeti ile iletişime izin ver** – Bu hizmet hakkında daha fazla bilgi için [MS-LSAD] ve [MS-LSAT] bölümüne bakın.

- **Uzak Kayıt Defteri hizmeti ile iletişime izin ver** – Bu hizmet hakkında daha fazla bilgi için [MS-RRP] bölümüne bakın.

- **Hizmet Denetimi Yöneticisi hizmeti ile iletişime izin ver** – Bu hizmet hakkında daha fazla bilgi için [MS-SCMR] bölümüne bakın.

- **Sunucu hizmeti ile iletişime izin ver** – Bu hizmet hakkında daha fazla bilgi için [MS-SRVS] bölümüne bakın.

- **Diğer hizmetlerle iletişime izin ver** – Diğer MSRPC hizmetleri.

Bağlı ağlar

Ağ bağdaştırıcılarının bağlı olduğu ağları gösterir. **Bağlı ağlar** ana menüde, **Ayarlar** > **Ağ koruması** bölümünde bulunabilir. Ağ adının altındaki bağlantıyı tıkladığınızda bağlandığınız ağ için bir koruma türü seçmeniz istenir.

Yapılandırma ağ koruması penceresinden seçebileceğiniz iki ağ koruma modu vardır:

- **Evet** - Güvenilir ağ (ev veya ofis ağı) için. Bilgisayarınız ve bilgisayarınızda depolanan paylaşılan dosyalar diğer ağ kullanıcıları tarafından görülür ve ağdaki diğer kullanıcılar sistem kaynaklarına erişilebilir. Güvenli bir yerel ağa erişirken bu ayarın kullanılması önerilir.

- **Hayır** - Güvenilir olmayan ağ (ortak ağ) için. Sisteminizdeki dosyalar ve klasörler ağdaki diğer kullanıcılarla paylaşılmaz veya bu kullanıcılar tarafından görülmez ve sistem kaynaklarının paylaşımı devre dışı bırakılır. Kablosuz ağlara erişirken bu ayarın kullanılması önerilir.

Aşağıdaki seçeneklerden birini belirlemek için bir ağın yanındaki dişli simgesini tıklayın (güvenilir olmayan ağlar için yalnızca **Ağı Düzenle** seçeneği kullanılabilir):

- **Ağı Düzenle** - Ağ düzenleyicisini açar.

- **Ağı Ağ Denetçisi ile tara** - Ağ taraması çalıştırmak için Ağ Denetçisi'ni açar.

- **"Ağım" olarak işaretle** - Ağa bir Ağım etiketi ekler. Daha iyi tanımlama ve güvenlik genel bakışı için ESET

Internet Security kullanımı boyunca bu etiket ağın yanında gösterilir.

- **"Ağım" işaretini kaldır** - Ağım etiketini kaldırır. Yalnızca ağ zaten etiketlenmişse kullanılabilir.

Her ağ bağdaştırıcısını ve atanmış güvenlik duvarı ile güvenilir bölgesini görüntülemek için **Ağ bağdaştırıcıları**'na tıklayın. Daha ayrıntılı bilgi için Ağ bağdaştırıcıları bölümüne bakın.

Ağ bağdaştırıcıları

Ağ bağdaştırıcıları penceresi ağ bağdaştırıcılarınız hakkında aşağıdaki bilgileri görüntüler:

- Ağ bağdaştırıcısı adı ve bağlantı türü (kablolu, sanal, vb.)
- MAC adresine sahip IP adresi
- Bağlı ağ (Ağım etiketini gösterir)
- Alt ağa sahip güvenilen bölgenin IP adresi
- Aktif profil (Ağ bağdaştırıcılarına atanan profiller bölümüne bakın)

Geçici IP adresi kara listesi

Saldırı kaynakları olduğu algılanan IP adresleri, bağlantının belirli bir süreliğine engellenmesi için kara listeye eklenir. Bu IP adreslerini görmek için ESET Internet Security ürününden **Ayarlar** > **Ağ koruması** > **Geçici IP adresi kara listesi**'ne gidin. Geçici olarak engellenen IP adresleri 1 saat boyunca engellenir.

Sütunlar

IP adresi - Engellenen bir IP adresini gösterir.

Engelleme nedeni – Adresten engellenen saldırı türünü (örneğin, TCP Bağlantı Noktası Tarama saldırısı) gösterir.

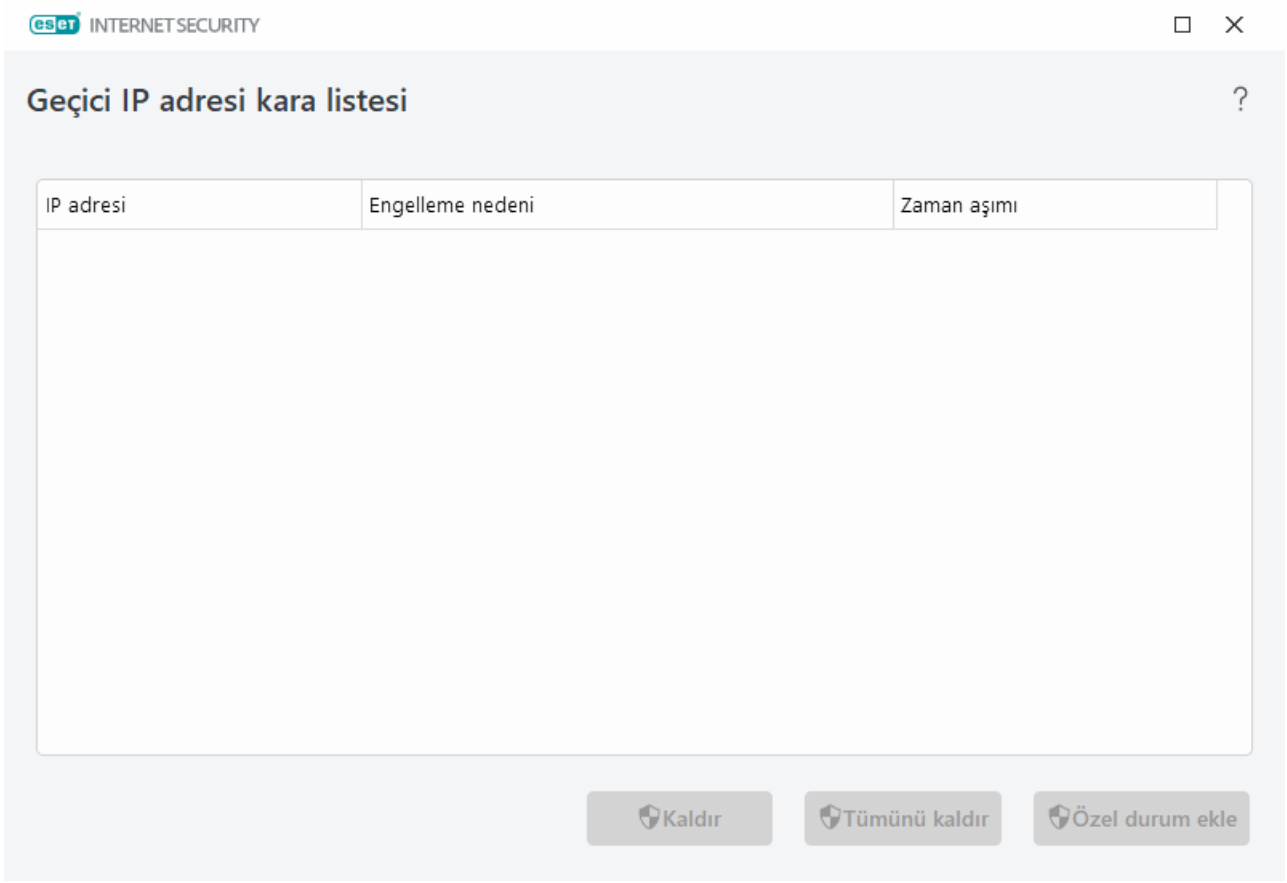
Zaman aşımı – Adresin kara listedeki süresinin dolacağı saati ve tarihi gösterir.

Denetim öğeleri

Kaldır – Kara listeden bir adresi, süresi dolmadan kaldırmak için tıklatın.

Tümünü kaldır – Kara listeden tüm adresleri hemen kaldırmak için tıklatın.

Özel durum ekle - IDS filtrelemesine güvenlik duvarı özel durumu eklemek için tıklatın.



Ağ koruma günlüğü

ESET Internet Security Ağ koruması, tüm önemli olayları ana menüden doğrudan görüntülenebilen bir günlük dosyasına kaydeder. **Araçlar** > **Diğer araçlar** > **Günlük dosyaları**'nı tıklayıp **Günlük** açılır menüsünden **Ağ koruması** seçeneğini belirleyin.

Günlük dosyaları hataları tespit etmek ve sistemdeki sızıntıları ortaya çıkarmak için kullanılabilir. ESET ağ koruma günlükleri aşağıdaki verileri içerir:

- Olay tarihi ve saati
- Olayın adı
- Kaynak
- Hedef ağ adresi
- Ağ iletişimi protokolü
- Uygulanan kural veya tanımlanmışsa solucanın adı
- İlgili uygulama
- Kullanıcı

Bu verilerin tam analizi, sistem güvenliğini tehlikeye atacak girişimlerin algılanmasına yardımcı olabilir. Başka birçok etken olası güvenlik risklerine işaret eder ve bunların etkilerini en aza indirmenize olanak tanır: bilinmeyen konumlardan sıklıkla bağlantı kurulması, birden çok bağlantı kurma girişimi, iletişim kuran bilinmeyen uygulamalar

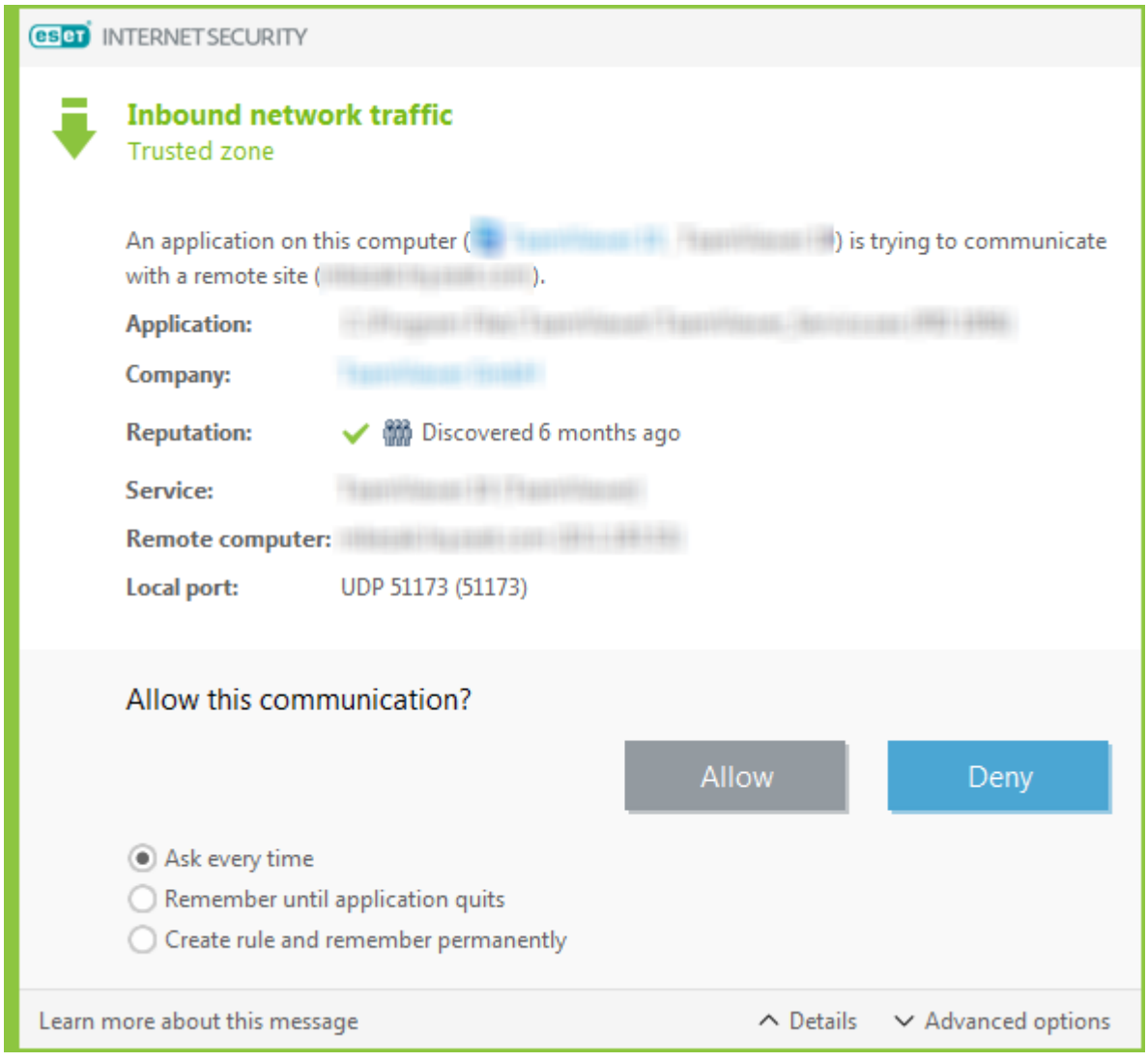
veya olağan dışı bağlantı noktası numaralarının kullanılması.

> **Güvenlik açığını kötüye kullanma**
> Kötüye kullanma girişimi gerçek bir kötüye kullanım işlemine dönüşmeden önce ağ düzeyinde tespit edilip engellendiğinden belirli bir güvenlik açığı zaten yamalı olsa bile güvenlik açığı kötüye kullanımıyla ilgili mesaj günlüğe kaydedilir.

Bağlantı kurma – algılama

Güvenlik duvarı yeni oluşturulan her ağ bağlantısını algılar. Etkin güvenlik duvarı modu yeni kuralda hangi eylemlerin gerçekleştirileceğini belirler. **Otomatik mod** veya **İlke tabanlı mod** etkinse, Güvenlik duvarı, kullanıcı etkileşimi olmadan önceden tanımlı eylemleri gerçekleştirir.

Etkileşimli mod, yeni ağ bağlantısının algılandığını bildiren, bağlantıyla ilgili ayrıntılı bilgilerle desteklenen bir bilgi penceresi görüntüler. Bağlantıya **İzin vermeyi** veya **Reddetmeyi** (engellemeyi) seçebilirsiniz. İletişim penceresinde aynı bağlantıya sürekli izin veriyorsanız, bağlantı için yeni bir kural oluşturmanızı öneririz. **Kuralı oluştur ve sürekli olarak hatırla** seçeneğini belirleyip eylemi Güvenlik duvarı için yeni kural olarak kaydedin. Güvenlik duvarı daha sonra aynı bağlantıyı tanıdığında kullanıcı etkileşimi gerektirmeden varolan kuralı uygular.



Yeni kural oluştururken yalnızca güvenli olduğunu bildiğiniz bağlantılara izin verin. Tüm bağlantılara izin verilirse, güvenlik duvarı amacını yerine getirmekte başarısız olur. Şunlar, bağlantılar için önemli parametrelerdir:

Uygulama - Yürütülebilir dosya konumu ve işlem kimliği. Bilinmeyen uygulama ve işlemler için bağlantılara izin vermeyin.

Şirket - Uygulamanın yayımcı adı. Şirket için bir güvenlik sertifikası göstermek üzere metni tıklayın.

Bilinirlik - Bağlantının risk düzeyi. Bağlantılara bir risk düzeyi atanır: Her bir bağlantının özelliklerini, kullanıcı sayısını ve keşif zamanlarını inceleyen bir dizi buluşsal kural kullanarak şu düzeylerden biri seçilir: İyi (yeşil), Bilinmeyen (turuncu) veya Riskli (kırmızı). Bu bilgiler ESET LiveGrid® teknolojisiyle toplanır.

Hizmet - Uygulama bir Windows hizmeti ise hizmetin adı.

Uzak bilgisayar - Uzak cihazın adresi. Yalnızca güvenilir ve bilinen adreslere bağlanmaya izin verin.

Uzak bağlantı noktası - İletişim bağlantı noktası. Genel bağlantı noktaları (ör., web trafiği, bağlantı noktası numarası 80.443) üzerindeki iletişime normal şartlarda izin verilebilir.

Bilgisayar sızıntıları sıkça uzak sistemlere yayılmaya yardımcı olmaları için Internet'i ve gizli bağlantıları kullanır. Kurallar doğru yapılandırılmışsa, Güvenlik duvarı çeşitli kötü amaçlı kod saldırılarına karşı korunmak için yararlı bir araca dönüşür.

ESET Güvenlik duvarı ile sorunları çözme

ESET Internet Security yüklüyken bağlantı sorunları yaşarsanız ESET Güvenlik Duvarı'nın bu soruna neden olup olmadığını belirlemenin çeşitli yolları vardır. Ayrıca ESET Güvenlik Duvarı bağlantı sorunlarını çözmek için yeni kurallar veya özel durumlar oluşturmanıza yardımcı olabilir.

ESET Güvenlik duvarı ile ilgili sorunları çözmeye yardımcı olması için aşağıdaki konulara bakın:

- Sorun giderme sihirbazı
- Günlüğe kaydetme ve günlükten kurallar ve özel durumlar oluşturma
- Güvenlik duvarı bildirimlerinden özel durumlar oluşturma
- Ağ koruması gelişmiş günlük kaydını
- Protokol filtreleme ile sorunları çözme

Sorun giderme sihirbazı

Sorun giderme sihirbazı; tüm engellenen bağlantıları sessizce izler ve belirli uygulamalar veya aygıtlar ile ilgili güvenlik duvarı sorunlarını düzeltmek üzere sorun giderme işlemi uygulamanız sırasında sizi yönlendirir. Ardından sihirbaz, onaylamanız durumunda uygulanacak yeni bir kural kümesi önerir. **Sorun giderme sihirbazı**, **Ayarlar** > **Ağ koruması** altındaki ana menüde bulunabilir.

Günlüğe kaydetme ve günlükten kurallar ve özel

durumlar oluşturma

Varsayılan olarak, ESET Güvenlik Duvarı tüm engellenen bağlantıları günlüğe kaydetmez. Ağ koruması tarafından nelerin engellendiğini görmek istiyorsanız **Araçlar** altındaki **Gelişmiş ayarlar** > **Tanılama** > **Gelişmiş günlük kaydı** > **Ağ koruması gelişmiş günlük kaydını etkinleştir**'de günlüğe kaydetmeyi etkinleştirin. Günlükte, Güvenlik duvarının engellemesini istemediğiniz şeyler görürseniz söz konusu öğeyi sağ tıklayarak ve **Gelecekte benzer olayları engelleme** seçeneğini işaretleyerek bunun için bir kural veya IDS kuralı oluşturabilirsiniz. Tüm engellenen bağlantılar günlüğünün binlerce öğe içerebileceğini ve bu günlükte belirli bir bağlantıyı bulmanın zor olabileceğini lütfen unutmayın. Sorununuzu çözdükten sonra günlüğe kaydetmeyi kapatabilirsiniz.

Günlük hakkında daha fazla bilgi için bkz. Günlük dosyaları.

> Ağ korumasının belirli bağlantıları engellediği sırayı görmek için günlük kaydını kullanın. Ayrıca günlükten kural oluşturma, tam olarak istediğinizi yapan kurallar oluşturmanıza olanak tanır.

Günlükten kural oluşturma

ESET Internet Security Ürününün yeni sürümü günlükten bir kural oluşturmanıza olanak tanır. Ana menüden **Araçlar** > **Diğer araçlar** > **Günlük dosyaları** seçeneğini tıklatın. Açılır menüden **Güvenlik duvarı** öğesini seçin, istediğiniz günlük girişini sağ tıklatın ve içerik menüsünden **Gelecekte benzer olayları engelleme** öğesini seçin. Yeni kuralınızı görüntüleyen bir bildirim penceresi açılır.

Günlükten yeni kurallar oluşturmaya izin vermek için, ESET Internet Security aşağıdaki ayarlarla yapılandırılmalıdır:

1. Minimum günlük ayrıntı düzeyini **Gelişmiş ayarlar** (F5) > **Araçlar** > **Günlük dosyaları** içinden **Tanılama** olarak ayarlayın.

2. **Gelişmiş ayarlar** (F5) > **Ağ koruması** > **Ağ saldırısına karşı koruma** > **Gelişmiş seçenekler** > **Yetkisiz giriş algılama** içinde **Güvenlik boşluklarına karşı gelen saldırılar için de bildirim göster** seçeneğini etkinleştirin.

Güvenlik duvarı bildirimlerinden özel durumlar oluşturma

ESET Güvenlik duvarı kötü amaçlı ağ etkinliği algıladığında olayı açıklayan bir bildirim penceresi görüntülenir. Bu bildirim, olay hakkında daha fazla bilgi edinebilmenizi ve isterseniz bu olay için kural ayarlayabilmenizi sağlayacak bir bağlantı içerir.

> Bir ağ uygulaması veya aygıt ağ standartlarını doğru şekilde uygulamazsa tekrarlanan güvenlik duvarı IDS bildirimlerini tetikleyebilir. ESET Güvenlik duvarının bu uygulamayı veya aygıtı algılamasını engellemek için doğrudan bir özel durum oluşturabilirsiniz.

Ağ koruması gelişmiş günlük kaydını

Bu özellik ESET Teknik Destek birimine daha karmaşık günlük dosyalarını sağlamayı amaçlar. Büyük bir günlük dosyası oluşturabileceğinden ve bilgisayarınızı yavaşlatabileceğinden bu özelliği yalnızca ESET Teknik destek ekibi tarafından istendiğinde kullanın.

1. **Gelişmiş ayarlar** > **Araçlar** > **Tanılama**'ya giderek **Ağ koruması gelişmiş günlük kaydını etkinleştir** seçeneğini etkinleştirin.

2. Karşılaştığınız sorunu yeniden üretmeye çalışın.

3. Ağ koruması gelişmiş günlük kaydını devre dışı bırakın.

4. Ağ koruması gelişmiş günlük kaydı tarafından oluşturulan PCAP günlük dosyası, tanılama bellek dökümlerinin oluşturulduğu dizinde bulunabilir: *C:\ProgramData\ESET\ESET Security\Diagnostics*

Protokol filtreleme ile sorunları çözme

Tarayıcınız veya e-posta istemciniz ile ilgili sorun yaşıyorsanız ilk adım bu sorunun protokol filtrelemeden kaynaklanıp kaynaklanmadığını belirlemektir. Bunu yapmak için gelişmiş ayarlar içinden uygulama protokolü filtrelemeyi geçici olarak devre dışı bırakmayı deneyin (işiniz bittikten sonra tekrar açmayı unutmayın, aksi takdirde tarayıcınız ve e-posta istemciniz korunmasız kalır). Sorun, devre dışı bıraktıktan sonra ortadan kalkarsa burada genel sorunların bir listesini ve bunları çözmenin yollarını bulabilirsiniz:

Güncelleme veya iletişim güvenliği sorunları

Uygulamanızla ilgili güncelleyememe veya iletişim kanalının güvenli olmaması gibi sorunlar meydana geliyorsa:

- SSL protokol filtreleme etkinse geçici olarak kapatmayı deneyin. Bu işe yararsa, SSL filtrelemeyi kullanmaya devam edebilirsiniz ve sorunlu iletişimi dışarıda bırakarak güncelleme işini yapabilirsiniz:
SSL protokol filtreleme modunu etkileşimli olarak değiştirin. Güncellemeyi yeniden çalıştırın. Şifreli ağ trafiği hakkında size bilgi veren bir iletişim kutusu açılmalıdır. Uygulamanın sorun gidermekte olduğunuz uygulama olduğundan ve sertifikanın güncellenen sunucudan geliyor gibi göründüğünden emin olun. Ardından bu sertifika için eylemin hatırlanmasını seçin ve yoksay seçeneğini tıklatın. İlgili başka iletişim penceresi görünmezse filtreleme modunu tekrar otomatik hale getirin. Bu sayede sorun çözülmüş olmalıdır.

- Söz konusu uygulama bir tarayıcı veya e-posta istemcisi değilse tamamen protokol filtrelemenin dışında bırakabilirsiniz (bunu tarayıcı veya e-posta istemcisi için yapmak korunmasız kalmanıza neden olur). Daha önce filtrelenen iletişime sahip bir uygulama, özel durum eklerken listede yer alıyor olmalıdır, bu nedenle el ile eklemeniz gerekmez.

Ağınızdaki aygıta erişim sorunu

Ağınızdaki bir cihazın herhangi bir işlevselliğinden yararlanamıyorsanız (örneğin, web kameranızın web sayfasını açma veya ev ortam yürütücüsünde video oynatma gibi), hariç bırakılan adresler listesine cihazın IPv4 ve IPv6 adreslerini eklemeyi deneyin.

Belirli bir web sitesi ile ilgili sorunlar

URL adres yönetimini kullanarak belirli web sitelerini protokol filtreleme dışında bırakabilirsiniz. Örneğin https://www.gmail.com/intl/en/mail/help/about.html adresine erişemiyorsanız, dışarıda bırakılan adresler listesine *gmail.com* adresini eklemeyi deneyin.

"Kök sertifikasını içe aktarabilen bazı uygulamalar çalışmaya devam ediyor" hatası.

SSL protokol filtrelemeyi etkinleştirdiğinizde ESET Internet Security; yüklenen uygulamaların sertifika depolarına sertifikayı alarak SSL protokolünü filtrelediğinden emin olmanızı sağlar. Bazı uygulamalar, bir sertifikayı içe aktarması için yeniden başlatma işlemi gerektirebilir. Buna Firefox ve Opera dahildir. Bunlardan hiçbirinin çalışmadığından emin olun (bunu yapmanın en iyi yolu Görev Yöneticisi'ni açıp İşlemler sekmesinde firefox.exe veya opera.exe uygulamalarının yer almadığından emin olmaktır), ardından tekrar deneyin.

Güvenilir olmayan sağlayıcı veya geçersiz imza ile ilgili hata

Bu genellikle yukarıda belirtilen alma işleminin başarısız olması anlamına gelir. Öncelikle yukarıda belirtilen uygulamaların herhangi birinin çalışmadığından emin olun. Ardından SSL protokol filtrelemeyi devre dışı bırakın ve tekrar etkinleştirin. Bu, almayı yeniden çalıştırır.

ESET Windows ev ürününde Protokol/SSL/TLS filtrelemesini yönetme ile ilgili bilgi edinmek için Bilgi Bankası makalesine bakın.

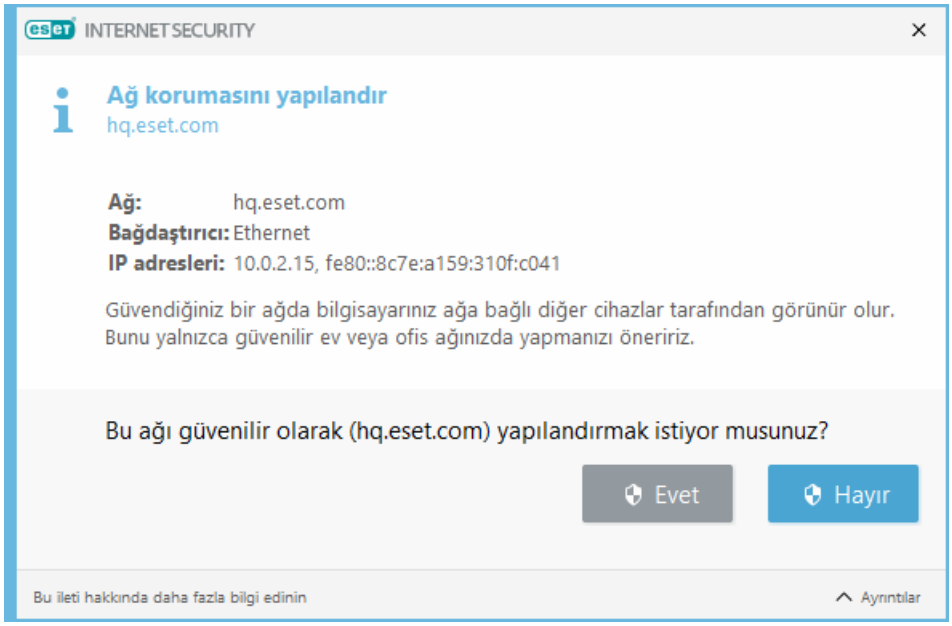
Yeni ağ algılandı

ESET Internet Security varsayılan olarak, yeni bir ağ tespit edildiğinde Windows ayarlarını kullanır. Yeni bir ağ tespit edildiğinde iletişim penceresi görüntülemek için kullanıcıya sormak üzere Bilinen ağlar'da yeni ağların koruma türünü değiştirin. Ardından, yeni bir ağa bağlantı tespit edilirse kullanıcı koruma düzeyini seçin. Bu ayar, ilgili ağdan tüm uzak bilgisayarlara yapılan bağlantılar için geçerli olacaktır.

Yapılandırma ağ koruması penceresinden seçebileceğiniz iki ağ koruma modu vardır:

- **Evet** - Güvenilir ağ (ev veya ofis ağı) için. Bilgisayarınız ve bilgisayarınızda depolanan paylaşılan dosyalar diğer ağ kullanıcıları tarafından görülür ve ağdaki diğer kullanıcılar sistem kaynaklarına erişilebilir. Güvenli bir yerel ağa erişirken bu ayarın kullanılması önerilir.

- **Hayır** - Güvenilir olmayan ağ (ortak ağ) için. Sisteminizdeki dosyalar ve klasörler ağdaki diğer kullanıcılarla paylaşılmaz veya bu kullanıcılar tarafından görülmez ve sistem kaynaklarının paylaşımı devre dışı bırakılır. Kablosuz ağlara erişirken bu ayarın kullanılması önerilir.



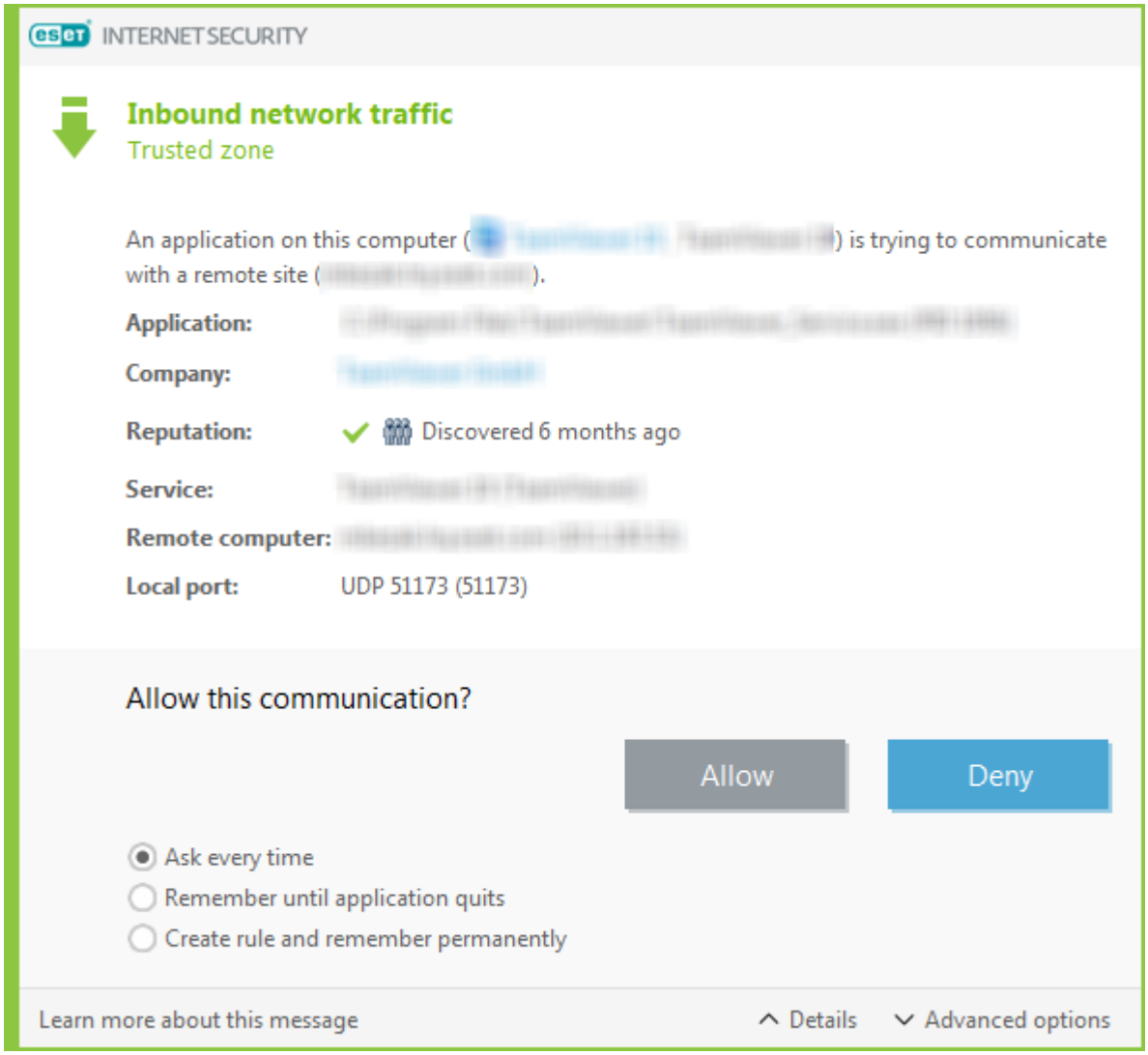
Ağ güvenilir olarak ayarlanırsa doğrudan bağlanan alt ağların otomatik olarak güvenilir olduğu kabul edilir.

Uygulama değişikliği

Güvenlik duvarı, bilgisayarınızdan giden bağlantılar oluşturmak için kullanılan bir uygulamada değişiklik olduğunu algıladı. Uygulama yalnızca yeni bir sürüme güncellenmiş de olabilir. Ancak diğer yandan, değişiklik kötü amaçlı bir uygulama tarafından da yapılmış olabilir. Herhangi bir yasal değişiklikten haberiniz yoksa, bağlantıyı reddetmenizi ve en yeni virüs imzaları veritabanını kullanarak bilgisayarınızı taramanızı öneririz.

Gelen güvenilen iletişim

Güvenilen bölge içinde gelen bağlantı örneği:
Bilgisayarınızda çalıştırılan yerel uygulamayla iletişim kurmaya çalışan, güvenilen bölgedeki bir uzak bilgisayar.



Uygulama – Uzak bilgisayarın iletişim kurduğu uygulama.

Şirket – Uygulamanın yayımcısı.

Bilinirlik – Uygulamanın, ESET LiveGrid® teknolojisinden elde edilmiş haliyle bilinirliği.

Servis – Bilgisayarınızda halihazırda çalışmakta olan servisin adı.

Uzak bilgisayar – Bilgisayarınızdaki uygulamayla iletişim kurmaya çalışan uzak bilgisayar.

Uzak bağlantı noktası – İletişim için kullanılan bağlantı noktası.

Her defasında sor – Bir kural için varsayılan eylem **Sor** olarak belirlenmişse kuralın her tetiklenişinde bir iletişim penceresi görüntülenir.

Uygulamadan çıkılana kadar hatırla – ESET Internet Security bir sonraki yeniden başlatma işlemine kadar seçili eylemi hatırlar.

Kural oluştur ve sürekli olarak hatırla – Bir iletişime izin vermeden veya iletişimi reddetmeden önce bu seçeneği belirlerseniz uzak bilgisayar uygulama ile tekrar iletişim kurduğunda ESET Internet Security eylemi anımsar ve kullanır.

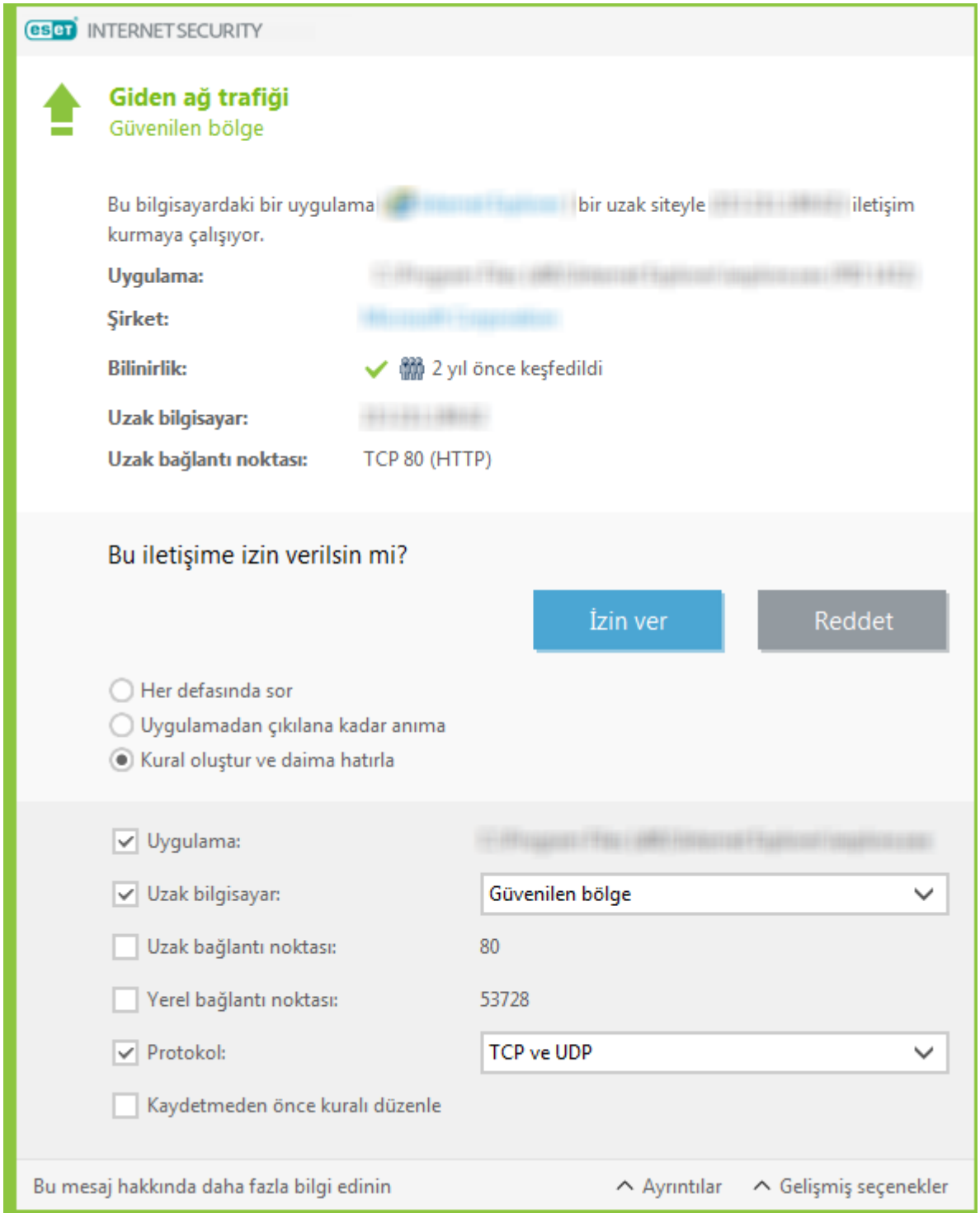
İzin ver – Gelen iletişime izin verir.

Reddet – Gelen iletişimi reddeder.

Gelişmiş seçenekler - Kural özelliklerini özelleştirmenize olanak verir.

Giden güvenilen iletişim

Güvenilen bölge içinde giden bağlantı örneği:
Yerel ağda veya güvenilen bölgedeki bir ağda bulunan başka bir bilgisayarla bağlantı kurmaya çalışan yerel uygulama.



Uygulama – Uzak bilgisayarın iletişim kurduğu uygulama.

Şirket – Uygulamanın yayımcısı.

Bilinirlik – Uygulamanın, ESET LiveGrid® teknolojisinden elde edilmiş haliyle bilinirliği.

Servis – Bilgisayarınızda halihazırda çalışmakta olan servisin adı.

Uzak bilgisayar – Bilgisayarınızdaki uygulamayla iletişim kurmaya çalışan uzak bilgisayar.

Uzak bağlantı noktası – İletişim için kullanılan bağlantı noktası.

Her defasında sor – Bir kural için varsayılan eylem **Sor** olarak belirlenmişse kuralın her tetiklenişinde bir iletişim penceresi görüntülenir.

Uygulamadan çıkılana kadar hatırla – ESET Internet Security bir sonraki yeniden başlatma işlemine kadar seçili eylemi hatırlar.

Kural oluştur ve sürekli olarak hatırla – Bir iletişime izin vermeden veya iletişimi reddetmeden önce bu seçeneği belirlerseniz uzak bilgisayar uygulama ile tekrar iletişim kurduğunda ESET Internet Security eylemi anımsar ve kullanır.

İzin ver – Gelen iletişime izin verir.

Reddet – Gelen iletişimi reddeder.

Gelişmiş seçenekler - Kural özelliklerini özelleştirmenize olanak verir.

Gelen iletişim

Gelen Internet bağlantısı örneği:
Bilgisayarda çalışan bir uygulamayla iletişim kurmaya çalışan uzak bilgisayar.

Uygulama – Uzak bilgisayarın iletişim kurduğu uygulama.

Şirket – Uygulamanın yayımcısı.

Bilinirlik – Uygulamanın, ESET LiveGrid® teknolojisinden elde edilmiş haliyle bilinirliği.

Servis – Bilgisayarınızda halihazırda çalışmakta olan servisin adı.

Uzak bilgisayar – Bilgisayarınızdaki uygulamayla iletişim kurmaya çalışan uzak bilgisayar.

Uzak bağlantı noktası – İletişim için kullanılan bağlantı noktası.

Her defasında sor – Bir kural için varsayılan eylem **Sor** olarak belirlenmişse kuralın her tetiklenişinde bir iletişim penceresi görüntülenir.

Uygulamadan çıkılana kadar hatırla – ESET Internet Security bir sonraki yeniden başlatma işlemine kadar seçili eylemi hatırlar.

Kural oluştur ve sürekli olarak hatırla – Bir iletişime izin vermeden veya iletişimi reddetmeden önce bu seçeneği belirlerseniz uzak bilgisayar uygulama ile tekrar iletişim kurduğunda ESET Internet Security eylemi anımsar ve kullanır.

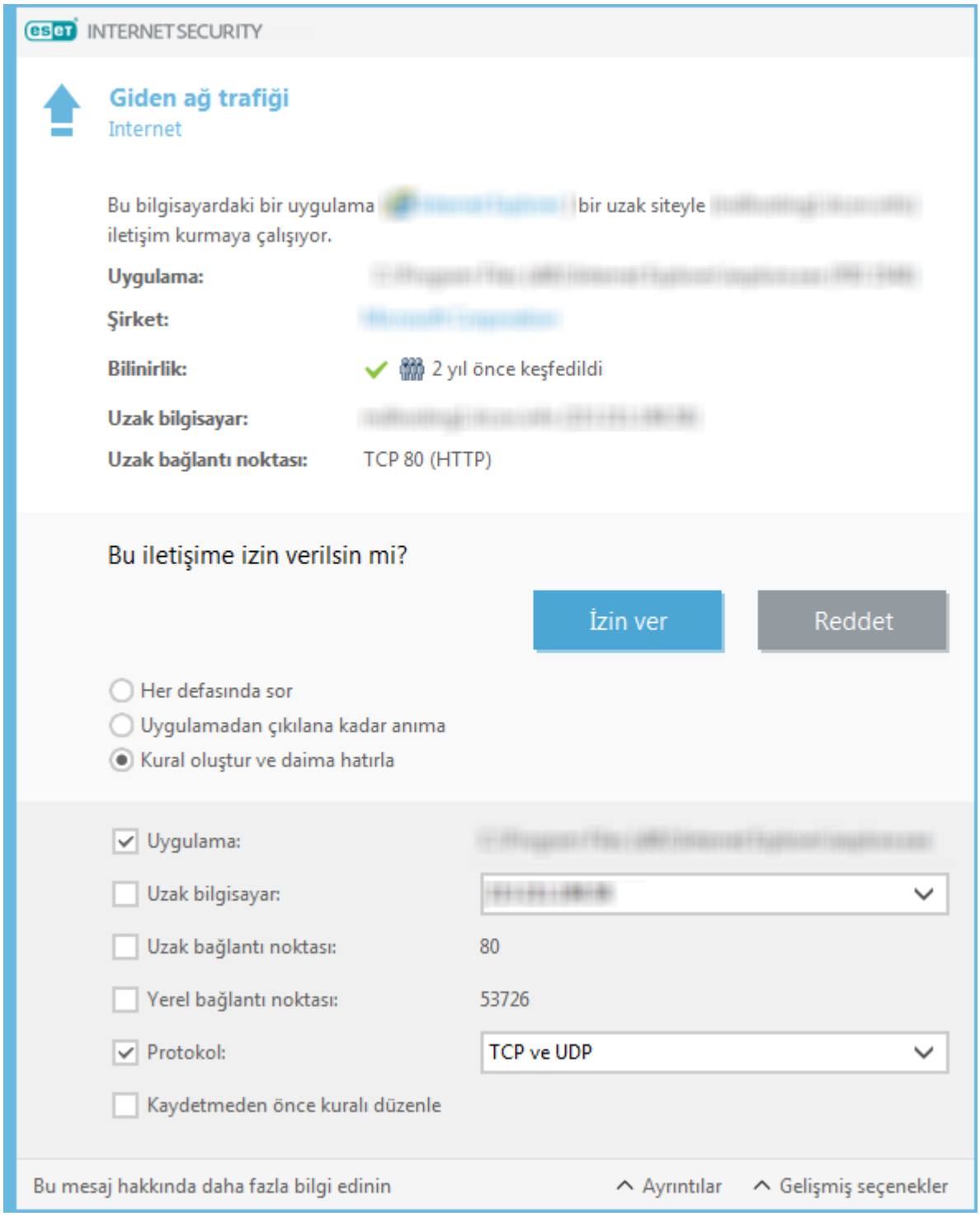
İzin ver – Gelen iletişime izin verir.

Reddet – Gelen iletişimi reddeder.

Gelişmiş seçenekler - Kural özelliklerini özelleştirmenize olanak verir.

Giden iletişim

Giden Internet bağlantısı örneği:
Internet bağlantısı kurmaya çalışan yerel bir uygulama.



Uygulama – Uzak bilgisayarın iletişim kurduğu uygulama.

Şirket – Uygulamanın yayımcısı.

Bilinirlik – Uygulamanın, ESET LiveGrid® teknolojisinden elde edilmiş haliyle bilinirliği.

Servis – Bilgisayarınızda halihazırda çalışmakta olan servisin adı.

Uzak bilgisayar – Bilgisayarınızdaki uygulamayla iletişim kurmaya çalışan uzak bilgisayar.

Uzak bağlantı noktası – İletişim için kullanılan bağlantı noktası.

Her defasında sor – Bir kural için varsayılan eylem **Sor** olarak belirlenmişse kuralın her tetiklenişinde bir iletişim penceresi görüntülenir.

Uygulamadan çıkılana kadar hatırla – ESET Internet Security bir sonraki yeniden başlatma işlemine kadar seçili eylemi hatırlar.

Kural oluştur ve sürekli olarak hatırla – Bir iletişime izin vermeden veya iletişimi reddetmeden önce bu seçeneği belirlerseniz uzak bilgisayar uygulama ile tekrar iletişim kurduğunda ESET Internet Security eylemi anımsar ve kullanır.

İzin ver – Gelen iletişime izin verir.

Reddet – Gelen iletişimi reddeder.

Gelişmiş seçenekler - Kural özelliklerini özelleştirmenize olanak verir.

Bağlantı görünüm ayarları

Dahil olan ek seçenekleri görüntülemek için bağlantının üzerini sağ tıklatın:

Ana bilgisayar adlarını çözümle – Mümkünse tüm ağ adresleri, sayısal IP adresi biçiminde değil DNS biçiminde görüntülenir.

Yalnızca TCP bağlantılarını göster – Listede yalnızca TCP protokol paketine ait olan bağlantılar görüntülenir.

Dinleyen bağlantıları göster – Bu seçeneği yalnızca herhangi bir iletişimin kurulmadığı, ancak sistemin bir bağlantı noktası açtığı ve bağlantı kurmayı beklediği türden bağlantıları görüntülemek için belirleyin.

Bilgisayardaki bağlantıları göster – Bu seçeneği yalnızca uzak tarafın yerel sistem olduğu ve bu nedenle localhost olarak adlandırılan bağlantıları görüntülemek için belirleyin.

Yenileme hızı – Etkin bağlantıları yenileme sıklığını seçin.

Şimdi yenile – **Ağ bağlantıları** penceresini yeniden yükler.

Güvenlik araçları

Güvenlik araçları ayarları, aşağıdaki modülleri ayarlamanıza olanak sağlar:

- **Bankacılık ve Ödeme Sistemleri Koruması** - Çevrim içi işlemler sırasında finansal verilerinizi korumak için tasarlanmış ek bir tarayıcı koruması katmanı sunar. Desteklenen tüm web tarayıcılarını güvenli modda

başlatmak için **Tüm tarayıcıları güvenli hale getir**'i etkinleştirin. Daha fazla bilgi için Bankacılık ve Ödeme Sistemleri Koruması'na bakın.

- **Anti-Theft** - Kayıp veya hırsızlık durumunda bilgisayarınızı korumak için Anti-Theft özelliğini etkinleştirin.

Bankacılık ve Ödeme Sistemleri Koruması

Bankacılık ve Ödeme koruması, çevrimiçi işlemleriniz sırasında finansal verilerini korumak için tasarlanan ek bir koruma katmanıdır.

Varsayılan olarak, desteklenen tüm web tarayıcıları güvenli modda başlatılır. Bu, internette gezinmenize, internet bankacılığına erişmenize ve yeniden yönlendirme olmadan tek bir güvenli tarayıcı penceresinde çevrim içi satın alma ve parasal işlemlerini yapmanıza olanak sağlar.

ESET LiveGrid® bilinirlik sistemi, Bankacılık ve Ödeme Sistemleri korumasının düzgün şekilde çalışması için etkinleştirilmelidir (varsayılan olarak etkindir).

Aşağıdaki güvenli tarayıcı davranışı yapılandırma seçeneklerinden birini belirleyin:

- **Tüm tarayıcıların güvenliğini sağla** - Varsayılan olarak, desteklenen tüm web tarayıcıları güvenli modda başlatılır. Bu, internette gezinmenize, internet bankacılığına erişmenize ve yeniden yönlendirme olmadan tek bir güvenli tarayıcı penceresinde çevrim içi satın alma ve parasal işlemlerini yapmanıza olanak sağlar.

- **Web sitelerinin yeniden yönlendirilmesi** - Korunan web siteleri listesinde yer alan web siteleri ve dahili internet bankacılığı listesi güvenli tarayıcıya yönlendirilir. Hangi tarayıcının (standart veya güvenli) açılacağını seçebilirsiniz.

Web sitelerinin yeniden yönlendirilmesi, ARM işlemcilerine sahip cihazlarda kullanılamaz.

- Önceki iki seçenek de devre dışı bırakıldı - Güvenli tarayıcıya erişmek için ESET Internet Security ürününde **Araçlar** > **Bankacılık ve Ödeme Sistemleri Koruması**'nı tıklayın veya **Bankacılık ve Ödeme Sistemleri Koruması** masaüstü simgesini tıklayın. Windows işletim sisteminde varsayılan olarak ayarlanmış tarayıcı güvenli modda açılır.

Güvenli tarayıcı davranışını yapılandırmak için Bankacılık ve Ödeme Sistemleri Koruması gelişmiş ayarları'na bakın. ESET Internet Security ürününde Tüm tarayıcıları güvenli hale getir özelliğini etkinleştirmek için **Ayarlar** > **Güvenlik araçları**'nı tıklayın ve **Tüm tarayıcıları güvenli hale getir** kaydırma çubuğunu etkinleştirin.

HTTPS şifreli iletişimin kullanımı, korumalı tarama gerçekleştirmek için gereklidir. Aşağıdaki tarayıcılar Bankacılık ve Ödeme Sistemleri Korumasını desteklemektedir:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

Yalnızca Firefox ve Microsoft Edge, ARM işleyicileri olan cihazlarda desteklemektedir.

Bankacılık ve Ödeme koruması özellikleri hakkında daha fazla bilgi için şu ESET Bilgi Bankası makalesini okuyun (makaleler İngilizce ve diğer dillerde mevcuttur):

- ESET Bankacılık ve Ödeme korumasını nasıl kullanırım?
- ESET Bankacılık ve Ödeme Sistemleri korumasını belirli bir web sitesi için etkinleştirme veya devre dışı bırakma
- ESET Windows ev ürünlerinde Bankacılık ve Ödeme Sistemleri Korumasını duraklatma veya devre dışı bırakma
- ESET Bankacılık ve Ödeme Sistemleri Koruması—sık karşılaşılan hatalar
- ESET sözlüğü | Bankacılık ve Ödeme Sistemleri Koruması

Bankacılık ve ödeme sistemleri koruması gelişmiş ayarları

Bu ayar **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **Bankacılık ve Ödeme koruması** bölümünde bulunabilir:

Temel

Bankacılık ve Ödeme Sistemleri Korumasını etkinleştir - Bankacılık ve Ödeme Sistemleri koruması etkinleştirildiğinde, desteklenen tüm web tarayıcıları varsayılan olarak güvenli modda başlatılır.

Tarayıcı koruması

Desteklenen tüm web tarayıcılarını güvenli modda başlatmak için **Tüm tarayıcıları güvenli hale getir**'i etkinleştirin.

Uzantı yükleme modu - Açılan menüden, ESET tarafından güvenli bir tarayıcıda hangi uzantıların yüklenmesine izin verileceğini seçebilirsiniz: Uzantı yükleme modunu değiştirmek, daha önce yüklenmiş olan tarayıcı uzantılarını etkilemez:

- **Temel uzantılar** - Sadece belirli bir tarayıcı üreticisi tarafından geliştirilen en önemli uzantılar.
- **Tüm uzantılar** - Belirli bir tarayıcı tarafından desteklenen tüm uzantılar.

Web sitelerinin yönlendirilmesi

Korunan web sitelerini yeniden yönlendirme özelliğini etkinleştir – Etkinleştirildiğinde korunan web siteleri listesindeki ve dahili internet bankacılığı listesindeki web siteleri güvenli tarayıcıya yönlendirilir.

Korunan web siteleri - Hangi tarayıcının (normal veya güvenli) açılacağını seçebileceğiniz web siteleri listesidir. Varsayılan olarak, güvenli taramanın etkin olduğunu bildirmek için tarayıcı içinde bilgilendirici bildirim ve tarayıcının etrafında bulunan yeşil çerçeve görüntülenir. Listeyi düzenlemek için Korunan web siteleri'ne bakın.

Web sitelerinin yeniden yönlendirilmesi, ARM işlemcilerine sahip cihazlarda kullanılamaz.

Güvenli tarayıcı

Gelişmiş bellek koruması – Etkinleştirildiğinde güvenli tarayıcının belleği diğer işlemlerin incelemesinden korunur.

Klavye koruması - Bu etkinleştirilirse klavye üzerinden güvenli tarayıcıya girilen bilgiler diğer uygulamalardan gizlenir. Bu, tuş kaydedicilere karşı korumayı artırır.

Tarayıcının yeşil çerçevesi - Devre dışı bırakılırsa bilgilendirici tarayıcı içi bildirim ve tarayıcı etrafındaki yeşil çerçeve gizlenir.

Korunan web siteleri

ESET Internet Security güvenli bir tarayıcının açılmasını tetikleyecek olan, önceden tanımlı web sitelerinden oluşan tümleşik bir liste içerir. Ürün yapılandırmasında web sitesi ekleyebilir veya web sitesi listesini düzenleyebilirsiniz.

Korunan web siteleri listesi **Gelişmiş ayarlar** (F5) > **Web ve e-posta** > **Bankacılık ve Ödeme koruması** > **Temel** > **Korunan web siteleri** > **Düzenle** bölümünden görüntülenip düzenlenebilir.

Korunan web siteleri listesinde yer alan kurallarda, belirli bir web sitesinin güvenli tarayıcıda mı yoksa normal bir tarayıcıda mı açılacağı ya da web sitesini her ziyaret edişinizde sorulması gerektiği belirtilir. Aşağıdaki **Web sitesini ekleme** bölümünde seçeneklerin açıklamasına bakın.

Denetim öğeleri

Ekle – Bilinen web siteleri listesine bir web sitesi eklemenize olanak sağlar.

Düzenle - Seçili web sitesini düzenlemenize olanak tanır.

Sil - Seçilen girişleri kaldırır.

İçe Aktar/Dışa Aktar - Korunan web siteleri listesini dışa aktarmanıza ve yeni bir cihaza aktarmanıza olanak sağlar.

Web sitesi ekle

Web sitesi sayfası - Kuralın uygulanacağı HTTPS web sitesi.

Bu web sitesini şununla aç - Web sitesini ziyaret ettiğinizde Bankacılık ve Ödeme Sistemleri Koruması davranışını seçin:

- **Güvenli tarayıcı** - Web sitesi güvenli tarayıcıya yeniden yönlendirilir ve Bankacılık ve Ödeme Sistemleri Koruması tarafından korunur.
- **Bana sor** - Web sitesini ziyaret ederken ilgili siteyi normal veya güvenli tarayıcıda açmayı seçebilirsiniz. ESET Internet Security eyleminizi hatırlayabilir veya tarayıcıyı manuel olarak da seçebilirsiniz.
- **Normal tarayıcı** - Web sitesi ek güvenlik olmaksızın normal bir tarayıcıda açılır.

Tarayıcı içi bildirim

Güvenli tarayıcı, tarayıcı içi bildirimler ve tarayıcı çerçevesinin rengi üzerinden mevcut durumu hakkında sizi bilgi verir.

Tarayıcı içi bildirimler sağ tarafta yer alan sekmede gösterilir.

Tarayıcı içi bildirimi genişletmek için ESET simgesini tıklayın. Bildirimi küçültmek için bildirim metnini tıklayın. Bildirimi ve yeşil tarayıcı çerçevesini kapatmak için kapat simgesini tıklayın.

Yalnızca bilgilendirici bildirim ve yeşil tarayıcı çerçevesi kapatılabilir.

Tarayıcı içi bildirimler

Bildirim türü	Durum
Bilgi içerikli bildirim ve yeşil tarayıcı çerçevesi	Maksimum koruma sağlanır ve tarayıcı içi bildirim varsayılan olarak küçültülür. Tarayıcı içi bildirimi genişletin ve Güvenlik araçları ayarlarını açmak için **Ayarlar**'ı tıklayın.
Uyarı ve turuncu tarayıcı çerçevesi	Güvenli tarayıcı, kritik olmayan bir soruna karşı sizi bilgilendirir. Sorun veya çözüm hakkında daha fazla bilgi için tarayıcı içi bildirimde yer alan talimatları uygulayın.
Güvenlik uyarısı ve kırmızı tarayıcı çerçevesi	Tarayıcı ESET Bankacılık ve Ödeme Sistemleri koruması tarafından korunmaz. Korumanın etkin olduğundan emin olmak için tarayıcıyı yeniden başlatın. Tarayıcıya yüklenen dosyalarla herhangi bir çakışmayı çözmek için Günlük dosyaları > Bankacılık ve Ödeme Sistemleri Koruması'nı açın ve tarayıcıyı bir sonraki başlatışınızda günlüğe kaydedilen dosyaların yüklenmediğinden emin olun. Sorun devam ederse Bilgi Bankası makalemizdeki talimatları izleyerek ESET Teknik Destek ekibiyle iletişime geçin.

Anti-Theft

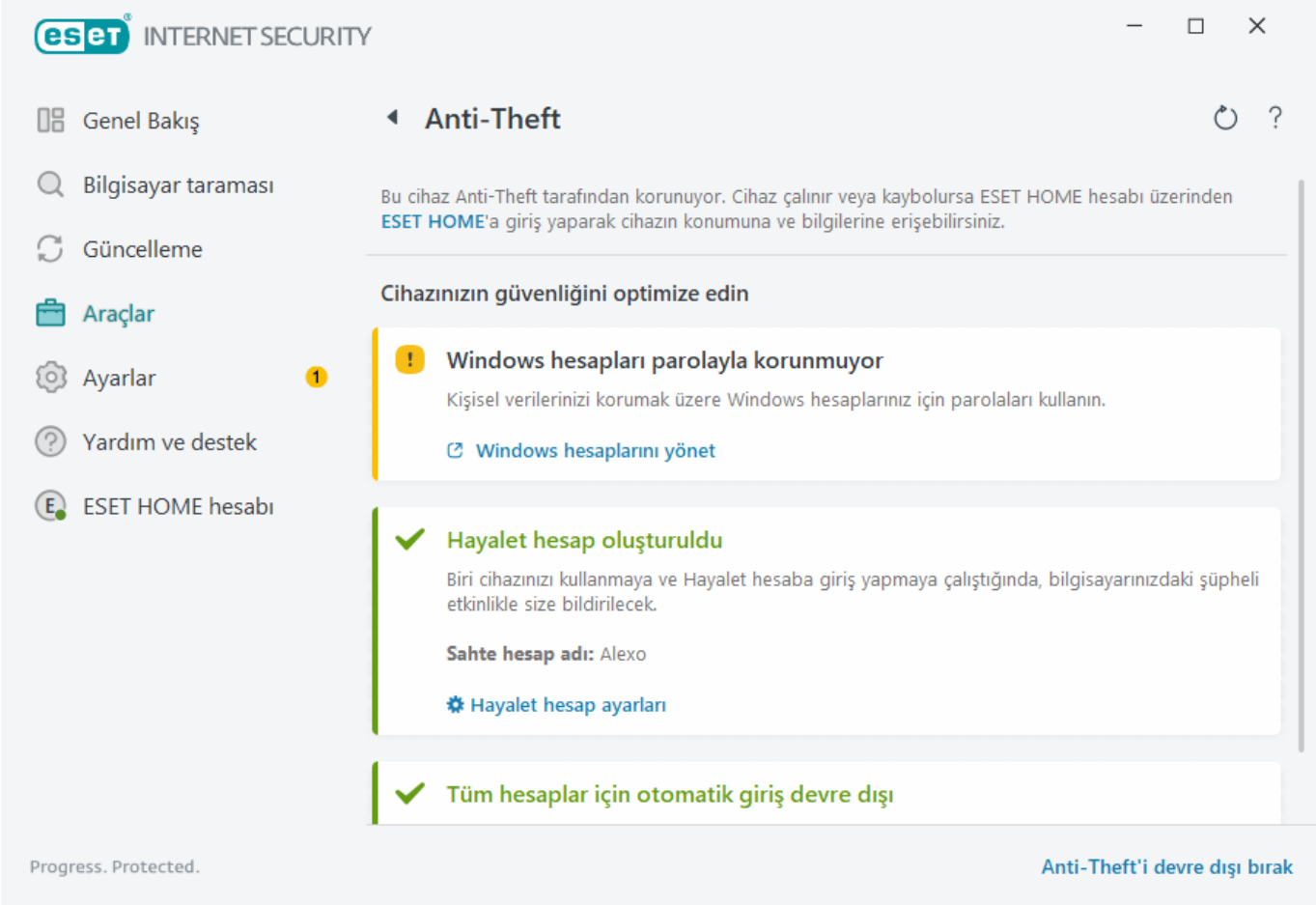
Evden işe veya başka kamusal alanlara yaptığımız günlük seyahatlerimizde kişisel cihazlarımız sürekli kaybolma veya çalınma riski altındadır. Anti-Theft cihazın kaybolması veya çalınması durumunda kullanıcı düzeyi güvenliği artıran bir özelliktir. Anti-Theft, ESET HOME portalındaki IP adresi ile yerini tespit etme özelliğini kullanarak kayıp cihazın kullanımını izlemenize ve cihazı takip etmenize olanak tanır, böylece cihazınızı geri alıp kişisel verilerinizi korumanıza yardımcı olur.

Anti-Theft, coğrafi IP adresi arama, web kamerası görüntüsü yakalama, kullanıcı hesabı koruması ve aygıt izleme gibi modern teknolojileri kullanarak, size ve bir emniyet kuruluşuna kaybolması veya çalınması durumunda bilgisayarınızı ya da aygıtınızı bulma konusunda yardımcı olabilir. ESET HOME portalında, bilgisayarınızda veya cihazınızda hangi etkinliklerin olduğunu görebilirsiniz.

ESET HOME portalında Anti-Theft ile ilgili daha fazla bilgi edinmek için ESET HOME Online Yardım'a bakın.

Anti-Theft, kullanıcı hesapları yönetimindeki kısıtlamalar nedeniyle etki alanlarındaki bilgisayarlarda düzgün çalışmayabilir.

Anti-Theft ürününü etkinleştirdikten sonra ana program penceresinde > **Araçlar** > **Anti-Theft** bölümünde cihazınızın güvenliğini optimize edebilirsiniz.



Optimizasyon seçenekleri

Hayalet hesap oluşturulmadı

Hayalet Hesap oluşturmak, kaybolan veya çalınan bir cihazın yerini bulma şansını artırır. Cihazınızı kayıp olarak işaretlerseniz Anti-Theft, hassas verilerinizi korumak için etkin kullanıcı hesaplarınıza erişimi engeller. Cihazı kullanmaya çalışanlara yalnızca Hayalet hesabı kullanma izni verilir. Hayalet Hesap, sınırlı izinlere sahip bir misafir hesabı biçimidir. Cihazınız kurtarıldı olarak işaretlenene kadar varsayılan sistem hesabı olarak kullanılır ve bu sayede kullanıcının diğer kullanıcı hesaplarına giriş yapılması veya kullanıcının verilerine erişilmesi önlenir.

Bilgisayarınız normal durumdayken biri Hayalet hesapta oturum açtığında, bilgisayarınızdaki şüpheli etkinlikle ilgili bilgileri içeren bir bildirim size e-posta ile gönderilir. E-posta bildirimini aldıktan sonra bilgisayarı kayıp olarak işaretlemek istediğinize karar verebilirsiniz.

Hayalet hesap oluşturmak için **Hayalet hesap oluştur**'u tıklayın, metin alanına **Hayalet hesap adını** yazın ve **Oluştur**'u tıklayın.

Hayalet hesap oluşturulduğunda, hesabı yeniden adlandırmak veya silmek için **Hayalet hesap ayarları**'nı tıklayın.

Windows hesapları parola koruması

Kullanıcı hesabınız parolayla korunmuyor. En az bir kullanıcı hesabı parolayla korunmadığında bu optimizasyon uyarısını alırsınız. Bilgisayarda tüm kullanıcılar için bir parola oluşturmak (**Hayalet hesap** hariç) bu sorunu çözer.

Kullanıcı hesabı için parola oluşturmak üzere **Windows** hesaplarını yönet**'i tıklayın** ve parolayı değiştirin veya aşağıdaki talimatları uygulayın:

1. Klavyenizde CTRL+Alt+Delete kombinasyonuna basın.

2. **Parolayı değiştir**'i tıklayın.

3. **Eski parola alanını** boş bırakın.

4. Parolayı **Yeni parola** ile **Parolayı onaylayın** alanlarına yazın ve **Enter** tuşuna basın.

Windows hesapları için otomatik giriş

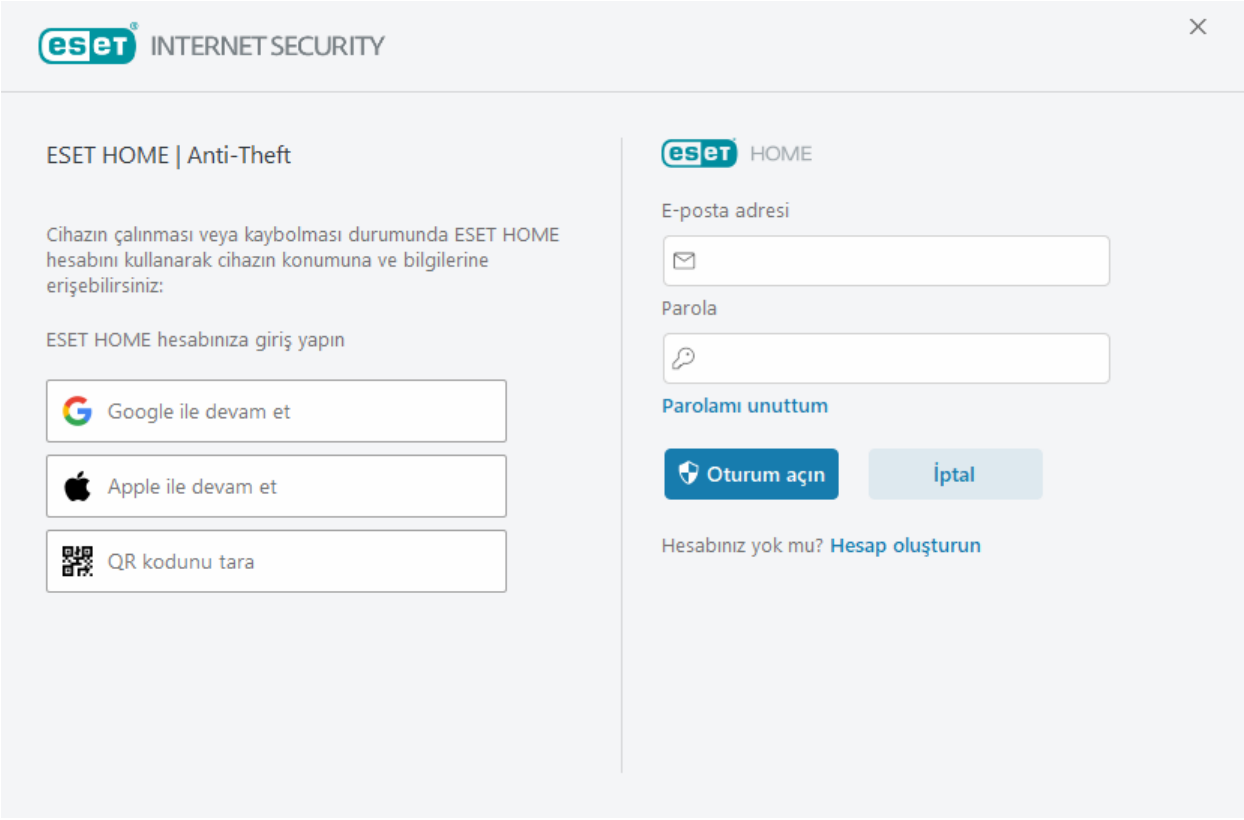
Kullanıcı hesabınızda otomatik giriş özelliği etkinleştirildi. Hesabınız yetkisiz erişime karşı korunmuyor. En az bir kullanıcı hesabında otomatik giriş özelliği etkinse bu optimizasyon uyarısını alırsınız. Bu optimizasyon sorununu çözmek için **Otomatik girişi devre dışı bırak**'ı tıklayın.

Hayalet hesap için otomatik giriş

Cihazınızda **Hayalet hesap** için otomatik giriş özelliği etkinleştirildi. Cihazınız normal durumdayken otomatik giriş özelliğini kullanmanızı önermiyoruz. Bu, gerçek kullanıcı hesabınıza erişimle ilgili sorunlara neden olabilir veya bilgisayarınızın kayıp durumuyla ilgili yanlış uyarılar gönderebilirsiniz. Bu optimizasyon sorununu çözmek için **Otomatik girişi devre dışı bırak**'ı tıklayın.

ESET HOME Hesabınıza giriş yapın

Anti-Theft aracını etkinleştirmek/devre dışı bırakmak, ayrıca cihaz konumuna ve ESET HOME portalındaki bilgilere erişmek için ESET HOME hesabınıza giriş yapın.



ESET HOME hesabınıza giriş yapmak için birkaç yöntem vardır:

- **ESET HOME E-posta adresinizi ve parolanızı kullanarak** - ESET HOME hesabınızı oluşturmak için kullandığınız **E-posta adresini** ve **Parolayı** yazın ve **Giriş yap**'ı tıklayın.

- **Google Hesabınızı/AppleID** kimliğinizi kullanarak - **Google** ile devam et veya **Apple** ile devam et'i tıklayıp ilgili hesaba giriş yapın. Başarıyla giriş yaptıktan sonra ESET HOME onayı için web sayfasına yönlendirilirsiniz. Devam etmek için ESET ürün pencerenize geri dönün. Google hesabı/AppleID ile giriş yapma hakkında daha fazla bilgi için ESET HOME Online Yardım bölümündeki talimatlara bakın.

- **QR kodunu tarayarak** - QR kodunu görüntülemek için **QR kodunu tara** seçeneğini tıklayın. ESET HOME mobil uygulamanızı açın ve QR kodunu tarayın veya cihaz kameranızı QR koduna tutun. Daha fazla bilgi için ESET HOME Online Yardım bölümündeki talimatlara bakın.

Giriş yapılamadı - sık karşılaşılan hatalar.

ESET HOME hesabınız yoksa kaydolmak için **Hesap oluştur**'u tıklayın veya ESET HOME Online Yardım bölümündeki talimatlara bakın.
Parolanızı unuttuysanız **Parolamı unuttum** seçeneğini tıklayın ve ekrandaki adımları uygulayın veya ESET HOME Online Yardım bölümüne bakın.

Anti-Theft, Microsoft Windows Home Server'ı desteklemiyor.

Cihaz adı belirleyin

Cihaz adı alanı tüm ESET HOME hizmetlerinde bir tanımlayıcı olarak gösterilecek bilgisayar (cihaz) adını temsil eder. Varsayılan olarak bilgisayarınızın bilgisayar adı kullanılır. Cihaz adını yazın veya varsayılanı kullanın ve **Devam**'ı tıklayın.

Anti-Theft etkin/devre dışı

Anti-Theft aracını etkinleştirdiğinizde/devre dışı bıraktığınızda bu pencerede bir onay mesajı yer alır:

- Etkin - Cihazınız artık Anti-Theft tarafından korunmaktadır. Cihazın güvenliğini ESET HOME portalında hesabınızı kullanarak uzaktan yönetebilirsiniz.

- Devre dışı bırakıldı - Anti-Theft bu cihazda devre dışı bırakıldı ve bu cihaz için <%ESET_ANTTHEFT%> ile ilgili tüm veriler ESET HOME portalından kaldırıldı.

Yeni aygıt eklenemedi

Anti-Theft Ürününü etkinleştirirken bir hata aldınız.

En yaygın senaryolar şu şekildedir:

- ESET HOME portalına giriş sırasında hata oluştu

- Internet bağlantısı yok (veya Internet şu anda işlevsel değil)

Sorunu çözemezseniz ESET Teknik Destek ekibiyle iletişime geçin.

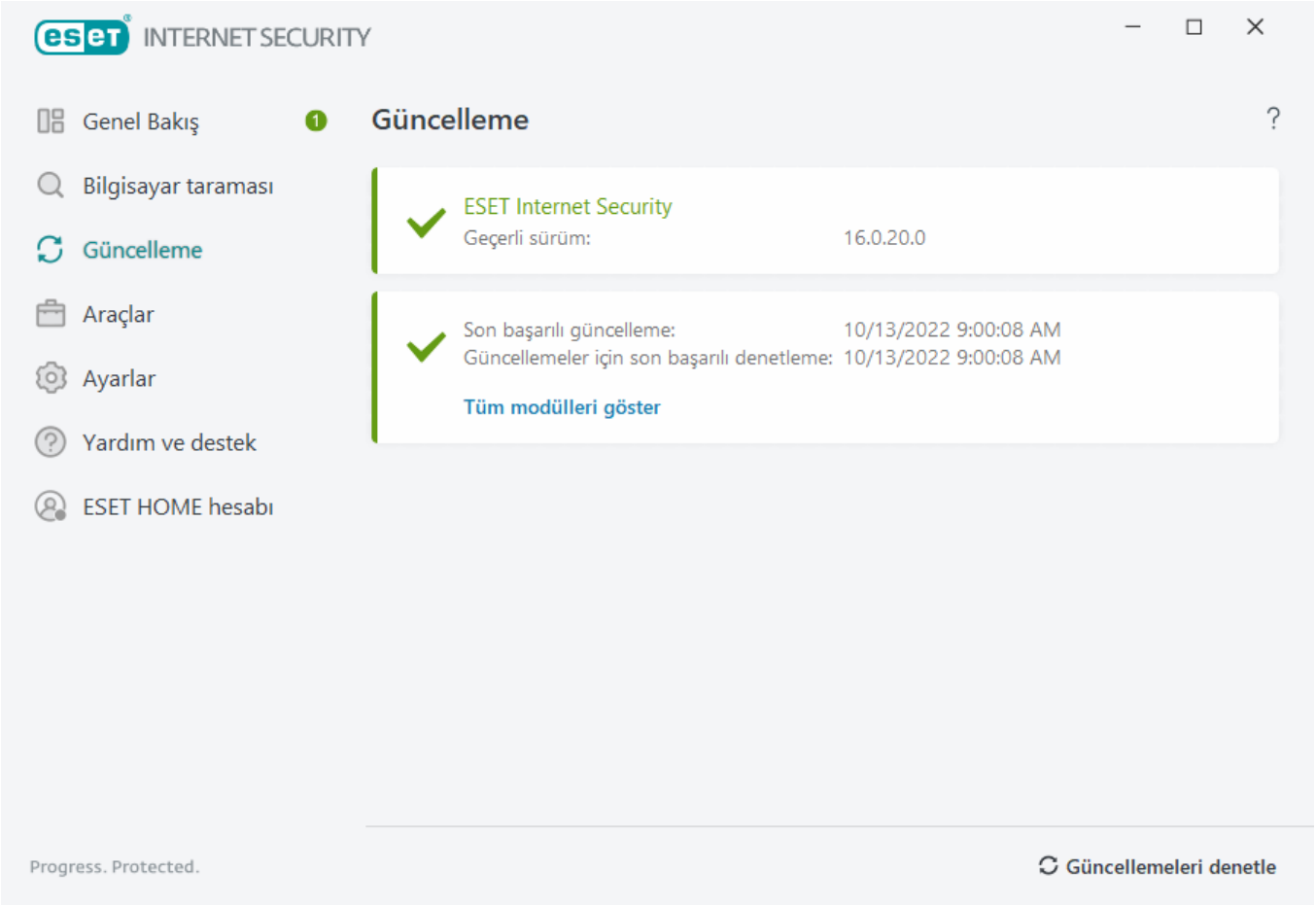
Programı güncelleme

ESET Internet Security ürününün düzenli olarak güncellenmesi, bilgisayarınızda maksimum güvenlik düzeyini sağlamak için en iyi yöntemdir. Güncelleme modülü hem program modüllerini hem de sistem bileşenlerini her zaman güncel tutmanıza olanak tanır.

Ana program penceresinde **Güncelle** seçeneğini tıklatarak, son başarılı güncellemenin tarih ve saati ile güncelleme gerekip gerekmediği de dahil olmak üzere geçerli güncelleme durumunu görüntüleyebilirsiniz.

Otomatik güncellemelerin yanı sıra bir manuel güncellemeyi başlatmak için **Güncellemeleri kontrol edin** seçeneğini tıklayabilirsiniz. Program modüllerini ve bileşenleri düzenli olarak güncellemek, kötü amaçlı koda karşı tam koruma sağlamanın önemli bir parçasıdır. Lütfen bu ürün modülleri yapılandırılmasına ve işleyişine dikkat edin. Güncellemeleri almak için Lisans anahtarınızı kullanarak ürününüzü etkinleştirmeniz gerekir. Kurulum esnasında bunu yapmadıysanız ESET güncelleme sürücülerine erişmek üzere, güncelleme yaparken ürününüzü etkinleştirmek için Lisans anahtarınızı girmeniz gerekir.

> Lisans anahtarınız ESET Internet Security ürününü satın aldıktan sonra ESET tarafından bir e-postada sağlanır.



Mevcut sürüm – Yüklediğiniz mevcut ürün sürümünün numarasını gösterir.

Son başarılı güncelleme – Son başarılı güncelleme tarihini gösterir. Yakın bir tarih göremezseniz, ürün modülleriniz güncel olmayabilir.

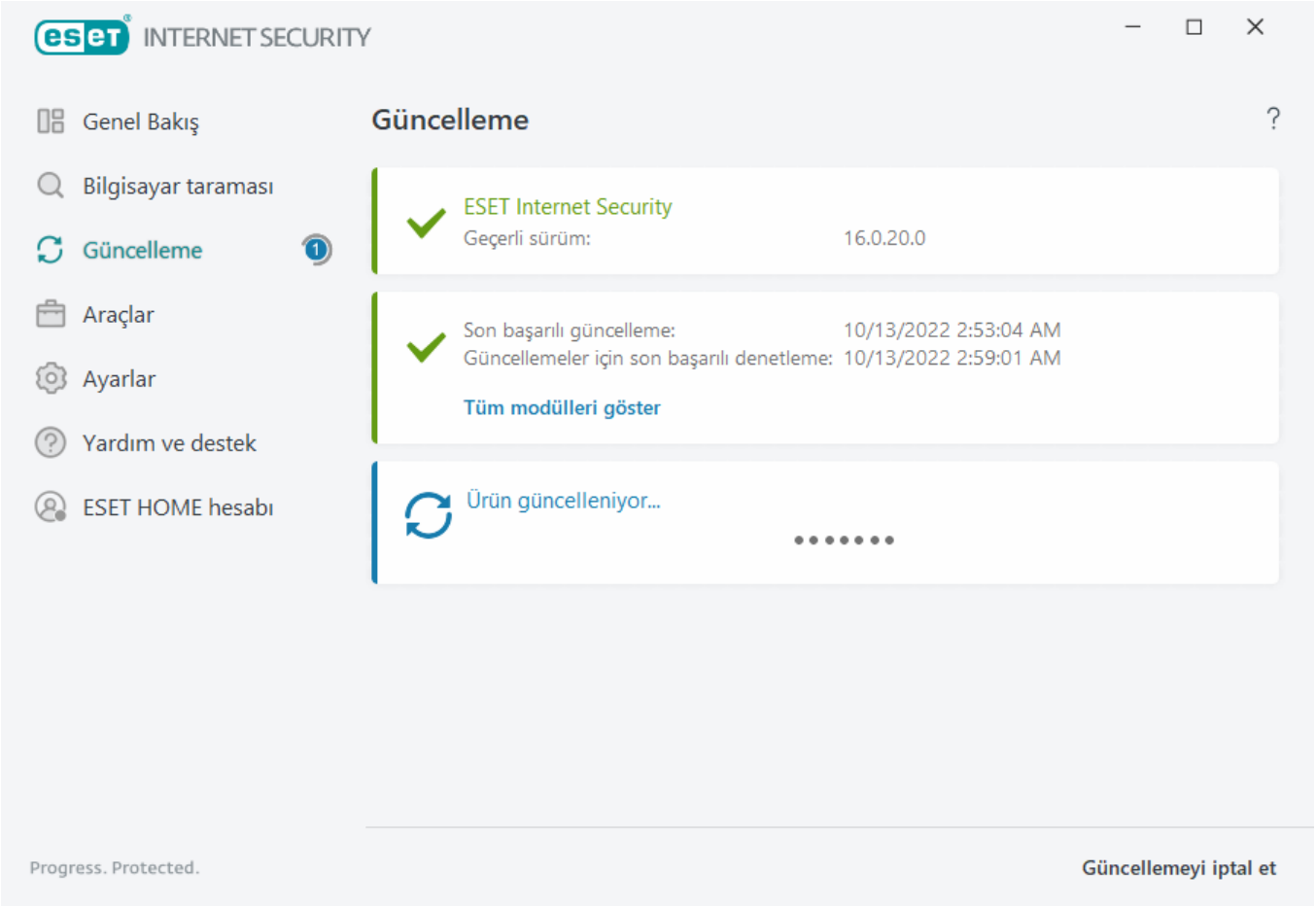
Güncellemeler için son başarılı kontrol – Güncellemeler için son başarılı kontrolün tarihini gösterir.

Tüm modülleri göster – Yüklenmiş olan program modüllerinin listesini gösterir.

Kullanılabilir en yeni ESET Internet Security sürümünü belirlemek için **Güncellemeleri denetle** öğesini tıklatın.

Güncelleme işlemi

Güncellemeleri kontrol et seçeneği tıklatıldıktan sonra indirme işlemi başlar. Karşıdan yükleme ilerleme çubuğu ve kalan yükleme zamanı görüntülenir. Güncellemeyi kesmek için **Güncellemeyi iptal et** seçeneğini tıklatın.



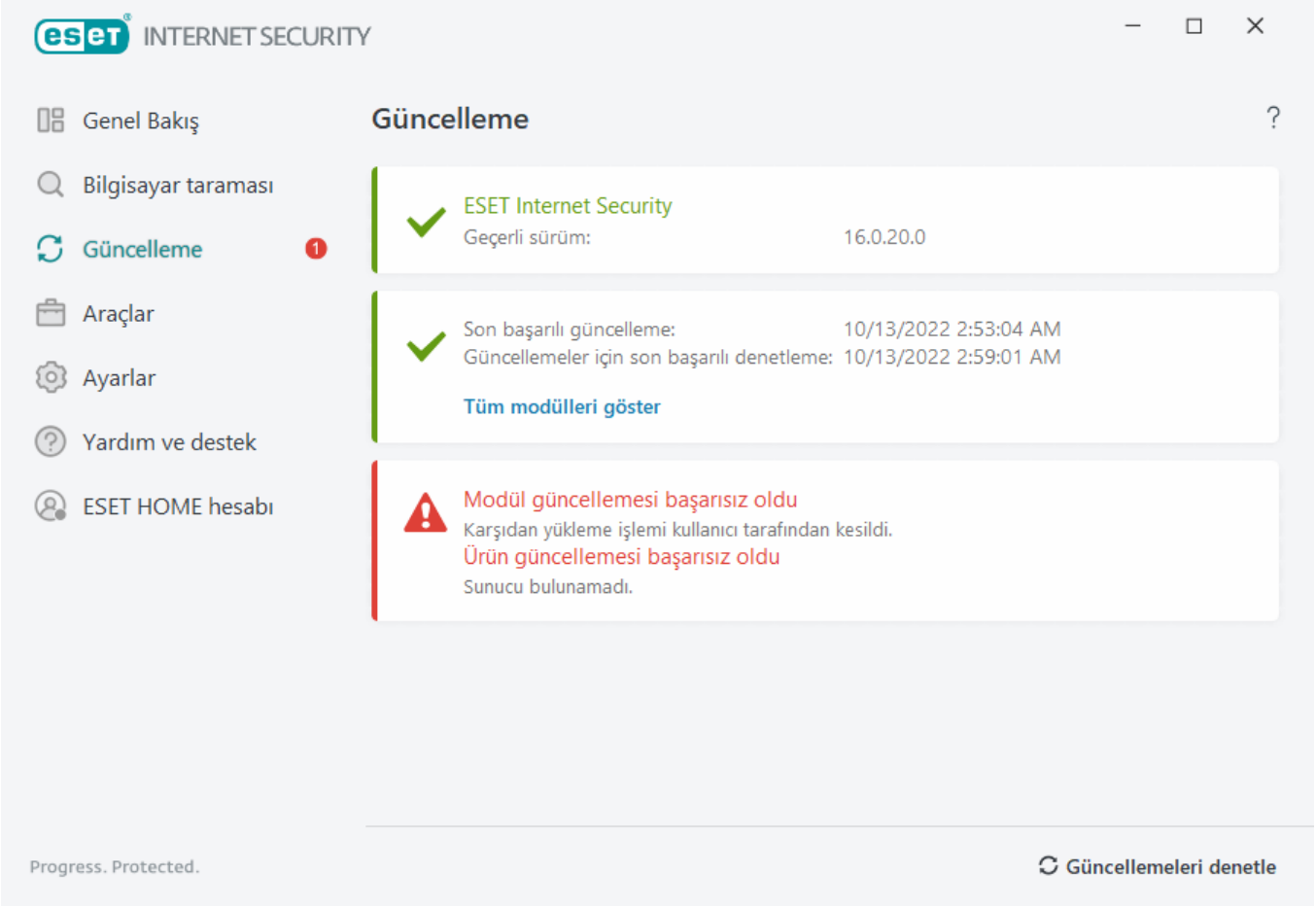
Normal şartlarda **Güncelleme** penceresinde programın güncel olduğunu belirten yeşil onay işaretini görürsünüz. Yeşil onay işaretini görmezseniz, program güncel değildir ve virüslere açıktır. Lütfen program modüllerini en kısa zamanda güncelleyin.

Başarısız güncelleme

Modül güncellemesinin başarısız olduğuyla ilgili bir ileti alırsanız nedeni şunlardan biri olabilir:

1. **Geçersiz lisans** - Etkinleştirme için kullanılan lisans geçersiz veya süresi dolmuş. Ana program penceresinde, **Yardım ve destek** > **Lisansı değiştir**'i tıklayıp ürününüzü etkinleştirin.

2. **Güncelleme dosyaları indirilirken bir hata oluştu** – Hatanın nedeni yanlış İnternet bağlantısı ayarları olabilir. Internet bağlantınızı denetlemenizi öneririz (web tarayıcınızda herhangi bir web sitesi açarak). Web sitesi açılmazsa İnternet bağlantısının kurulmamış olması veya bilgisayarınızda bağlantı sorunları bulunması mümkündür. Etkin bir İnternet bağlantınız yoksa lütfen İnternet Hizmet Sağlayıcınız (ISP) ile bunu denetleyin.



Tüm program modüllerinin doğru şekilde güncellendiğinden emin olmak için yeni bir ürün sürümüne başarılı ESET Internet Security güncellemesinden sonra bilgisayarınızı yeniden başlatmanızı öneririz. Normal modül güncellemelerinin ardından bilgisayarınızın yeniden başlatılması gerekmez.

Daha fazla bilgi için lütfen "Modül güncellemesi başarısız oldu" iletisi için sorun giderme bölümüne bakın.

Güncelleme ayarları

Güncelleme ayarları seçenekleri **Güncelle** > **Temel** alanında **Gelişmiş ayarlar** ağacında (F5) bulunur. Bu bölüm, kullanılan güncelleme sunucuları gibi güncelleme kaynağı bilgilerini ve bu sunucular için kimlik doğrulama verilerini belirtir.

Temel

Şu anda kullanımda olan güncelleme profili (**Gelişmiş ayarlar** > **Güvenlik duvarı** > **Bilinen ağlar** altında belirli bir profil ayarlanmamışsa) **Varsayılan güncelleme profilini seç** açılır menüsünde gösterilir.

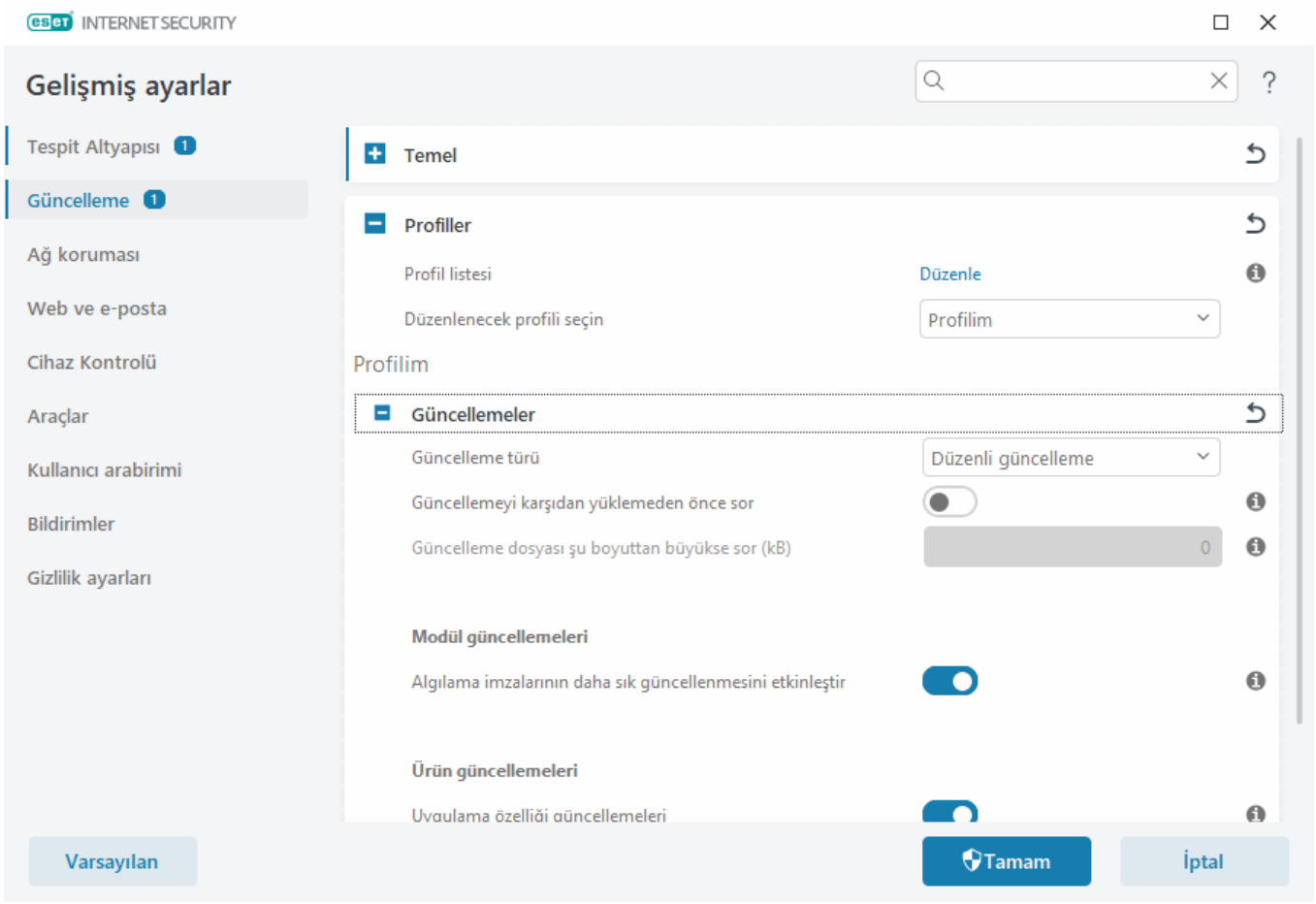
Yeni bir profil oluşturmak için Güncelleme profilleri bölümüne bakın.

Otomatik profil değiştirme – Belirli ağ için profili değiştirmenize olanak tanır.

Algılama altyapısı veya modül güncellemelerini indirmek istediğinizde sorun yaşıyorsanız geçici güncelleme dosyalarını/ön belleği silmek için **Temizle**'yi tıklayın.

Modül geri alımı

Algılama altyapısının ve/veya program modüllerinin yeni güncellemesinin istikrarsız veya bozuk olduğundan şüpheleniyorsanız, önceki sürüme geri alabilir ve belirlediğiniz bir süre boyunca güncellemeleri devre dışı bırakabilirsiniz.



Güncellemelerin karşıdan düzgün bir şekilde yüklenmesi için tüm güncelleme parametrelerini doğru doldurmanız önemlidir. Güvenlik duvarı kullanıyorsanız, ESET programınızın İnternet iletişimi (örneğin, HTTP iletişimi) kurmasına izin verildiğinden emin olun.

Profiller

Çeşitli güncelleme yapılandırmaları ve görevleri için güncelleme profilleri oluşturulabilir. Güncelleme profilleri oluşturmak, özellikle düzenli olarak değişen Internet bağlantısı özellikleri için alternatif bir profile ihtiyaç duyan mobil kullanıcılar için kullanışlıdır.

Düzenlenecek profili seç açılır menüsü, halihazırda seçili olan profili gösterir ve varsayılan olarak **Profilim** şeklinde ayarlanır. Yeni profil oluşturmak için, **Profil listesi**'nin yanındaki **Düzenle** seçeneğini tıklayın ve ardından kendi **Profil adınızı** girip **Ekle**'yi tıklayın.

Güncellemeler

Varsayılan olarak, güncelleme dosyalarının en az ağ trafiğine sahip ESET sunucusundan otomatik olarak yüklenmesini sağlamak için **Güncelleme türü Düzenli güncelle** olarak ayarlanır. Sınama modu güncellemeleri (**Sınama modu güncellemesi** seçeneği), dahili sınamadan geçen ve kısa bir süre sonra genel olarak kullanılabilir duruma gelecek güncellemelerdir. En son algılama yöntemlerine ve düzeltmelere erişim elde ederek sınama modu güncellemelerini etkinleştirme avantajından faydalanabilirsiniz. Ancak, sınama modu güncellemeleri her zaman yeterince kararlı olmayabilir ve maksimum kullanılabilirlik ve kararlılık gerektiren üretim sunucularında ve iş istasyonlarında KULLANILMAMALIDIR.

Güncellemeyi indirmeden önce sor – Programda, güncelleme dosyası indirmelerini onaylamayı veya reddetmeyi seçebileceğiniz bir bildirim görüntülenir.

Bir güncelleme dosyasının boyutu şu değerden büyükse sor (kB) – Güncelleme dosyasının boyutu belirtilen değerden büyükse programda bir onay iletişim kutusu görüntülenir. Güncelleme dosyası 0 kB olarak ayarlanırsa program her zaman bir onay iletişim kutusu gösterir.

Modül güncellemeleri

Algılama imzalarının daha sık güncellemelerini etkinleştir – Algılama imzaları daha kısa aralıklarla güncellenir. Bu ayarı devre dışı bırakmak algılama hızını olumsuz etkileyebilir.

Ürün güncellemeleri

Uygulama özelliği güncellemeleri - ESET Internet Security ürününün yeni sürümlerini otomatik olarak yükler.

Bağlantı seçenekleri

Güncellemeleri indirmek için proxy sunucusu kullanmak üzere Bağlantı seçenekleri bölümüne bakın.

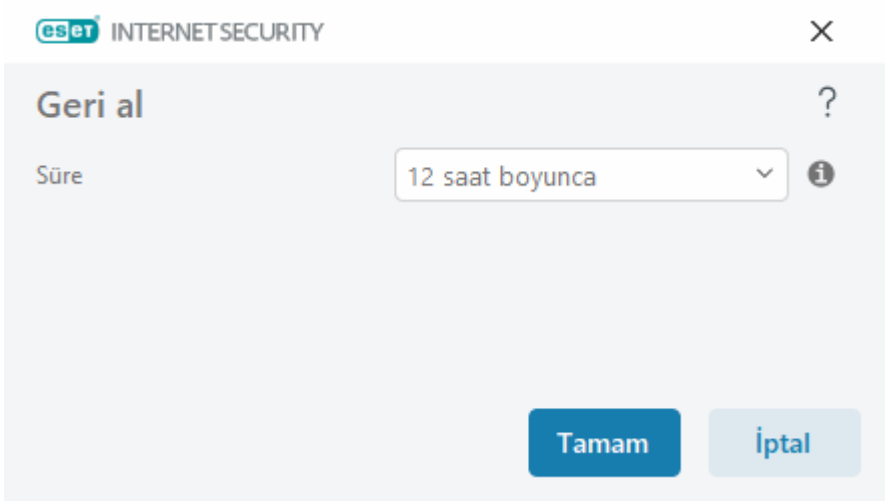
Geri almayı güncelle

Tespit altyapısının veya program modüllerinin yeni güncellemesinin istikrarsız veya bozuk olduğundan şüpheleniyorsanız önceki sürüme geri alabilir ve güncellemeleri geçici olarak devre dışı bırakabilirsiniz. Alternatif olarak, süresiz bir şekilde ertelediyseniz önceden devre dışı bıraktığınız güncellemeleri etkinleştirebilirsiniz.

ESET Internet Security, geri alma özelliğiyle birlikte kullanılmak üzere tespit altyapısının ve program modüllerinin sistem görüntülerini kaydeder. Virüs veri tabanı sistem görüntülerini oluşturmak için **Modüllerin sistem görüntülerini oluştur** seçeneğini etkin durumda bırakın. **Modüllerin sistem görüntülerini oluştur** etkinleştirildiğinde ilk sistem görüntüsü ilk güncelleme sırasında oluşturulur. Bir sonraki 48 saat sonra oluşturulur. **Yerel olarak depolanan sistem görüntüleri sayısı** alanı, depolanan tespit altyapısı sistem görüntülerinin sayısını tanımlar.

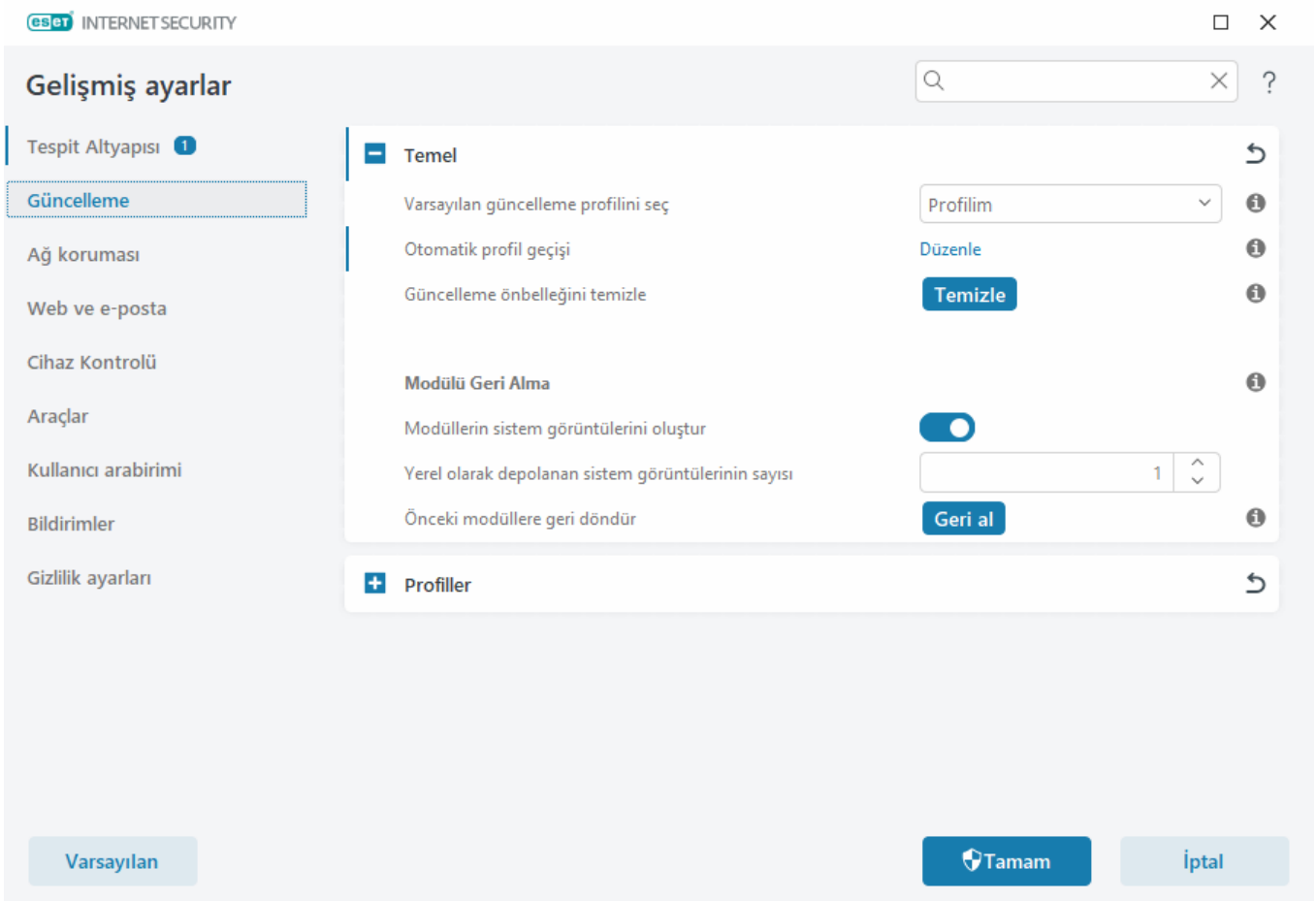
> Maksimum sistem görüntüsü sayısına ulaşıldıysa (örneğin üç), en eski sistem görüntüsü 48 saatte bir yeni bir sistem görüntüsüyle değiştirilir. ESET Internet Security, tespit altyapısı ve program modülü güncelleme sürümlerini en eski sistem görüntüsüne döndürür.

Geri al (**Gelişmiş ayarlar** (F5) > **Güncelle** > **Temel**) seçeneğini tıklarsanız, **Süre** açılır menüsünden algılama altyapısı ve program modülü güncellemelerinin duraklatılacağı süreyi temsil eden bir zaman aralığı seçmeniz gerekir.



Güncelleme işlevini manuel olarak geri yükleyene kadar düzenli güncellemeleri süresiz bir şekilde ertelemek için **İptal edilene kadar** ayarını işaretleyin. ESET, potansiyel olarak güvenlik riski taşıdığından bu seçeneği işaretlemenizi önermez.

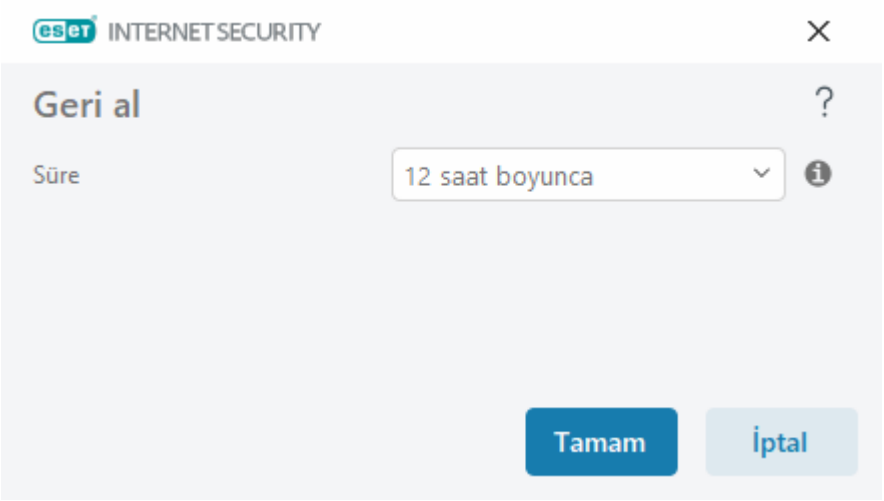
Geri alma gerçekleştirilirse **Geri al** düğmesi **Güncellemelere izin ver** olarak değişir. **Güncellemeleri askıya al** açılır menüsünden seçilen zaman aralığı süresince hiçbir güncellemeye izin verilmez. Tespit altyapısı sürümü kullanılabilir en eski sürüme geri döndürülür ve yerel bilgisayar dosya sisteminde sistem görüntüsü olarak kaydedilir.



22700'ün en son tespit altyapısı sürüm numarası olduğunu, 22698 ve 22696'nın da tespit altyapısı sistem görüntüleri olarak depolandığını varsayalım. 22697'nin kullanılamıyor olduğunu unutmayın. Bu örnekte, bilgisayar 22697 güncellemesi sırasında kapalıdır ve 22697 indirilmeden önce daha yeni bir güncelleme yapılmıştır. **Yerel olarak depolanan sistem görüntüleri sayısı** alanı iki ise ve **Geri Al**'ı tıklarsanız tespit altyapısı (program modülleri dahil) 22696 sürüm numarasına geri yüklenir. Bu işlem biraz zaman alır. Tespit altyapısı sürümünün Güncelleme ekranında eski sürüme döndürüldüğünü doğrulayın.

Geri alma zaman aralığı

Geri al (**Gelişmiş ayarlar** (F5) > **Güncelle** > **Temel**) seçeneğini tıklarsanız, **Süre** açılır menüsünden algılama altyapısı ve program modülü güncellemelerinin duraklatılacağı süreyi temsil eden bir zaman aralığı seçmeniz gerekir.



Güncelleme işlevini manuel olarak geri yükleyene kadar düzenli güncellemeleri süresiz bir şekilde ertelemek için **İptal edilene kadar** ayarını işaretleyin. ESET, potansiyel olarak güvenlik riski taşıdığından bu seçeneği işaretlemenizi önermez.

Ürün güncellemeleri

Ürün güncellemeleri bölümü, kullanıma hazır yeni özellik güncellemelerini otomatik olarak yüklemenize olanak sağlar.

Uygulama özelliği güncellemeleri yeni özellikler sunar veya önceki sürümlerde zaten mevcut olan özelliklerde değişiklikler yapar. Kullanıcı müdahalesi olmadan otomatik olarak gerçekleştirilebilir ya da bildirim almayı seçebilirsiniz. Uygulama özelliği güncellemesi yüklendikten sonra bilgisayarı yeniden başlatmak gerekebilir.

Uygulama özelliği güncellemeleri - Bu etkinleştirildiğinde uygulama özelliği güncellemeleri otomatik olarak gerçekleştirilir.

Bağlantı seçenekleri

Belirli bir güncelleme profili için proxy sunucu ayarları seçeneklerine erişmek üzere **Gelişmiş ayarlar** ağacından (F5) **Güncelle** seçeneğini, ardından **Profiller** > **Güncellemeler** > **Bağlantı seçenekleri**'ni tıklayın. Açılır menüden **Proxy modu**'nu tıklayın ve aşağıdaki üç seçenekten birini belirleyin:

- Proxy sunucu kullanma
- Proxy sunucuyla bağlan
- Genel proxy sunucu ayarlarını kullan

Gelişmiş ayarlar ağacının **Araçlar** > **Proxy sunucu** dalı altında halihazırda belirtilmiş olan proxy sunucu yapılandırması seçeneklerini kullanmak için **Genel proxy sunucu ayarlarını kullan** seçeneğini belirleyin.

ESET Internet Security uygulamasını güncellemek için proxy sunucusu kullanılmayacağını belirtmek üzere **Proxy sunucu kullanma** seçeneğini belirleyin.

Şu durumlarda **Proxy sunucu üzerinden bağlan** seçeneği belirlenmelidir:

- **Araçlar** > **Proxy sunucu** konumunda tanımlanandan farklı bir proxy sunucu kullanılarak ESET Internet Security ürünü güncellenir. Bu yapılandırmada, yeni proxy için bilgiler **Proxy sunucu** adresi, iletişim **Bağlantı Noktası** (varsayılan olarak 3128) ve gerekirse proxy sunucusu için **Kullanıcı adı** ile **Parola** altında belirtilmelidir.

- Proxy sunucusu ayarları genel olarak belirlenmedi, ancak ESET Internet Security güncellemeler için bir proxy sunucusuna bağlanacak.
- Bilgisayarınız İnternet'e bir proxy sunucu üzerinden bağlanıyor. Ayarlar program yüklemesi sırasında Internet Explorer'dan alınır, ancak değiştirilmeleri durumunda (örneğin ISP'nizi değiştirirseniz) lütfen bu pencerede listelenen proxy ayarlarının doğru olduğundan emin olun. Aksi takdirde, program güncelleme sunucularına bağlanamaz.

Proxy sunucu için varsayılan ayar **Genel proxy sunucu ayarlarını kullan**'dır.

Proxy kullanılamıyorsa doğrudan bağlantıyı kullan – Proxy erişilebilir olmadığında güncelleme sırasında atlanır.

> Bu bölümdeki **Kullanıcı adı** ve **Parola** alanları proxy sunucusuna özeldir. Bu alanları yalnızca, proxy sunucusuna erişmek için kullanıcı adı ve parola gerekliyse doldurun. Bu alanlar yalnızca internete proxy sunucusu aracılığıyla erişmek için parolaya gereksinim duyduğunuzu biliyorsanız doldurulmalıdır.

Güncelleme görevleri nasıl oluşturulur?

Güncellemeler, ana menüden **Güncellemeleri kontrol et** tıklatıldıktan sonra görüntülenen ana pencerede **Güncelle** tıklatılarak manuel olarak tetiklenebilir.

Güncellemeler ayrıca zamanlanan görev olarak da çalıştırılabilir. Zamanlanan bir görevi yapılandırmak için **Araçlar** > **Diğer Araçlar** > **Zamanlayıcı**'yı tıklayın. Varsayılan olarak, ESET Internet Security içinde aşağıdaki görevler etkinleştirilir:

- **Düzenli otomatik güncelleme**
- **Çevirmeli bağlantıdan sonra otomatik güncelleme**
- **Kullanıcı oturum açtıktan sonra otomatik güncelleme**

Her güncelleme görevi, ihtiyaçlarınızı karşılayacak şekilde değiştirilebilir. Varsayılan güncelleme görevlerinin dışında, kendi tanımlı yapılandırmayla yeni güncelleme görevleri oluşturabilirsiniz. Güncelleme görevleri

oluşturma ev yapılandırma hakkında daha fazla bilgi için Zamanlayıcı bölümüne bakın.

İletişim penceresi - Yeniden başlatma gerekli

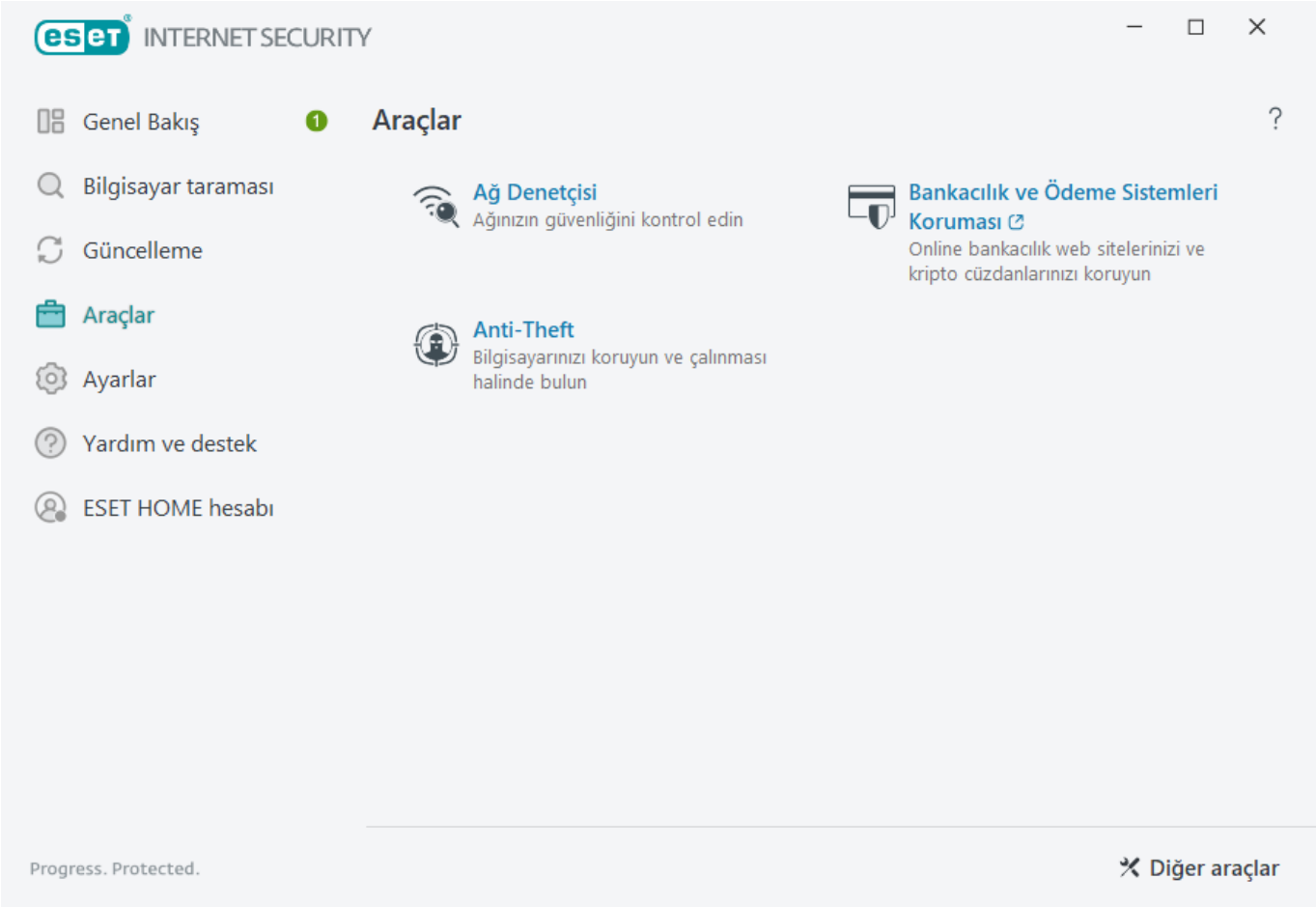
ESET Internet Security ürününü yeni bir sürüme güncelledikten sonra bilgisayarın yeniden başlatılması gerekir. ESET Internet Security yeni sürümleri, iyileştirmeleri uygulayacak veya program modüllerinin otomatik güncellemelerinin çözemediği sorunları düzeltecek şekilde tasarlanmıştır.

ESET Internet Security yeni sürümü program güncelleme ayarlarınıza göre otomatik olarak veya yeni bir sürümü indirerek ve önceki sürümün üzerine yükleyerek manuel olarak yüklenebilir.

Bilgisayarınızı yeniden başlatmak için **Şimdi yeniden başlat**'ı tıklayın. Bilgisayarınızı daha sonra yeniden başlatmayı planlıyorsanız **Daha sonra hatırlat**'ı tıklayın. Daha sonra, ana program penceresindeki **Genel bakış** bölümünden bilgisayarınızı manuel olarak yeniden başlatabilirsiniz.

Araçlar

Araçlar menüsü, program yönetimini basitleştirmeye yardımcı olan ve ileri düzey kullanıcılar için ek seçenekler sunan modüller içerir.



Ağ Denetçisi - Bir ağa bağlanırken güvenlik sorunları riskini azaltın.

Bankacılık ve Ödeme Sistemleri Koruması - Varsayılan tarayıcınız güvenli bir modda açılır. ESET Internet

Security aracı ödemelerinizi, bankacılık işlemlerinizi ve favori tarayıcınızdaki hassas verilerinizi korur.

 Anti-Theft - Kayıp veya çalıntı durumunda kayıp cihazınızı tespit edin ve koruyun.

Bilgisayarınızı korumak için diğer araçları görüntülemek üzere Diğer araçlar'ı (Karantina gibi) tıklayın.

Ağ Denetçisi

Ağ Denetçisi, güvenli (ev veya iş yeri) ağınızdaki güvenlik açıklarını (örneğin, açık bağlantı noktaları veya zayıf yönlendirici parolası) belirlemeye yardımcı olabilir. Ayrıca ağınıza nelerin bağlı olduğunu göstermek için (örneğin oyun konsolu, IoT veya diğer akıllı ev cihazları) cihaz türüne göre (örneğin yazıcı, yönlendirici, mobil cihaz vs.) sınıflandırılan bağlı cihazların bir listesini sağlar.

Ağ Denetçisi, bir yönlendiricinin güvenlik açıklarını tespit etmenize yardımcı olur ve bir ağa bağlanıldığında koruma düzeyinizi artırır.

Ağ Denetçisi yönlendiricinizi sizin için yeniden yapılandırmaz. Yönlendiricinizin özel arabirimini kullanarak değişiklikleri kendiniz yaparsınız. Ev yönlendiricileri dağıtılan hizmet dışı saldırılarını (DDoS) başlatmak için kullanılan zararlı yazılımlara karşı son derece savunmasız olabilir. Yönlendirici parolası kullanıcı tarafından varsayılan değerinden başka bir değere değiştirilmezse saldırganların tahmin etmesi kolaylaşır ve saldırganlar yönlendiricinize giriş yapıp ağınızı tehlikeye düşürmek için yeniden yapılandırabilirler.

Yeterince uzun olan güçlü bir parola oluşturmanızı ve parolanın sayı, simge veya büyük harf içermesini önemle tavsiye ederiz. Parolanın kırılmasını zorlaştırmak için farklı türde karakterleri karışık olarak kulanın.

Bağlı olduğunuz ağ güvenli olarak yapılandırılmışsa ağı "Ağım" olarak işaretleyebilirsiniz. Ağa bir Ağım etiketi eklemek için **"Ağım" olarak işaretle**'yi tıklayın. Daha iyi tanımlama ve güvenlik genel bakışı için ESET Internet Security kullanımı boyunca bu etiket ağın yanında gösterilir. Etiketi kaldırmak için **"Ağım" etiketini kaldır** seçeneğini tıklayın.

Ağınıza bağlanan her cihaz, temel bilgileriyle birlikte bir liste görünümünde gösterilir. Cihazı düzenlemek veya cihazla ilgili ayrıntılı bilgileri görüntülemek için ilgili cihazı tıklayın.

Ağlar açılır menüsü, cihazları aşağıdaki kriterlere göre filtrelemenize olanak tanır:

- Belirli bir ağa bağlanan cihazlar
- **Tüm ağlara** bağlanan cihazlar
- Sınıflandırılmamış aygıtlar

Tüm bağlı cihazları sonar görünümde görmek için sonar simgesini tıklayın. Ağ adı ve görüntülendiği son tarih gibi temel bilgileri görmek için imlecinizle cihaz simgesinin üzerine gelin.

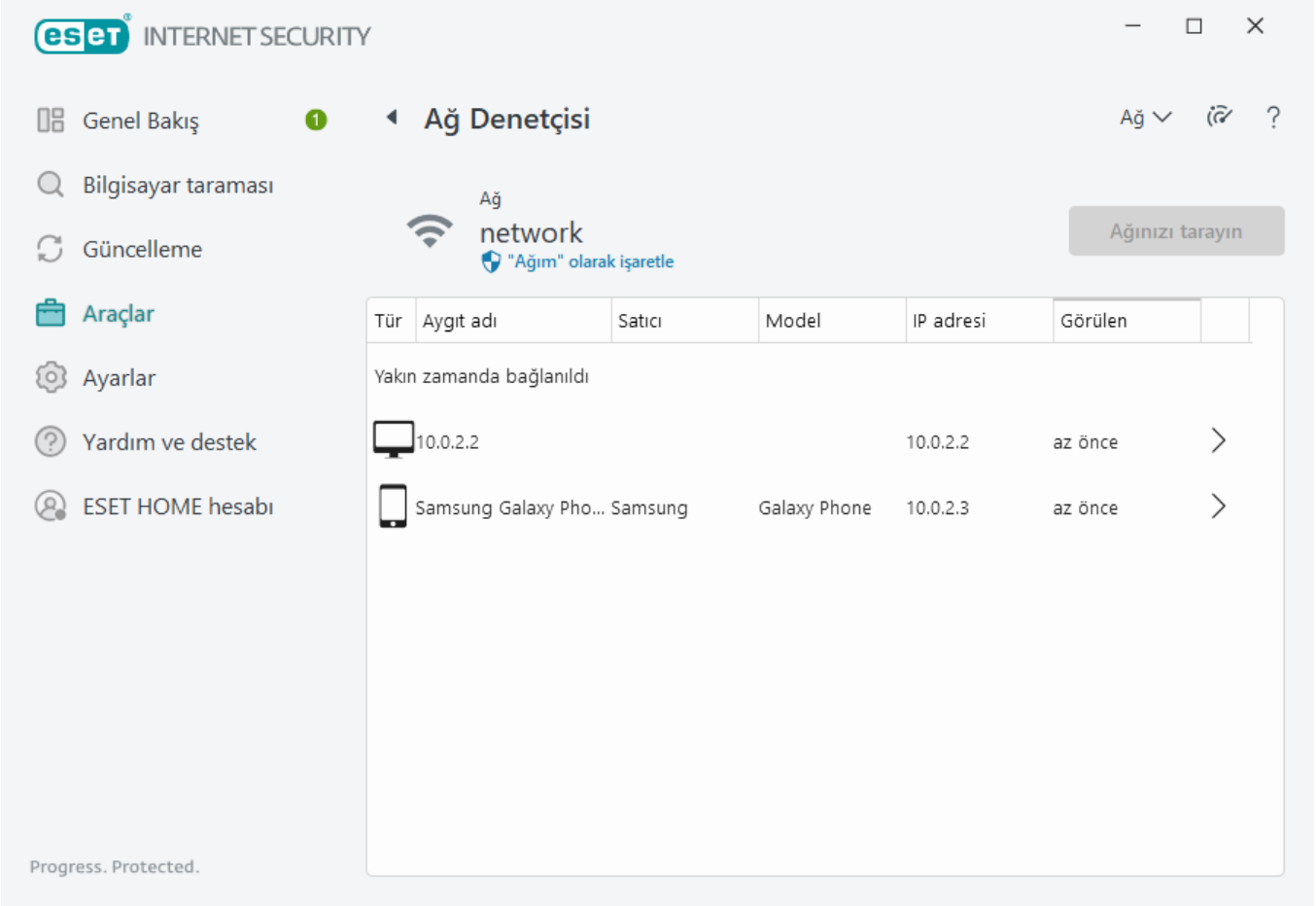
Cihazı düzenlemek veya cihazla ilgili detaylı bilgileri görüntülemek için cihaz simgesini tıklayın. Bu sayede, söz konusu cihazları kolayca tespit edebilirsiniz.

Halihazırda bağlı bulunduğunuz yönlendiriciyi manuel olarak taramak için **Ağınızı tarayın**'ı tıklayın. **Ağınızı tarayın**, yalnızca güvenilir bir ağ için kullanılabilir. Ağ ayarlarınızı gözden geçirmek veya düzenlemek için Bilinen ağlar'a bakın.

Aşağıdaki tarama türleri arasından seçim yapabilirsiniz:

- Her şeyi tara
- Yalnızca yönlendiriciyi tara
- Yalnızca aygıtları tara

Ağ taramalarını yalnızca güvenilir ağ üzerinde gerçekleştirin! Bu işlemi güvenilir olmayan ağlarda yaparsanız olası tehlikeyi dikkate alın.



Tarama işlemi tamamlandığında aygıtla ilgili temel bilgileri içeren bir bildirim gösterilir veya listedeki ya da sonar görünümdeki şüpheli aygıtı çift tıklayabilirsiniz. Yakın zamanda engellenen iletişimleri görmek için **Sorun giderme**'yi tıklayın. Güvenlik duvarı sorunlarını giderme hakkında daha fazla bilgi.

Ağ Denetçisi modülü tarafından gösterilen iki tür bildirim vardır:

- **Ağa bağlanan yeni aygıt** – Kullanıcı bağlıyken daha önce görülmemiş bir aygıt ağa bağlanırsa görüntülenir.
- **Yeni ağ cihazı bulundu** - Güvenilir ağınıza yeniden bağlanırsanız ve daha önce görülmemiş bir cihaz ortaya çıktığında bu uyarı görüntülenir.

İki bildirim türü de yetkisiz bir cihazın ağınıza bağlanmaya çalıştığını bildirir. Cihaz ayrıntılarının gösterilmesi için **cihazı göster** tıklayın.

Ağ Denetçisi'ndeki cihazlarda yer alan simgeler ne anlama gelir?

	Sarı yıldız simgesi, ağa yeni gelen veya ESET tarafından ilk kez algılanan cihazları gösterir.
	Sarı uyarı simgesi, yönlendiricinizin güvenlik açıkları içerebileceğini gösterir. Bu sorunla ilgili daha ayrıntılı bilgi için ürününüzdeki simgeyi tıklayın.
	Kırmızı uyarı simgesi, yönlendiricinizin güvenlik açıkları içerdiğini ve enfekte olmuş olabileceğini gösterir. Bu sorunla ilgili daha ayrıntılı bilgi için ürününüzdeki simgeyi tıklayın.
	ESET ürününüz yönlendiriciniz için ek bilgilere sahip olduğunda mavi simge gösterilebilir, ancak güvenlik riski bulunmadığından hemen dikkat etmenizi gerektirmez. Daha ayrıntılı bilgi için ürününüzdeki simgeyi tıklayın.

Ağ Denetçisi'nde ağ cihazı

Aygıtla ilgili, aşağıdakiler dahil olmak üzere ayrıntılı bilgiler burada bulunabilir:

- Aygıt adı
- Aygıt türü
- Son görülme zamanı
- Ağ adı
- IP adresi
- MAC adresi
- İşletim sistemi

Kalem simgesi, aygıt adını düzenleyebileceğiniz veya aygıt türünü değiştirebileceğiniz anlamına gelir.

Geçmişten kaldır - Cihazı cihaz listesinden silin. Bu seçenek yalnızca şu anda ağınıza bağlanmayan cihazlar için kullanılabilir.

Her cihaz türü için şu işlemler yapılabilir:

Yönlendirici

Yönlendirici ayarları – Yönlendirici ayarlarına web arayüzünden veya mobil uygulamadan erişebilir veya **Yönlendirici arayüzünü aç**'ı tıklayabilirsiniz. İnternet servis sağlayıcınız tarafından sağlanan bir yönlendiriciniz varsa algılanan güvenlik sorunlarını çözmek için internet servis sağlayıcınızın destek kaynaklarına veya yönlendiricinizin üreticisine başvurmanız gerekebilir. Her zaman, yönlendiricinizin dokümanlarında belirtildiği şekilde uygun güvenlik önlemlerini takip edin.
Koruma – Yönlendiricinizi ve ağınızı siber güvenlik saldırılarından korumak için şu temel önerileri uygulayın.

Ağ aygıtı

Cihaz tanımlama – Ağınıza bağlanan cihazdan emin değilseniz cihaz adının altındaki satıcı veya üretici adını kontrol edin. Bunun nasıl bir cihaz olduğunu tanımlamanıza yardımcı olabilir. Gelecek referanslar için cihazın adını değiştirebilirsiniz.
Cihazın bağlantısını kaldırma – Bağlı bir cihazın ağınız veya cihazlarınız için güvenli olduğundan emin değilseniz yönlendirici ayarlarınızda bu cihaz için ağ erişimini yönetin veya ağınızın parolasını değiştirin.
Koruma – Cihazınızı saldırılardan ve zararlı yazılımlardan korumak için cihazınıza siber güvenlik koruması yükleyin ve işletim sisteminizi ve yüklenen yazılımı daima güncel tutun. Korunmaya devam etmek için güvenilir olmayan Wi-Fi ağlarına bağlanmayın.

Bu cihaz

Bu cihaz ağda bilgisayarınızı temsil etmektedir.
Ağ bağdaştırıcıları – Ağ bağdaştırıcıları bilgilerinizi gösterin.

Bildirimler | Ağ Denetçisi

ESET Internet Security, yönlendiricinizde bir güvenlik açığı sorunu tespit ettiğinde gösterilebilecek çeşitli bildirimler aşağıda verilmiştir. Her bildirim, kısa bir açıklama içerir ve yönlendiricinizde güvenlik açığı riskini en düşük düzeye indirmek için başvurulabilecek çözümleri veya atılacak adımları sunar. Yönlendirici değişiklikleri hakkında bilginiz yoksa yönlendirici üreticinize veya internet sağlayıcınıza ulaşmanızı öneririz.

Olası güvenlik açığı bulundu
Yönlendiriciniz, saldırıları veya saldırılara açık hale gelmeyi kolaylaştıracak bilinen güvenlik açıkları içerebilir. Yönlendiricinizin bellenimini güncelleyin.

Güvenlik açığı bulundu
Yönlendiriciniz, saldırıları veya saldırılara açık hale gelmeyi kolaylaştıracak bilinen güvenlik açıklarını içeriyor. Yönlendiricinizin bellenimini güncelleyin.

Tehdit bulundu
Yönlendiriciniz zararlı bir yazılımdan etkilendi. Yönlendiricinizi yeniden başlatın ve taramayı tekrarlayın.

Zayıf yönlendirici parolası
Yönlendiricinizin parolası zayıf ve başka biri tarafından kolayca tahmin edilebilir. Yönlendiricinizin parolasını değiştirin.

Kötü amaçlı ağ yeniden yönlendirmesi
İnternet trafiğinizin kötü amaçlı web sitelerine yönlendirildiği görülüyor. Bu, yönlendiricinizin tehlikeye düştüğü anlamına gelebilir. Yönlendiricinizin DNS sunucusu ayarını değiştirin.

Açık ağ hizmetleri
Yönlendiriciniz başkaları tarafından kötüye kullanılabilecek ağ hizmetleri çalıştırıyor. Bu, zayıf yapılandırmadan veya tehlikeye düşmüş bir yönlendiriciden kaynaklanıyor olabilir. Yönlendiricinizin yapılandırmasını kontrol edin.

Açık hassas ağ hizmetleri
Yönlendiriciniz başkaları tarafından kötüye kullanılabilecek hassas ağ hizmetleri çalıştırıyor. Bu, zayıf yapılandırmadan veya tehlikeye düşmüş bir yönlendiriciden kaynaklanıyor olabilir. Yönlendiricinizin yapılandırmasını kontrol edin.

Eski bellenim
Yönlendiricinizdeki bellenim eski ve güvenlik açıkları içerebilir. Yönlendiricinizin bellenimini güncelleyin.

Kötü amaçlı yönlendirici ayarı
Kullandığınız bu DNS sunucusu kötü amaçlı ve sizi tehlikeli web sitelerine yönlendirebilir. Bu, yönlendiricinizin tehlikeye düştüğü anlamına gelebilir. Yönlendiricinizin DNS sunucusu ayarını değiştirin.

Ağ hizmetleri
Yönlendiriciniz genel ağ hizmetlerini çalıştırıyor. Bunlar ağ için gerekli olup muhtemelen güvenlidir. Yönlendiricinizin yapılandırmasını kontrol edin.

ESET Internet Security içindeki araçlar

Araçlar menüsü, program yönetimini basitleştirmeye yardımcı olan ve ileri düzey kullanıcılar için ek seçenekler sunan modüller içerir. Bu araçlar yalnızca sağ alttaki **Diğer araçlar**'ı tıklarsanız görünür.

Bu menüde şu araçlar bulunur:

 Günlük dosyaları

 Güvenlik raporu

 Çalışan işlemler (ESET Internet Security ürününde ESET LiveGrid® etkinse)

 Ağ bağlantıları (Kişisel güvenlik duvarı ESET Internet Security ürününde etkinse)

 ESET SysInspector

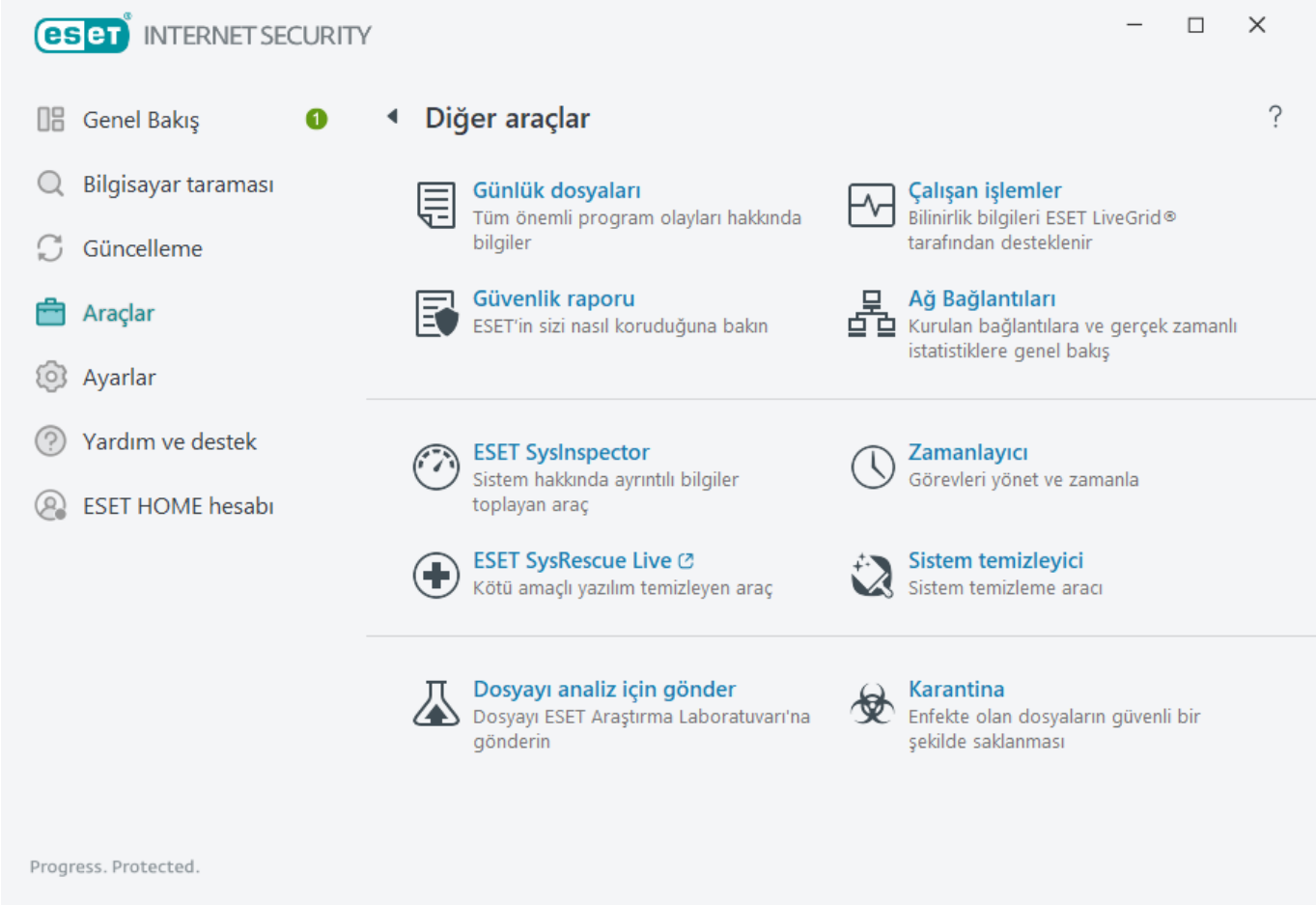
 ESET SysRescue Live - Sizi ESET SysRescue Live sayfasına yönlendirir, burada ESET SysRescue Live .iso CD/DVD resmini indirebilirsiniz.

 Zamanlayıcı

 Sistem temizleyici – Tehdidi temizledikten sonra bilgisayarı kullanılabilir bir duruma geri yüklemenize yardımcı olur.

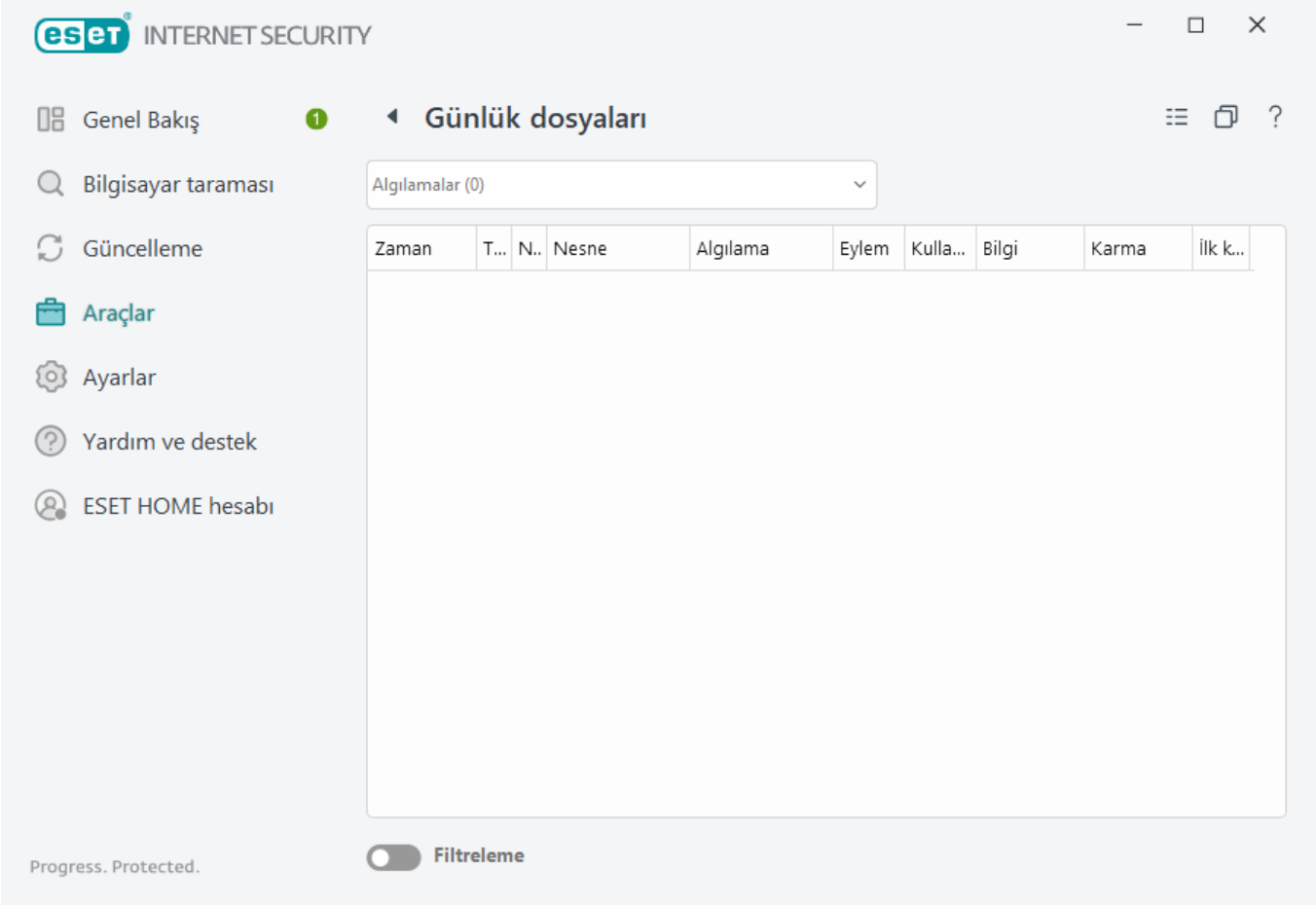
 Dosyayı analiz için gönder – Şüpheli bir dosyayı analiz için ESET Araştırma Laboratuvarı'na göndermenizi sağlar (ESET LiveGrid® yapılandırmanıza bağlı olarak kullanılamayabilir).

 Karantina



Günlük dosyaları

Günlük dosyaları, gerçekleşen önemli program olayları hakkında bilgi içerir ve algılanan tehditlere genel bir bakış sağlar. Günlüğe kaydetme işlemi, sistem çözümlemesi, tehdit algılama ve sorun giderme işlemlerinin önemli bir parçasıdır. Günlüğe kaydetme işlemi herhangi bir kullanıcı müdahalesi olmadan arka planda etkin biçimde gerçekleşir. Bilgiler, geçerli günlük ayrıntı ayarlarına göre kaydedilir. Doğrudan ESET Internet Security içinden metin iletileri ile günlükleri görüntülemek ve günlükleri arşivlemek mümkündür.



Günlük dosyalarına, ana program menüsünden **Araçlar** > **Diğer araçlar** > **Günlük dosyaları**. Günlük açılır menüsünden istediğiniz günlük türünü seçin.

- **Tespitler** – Bu günlük, ESET Internet Security tarafından algılanan tespitler ve sızıntılar hakkında ayrıntılı bilgiler sunar. Günlük bilgileri tespit zamanı, tarayıcı türü, nesne türü, nesnenin konumu, tespit adı, yapılan işlem ve sızıntı tespit edildiğinde oturum açmış olan kullanıcının adı, hash ve ilk gerçekleşme zamanını içerir. Temizlenmeyen sızıntılar her zaman, açık kırmızı arka planda kırmızı metinle belirtilir. Temizlenen sızıntılar ise beyaz arka planda sarı metinle belirtilir. Temizlenmeyen PUA'lar veya Tehlikeli olabilecek uygulamalar beyaz arka planda sarı metinle belirtilir.

- **Olaylar** – ESET Internet Security tarafından gerçekleştirilen tüm önemli işlemler, Olay günlüklerine kaydedilir. Olay günlüğünde olaylarla ilgili bilgiler ve programda oluşan hatalar bulunur. Sistem yöneticilerinin ve kullanıcıların sorunları çözmesi için tasarlanmıştır. Burada bulunan bilgiler genellikle programda oluşan bir soruna çözüm bulmanıza yardımcı olabilir.

- **Bilgisayar taraması** - Önceki taramaların tümünün sonuçları bu pencerede görüntülenir. Her satır tek bir bilgisayar denetimine karşılık gelir. Seçilen taramanın ayrıntılarını görmek için herhangi bir girişi çift tıklayın.

- **HIPS** – Kayıt için işaretlenmiş belirli HIPS kurallarının kayıtlarını içerir. Protokol, işlemi tetikleyen uygulamayı, sonucu (kuralın izin verilme veya yasaklanma durumu) ve kural adını gösterir.

- **Bankacılık ve Ödeme Sistemleri Koruması** - Tarayıcıya yüklenen doğrulanmamış/güvenilmeyen dosyaların kayıtlarını içerir.

- **Ağ koruması** – Ağ koruması günlüğü Güvenlik Duvarı, Ağ saldırısına karşı koruma (IDS) ve Botnet koruması tarafından tespit edilen tüm uzaktan saldırıları görüntüler. Burada bilgisayarınıza yapılan tüm saldırılarla ilgili bilgileri bulabilirsiniz. Olay sütununda tespit edilen saldırılar listelenir. Kaynak sütununda, saldırgan hakkında

daha fazla bilgi verilir. Protokol sütununda, saldırı için kullanılan iletişim protokolü gösterilir. Ağ koruması günlüğünün analizi, sisteminize yetkisiz erişimi engellemek için zaman içinde sisteme yönelik gerçekleştirilen sızıntı girişimlerini tespit etmenize yardımcı olur. Ağ saldırıları ile ilgili daha fazla ayrıntı için IDS ve gelişmiş seçenekler bölümüne bakın.

- **Filtrelenen web siteleri** -Web erişimi koruması veya Ebeveyn kontrolü tarafından engellenmiş web sitelerinin listesini görüntülemek isterseniz bu liste faydalıdır. Her günlük saat, URL adresi, kullanıcı ve belirli bir web sitesi ile bağlantı kuran uygulamayı içerir.

- **Antispam koruması** – İstenmeyen posta olarak işaretlenen e-posta iletileriyle ilgili kayıtları içerir.

- **Ebeveyn kontrolü** - Ebeveyn kontrolü tarafından engellenen veya izin verilen web sayfalarını gösterir. Eşleşme türü ve Eşleşme değerleri sütunları filtreleme kurallarının nasıl uygulandığını gösterir.

- **Aygıt denetimi** – Bilgisayara bağlanan çıkarılabilir medya veya aygıtların kayıtlarını içerir. Yalnızca ilgili Aygıt denetimi kurallarına sahip aygıtlar günlük dosyasına kaydedilir. Kural, bağlı bir aygıtla eşleşmiyorsa, bağlı aygıta yönelik bir günlük girdisi oluşturulmaz. Ayrıca aygıt türü, seri numarası, satıcı adı ve medya boyutu (varsa) gibi ayrıntılara da bakabilirsiniz.

- **Web kamerası koruması** - Web kamerası koruması tarafından engellenen uygulamalarla ilgili kayıtları içerir.

Herhangi bir günlüğün içeriklerini seçin ve panoya kopyalamak için **CTRL + C** kısayoluna basın. Birden çok giriş seçmek için **CTRL** veya **SHIFT** tuşlarını basılı tutun.

Filtreleme öğesini tıklatarak filtreleme ölçütlerini tanımlayabileceğiniz Günlük filtreleme penceresini açabilirsiniz.

İçerik menüsünü açmak için belirli bir kaydı sağ tıklatın. İçerik menüsünde aşağıdaki seçenekler bulunur:

- **Göster**– Yeni bir pencerede, seçilen günlük hakkında daha ayrıntılı bilgileri görüntüler.

- **Aynı kayıtları filtrele** – Bu filtreyi etkinleştirdikten sonra yalnızca aynı türdeki kayıtları (tanılama, uyarılar, ...) görürsünüz.

- **Filtrele** - Bu seçeneği tıkladıktan sonra Günlük filtreleme penceresi belirli günlük girişleri için filtreleme ölçütleri tanımlayabilmenize olanak tanır.

- **Filtreyi etkinleştir** – Filtre ayarlarını etkinleştirir.

- **Filtreyi devre dışı bırak** – Tüm filtre ayarlarını temizler (yukarıda açıklandığı şekilde).

- **Kopyala/Tümünü kopyala** - Seçili kayıtlarla ilgili bilgileri kopyalar.

- **Hücreyi kopyala** - Sağ tıklanan hücrenin içeriğini kopyalar.

- **Sil/Tümünü sil** - Seçili kayıtları veya görüntülenen tüm kayıtları siler. Bu işlem için yönetici ayrıcalıkları gereklidir.

- **Dışa aktar/Tümünü dışa aktar** - Seçili kayıtlar veya XML biçimindeki tüm kayıtlarla ilgili bilgiler dışa aktarılır.

- **Bul/Sonrakini bul/Öncekini bul** - Bu seçeneği tıklarsanız Günlük filtreleme penceresini kullanarak belirli

girişi vurgulamak için filtreleme ölçütleri tanımlayabilirsiniz.

- **Tespit açıklaması** - Kaydedilen sızıntının tehlikeleri ve belirtileri ile ilgili ayrıntılı bilgiler içeren ESET Tehdit Ansiklopedisi açılır.

- **Tarama dışı öğe oluştur** – Bir sihirbaz kullanarak yeni bir Algılamayla ilgili tarama dışı bırakma işlemi oluşturun (Zararlı yazılım algılamaları için kullanılamaz).

Günlük filtreleme

Filtreleme kriterlerini tanımlamak için **Filtreleme**'yi tıklayın (**Araçlar** > **Diğer araçlar** > **Günlük dosyaları** bölümünde yer alır).

Günlük filtreleme özelliği, özellikle çok fazla kayıt olduğunda aradığınız bilgileri bulmanıza yardımcı olur. Günlük kayıtlarını daraltmanıza olanak tanır, örneğin belirli bir olay türü, durum veya zaman aralığı için arama yaparken. Belirli arama seçeneklerini belirterek günlük kayıtlarını filtreleyebilirsiniz. Günlük dosyaları penceresinde yalnızca alakalı olan kayıtlar (arama seçeneklerine göre) gösterilir.

Metin bul alanına aradığınız anahtar kelimeyi girin. Aramanızı daraltmak için **Sütunlarda ara** açılır menüsünü kullanın. **Kayıt günlük türleri** açılır menüsünden bir veya iki kayıt seçin. Sonuçlar görmek istediğiniz **Zaman dilimini** tanımlayın. Ayrıca **Yalnızca tam sözcükleri eşleştir** veya **Büyük küçük harf duyarlı** gibi diğer arama seçeneklerini de kullanabilirsiniz.

Metin bul

Bir dize girin (kelime veya kelimenin bir bölümü). Sadece bu dizeyi içeren kayıtlar gösterilir. Diğerleri sonuçlar arasına alınmaz.

Sütunlarda ara

Arama yaparken hangi sütunların dikkate alınacağını seçin. Arama için kullanılacak bir veya daha fazla sütun işaretleyebilirsiniz.

Kayıt türleri

Açılır menüden bir veya daha fazla kayıt günlüğü türü seçin:

- **Tanılama** – Programla ilgili hassas ayarlama gerektiren bilgileri ve yukarıdaki tüm kayıtları günlüğe kaydeder.

- **Bilgilendirici** – Başarılı güncelleme iletileri dahil olmak üzere bilgilendirici iletileri ve yukarıdaki tüm kayıtları kaydeder.

- **Uyarılar** – Kritik hataları ve uyarı iletilerini kaydeder.

- **Hatalar** – "Dosya indirme hatası" gibi hatalar ve kritik hatalar kaydedilir.

- **Kritik** – Yalnızca kritik hatalar (Antivirus korumasını,

Zaman dilimi

Görüntülenmesini istediğiniz sonuçların ait olduğu zaman dilimini tanımlayın.

- **Belirtilmiyor** (varsayılan) - Zaman diliminde arama yapmaz, tüm günlükte arar.
- **Son gün**
- **Son hafta**
- **Son ay**
- **Zaman dilimi** - Yalnızca belirtilen zaman dilimindeki kayıtları filtrelemek için tam zaman dilimini (Başlangıç: ve Bitiş:) belirtebilirsiniz.

Yalnızca tam sözcükleri eşleştir

Daha hassas sonuçlar için tam sözcükleri aramak istiyorsanız onay kutusunu işaretleyin.

Büyük küçük harf duyarlı

Filtreleme sırasında büyük/küçük harf sizin için önemliyse bu seçeneği etkinleştirin. Filtreleme/arama seçeneklerini yapılandırdıktan sonra filtrelenen günlük kayıtlarını görmek için **Tamam**'ı veya aramaya başlamak için **Bul**'u tıklayın. Günlük dosyaları mevcut konumunuzdan (vurgulanan kayıttan) başlayarak yukarıdan aşağı doğru aranır. İlk ilgili kayıt bulunduğunda arama durur. Bir sonraki kaydı aramak için **F3**'e basın veya arama seçeneklerinizi hassaslaştırmak için sağ tıklayıp **Bul**'u seçin.

Günlüğe Kaydetme Yapılandırması

ESET Internet Security günlük yapılandırmasına, ana program penceresinden erişilebilir. **Ayarlar** > **Gelişmiş Ayarlar** > **Araçlar** > **Günlük dosyaları** öğesini tıklatın. Günlük bölümü günlüklerin nasıl yönetileceğini belirlemek için kullanılır. Program sabit disk alanından tasarruf etmek için eski günlükleri otomatik olarak siler. Günlük dosyaları için aşağıdaki seçenekleri belirleyebilirsiniz:

En düşük günlük ayrıntı düzeyi - Günlüğe kaydedilecek olayların en düşük ayrıntı düzeyini belirtir:

- **Tanılama** – Programla ilgili hassas ayarlama gerektiren bilgileri ve yukarıdaki tüm kayıtları günlüğe kaydeder.
- **Bilgilendirici** – Başarılı güncelleme iletileri dahil olmak üzere bilgilendirici iletileri ve yukarıdaki tüm kayıtları kaydeder.
- **Uyarılar** – Kritik hataları ve uyarı iletilerini kaydeder.
- **Hatalar** – "Dosya indirme hatası" gibi hatalar ve kritik hatalar kaydedilir.
- **Kritik** - Yalnızca kritik hatalar (Antivirus korumasını,, Güvenlik duvarıvb.) günlüğe kaydedilir.

Engellenen tüm bağlantılar Tanılama ayrıntı düzeyini seçtiğinizde kaydedilir.

(Gün) günden eski kayıtları otomatik olarak sil alanında belirtilen günden daha eski günlük girişleri otomatik silinir.

Günlük dosyalarını otomatik olarak en iyi duruma getir – Bu seçenek işaretlendiğinde, **Kullanılmayan kayıt sayısı şu değeri aşarsa (%)** alanında belirtilen değerden fazlaysa, günlük dosyaları otomatik olarak birleştirilir.

Günlüklerin birleştirilmesi işlemini başlatmak için **En iyi duruma getir** seçeneğini tıklatın. Bu işlem sırasında tüm boş günlük girdileri kaldırılır, böylece performans ve günlük işleme hızı artar. Bu iyileşme özellikle çok sayıda girdi içeren günlüklerde belirgin olarak gözlenir.

Günlük dosyaları'ndan farklı dosya biçimlerinde günlükleri depolamayı etkinleştirmek için **Metin protokolünü etkinleştir** seçeneğini etkinleştirin:

- **Hedef dizin** – Günlük dosyalarının depolanacağı dizin (yalnızca Metin/CSV için geçerlidir). Her günlük bölümünün önceden tanımlı dosya adına sahip kendi dosyası vardır (örneğin, günlükleri depolamak için düz metin dosya biçimi kullanıyorsanız günlük dosyalarının **Algılamalar** bölümü için virlog.txt kullanılır).

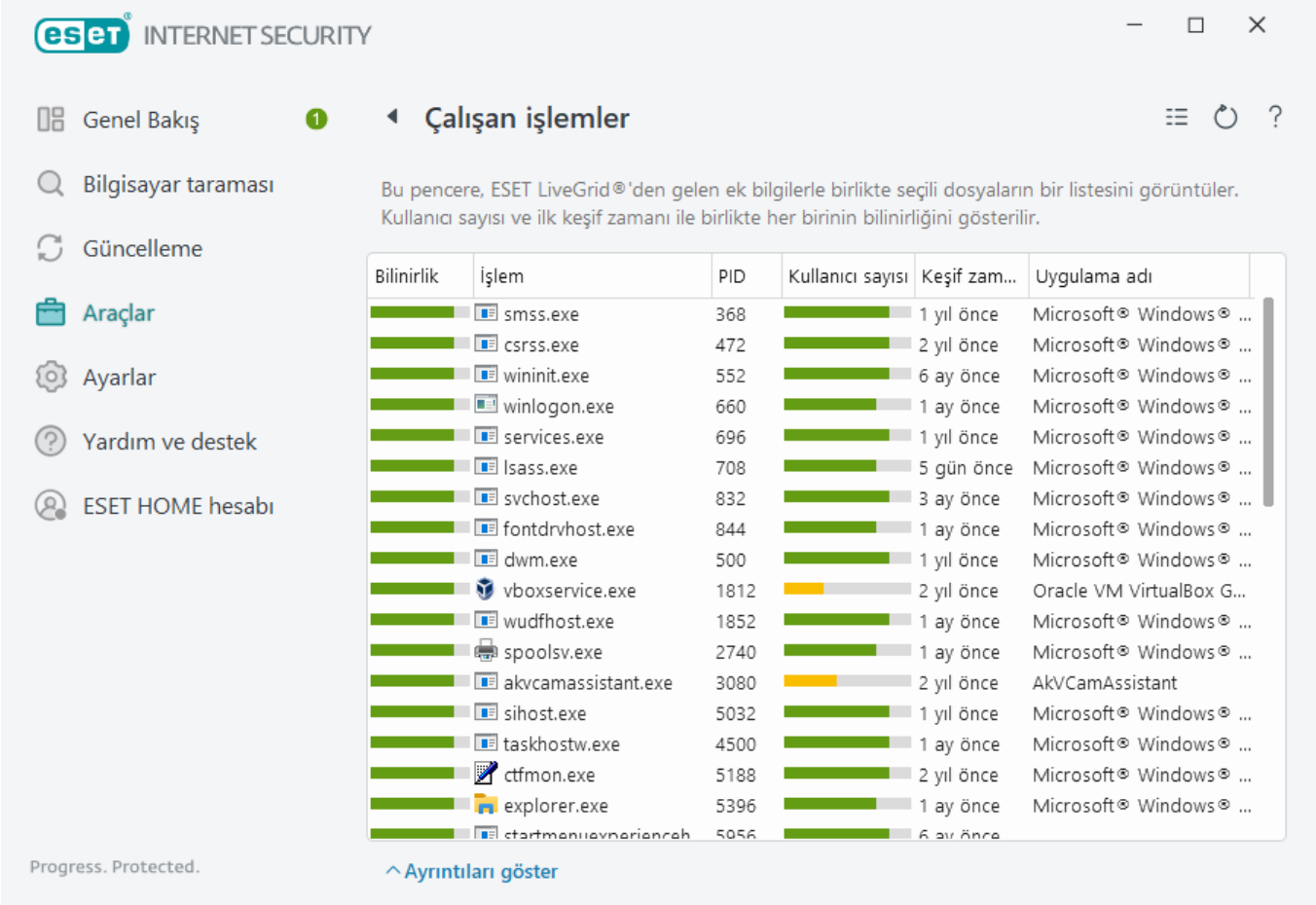
- **Tür** – **Metin** dosyası biçimini seçerseniz, günlükler bir metin dosyasına depolanır ve veriler ayrı ayrı sekmeler haline getirilir. Aynısı, virgülle ayrılan **CSV** dosya biçimi için de uygulanır. **Olay** seçeneğini belirlerseniz günlükler, dosya yerine Windows Olay günlüğüne depolanır (Denetim masasındaki Olay Görüntüleyici kullanılarak görüntülenebilir).

- **Tüm günlük dosyalarını sil** – **Tür** açılır menüsünde seçili olan depolanmış günlüklerin tamamını siler. Günlüklerin başarılı bir şekilde silinmesinin ardından bir bildirim gösterilir.

> Sorunları daha hızlı çözmeye yardımcı olmak adına ESET bilgisayarınızdan günlükler sağlamanızı isteyebilir. ESET Log Collector, istenen bilgileri toplamanızı kolaylaştırır. ESET Log Collector hakkında daha fazla bilgi için lütfen ESET Bilgi Bankası makalemize bakın.

Çalışan işlemler

Çalışan işlemler, bilgisayarınızda çalışan programları veya işlemleri görüntüler ve ESET'i hemen ve sürekli olarak yeni sızıntılarla ilgili bilgilendirir. ESET Internet Security, kullanıcıları ESET LiveGrid® teknolojisiyle korumak için çalışan işlemlerle ilgili ayrıntılı bilgi sağlar.



Bilinirlik – Çoğu durumda, ESET Internet Security ve ESET LiveGrid® teknolojisi, her nesnenin özelliklerini inceleyen ve ardından nesnenin kötü amaçlı etkinlik olasılığını ölçen bir sezgisel tarama kuralı dizisini kullanarak nesnelere (dosyalar, işlemler, kayıt defteri anahtarları vb.) risk seviyeleri atar. Bu sezgisel taramalar esas alınarak nesnelere 1 - İyi (yeşil) ile 9 - Riskli (kırmızı) arasında bir risk düzeyi atanır.

Süreç – Halihazırda bilgisayarınızda çalışan programın veya işlemin görüntü adı. Ayrıca, bilgisayarınızda çalışmakta olan tüm işlemleri görmek için Windows Görev Yöneticisini de kullanabilirsiniz. Görev Yöneticisi'ni açmak için görev çubuğunda boş bir alanı sağ tıklatıp ardından **Görev Yöneticisi**'ni tıklatın veya klavyenizde **Ctrl**+**Shift**+**Esc** tuşlarına basın.

İyi (yeşil) olarak işaretlenmiş olan bilinen uygulamalar kesinlikle temizdir (beyaz listeye alınmıştır) ve performansı artırmak için tarama dışında bırakılırlar.

PID – İşlem tanıtma numarası işlemin önceliğini ayarlama gibi çeşitli işlevlerde parametre olarak kullanılabilir.

Kullanıcı sayısı – Belirli bir uygulamayı kullanan kullanıcıların sayısı. Bu bilgiler ESET LiveGrid® teknolojisiyle toplanır.

Keşif zamanı – Uygulamanın ESET LiveGrid® teknolojisi tarafından tespit edilmesinden o ana kadar geçen süre.

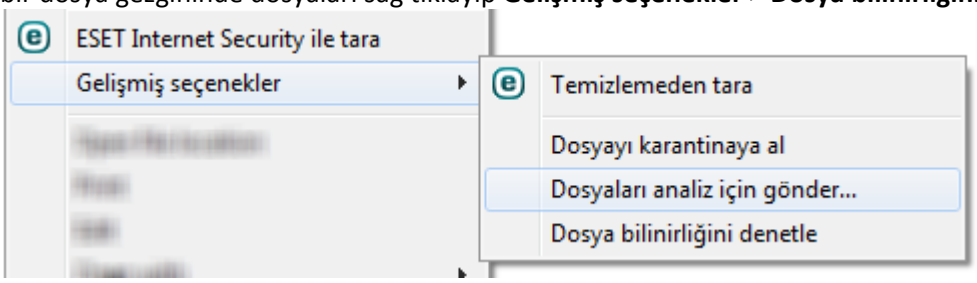
Bilinmiyor (turuncu) olarak işaretlenen bir uygulama kötü amaçlı yazılım olmayabilir. Bu genellikle daha yeni bir uygulamadır. Dosyadan emin değilseniz ESET Araştırma Laboratuvarına dosyayı analiz için gönderebilirsiniz. Dosyanın kötü amaçlı bir uygulama veya web sitesi olduğu belirlenirse, bu dosyanın algılanması gelecek güncellemeye eklenir.

Uygulama adı – Bir programın veya işlemin adı.

Bir uygulamayla ilgili şu bilgileri görüntülemek için söz konusu uygulamayı tıklatın:

- **Yol** – Bilgisayarınızdaki bir uygulamanın konumu.
- **Boyut** – kB (kilobayt) veya MB (megabayt) cinsinden dosya boyutu.
- **Açıklama** – İşletim sistemindeki açıklamaya dayalı dosya özellikleri.
- **Şirket** – Satıcının veya uygulama işleminin adı.
- **Sürüm** – Uygulama yayımcısından gelen bilgiler.
- **Ürün** – Uygulama adı ve/veya ticari ad.
- **Oluşturulma/Değiştirilme tarihi** - Oluşturulduğu (değiştirildiği) tarih ve saat.

Çalışan programlar/işlemler olarak işlev görmeyen dosyaların bilinirliğini de kontrol edebilirsiniz. Bunun için, bir dosya gezgininde dosyaları sağ tıklayıp **Gelişmiş seçenekler** > **Dosya bilinirliğini denetle**'yi tıklayın.



Güvenlik raporu

Bu özellik, şu kategoriler için istatistiklere genel bakış sunar:

- **Web sayfaları engellendi** – Engellenen web sayfalarının sayısını gösterir (PUA, kimlik avı, saldırıya uğrayan yönlendirici, IP veya sertifika için kara listeye alınan URL).
- **Enfekte olan e-posta nesneleri algılandı** – Algılanan, enfekte olmuş posta nesnelerinin sayısını gösterir.
- **Ebeveyn kontrolünde web sayfaları engellendi** – Ebeveyn kontrolünde engellenen web sayfalarının sayısını gösterir.
- **PUA algılandı** – İstenmeyen türden olabilecek uygulamaların (PUA) sayısını gösterir.
- **Spam e-postaları algılandı** – Algılanan spam e-postalarının sayısını gösterir.
- **Web kamerasına erişimler engellendi** – Web kamerasına yönelik engellenen erişim sayısını gösterir.
- **Korunan internet bankacılığı bağlantıları** – Bankacılık ve Ödeme koruması özelliği üzerinden korunan web sitesi erişimlerinin sayısını gösterir.
- **Kontrol edilen belgeler** – Taranan doküman nesnelerinin sayısını gösterir.
- **Taranan uygulamalar** – Taranan yürütülebilir nesnelerinin sayısını gösterir.
- **Kontrol edilen diğer nesneler** – Taranan diğer nesnelerin sayısını gösterir.

- **Taranan web sayfası nesneleri** – Taranan web sayfası nesnelerinin sayısını gösterir.
- **Taranan e-posta nesneleri** – Taranan e-posta nesnelerinin sayısını gösterir.

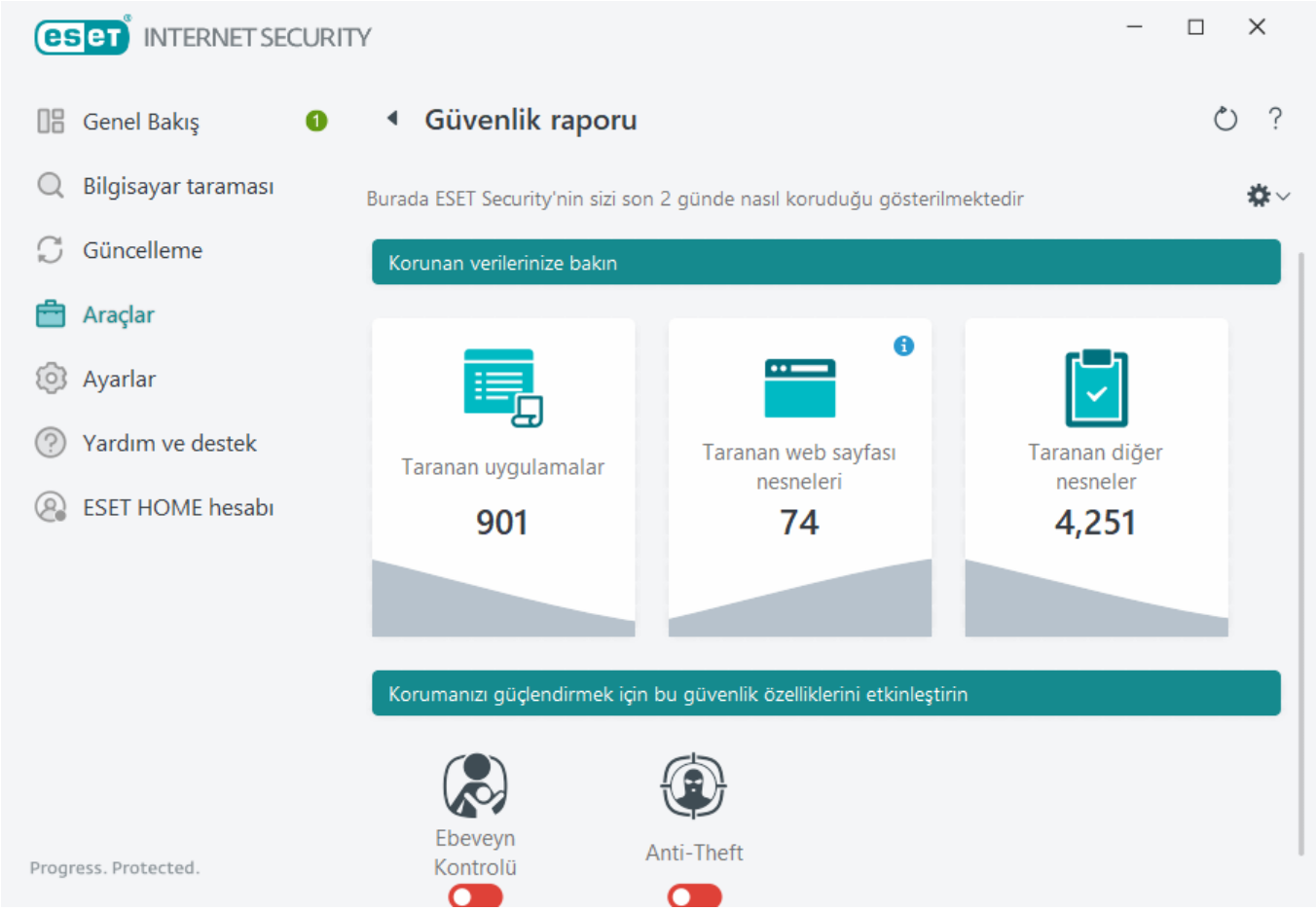
Bu kategorilerin sırası, en yüksekten en düşüğe olacak şekilde sayısal değer temelindedir. Sıfır değerine sahip kategoriler gösterilmez. Gizli kategorileri genişletmek ve görüntülemek için **Daha fazla** göster'i tıklayın.

Güvenlik raporunun son bölümü şu özellikleri etkinleştirme olanağı sunar:

- Ebeveyn Kontrolü
- Anti-Theft

Özellik etkinleştirildiğinde Güvenlik raporunda artık işlevsiz olarak gösterilmez.

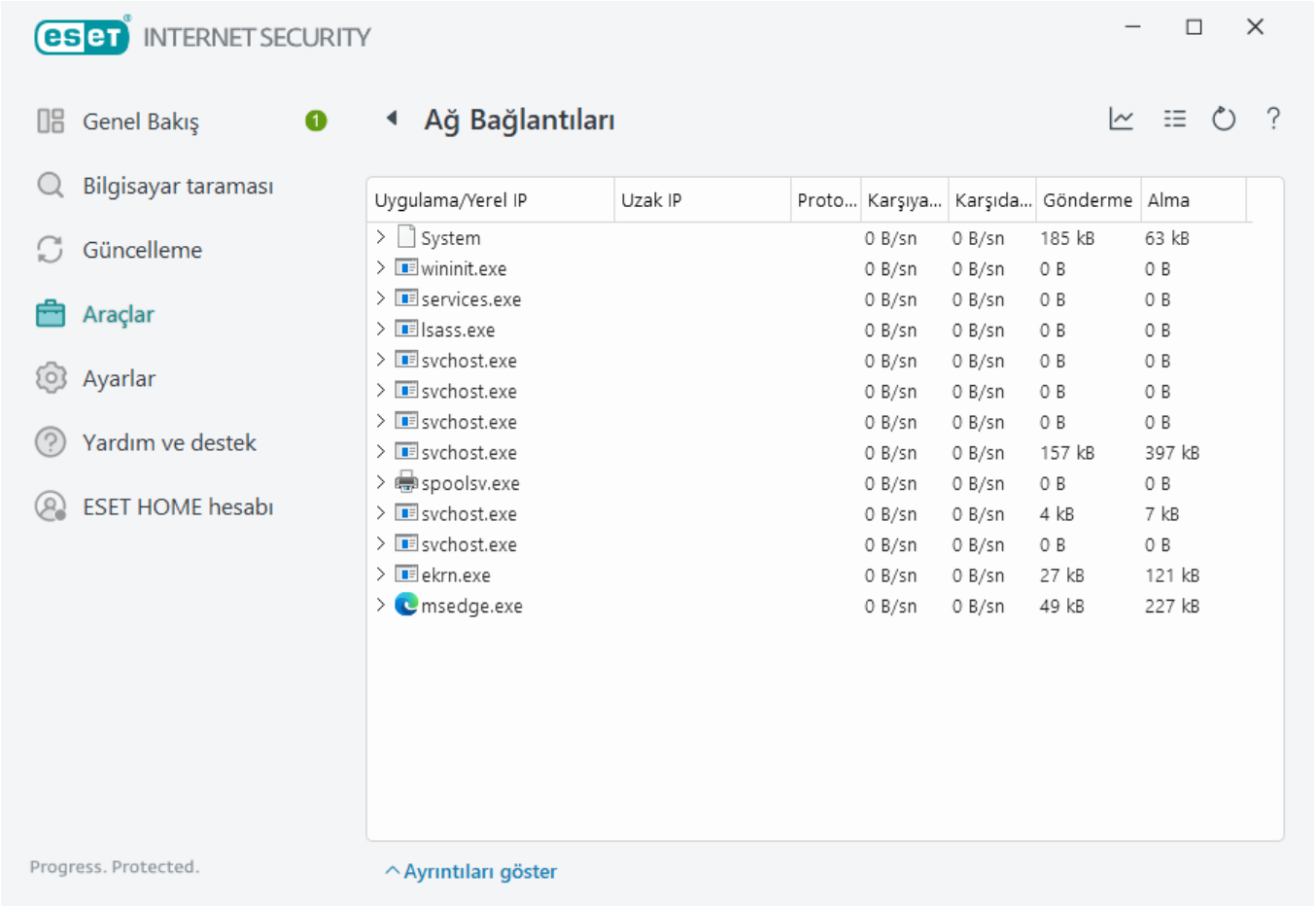
Sağ üst köşedeki dişli simgesini tıklayarak **Güvenlik raporu bildirimlerini etkinleştirebilir/devre dışı bırakabilir** veya verilerin son 30 gün boyunca ya da ürünün etkinleştirilmesinden bu yana gösterilmesini seçebilirsiniz. ESET Internet Security ürünü 30 günden kısa bir süre önce yüklenmişse, yalnızca yüklemeden sonraki gün sayısı seçilebilir. 30 günlük süre varsayılan olarak ayarlanmıştır.



Verileri sıfırla seçeneği, tüm istatistikleri temizler ve Güvenlik raporu için mevcut verileri siler. **İstatistikleri sıfırlamadan önce sor** seçeneğinin (**Gelişmiş ayarlar** > **Bildirimler** > **Etkileşimli uyarılar** > **Onay mesajları** > **Düzenle** altında) işaretini kaldırdığınız durumlar dışında bu işlemin onaylanması gerekir.

Ağ bağlantıları

Ağ bağlantıları bölümünde, etkin ve bekleyen bağlantıların listesini görebilirsiniz. Bu, giden bağlantı oluşturan tüm uygulamaları denetlemenize yardımcı olur.



Ağ etkinliğini açmak için grafik simgesini tıklayın.

Birinci satır, uygulamanın adını ve veri aktarım hızını görüntüler. Uygulama tarafından kurulan bağlantıların listesini (ve daha fazla ayrıntılı bilgileri) görmek için, **>** öğesini tıklayın.

Sütunlar

Uygulama/Yerel IP – Uygulamanın adı, yerel IP adresleri ve iletişim bağlantı noktaları.

Uzak IP – Belirli bir uzak bilgisayarın IP adresi ve bağlantı noktası numarası.

Protokol – Kullanılan aktarım protokolü.

Karşıya Yükleme Hızı/Karşıdan Yükleme Hızı – Giden ve gelen verilerin geçerli hızı.

Gönderildi/Alındı – Bağlantıda alınıp verilen veri miktarı.

Ayrıntıları göster - Seçili bağlantıyla ilgili ayrıntılı bilgi görüntülemek için bu seçeneği belirleyin.

Dahil olan ek seçenekleri görüntülemek için bağlantının üzerini sağ tıklatın:

Ana bilgisayar adlarını çözümle – Mümkünse tüm ağ adresleri, sayısal IP adresi biçiminde değil DNS biçiminde görüntülenir.

Yalnızca TCP bağlantılarını göster – Listede yalnızca TCP protokol paketine ait olan bağlantılar görüntülenir.

Dinleyen bağlantıları göster – Bu seçeneği yalnızca herhangi bir iletişimin kurulmadığı, ancak sistemin bir bağlantı noktası açtığı ve bağlantı kurmayı beklediği türden bağlantıları görüntülemek için belirleyin.

Bilgisayardaki bağlantıları göster – Bu seçeneği yalnızca uzak tarafın yerel sistem olduğu ve bu nedenle localhost olarak adlandırılan bağlantıları görüntülemek için belirleyin.

Yenileme hızı – Etkin bağlantıları yenileme sıklığını seçin.

Şimdi yenile – **Ağ bağlantıları** penceresini yeniden yükler.

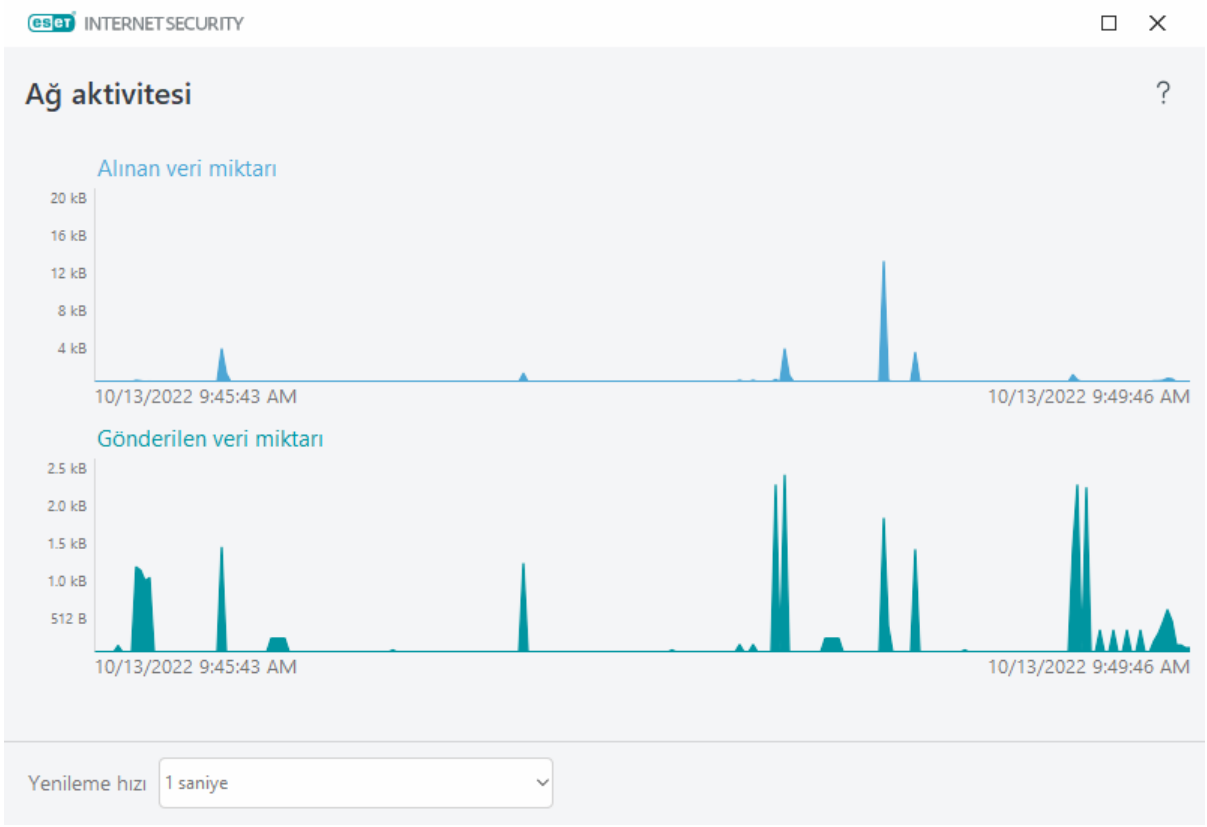
Aşağıdaki seçenekler, yalnızca bir uygulama veya işlem (etkin bağlantı değil) tıklatıldıktan sonra kullanılabilir:

İşlem için iletişimi geçici olarak reddet – Belirtilen uygulama için geçerli bağlantıları reddeder. Yeni bir bağlantı kurulduğunda, güvenlik duvarı önceden tanımlı bir kural kullanır. Ayarların açıklaması Kuralların yapılandırılması ve kullanılması bölümünde bulunabilir.

İşlem için iletişime geçici olarak izin ver – Belirtilen uygulama için geçerli bağlantılara izin verir. Yeni bir bağlantı kurulduğunda, güvenlik duvarı önceden tanımlı bir kural kullanır. Ayarların açıklaması Kuralların yapılandırılması ve kullanılması bölümünde bulunabilir.

Ağ aktivitesi

Geçerli **Ağ etkinliğini** grafik formunda görmek için **Araçlar** > **Diğer araçlar** > **Ağ bağlantıları**'nı tıklayın ve ardından grafik simgesini tıklayın. Grafiğin alt kısmında, seçilen zaman aralığına göre ağ etkinliğini gerçek zamanlı olarak kaydeden bir zaman çizelgesi yer alır. Zaman aralığı değiştirmek için **Yenileme hızı** açılır menüsünden uygun değeri seçin.



Aşağıdaki seçenekler kullanılabilir:

- **1 saniye** – Grafik her saniye yenilenir ve zaman çizelgesi son 4 dakikayı kapsar.
- **1 dakika (son 24 saat)** – Grafik her dakika yenilenir ve zaman çizelgesi son 24 saati kapsar.
- **1 saat (geçen ay)** – Grafik her saat yenilenir ve zaman çizelgesi son ayı kapsar.

Grafiğin dikey ekseni, alınan veya gönderilen veri miktarını temsil eder. Belirli bir zamanda tam olarak alınan/gönderilen verilerin miktarını görmek için farenizle grafiğin üzerine gelin.

ESET SysInspector

ESET SysInspector, bilgisayarınızın tamamını inceleyen, sürücüler ve uygulamalar, ağ bağlantıları veya önemli kayıt defteri girişleri gibi sistem bileşenleri hakkında ayrıntılı bilgiler toplayan ve her bileşenin risk düzeyini değerlendiren bir uygulamadır. Bu bilgiler, yazılım veya donanım uyumsuzluğundan ya da kötü amaçlı yazılımın etkilemesinden kaynaklanabilecek şüpheli sistem davranışının nedenini belirlemenize yardımcı olabilir. ESET SysInspector ürününü nasıl kullanabileceğinizi öğrenmek için ESET SysInspector Online Yardım'a bakın.

ESET SysInspector penceresi, günlükler hakkında aşağıdaki bilgileri görüntüler:

- **Saat** – Günlük oluşturma zamanı.
- **Yorum** – Kısa bir yorum.
- **Kullanıcı** – Günlüğü oluşturan kullanıcının adı.
- **Durum** – Günlük oluşturma durumu.

Kullanılabilir eylemler şunlardır:

- **Göster** - ESET SysInspector ürününde seçili günlüğü açar. Ayrıca belirli bir günlük dosyasını sağ tıklatıp içerik menüsünden **Göster**'i seçebilirsiniz.
- **Oluştur** – Yeni bir günlük oluşturur. Günlüğe erişmeyi denemeden önce ESET SysInspector aracı oluşturulana kadar (**Oluşturuldu** durumu) bekleyin.
- **Sil** - Seçili günlükleri listeden kaldırır.

Bir veya daha fazla günlük dosyası seçildiğinde bağlam menüsünde aşağıdaki öğeler yer alır:

- **Göster** – Seçili günlüğü ESET SysInspector içinde açar (bir günlüğü çift tıklatmakla aynı işlevdir).
- **Oluştur** – Yeni bir günlük oluşturur. Günlüğe erişmeyi denemeden önce ESET SysInspector aracı oluşturulana kadar (**Oluşturuldu** durumu) bekleyin.
- **Sil** - Seçili günlükleri listeden kaldırır.
- **Tümünü sil** - Tüm günlükleri siler.
- **Ver** - Günlüğü bir .xml dosyası veya sıkıştırılmış .xml olarak verir. Günlük, C:\ProgramData\ESET\ESET Security\SysInspector yoluna aktarılır.

Zamanlayıcı

Zamanlayıcı, zamanlanan görevleri önceden tanımlanmış yapılandırma ve özelliklerle başlatır ve yönetir.

Zamanlayıcıya **Araçlar** > **Diğer araçlar** > **Zamanlayıcı** öğeleri tıklanarak ESET Internet Security ana program penceresinden erişilebilir. **Zamanlayıcı**, tüm zamanlanan görevlerin ve önceden tanımlı tarih, saat ve kullanılan tarama profili gibi yapılandırma özelliklerinin listesini içerir.

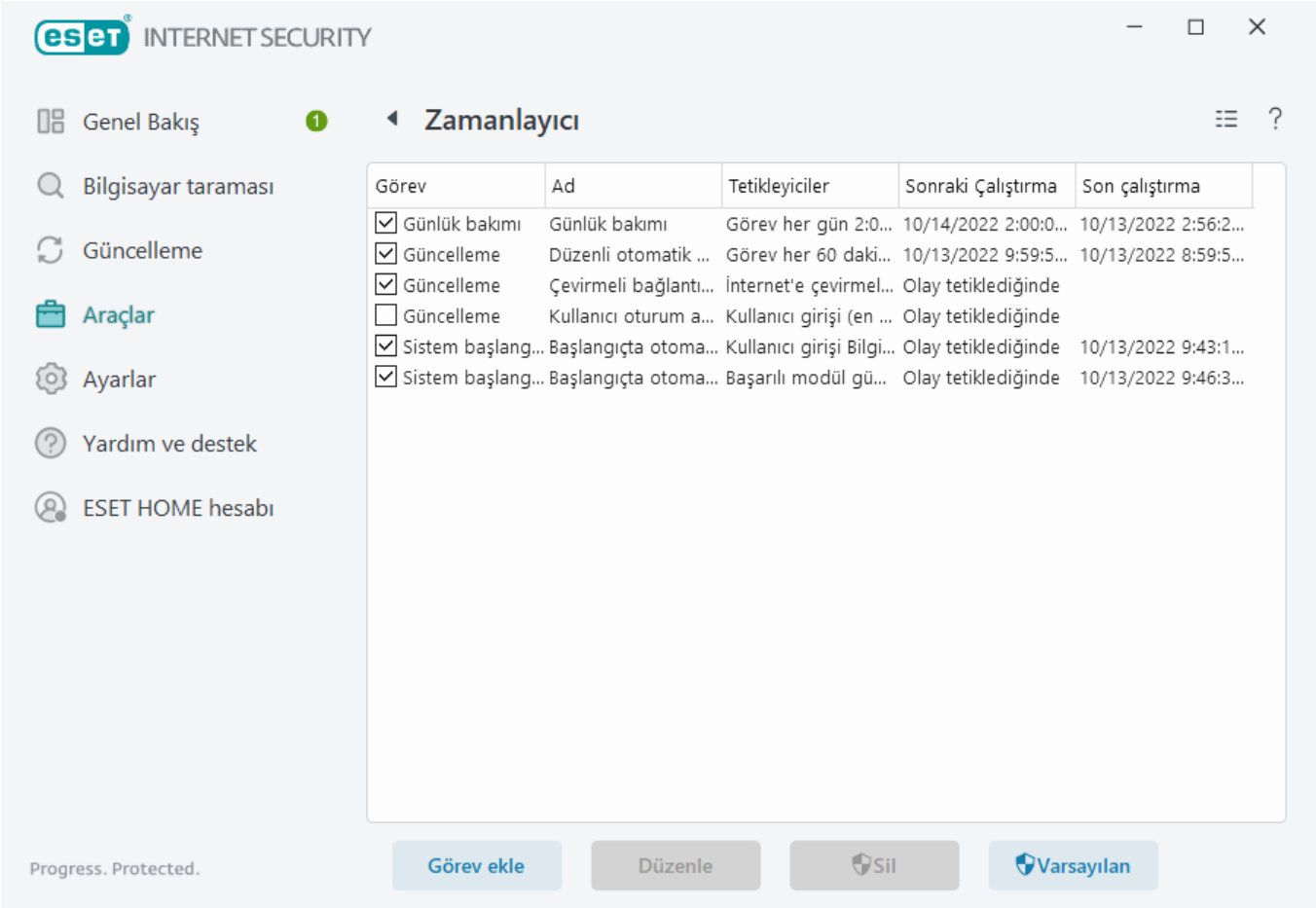
Zamanlayıcı aşağıdaki görevleri zamanlamak için kullanılır: güncelleme modülleri, tarama görevi, sistem başlangıcında dosya denetimi ve günlük bakımı. Görevleri, ana Zamanlayıcı penceresinden doğrudan ekleyebilir veya silebilirsiniz (alttaki **Görev ekle** veya **Sil** seçeneğini tıklatın). **Varsayılan**'ı tıklayarak zamanlanan görevler listesini varsayılan değerlere dönüştürebilir ve tüm değişiklikleri silebilirsiniz. Aşağıdaki eylemleri gerçekleştirmek için Zamanlayıcı penceresinde herhangi bir yere sağ tıklatın: ayrıntılı bilgi görüntüleme, görevi hemen gerçekleştirme, yeni bir görev ekleme ve var olan görevi kaldırma. Görevleri etkinleştirmek/devre dışı bırakmak için ilgili girişlerin başındaki onay kutularını kullanın.

Varsayılan olarak, **Zamanlayıcı**'da aşağıdaki zamanlanan görevler görüntülenir:

- **Günlük bakımı**
- **Düzenli otomatik güncelleme**
- **Çevirmeli bağlantıdan sonra otomatik güncelleme**
- **Kullanıcı oturum açtıktan sonra otomatik güncelleme**
- **Başlangıçta otomatik dosya denetimi** (kullanıcı oturum açtıktan sonra)

- **Başlangıçta otomatik dosya denetimi** (algılama altyapısının başarılı güncellemesinden sonra)

Mevcut bir zamanlanan görevin (varsayılan veya kullanıcı tanımlı) yapılandırmasını düzenlemek için, görevi sağ tıklayıp **Düzenle** seçeneğini tıklayın veya değiştirmek istediğiniz görevi seçip **Düzenle** seçeneğini tıklayın.



Yeni görev ekleme

1. Pencerenin altındaki **Görev ekle** öğesini tıklatın.

2. Görev adı girin.

3. Aşağı açılır menüden istediğiniz görevi seçin:

   - **Harici uygulama çalıştır** – Harici bir uygulamanın yürütülmesini zamanlar.

   - **Günlük bakımı** - Günlük dosyaları ayrıca, silinen kayıtlardan kalanları da içerir. Bu görev, etkin çalışma sağlamak için günlük dosyalarındaki kayıtları düzenli olarak en iyi duruma getirir.

   - **Sistem başlangıç dosyası denetimi** – Sistem başlangıcında veya oturum açıldığında çalıştırılmasına izin verilen dosyaları denetler.

   - **Bilgisayar taraması oluştur** – ESET SysInspector bilgisayar sistem görüntüsünü oluşturur; sistem bileşenleri (örneğin, sürücüler, uygulamalar) hakkında ayrıntılı bilgi toplar ve her bileşenin risk düzeyini değerlendirir.

   - **İsteğe bağlı bilgisayar taraması** – Bilgisayarınızdaki dosya ve klasörlerin bilgisayar taramasını gerçekleştirir.

   - **Güncelleme** – Modülleri güncelleyerek bir Güncelleme görevi zamanlar.

4. Görevi etkinleştirmek isterseniz **Etkin** seçeneğinin yanındaki kaydırma çubuğunu tıklayın (zamanlanan görevler listesinden onay kutusunu işaretleyerek/işaretini kaldırarak bu işlemi daha sonra yapabilirsiniz), **İleri**'yi tıklayın ve zamanlama seçeneklerinden birini belirleyin:

- **Bir kere** – Görev önceden tanımlanan tarih ve saatte gerçekleştirilir.
- **Yinelenen** – Görev belirtilen zaman aralığında gerçekleştirilir.
- **Günlük** – Görev her gün tekrarlayan bir şekilde belirtilen saatte çalıştırılır.
- **Haftalık** – Görev seçilen tarih ve saatte çalıştırılır.
- **Olay tetiklediğinde** - Görev belirtilen bir olayda gerçekleştirilir.

5. Dizüstü bilgisayar pil gücüyle çalışırken sistem kaynaklarının kullanımını en aza indirmek için **Pil gücüyle çalışırken görevi atla** öğesini seçin. Görev, **Görev yürütme** alanlarında belirtilen tarihte ve saatte çalışır. Görev önceden tanımlanan saatte çalıştırılamadıysa, tekrar ne zaman gerçekleştirileceğini belirtebilirsiniz:

- **Bir sonraki zamanlanan saatte**
- **En kısa sürede**
- **Son çalıştırmadan itibaren geçen süre (saat) aşılırsa hemen** - Görevin ilk atlanan çalıştırması bu yana geçen süreyi temsil eder. Bu süre aşılırsa görev hemen çalıştırılır. Aşağıdaki döndürücüyü kullanarak zamanı ayarlayın.

Zamanlanan görevi gözden geçirmek için görevi sağ tıklayıp **Görev ayrıntılarını göster**'i tıklayın.

Zamanlanan tarama seçenekleri

Bu pencerede, zamanlanan bir bilgisayar taraması görevi için gelişmiş seçenekleri belirleyebilirsiniz.

Temizleme işlemi olmadan bir tarama çalıştırmak için **Gelişmiş ayarları** tıklayın ve **Temizlemeden tara**'yı seçin. Tarama geçmişi tarama günlüğüne kaydedilir.

Özel durumları yoksay seçildiğinde, daha önce tarama dışında bırakılan uzantılara sahip dosyalar özel durum olmadan taranır.

Taramadan sonraki işlem açılır menüsü, taramanın tamamlanmasının ardından otomatik olarak gerçekleştirilecek işlemi belirlemenize olanak tanır:

- **Eylem yok** - Tarama tamamlandıktan sonra hiçbir eylem gerçekleştirilmez.
- **Kapat** – Bilgisayar, tarama tamamlandıktan sonra kapatılır.
- **Gerekirse yeniden başlat** - Bilgisayar yalnızca tespit edilen tehditlerin temizlenmesi işlemini tamamlamak için gerekirse yeniden başlatılır.
- **Yeniden başlat** – Taramanın ardından tüm açık programları kapatır ve bilgisayarı yeniden başlatır.
- **Gerekirse yeniden başlatmayı zorla** - Bilgisayar yalnızca tespit edilen tehditlerin temizlenmesi işlemini tamamlamak için gerekirse yeniden başlamaya zorlanır.

• **Yeniden başlatmayı zorla** - Kullanıcı etkileşimini beklemeden tüm açık programların kapatılmasını zorlar ve tarama tamamlandıktan sonra bilgisayarı yeniden başlatır.

• **Uykuya geç** – Oturumunuzu korur ve bilgisayarı düşük güç moduna getirir ve bu sayede işinize hızlı bir şekilde devam edebilirsiniz.

• **Hazırda beklet** – RAM'de çalışan her şeyi alıp sabit sürücünüzde özel bir dosyaya taşır. Bilgisayarınız kapanır, ancak daha sonra başlattığınızda önceki durumundan devam eder.

Uyku veya **Hazırda Beklet** işlemleri bilgisayarınızın Güç ve uyku işletim sistemi ayarlarına veya bilgisayar/dizüstü bilgisayar özelliklerine dayalı olarak kullanılabilir. Uyuyan bir bilgisayarın hâlâ çalışan bir bilgisayar olduğunu lütfen unutmayın. Bilgisayarınız pil gücü ile çalıştığı sırada temel işlevleri çalıştırmaya ve elektrik kullanmaya devam eder. Örneğin ofis dışında seyahat ederken pil ömrünü korumak için Hazırda Beklet seçeneğini kullanmanızı öneririz.

Seçilen eylem, çalışan tüm taramaların tamamlanmasının ardından başlatılacak. **Kapat** veya **Yeniden Başlat**'ı seçtiğinizde onay iletişim penceresinde 30 saniyelik bir geri sayım görüntülenir (istenen işlemi devre dışı bırakmak için **İptal**'i tıklayın).

Önceliği olmayan kullanıcıların tarama sonrasındaki işlemleri durdurmalarına engel olmak için **Tarama iptal edilemez** seçeneğini işaretleyin.

Sınırlı kullanıcıya bilgisayar taramasını belirli bir süre boyunca duraklatma izni vermek istiyorsanız **Taramanın kullanıcı tarafından duraklatılabileceği süre (dk)** seçeneğini belirleyin.

Tarama ilerleme bölümüne de bakın.

Zamanlanan göreve genel bakış

Bu iletişim penceresi, belirli bir görevi çift tıklattığınızda veya özel zamanlayıcı görevini sağ tıklattığınızda ve ardından **Görev ayrıntılarını göster** seçeneğini tıklattığınızda, belirlenen zamanlanan görev hakkında ayrıntılı bilgileri görüntüler.

Görev ayrıntıları

Görev adını yazın, **Görev türü** seçeneklerinden birini belirleyin ve **Sonraki**'ni tıklayın:

• **Harici uygulama çalıştır** – Harici bir uygulamanın yürütülmesini zamanlar.

• **Günlük bakımı** - Günlük dosyaları ayrıca, silinen kayıtlardan kalanları da içerir. Bu görev, etkin çalışma sağlamak için günlük dosyalarındaki kayıtları düzenli olarak en iyi duruma getirir.

• **Sistem başlangıç dosyası denetimi** – Sistem başlangıcında veya oturum açıldığında çalıştırılmasına izin verilen dosyaları denetler.

• **Bilgisayar taraması oluştur** – ESET SysInspector bilgisayar sistem görüntüsünü oluşturur; sistem bileşenleri (örneğin, sürücüler, uygulamalar) hakkında ayrıntılı bilgi toplar ve her bileşenin risk düzeyini değerlendirir.

• **İsteğe bağlı bilgisayar taraması** – Bilgisayarınızdaki dosya ve klasörlerin bilgisayar taramasını gerçekleştirir.

- **Güncelleme** – Modülleri güncelleyerek bir Güncelleme görevi zamanlar.

Görev zamanlaması

Görev belirtilen zaman aralığında yinelenerek gerçekleştirilir. Zamanlama seçeneklerinden birini belirleyin:

- **Bir kere** – Görev önceden tanımlanan tarih ve saatte yalnızca bir kere gerçekleştirilir.
- **Yinelenen** – Görev belirtilen zaman aralığında (saat) gerçekleştirilir.
- **Günlük** – Görev her gün tekrarlayan bir şekilde belirtilen saatte çalıştırılır.
- **Haftalık** – Görev seçilen günde (günlerde) ve saatte haftada bir veya birkaç kere çalıştırılır.
- **Olay tetiklediğinde** – Görev belirtilen bir olayda gerçekleştirilir.

Pil gücüyle çalışırken görevi atla – Görev başlatıldığı sırada bilgisayar pil gücüyle çalışıyorsa görev başlatılmaz. Bu UPS gücüyle çalıştırılan bilgisayarlar için de geçerlidir.

Görev zamanlaması - Bir kez

Görev yürütme - Belirtilen görev belirtilen tarihte ve saatte yalnızca bir kez çalıştırılır.

Görev zamanlaması - Günlük

Görev her gün tekrarlayan bir şekilde belirtilen saatte çalıştırılır.

Görev zamanlaması - Haftalık

Görev her hafta seçilen gün ve saatte yinelenir.

Görev zamanlaması - Tetiklenen olay

Görev aşağıdaki olaylardan biri tarafından tetiklenir:

- **Bilgisayarın her başlatılışında**
- **Her gün, bilgisayar ilk açıldığında**
- **Çevirmeli İnternet/VPN bağlantısında**
- **Başarılı modül güncellemesi**
- **Başarılı ürün güncellemesi**
- **Kullanıcı oturum açtığında**

- **Tehdit algılama**

Olay tarafından tetiklenen bir görev zamanlandığında, görevin iki tamamlanışı arasındaki en düşük zaman aralığını belirtebilirsiniz. Örneğin, bilgisayarınızda gün içinde birkaç defa oturum açıyorsanız, görevin yalnızca söz konusu gün ilk kez oturum açıldığında ve sonra ertesi gün gerçekleştirilmesini sağlamak için 24 saat seçeneğini belirleyin.

Atlanan görev

Bilgisayar kapalıysa veya pil gücüyle çalışıyorsa ya da gücü kapatılmışsa görev atlanabilir. Bu seçeneklerden biri ile görevin çalıştırılacağı zamanı seçin ve **İleri**'yi tıklatın:

- **Bir sonraki zamanlanan saatte** - Bilgisayar bir sonraki zamanlanan saatte açıksa görev çalıştırılır.
- **En kısa sürede** - Görev bilgisayar açık olduğunda çalıştırılır.
- **Son zamanlanan çalıştırmadan itibaren geçen süre (saat) aşılırsa hemen** - Görevin ilk atlanan çalıştırılmasından bu yana geçen süreyi temsil eder. Bu süre aşılırsa görev hemen çalıştırılır.

Son zamanlanan çalıştırmadan beri geçen süre şu kadar saati aştıysa hemen – örnekler

Örnek görev her saat yinelenerek çalışacak şekilde ayarlanır. **Son zamanlanan çalıştırmadan itibaren geçen süre (saat) aşılırsa hemen** seçilir ve aşılan süre iki saat olarak ayarlanır. Görev saat 13:00'te çalışır ve tamamlandığında bilgisayar uyku moduna geçer:

- Bilgisayar saat 15:30'da uyanır. Görevin ilk atlanan çalıştırılması saat 14:00'teydi. Saat 14:00'ten itibaren yalnızca 1,5 saat geçti. Bu nedenle görev saat 16:00'da çalıştırılacak.
- Bilgisayar 16:30'da uyanır. Görevin ilk atlanan çalıştırılması saat 14:00'teydi. Saat 14:00'ten itibaren iki buçuk saat geçtiği için görev hemen çalıştırılacaktır.

Görev ayrıntıları - Güncelleme

Programı iki güncelleme sunucusundan güncellemek istiyorsanız, iki farklı güncelleme profili oluşturulması gerekir. Birincisi güncelleme dosyalarını karşıdan yükleyemezse, program otomatik olarak diğerine geçiş yapar. Bu, örneğin normalde yerel bir LAN güncelleme sunucusundan güncelleme yapan ancak sahipleri genellikle başka ağlar kullanarak Internet'e bağlanan dizüstü bilgisayarlar için uygundur. Böylece, birinci profil başarısız olursa, ikinci profil otomatik olarak ESET'in güncelleme sunucularından güncelleme dosyalarını yükleyecektir.

Görev ayrıntıları - Uygulamayı çalıştır

Bu görev, harici bir uygulamanın çalıştırılmasını zamanlar.

Çalıştırılabilir dosya – Dizin ağacından bir çalıştırılabilir dosya seçin, **...** seçeneğini tıklatın veya yolu el ile girin.

Çalışma klasörü - Harici uygulamanın çalışma klasörünü tanımlayın. Seçili **Çalıştırılabilir dosyanın** tüm geçici dosyaları, bu dizin içinde oluşturulacaktır.

Parametreler – Uygulamaya yönelik komut satırı parametreleri (isteğe bağlı).

Görevi uygulamak için **Son**'u tıklatın.

Sistem temizleyici

Sistem temizleyici, tehdidi temizledikten sonra bilgisayarı kullanılabilir bir duruma geri yüklemenize yardımcı olan bir araçtır. Kötü amaçlı yazılım Kayıt Defteri Düzenleyici, Görev yöneticisi veya Windows Güncellemeleri gibi sistem yardımcı programlarını devre dışı bırakabilir. Sistem temizleyici, varsayılan değerleri ve seçili sistem için ayarları tek tıklamayla geri yükler.

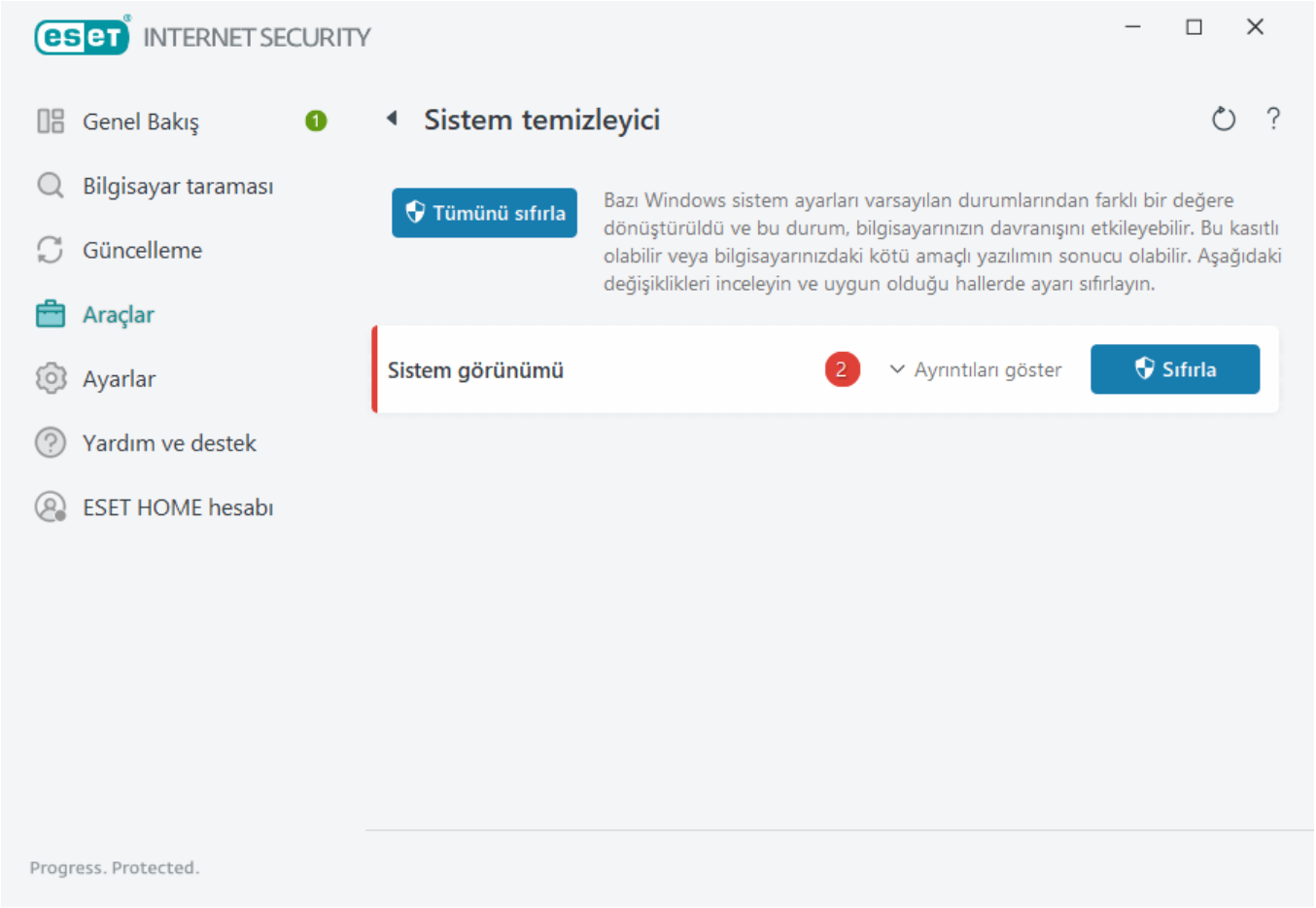
Sistem temizleyici beş ayar kategorisi için sorunları bildirir:

- **Güvenlik ayarları**: Windows Güncellemesi gibi, bilgisayarınızda ileri düzeyde hassasiyete neden olabilecek ayarlardaki değişiklikler
- **Sistem ayarları**: Dosya ilişkilendirmeleri gibi, bilgisayarınızın davranışını değiştirebilecek olan sistem ayarlarındaki değişiklikler
- **Sistem görünümü**: Masaüstü duvar kağıdınız gibi, sisteminizin görünümünü etkileyecek ayarlar.
- **Devre dışı bırakılan özellikler**: Devre dışı bırakılabilecek önemli özellik ve uygulamalar
- **Windows Sistemi Geri Yüklemesi**: Sisteminizi bir önceki durumuna geri döndürmenize olanak sağlayan Windows Sistemi Geri Yükleme özelliği için ayarlar

Sistem temizleyici şu durumlarda istenebilir:

- tehdit bulunduğunda
- kullanıcı **Sıfırla'yı tıklattığında**

Uygun olması halinde, değişiklikleri gözden geçirebilir ve ayarları sıfırlayabilirsiniz.



Yalnızca Yönetici haklarına sahip kullanıcı, Sistem temizleyicideki işlemleri yapabilir.

ESET SysRescue Live

ESET SysRescue Live, önyüklenebilir bir kurtarma CD/DVD'si veya USB sürücüsü oluşturmanıza olanak tanıyan ücretsiz bir yardımcı programdır. Herhangi bir etkilenmiş bilgisayarı kurtarma medyanızdan açarak kötü amaçlı yazılımlara karşı tarayabilir veya etkilenmiş dosyaları temizleyebilirsiniz.

ESET SysRescue Live uygulamasının başlıca avantajı, çözümünün diske ve dosya sistemine doğrudan erişime sahip olurken ana bilgisayar işletim sisteminden bağımsız şekilde çalışmasıdır. Böylece, normal işletim koşullarında silinmesi mümkün olmayan (ör. işletim sistemi çalışırken vb.) tehditleri kaldırmak mümkün olabilir.

- ESET SysRescue Live İçin online yardım

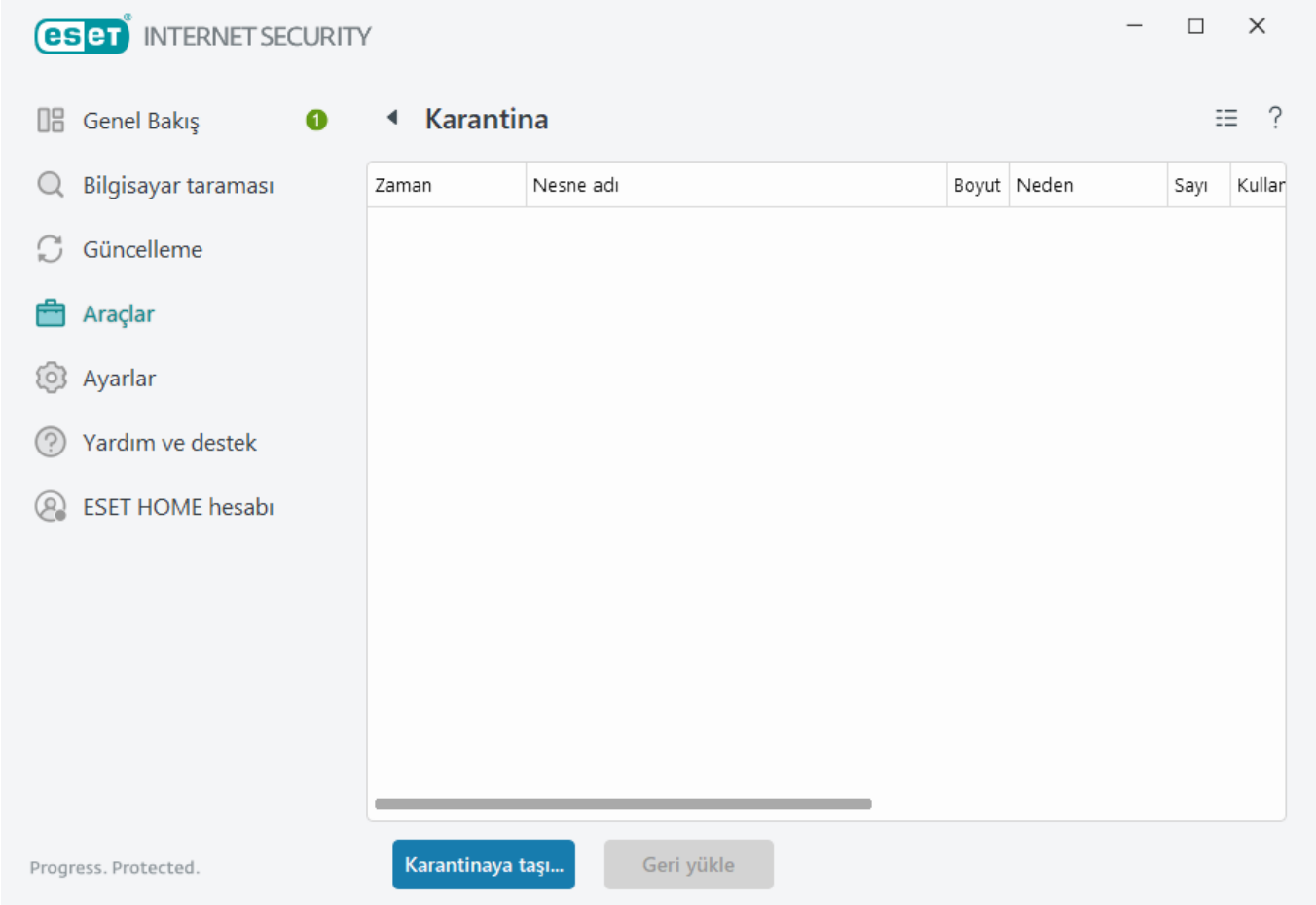
Karantina

Karantinanın temel işlevi, bildirilen nesneleri (kötü amaçlı yazılım, enfekte olan dosyalar veya istenmeyen türden olabilecek uygulamalar gibi) güvenli bir şekilde depolamaktır.

Karantinaya ESET Internet Security ana program penceresinden **Araçlar** > **Diğer araçlar** > **Karantina** öğeleri tıklanarak erişilebilir.

Karantina klasöründe depolanan dosyalar şunları içeren bir tabloda görüntülenebilir:

- karantina tarihi ve saati,
- dosyanın orijinal konumuna giden yol,
- bayt olarak dosya boyutu,
- nedeni (örneğin, kullanıcı tarafından eklenen nesne),
- ve bir dizi tespit (örneğin, aynı dosyanın yinelenen tespitleri veya birden çok sızıntı içeren bir arşiv olup olmadığı).



Dosyaları karantinaya alma

ESET Internet Security, silinen dosyaları otomatik olarak karantinaya alabilirsiniz (uyarı penceresinde bu seçeneği iptal etmediyseniz).

Ek dosyalar şu durumlarda karantinaya alınmalıdır:

a.temizlenemez,

b.güvenli değilse veya silinmeleri önerilirse,

c.ESET Internet Security tarafından hatalı bir şekilde tespit edilirse

d.veya bir dosya şüpheli bir şekilde davranırsa ancak tarayıcı tarafından algılanmazsa.

Bir dosyayı karantinaya almak için birkaç seçenek bulunmaktadır:

a.Bir dosyayı karantinaya almak için sürükle-bırak özelliğini kullanabilirsiniz. Bunun için dosyayı tıklayın, fare düğmesini basılı tutarken imleci işaretli alana taşıyıp bırakın. Bunun ardından, uygulama ön plana taşınır.

b.Dosyayı sağ tıklayın, **Gelişmiş seçenekler** > **Dosyayı karantinaya al** seçeneğini tıklayın.

c.**Karantina** penceresinden **Karantinaya taşı** seçeneğini tıklayın.

d.İçerik menüsü de bu amaç için kullanılabilir. **Karantina** penceresinde sağ tıklayın ve **Karantina**'yı seçin.

Karantinadan geri yükleme

Karantinaya alınan dosyalar da orijinal konumlarına geri yüklenebilir:

- Bunun için, Karantinadaki belirli bir dosyayı sağ tıklayarak içerik menüsünden **Geri Yükle** özelliğini kullanın.
- Bir dosya istenmeyen türden olabilecek uygulama olarak işaretlenmişse, **Geri yükle ve tarama dışı bırak** seçeneği etkinleştirilir. Ayrıca Tarama dışı bırakma bölümüne de bakın.
- İçerik menüsü **Şuna geri yükle** seçeneğini de sunar. Bu seçenek, bir dosyayı silindiği konumdan başka bir konuma geri yüklemenize olanak tanır.
- Geri yükleme işlevi bazı durumlarda (örneğin, salt okunur ağ paylaşımında bulunan dosyalar için) kullanılamaz.

Karantinadan silme

Belirli bir öğeyi sağ tıklayıp **Karantinadan Sil**'i seçin veya silmek istediğiniz öğeyi seçip klavyenizde **Delete** düğmesine basın. Ayrıca birden fazla öğe seçebilir ve hepsini birden silebilirsiniz. Silinen öğeler cihazınızdan ve karantinadan kalıcı olarak kaldırılır.

Karantinadaki bir dosyayı gönderme

Program tarafından algılanmayan şüpheli bir dosyayı karantinaya aldıysanız veya bir dosya yanlışlıkla etkilenmiş olarak değerlendirilmiş (örneğin, kodun sezgisel tarama analizi tarafından) ve sonra da karantinaya alınmışsa, lütfen örneği analiz için ESET Araştırma Laboratuvarı'na gönderin. Göndermek istediğiniz dosyayı sağ tıklayın ve içerik menüsünden **Analiz için gönder**'i seçin.

Tespit açıklaması

Kaydedilen sızıntının tehlikeleri ve belirtileri ile ilgili ayrıntılı bilgiler içeren ESET Tehdit Ansiklopedisi'ni açmak için bir öğeyi sağ tıklayıp **Tespit açıklaması**'nı tıklayın.

Resimli talimatlar

Aşağıdaki ESET Bilgi Bankası makaleleri sadece İngilizce dilinde mevcuttur:

- ESET Internet Security ürününde karantinaya alınmış bir dosyayı geri yükleme
- ESET Internet Security ürününde karantinaya alınmış bir dosyayı silme
- ESET ürünüm bir tespit hakkında bana bildirim gönderdi. Bu durumda ne yapmalıyım?

Karantinaya alma işlemi başarısız oldu

Belirli dosyaların Karantinaya taşınamamasıyla ilgili nedenler şu şekildedir:

- **Okuma izinleriniz yok** - Bu, bir dosyanın içeriğini göremeyeceğiniz anlamına gelir.
- **Yazma izinleriniz yok** - Dosyanın içeriklerini değiştiremeyeceğiniz anlamına gelir; başka bir ifadeyle, yeni içerik ekleyemez veya mevcut içeriği silemezsiniz.
- **Karantinaya almaya çalıştığınız dosya çok büyük** - Dosya boyutunu küçültmeniz gerekir.

"Karantinaya alınamadı" hata iletisini alırsanız **Daha fazla bilgi**'yi tıklayın. Karantina hata listesi penceresi açılır ve dosyanın adını ve nedenini, dosyanın neden karantinaya alınamadığını görebilirsiniz.

Proxy sunucu

Büyük LAN ağlarında, bilgisayarınız ve İnternet arasındaki iletişim proxy sunucusu aracılığıyla gerçekleştirilir. Bu yapılandırmayı kullanarak aşağıdaki ayarların tanımlanması gerekir. Aksi takdirde, program kendini otomatik olarak güncelleyemez. ESET Internet Security içinde proxy sunucu ayarları Gelişmiş ayarlar ağacındaki iki farklı bölümden kullanılabilir.

Öncelikle proxy sunucu ayarları **Araçlar** > **Proxy sunucu** öğesi altında **Gelişmiş ayarlar**'da yapılandırılabilir. Proxy sunucunun bu düzeyde belirtilmesi, tüm ESET Internet Security için global proxy sunucu ayarlarını belirler. Buradaki parametreler İnternet bağlantısının gerekli olduğu tüm modüller tarafından kullanılır.

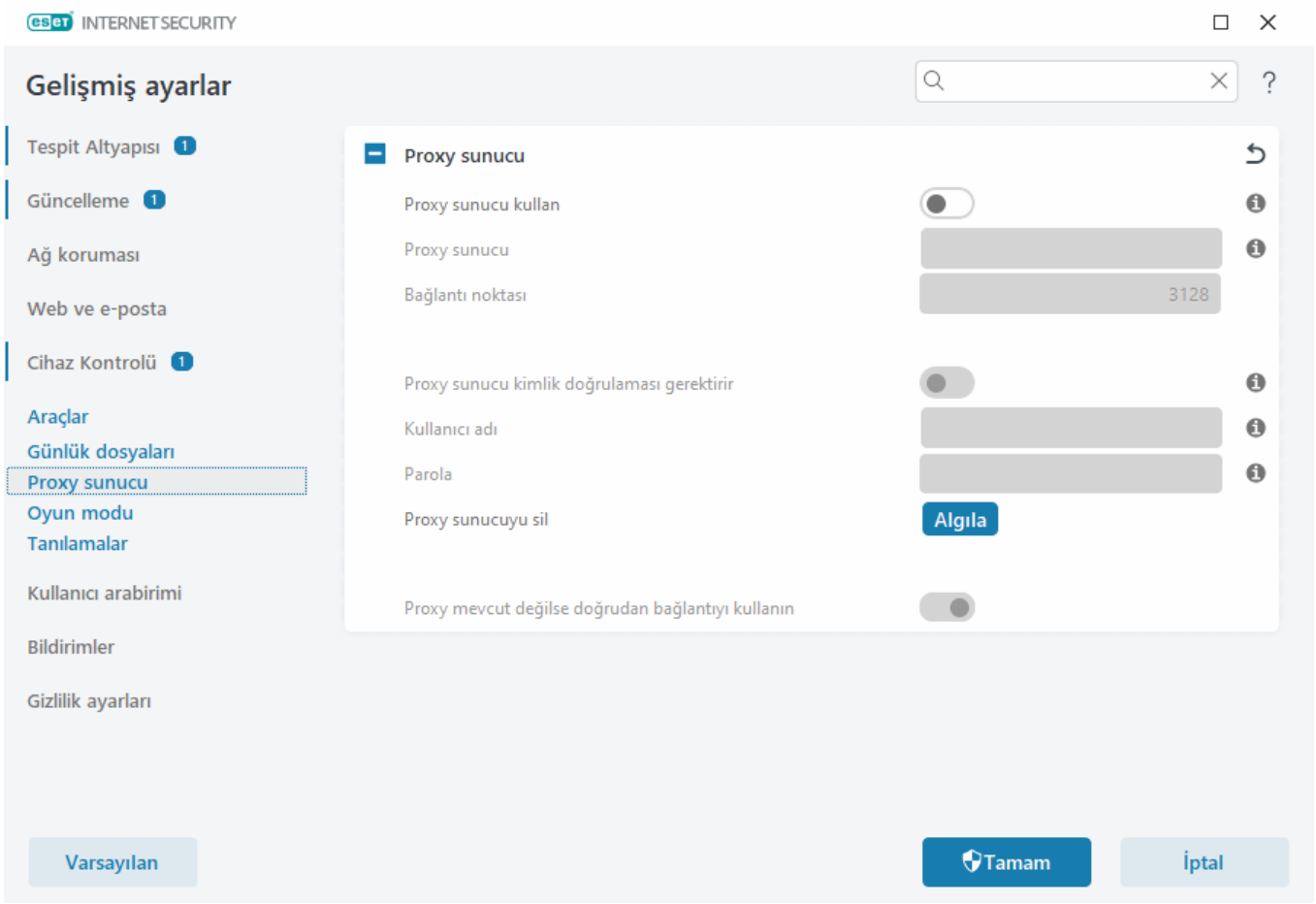
Bu düzey için proxy sunucu ayarlarını belirlemek üzere **Proxy sunucu kullan**'ı seçin ve ardından **Proxy sunucu** alanına proxy sunucu adresini ve proxy sunucusunun **Bağlantı noktası** numarasını girin.

Proxy sunucu ile iletişim için kimlik doğrulaması gerekliyse **Proxy sunucu kimlik doğrulaması gerektirir** seçeneğini işaretleyip ilgili alanlara geçerli **Kullanıcı adı** ve **Parola**'yı girin. Proxy sunucu ayarlarını otomatik olarak algılamak ve doldurmak için **Proxy sunucuyu algıla**'yı tıklayın. İnternet seçenekleri'nde Internet Explorer veya Google Chrome için belirtilen parametreler kopyalanır.

Proxy sunucu ayarlarında Kullanıcı Adı ve Parolanızı manuel olarak girmeniz gerekir.

Proxy kullanılamıyorsa doğrudan bağlantı kullan – ESET Internet Security ürünü proxy kullanacak şekilde yapılandırılmışsa ancak proxy'e ulaşılamıyorsa ESET Internet Security, proxy'i atlayarak doğrudan ESET sunucularıyla iletişim kurar.

Proxy sunucu ayarları, Gelişmiş güncelleme ayarlarından da (**Gelişmiş ayarlar** > **Güncelle** > **Profiller** > **Güncellemeler** > **Bağlantı seçenekleri**, **Proxy modu** açılır menüsünden **Proxy sunucusu üzerinden bağlantı** seçilerek) yapılabilir. Bu ayar belirli güncelleme profili için geçerlidir ve virüs imza güncellemelerini çoğu zaman farklı konumlardan alan dizüstü bilgisayarlar için önerilir. Bu ayar hakkında daha fazla bilgi için Gelişmiş güncelleme ayarları bölümüne bakın.



Analiz için örnek seçin

Bilgisayarınızda şüpheli bir dosya veya internette şüpheli bir site bulursanız, bunu analiz için ESET Araştırma Laboratuvarı'na gönderebilirsiniz (ESET LiveGrid® yapılandırmanıza bağlı olarak kullanılamayabilir).

Örnekleri ESET'e göndermeden önce

Aşağıdaki kriterlerden en az birini karşılamadığı sürece örneği göndermeyin:

- Örnek ESET ürününüz tarafından hiçbir şekilde algılanmıyor
- Örnek hatalı bir şekilde tehdit olarak algılandı
- Kişisel dosyalarınızı (ESET tarafından kötü amaçlı yazılımlara karşı taranmasını istediğiniz dosyaları) örnek olarak kabul etmeyiz (ESET Araştırma Laboratuvarı kullanıcılar için isteğe bağlı tarama gerçekleştirmez)
- Açıklayıcı bir konu kullanın ve dosyayla ilgili olabildiğince çok bilgi (örneğin ekran görüntüsü veya dosyayı indirdiğiniz web sitesi) ekleyin.

Şu yöntemlerden birini kullanarak analiz için ESET'e örnek (dosya veya web sitesi) gönderebilirsiniz:

1. Ürününüzdeki gönderme formunu kullanın. Bu form, **Araçlar** > **Analiz için örnek gönder** bölümünde yer almaktadır. Gönderilen bir örnek maksimum 256 MB boyutunda olabilir.

2. Alternatif olarak dosyayı e-posta ile de gönderebilirsiniz. Bu seçeneği tercih ederseniz, dosyaları WinRAR/WinZIP kullanarak paketleyin, arşivi "etkilenmiş" parolasıyla korumaya alın ve samples@eset.com adresine gönderin.

3. Spam, hatalı pozitif spam veya Ebeveyn Kontrolü modülü tarafından hatalı bir şekilde kategorilendirilen web sitelerini bildirmek için lütfen ESET Bilgi Bankası makalemize başvurun.

Analiz için örnek seçme formunda **Örneği gönderme nedeni** açılır menüsünden iletinizin amacına en uygun olan açıklamayı seçin:

- Şüpheli dosya
- Şüpheli site (herhangi bir kötü amaçlı yazılımdan etkilenen web sitesi),
- Hatalı pozitif site
- Hatalı pozitif dosya (etkilenmiş olarak algılanan ancak etkilenmemiş olan dosya),
- Diğer

Dosya/Site – Göndermek istediğiniz dosyanın veya web sitesinin yolu.

İletişim e-postası – Şüpheli dosyalarla birlikte iletişim e-postası da ESET'e gönderilir ve analiz için ek bilgiler gerekirse sizinle iletişim kurmak için kullanılabilir. İletişim e-posta adresi girmek isteğe bağlıdır. Boş bırakmak için **Anonim olarak gönder**'i işaretleyin.

> **ESET'ten yanıt almayabilirsiniz**
> Daha fazla bilgi gerekmedikçe ESET'ten yanıt almazsınız. Sunucularımıza her gün on binlerce dosya geldiğinden tüm bu gönderimleri yanıtlamamız olanaksız olduğu için.
> Örneğin kötü amaçlı bir uygulama veya web sitesi olduğu belirlenirse, bu örneğin algılanması yaklaşan bir ESET güncellemesine eklenir.

Analiz için örnek seçin - Şüpheli dosya

Gözlemlenen kötü amaçlı yazılımdan etkilenme işaretleri ve belirtileri – Bilgisayarınızda gözlemlenen kötü amaçlı yazılım davranışlarının açıklamasını girin.

Dosya kaynağı (URL adresi veya satıcı) – Lütfen dosyanın kaynağını (nereden edindiğinizi) ve bu dosyaya ne şekilde ulaştığınızı yazın.

Notlar ve ek bilgiler - Buraya şüpheli dosya işlenirken yardımcı olabilecek ek bilgileri veya açıklamaları ekleyebilirsiniz.

> İlk parametre – **Gözlemlenen kötü amaçlı yazılımdan etkilenme işaretleri ve belirtileri** - Bunun belirtilmesi zorunludur. Ancak tanımlama sürecinde ve örneklerin işlenmesinde laboratuvarlarımıza büyük oranda yardımcı olacak ek bilgiler de sağlanmalıdır.

Analiz için örnek seçin - Şüpheli site

Lütfen **Siteyle ilgili sorun nedir?** açılır menüsünden aşağıdakilerden birini seçin:

- **Etkilenmiş** – Çeşitli yöntemlerle dağıtılan virüsleri ve diğer kötü amaçlı yazılımları içeren bir web sitesi.
- **Kimlik avının** amacı genellikle banka hesabı numaraları, PIN numaraları ve daha fazlası gibi hassas verilere erişmektir. Bu saldırı türüyle ilgili daha fazla bilgi sözlük'ten edinilebilir.
- **Sahtekarlık** - Özellikle çabuk kâr etmeye yönelik sahtekarlık veya dolandırma amaçlı web sitesi.

- Yukarıdaki seçenekler göndereceğiniz siteye yer vermiyorsa **Diğer**'i seçin.

Notlar ve ek bilgiler - Şüpheli web sitesini analiz etmenize yardımcı olacak ek bilgileri veya açıklamaları yazabilirsiniz.

Analiz için örnek seçin - Hatalı pozitif dosya

Antivirus ve antispyware altyapımızı geliştirmek ve diğer kullanıcıların korunmasına yardımcı olmak için, etkilenmiş olarak algılanan ancak etkilenmemiş olan dosyaları göndermeniz istenir. Hatalı pozitif (HP) algılamaları bir dosya düzeninin, algılama altyapısında yer alan aynı düzenle eşleşmesi halinde meydana gelebilir.

Uygulama adı ve sürümü – Programın başlığı ve sürümü (örneğin, numarası, diğer adı veya kod adı).

Dosya kaynağı (URL adresi veya satıcı) – Lütfen dosyanın kaynağını (nereden edindiğinizi) girin ve bu dosyaya ne şekilde ulaştığınızı not edin.

Uygulamanın amacı – Uygulamanın genel açıklaması, uygulamanın türü (ör. tarayıcı, ortam yürütücüsü,...) ve işlevleri.

Notlar ve ek bilgiler - Buraya şüpheli dosya işlenirken yardımcı olabilecek ek bilgileri veya açıklamaları ekleyebilirsiniz.

> Yasal uygulamaların tanımlanabilmesi ve kötü amaçlı kodlardan ayırt edilebilmesi için ilk üç parametrenin sağlanması zorunludur. Ek bilgi sağlayarak tanımlama sürecinde ve örneklerin işlenmesinde laboratuvarlarımıza büyük oranda yardımcı olabilirsiniz.

Analiz için örnek seçin - Hatalı pozitif site

Etkilenmiş, kimlik bilgilerini çalmaya veya kimlik avına yönelik olarak algılanan ancak bunlardan herhangi biri olmayan siteleri göndermeniz istenir. Hatalı pozitif (HP) algılamaları bir dosya düzeninin, algılama altyapısında yer alan aynı düzenle eşleşmesi halinde meydana gelebilir. Antivirus ve kimlik avı koruması altyapımızı geliştirmek ve diğerlerinin korunmasına yardımcı olmak için lütfen bu web sitesini bize iletin.

Notlar ve ek bilgiler - Buraya şüpheli web sitesi işlenirken yardımcı olabilecek ek bilgileri veya açıklamaları ekleyebilirsiniz.

Analiz için örnek seçin - Diğer

Şüpheli dosya veya **Hatalı pozitif** olarak sınıflandırılamayacak dosyalar için bu formu kullanın.

Dosyayı gönderme nedeni - Lütfen detaylı bir açıklama ve dosyanın neden gönderildiğini girin.

Microsoft Windows® güncellemesi

Windows update özelliği, kullanıcıları kötü amaçlı yazılımlardan korumaya yönelik önemli bir bileşendir. Bu nedenle, Microsoft Windows güncellemelerini kullanılabilir olduklarında hemen yüklemeniz büyük önem taşır. ESET Internet Security, belirttiğiniz düzeye göre eksik güncellemeleri size bildirir. Şu düzeyler kullanılabilir:

- **Güncelleme yok** – İndirme için sistem güncellemesi sunulmaz.
- **İsteğe bağlı güncellemeler** – Düşük ve üzeri önceliğe sahip olarak işaretlenen güncellemeler, indirilmek üzere sunulur.
- **Önerilen güncellemeler** – Genel ve üzeri önceliğe sahip olarak işaretlenen güncellemeler indirilmek üzere sunulur.
- **Önemli güncellemeler** – Önemli ve üzeri önceliğe sahip olarak işaretlenen güncellemeler, indirilmek üzere sunulur.
- **Kritik güncellemeler** - Yalnızca kritik güncellemeler indirilmek üzere sunulur.

Değişiklikleri kaydetmek için **Tamam**'ı tıklatın. Güncelleme sunucusuyla durum doğrulamasının ardından Sistem güncellemeleri penceresi görüntülenir. Bundan dolayı, sistem güncelleme bilgileri değişiklikler kaydedildikten hemen sonra kullanılamayabilir.

İletişim penceresi - Sistem güncellemeleri

İşletim sisteminiz için güncellemeler varsa ESET Internet Security ana program penceresi > **Genel bakış**'ta bir bildirim görüntüler. Sistem güncellemeleri penceresini açmak için **Daha fazla bilgi**'yi tıklayın.

Sistem güncellemeleri penceresinde, karşıdan yüklenip kurulmaya hazır güncellemelerin listesi gösterilir. Güncelleme türü, güncelleme adının yanında gösterilir.

Ek bilgiler içeren Güncelleme bilgileri penceresinin görüntülenmesi için herhangi bir güncellemeyi çift tıklayın.

Listelenen tüm işletim sistemi güncellemelerini indirmek ve yüklemek için **Sistem güncellemesini çalıştır**'ı tıklayın.

Bilgileri güncelle

Sistem güncellemeleri penceresinde, karşıdan yüklenip kurulmaya hazır güncellemelerin listesi gösterilir. Güncelleme öncelik düzeyi, güncelleme adının yanında gösterilir.

İşletim sistemi güncellemelerini karşıdan yükleme ve kurma işlemini başlatmak için **Sistem güncellemesini çalıştır** seçeneğini tıklatın.

Ek bilgi içeren bir açılır pencere görüntülemek için bir güncelleme satırını sağ tıklatın ve **Bilgileri göster**'i tıklatın.

Yardım ve destek

ESET Internet Security, karşılaşabileceğiniz sorunları çözmede size yardımcı olacak sorun giderme araçlarını ve destek bilgilerini içerir.

Lisans

- **Lisans sorun giderme** - Etkinleştirme veya lisans değişikliğiyle ilgili sorunlara çözüm bulmak için bu bağlantıyı tıklayın.

• **Lisansı yönet** – Etkinleştirme penceresini başlatmak ve ürününüzü etkinleştirmek için tıklatın. Cihazınız ESET HOME ürününe bağlıysa ESET HOME hesabınızdan bir lisans seçin veya yeni bir lisans ekleyin.

Yüklenen ürün

• **Yenilikler** - Yeni ve geliştirilmiş özelliklerle ilgili bilgi penceresini açmak için bunu tıklayın.

• **ESET Internet Security Hakkında** – ESET Internet Security ürününüzün kopyası hakkındaki bilgileri görüntüler.

• **Ürünle ilgili sorun giderme**– En sık karşılaşılan sorunlara çözüm bulmak için bu bağlantıyı tıklayın.

• **Ürünü değiştir** - ESET Internet Security ürününü mevcut lisansla farklı bir ürün serisine dönüştürme imkanı olup olmadığını anlamak için tıklayın.

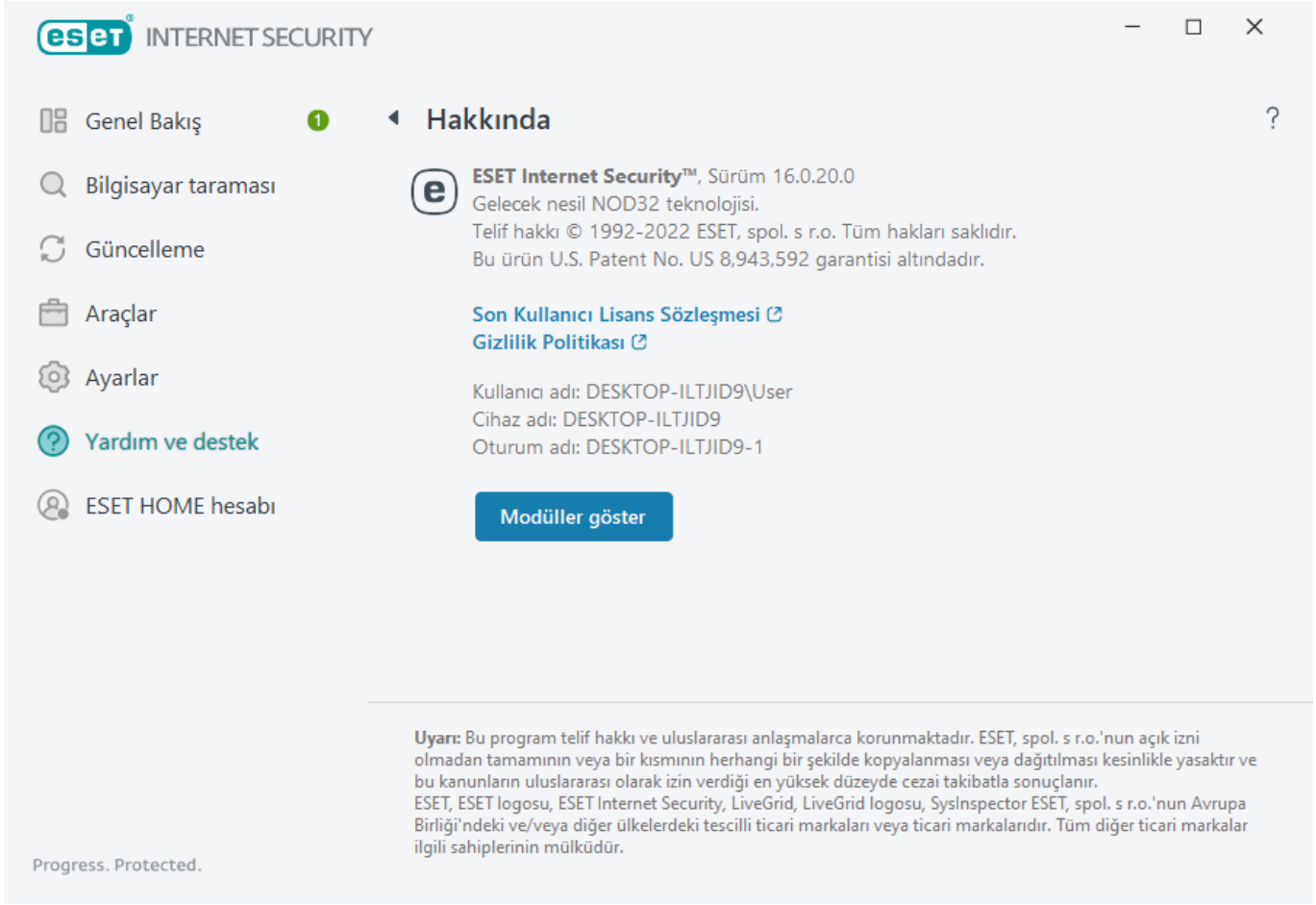
Yardım sayfası – ESET Internet Security yardım sayfalarını açmak için bu bağlantıyı tıklatın.

Teknik Destek

Bilgi Bankası – ESET Bilgi Bankası, en sık sorulan soruların yanıtlarının yanı sıra, çeşitli konular için önerilen çözümleri içerir. ESET teknik uzmanları tarafından düzenli olarak güncellenen Bilgi Bankası, çeşitli sorunları gidermek için kullanılabilecek en güçlü araçtır.

ESET Internet Security Hakkında

Bu pencerede, ESET Internet Security ürününün yüklenmiş sürümü ve bilgisayarınızla ilgili bilgiler sağlanır.



Yüklenen program modülleri listesiyle ilgili bilgileri görmek için **Modülleri göster**'i tıklayın.

- **Kopyala**'yı tıklatarak modüller hakkındaki bilgileri panoya kopyalayabilirsiniz. Bu özellik Teknik Destekle iletişim kurarken veya sorun giderme sırasında faydalı olabilir.

- ESET Tespit Altyapısı'nın her sürümüyle ilgili bilgiler içeren ESET Virus Radar'ı açmak için Modüller penceresinden **Tespit Altyapısı**'nı tıklayın.

ESET News

Bu pencerede ESET Internet Security, ESET haberleri hakkında sizi düzenli olarak bilgilendirir.

Ürün içi mesajlaşma, ESET haberleri ve diğer iletişimler hakkında kullanıcıları bilgilendirmek üzere tasarlanmıştır. Pazarlama iletileri göndermek için kullanıcının onayı gerekir. Bu nedenle, pazarlama iletileri varsayılan olarak kullanıcıya gönderilmez (soru işaretiyle gösterilir). Bu seçeneği etkinleştirerek ESET pazarlama iletilerini almayı kabul edersiniz. ESET pazarlama malzemelerini almak istemiyorsanız **Pazarlama iletilerini göster** seçeneğini devre dışı bırakın.

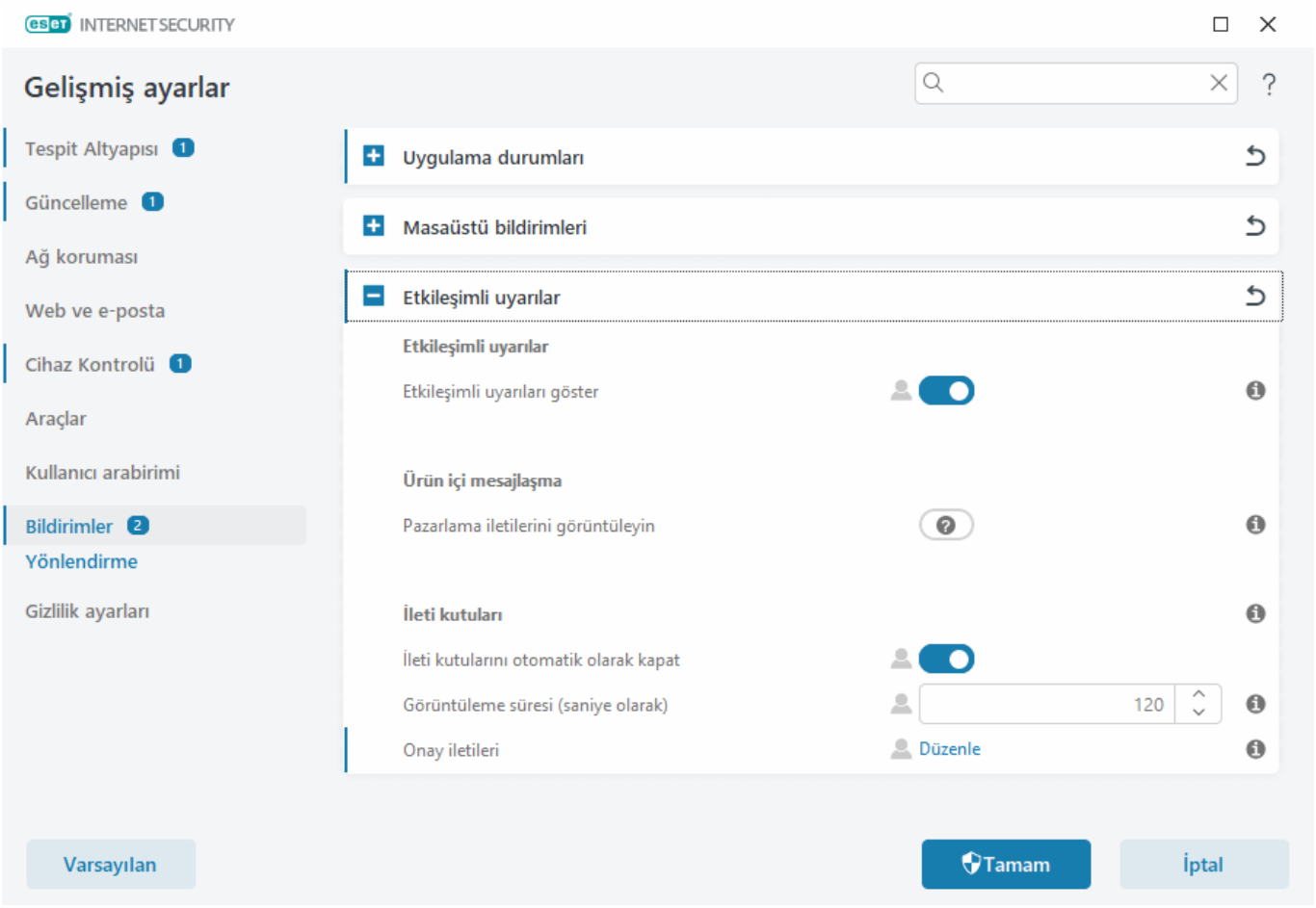
Açılır pencere üzerinden pazarlama iletilerini almayı etkinleştirmek veya devre dışı bırakmak için aşağıdaki talimatları uygulayın.

1. ESET ürününüzün ana penceresini açın.

2. **Gelişmiş ayarlar**'a erişmek için **F5** tuşuna basın.

3. **Bildirimler** > **Etkileşimli Uyarıları** tıklayın.

4. **Pazarlama iletilerini göster** seçeneğini değiştirin.



Sistem konfigürasyon verilerini gönder

ESET, mümkün olduğu kadar çabuk ve doğru bir şekilde destek sağlamak amacıyla, ESET Internet Security yapılandırması hakkındaki bilgilere, ayrıntılı sistem bilgilerine ve çalışan işlemlere (ESET SysInspector günlük dosyası) ve kayıt defteri verilerine ihtiyaç duyar. ESET bu verileri yalnızca müşteriye teknik destek sağlamak amacıyla kullanır.

Web formunu gönderdiğinizde sistem yapılandırma verileriniz ESET'e iletilir. Bu süreç için bu işlemin hatırlanmasını istiyorsanız **Bu bilgileri her zaman gönder**'i seçin. Hiçbir veri göndermeden formu iletmek için **Verileri gönderme**'yi tıklayın; online destek formunu kullanarak ESET Teknik Destek ile iletişim kurabilirsiniz.

Ayrıca bu ayar, **Gelişmiş ayarlar** > **Araçlar** > **Tanılama** > Teknik Destek bölümünden de yapılandırılabilir.

> Sistem verilerini göndermeye karar verdiyseniz web formunu doldurup göndermeniz gerekir, aksi takdirde biletiniz oluşturulmaz ve sistem verileriniz kaybolur.

Teknik Destek

Ana program penceresinde **Yardım ve Destek** > **Teknik Destek** seçeneğini tıklayın.

Teknik Destek İle İletişim Kurun

Destek isteği - Sorununuza yanıt bulamıyorsanız ESET Teknik Destek bölümüyle hemen iletişim kurmak için ESET web sitesinde bulunan bu formu kullanabilirsiniz. Ayarlarınıza bağlı olarak, web formunu doldurmadan önce sistem yapılandırma verilerinizi gönderme penceresi görüntülenir.

Teknik Destekle ilgili bilgi alın

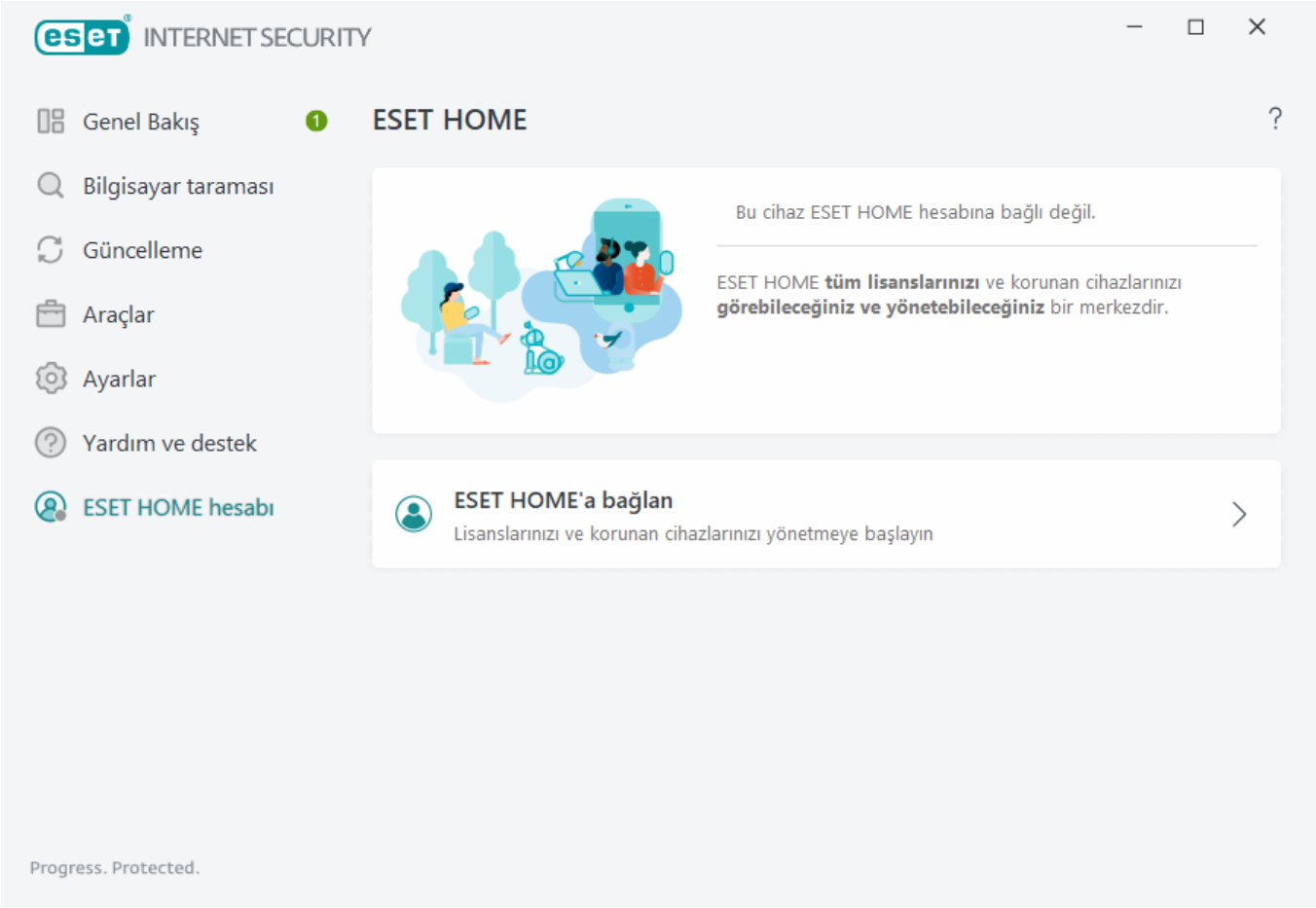
Teknik Destek ayrıntıları - İstendiğinde bilgileri (örneğin lisan bilgileri, ürün adı, ürün sürümü, işletim sistemi ve bilgisayar bilgileri) kopyalayıp ESET Teknik Destek bölümüne gönderebilirsiniz.

ESET Log Collector – ESET Log Collector yardımcı programını indirebileceğiniz ESET Bilgi Bankası makalesine bağlanır. Bu, sorunları daha hızlı bir şekilde çözmeye yardımcı olacak bir bilgisayardan bilgileri ve günlükleri otomatik olarak toplayan bir uygulamadır. Daha fazla bilgi için ESET Log Collectorburayı tıklayın.

Geliştiricilerin sorunları tanılamasına ve çözmesine yardımcı olmak için kullanılabilir tüm özelliklerle ilgili gelişmiş günlükler oluşturmak amacıyla Gelişmiş günlük kaydını etkinleştir'i tıklayın. Minimum kayıt ayrıntısı düzeyi Tanı amaçlı olarak ayarlanmıştır. Gelişmiş günlük kaydı; Gelişmiş günlük kaydını durdur'u tıklayarak daha önce durdurmadığınız takdirde iki saatin sonunda otomatik olarak devre dışı bırakılır. Tüm günlükler oluşturulduğunda, oluşturulan günlüklerle birlikte Tanılama klasörüne doğrudan erişim sağlayan bildirim penceresi gösterilir.

ESET HOME hesabı

ESET HOME hesap bağlantı durumunu ana program penceresi > **ESET HOME hesabı**'ndan inceleyebilirsiniz.



Bu cihaz bir ESET HOME hesabına bağlı değil

Cihazınızı ESET HOME portalına bağlamak, ayrıca lisanslarınızı ve korunan cihazlarınızı yönetmek için ESET HOME portalına bağlan'ı tıklayın. Lisansınızı yenileyebilir, yükseltebilir veya uzatabilir ve önemli lisans ayrıntılarını görüntüleyebilirsiniz. ESET HOME yönetim portalında veya mobil uygulamada farklı lisanslar ekleyebilir, ürünleri cihazlarınıza indirebilir, ürün güvenlik durumunu kontrol edebilir veya lisansları e-posta üzerinden paylaşabilirsiniz. Daha fazla bilgi için ESET HOME Online Yardım'ı ziyaret edin.

Bu cihaz bir ESET HOME hesabına bağlı

ESET HOME Portalını veya mobil uygulamayı kullanarak cihazınızın güvenliğini uzaktan yönetebilirsiniz. ESET HOME mobil uygulamasını App Store'dan veya Google Play'den indirmek istiyorsanız mobil telefonunuzla tarayabileceğiniz bir QR kodu görüntülemek için **App Store** veya **Google Play**'i tıklayın.

ESET HOME hesabı - ESET HOME hesabı adınız.

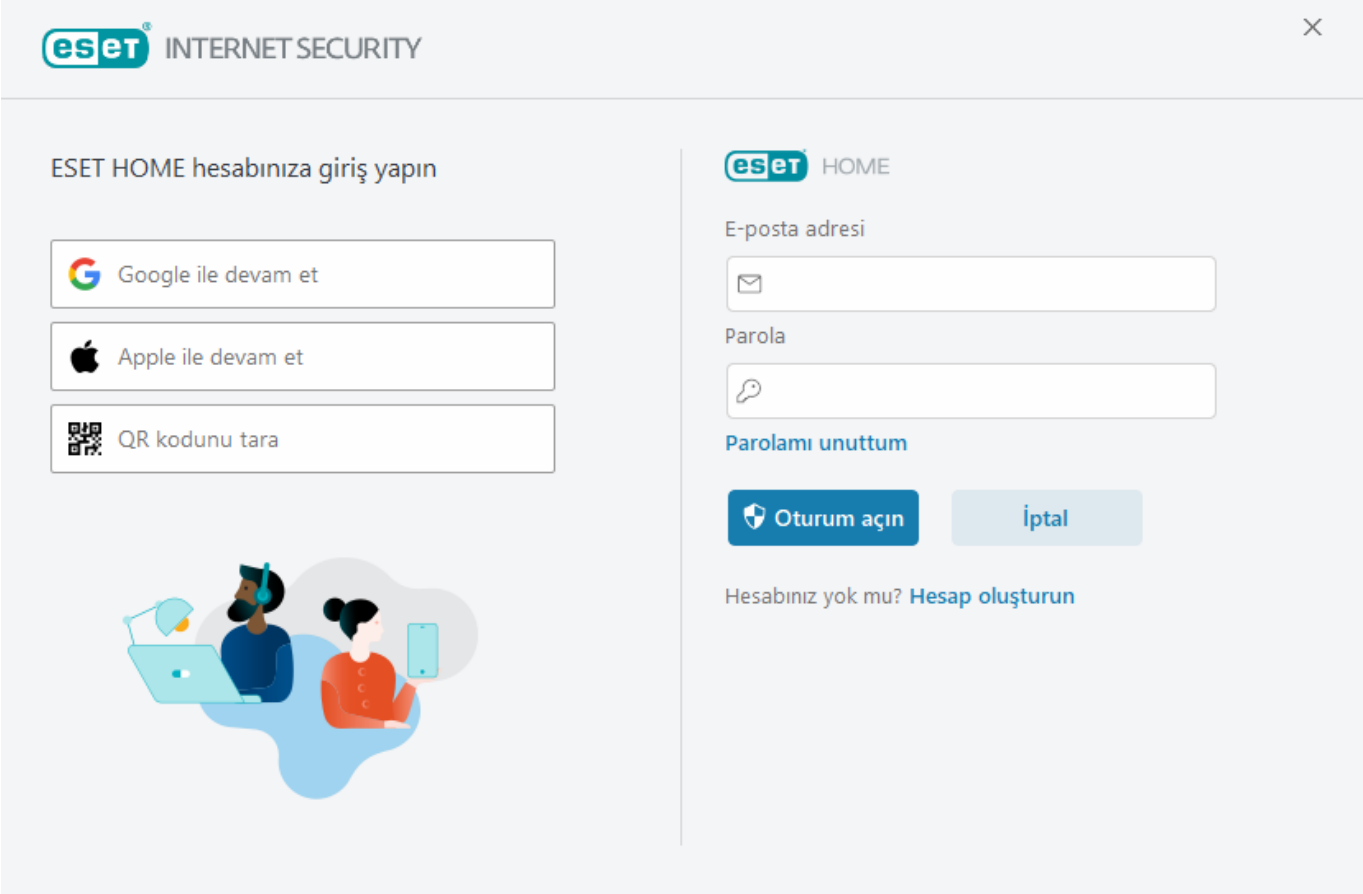
Cihaz adı - Bu cihazın ESET HOME hesabında gösterilen adı.

ESET HOME portalını aç - ESET HOME yönetim portalını açar.

Cihazınızın ESET HOME hesabınızla bağlantısını kesmek için **ESET HOME ile bağlantıyı kes** > **Bağlantıyı kes**'i tıklayın. Etkinleştirme için kullanılan lisans etkin halde kalır ve cihazınız korunur.

ESET HOME Hesabınıza bağlanın

Etkinleştirilen tüm ESET lisanslarınızı ve cihazlarınızı görüntülemek ve yönetmek için cihazınızı ESET HOME hesabına bağlayın. Lisansınızı yenileyebilir, yükseltebilir veya uzatabilir ve önemli lisans ayrıntılarını görüntüleyebilirsiniz. ESET HOME yönetim portalında veya mobil uygulamada farklı lisanslar ekleyebilir, ürünleri cihazlarınıza indirebilir, ürün güvenlik durumunu kontrol edebilir veya lisansları e-posta üzerinden paylaşabilirsiniz. Daha fazla bilgi için ESET HOME Online Yardım'ı ziyaret edin.



Cihazınızı ESET HOME'a bağlayın:

> Yükleme sırasında ESET HOME portalına bağlanıyorsanız veya etkinleştirme yöntemi olarak **ESET HOME hesabını kullan**'ı seçerken ESET HOME hesabını kullanma başlığındaki talimatları uygulayın.
> ESET Internet Security Ürünü zaten yüklenmişse ve ESET HOME hesabınıza eklenmiş bir lisansla etkinleştirilmişse cihazınızı ESET HOME portalını kullanarak ESET HOME aracına bağlayabilirsiniz. ESET HOME Online Yardım kılavuzundaki talimatları uygulayın ve ESET Internet Security ürününde bağlantıya izin verin.

1. Ana program penceresinde, **ESET HOME hesabı** > **ESET HOME ürününe bağlan**'ı veya **Bu cihazı bir ESET HOME hesabına bağlayın** bildirimindeki **ESET HOME ürününe bağlan**'ı tıklayın.

2. ESET HOME hesabınıza giriş yapın.

> ESET HOME hesabınız yoksa kaydolmak için **Hesap oluştur**'u tıklayın veya ESET HOME Online Yardım bölümündeki talimatlara bakın.
> Parolanızı unuttuysanız **Parolamı unuttum** seçeneğini tıklayın ve ekrandaki adımları uygulayın veya ESET HOME Online Yardım bölümüne bakın.

3. Bir **Cihaz adı** belirleyip **Devam**'ı tıklayın.

4. Başarılı bir bağlantının ardından ayrıntılar penceresi görüntülenir. **Bitti**'yi tıklayın.

ESET HOME hesabına giriş yapın

ESET HOME hesabınıza giriş yapmak için birkaç yöntem vardır:

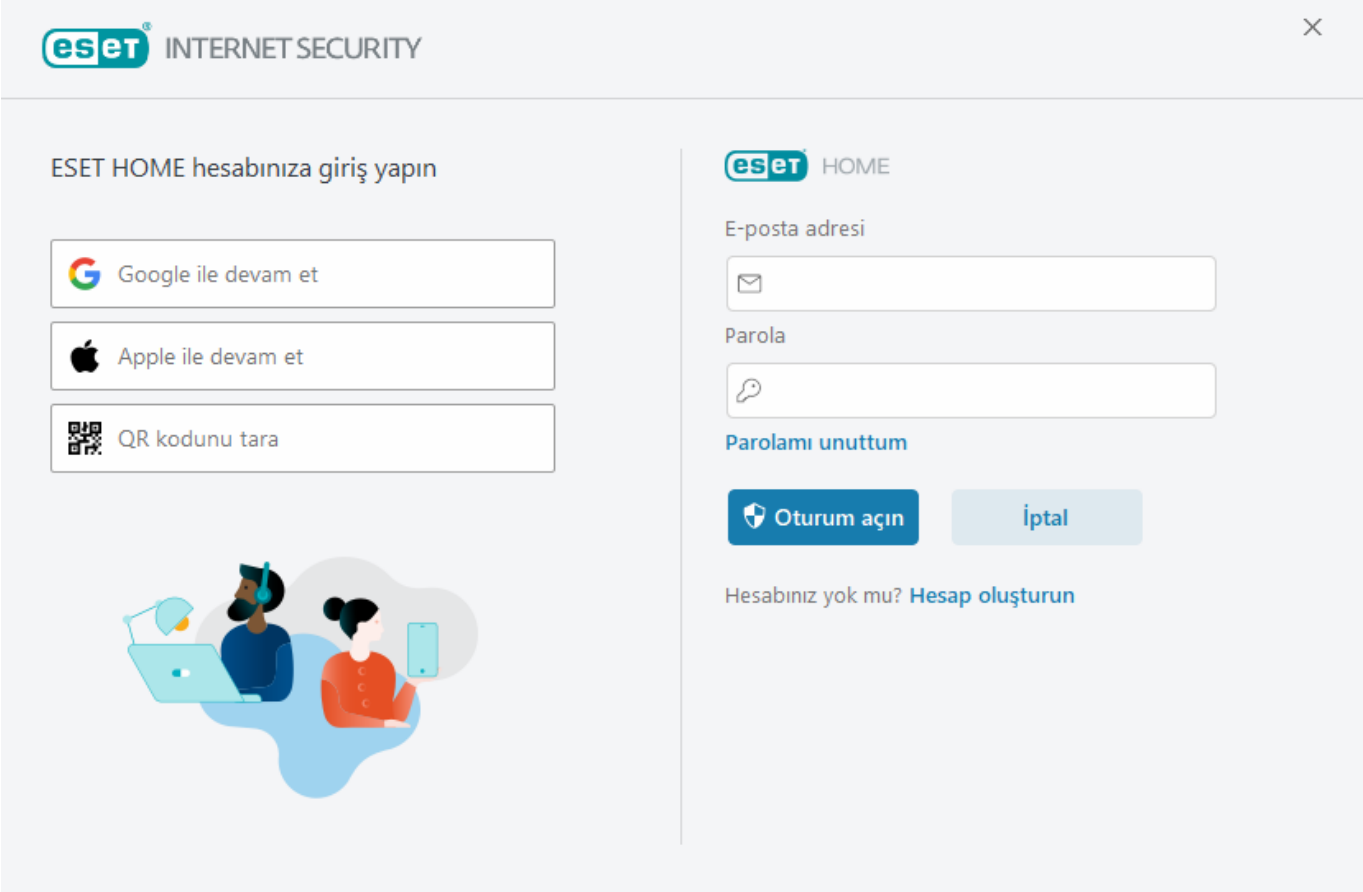
• **ESET HOME E-posta adresinizi ve parolanızı kullanarak** - ESET HOME hesabınızı oluşturmak için kullandığınız **E-posta adresini** ve **Parolayı** yazın ve **Giriş yap**'ı tıklayın.

• **Google Hesabınızı/AppleID** kimliğinizi kullanarak - **Google** ile devam et veya **Apple** ile devam et'i tıklayıp ilgili hesaba giriş yapın. Başarıyla giriş yaptıktan sonra ESET HOME onayı için web sayfasına yönlendirilirsiniz. Devam etmek için ESET ürün pencerenize geri dönün. Google hesabı/AppleID ile giriş yapma hakkında daha fazla bilgi için ESET HOME Online Yardım bölümündeki talimatlara bakın.

• **QR kodunu tarayarak** - QR kodunu görüntülemek için **QR kodunu tara** seçeneğini tıklayın. ESET HOME mobil uygulamanızı açın ve QR kodunu tarayın veya cihaz kameranızı QR koduna tutun. Daha fazla bilgi için ESET HOME Online Yardım bölümündeki talimatlara bakın.

ESET HOME hesabınız yoksa kaydolmak için **Hesap oluştur**'u tıklayın veya ESET HOME Online Yardım bölümündeki talimatlara bakın.
Parolanızı unuttuysanız **Parolamı unuttum** seçeneğini tıklayın ve ekrandaki adımları uygulayın veya ESET HOME Online Yardım bölümüne bakın.

Giriş yapılamadı - sık karşılaşılan hatalar.



Giriş yapılamadı - sık karşılaşılan hatalar

Girilen e-posta adresiyle eşleşen bir hesap bulamadık

Girdiğiniz e-posta adresi hiçbir ESET HOME hesabıyla eşleşmiyor. **Geri**'yi tıklayın ve doğru e-posta adresi ile parolayı yazın.

Giriş yapmak için bir ESET HOME hesabı oluşturmanız gerekir. ESET HOME Hesabınız yoksa **Geri** > **Hesap oluştur**'u tıklayın veya Yeni ESET HOME hesabı oluşturun seçeneğini tıklayın.

Kullanıcı adı ve parola eşleşmiyor

Girilen parola, girilen e-posta adresiyle eşleşmiyor. **Geri**'yi tıklayın, doğru parolayı girin ve girilen e-posta adresinin doğru olduğundan emin olun. Yine de oturum açamazsanız **Geri** > **Parolamı unuttum**'u tıklayarak parolanızı sıfırlayın ve ekran adımlarını takip edin veya ESET HOME parolamı unuttum bölümüne bakın.

Seçili giriş yapma seçeneği hesabınızla eşleşmiyor

Hesabınız sosyal medya hesabınıza bağlandı. ESET HOME hesabına giriş yapmak için **Google ile devam et** veya **Apple ile devam et'i** tıklayın ve ilgili hesaba giriş yapın. Başarıyla giriş yaptıktan sonra ESET HOME onayı için web sayfasına yönlendirilirsiniz. ESET HOME portalında ESET HOME hesabınızdan sosyal medya hesabınızın bağlantısını kesebilirsiniz.

Yanlış parola

Bu hata, ESET Internet Security ürününüz halihazırda ESET HOME hesabına bağlıysa ve giriş yapmanızı gerektiren değişiklikler yapıyorsanız (örneğin, Anti-Theft'i devre dışı bırakmak) ve girdiğiniz parola hesabınızla eşleşmiyorsa ortaya çıkabilir. **Geri**'yi tıklayın ve doğru parolayı yazın. Yine de oturum açamazsanız **Geri** > **Parolamı unuttum**'u tıklayarak parolanızı sıfırlayın ve ekran adımlarını takip edin veya ESET HOME parolamı unuttum bölümüne bakın.

ESET HOME portalında cihaz ekleme

ESET Internet Security ürünü zaten yüklenmişse ve ESET HOME hesabınıza eklenmiş bir lisansla etkinleştirilmişse cihazınızı ESET HOME portalını kullanarak ESET HOME aracına bağlayabilirsiniz:

1. Cihazınıza bir bağlantı isteği gönderin.

2. ESET Internet Security, ESET HOME hesap adıyla birlikte **Bu cihazı bir ESET HOME hesabına bağlayın** iletişim kutusunu görüntüler. Cihazı belirtilen ESET HOME hesabına bağlamak için **İzin ver**'i tıklayın.

Herhangi bir etkileşim olmazsa bağlantı isteği yaklaşık 30 dakika sonra otomatik olarak iptal edilir.

Kullanıcı arabirimi

Programın grafik kullanıcı arabirimi (GUI) davranışını yapılandırmak için ana program penceresinde, **Ayarlar** > **Gelişmiş ayarlar** (F5) >**Kullanıcı arabirimi**'ni tıklayın.

Kullanıcı arabirimi öğeleri Gelişmiş ayarlar ekranında programın görsel görünümünü ve efektlerini düzenleyebilirsiniz.

Güvenlik yazılımınızın maksimum güvenliğini temin etmek için Erişim ayarları aracını kullanarak bir parolayla ayarları koruyabilir ve bu sayede yüklemeyi kaldırma veya yetkisiz değişiklikleri önleyebilirsiniz.

Sistem bildirimlerinin, tespit uyarılarının ve uygulama durumlarının davranışını yapılandırmak için Bildirimler bölümüne bakın.

Kullanıcı arabirimi öğeleri

ESET Internet Security çalışma ortamını (GUI) **Gelişmiş ayarlar** (F5) > **Kullanıcı arabirimi** > **Kullanıcı arabirimi öğeleri**'nde ihtiyaçlarınızı karşılayacak şekilde ayarlayabilirsiniz.

Renk modu - Açılır menüden ESET Internet Security GUI'sinin renk düzenini seçin:

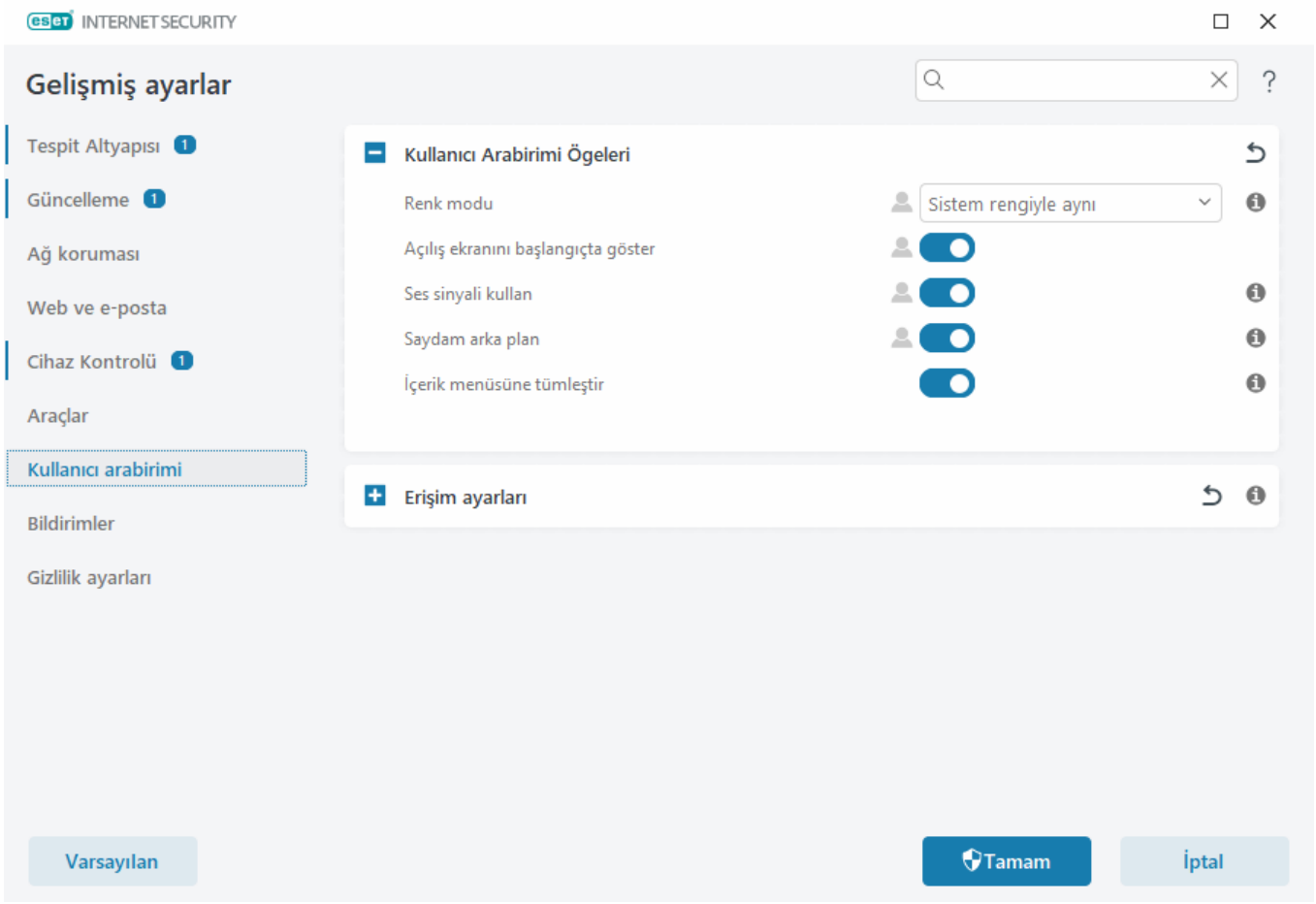
- **Sistem rengiyle aynı** - İşletim sistemi ayarlarınıza göre ESET Internet Security renk düzenini ayarlar.
- **Koyu mod** - ESET Internet Security koyu renk düzeni (koyu mod) sahip olur.
- **Açık** - ESET Internet Security standart, açık renk düzenine sahip olur.

Başlangıçta giriş ekranını göster - Başlatma sırasında ESET Internet Security giriş ekranı görüntülenir.

Ses sinyali kullan - Bir tarama sırasında önemli olaylar gerçekleştiğinde (örneğin, bir tehdit algılandığında veya tarama sona erdiğinde) sesli uyarı verir.

Saydam arka plan - Ana program penceresi için saydam bir arka plan etkisi sağlar. Saydam arka plan yalnızca en son Windows sürümleri (RS4 ve sonrası) için kullanılabilir.

İçerik menüsüne entegre et - ESET Internet Security denetim öğelerini içerik menüsüne dahil eder.



Erişim ayarları

ESET Internet Security ayarları, güvenlik politikanızın önemli bir parçasıdır. Yetkisiz olarak yapılabilecek değişiklikler sisteminizin kararlılığını ve korunmasını tehlikeye atma olasılığı taşır. Yetkisiz değişiklikleri engellemek için ESET Internet Security ürününün ayar parametreleri ve kaldırılması parola korumalı hale getirilebilir.

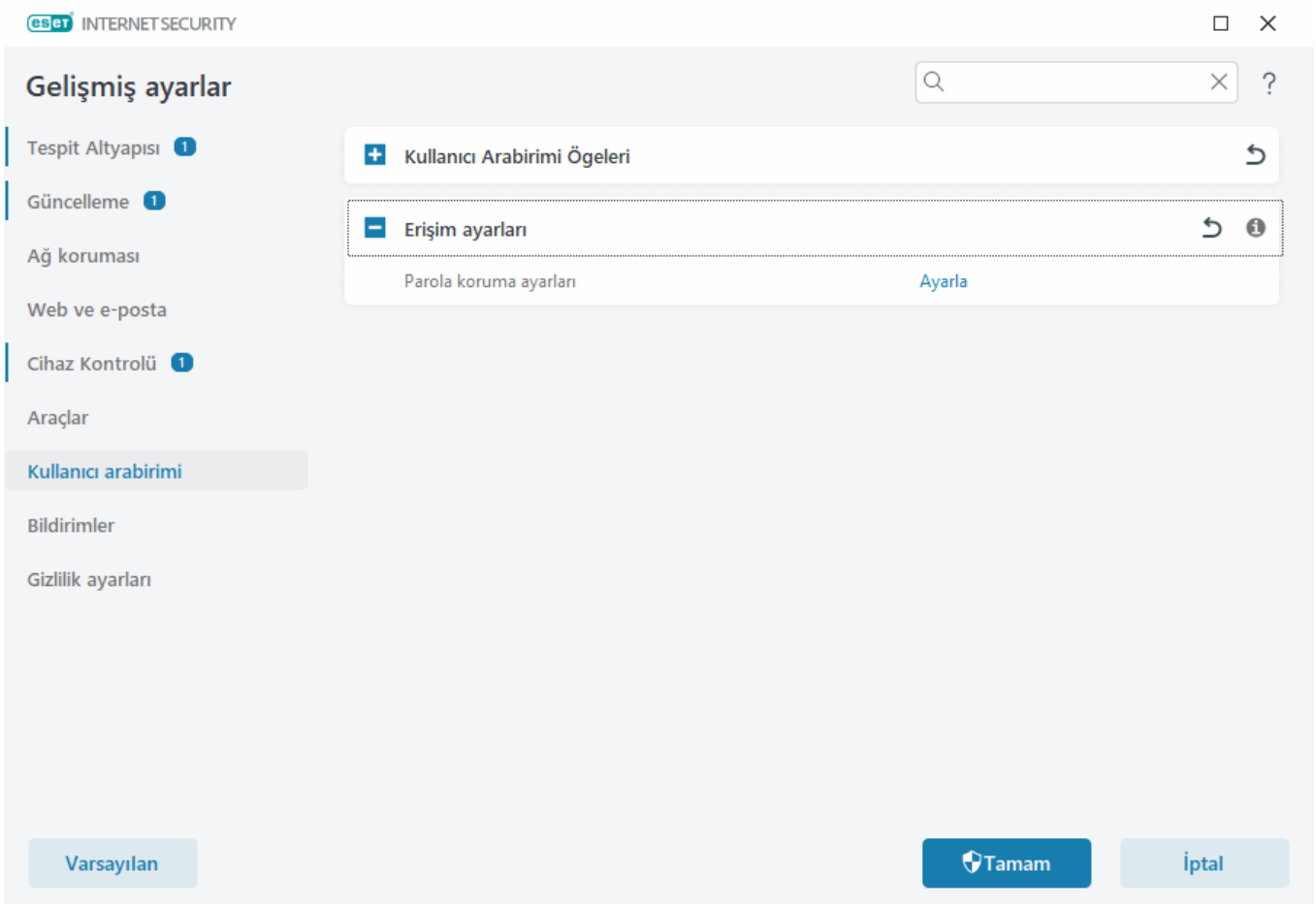
Kurulum parametrelerini korumak ve ESET Internet Security yüklemesini kaldırmayı korumak için **Parola koruma ayarlarının** yanındaki **Ayarla**'yı tıklayın.

Korumalı Gelişmiş ayarlara erişmek istediğinizde parola girişi için bir pencere görüntülenir. Parolanızı unutur veya kaybederseniz, alt taraftaki **Parolayı geri yükle** seçeneğini tıklayın ve lisans kaydı için kullandığınız e-posta adresini girin. ESET size doğrulama kodunu içeren bir e-posta ile parolanızı nasıl sıfırlayacağınızla ilgili talimatları gönderir.

- Gelişmiş ayarların kilidi nasıl açılır?

Parolanızı değiştirmek için **Parola koruma ayarlarının** yanındaki **Parolayı değiştir**'i tıklayın.

Parolanızı kaldırmak için **Parola koruma ayarlarının** yanındaki **Kaldır**'ı tıklayın.



Gelişmiş ayarlar için parola

ESET Internet Security Gelişmiş ayarları'nı korumak ve yetkisiz değişiklikleri önlemek için yeni parolanızı **Yeni parola** ve **Parolayı onaylayın** alanlarına yazın. **Tamam**'ı tıklayın.

Mevcut bir parolayı değiştirmek isterseniz:

1. Eski parolanızı **Eski Parola** alanına yazın.

2. Yeni parolanızı **Yeni Parola** ve **Parolayı onaylayın** alanlarına girin.

3. **Tamam**'ı tıklayın.

Bu parola Gelişmiş ayarlar'a erişim için gerekli olacaktır.

Parolanızı unutursanız ESET ev ürünlerinde ayar koruma parolanızın kilidini açma bölümüne bakın.

Kayıp ESET lisans anahtarınızı kurtarmak veya lisansınızın son kullanma tarihini ya da ESET Internet Security için diğer lisans bilgilerini görmek üzere Lisans anahtarımı kaybettim bölümüne bakın.

Sistem tepsisi simgesi

En önemli kurulum seçeneklerinden ve özelliklerinden bazıları sistem tepsisi simgesini sağ tıklattığınızda kullanılabilir.

Korumayı duraklat - Dosya, web ve e-posta iletişimlerini denetleyerek saldırılara karşı koruma sağlayan Algılama altyapısı'nı devre dışı bırakan onay iletişim kutusunu görüntüler. **Zaman aralığı** açılır menüsü, korumanın ne kadar süreyle devre dışı bırakılacağını belirtmenize olanak sağlar.

Güvenlik duvarını duraklat (tüm trafiğe izin ver) - Güvenlik duvarının etkin olmayan duruma geçmesini sağlar. Daha fazla bilgi için bkz. Ağ.

Tüm ağ trafiğini engelle – Tüm ağ trafiğini engeller. **Tüm ağ trafiğini engellemeyi durdur** öğesini tıklatarak trafiği yeniden etkinleştirebilirsiniz.

Gelişmiş ayarlar - ESET Internet Security Gelişmiş Ayarları'nı açar. Ana ürün penceresinden Gelişmiş ayarları açmak için klavyenizde F5 tuşuna basın veya **Ayarlar** > **Gelişmiş ayarlar**'ı tıklayın.

Günlük dosyaları - Günlük dosyaları, gerçekleşen önemli program olayları hakkında bilgiler içerir ve algılamalara genel bakış sunar.

ESET Internet Security Ürününü aç - ESET Internet Security ana program penceresini açar.

Pencere düzenini sıfırla – ESET Internet Security penceresini ekran üzerindeki varsayılan boyutuna ve konumuna sıfırlar.

Renk modu - GUI'nin renk düzenini değiştirebileceğiniz Kullanıcı Arabirimi ayarları'nı açar.

Güncellemeleri kontrol edin - Korunduğunuzdan emin olmak için bir modül veya ürün güncellemesi başlatır. ESET Internet Security günde birkaç kez otomatik olarak güncellemeleri denetler.

Hakkında - Sistem bilgilerini, ESET Internet Security ürününün yüklü sürümüyle ilgili bilgileri ve yüklenen program modüllerinin yanı sıra işletim sistemi ile sistem kaynakları hakkındaki bilgileri de sağlar.

Ekran okuyucusu desteği

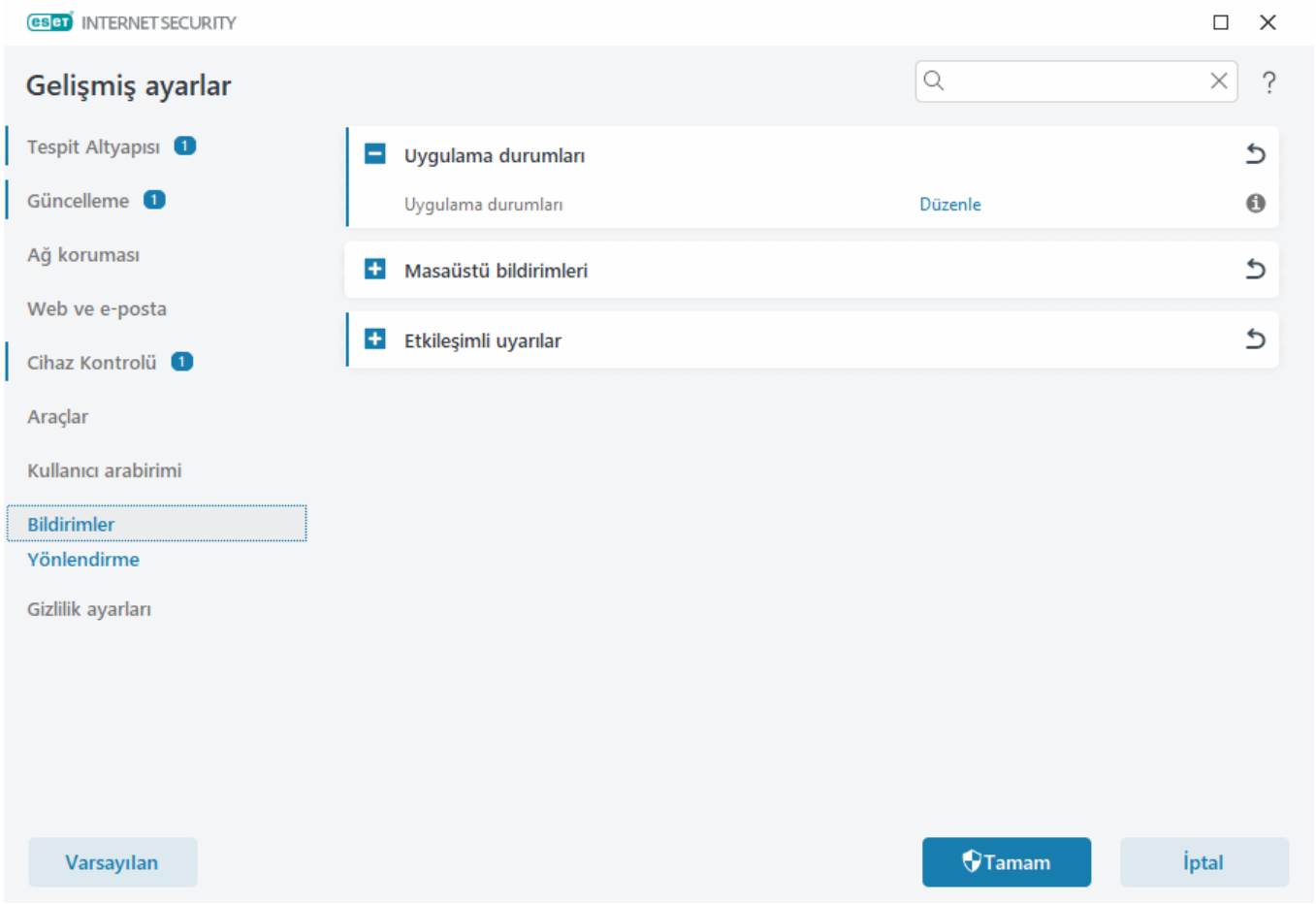
ESET Internet Security, görme bozukluğu olan ESET kullanıcılarının üründe gezinmelerine veya ayarları yapılandırmalarına olanak sağlamak için ekran okuyucularla birlikte kullanılabilir. Aşağıdaki ekran okuyucular desteklenmektedir: (JAWS, NVDA, Narrator) .

Ekran okuyucu yazılımının ESET Internet Security GUI'sine doğru şekilde erişebilmesini sağlamak için Bilgi Bankası makalemizdeki talimatları izleyin.

Bildirimler

ESET Internet Security bildirimlerini yönetmek için **Gelişmiş ayarlar** (F5) > **Bildirimler**'i açın. Aşağıdaki bildirim türlerini yapılandırabilirsiniz:

- Uygulama durumları - Ana program penceresi > **Genel bakış** bölümünde gösterilen bildirimler.
- Masaüstü bildirimleri - Sistem görev çubuğunun yanında küçük açılır pencereler.
- Etkileşimli uyarılar - Kullanıcı etkileşimi gerektiren uyarı pencereleri ve mesaj kutuları.
- Yönlendirme (E-posta bildirimleri) – E-posta bildirimleri belirtilen e-posta adresine gönderilir.



Uygulama durumları

Uygulama durumları - Ana program penceresi > **Genel bakış** bölümünde hangi uygulama durumlarının görüntüleneceğini seçmek için **Düzenle**'yi tıklayın.

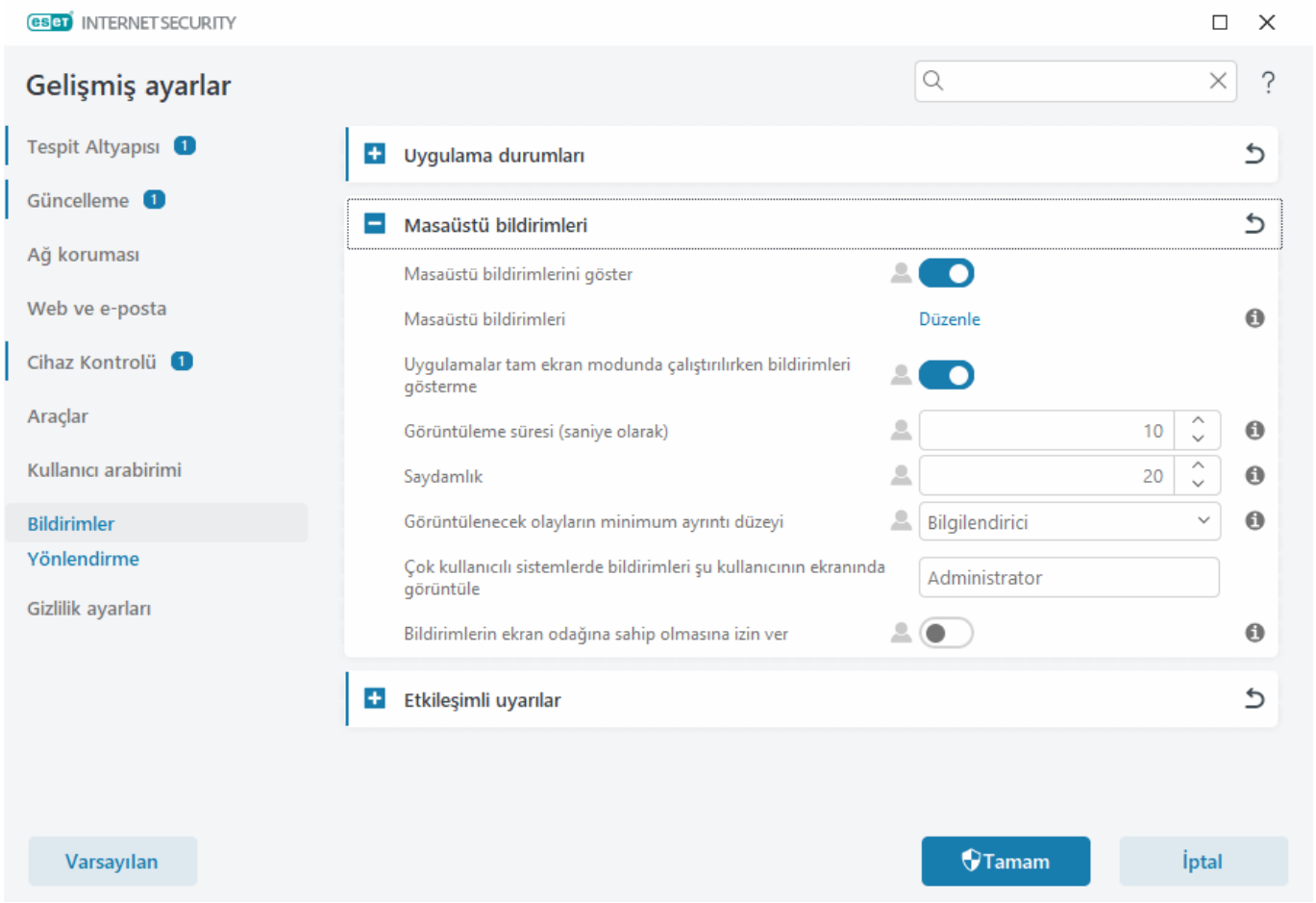
İletişim penceresi - Uygulama durumları

Bu iletişim penceresinde, hangi uygulama durumlarının görüntüleneceğini seçebilirsiniz. Örneğin, Antivirus ve antispyware korumasını duraklattığınızda veya Oyun modunu etkinleştirdiğinizde.

Ayrıca uygulama durumu, ürününüz etkinleştirilmediğinde veya lisansınızın süresi dolduğunda da gösterilir.

Masaüstü bildirimleri

Masaüstü bildirimleri sistem görev çubuğunun yanında küçük bir açılır pencereyle temsil edilir. Varsayılan olarak 10 saniye gösterilecek şekilde ayarlanmıştır, ardından yavaşça kaybolur. Bildirimler; başarılı ürün güncellemeleri, yeni bağlanan cihazlar, virüs tarama görevlerinin tamamlanması veya yeni tehditlerin bulunmasını kapsayabilir.



Bildirimleri masaüstünde göster - Bu seçeneğin etkin halde kalmasını öneririz. Bu sayede, ürün yeni bir olay olduğunda sizi bilgilendirebilir.

Uygulama bildirimleri - Belirli Masaüstü bildirimleri'ni etkinleştirmek veya devre dışı bırakmak için **Düzenle**'yi tıklayın.

Uygulamalar tam ekran modunda çalıştırılırken bildirimleri göster - Uygulamalar tam ekran modunda çalıştırılırken interaktif olmayan tüm bildirimleri bastırır.

Saniye cinsinden zaman aşımı - Bildirim görünürlüğü süresini ayarlayın. Değer 3-30 saniye arasında olmalıdır.

Şeffaflık - Bildirim saydamlığı yüzdesini ayarlayın. Desteklenen aralık 0 (şeffaflık yok) - 80 (çok yüksek şeffaflık) arasındadır.

Görüntülenecek olayların minimum ayrıntı düzeyi – Gösterilen başlangıç bildirimi önem derecesi düzeyini ayarlayın. Açılır menüden aşağıdaki seçeneklerden birini belirleyin:

- **Tanılama** - Programla ilgili hassas ayarlama gerektiren bilgileri ve yukarıdaki tüm kayıtları günlüğe kaydeder.
- **Bilgilendirici** – Başarılı güncelleme iletileri dahil olmak üzere, standart olmayan ağ olayları gibi bilgilendirici iletileri ve yukarıdaki tüm kayıtları kaydeder.
- **Uyarılar** - Uyarı mesajları, hatalar ve kritik hataları gösterir (Antistealth düzgün bir şekilde çalışmıyor veya güncelleme başarısız).
- **Hatalar** - Hataları (örneğin, belge koruması başlatılmadı) ve kritik hataları görüntüler.

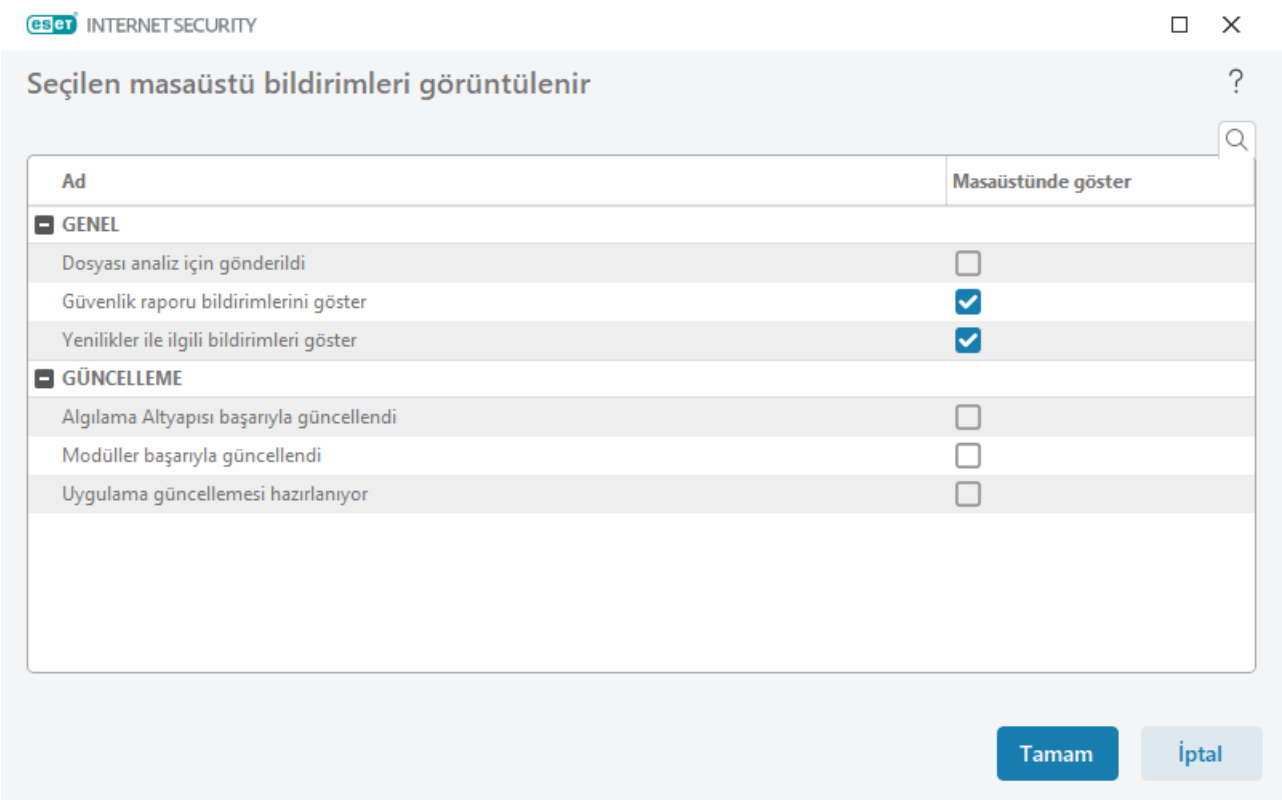
- **Kritik** - Yalnızca kritik hataları gösterir (Antivirus korumasının veya virüs bulaşmış sistemin başlatılmasıyla ilgili hata).

Çok kullanıcılı sistemlerde bildirimleri bu kullanıcının ekranında göster - Seçili hesabın masaüstü bildirimlerini almasına olanak tanır. Örneğin Yönetici hesabını kullanmıyorsanız tam hesap adını yazdığınızda masaüstü bildirimleri belirtilen hesap için gösterilecektir. Yalnızca bir kullanıcı hesabı masaüstü bildirimleri alabilir.

Bildirimlerin ekran odaklı olmasına izin ver - Bildirimlerin ekran odaklı olmasına ve **ALT + Tab** ile erişilebilir olmasına olanak sağlar.

Masaüstü bildirimleri listesi

Masaüstü bildirimlerinin görünürlüğünü ayarlamak için (ekranın sağ alt kısmında görüntülenir) **Gelişmiş ayarlar** (F5) > **Bildirimler** > **Masaüstü bildirimleri**'ni açın. **Masaüstü bildirimlerinin** yanındaki **Düzenle**'yi tıklayın ve ilgili **Göster** onay kutusunu işaretleyin.



Genel

Ekran Güvenliği raporu bildirimleri - Yeni bir Güvenlik raporu üretilen bir bildirim alırsınız.

Yenilikler ile ilgili bildirimleri göster - En son ürün sürümünün tüm yeni ve gelişmiş özellikleriyle ilgili bildirimler.

Dosya analiz için gönderildi - ESET Internet Security ürününün analiz için dosya gönderdiği her seferinde bir bildirim alırsınız.

Güncelleme

Uygulama güncellemesi hazırlanıyor - Hazırlanacak yeni ESET Internet Security sürümüne güncelleme olduğunda

bildirim alırsınız.

Tespit Altyapısı başarıyla güncellendi - Ürün Tespit Altyapısı modüllerini güncellediğinde bir bildirim alırsınız.

Modüller başarıyla güncellendi - Ürün program bileşenlerini güncellediğinde bildirim alırsınız.

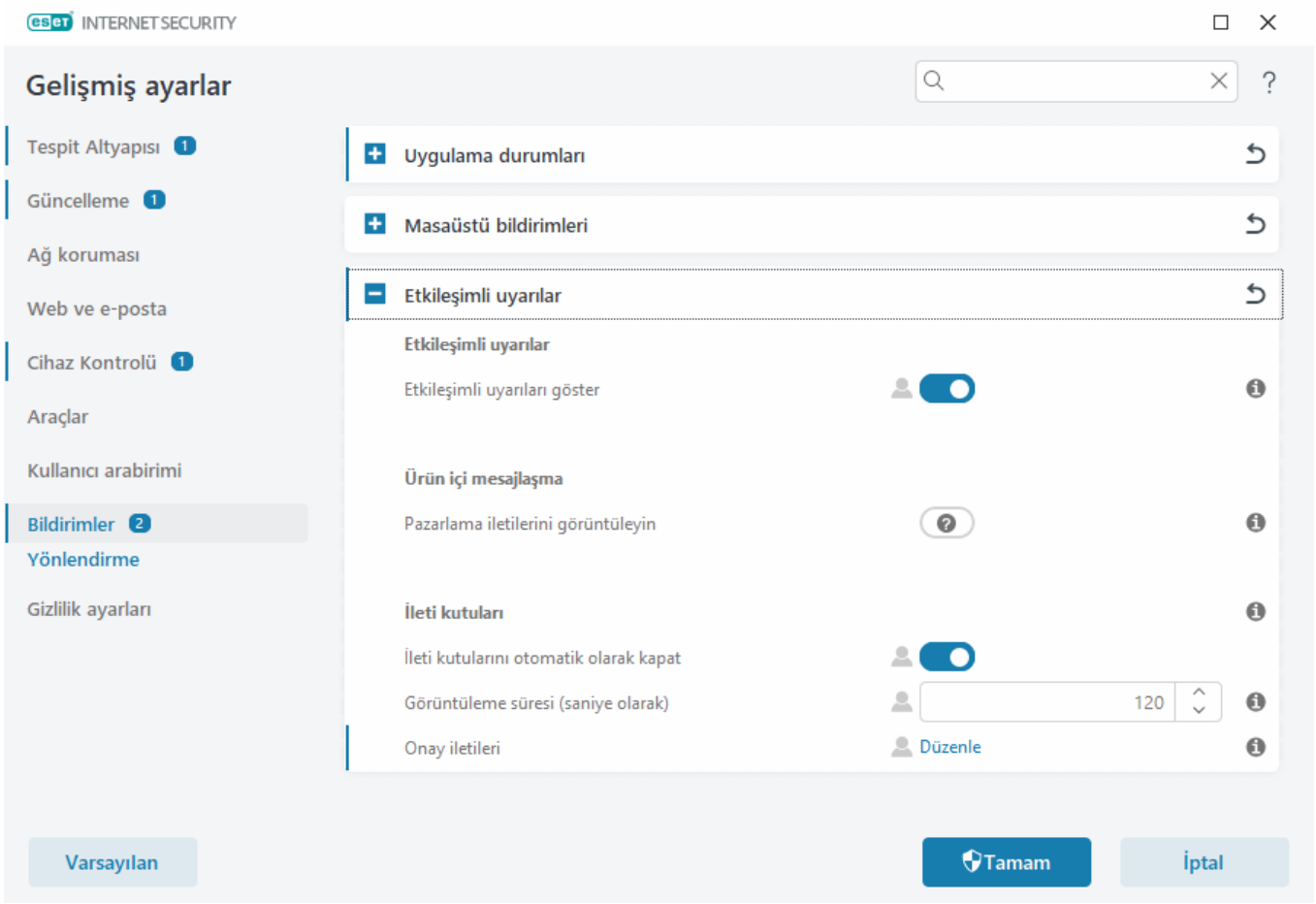
Masaüstü bildirimleri için genel ayarları yapmak üzere (örneğin bir mesajın ne kadar süre gösterileceği veya gösterilecek olayların en düşük ayrıntı düzeyi gibi) **Gelişmiş ayarlar** (F5) > **Bildirimler**'de Masaüstü bildirimleri bölümüne bakın.

Etkileşimli uyarılar

Genel uyarılar ve bildirimler hakkında bilgi edinmek mi istiyorsunuz?

- Tehdit bulundu
- Adres engellendi
- Ürün etkinleştirilmedi
- Daha fazla özelliğe sahip bir ürüne geçiş yapın
- Daha az özelliklere sahip bir ürüne geçiş yapın
- Güncelleme mevcut
- Güncelleme bilgileri tutarlı değil
- "Modül güncellemesi başarısız oldu" iletisi için sorun giderme
- Modül güncelleme hatalarını çözümleme
- Ağ tehdidi engellendi
- Web sitesi sertifikası iptal edildi

Gelişmiş ayarlar (F5) > **Bildirimler**'deki **Etkileşimli uyarılar** bölümü, bir kullanıcı tarafından verilmesi gereken bir karar olması halinde (örneğin, potansiyel kimlik avı web sitesi) tespitler için mesaj kutularının ve interaktif uyarıların ESET Internet Security tarafından algılamalar nasıl işleneceğini yapılandırmanıza olanak tanır.



Etkileşimli uyarılar

İnteraktif uyarıları göster seçeneği devre dışı bırakıldığında, tüm uyarı pencereleri ve tarayıcı içi iletişim kutuları gizlenir. Bu nedenle, bu seçenek yalnızca sınırlı sayıda özel durum için uygundur. ESET bu seçeneğin etkin halde kalmasını önerir.

Ürün içi mesajlaşma

Ürün içi mesajlaşma, ESET haberleri ve diğer iletişimler hakkında kullanıcıları bilgilendirmek üzere tasarlanmıştır. Pazarlama iletileri göndermek için kullanıcının onayı gerekir. Bu nedenle, pazarlama iletileri varsayılan olarak kullanıcıya gönderilmez (soru işaretiyle gösterilir). Bu seçeneği etkinleştirerek ESET pazarlama iletilerini almayı kabul edersiniz. ESET pazarlama malzemelerini almak istemiyorsanız **Pazarlama iletilerini göster** seçeneğini devre dışı bırakın.

İleti kutuları

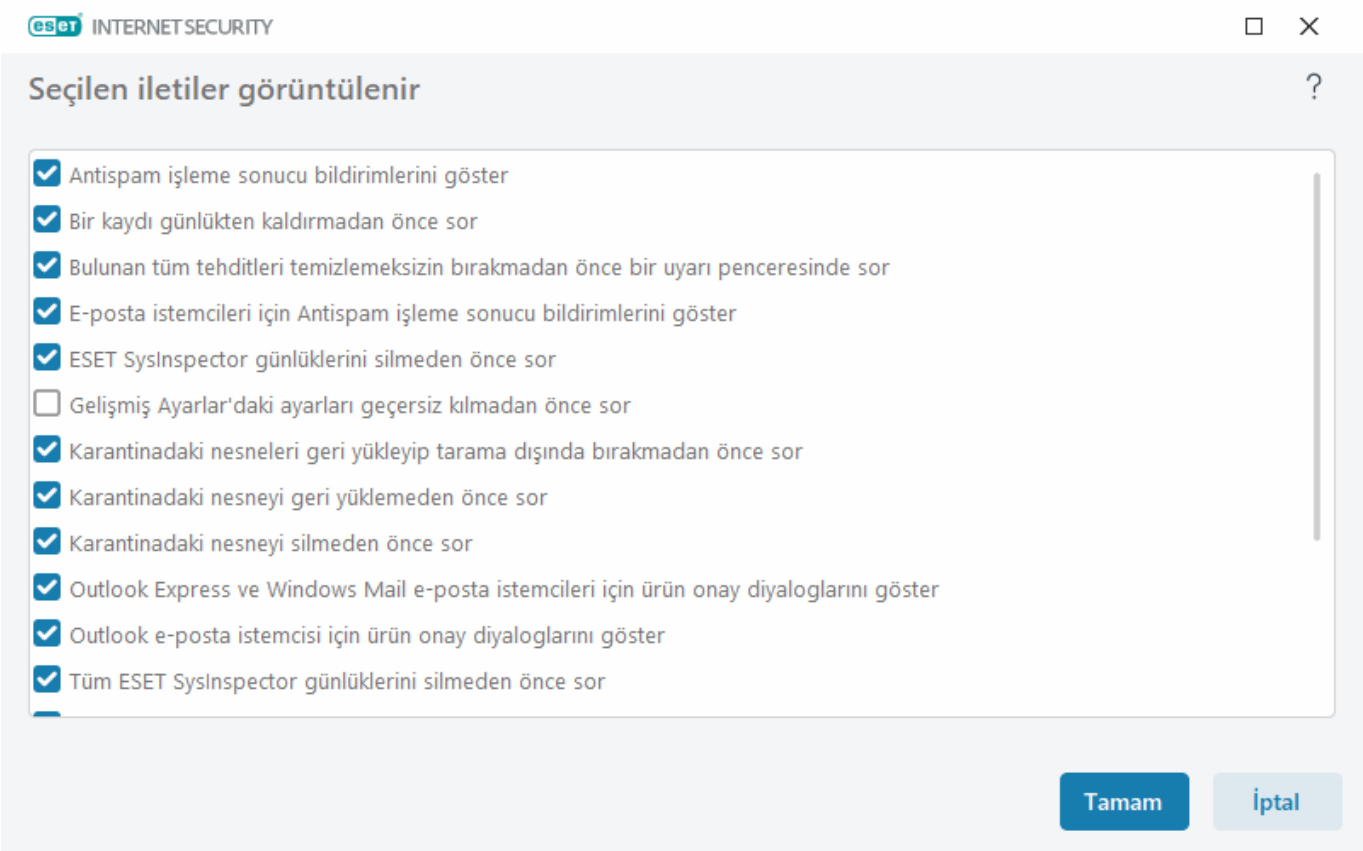
Mesaj kutularını belirli bir sürenin ardından otomatik olarak kapatmak için **Mesaj kutularını otomatik olarak kapat**'ı seçin. Kutular manuel olarak kapatılmazlarsa belirtilen süre geçtikten sonra uyarı pencereleri otomatik olarak kapatılır.

Saniye cinsinden zaman aşımı - Bildirim görünürlüğü süresini ayarlar. Değer 10-999 saniye arasında olmalıdır.

Onay mesajları - Görüntülenmesini veya görüntülenmemesini seçebileceğiniz onay mesajları listesini görmek için **Düzenle**'yi tıklayın.

Onay iletileri

Onay mesajlarını ayarlamak için **Gelişmiş ayarlar** (F5) > **Bildirimler** > **İnteraktif uyarılar**'a gidin ve **Onay mesajları**'nın yanındaki **Düzenle**'yi tıklayın.



Bu iletişim penceresi herhangi bir eylem gerçekleştirilmeden önce ESET Internet Security tarafından gösterilecek onay iletilerini görüntüler. İzin vermek veya devre dışı bırakmak için her bir onay iletisinin yanındaki kutuyu işaretleyin veya işaretini kaldırın.

Onay iletileriyle ilgili belirli özellik hakkında daha fazla bilgi:

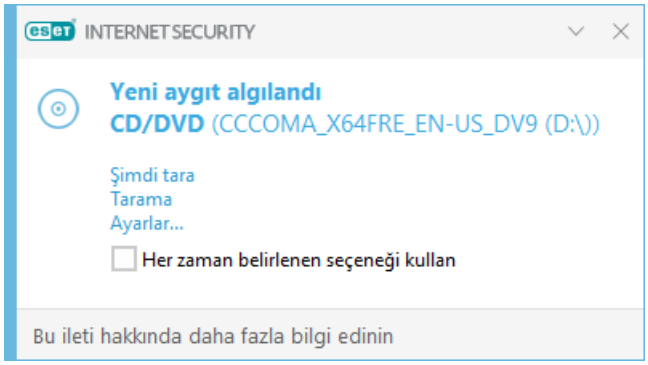
- ESET SysInspector günlüklerini silmeden önce sor
- Tüm ESET SysInspector günlüklerini silmeden önce sor
- Karantinadaki nesneyi silmeden önce sor
- Gelişmiş Ayarlar'daki ayarları geçersiz kılmadan önce sor
- Bulunan tüm tehditleri temizlemeksizin bırakmadan önce bir uyarı penceresinde sor
- Bir kaydı günlükten kaldırmadan önce sor
- Zamanlayıcıda zamanlanmış bir görevi kaldırmadan önce sor
- Tüm günlük kayıtlarını kaldırmadan önce sor
- İstatistikleri sıfırlamadan önce sor

- Karantinadaki nesneyi geri yüklemeden önce sor
- Karantinadaki nesneleri geri yükleyip tarama dışında bırakmadan önce sor
- Zamanlayıcıda zamanlanmış bir görevi çalıştırmadan önce sor
- Antispam işleme sonucu bildirimlerini göster
- E-posta istemcileri için Antispam işleme sonucu bildirimlerini göster
- Outlook Express ve Windows Mail e-posta istemcileri için ürün onay diyaloglarını göster
- Windows Live Mail için ürün onay diyaloglarını göster
- Outlook e-posta istemcisi için ürün onay diyaloglarını göster

Çıkarılabilir medya

ESET Internet Security, bilgisayara takılan çıkarılabilir medya (CD/DVD/USB vs.) için otomatik bir tarama işlemi yapar. Bu işlem, bilgisayar yöneticisi, kullanıcıların izinsiz içerik bulunan çıkarılabilir medyayı kullanmalarını engellemek istediğinde faydalı olabilir.

Çıkarılabilir medya takıldığında ve ESET Internet Security ürününde **Tarama seçeneklerini göster** ayarı seçilmişse aşağıdaki iletişim kutusu gösterilir:



Bu iletişim kutusu için seçenekler:

- **Şimdi tara** – Bu seçenek, çıkarılabilir medyanın taranması işlemini başlatır.
- **Tarama** - Çıkarılabilir medya taranmayacak.
- **Ayarlar** – **Gelişmiş ayarlar** bölümünü açar.
- **Her zaman belirlenen seçeneği kullan** – Bu seçenek belirlendiğinde, çıkarılabilir medyanın her takılışında aynı eylem gerçekleştirilir.

Ayrıca, ESET Internet Security, belirli bir bilgisayarda harici aygıtları kullanmaya yönelik kuralları tanımlayabilme olanağı sağlayan Aygıt denetimi işlevi özelliğine sahiptir. Aygıt denetimi ile ilgili daha fazla ayrıntı Aygıt denetimi bölümünde bulunabilir.

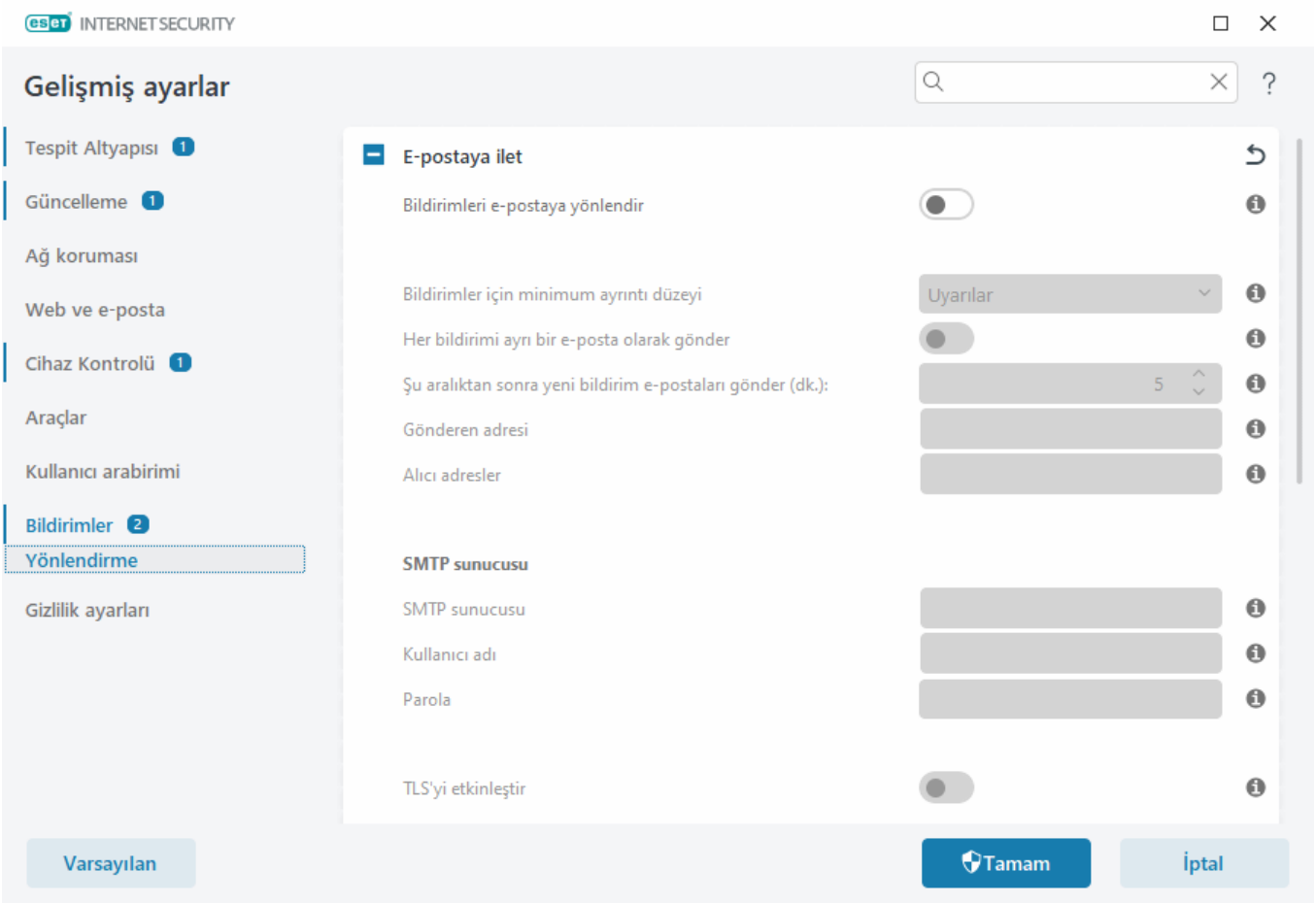
Çıkarılabilir medya taraması ayarlarına erişmek için Gelişmiş ayarlar (**F5**) > **Algılama altyapısı** > **Kötü amaçlı yazılım taramaları** > **Çıkarılabilir medya**'yı açın.

Çıkarılabilir medya takıldıktan sonra gerçekleştirilecek işlem – Bilgisayara bir çıkarılabilir medya (CD/DVD/USB) takıldığında gerçekleştirilecek olan varsayılan işlemi seçin. Bilgisayara bir çıkarılabilir medya takıldığında yapılmasını istediğiniz işlemi seçin:

- **Tarama** – Herhangi bir işlem gerçekleştirilmez ve **Yeni cihaz algılandı** penceresi açılmaz.
- **Otomatik cihaz taraması** – Takılan çıkarılabilir medya cihazı için bir bilgisayar taraması gerçekleştirilir.
- **Tarama seçeneklerini göster** - **Çıkarılabilir medya** ayarları bölümünü açar.

Yönlendirme

ESET Internet Security, seçili ayrıntı düzeyine sahip bir olay meydana gelirse otomatik olarak bildirim e-postaları gönderebilir. **Gelişmiş ayarlar** (F5) > **Bildirimler** > **Yönlendirme**'yi açın ve e-posta bildirimlerini etkinleştirmek için **Bildirimleri e-postaya yönlendir** ayarını etkinleştirin.



Bildirimler için en düşük ayrıntı düzeyi açılır menüsünden, gönderilecek bildirimlerin önemi için başlangıç düzeyi seçebilirsiniz.

- **Tanılama** – Programla ilgili hassas ayarlama gerektiren bilgileri ve yukarıdaki tüm kayıtları günlüğe kaydeder.
- **Bilgilendirici** – Başarılı güncelleme iletileri dahil olmak üzere, standart olmayan ağ olayları gibi bilgilendirici

iletileri ve yukarıdaki tüm kayıtları kaydeder.

• **Uyarılar** - Kritik hataları ve uyarı mesajlarını kaydeder (örneğin, Antistealth düzgün bir şekilde çalışmıyor veya Güncelleme başarısız oldu).

• **Hatalar** – Hatalar (belge koruması başlatılmadı) ve kritik hatalar kaydedilir.

• **Kritik** - Yalnızca kritik hataları günlüğe kaydeder (örneğin, Antivirus korumasını başlatma hatası veya Tehdit bulundu).

Her bildirimi ayrı bir e-posta olarak gönder - Etkinleştirildiğinde alıcı her bildirim için yeni bir e-posta alır. Bu, kısa bir sürede çok sayıda e-posta alınmasına neden olabilir.

Yeni bildirim e-postalarının gönderilme aralığı (dk.) – Dakika cinsinden belirtilen aralığın ardından yeni bildirimler e-posta adresine gönderilir. Bu değeri 0'a ayarlarsanız bildirimler hemen gönderilir.

Gönderen adresi – Bildirim e-postalarının üst bilgisinde görüntülenecek gönderen adresini belirtin.

Alıcı adresi - Bildirim e-postalarının başlığında gösterilecek alıcı adreslerini belirtin. Birden çok değer desteklenir. Lütfen ayırıcı olarak noktalı virgül kullanın.

SMTP sunucusu

SMTP sunucusu - Bildirimleri göndermek için kullanılan SMTP sunucusu (örneğin smtp.provider.com:587, önceden tanımlı bağlantı noktası 25).

TLS şifrelemesine sahip SMTP sunucuları ESET Internet Security tarafından desteklenir.

Kullanıcı adı ve **parola** – SMTP sunucusu kimlik doğrulaması gerektiriyorsa SMTP sunucusuna erişmek için bu alanlar geçerli bir kullanıcı adı ve parola ile doldurulmalıdır.

TLS'yi etkinleştir – TLS şifrelemesini kullanan Secure Alert ve bildirimler.

SMTP bağlantısını test et – Alıcının e-posta adresine bir test e-postası gönderilir. SMTP sunucusu, Kullanıcı Adı, Parola, Gönderici adresi ve Alıcı adresleri alanlarının doldurulması gerekir.

İleti biçimi

Program ile uzak kullanıcı veya sistem yöneticisi arasındaki iletişimler, e-posta veya LAN mesajları (Windows mesaj hizmeti kullanılarak) üzerinden yapılır. Uyarı mesajları ve bildirimleri için **Varsayılan mesaj biçimini kullan** ayarı pek çok durum için en uygun biçimdir. Bazı durumlarda olay mesajlarının mesaj biçimini değiştirmeniz gerekebilir.

Olay iletilerinin biçimi – Uzak bilgisayarlarda görüntülenen olay iletilerinin biçimidir.

Tehdit uyarı mesajlarının biçimi - Tehdit uyarısı ve bildirim mesajları önceden tanımlı varsayılan bir biçime sahiptir. ESET bu biçimi değiştirmemenizi önerir. Ancak bazı durumlarda (örneğin, otomatik e-posta işleme sisteminiz varsa) mesaj biçimini değiştirmeniz gerekebilir.

Karakter kümesi – Bir e-posta iletisini Windows Bölgesel ayarlarına dayalı olarak (örneğin, windows-1250, Unicode (UTF-8), ACSII 7-bit veya Japonca (ISO-2022-JP)) ANSI karakter kodlamasına dönüştürür. Bunun sonucunda, "á", "a" şekline ve bilinmeyen bir sembol de "?" haline dönüşür.

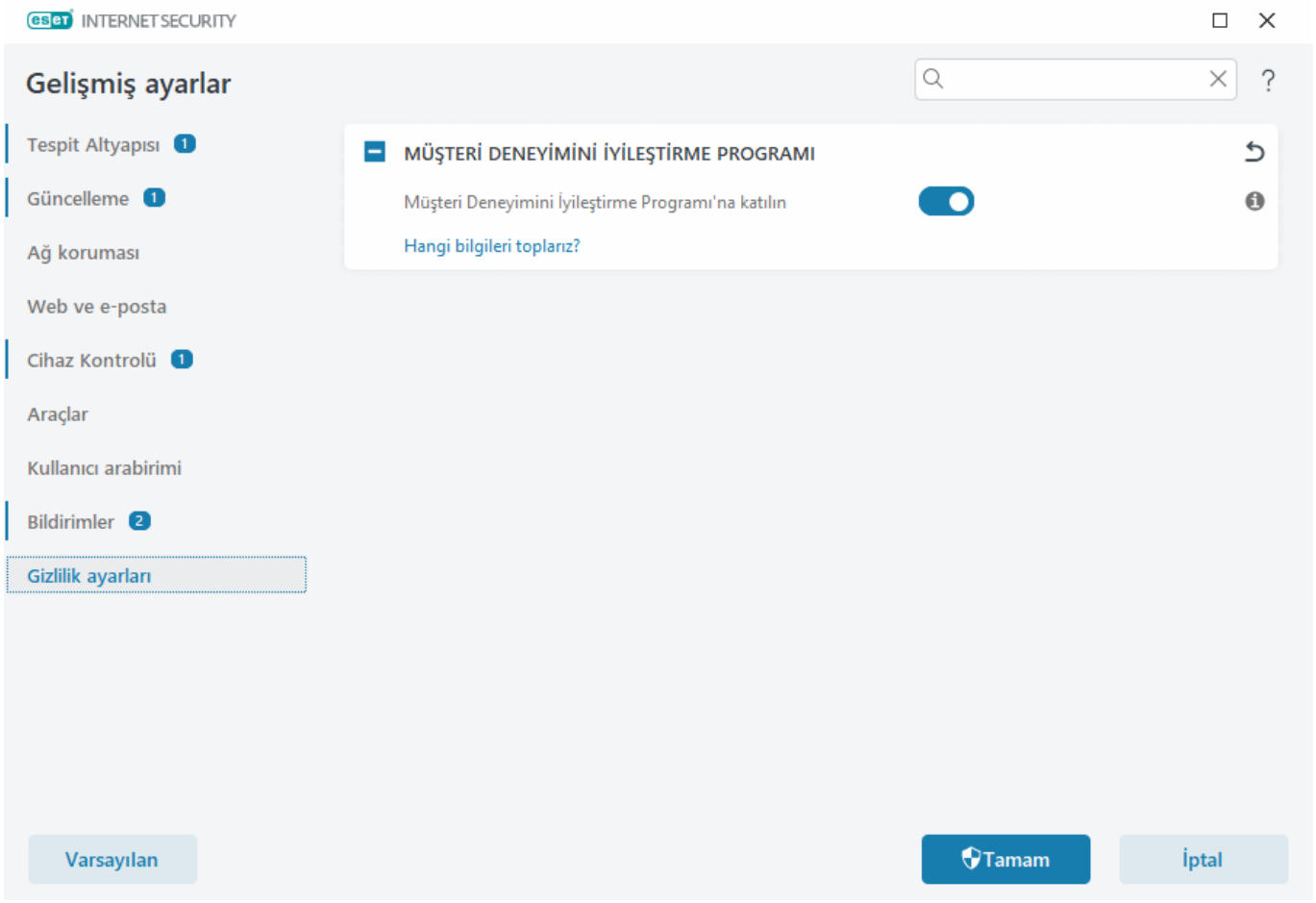
Tırnaklı basılabilir kodlamayı kullan – E-posta iletisi kaynağı, ASCII karakterlerini kullanan ve özel ulusal karakterleri e-posta yoluyla 8 bit biçiminde (áéíóú) düzgün bir şekilde iletebilen Tırnaklı basılabilir (QP) biçimde kodlanır.

- **%TimeStamp%** – Olayın tarihi ve saati
- **%Scanner%** – İlgili modül
- **%ComputerName%** – Uyarının oluştuğu bilgisayarın adı
- **%ProgramName%** – Uyarıyı oluşturan program
- **%InfectedObject%** – Enfekte olan dosyanın, mesajın vs. adı
- **%VirusName%** – Etkilenmenin tanımı
- **%Action%** – Sızıntı üzerine yapılan işlem
- **%ErrorDescription%** – Virüs olmayan olayın açıklaması

%InfectedObject% ve **%VirusName%** anahtar sözcükleri yalnızca tehdit uyarısı iletilerinde kullanılır ve **%ErrorDescription%** yalnızca olay iletilerinde kullanılır.

Gizlilik ayarları

Ana program penceresinde **Ayarlar** > **Gelişmiş ayarlar** (F5) > **Gizlilik ayarları** seçeneğini tıklayın.



Müşteri Deneyimini İyileştirme Programı

Müşteri Deneyimini İyileştirme Programı'na katılmak için **Müşteri Deneyimini İyileştirme Programına Katılın** seçeneğinin yanındaki kaydırma çubuğunu etkinleştirin. Programa katılarak ESET'e ESET ürünlerinin kullanımıyla ilgili anonim bilgileri sağlarsınız. Toplanan veriler, deneyimlerinizi iyileştirmemiz için bize yardımcı olacak ve üçüncü taraflarla hiçbir zaman paylaşılmayacaktır. Hangi bilgileri toplarız?

Profiller

Profil yöneticisi ESET Internet Security ürününde iki yerde kullanılır: **İsteğe bağlı bilgisayar taraması** bölümünde ve **Güncelleme** bölümünde.

Bilgisayar taraması

ESET Internet Security ürününde önceden tanımlanmış 4 tarama profili bulunmaktadır:

- **Smart tarama** – Bu varsayılan gelişmiş tarama profilidir. Smart tarama profili, önceki bir taramada temiz olduğu tespit edilen ve bu taramadan beri değiştirilmemiş dosyaları hariç tutan Smart Optimizasyon teknolojisini kullanır. Bu, sistem güvenliğine en az etkiyle daha kısa tarama süreleri sağlar.

- **İçerik menüsü taraması** – İçerik menüsünden herhangi bir dosyanın isteğe bağlı taramasını başlatabilirsiniz. İçerik menüsü tarama profili, taramayı bu şekilde tetiklediğinizde kullanılacak bir tarama yapılandırması tanımlamanıza olanak tanır.

- **Kapsamlı tarama** – Kapsamlı tarama profili varsayılan olarak Akıllı optimizasyonu kullanmadığından bu profil kullanıldığında hiçbir dosya taramadan hariç tutulmaz.

- **Bilgisayar taraması** – Standart bilgisayar taramasında kullanılan varsayılan profildir.

Tercih edilen tarama parametreleriniz daha sonraki taramalar için kaydedilebilir. Düzenli olarak kullanılan her tarama için farklı bir profil (çeşitli tarama hedefleriyle, tarama yöntemleriyle ve diğer parametrelerle) oluşturmanızı öneririz.

Yeni bir profil oluşturmak için Gelişmiş ayarlar penceresini (F5) açın ve **Algılama altyapısı** > **Kötü amaçlı yazılım taramaları** > **İsteğe bağlı tarama** > **Profil listesi**'ni tıklayın. **Profil yöneticisi** penceresi, mevcut tarama profillerini listeleyen bir **Seçilen profil** açılır menüsü ve yeni bir profil oluşturma seçeneği içerir. İhtiyaçlarınıza uygun bir tarama profili oluşturmanıza yardımcı olması için, tarama ayarlarının her bir parametresine yönelik bir açıklama içeren ThreatSense altyapısı parametre ayarları bölümüne bakın.

> Kendi tarama profilinizi oluşturmak istediğinizi ve **Bilgisayarınızı tarayın** yapılandırmasının kısmi olarak uygun olduğunu, ancak tarama çalışma zamanı paketleyicileri veya tehlikeli olabilecek uygulamaları istemezken, **Algılamayı her zaman düzelt** uygulamak istediğinizi varsayalım. **Profil yöneticisi** penceresinde yeni profilinizin adını girin ve **Ekle** seçeneğini tıklayın. **Seçilen profil** açılır menüsünden yeni profilinizi seçip kalan parametreleri gereksinimlerinize göre ayarladıktan sonra yeni profilinizi kaydetmek için **Tamam**'ı tıklayın.

Güncelleme

Güncelleme ayarları bölümündeki profil düzenleyicisi kullanıcıların yeni güncelleme profilleri oluşturmasına olanak verir. Yalnızca bilgisayarınızda güncelleme sunucularına bağlanmak için birden fazla yöntem kullanılıyorsa

(varsayılan **Profilim** dışında) özel profiller oluşturun ve kullanın.

Örnek olarak, normalde yerel ağdaki yerel bir sunucuya (Yansı) bağlanan, ancak yerel ağ bağlantısı olmadığında (iş gezisi) güncellemeleri doğrudan ESET güncelleme sunucularından indiren bir dizüstü bilgisayar iki profil kullanabilir: İlki yerel sunucuya bağlanmak için diğeri de ESET sunucularından birine bağlanmak için. Bu profiller yapılandırıldıktan sonra **Araçlar** > **Zamanlayıcı** seçeneğine gidin ve güncelleme görevi parametrelerini düzenleyin. Profillerden birini birincil, diğerini de ikincil olarak belirleyin.

Güncelleme profili – Kullanılmakta olan güncelleme profili. Bunu değiştirmek için açılır menüden bir profil seçin.

Profil listesi - Yeni güncelleme profilleri oluşturun veya mevcut güncelleme profillerini kaldırın.

Klavye kısayolları

ESET Internet Security içinde daha iyi gezinmek için aşağıdaki klavye kısa yollarını kullanabilirsiniz:

Klavye kısayolları	Eylem
F1	Yardım sayfalarını açar
F5	Gelişmiş ayarları açar
Yukarı Ok/Aşağı Ok	açılır menü öğelerinde gezinme
TAB	pencerede bir sonraki GUI öğesine taşı
Shift+TAB	bir pencerede bir önceki GUI öğesine taşı
ESC	Etkin iletişim penceresini kapatır
Ctrl+U	ESET lisansıyla ve bilgisayarınızla ilgili bilgileri (Teknik Destek Ayrıntıları) gösterir
Ctrl+R	ürün penceresini ekran üzerindeki varsayılan boyutuna ve konumuna sıfırlar
ALT + Sol Ok	geri git
ALT + Sağ Ok	ileri git
ALT+Home	ana sayfaya git

Ayrıca gezinmek için fare düğmelerini geri veya ileri yönde kullanabilirsiniz.

Tanılamalar

Tanılamalar, ESET işlemleri için uygulamanın kilitlendiği durumların dökümünü sağlar (örneğin: ekrn). Bir uygulama kilitlendiğinde döküm oluşturulur. Bu, geliştiricilerin hataları düzeltmesine ve ESET Internet Security sorunları gidermesine yardımcı olabilir.

Döküm türü öğesinin yanındaki açılır menüyü tıklatın ve mevcut üç seçenekten birini belirleyin:

- Bu özelliği devre dışı bırakmak için **Devre dışı bırak** öğesini seçin.

- **Mini** (varsayılan) – Uygulamanın neden beklenmedik bir şekilde kilitlendiğini belirlemeye yardımcı olabilecek faydalı bilgilerin yer aldığı en küçük kümeyi kaydeder. Bu bilgi döküm dosyası türü, alan kısıtlı olduğunda faydalı olabilir. Ancak dahil edilen bilgiler sınırlı olduğundan bu dosya analiz edildiğinde, sorun oluştuğu sırada çalışan tehdit tarafından doğrudan oluşturulmayan hataların tespit edilmesi mümkün olmayabilir.

- **Tam** – Uygulama beklenmedik bir şekilde durduğunda sistem belleğinin tüm içeriklerini kaydeder. Tam bellek dökümü, bellek dökümü toplanırken çalışmakta olan tüm işlemler hakkında veri içerebilir.

Hedef dizin – Kilitlenme sırasında dökümün oluşturulacağı dizin.

Tanılamalar klasörünü aç – Bu dizini yeni bir *Windows explorer* penceresinde açmak için **Aç** öğesini tıklatın.

Tanı amaçlı döküm oluştur - **Oluştur**'u tıklatarak **Hedef dizinde** tanı amaçlı döküm dosyaları oluşturabilirsiniz.

Gelişmiş günlük kaydı

Pazarlama iletilerinde gelişmiş günlük kaydını etkinleştir - Ürün içindeki pazarlama iletileriyle ilgili tüm olayları günlüğe kaydeder.

Antispam altyapısı gelişmiş günlük kaydı özelliğini etkinleştir – Antispam taraması esnasında meydana gelen tüm olayları kaydeder. Bu, geliştiricilerin ESET Antispam altyapısı ile ilgili sorunları tanılamasına ve düzeltmesine yardımcı olabilir.

Anti-Theft altyapısı gelişmiş günlük kaydını etkinleştirin – Tanılama ve sorunları çözme işlemlerine izin vermek için Anti-Theft yazılımında gerçekleşen tüm olayları kaydeder.

Bankacılık ve Ödeme Sistemleri koruması gelişmiş günlük kaydını etkinleştir - Bankacılık ve Ödeme Sistemleri korumasında meydana gelen tüm olaylar günlüğe kaydedilir.

Bilgisayar Tarayıcısı gelişmiş günlük kaydını etkinleştir - Dosyalar ve klasörler Bilgisayar taraması tarafından taranırken ortaya çıkan sorunları kaydeder.

Cihaz Kontrolü gelişmiş oturum açma özelliğini etkinleştir – Cihaz Kontrolü'nde, gerçekleşen tüm olaylar kaydedilir. Bu, geliştiricilerin Cihaz Kontrolü ile ilgili sorunları tanılamasına ve düzeltmesine yardımcı olabilir.

Direct Cloud gelişmiş günlük kaydını etkinleştir - ESET LiveGrid® meydana gelen tüm olayları kaydeder. Bu, geliştiricilerin ESET LiveGrid® ile ilgili sorunları tanılamasına ve düzeltmesine yardımcı olabilir.

Belge koruması gelişmiş günlük kaydını etkinleştir – Sorunların tanılanmasına ve çözümlenmesine izin vermek için Belge korumasında gerçekleşen tüm olayları kaydedin.

E-posta istemci koruması gelişmiş günlük kaydını etkinleştir - Sorunların tanılanmasını ve çözümlenmesini sağlamak için E-posta istemci koruması ve e-posta istemcisi eklentisinde meydana gelen tüm olayları günlüğe kaydeder.

Kernel gelişmiş günlük kaydını etkinleştir - ESET kernel'de (ekrn) gerçekleşen tüm olayları kaydeder.

Lisans gelişmiş günlük kaydını etkinleştir – ESET etkinleştirmesi veya ESET License Manager sunucularıyla gerçekleşen tüm ürün iletişimlerini kaydeder.

Bellek takibini etkinleştir - Geliştiricilerin bellek sızıntılarını tespit etmesine yardımcı olacak tüm olayları kaydeder.

Ağ koruması gelişmiş günlük kaydını etkinleştir – Geliştiricilerin Güvenlik Duvarı ile ilgili sorunları tespit edip onarmasına yardımcı olmak için Güvenlik Duvarından geçen tüm ağ verilerini PCAP biçiminde kaydeder.

İşletim Sistemi gelişmiş günlük kaydı özelliğini etkinleştir - Çalışan işlemler, CPU etkinliği, disk işlemleri gibi işletim sistemi ile ilgili ek bilgiler kaydedilir. Bu, geliştiricilerin işletim sisteminizde çalışmakta olan ESET ürünüyle ilgili sorunları teşhis edip gidermesine yardımcı olabilir.

Ebeveyn kontrolü gelişmiş oturum açma özelliğini etkinleştir – Ebeveyn kontrolünde meydana gelen tüm olayları kaydeder. Bu, geliştiricilerin Ebeveyn kontrolü ile ilgili sorunları tanılamasına ve düzeltmesine yardımcı olabilir.

Protokol filtrelemesi gelişmiş günlük kaydını etkinleştir – Geliştiricilerin Protokol filtrelemesi ile ilgili sorunları tespit edip onarmasına yardımcı olmak için Protokol filtreleme motorundan geçen tüm verileri PCAP biçiminde kaydedin.

Push mesajlaşması gelişmiş günlük kaydını etkinleştir - Push mesajlaşması sırasında oluşan tüm olayları kaydeder.

Gerçek zamanlı dosya sistemi koruması gelişmiş günlük kaydını etkinleştir - Dosyalar ve klasörler Gerçek zamanlı dosya sistemi koruması tarafından taranırken gerçekleşen tüm olaylar kaydeder.

Altyapı gelişmiş günlük kaydı güncellemesini etkinleştir – Güncelleme işlemi sırasında gerçekleşen tüm olayları kaydedin. Bu, geliştiricilerin Altyapı güncellemesiyle ilgili sorunları teşhis edip gidermesine yardımcı olabilir.

Günlük dosyaları *C:\ProgramData\ESET\ESET Security\Diagnostics* konumunda bulunur.

Teknik Destek

ESET Internet Security ürününden ESET Teknik Destek ile iletişim kurduğunuzda sistem yapılandırma verilerini gönderebilirsiniz. Verileri otomatik olarak göndermek için **Sistem konfigürasyon verilerini gönder** açılır menüsünden **Her zaman gönder**'i seçin veya verileri göndermeden önce sorulması için **Göndermeden önce sor** seçeneğini belirleyin.

Ayarları al ve ver

Özelleştirilmiş ESET Internet Security.xml yapılandırma dosyanızı **Ayarlar** menüsünde alabilir veya verebilirsiniz.

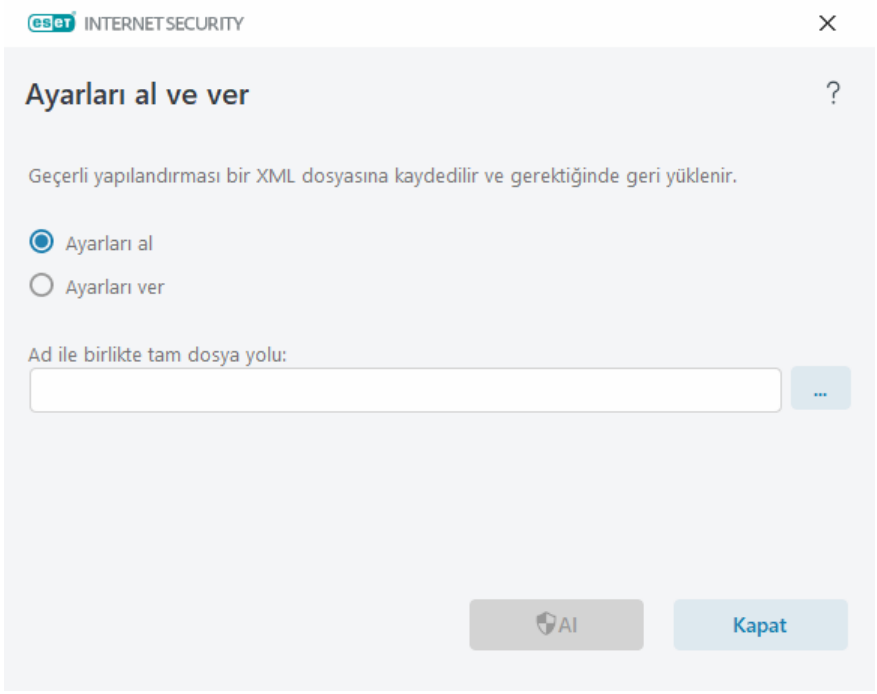
> **Resimli talimatlar**
> İngilizce ve diğer bazı dillerde mevcut olan resimli talimatlar için bir .xml dosyası kullanarak ESET yapılandırma ayarlarını içe veya dışa aktarma bölümüne bakın.

Geçerli ESET Internet Security yapılandırmasını daha sonra kullanmak için yedeklemeniz gerekiyorsa yapılandırma dosyalarını içe veya dışa aktarma işlemi kullanışlıdır. Ayarları dışa aktarma seçeneği aynı zamanda tercih ettiğiniz yapılandırmayı birden fazla sistem üzerinde kullanmak istediğinizde de yararlıdır. Bu ayarları aktarmak için bir .xml dosyasını içe aktarabilirsiniz.

Yapılandırmayı içe aktarmak son derece kolaydır. Ana program penceresi > **Ayarlar** > **Ayarları içe/dışa aktar** öğesini tıklayın ve ardından **Ayarları içe aktar** seçeneğini belirleyin. Yapılandırma dosyasının adını girin veya içe aktarmak istediğiniz yapılandırma dosyasına göz atmak için **...** düğmesini tıklayın.

Bir yapılandırmayı dışa aktarmak için ana program penceresinde **Ayarlar Ayarları İçe/Dışa Aktar**'ı tıklayın. **Ayarları dışa aktar**'ı seçin ve adla birlikte tam dosya yolunu yazın. Yapılandırma dosyasını kaydetmek için bilgisayarınızda bir konuma gitmek üzere **...** seçeneğini tıklayın.

> Verilen dosyanın belirtilen dizine yazılması için yeterli yetkiniz yoksa, ayarları verme işlemi sırasında bir hata ile karşılaşabilirsiniz.



Geçerli bölümdeki tüm ayarları döndürme

Mevcut bölümdeki tüm ayarları ESET tarafından tanımlanan varsayılan ayarlara sıfırlamak için eğik oku tıklayın.

Yapılan tüm değişikliklerin **Varsayılana döndür** seçeneğini tıkladıktan sonra kaybolacağını unutmayın.

Tabloların içeriklerini geri al - Etkinleştirildiğinde, manuel veya otomatik olarak eklenmiş kurallar, görevler veya profiller kaybolacaktır.

Ayarları içe ve dışa aktarma bölümüne de bakın.

Varsayılan ayarlara döndür

Tüm program ayarları, tüm modüller için sahip oldukları durumlara döndürmek amacıyla **Gelişmiş ayarlar'da** (F5) **Varsayılan**'ı tıklayın. Bu, ayarları yeni bir yüklemenin ardından sahip olacakları değerlere sıfırlar.

Ayarları içe ve dışa aktarma bölümüne de bakın.

Yapılandırma kaydedilirken hata oluştu

Bu hata iletisi, bir hata nedeniyle ayarların doğru şekilde kaydedilmediğini belirtir.

Bu, program parametrelerini değiştirmeye çalışan kullanıcı için genellikle şu anlamlara gelir:

- Kullanıcı hakları yeterli değildir veya kullanıcının yapılandırma dosyalarını ve sistem kayıt defterini değiştirmek için gereken işletim sistemi izinleri yoktur.
  > İstenen değişiklikleri yapmak için sistem yöneticisinin oturum açması gerekir.

- Yakın zamanda Host Tabanlı Saldırı Önleme Sistemi (HIPS) veya Güvenlik Duvarı'nda Öğrenme modunu etkinleştirmiş ve Gelişmiş ayarlar'da değişiklik yapmaya çalışmıştır.

> Yapılandırmayı kaydetmek ve yapılandırma çakışmalarını önlemek için kaydetmeden Gelişmiş ayarlar'ı kapatıp istenen değişiklikleri yapmayı tekrar deneyin.

En sık görülen ikinci neden, programın artık düzgün çalışmaması, bozulmuş olması ve bu sebeple yeniden yüklenmesi gerektiği olabilir.

Komut satırı tarayıcısı

ESET Internet Security antivirus modülü komut satırı ile başlatılabilir: manuel olarak (“ecls” komutu yoluyla) veya toplu (“bat”) dosyasıyla.

ESET Komut satırı tarayıcı kullanımı:

```
ecls [OPTIONS..] FILES..
```

Komut satırından isteğe bağlı tarayıcı çalıştırılırken aşağıdaki parametreler ve anahtarlar kullanılabilir:

Seçenekler

/base-dir=KLASÖR	KLASÖR içindeki modülleri yükle
/quar-dir=KLASÖR	karantina KLASÖRÜ
/exclude=MASKE	MASKE ile eşleşen dosyaları tarama dışında bırak
/subdir	alt klasörleri tara (varsayılan)
/no-subdir	alt klasörleri tarama
/max-subdir-level=DÜZEY	taranacak klasörlerdeki maksimum klasör alt seviyesi
/symlink	sembolik bağlantıları izle (varsayılan)
/no-symlink	sembolik bağlantıları atla
/ads	ADS'leri tara (varsayılan)
/no-ads	ADS'leri tarama
/log-file=DOSYA	çıkışı DOSYA'ya kaydet
/log-rewrite	çıkış dosyasının üzerine yaz (varsayılan – sonuna ekle)
/log-console	çıkışı konsola kaydet (varsayılan)
/no-log-console	çıkışı konsola kaydetme
/log-all	ayrıca temiz dosyaları da günlüğe kaydet
/no-log-all	temiz dosyaları günlüğe kaydetme (varsayılan)
/aind	aktivite göstergesini göster
/auto	tüm yerel diskleri otomatik olarak tara ve temizle

Tarayıcı seçenekleri

/files	dosyaları tara (varsayılan)
/no-files	dosyaları tarama
/memory	belleği tara

/boots	önyükleme kesimlerini tara
/no-boots	önyükleme kesimlerini tarama (varsayılan)
/arch	arşivleri tara (varsayılan)
/no-arch	arşivleri tarama
/max-obj-size=BOYUT	yalnızca BOYUT megabayt'tan küçük dosyaları tara (varsayılan 0 = sınırsız)
/max-arch-level=DÜZEY	taranacak arşivlerdeki (derin arşivler) maksimum arşiv alt seviyesi
/scan-timeout=SINIR	arşivleri en çok SINIR saniye süreyle tara
/max-arch-size=BOYUT	arşivlerde yalnızca BOYUT (varsayılan 0 = sınırsız) boyutundan küçük dosyaları tara
/max-sfx-size=BOYUT	kendiliğinden açılan arşiv dosyalarını yalnızca BOYUT megabayt'tan (varsayılan 0 = sınırsız) küçükse tara
/mail	e-posta dosyalarını tara (varsayılan)
/no-mail	e-posta dosyalarını tarama
/mailbox	posta kutularını tara (varsayılan)
/no-mailbox	posta kutularını tarama
/sfx	kendiliğinden açılan arşiv dosyalarını tara (varsayılan)
/no-sfx	kendiliğinden açılan arşiv dosyalarını tarama
/rtp	çalışma zamanı paketleyicilerini tara (varsayılan)
/no-rtp	çalışma zamanı paketleyicilerini tarama
/unsafe	tehlikeli olabilecek uygulamaları tara
/no-unsafe	tehlikeli olabilecek uygulamaları tarama (varsayılan)
/unwanted	istenmeyen türden olabilecek uygulamaları tara
/no-unwanted	istenmeyen türden olabilecek uygulamaları tarama (varsayılan)
/suspicious	şüpheli uygulamaları tara (varsayılan)
/no-suspicious	şüpheli uygulamaları tarama
/pattern	imzaları kullan (varsayılan)
/no-pattern	imzaları kullanma
/heur	sezgisel taramayı etkinleştir (varsayılan)
/no-heur	sezgisel taramayı devre dışı bırak
/adv-heur	Gelişmiş sezgisel taramayı etkinleştir (varsayılan)
/no-adv-heur	Gelişmiş sezgisel taramayı devre dışı bırak
/ext-exclude=UZANTILAR	iki noktayla ayrılmış UZANTILAR dosyası tarama dışında kalsın
/clean-mode=MOD	etkilenmiş nesneler için temizleme MODUNU kullan Aşağıdaki seçenekler kullanılabilir: • `none` (varsayılan) – Otomatik temizleme oluşmaz. • `standard` – ecls.exe etkilenen dosyaları otomatik olarak temizlemeye veya silmeye çalışır. • `katı` – ecls.exe kullanıcı müdahalesi olmadan etkilenen dosyaları otomatik olarak temizlemeye veya silmeye çalışır (dosyalar silinmeden önce sizden herhangi bir istemde bulunulmaz). • `ayrıntılı` – ecls.exe dosyanın ne olduğu fark etmeksizin, temizlemeye çalışmadan dosyaları siler. • `sil` – ecls.exe temizlemeye çalışmadan dosyaları siler, ancak Windows sistem dosyaları gibi hassas dosyaları silmekten kaçınır.

/quarantine	etkilenen dosyaları (temizlendiyse) Karantinaya kopyala (temizleme işlemi sırasında gerçekleştirilen eylemi tamamlar)
/no-quarantine	etkilenen dosyaları Karantinaya kopyalama

Genel seçenekler

/help	yardımı göster ve çık
/version	sürüm bilgisini göster ve çık
/preserve-time	son erişim zaman damgasını koru

Çıkış kodları

0	tehdit bulunmadı
1	tehdit bulundu ve temizlendi
10	bazı dosyalar taranamadı (tehdit olabilirler)
50	tehdit bulundu
100	hata

100'den büyük çıkış kodları dosyanın taranmamış olduğu ve bu nedenle etkilenmiş olabileceği anlamına gelir.

ESET CMD

Bu, gelişmiş ecmd komutlarını etkinleştiren bir özelliktir. Komut dosyasını kullanarak (ecmd.exe) ayarları dışa ve içe aktarmanıza olanak sağlar. Şimdiye kadar, GUI kullanılarak ayarları yalnızca dışarı aktarmak mümkündü. ESET Internet Security yapılandırması bir *.xml* dosyasına aktarılabilir.

ESET CMD özelliğini etkinleştirdiğinizde, iki yetkilendirme yöntemi kullanılabilir:

- **Yok** – Yetkilendirme yoktur. Bu yöntem imzalanmamış tüm yapılandırmaların içe aktarılmasına izin vereceğinden ve bu durum potansiyel risk taşıyacağından, bu yöntemi kullanmanızı önermeyiz.
- **Gelişmiş ayarlar parolası** – Bir yapılandırmayı .xml dosyasından içe aktarmak için parola gereklidir. Bu dosya imzalanmış olmalıdır (aşağıda .xml yapılandırma dosyasının imzalanması bölümüne bakın). Erişim Ayarları'nda belirtilen parola, yeni yapılandırma içe aktarılmadan önce sağlanmalıdır. Erişim ayarlarınız etkin değilse, parolanız eşleşmez veya .xml yapılandırma dosyası imzalanmaz, bu durumda yapılandırma içe aktarılmayacaktır.

ESET CMD etkinleştirildikten sonra, ESET Internet Security yapılandırmalarını içe veya dışa aktarmak için komut satırını kullanabilirsiniz. Bunu manuel olarak yapabilir veya otomasyon amacıyla bir betik oluşturabilirsiniz.

Gelişmiş ecmd komutlarını kullanmak için bu komutları yönetici haklarıyla çalıştırmanız veya **Yönetici olarak çalıştır** seçeneğini kullanarak Windows Komut İstemi'ni (cmd) açmanız gerekir. Aksi halde, **Error executing command** mesajı alırsınız. Ayrıca yapılandırmayı dışa aktarmak için hedef klasör mevcut olmalıdır. Dışa aktarma komutu, ESET CMD ayarı kapatıldığında da çalışmaya devam eder.

Dışa aktarma ayarları komutu:
`ecmd /getcfg c:\config\settings.xml`

İçe aktarma ayarları komutu:
`ecmd /setcfg c:\config\settings.xml`

Gelişmiş ecmd komutları yalnızca yerel olarak çalıştırılabilir.

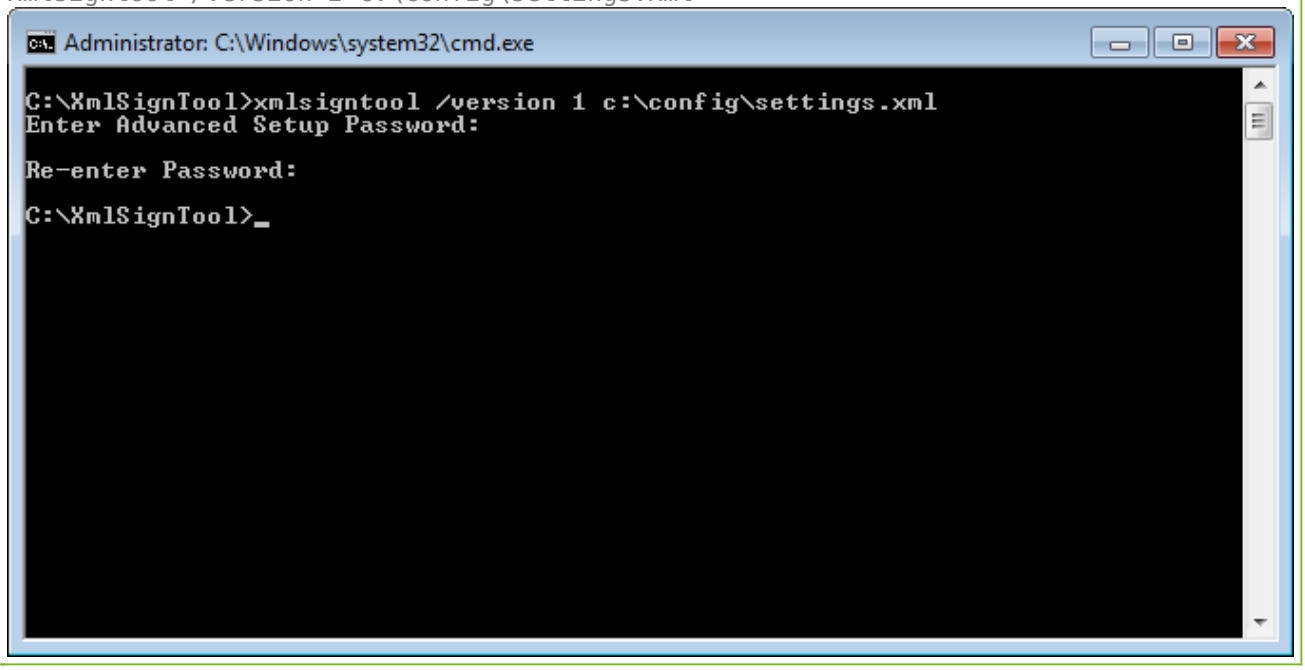
.xml yapılandırma dosyasını imzalama:

1. XmlSignTool yürütülebilir dosyasını indirin.
2. Windows Komut İstemi'ni (cmd) **Yönetici olarak çalıştır** seçeneğini kullanarak açın.
3. Şu dosyanın kayıt konumuna gidin: `xmlsigntool.exe`
4. *.xml* yapılandırma dosyasını imzalamak için bir komut yürütün. Kullanım: `xmlsigntool /version 1|2 <xml_file_path>`

`/version` Parametresinin değeri kullandığınız ESET Internet Security sürümüne bağlıdır. ESET Internet Security 11.1'den daha eski sürümler için `/version 1` kullanın. Geçerli ESET Internet Security sürümü içinse `/version 2` sürümünü kullanın.

5. Gelişmiş Ayarlar Parolanızı XmlSignTool tarafından istendiğinde girin ve yeniden girin. *.xml* yapılandırma dosyanız şimdi imzalanmıştır ve parola yetkilendirme yöntemi kullanılarak ESET CMD ile başka bir ESET Internet Security bilgisayarında içe aktarma için kullanılabilir.

Dışa aktarılan yapılandırma dosyası imzalama komutu:
`xmlsigntool /version 2 c:\config\settings.xml`



Erişim Ayarı parolası değiştirilirse ve önceden eski bir parolayla imzalanmış bir yapılandırmayı içe aktarmak istiyorsanız *.xml* yapılandırma dosyasını geçerli parolanızı kullanarak yeniden imzalayabilirsiniz. Bu, içe aktarma işleminden önce ESET Internet Security aracını çalıştırarak dosyayı başka bir makineye aktarmanıza gerek kalmadan, eski yapılandırma dosyasını kullanmanıza olanak sağlar.

ESET CMD'yi kimlik doğrulama yöntemi olmadan etkinleştirmeniz önerilmez. Bu durum, imzalanmamış tüm yapılandırmanın içe aktarılmasına izin verecektir. Bu durum, imzalanmamış tüm yapılandırmanın içe aktarılmasına izin verecektir. Kullanıcılar tarafından yetkisiz değişiklikler yapılmasını önlemek için **Gelişmiş ayarlar** > **Kullanıcı arabirimi** > **Erişim ayarları** bölümünde parola ayarlayın.

Boşta durumunun algılanması

Boşta durumunu algılama ayarları, **Gelişmiş ayarlar**'da, **Algılama altyapısı** > **Kötü amaçlı yazılım taramaları** > **Boşta durumu taraması** > **Boşta durumunun algılaması** altında yapılandırılabilir. Bu ayarlar Boşta durumu taraması için şu durumlarda tetikleme gerçekleştirir:

- **Kilit ekranı veya ekran koruyucu**
- **Bilgisayar kilidi**
- **Kullanıcı oturumunu kapatma**

Farklı boşta durumu tespit tetikleyicilerini etkinleştirmek veya devre dışı bırakmak için her bir ilgili durumun kaydırma çubuğunu kullanın.

Genel Sorular

En sık sorulan soruların ve karşılaşılan sorunların bazılarını aşağıda bulabilirsiniz. Sorununuzu nasıl çözebileceğinizi bulmak için konu başlığını tıklatın:

- ESET Internet Security nasıl güncellenir?
- Bilgisayarımdaki virüsü nasıl kaldırırım
- Belirli bir uygulama için iletişime nasıl izin verilir
- Bir hesap için Ebeveyn kontrolünün etkinleştirilmesi
- Zamanlayıcıda yeni bir görev oluşturulması
- Tarama görevini (haftalık olarak) zamanlama
- "Bankacılık ve Ödeme Sistemleri Koruması istenen web sayfasına yönlendiremedi" hatası nasıl çözümlenir?
- Gelişmiş ayarların kilidi nasıl açılır?
- Ürünün ESET HOME üzerinden devre dışı bırakılması nasıl çözümlenir?

Sorununuz yukarıdaki listede yer almıyorsa ESET Internet Security Online Yardım'da aramayı deneyin.

Sorununuzun çözümünü veya sorunuzun yanıtını ESET Internet Security Online Yardım'da bulamazsanız düzenli olarak güncellenen online ESET Bilgi Bankası'nı ziyaret edebilirsiniz. En popüler Bilgi Bankası makalelerimizin bağlantıları aşağıda yer almaktadır:

- Lisansımı nasıl yenileyeceğim?

- ESET ürünümü yüklerken bir etkinleştirme hatası aldım. Bunun anlamı nedir?
- Lisans anahtarını kullanarak ESET Windows ev ürünümü etkinleştirme
- ESET ev ürünümü kaldır veya yeniden yükle
- ESET yüklememin zamanından önce sona erdiğine ilişkin ileti aldım
- Lisansımı yeniledikten sonra ne yapmam gerekir? (Ev sürümü kullanıcıları)
- E-posta adresimi değiştirirsem ne olur?
- ESET ürünümü yeni bir bilgisayara veya cihaza aktarma
- Windows, Güvenli Modda veya ağ ile Güvenli Modda nasıl başlatılır?
- Güvenilir bir web sitesini engelleme işlevinin dışında bırakma
- ESET GUI'sine ekran okuyucu yazılımı için erişim izni verin

Gerektiğinde sorularınız veya sorunlarınız için Teknik Destek bölümümüzle iletişim kurabilirsiniz.

ESET Internet Security nasıl güncellenir?

ESET Internet Security güncellemesi manuel veya otomatik olarak gerçekleştirilebilir. Güncellemeyi başlatmak için **Güncelle** bölümünde **Şimdi güncelle** seçeneğini tıklayın.

Varsayılan yükleme ayarları, her saat gerçekleştirilen otomatik bir güncelleme görevi oluşturur. Aralığı değiştirmeniz gerekirse lütfen şuraya gidin: **Araçlar** > **Diğer araçlar** > **Zamanlayıcı**.

Bilgisayarımdaki virüsü nasıl kaldırırım

Bilgisayarınız kötü amaçlı yazılımdan etkilenme belirtileri gösteriyorsa, örneğin yavaşlıyor, sıkça kilitleniyorsa aşağıdakileri yapmanızı öneririz:

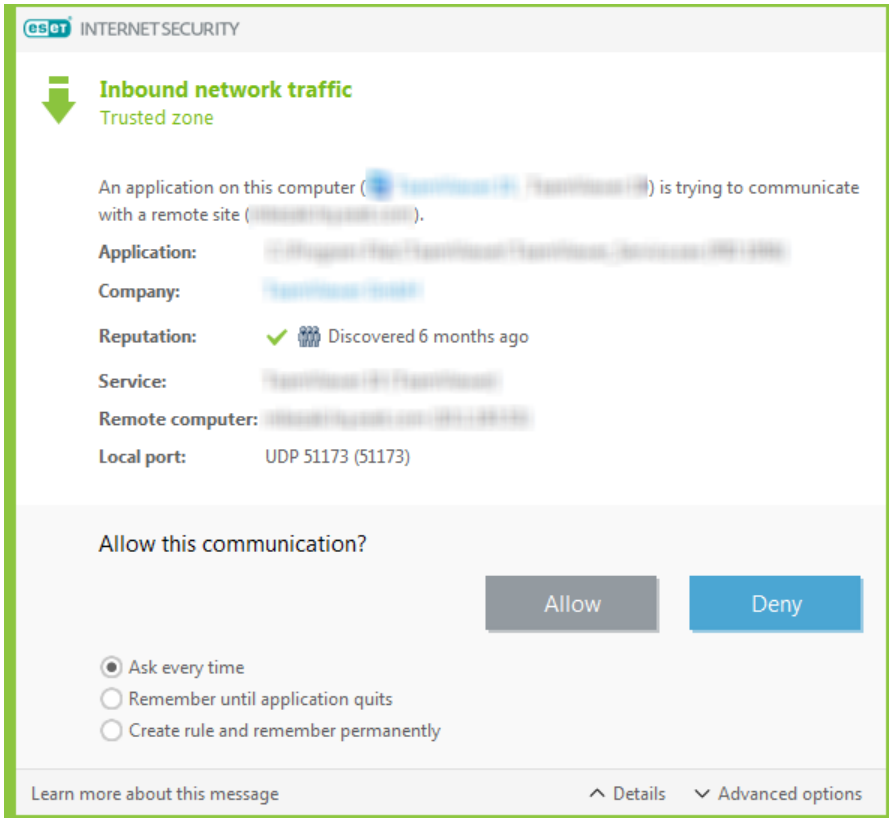
1. Ana program penceresinde **Bilgisayar taraması** seçeneğini tıklatın.
2. Sisteminizi taramaya başlamak için **Bilgisayarınızı tarayın** seçeneğine tıklatın.
3. Tarama bittikten sonra günlüğe bakarak taranan, etkilenen ve temizlenen dosya sayısını inceleyin.
4. Diskinizin yalnızca belirli bir bölümünü taramak istiyorsanız **Özel tarama**'yı tıklayın ve virüs taraması yapılacak hedefleri seçin.

Ek bilgiler için lütfen düzenli olarak güncellenen ESET Bilgi Bankası makalesini okuyun.

Belirli bir uygulama için iletişime nasıl izin verilir

Etkileşimli modda yeni bir bağlantı tespit edilirse ve eşleşen bir kural yoksa sizden bağlantıya izin **vermeniz** veya **engellemeniz** istenir. Uygulama bağlantı kurmayı denediği her defasında ESET Internet Security uygulamasının

aynı işlemi yapmasını istiyorsanız **Kural oluştur ve her zaman hatırla** onay kutusunu seçin.



Güvenlik duvarı kurulumunda, ESET Internet Security tarafından algılanmadan önce uygulamalar için yeni Güvenlik duvarı kuralları oluşturabilirsiniz. Ana program penceresi > **Ayarlar** > **Ağ Koruması**'nı açın > **Güvenlik Duvarı** > **Yapılandır** > **Gelişmiş** > **Kurallar** > **Düzenle**'nin yanındaki seçeneğini tıklayın.

Ekle düğmesini tıklayın ve **Genel** sekmesinde kural için ad, yön ve iletişim protokolü girin. Bu pencere, kural uygulandığında yapılacak işlemi tanımlamanıza olanak sağlar.

Yerel sekmesinde uygulamanın yürütülebilir dosyasının yolunu ve yerel iletişim bağlantı noktasını girin. Uzak adresi ve bağlantı noktasını (varsa) girmek için **Uzak** sekmesini tıklatın. Uygulama yeniden iletişim kurmayı dener denemez, yeni oluşturulan kural uygulanır.

Bir hesap için Ebeveyn kontrolünün etkinleştirilmesi

Belirli bir kullanıcı hesabı için Ebeveyn kontrolünü etkinleştirmek üzere aşağıdaki adımları uygulayın:

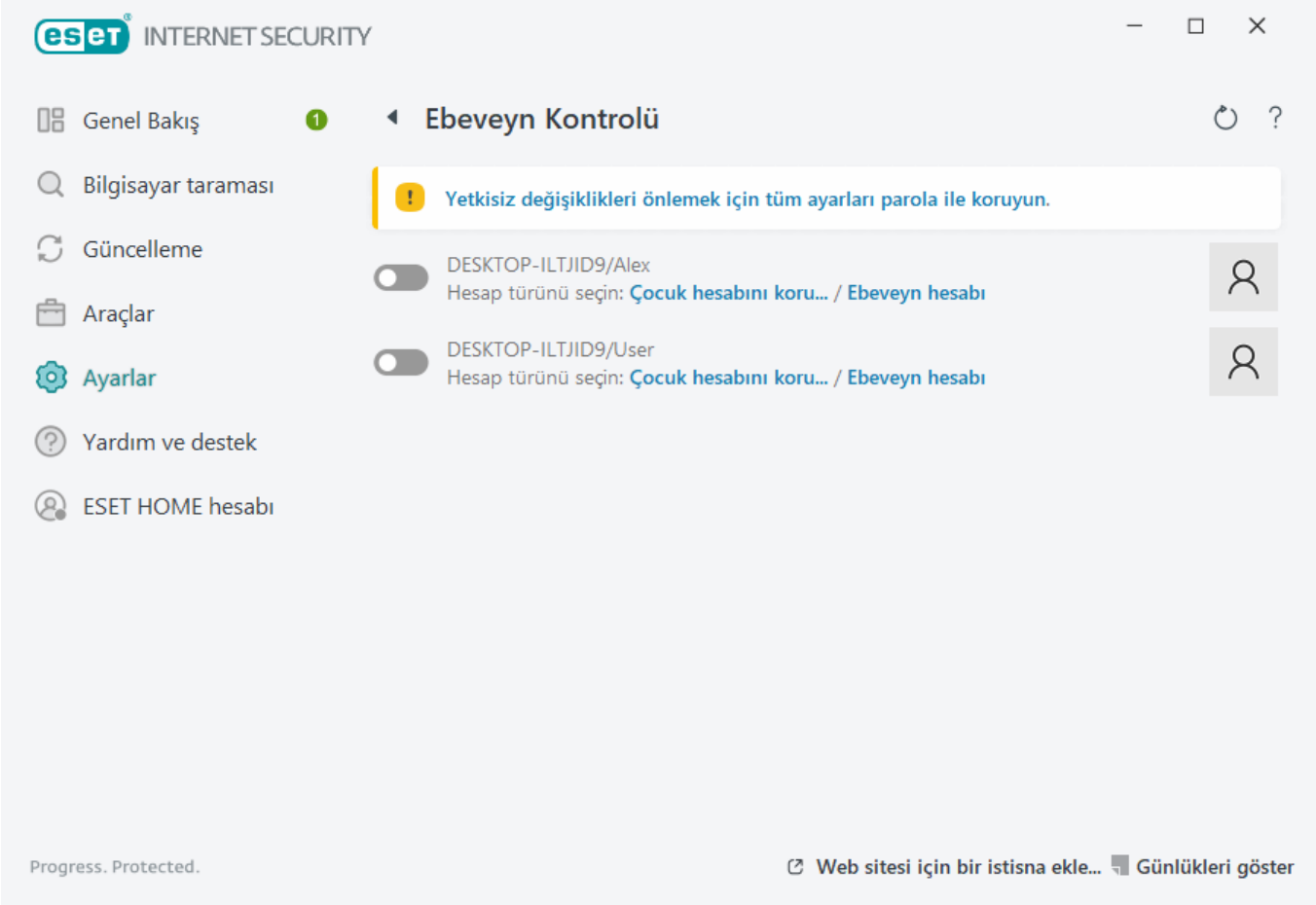
1. Varsayılan olarak, Ebeveyn kontrolleri ESET Internet Security içinde devre dışıdır. Ebeveyn kontrolünün etkinleştirilmesine yönelik iki yöntem bulunur:

   • Ana program penceresinde **Ayarlar** > **İnternet koruması** > **Ebeveyn Kontrolü** bölümünde simgesine tıklatın ve Ebeveyn kontrolü durumunu etkin olarak değiştirin.

   • F5 tuşuna basarak **Gelişmiş Ayarlar** ağacına erişin, **Web ve e-posta** > **Ebeveyn Kontrolü**'ne gidin ve **Ebeveyn Kontrolü'nü etkinleştir** seçeneğinin yanındaki kaydırma çubuğunu etkinleştirin.

2. Ana program penceresinden **Ayarlar** > **İnternet koruması** > **Ebeveyn kontrolü**'nü tıklayın. **Ebeveyn kontrolü** öğesinin yanında **Etkin** durumu görünse bile, ok simgesini tıklayarak istenen hesap için Ebeveyn Kontrolünü yapılandırmanız gerekir. Bunun ardından bir sonraki pencerede **Alt hesabı koru** veya **Üst hesap** seçeneğini

tıklayın. Sonraki penceredeyse, erişim düzeyini ve yaşa uygun önerilen web sayfalarını belirlemek için bir doğum tarihi girin. Ebeveyn kontrolü artık belirtilen kullanıcı hesabı için etkinleşmiştir. Kategoriler sekmesinde izin vermek veya engellemek istediğiniz kategorileri özelleştirmek için hesap adının altındaki **Engellenen içerik ve ayarlar** öğesini tıklayın. Bir kategoriyle eşleşmeyen özel web sayfalarına izin vermek veya bunları engellemek için Özel Durumlar sekmesini tıklayın.



Zamanlayıcıda yeni bir görev oluşturulması

Araçlar > **Diğer araçlar** > **Zamanlayıcı** içinde yeni bir görev oluşturmak için **Ekle** seçeneğini tıklayın veya içerik menüsünden **Ekle** seçeneğini belirleyin. Beş tür zamanlanmış görev kullanılabilir:

- **Harici uygulama çalıştır** – Harici bir uygulamanın yürütülmesini zamanlar.
- **Günlük bakımı** – Günlük dosyaları ayrıca, silinen kayıtlardan kalanları da içerir. Bu görev, etkin çalışma sağlamak için günlük dosyalarındaki kayıtları düzenli olarak en iyi duruma getirir.
- **Sistem başlangıç dosyası denetimi** – Sistem başlangıcında veya oturum açıldığında çalıştırılmasına izin verilen dosyaları denetler.
- **Bilgisayar taraması oluştur** – ESET SysInspector bilgisayar sistem görüntüsünü oluşturur; sistem bileşenleri (örneğin, sürücüler, uygulamalar) hakkında ayrıntılı bilgi toplar ve her bileşenin risk düzeyini değerlendirir.
- **İsteğe bağlı bilgisayar taraması** – Bilgisayarınızdaki dosya ve klasörlerin bilgisayar taramasını gerçekleştirir.
- **Güncelleme** – Modülleri güncelleyerek bir Güncelleme görevi zamanlar.

Güncelleme en sık kullanılan zamanlanan görevlerden biri olduğu için, yeni güncelleme görevinin nasıl ekleneceğini aşağıda açıklayacağız:

Zamanlanan görev açılır menüsünden **Güncelle** öğesini seçin. **Görev adı** alanına görevin adını girin ve **İleri** seçeneğini tıklatın. Görevin sıklığını seçin. Aşağıdaki seçenekler kullanılabilir: **Bir kere**, **Yinelenen**, **Günlük**, **Haftalık** ve **Olay tetiklendiğinde**. Dizüstü bilgisayar pil gücüyle çalışırken sistem kaynaklarının kullanımını en aza indirmek için **Pil gücüyle çalışırken görevi atla** öğesini seçin. Görev, **Görev yürütme** alanlarında belirtilen tarihte ve saatte çalışır. Ardından, görev zamanlanan saatte yapılamadığında veya tamamlanamadığında hangi eylemin gerçekleştirileceğini tanımlayın. Aşağıdaki seçenekler kullanılabilir:

- **Bir sonraki zamanlanan saatte**
- **En kısa sürede**
- **Son çalıştırmadan itibaren geçen süre belirtilen değeri geçiyorsa hemen** (aralık, **Son çalıştırmadan itibaren geçen süre (saat)** kaydırma kutusu kullanılarak tanımlanabilir)

Sonraki adımda geçerli zamanlanan görev hakkında bilgiler içeren özet penceresi görüntülenir. Değişiklik yapmayı sonlandırdığınızda **Son** seçeneğini tıklatın.

Zamanlanan görev için kullanılacak profilleri seçebileceğiniz iletişim penceresi açılır. Buradan birincil ve alternatif profili seçebilirsiniz. Görev birincil profil kullanılarak tamamlanamazsa alternatif profil kullanılır. **Son** seçeneğini tıklatarak onayladığınızda yeni zamanlanan görev, geçerli olan zamanlanan görevler listesine eklenir.

Haftalık bir bilgisayar taraması zamanlama

Düzenli bir görevi zamanlamak için ana program penceresini açın ve **Araçlar** > **Diğer Araçlar** > **Zamanlayıcı**'yı tıklayın. Aşağıda, yerel disklerinizi her hafta taramak üzere bir görevi nasıl zamanlayacağınıza ilişkin kısa bir kılavuz bulabilirsiniz. Daha ayrıntılı açıklamalar için Bilgi Bankası makalemize bakın.

Bir tarama görevini zamanlamak için:

1. Ana Zamanlayıcı ekranında **Ekle**'yi tıklatın.
2. Görev için bir ad girin ve **Görev türü** açılır menüsünden **İsteğe bağlı bilgisayar taraması**'nı seçin.
3. Görev sıklığı için **Haftalık** seçeneğini işaretleyin.
4. Görevin çalıştırılacağı günü ve saati ayarlayın.
5. Zamanlanan görev herhangi bir nedenle başlatılamazsa (örneğin bilgisayarın kapatılması durumunda) görevi daha sonra gerçekleştirmek üzere **Görevi en kısa sürede çalıştır** seçeneğini belirleyin.
6. Zamanlanan görevin özetini inceleyin ve **Son**'u tıklatın.
7. **Hedefler** açılır menüsünden **Yerel sürücüler** seçeneğini belirleyin.
8. Görevi uygulamak için **Son**'u tıklatın.

"Bankacılık ve Ödeme koruması istenen web sayfasına yönlendiremedi" hatası nasıl çözümlenir?

Web sitesi yeniden yönlendirmesi yerine Tüm tarayıcıları güvenli hale getir seçeneğini kullanın

Varsayılan olarak Bankacılık ve Ödeme Sistemleri Koruması güvenli tarayıcısı, bilinen bir bankacılık web sitesini ziyaret ettikten sonra halihazırda kullanılan tarayıcıda başlatılır. Web sitesi yeniden yönlendirmesi yerine, desteklenen tüm tarayıcıları güvenli modda başlatmak için Tüm tarayıcıları güvenli hale getir seçeneğini kullanabilirsiniz. Bu; internette gezinmenize, internet bankacılığına erişmenize ve tek bir güvenli tarayıcı penceresinden yeniden yönlendirme olmadan çevrim içi işlemler yapmanıza olanak tanır.
Tüm tarayıcıları güvenli hale getir seçeneğini kullanmak için ana program penceresini açın, **Ayarlar** > **Güvenlik Araçları**'na gidin ve **Tüm tarayıcıları güvenli hale getir** seçeneğinin yanındaki kaydırma çubuğunu etkinleştirin.

Web sitesi yeniden yönlendirme hatasını çözmek için aşağıdaki talimatları izleyin:

Her bir adımı tamamlamanızın ardından Bankacılık ve Ödeme korumasının çalışıp çalışmadığını kontrol edin

Tarayıcı penceresi hala çalışmıyorsa tekrar çalışana kadar bir sonraki adımı tamamlayın.

1. Bilgisayarınızı yeniden başlatın.

2. Windows İşletim sisteminizin ve ESET Internet Security ürününüzün en son sürümünü kullandığınızdan emin olun: ESET Windows ev ürünlerini en son sürüme yükseltin.

3. Üçüncü taraf güvenlik yazılımınız, VPN veya güvenlik duvarınız ile çakışma olabilir. Tarayıcıda yüklenen dosyalarla çakışmaları gözden geçirmek için Günlük dosyaları > Bankacılık ve Ödeme Sistemleri Koruması'nı açın ve giriş yapan yazılımı geçici olarak devre dışı bırakın veya yüklemesini kaldırın.

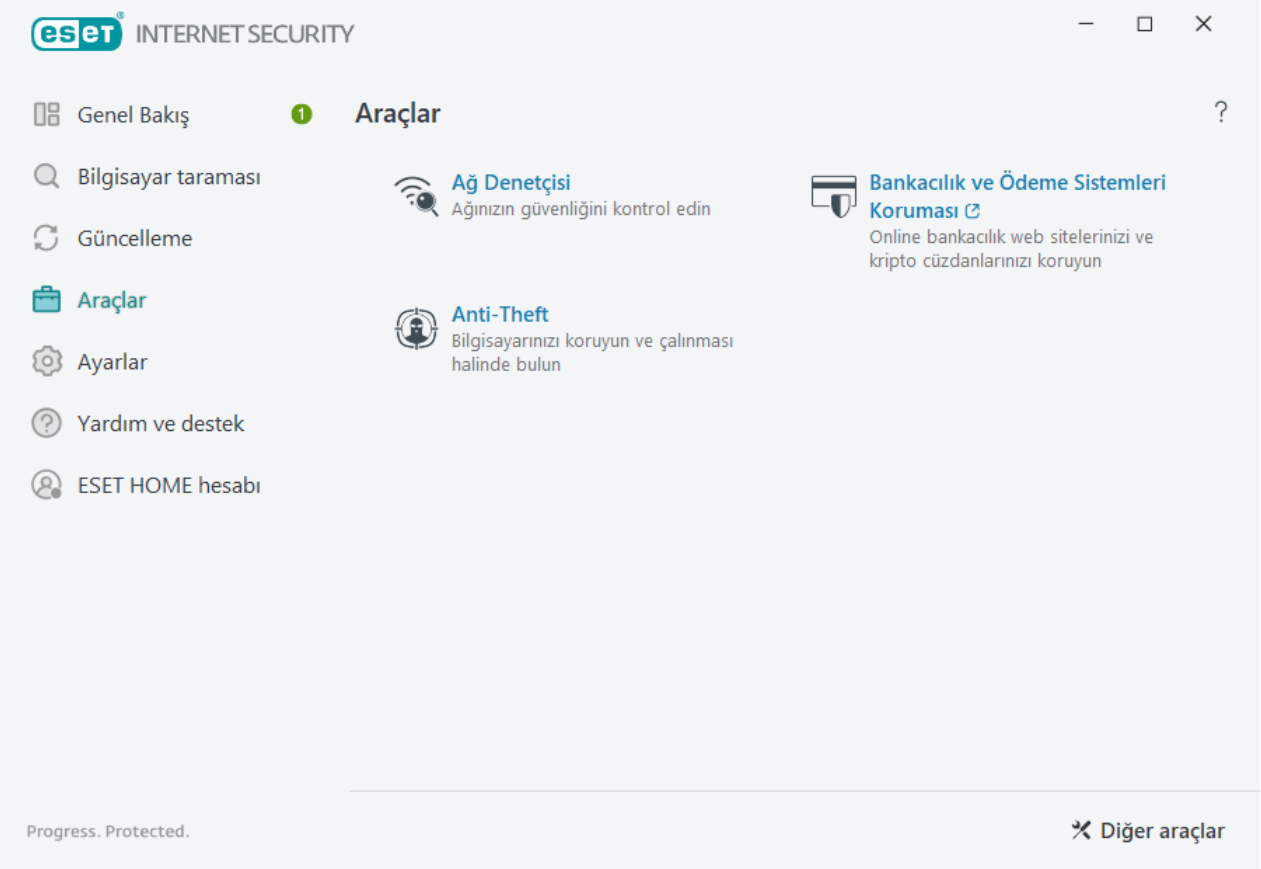
4. Tüm üçüncü taraf tarayıcı uzantılarını devre dışı bırakın.

5. Tarayıcı önbelleğini temizleyin. Tarayıcımda Firefox önbelleği veya Google Chrome önbelleği nasıl temizlenir?

6. Varsayılan tarayıcınızın **Gelişmiş ayarlar** > **Web ve e-posta** > **Protokol filtrelemesi** > **Hariç tutulan uygulamalar** bölümünde hariç tutulmadığından emin olun. Gelişmiş ayarlar'a erişin.

7. Önceki adımlarda ESET ürününüzü yükseltmediyseniz ESET ürününü kaldırıp tekrar yükleyin. Yüklemenin ardından bilgisayarınızı yeniden başlatın.

8. Sorun devam ederse Tüm tarayıcıları güvenli hale getir seçeneğini etkinleştirebilirsiniz veya ana program penceresi > **Araçlar** > **Bankacılık ve Ödeme Sistemleri Koruması**'ndan güvenli tarayıcıya erişebilirsiniz.



Bankacılık ve Ödeme koruması, çevrimiçi işlemleriniz sırasında finansal verilerini korumak için tasarlanan ek bir koruma katmanıdır.

Varsayılan olarak, desteklenen tüm web tarayıcıları güvenli modda başlatılır. Bu, internette gezinmenize, internet bankacılığına erişmenize ve yeniden yönlendirme olmadan tek bir güvenli tarayıcı penceresinde çevrim içi satın alma ve parasal işlemlerini yapmanıza olanak sağlar.

ESET LiveGrid® bilinirlik sistemi, Bankacılık ve Ödeme Sistemleri korumasının düzgün şekilde çalışması için etkinleştirilmelidir (varsayılan olarak etkindir).

Aşağıdaki güvenli tarayıcı davranışı yapılandırma seçeneklerinden birini belirleyin:

- **Tüm tarayıcıların güvenliğini sağla** - Varsayılan olarak, desteklenen tüm web tarayıcıları güvenli modda başlatılır. Bu, internette gezinmenize, internet bankacılığına erişmenize ve yeniden yönlendirme olmadan tek bir güvenli tarayıcı penceresinde çevrim içi satın alma ve parasal işlemlerini yapmanıza olanak sağlar.

- **Web sitelerinin yeniden yönlendirilmesi** - Korunan web siteleri listesinde yer alan web siteleri ve dahili internet bankacılığı listesi güvenli tarayıcıya yönlendirilir. Hangi tarayıcının (standart veya güvenli) açılacağını seçebilirsiniz.

Web sitelerinin yeniden yönlendirilmesi, ARM işlemcilerine sahip cihazlarda kullanılamaz.

- Önceki iki seçenek de devre dışı bırakıldı - Güvenli tarayıcıya erişmek için ESET Internet Security ürününde **Araçlar** > **Bankacılık ve Ödeme Sistemleri Koruması**'nı tıklayın veya **Bankacılık ve Ödeme Sistemleri Koruması** masaüstü simgesini tıklayın. Windows işletim sisteminde varsayılan olarak ayarlanmış tarayıcı

güvenli modda açılır.

Güvenli tarayıcı davranışını yapılandırmak için Bankacılık ve Ödeme Sistemleri Koruması gelişmiş ayarları'na bakın. ESET Internet Security ürününde Tüm tarayıcıları güvenli hale getir özelliğini etkinleştirmek için **Ayarlar** > **Güvenlik araçları**'nı tıklayın ve **Tüm tarayıcıları güvenli hale getir** kaydırma çubuğunu etkinleştirin.

HTTPS şifreli iletişimin kullanımı, korumalı tarama gerçekleştirmek için gereklidir. Aşağıdaki tarayıcılar Bankacılık ve Ödeme Sistemleri Korumasını desteklemektedir:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

Yalnızca Firefox ve Microsoft Edge, ARM işleyicileri olan cihazlarda desteklemektedir.

Bankacılık ve Ödeme koruması özellikleri hakkında daha fazla bilgi için şu ESET Bilgi Bankası makalesini okuyun (makaleler İngilizce ve diğer dillerde mevcuttur):

- ESET Bankacılık ve Ödeme korumasını nasıl kullanırım?
- ESET Bankacılık ve Ödeme Sistemleri korumasını belirli bir web sitesi için etkinleştirme veya devre dışı bırakma
- ESET Windows ev ürünlerinde Bankacılık ve Ödeme Sistemleri Korumasını duraklatma veya devre dışı bırakma
- ESET Bankacılık ve Ödeme Sistemleri Koruması—sık karşılaşılan hatalar
- ESET sözlüğü | Bankacılık ve Ödeme Sistemleri Koruması

Sorununuzu nasıl çözebileceğinizden hala emin değilseniz lütfen ESET Teknik Desteği'ne e-posta gönderin.

Parola korumalı Gelişmiş ayarların kilidi nasıl açılır?

Korumalı Gelişmiş ayarlara erişmek istediğinizde parola girişi için bir pencere görüntülenir. Parolanızı unutur veya kaybederseniz **Parolayı geri yükle** seçeneğini tıklayın ve lisans kaydı için kullandığınız e-posta adresini girin. ESET size doğrulama kodunu içeren bir e-posta gönderir. Doğrulama kodunu girin ve yeni parolayı yazıp onaylayın. Doğrulama kodu yedi gün boyunca geçerlidir.

Parolayı ESET HOME hesabınız üzerinden geri yükleyin - Etkinleştirme için kullanılan lisans ESET HOME hesabınızla ilişkilendirilmişse bu seçeneği kullanın. ESET HOME hesabınıza giriş yapmak için kullandığınız e-posta adresini girin.

E-posta adresinizi hatırlamıyorsanız veya parolayı geri yüklemekle ilgili sorunlarla karşılaşırsanız **Teknik Destek ile iletişime geçin**. Teknik Destek bölümümüzle iletişim kurmak için ESET web sitesine yönlendirilirsiniz.

Teknik Destek için kod oluştur - Bu seçenek, Teknik Destek için bir kod oluşturur. Teknik Destek tarafından sağlanan kodu kopyalayın ve **Doğrulama kodum var**'ı tıklayın. Doğrulama kodunu girdikten sonra yeni parolanızı yazıp onaylayın. Doğrulama kodu yedi gün boyunca geçerlidir.

Daha fazla bilgi için ESET Windows ev ürünlerinde ayar koruma parolanızın kilidini açma bölümüne bakın.

Ürünün ESET HOME üzerinden devre dışı bırakılması nasıl çözümlenir?

Ürün etkinleştirilmedi

Lisans sahibi ESET HOME portalından ESET Internet Security hesabınızı devre dışı bıraktığında veya ESET HOME hesabınızla paylaşılan lisans artık paylaşılmadığında bu hata iletisi görüntülenir. Bu sorunu çözmek için:

- **Etkinleştir**'i tıklayın ve ESET Internet Security ürününü etkinleştirmek için Etkinleştirme yöntemlerinden birini kullanın.
- ESET Internet Security Ürününüzün lisans sahibi tarafından devre dışı bırakıldığı veya lisansın artık sizinle paylaşılmadığı bilgisiyle lisans sahibiyle iletişime geçin. Lisans sahibi bu sorunu ESET HOME çözebilir.

Ürün devre dışı bırakıldı, cihazın bağlantısı kesildi

Bir cihaz ESET HOME hesabı kaldırıldıktan sonra bu hata mesajı görüntülenir. Bu sorunu çözmek için:

- **Etkinleştir**'i tıklayın ve ESET Internet Security ürününü etkinleştirmek için Etkinleştirme yöntemlerinden birini kullanın.
- ESET Internet Security ürününüzün devre dışı bırakıldığı ve cihazın ESET HOME üzerinden bağlantısının kesildiği bilgisiyle beraber lisans sahibiyle iletişime geçin.
- Lisans sahibi sizseniz ve bu değişikliklerden haberiniz yoksa ESET HOME Etkinlik feed'inizi gözden geçirebilirsiniz. Şüpheli bir aktivite bulursanız hesap ESET HOME hesabına ait parolanızı değiştirin ve ESET Teknik Destek ekibiyle iletişime geçin.

Ürün devre dışı bırakıldı, cihazın bağlantısı kesildi

Bir cihaz ESET HOME hesabı kaldırıldıktan sonra bu hata mesajı görüntülenir. Bu sorunu çözmek için:

- **Etkinleştir**'i tıklayın ve ESET Internet Security ürününü etkinleştirmek için Etkinleştirme yöntemlerinden birini kullanın.
- ESET Internet Security ürününüzün devre dışı bırakıldığı ve cihazın ESET HOME üzerinden bağlantısının kesildiği bilgisiyle beraber lisans sahibiyle iletişime geçin.
- Lisans sahibi sizseniz ve bu değişikliklerden haberiniz yoksa ESET HOME Etkinlik feed'inizi gözden geçirebilirsiniz. Şüpheli bir aktivite bulursanız hesap ESET HOME hesabına ait parolanızı değiştirin ve ESET Teknik Destek ekibiyle iletişime geçin.

Ürün etkinleştirilmedi

Lisans sahibi ESET HOME portalından ESET Internet Security hesabınızı devre dışı bıraktığında veya ESET HOME hesabınızla paylaşılan lisans artık paylaşılmadığında bu hata iletisi görüntülenir. Bu sorunu çözmek için:

- **Etkinleştir**'i tıklayın ve ESET Internet Security ürününü etkinleştirmek için Etkinleştirme yöntemlerinden birini kullanın.
- ESET Internet Security Ürününüzün lisans sahibi tarafından devre dışı bırakıldığı veya lisansın artık sizinle paylaşılmadığı bilgisiyle lisans sahibiyle iletişime geçin. Lisans sahibi bu sorunu ESET HOME çözebilir.

Müşteri Deneyimini İyileştirme Programı

Müşteri Deneyimini İyileştirme Programı'na katılarak ESET'e ürünlerimizin kullanımıyla ilgili anonim bilgileri sağlarsınız. Veri işleme ile ilgili daha fazla bilgiyi Gizlilik Politikamızda bulabilirsiniz.

Onayınız

Programa katılım gönüllülük esasına dayalıdır ve rızanıza bağlıdır. Katıldıktan sonra, herhangi bir işlem yapmanız gerekmez, yani bu pasif bir katılımdır. Ürün ayarlarını değiştirerek dilediğiniz zaman onayınızı geri çekebilirsiniz. Bu, anonim verilerinizi daha fazla işlememize engel olacaktır.

Ürün ayarlarını değiştirerek dilediğiniz zaman onayınızı geri çekebilirsiniz:

- ESET Windows ev ürünlerinde Özel Müşteri Deneyimini İyileştirme Programı ayarlarını değiştirme

Ne tür bilgiler toplarız?

Ürünle etkileşim ile ilgili veriler

Bu bilgiler, bize ürünlerimizin nasıl kullanıldığı hakkında daha fazla veri sunar. Bu veriler sayesinde, örneğin hangi işlevlerin sıkça kullanıldığını, kullanıcıların hangi ayarları değiştirdiğini veya ürünü kullanırken ne kadar süre harcadıklarını bilebiliriz.

Aygıtlarla ilgili veriler

Bu bilgileri, ürünlerimizin nerede ve hangi aygıtlarda kullanıldığını anlamak için toplarız. Tipik örnekler arasında aygıt modeli, ülke, işletim sisteminin sürümü ve adı yer alır.

Hata tanılama verileri

Ayrıca hatalarla ve kilitlenme durumlarıyla ilgili bilgiler de toplanır. Örneğin, oluşan hatalar ve bu hataya neden olan işlemler.

Bu bilgileri neden topluyoruz?

Bu anonim bilgiler, ürünlerimizi siz kullanıcılarımız için iyileştirmemize olanak tanır. Ürünleri mümkün olduğunda alakalı, kullanımı kolay ve hatasız bir hale getirmemize yardımcı olurlar.

Bu bilgileri kim kontrol ediyor?

ESET, spol. s r.o. bu Program kapsamında toplanan verilerin yegane denetleyicisidir. Bu bilgiler üçüncü taraflarla paylaşılmaz.

Son Kullanıcı Lisans Sözleşmesi

19 Ekim 2021 itibarıyla geçerlidir.

ÖNEMLİ: İndirme, yükleme, kopyalama veya kullanmadan önce, lütfen bu ürüne ilişkin aşağıdaki hükümleri dikkatlice okuyun. **YAZILIMI İNDİREREK, YÜKLEYEREK, KOPYALAYARAK VEYA KULLANARAK, BU HÜKÜM VE KOŞULLARI ONAYLADIĞINIZI VE GİZLİLİK POLİTİKASINI KABUL ETTİĞİNİZİ İFADE ETMİŞ OLURSUNUZ.**

Son Kullanıcı Lisans Sözleşmesi

Einsteinova 24, 85101 Bratislava, Slovak Republic Cumhuriyeti adresinde mukim ve Bratislava I. Bölge Mahkemesinin Ticari Sicil Kaydında Bölüm Sro, Giriş No 3586/B, İşyeri Sicil Numarası: 31333532 olarak kayıtlı ESET, spol. s r. o. olarak kayıtlı ESET, spol. s r. o. (“ESET” veya “Sağlayıcı” olarak anılacaktır) tarafından ve fiziksel veya tüzel bir kişi olan siz (“Siz” ya da “Son Kullanıcı” olarak anılacaktır) arasında yapılan bu Yazılım Son Kullanıcı Lisans Sözleşmesi (“Sözleşme” olarak anılacaktır) koşullarına göre, size bu Sözleşmenin 1. Bu Sözleşmenin 1. Maddesinde tanımlanan Yazılım bir veri taşıyıcısında saklanabilir, elektronik posta üzerinden gönderilebilir, İnternet üzerinden yüklenebilir, Sağlayıcının sunucularından yüklenebilir ya da aşağıda ifade edilen hüküm ve koşullara bağlı olarak diğer kaynaklardan elde edilebilir.

BU BİR SATIN ALMA SÖZLEŞMESİ DEĞİL, SON KULLANICI HAKLARI İLE İLGİLİ BİR SÖZLEŞMEDİR. Sağlayıcı ticari ambalajda bulunan Yazılım kopyası ile fiziksel ortamın ve Son Kullanıcının bu Sözleşme uyarınca oluşturmaya hak kazandığı diğer tüm kopyaların sahibi olarak kalır.

Yazılımı yüklerken, indirirken, kopyalarken veya kullanırken "Kabul Ediyorum" veya "Kabul Ediyorum…" düğmesini tıklayarak bu Sözleşmenin şartlarını ve koşullarını kabul etmiş, Gizlilik Politikası'nı onaylamış olursunuz. Bu Sözleşmedeki ve/veya Gizlilik Politikasındaki tüm şartları ve koşulları kabul etmiyorsanız, hemen iptal seçeneğini tıklayın; yükleme ya da indirme işlemini iptal edin veya Yazılım, yükleme ortamı, birlikte sağlanan belgeler ve satın alma makbuzunu yok edin ya da Sağlayıcıya veya Yazılımı edindiğiniz satış yerine iade edin.

YAZILIMI KULLANMANIZIN, BU SÖZLEŞMEYİ OKUDUĞUNUZ, ANLADIĞINIZ VE HÜKÜMLERİNE VE KOŞULLARINA TABİ OLMAYI KABUL ETTİĞİNİZ ANLAMINA GELDİĞİNİ KABUL ETMİŞ SAYILIRSINIZ.

1. **Yazılım.** Bu Sözleşmede kullanıldığı şekliyle "Yazılım" şu anlama gelmektedir: (i) bu Sözleşme ile birlikte sağlanan bilgisayar programı ve ilgili tüm bileşenleri; (ii) disklerin, CD-ROM'ların, DVD'lerin, e-postaların ve tüm eklerin veya veri taşıyıcısında, elektronik postayla veya İnternet üzerinden indirilmek üzere sağlanan Yazılımın nesne kodu biçimi de dahil olmak üzere, beraberinde bu Sözleşmenin sağlandığı diğer medyaların içerikleri; (iii) ilgili tüm açıklayıcı yazılı malzeme ve Yazılımla ilgili olası tüm Dokümantasyon ve Yazılımla ilgili tüm açıklamalar, Yazılımın teknik özellikleri, Yazılım özellikleri veya çalışması ile ilgili açıklamalar, Yazılımın kullanıldığı işletim ortamıyla ilgili tüm açıklamalar, Yazılımın kullanımı veya yüklenmesi ile ilgili tüm talimatlar veya Yazılımın nasıl kullanılacağına ilişkin tüm açıklamalar ("Dokümantasyon"); (iv) Yazılımın kopyaları, Yazılımda olabilecek hatalar için yamalar, Yazılıma ekler, Yazılımın uzantıları, varsa Yazılımın değiştirilen sürümleri ve Yazılım bileşenlerinin güncellemeleri. Maddesi uyarınca size Lisans hakkını tanıdığı Yazılım bileşenleri güncellemelerini içerir. Yazılım yalnızca yürütülebilir nesne kodu biçiminde sağlanır.

2. **Yükleme, Bilgisayar ve Lisans anahtarı**. Veri taşıyıcısında sağlanan, elektronik posta ile gönderilen, internetten indirilen, Sağlayıcının sunucularından indirilen veya başka kaynaklardan elde edilen Yazılım yükleme işlemi

gerektirir. Yazılımı en azından Belgeler'de belirtilen gereksinimleri karşılayan doğru şekilde yapılandırılmış bir Bilgisayara yüklemeniz gerekir. Yükleme yöntemi Belgeler'de açıklanmaktadır. Yazılım üzerinde ters bir etki yapabilecek hiçbir bilgisayar programı veya donanım, Yazılımı yüklediğiniz bilgisayara yüklenemez. Bilgisayar; kişisel bilgisayarlar, dizüstü bilgisayarlar, iş istasyonları, avuç içi bilgisayarlar, akıllı telefonlar, elektronik el cihazları veya Yazılımın tasarlanmış olduğu ve yükleneceği, kurulacağı ve/veya kullanılacağı diğer elektronik cihazlar dahil ancak bunlarla sınırlı olmamak üzere donanım anlamına gelmektedir. Lisans anahtarı Yazılımın yasal kullanımına, spesifik sürümüne veya Lisans süresinin uzatılmasına bu Sözleşmeye uygun şekilde izin vermek için Son Kullanıcıya sağlanan benzersiz dizi veya sembol, harf, sayı ya da özel işaretler anlamına gelir.

3. **Lisans**. Bu Sözleşmenin hükümlerini kabul etmeniz ve burada belirtilen tüm hükümlere ve koşullara uymanız durumunda, Sağlayıcı size aşağıdaki hakları ("Lisans") sağlar:

a) **Yükleme ve kullanım.** Yazılımı bir bilgisayarın sabit sürücüsüne veya veri depolama için benzer bir kalıcı ortama yüklemek, Yazılımı bir bilgisayar sisteminin belleğine yüklemek ve depolamak ve Yazılımı uygulamak, depolamak ve görüntülemek için münhasır olmayan ve devredilemeyen bir hakka sahip olursunuz.

b) **Lisans sayısı koşulu.** Yazılımı kullanma hakkı, Son Kullanıcı sayısına bağlıdır. Bir Son Kullanıcı şunları ifade eder: (i) bir bilgisayar sistemindeki Yazılım kurulumu veya (ii) bir lisansın kapsamı posta kutusu sayısıyla sınırlıysa, tek Son Kullanıcı bir Posta Kullanıcı Aracısı (“PKA”) üzerinden elektronik posta alan bir bilgisayar kullanıcısını ifade eder. PKA elektronik postayı kabul eder ve ardından otomatik olarak birçok kullanıcıya gönderirse, Son Kullanıcı sayısı elektronik postanın dağıtıldığı gerçek kullanıcı sayısına göre belirlenir. Bir posta sunucusu bir posta geçidinin işlevini gerçekleştiriyorsa, Son Kullanıcı sayısı söz konusu geçidin hizmet verdiği posta sunucusu kullanıcılarının sayısına eşit olur. Belirli olmayan bir sayıda elektronik posta adresi tek bir kullanıcıya yönlendirilir ve tek bir kullanıcı tarafından kabul edilirse (ör. öteki adlar yoluyla) ve postalar istemci tarafından daha fazla sayıda kullanıcıya otomatik olarak dağıtılmıyorsa, Lisans tek bir bilgisayar için gereklidir. Bir Lisansı aynı anda birden fazla bilgisayarda kullanmamalısınız. Son Kullanıcı, Sağlayıcı tarafından verilen Lisansların sayısından doğan sınırlamaya uygun olarak Son Kullanıcının Yazılımı kullanma hakkına sahip olduğu ölçüye kadar Yazılıma Lisans Anahtarı girmekle yükümlüdür. Lisansı üçüncü taraflarla paylaşamaz veya bu Sözleşme ya da Sağlayıcı tarafından izin verilmediği sürece Lisans anahtarını kullanması için üçüncü taraflara izin veremezsiniz. Lisans anahtarınız tehlikeye girerse Sağlayıcıyı hemen bilgilendirin.

c) **Ev Sürümü/Kurumsal Sürüm.** Yazılımın Ev Sürümü yalnızca ev ve aile kullanımı için özel ortamda ve/veya ticari amaçlı olmayan ortamda münhasıran kullanılır. Yazılımın Kurumsal Sürümü ticari bir ortamın yanı sıra posta sunucularında, posta geçişlerinde, posta ağ geçitlerinde veya İnternet ağ geçitlerinde kullanılması için edinilmelidir.

d) **Lisans Hükmü.** Yazılımı kullanma hakkınız zamanla sınırlıdır.

e) **OEM Yazılımı.** "OEM" olarak sınıflandırılan Yazılım, yalnızca onu kullanmak için edindiğiniz bilgisayarla sınırlıdır. Başka bir bilgisayara aktarılamaz.

f) **SO, DENEME Yazılımı.** "Satılık Olmayan", SO veya DENEME olarak sınıflandırılan Yazılım ücretle satılamaz ve sadece Yazılımın özelliklerinin tanıtılması veya test edilmesi için kullanılmalıdır.

g) **Lisansın Sonlandırılması.** Lisans, kullanımı için verilen sürenin sonunda otomatik olarak sonlandırılır. Bu Sözleşmedeki hükümlerden herhangi birine uymamanız durumunda Sağlayıcı, bu gibi bir koşulda Sağlayıcı için geçerli olan herhangi bir yetkiye veya yasal çözüme halel gelmeksizin Sözleşmeden çekilme hakkına sahiptir. Lisansın iptal edilmesi durumunda, Yazılımı ve yedeklenmiş tüm kopyalarını derhal silmeniz, imha etmeniz ya da ESET’e veya Yazılımı edindiğiniz satış noktasına masrafları size ait olmak üzere iade etmeniz gerekir. Lisansın sonlandırılması durumunda, Sağlayıcı, Son Kullanıcının Yazılım işlevlerini kullanma yetkisini iptal etme hakkına sahiptir ve bu iptal işlemi, Sağlayıcının sunucularına veya üçüncü taraf sunucularına bağlantı gerektirir.

4. **Veri toplama işlevleri ve internet bağlantısı gereksinimleri.** Yazılımı düzgün şekilde kullanmak, İnternet bağlantısı gerektirir ve düzenli aralıklarla Sağlayıcının sunucularına veya üçüncü taraf sunucularına ve Gizlilik Politikasına uygun olarak geçerli veri toplama işleminin yapılması gerekir. İnternete bağlanmak ve geçerli veri toplama Yazılımın şu işlevleri için gereklidir:

a) **Yazılım Güncellemeleri.** Sağlayıcı Yazılım için zaman zaman güncellemeler ve yükseltmeler yayımlama hakkına sahiptir ("Güncellemeler") ancak Güncellemeler sağlamakla yükümlü değildir. Bu işlev Yazılımın standart ayarlarında etkinleştirilmiştir ve bu nedenle Son Kullanıcı Güncellemelerin otomatik olarak yüklenmesini devre dışı bırakmadığı sürece, Güncellemeler otomatik olarak yüklenirler. Güncellemelerin sağlanması amacına yönelik olarak, Bilgisayar ve/veya Yazılımın yüklendiği platformla ilgili bilgiler dahil olmak üzere, Gizlilik Politikasına uygun olarak bir Lisans kimlik doğrulama işlemi gereklidir.

Herhangi bir Güncellemenin sağlanması, Kullanım Ömrü Sonu Politikasına ("EOL Politikası") tabi olabilir ve bu politika https://go.eset.com/eol_home adresinde bulunabilir. Yazılım veya özelliklerinden herhangi biri Kullanım Ömrü Sonu Politikasında tanımlanan Kullanım Ömrü tarihine ulaştığında herhangi bir Güncelleme sağlanmaz.

b) **İzinsiz girişlerin ve bilgilerin Sağlayıcıya iletilmesi**. Yazılım; bilgisayar virüslerinin ve diğer kötü amaçlı bilgisayar programlarının ve dosyalar, URL'ler, IP paketleri ve ethernet çerçeveleri gibi şüpheli, sorunlu, istenmeyen türden olabilecek veya tehlikeli olabilecek nesnelerin ("Sızıntılar") örneklerini toplayan işlevler içerir; bu işlevler söz konusu sızıntıları yükleme süreci, Bilgisayar ve/veya Yazılımın yüklendiği platform hakkındaki bilgiler ile Yazılımın işlemleri ve işlevleri hakkındaki bilgiler de dahil, ancak bunlarla sınırlı olmamak üzere (sonra "Bilgiler") Sağlayıcıya gönderilir. Bilgiler ve Sızıntılar Son Kullanıcı veya Yazılımın yüklü olduğu bilgisayarın diğer kullanıcıları hakkında veriler (tesadüfen veya yanlışlıkla elde edilen kişisel bilgiler de dahil) ve ilişkili meta verilere sahip Sızıntılardan etkilenen dosyaları içerebilir.

Bilgiler ve Sızıntılar Yazılımın şu işlevleri tarafından toplanabilir:

i. LiveGrid Saygınlık Sistemi işlevi Sızıntılarla ilişkili tek yönlü karmaların toplanmasını ve Sağlayıcıya gönderilmesini içerir. Bu işlev, Yazılımın standart ayarları altında etkinleştirilmiştir.

ii. LiveGrid Geri Bildirim Sistemi işlevi, Sızıntıların toplanmasını ve ilişkilendirilen meta veriler ve Bilgiler ile birlikte Sağlayıcıya gönderilmesini içerir. Bu işlev, Yazılımı yükleme esnasında Son Kullanıcı tarafından etkinleştirilebilir.

Sağlayıcı alınan Bilgileri ve Sızıntıları yalnızca Sızıntıların analizi ve araştırılması, Yazılımın ve Lisans kimlik doğrulamasının iyileştirilmesi amaçlarına yönelik olarak kullanacaktır ve alınan Sızıntıların ve Bilgilerin güvende kalmasını sağlamak için uygun olan önlemleri alacaktır. Yazılımın bu işlevini etkinleştirdiğinizde, Sızıntılar ve Bilgiler Sağlayıcı tarafından, Gizlilik Politikasında belirtildiği şekilde ve ilgili yasal düzenlemelere uygun olarak toplanabilir ve işlenebilir. Bu işlevleri dilediğiniz zaman devre dışı bırakabilirsiniz.

Bu Sözleşmenin amacına uygun olarak, Sağlayıcının Sizi Gizlilik Politikasına uygun olarak tanımlamasına olanak tanıyan verileri toplamak, işlemek ve depolamak gerekir. Sağlayıcının kendi araçlarını kullanarak Yazılımın Sizin tarafınızdan bu Sözleşmenin şartlarına uygun şekilde kullanılıp kullanılmadığını kontrol edeceğini burada kabul edersiniz. Bu Sözleşmenin amacına uygun olarak verilerinizin Yazılım ve Sağlayıcının bilgisayar sistemleri arasındaki iletişim esnasında aktarılması gerektiğini ve Yazılımın işlevinin sağlanması için ağa destek ve Yazılımı kullanmak ve Sağlayıcının haklarının korunması için yetki vermek gerektiğini kabul edersiniz.

Bu Sözleşmenin neticelendirilmesinin ardından, Sağlayıcı veya Sağlayıcının dağıtım ve destek ağının parçası olarak herhangi bir iş ortağı, faturalandırma amaçlı olarak veya bu Sözleşmenin uygulanması amacıyla Sizi tanımlamak için gerekli olan verileri aktarma, işleme ve depolama hakkına sahip olur.

Gizlilik, kişisel veri koruması ve veri öznesi olarak Sizin Haklarınız hakkındaki detaylar, Sağlayıcının web sitesinde yer alan ve yükleme işleminden doğrudan erişilebilen Gizlilik Politikasında bulunabilir. Ayrıca Yazılımın yardım bölümünden de ziyaret edebilirsiniz.

5. **Son Kullanıcı haklarının kullanılması**. Son Kullanıcı haklarını bizzat veya çalışanlarınız yoluyla kullanmalısınız. Yazılımı yalnızca işlemlerinizi güvence altına almak ve Lisansı aldığınız Bilgisayarlar veya bilgisayar sistemlerine koruma sağlamak için kullanma hakkına sahipsiniz.

6. **Hakların kısıtlanması.** Yazılımı kopyalayamaz, dağıtamaz, bileşenlerine ayıramaz veya türetilmiş sürümlerini oluşturamazsınız. Yazılımı kullanırken aşağıdaki kısıtlamalara uymanız gerekmektedir:

a) Arşivlenen yedek kopyanızın başka bir bilgisayara yüklenmemesi veya başka bir bilgisayarda kullanılmaması kaydıyla, arşiv amaçlı olarak kalıcı bir saklama ortamına Yazılımın bir kopyasını kaydedebilirsiniz. Oluşturacağınız diğer her türlü kopya, bu Sözleşmeyi ihlal eder.

b) Bu Sözleşmede ifade edilen yolların dışında, Yazılımı kullanamaz, değiştiremez, çeviremez, çoğaltamaz ya da Yazılımın veya Yazılımın kopyalarını kullanım haklarını aktaramazsınız.

c) Yazılımı satamaz, alt lisansını veremez, kiralayamaz, ödünç veremez veya ödünç alamaz ya da ticari hizmet sağlamak için kullanamazsınız.

d) Bu kısıtlamanın yasalarla açık bir şekilde yasaklandığı durumlar haricinde, Yazılımda ters mühendislik uygulayamaz, geri derleme yapamaz, Yazılımın derlemesini açamaz ya da başka bir şekilde kaynak kodunu bulmaya çalışamazsınız.

e) Yazılımı, yalnızca Yazılımı kullandığınız yerde geçerli olan yargı alanının, telif hakkı ve diğer fikri mülkiyet haklarıyla ilgili geçerli kısıtlamalar dahil ancak bunlarla sınırlı olmamak kaydıyla, tüm geçerli yasalarıyla uyumlu bir yolla kullanacağınızı kabul etmiş olursunuz.

f) Yazılımı ve işlevlerini, yalnızca diğer Son Kullanıcıların bu hizmetlere erişim olanaklarını sınırlamayacak şekilde kullanacağınızı kabul edersiniz. Sağlayıcı, hizmetlerin mümkün olan en çok sayıda Son Kullanıcı tarafından kullanılmasını sağlamak üzere, Son Kullanıcılara ayrı ayrı sağlanan hizmetlerin kapsamını sınırlama hakkını saklı tutar. Hizmetlerin kapsamının sınırlanması aynı zamanda, Yazılım işlevlerinden herhangi birinin kullanılma olasılığının tamamen sonlandırılması ve Sağlayıcının sunucularındaki ya da üçüncü şahıs sunucularındaki Yazılımın belirli bir işleviyle ilgili Verilerin ve bilgilerin silinmesi anlamına da gelir.

g) Lisans anahtarının kullanımını içeren, bu Sözleşmenin şartlarına aykırı olan veya Yazılımı kullanma yetkisi olmayan herhangi bir kişiye Lisans anahtarı sağlamaya yol açan, kullanılan ya da kullanılmayan Lisans anahtarını herhangi bir biçimde aktarma, yetkisiz yeniden üretme ya da çoğaltılan veya oluşturulan Lisans anahtarlarını dağıtma ya da Yazılımı Sağlayıcı dışında bir kaynaktan elde edilen Lisans anahtarının kullanımının sonucu olarak kullanma gibi hiçbir faaliyette bulunmayacağınızı kabul edersiniz.

7. **Telif Hakkı**. Yazılım ve mülkiyet hakları ve fikri mülkiyet hakları dahil ancak bunlarla sınırlı kalmamak kaydıyla Yazılımın tüm hakları ESET ve/veya onun adına lisans veren taraflara aittir. ESET ve/veya lisans veren taraflar uluslararası anlaşma hükümleri ve Yazılımın kullanıldığı ülkedeki ilgili tüm diğer ulusal yasalar tarafından korunur. Yazılımın yapısı, düzeni ve kodu ESET'e ve/veya onun adına lisans veren taraflara ait değerli ticari sırlarıdır ve gizli bilgilerdir. 6(a) Maddesi altında belirtilen durumlar dışında Yazılımı kopyalayamazsınız. Bu Sözleşme kapsamında oluşturma hakkınızın olduğu tüm kopyaların Yazılımda bulunan telif hakkı ve diğer mülkiyet hakkı bildirimlerini içermesi gerekir. Bu Sözleşmenin hükümlerini ihlal edecek şekilde Yazılıma ters mühendislik uygulamanız, geri derleme yapmanız, Yazılımın derlemesini açmanız ya da başka bir şekilde kaynak kodunu bulmaya çalışmanız halinde, bu şekilde elde edilen her türlü bilginin ortaya çıktığı andan itibaren, Sağlayıcının bu Sözleşmenin ihlaline dair haklarından bağımsız olarak, otomatik olarak ve geri alınamaz şekilde tamamen Sağlayıcıya devredilmiş ve Sağlayıcıya ait sayılacağını kabul etmiş olursunuz.

8. **Hakların saklı tutulması**. Sağlayıcı, bu Sözleşme hükümleri kapsamında Yazılımın Son Kullanıcısı olarak Size açıkça verilen hakların dışında, Yazılıma dair tüm haklarını saklı tutar.

9. **Çoklu dil sürümleri, çift ortamlı yazılım, çoklu kopyalar**. Yazılımın birden fazla platformu veya dili desteklemesi durumunda veya Yazılımın birden fazla kopyasını edinmişseniz, Yazılımı yalnızca Lisansını aldığınız sayıda bilgisayar sistemi ve sürümü için kullanabilirsiniz. Kullanmadığınız Yazılım sürümlerini veya kopyalarını satamaz, kiralayamaz, finansal kiralama yoluyla veremez, alt lisansını veremez, ödünç veremez ya da aktaramazsınız.

10. **Sözleşmenin başlangıcı ve sonlandırılması.** Bu Sözleşme, Sözleşmenin hükümlerini kabul ettiğiniz andan itibaren geçerli olur. Yazılımı, tüm yedeklenmiş kopyalarını ve Sağlayıcı veya iş ortakları tarafından sağlanan tüm ilgili malzemeleri kalıcı olarak silerek, yok ederek ve masrafları size ait olmak üzere geri yollayarak, istediğiniz zaman bu Sözleşmeyi sonlandırabilirsiniz. Yazılımı ve özelliklerinden herhangi birini kullanma hakkınız (Kullanım Ömrü Sonu) EOL Politikası'na tabi olabilir. Yazılım veya özelliklerinden herhangi biri Kullanım Ömrü Sonu Politikasında tanımlanan Kullanım Ömrü tarihine ulaşıldığında Yazılımı kullanma hakkınız sonlandırılır. Bu Sözleşme ne biçimde sonlandırılmış olursa olsun, 7, 8, 11, 13, 19 ve 21. maddelerin hükümleri süre sınırı olmaksızın geçerli kalır.

11. **SON KULLANICI BEYANLARI**. SON KULLANICI OLARAK, YAZILIMIN HİÇBİR AÇIK VEYA ZIMNİ BİR GARANTİ OLMAKSIZIN VE İLGİLİ YASALARIN İZİN VERDİĞİ AZAMİ ÖLÇÜDE, "OLDUĞU GİBİ" SAĞLANDIĞINI KABUL ETMİŞ OLURSUNUZ. SAĞLAYICI, ONUN ADINA LİSANS VEREN TARAFLAR VEYA BAĞLI ŞİRKETLERİ YA DA TELİF HAKKI SAHİPLERİ, PAZARLANABİLİRLİK GARANTİSİ VEYA BELLİ BİR AMACA UYGUNLUK GARANTİSİ YA DA YAZILIMIN ÜÇÜNCÜ TARAF PATENTLERİNİ, TELİF HAKLARINI, TİCARİ MARKALARINI VEYA DİĞER HAKLARINI İHLAL ETMEMESİ DAHİL ANCAK BUNLARLA SINIRLI OLMAMAK KAYDIYLA HİÇBİR AÇIK VEYA ZIMNİ BEYANDA BULUNMAZ VEYA GARANTİ VERMEZ. SAĞLAYICI VEYA DİĞER BİR TARAF, YAZILIMIN İŞLEVLERİNİN İHTİYAÇLARINIZI KARŞILAYACAĞI VEYA YAZILIMIN KESİNTİSİZ ÇALIŞACAĞI YA DA HATASIZ OLACAĞI GARANTİSİNİ VERMEZ. HEDEFLEDİĞİNİZ SONUÇLARA ERİŞMEK İÇİN YAZILIMIN SEÇİLMESİ VE YAZILIMIN YÜKLENMESİ, KULLANILMASI VE BUNUN SONUCUNDA ELDE EDİLEN SONUÇLARA DAİR HER TÜRLÜ SORUMLULUĞUN VE RİSKİN TARAFINIZA AİT OLDUĞUNU KABUL ETMİŞ OLURSUNUZ.

12. **Başka yükümlülük kabul edilmez**. Bu Sözleşme, burada özel olarak belirtilenlerin dışında Sağlayıcı ve onun adına lisans veren taraflar için hiçbir yükümlülük teşkil etmez.

13. **YÜKÜMLÜLÜKLERİN SINIRLANDIRILMASI**. GEÇERLİ YASALARIN İZİN VERDİĞİ AZAMİ ÖLÇÜDE SAĞLAYICI, SAĞLAYICININ ÇALIŞANLARI VEYA ADINA LİSANS VEREN TARAFLAR HİÇBİR DURUMDA SÖZLEŞMEDEN, HAKSIZ FİİLDEN, İHMALDEN VEYA YÜKÜMLÜLÜK DOĞURAN BAŞKA BİR NEDENDEN ÖTÜRÜ OLUŞAN VEYA BUNLARDAN KAYNAKLANAN, YAZILIMIN YÜKLENMESİNDEN, KULLANILMASINDAN VEYA KULLANILAMAMASINDAN KAYNAKLANAN HER TÜRLÜ KÂR, GELİR, SATIŞ VEYA VERİ KAYBINDAN YA DA YEDEK PARÇA VEYA SERVİS ALINMASI MASRAFLARINDAN, MALA GELEN HASARLARDAN, KİŞİSEL YARALANMADAN, İŞTE MEYDANA GELEN KESİNTİDEN, TİCARİ BİLGİLERİN KAYBINDAN YA DA ÖZEL, DOĞRUDAN, DOLAYLI, ARIZİ, EKONOMİK, TELAFİ GEREĞİ, CEZAİ, ÖZEL VEYA DOLAYLI HASARLARDAN ÖTÜRÜ, SAĞLAYICININ VEYA ADINA LİSANS VEREN TARAFLARIN YA DA BAĞLI ŞİRKETLERİN BU GİBİ ZARARLARIN MÜMKÜN OLDUĞUNA DAİR HABERDAR EDİLMELERİ DURUMUNDA BİLE, SORUMLU TUTULAMAZLAR. BAZI ÜLKELERDE VE YARGI ALANLARINDA YÜKÜMLÜLÜKLERİN REDDİNE DEĞİL ANCAK SINIRLANDIRILMASINA İZİN VERİLDİĞİNDEN, SAĞLAYICI, SAĞLAYICININ ÇALIŞANLARI VEYA ADINA LİSANS VEREN TARAFLAR VEYA BAĞLI ŞİRKETLERİN YÜKÜMLÜLÜĞÜ LİSANS İÇİN ÖDEDİĞİNİZ ÜCRETLE SINIRLANDIRILMIŞTIR.

14. Bu Sözleşmede bulunan hiçbir hüküm, aksine yorumlanabilmesine bakılmaksızın, müşteri olarak kabul edilen bir tarafın yasal haklarını ihlal etmez.

15. **Teknik destek**. ESET veya ESET tarafından yetkilendirilen üçüncü taraflar, teknik desteği herhangi bir garanti veya beyanat olmaksızın, kendi takdirlerine göre sağlarlar. Yazılım veya özelliklerinden herhangi biri Kullanım Ömrü Sonu Politikasında tanımlanan Kullanım Ömrü Sonu tarihine ulaştığında herhangi bir teknik destek sağlanmaz. Son Kullanıcının, teknik desteğin tedarik edilmesinden önce tüm mevcut verileri, yazılım ve program tesislerini yedeklemesi gerekir. ESET ve/veya ESET tarafından yetkilendirilen üçüncü taraflar, teknik destek tedariki nedeniyle veri, mal, yazılım veya donanım hasarı veya kaybı ya da gelir kaybından ötürü yükümlülük kabul etmezler. ESET ve/veya ESET tarafından yetkilendirilen üçüncü taraflar, sorunun çözülmesinin teknik desteğin

kapsamının dışında olduğuna hükmetme hakkını saklı tutarlar. ESET kendi takdirine bağlı olarak teknik destek tedarikini reddetme, askıya alma veya sonlandırma hakkını saklı tutar. Lisans bilgileri, Bilgiler ve Gizlilik Politikasına uygun diğer veriler, teknik destek sağlama amacına yönelik olarak gerekebilir.

16. **Lisansın Aktarılması**. Sözleşmedeki hükümlerle çelişmediği sürece, Yazılım bir bilgisayar sisteminden başka bir bilgisayar sistemine aktarılabilir. Bu Sözleşmenin hükümlerine aykırı olmadığı sürece, Son Kullanıcı yalnızca Sağlayıcının onayı olması durumunda, (i) orijinal Son Kullanıcının Yazılımın hiçbir kopyasını elde tutmaması; (ii) hakların aktarılmasının doğrudan yapılması, yani orijinal Son Kullanıcıdan yeni Son Kullanıcıya aktarılması; (iii) yeni Son Kullanıcının bu Sözleşme hükümlerine göre sorumlu olduğu tüm hakları ve yükümlülükleri kabul etmesi; (iv) orijinal Son Kullanıcının 17. Maddede belirtilen şekilde Yazılımın gerçek olduğunu kanıtlamasını sağlayacak belgeleri yeni Son Kullanıcıya sağlaması koşullarına bağlı olarak, Lisansı ve bu Sözleşmeden doğan tüm hakları kalıcı olarak başka bir Son Kullanıcıya aktarma hakkına sahip olur.

17. **Yazılımın orijinal olduğunun doğrulanması.** Son Kullanıcı şu yöntemlerden biriyle Yazılımı kullanma hakkına sahip olduğunu gösterebilir: (i) Sağlayıcı veya Sağlayıcı tarafından görevlendirilmiş bir üçüncü tarafın verdiği lisans sertifikası; (ii) daha önce düzenlenmişse, yazılı bir lisans sözleşmesi; (iii) lisans ayrıntılarını (kullanıcı adı ve parola) içeren, Sağlayıcı tarafından gönderilen bir e-postanın sunulması. Gizlilik Politikasına uygun olarak lisans bilgileri ve Son Kullanıcı tanımlama verileri Yazılımın orijinalliğinin doğrulanması amacına yönelik olarak gerekebilir.

18. **Kamu kuruluşları ve ABD Hükümeti için lisans verme**. Yazılım Amerika Birleşik Devletleri Hükümeti dahil olmak üzere devlet makamlarına, bu Sözleşmede açıklanan lisans hakları ve kısıtlamalar uyarınca sağlanır.

19. **Ticari denetim uygunluğu**.

a) Yazılımı doğrudan veya dolaylı olarak ihraç edemez, yeniden ihraç edemez, transfer edemez veya başka bir şekilde herhangi bir kişinin kullanımına sunamaz ya da ESET'i veya holding şirketlerini, bağlı şirketleri ve herhangi bir holding şirketinin bağlı şirketlerinin yanı sıra holding şirketleri tarafından kontrol edilen kuruluşları ("Bağlı Kuruluşlar"), aşağıdakileri içeren Ticari Denetim Kanunlarını ihlal eder bir durumda veya bu kanunlar nezdinde negatif sonuçlara maruz bırakacak bir şekilde kullanamaz ya da bunlardan herhangi biriyle sonuçlanabilecek bir edime dahil olamazsınız:

i. Amerika Birleşik Devletleri, Singapur, Birleşik Krallık, Avrupa Birliği veya bağlı devlerinin ya da Sözleşme yükümlülüklerinin yerine getirileceği veya ESET'in veya Bağlı Kuruluşlarından herhangi birinin dahil olduğu ya da faaliyet gösterdiği bir ülkenin hükümeti, eyaleti ya da yetkili düzenleme kurumu tarafından çıkarılan ya da benimsenen; malların, yazılımların, teknolojinin ya da hizmetlerin ihracatı, yeniden ihracatı veya transferiyle ilgili lisans gereksinimlerini kontrol eden, sınırlandıran ya da dayatan tüm kanunlar ve

ii. Amerika Birleşik Devletleri, Singapur, Birleşik Krallık, Avrupa Birliği veya bağlı devlerinin ya da Sözleşme yükümlülüklerinin yerine getirileceği veya ESET'in veya Bağlı Kuruluşlarından herhangi birinin dahil olduğu ya da faaliyet gösterdiği bir ülkenin hükümeti, eyaleti ya da yetkili düzenleme kurumu tarafından getirilen tüm ekonomik, mali, ticari veya diğer yasaklar, kısıtlamalar, ambargolar, ithalat veya ihracat yasakları, fon ya da varlıkların aktarımıyla veya hizmetlerin sağlanmasıyla ilgili yasaklamalar ya da eş değer tedbirler.

(yukarıdaki i ve ii maddelerinde belirtilen yasal işlemler bir arada "Ticari Denetim Kanunları" olarak adlandırılır).

b) ESET aşağıdakilerin gerçekleşmesi durumunda hemen geçerli olmak üzere bu Şartlar nezdindeki yükümlülüklerini askıya alma veya bu Şartları sonlandırma hakkını saklı tutar:

i. ESET, kendi makul gerekçelerine dayalı fikrince, Kullanıcının Sözleşmenin Madde 19 a) altında belirtilen ihlal şartını ihlal ettiğine veya ihlal etme olasılığının yüksek olduğuna karar verirse veya

ii. Son Kullanıcı ve/veya Yazılım Ticari Denetim Kanunlarının öznesi haline gelirse ve bunun sonucu olarak ESET kendi makul gerekçelerine dayalı fikrince, Sözleşme nezdindeki yükümlülüklerini uygulamaya devam etmesinin,

ESET'i veya Bağlı Kuruluşlarını Ticari Denetim Kanunlarını ihlal eder bir durumda bırakacağına ya da bu Kanunlar nezdinde olumsuz sonuçlara maruz bırakacağına karar verirse.

c) Sözleşmedeki herhangi bir ifade, taraflardan herhangi birinin geçerli Ticari Denetim Kanunları ile tutarsız olan, bu Kanunlar nezdinde cezalandırılacak olan ya da yasaklanmış olan herhangi bir edimde bulunmasına neden olacak veya böyle bir edimde bulunmasını gerektirecek ya da Kanunlar nezdinde uygun olan bir edimde bulunmamasına neden olacak ya da bulunmamasını gerektirecek şekilde davranması (veya bunları yapmayı kabul etmesi) için tasarlanmamıştır ve bu şekilde yorumlanamaz ya da tahlil edilemez.

20. **Bildirimler**. Yazılım ve Belgelerin tüm bildirimleri ve iadeleri şuraya yapılmalıdır: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic ve bu iade durumlarında Sözleşmenin 22. maddesine uygun olarak ESET'in bu Sözleşme, Gizlilik Politikaları, Kullanım Ömrü Donu Politikası ve Belgelerdeki herhangi bir değişiklik konusunda Sizinle iletişime geçme hakkına zarar vermez. ESET, Size e-posta, Yazılım üzerinden uygulama içi bildirimler gönderebilir veya iletişimi web sitemizde yayınlayabilir. Şartlar, Özel Şartlar veya Gizlilik Politikalarında yapılan değişikliklerle ilgili iletişimler, yanıtlamanız için sunulan tüm sözleşme teklifleri/kabuller ya da davetiyeler, bildirimler veya diğer yasal iletişimler dahil olmak üzere ESET'ten yasal iletişimleri elektronik ortamda almayı kabul edersiniz. Bu tür elektronik iletişimler, geçerli yasalarca özel olarak farklı bir iletişim biçimi gerektirilmediği sürece yazılı olarak alınmış kabul edilecektir.

21. **Geçerli yasa**. Bu Sözleşme Slovakya Cumhuriyeti yasalarına tabidir ve bu yasalara uygun şekilde yorumlanır. Son Kullanıcı ve Sağlayıcı, yasalar ve Malların Uluslararası Satışına İlişkin Anlaşmalar hakkındaki Birleşmiş Milletler Konvansiyonu arasındaki ihtilaflı hükümlerin geçerli olmadığını kabul etmiş sayılır. Sağlayıcıyla ilgili olarak bu Sözleşmeden kaynaklanan tüm anlaşmazlıkların veya iddiaların ya da Yazılımın kullanımı ile ilgili tüm anlaşmazlıkların veya iddiaların Bratislava I. Bölge Mahkemesinde çözümleneceğini ve adı geçen mahkemenin yargı yetkisini uygulamasını açıkça kabul etmiş olursunuz.

22. **Genel hükümler**. Bu Sözleşmenin herhangi bir hükmünün geçersiz veya uygulanamaz olması durumunda, bu Sözleşmenin diğer hükümlerinin geçerliliği etkilenmez ve bu hükümler bu belgede belirtilen koşullar doğrultusunda geçerli ve uygulanabilir kalırlar. Bu Sözleşme İngilizce dilinde gerçekleştirilmiştir. Kolaylık açısından veya başka bir amaca yönelik olarak sözleşmenin herhangi bir çevirisi hazırlanmışsa ya da bu Sözleşmenin dil versiyonları arasında bir çatışma olması halinde İngilizce versiyon esas kabul edilecektir.

ESET, Yazılımda değişiklik yapma ve bu Sözleşmenin şartlarını, Eklentilerini, İlave Sözleşmelerini, Gizlilik Politikasını, Kullanım Ömrü Sonu (EOL) Politikasını ve Belgeleri veya bunların herhangi bir bölümünü herhangi bir zamanda değiştirme hakkını saklı tutar. Bu değişiklikleri (i) Yazılım veya ESET'in iş yapma şeklinde yapılan değişiklikleri yansıtmak üzere, (ii) yasal veya düzenleyici nedenlerle ya da güvenlik gerekçeleriyle veya (iii) kötüye kullanım ya da zararı önlemek amacıyla ilgili dokümanı güncelleyerek yapar. Sözleşmede yapılan herhangi bir revizyonla ilgili olarak e-posta, uygulama içi bildirim veya diğer elektronik araçlar üzerinden bilgilendirilirsiniz. Sözleşmede yapılan değişiklikleri kabul etmezseniz değişiklik bildirimini aldıktan sonraki 30 gün içinde 10. Maddeye uygun olarak bu sözleşmeyi sonlandırabilirsiniz. Bu süre içerisinde Sözleşmeyi sonlandırmazsanız yapılan değişiklikler kabul edilmiş sayılır ve değişiklik bildirimini aldığınız tarihten itibaren Sizin için geçerli hale gelmiş olur.

Bu Sözleşme, Sağlayıcı ve Sizin aranızdaki Yazılım için geçerli olan tüm Sözleşmeyi temsil eder ve Yazılıma ilişkin daha önceki tüm beyanları, görüşmeleri, yükümlülükleri, haberleşmeleri veya tanıtımları geçersiz kılar ve bunların yerine geçer.

SÖZLEŞMEYE EK

Ağ Bağlantılı Cihazlar İçin Güvenlik Değerlendirmesi. Ağ Bağlantılı Cihazlar İçin Güvenlik Değerlendirmesi sürecinde aşağıdaki ek hükümler geçerlidir:

Yazılım lisans bilgileriyle bağlantılı olarak, yerel ağ adını ve yerel ağdaki cihazın varlığı, türü, adı, IP adresi ve MAC adresi gibi bilgileri gerektiren Son Kullanıcı'nın yerel ağı ve yerel ağdaki cihazların güvenliğini denetleme amaçlı bir

işlev içerir. Bu bilgiler aynı zamanda yönlendirici cihazlar için kablosuz güvenlik türü ve kablosuz şifreleme türünü de içerir. Bu işlev, yerel ağdaki cihazların güvenliğini sağlamak için güvenlik yazılımı çözümünün kullanılabilirliği ile ilgili bilgiler de sağlayabilir.

Verilerin Kötüye Kullanılmasına Karşı Koruma. Verilerin Kötüye Kullanılmasına Karşı Koruma için aşağıdaki ek hükümler geçerlidir:

Yazılım, bilgisayarın çalınması ile doğrudan bağlantı sonucu önemli verilerin kaybolmasını veya kötü amaçla kullanılmasını önleyen bir işlev içerir. Bu işlev Yazılımın varsayılan ayarlarından kapatılır. ESET HOME Hesabının etkinleştirilmesi için oluşturulması gerekir. Böylelikle, bir bilgisayar hırsızlığı durumunda işlev veri toplama işlemini etkinleştirir. Yazılımın bu işlevini etkinleştirmeyi seçmeniz durumunda, bilgisayarın ağ konumu, bilgisayar ekranında görüntülenen içerikle ilgili veriler, bilgisayarın yapılandırması ya da bilgisayara bağlı bir kamera tarafından kaydedilen verilerin dahil olabileceği çalınmış bilgisayarla ilgili verilerin (buradan sonra "Veriler" olarak anılacaktır) toplanmasını ve Sağlayıcıya gönderilmesini kabul etmiş olursunuz. Son Kullanıcı, bu işlevle elde edilen ve ESET HOME Hesabı üzerinden sağlanan Verileri yalnızca bir Bilgisayar hırsızlığının neden olduğu olumsuz bir durumu gidermek amacıyla kullanma hakkına sahip olur. Sadece bu İşlevin amacına yönelik olarak Sağlayıcı, Verileri Gizlilik Politikasında belirtildiği şekilde ve ilgili yasal düzenlemelere uygun olarak işler. Sağlayıcı verilerin alınması amacının gerçekleştirilmesi için gerekli olan süre boyunca, Son Kullanıcının Verilere erişmesine izin verir ve bu süre Gizlilik Politikası'nda belirtilen elde bulundurma süresini aşamaz. Verilerin kötü amaçla kullanılmasına karşı koruma, yalnızca Son Kullanıcının yasal erişme hakkına sahip olduğu Bilgisayarlar ve hesaplarla kullanılır. Yasa dışı kullanımlar yetkili merciye bildirilir. Sağlayıcı, ilgili kanunlara uyar ve kötü amaçlı kullanım durumunda emniyet sorumlularına yardımcı olur. ESET HOME hesabına erişim için kullanılan parolanın korunmasından sorumlu olduğunuzu kabul edip onaylar ve parolanızı herhangi bir üçüncü tarafa açıklamayacağınızı kabul edersiniz. Son Kullanıcı; Verilerin Kötü Amaçla Kullanılmasına Karşı Koruma işlevi ile ESET HOME hesabının izinli veya izinsiz kullanılması faaliyetlerinden sorumludur. ESET HOME hesabının tehlikede olması durumunda bunu derhal Sağlayıcıya bildirin. Verilerin Kötüye Kullanılmasına Karşı Koruma için ek hükümler, münhasır olarak ESET Internet Security ve ESET Smart Security Premium Son Kullanıcıları için uygulanır.

ESET Secure Data. ESET Secure Data için aşağıdaki ek hükümler geçerlidir:

1. Tanımlar. ESET Secure Data için geçerli olan bu ek hükümlerde aşağıdaki sözcükler şu anlamlarda kullanılır:

a) "Bilgiler" yazılım kullanılarak şifrelenen veya deşifre edilen her türlü bilgi ve veriler;

b) "Ürünler" ESET Secure Data yazılımı ve belgeleri;

c) "ESET Secure Data" elektronik verilerin şifrelenmesi ve deşifre edilmesi için kullanılan yazılım(lar);

Çoğul içeren tüm referanslar tekil ifadeler kapsadığı gibi eril ifade içeren tüm referanslar da dişil ve nötr ifadeleri kapsar ve bunların tersi de geçerlidir. Belirli tanımlamaya sahip olmayan sözcükler Sözleşme tarafından belirtilen tanımlara uygun olarak kullanılmaktadır.

2. Ek Son Kullanıcı açıklaması. Şunları anlar ve kabul edersiniz:

a) Bilgileri korumak, onarmak ve yedeklemek sizin sorumluluğunuzdur;

b) ESET Secure Data yazılımını yüklemeden önce Bilgisayarınızdaki tüm bilgileri ve verileri (kritik bilgi ve veriler dahil ancak bunlarla sınırlı olmamak üzere) tam olarak yedeklemelisiniz;

c) ESET Secure Data yazılımını kurmak ve kullanmak için gereken tüm parolaların veya diğer bilgilerin güvenli bir kaydını tutmalısınız, ayrıca tüm şifreleme anahtarlarının, lisans kodlarının, anahtar dosyalarının ve ayrı bir depolama ortamında oluşturulan diğer verilerin yedek kopyalarını oluşturmalısınız;

d) Ürünlerin kullanımından siz sorumlusunuz. Sağlayıcı, bilgilerin veya verilerin, nerede ve ne şekilde depolandığından bağımsız olan bilgiler de dahil ancak bunlarla sınırlı olmamak üzere, herhangi bir yetkisiz veya hatalı şifrelenmesi veya deşifresi sonucunda ortaya çıkan hiçbir zarar, talep veya hasardan sorumlu tutulamaz;

e) Sağlayıcı her ne kadar ESET Secure Data yazılımının doğruluğu ve güvenliğini sağlamak için gereken tüm makul adımları atmış olsa da ürünler (veya ürünlerden herhangi biri) arızaya bağışık bir güvenlik düzeyine bağımlı olan bir alanda veya riskli ya da tehlikeli olabilecek bir alanda (nükleer tesisler, uçak navigasyonu, kontrol veya haberleşme sistemleri, silah ve savunma sistemleri ve yaşam destek ya da yaşam izleme sistemleri dahil ancak bunlarla sınırlı olmamak üzere) kullanılmamalıdır;

f) Ürünler tarafından sağlanan güvenlik ve şifreleme düzeyinin İhtiyaçlarınızı karşıladığından emin olmak Son Kullanıcının sorumluluğudur;

g) Ürünleri veya ürünlerden herhangi birini Kullanımız, söz konusu kullanımın Slovak Cumhuriyeti veya ürünün kullanıldığı diğer ülke, bölge veya eyaletin geçerli olan tüm yasa ve düzenlemelerine uygun olduğunu sağlamak dahil ancak bununla sınırlı olmamak üzere sizin sorumluğunuzdadır. Ürünlerin kullanımından önce, hiçbir hükümet (Slovak Cumhuriyeti veya başka bir şekilde) ambargosunu ihlal etmediğinizden emin olmanız gerekir;

h) ESET Secure Data yazılımı; lisans bilgilerini, kullanılabilir yamaları, hizmet paketlerini ve ESET Secure Data yazılımını iyileştirebilecek, sürdürebilecek, değiştirebilecek veya geliştirebilecek diğer güncellemeleri kontrol etmek için zaman zaman Sağlayıcı sunucularıyla iletişim kurabilir ve Gizlilik Politikasına uygun olarak, işleviyle ilgili genel sistem bilgilerini gönderebilir.

i) Sağlayıcı; parolaların, şifreleme anahtarlarının, lisans etkinleştirme kodlarının ve yazılımın kullanımı sırasında oluşturulan veya depolanan diğer verilerin kaybından, çalınmasından, kötüye kullanımından, zarar görmesinden veya yok edilmesinden kaynaklanan hiçbir kayıptan, zarardan, maliyetten veya talepten sorumlu tutulamaz.

ESET Secure Data için geçerli olan ek hükümler münhasır olarak ESET Smart Security Premium Son Kullanıcıları için geçerlidir.

Password Manager Yazılım. Password Manager Yazılımı için aşağıdaki ek hükümler geçerlidir:

1. Ek Son Kullanıcı açıklaması. Şunları yapamayacağınızı anlar ve kabul edersiniz:

a) İnsan hayatının veya mülkün tehdit altında olduğu hiçbir kritik görev uygulamasını çalıştırmak için Password Manager Yazılımını kullanamazsınız. Password Manager Yazılımının bu tür amaçlar için tasarlanmadığını ve bu tür durumlarda başarısız olmasının ölüme, yaralanmaya veya ciddi mülk veya çevre hasarına neden olabileceğini ve Sağlayıcının bunlardan sorumlu olmadığını anlarsınız.

PASSWORD MANAGER YAZILIMI NÜKLEER TESİSLERİN, UÇAK NAVİGASYONUNUN VEYA HABERLEŞME SİSTEMLERİNİN, HAVA TRAFİĞİ KONTROLÜNÜN VE YAŞAM DESTEĞİ YA DA SİLAH SİSTEMLERİNİN TASARIMI, YAPIMI, BAKIMI VE FAALİYETİ DAHİL ANCAK BUNLARLA SINIRLI OLMAMAK ÜZERE ARIZA DURUMUNA BAĞIŞIK DENETİMLER GEREKTİREN TEHLİKELİ ORTAMLARDA KULLANIM İÇİN TASARLANMAMIŞ, OLUŞTURULMAMIŞ VE LİSANSLANDIRILMAMIŞTIR. SAĞLAYICI ÖZEL OLARAK BU TÜR AMAÇLAR İÇİN AÇIK VEYA ZIMNİ TÜM GARANTİLERİ REDDEDER.

b) Password Manager Yazılımını bu sözleşmeyi veya Slovak Cumhuriyeti'nin veya bulunduğunuz anayasal alanın kanunlarını ihlal edecek şekilde kullanamazsınız. Özellikle, Password Manager Yazılımını zararlı içerik veya yasa dışı faaliyetler için kullanılabilecek olan içerik ya da herhangi bir şekilde yasayı ya da herhangi bir üçüncü taraf haklarını (tüm fikri mülkiyet hakları da dahil) ihlal eden içerik verilerini yüklemek dahil ancak bununla sınırlı olmamak üzere, Depolamadaki hesaplara (Password Manager Yazılımı için geçerli olan bu ek şartların amaçlarına uygun olarak "Depolama", senkronizasyonu etkinleştirme ve kullanıcı verilerinin yedeklenmesi amacına yönelik olarak Sağlayıcı tarafından veya Sağlayıcı dışındaki bir üçüncü tarafça ve kullanıcı tarafından yönetilen veri

depolama alanı anlamına gelmektedir) veya diğer Password Manager Yazılımı ya da Depolama kullanıcılarının herhangi bir hesabına ve verilerine erişim elde etmek için bulunulan tüm girişimler dahil ancak bunlarla sınırlı olmamak üzere, herhangi bir yasa dışı faaliyet gerçekleştirmek veya bu türden faaliyetlerin tanıtımını yapmak için kullanamazsınız. Bu şartlardan herhangi birini ihlal ederseniz Sağlayıcı bu sözleşmeyi derhal sonlandırma ve gerekli tüm tazminatların maliyetini tarafınıza yönlendirme, aynı zamanda para iadesi yapılmaksızın Password Manager Yazılımının daha fazla kullanılmasını önlemek için gereken tüm adımları atmaya hak kazanır.

2. YÜKÜMLÜLÜKLERİN SINIRLANDIRILMASI. PASSWORD MANAGER YAZILIMI "OLDUĞU GİBİ" SAĞLANIR. HERHANGİ TÜRDE BİR GARANTİ İFADE VEYA İMA EDİLMEZ. YAZILIMI KENDİ RİSKİNİZİ TAŞIYARAK KULLANIRSINIZ. ÜRETİCİ; VERİ KAYBI, HASAR, VERİ SENKRONİZASYONU VE YEDEKLEME İÇİN PASSWORD MANAGER YAZILIMI TARAFINDAN HARİCİ DEPOLAMAYA GÖNDERİLEN TÜM VERİLER DAHİL HİZMET KULLANILABİLİRLİĞİNİN KISITLANMASI İÇİN SORUMLU TUTULAMAZ. VERİLERİ PASSWORD MANAGER YAZILIMI KULLANARAK ŞİFRELEMEK, SÖZ KONUSU VERİLERİN GÜVENLİĞİ AÇISINDAN SAĞLAYICIYA HİÇBİR SORUMLULUK YÜKLEMEZ. ELDE EDİLEN, KULLANILAN, ŞİFRELENEN, DEPOLANAN, SENKRONİZE EDİLEN VEYA PASSWORD MANAGER YAZILIMI KULLANILARAK GÖNDERİLEN VERİLERİN ÜÇÜNCÜ TARAF SUNUCULARINDA DA DEPOLANABİLECEĞİNİ AÇIKÇA KABUL EDERSİNİZ (BU DURUM YALNIZCA SENKRONİZASYON VE YEDEKLEME HİZMETLERİNİN ETKİNLEŞTİRİLDİĞİ PASSWORD MANAGER YAZILIMININ KULLANIMI İÇİN GEÇERLİDİR). SAĞLAYICI TAMAMEN KENDİ TAKDİRİNE BAĞLI OLARAK BU TÜRDEN BİR ÜÇÜNCÜ TARAF DEPOLAMA, WEB SİTESİ, WEB PORTALI, SUNUCU VEYA HİZMETİ KULLANMAYI TERCİH EDERSE, SAĞLAYICI BU TÜRDEN BİR ÜÇÜNCÜ TARAF HİZMETİNİN KALİTESİ, GÜVENLİĞİ VEYA KULLANILABİLİRLİĞİ İÇİN SORUMLU TUTULAMAZ VE SAĞLAYICI HİÇBİR ŞEKİLDE ÜÇÜNCÜ TARAFLARCA YAPILAN SÖZLEŞMEDEN VEYA YASALARDAN KAYNAKLANAN YÜKÜMLÜLÜKLERİN İHLALİ İÇİN SİZE KARŞI HİÇBİR ŞEKİLDE SORUMLU DEĞİLDİR, AYRICA SAĞLAYICI BU YAZILIMIN KULLANIMI ESNASINDA ORTAYA ÇIKAN ZARARLAR, KAR KAYBI, FİNANSAL VEYA FİNANSAL OLMAYAN ZARARLAR VEYA BAŞKA HERHANGİ TÜRDEN BİR KAYIP İÇİN DE SORUMLU TUTULAMAZ. SAĞLAYICI PASSWORD MANAGER YAZILIMI KULLANILARAK ELDE EDİLEN, KULLANILAN, ŞİFRELENEN, DEPOLANAN, SENKRONİZE EDİLEN VEYA GÖNDERİLEN VEYA DEPOLAMADA BULUNAN HİÇBİR VERİ İÇERİĞİ İÇİN SORUMLU TUTULAMAZ. SAĞLAYICININ DEPOLANAN VERİLERE ERİŞİMİNİN OLMADIĞINI VE BUNLARI İZLEME VEYA YASAL OLARAK ZARARLI İÇERİKLERİ KALDIRMA BECERİSİNİN OLMADIĞINI KABUL EDERSİNİZ.

Sağlayıcı, Password MANAGER Yazılımıyla ilgili tüm iyileştirmeler, yükseltmeler ve onarımların ("İyileştirmeler"), söz konusu iyileştirmeler sizin tarafınızdan herhangi bir biçimde iletilen geribildirimlere, görüşlere veya önerilere dayalı olsa bile tüm haklarına sahiptir. Bu türden İyileştirmelere yönelik olarak telif hakları da dahil olmak üzere hiçbir tazminat alma hakkınız yoktur.

SAĞLAYICI KURUMLARI VE LİSANS VEREN TARAFLAR SİZİN VEYA ÜÇÜNCÜ TARAFLARIN PASSWORD MANAGER YAZILIMINI KULLANMANIZ, HERHANGİ BİR ARACI FİRMA VEYA SATICININ KULLANILMASI VEYA KULLANILMAMASI YA DA HERHANGİ BİR GÜVENLİĞİN SATIN ALINMASI VEYA SATILMASI SONUCU VEYA BU TÜR KULLANIMLA HERHANGİ BİR ŞEKİLDE İLİŞKİLİ OLARAK ORTAYA ÇIKAN TALEPLER VE SORUMLULUKLAR İÇİN, SÖZ KONUSU TALEP VE SORUMLULUKLARIN HERHANGİ BİR YASAL YA DA EŞDEĞER TEORİYE DAYANIP DAYANMAMASINDAN BAĞIMSIZ OLARAK, SİZE KARŞI SORUMLU TUTULAMAZ.

SAĞLAYICI KURUMLARI VE LİSANS VEREN TARAFLAR; HERHANGİ BİR ÜÇÜNCÜ TARAF YAZILIM, PASSWORD MANAGER YAZILIMI ÜZERİNDEN ERİŞİLEN HERHANGİ BİR VERİ TABANI, PASSWORD MANAGER YAZILIMINI KULLANMANIZ VEYA KULLANAMAMANIZ YA DA ERİŞEMEMENİZ SONUCU OLARAK VEYA BU TÜRDE BİR DURUMLA İLİŞKİLİ OLARAK ORTAYA ÇIKAN HİÇBİR DOĞRUDAN, TESADÜFİ, ÖZEL, DOLAYLI VEYA KOŞULLARA BAĞLI HASAR İÇİN, SÖZ KONUSU ZARARA YÖNELİK TALEPLER HERHANGİ BİR KANUN TEORİSİNE VEYA EŞDEĞER TEORİYE DAYANDIRILSA DAHİ SİZE KARŞI SORUMLU TUTULAMAZ. BU ŞART KAPSAMINDA HARİÇ BIRAKILAN ZARARLAR, BUNLARLA KISITLI OLMAMAKLA BİRLİKTE, İŞLETME KARININ KAYBINI, KİŞİYE VEYA MÜLKE VERİLEN ZARARLARI, İŞ KESİNTİLERİNİ, İŞ VEYA KİŞİSEL BİLGİLERİN KAYBINI İÇERİR. BAZI YARGI ALANLARI TESADÜFİ VEYA KOŞULLARA BAĞLI ZARARLARIN KISITLANMASINA İZİN VERMEDİĞİ İÇİN BU KISITLAMA SİZİN İÇİN GEÇERLİ OLMAYABİLİR. BU DURUMDA SAĞLAYICININ SORUMLULUĞU GEÇERLİ YASALARCA İZİN VERİLEN MİNİMUM DÜZEYDEDİR.

HİSSE SENEDİ FİYATLARI, ANALİZLER, PAZAR BİLGİLERİ, HABERLER VE FİNANSAL VERİLER DAHİL PASSWORD

MANAGER YAZILIMI ÜZERİNDEN SAĞLANAN BİLGİLER GECİKEBİLİR, DOĞRU OLMAYABİLİR VEYA HATALAR YA DA GÖZ ARDI EDİLEN UNSURLAR İÇEREBİLİR; SAĞLAYICI KURUMLARI VE LİSANS VEREN TARAFLAR BU DURUMDAN HİÇBİR ŞEKİLDE SORUMLU DEĞİLDİR. SAĞLAYICI PASSWORD MANAGER YAZILIMININ HERHANGİ BİR BÖLÜMÜNÜ VEYA ÖZELLİĞİNİ YA DA PASSWORD MANAGER YAZILIMINDAKİ ÖZELLİKLERİN YA DA TEKNOLOJİNİN TÜMÜNÜN VEYA HERHANGİ BİRİNİN KULLANIMINI DİLEDİĞİ ZAMAN TARAFINIZA ÖNCEDEN BİLDİRİMDE BULUNMAKSIZIN DEĞİŞTİREBİLİR VEYA SONLANDIRABİLİR.

BU MADDEDEKİ ŞARTLAR HERHANGİ BİR NEDENDEN ÖTÜRÜ GEÇERSİZ OLURSA YA DA SAĞLAYICI GEÇERLİ YASALAR ALTINDA ZARARLAR, HASARLAR VS. İÇİN SORUMLU TUTULURSA, TARAFLAR SAĞLAYICININ SİZE KARŞI SORUMLULUĞUNUN TARAFINIZDAN ÖDENMİŞ OLAN LİSANS ÜCRETLERİNİN TOPLAM TUTARI İLE SINIRLANDIRILACAĞINI KABUL EDERLER.

SAĞLAYICIYI VE ÇALIŞANLARINI, BAĞLI ŞİRKETLERİNİ, İŞ ORTAKLARINI, YENİDEN MARKALANDIRMA VE DİĞER ORTAKLARI; HERHANGİ BİR ÜÇÜNCÜ TARAFA VE TÜM ÜÇÜNCÜ TARAFLARA (AYGIT SAHİPLERİ VEYA HAKLARI PASSWORD MANAGER YAZILIMINDA VEYA DEPOLAMADA KULLANILAN VERİLERCE ETKİLENMİŞ OLAN TARAFLAR DA DAHİL) VE BU ÜÇÜNCÜ TARAFLARDAN YAPILAN TALEPLERE, SORUMLULUKLARA, HASARLARA, KAYIPLARA, MALİYETLERE, SÖZ KONUSU TARAFLARIN PASSWORD MANAGER YAZILIMINI KULLANMANIZ SONUCUNDA İSTEYEBİLECEĞİ ÜCRETLERE KARŞI TAZMİN ETMEYİ, SAVUNMAYI VE ZARAR GÖRMEMELERİNİ SAĞLAMAYI KABUL EDERSİNİZ.

3. Password Manager Yazılımındaki Veriler. Tarafınızdan başka bir şekilde ve açıkça tercih edilmediği sürece, bir Password Manager Yazılımına kaydedilen, sizin tarafınızdan girilen tüm veriler bilgisayarınızda veya tanımladığınız başka bir depolama aygıtında depolanır. Herhangi bir Password Manager Yazılımı veri tabanının veya diğer dosyaların silinmesi ya da hasar görmesi durumunda, bunlar içinde bulunan verilerin geri döndürülemez bir şekilde kaybolduğunu anlarsınız ve söz konusu kaybın riskini anlar ve kabul edersiniz. Kişisel verilerinizin bilgisayarda şifrelenmiş halde depolanması, bu bilgilerin çalınamayacağı veya veri tabanını açmak için Ana Parolayı keşfeden ya da müşteri tarafından tanımlanan etkinleştirme aygıtına erişim elde eden birisi tarafından kötüye kullanılamayacağı anlamına gelmez. Tüm erişim yöntemlerinin güvenliğini sürdürmekten siz sorumlusunuz.

4. Kişisel Verilerin Sağlayıcıya veya Depolamaya Aktarımı. Bu şekilde tercih etmeniz halinde ve yalnızca zamanında veri senkronizasyonu ve yedekleme yapılması amacına yönelik olarak, Password Manager Yazılımı; Password Manager Yazılımı veri tabanındaki kişisel verileri (başka bir ifadeyle parolalar, giriş bilgileri, Hesaplar ve Kimlikler) İnternet üzerinden Depolamaya aktarır veya gönderir. Veriler özel olarak şifrelenmiş biçimde iletilir. Password Manager Yazılımının çevrimiçi formları parolalarla, giriş bilgileriyle veya diğer bilgilerle doldurmak için kullanılması, söz konusu bilgilerin İnternet üzerinden sizin tarafınızdan tanımlanan web sitesine gönderilmesini gerektirebilir. Bu veri aktarımı, Password Manager Yazılımı tarafından başlatılmaz ve bu nedenle Sağlayıcı çeşitli sağlayıcılar tarafından desteklenen web siteleriyle bulunulan bu tür etkileşimlerin güvenliğinden sorumlu tutulamaz. İnternet üzerinden yapılan tüm işlemler, Password Manager Yazılımı ile bağlantılı olsun veya olmasın, tamamen kendi kararınız ve riskiniz üzerine yapılır ve bu türden herhangi bir malzeme veya hizmetin indirilmesinden ve/veya kullanılmasından doğan, bilgisayar sisteminizde oluşan her türlü hasardan veya veri kaybından yalnızca siz sorumlu olursunuz. Değerli verilerin kaybolması riskini en düşük düzeye indirmek için Sağlayıcı müşterilerin veri tabanının ve diğer hassas dosyaların düzenli olarak harici sürücülere yedeklenmesini önerir. Sağlayıcı kaybolan veya zarar gören verilerin kurtarılmasında size herhangi bir destek sağlayamaz. Sağlayıcı Son Kullanıcının bilgisayarındaki dosyaların zarar görmesi veya silinmesi halinde Son Kullanıcı veri tabanı dosyaları için yedekleme hizmetleri sağlarsa, söz konusu yedekleme hizmeti için hiçbir garanti verilmez ve Sağlayıcı size karşı hiçbir şekilde herhangi bir sorumluluk altına girmez.

Password Manager Yazılımını kullanarak yazılımın; lisans bilgilerini, kullanılabilir yamaları, hizmet paketlerini ve Password Manager Yazılımını iyileştirebilecek, sürdürebilecek, değiştirebilecek veya geliştirebilecek diğer güncellemeleri kontrol etmek için zaman zaman Sağlayıcı sunucularıyla iletişim kurabileceğini kabul edersiniz. Yazılım Password Manager Yazılımının işleviyle ilgili genel sistem bilgilerini Gizlilik Politikasına uygun olarak gönderebilir.

5. Yükleme kaldırma bilgileri ve talimatları. Veri tabanından almak istediğiniz tüm bilgilerin, Password Manager Yazılımının yüklemesi kaldırılmadan önce dışa aktarılması gerekir.

Password Manager Yazılımı için ek hükümler münhasır olarak ESET Smart Security Premium Son Kullanıcıları için geçerlidir.

ESET LiveGuard. ESET LiveGuard için aşağıdaki ek hükümler geçerlidir:

Yazılım, Son Kullanıcı tarafından gönderilen dosyaların ek analizini yapan bir işlev içerir. Sağlayıcı, Son Kullanıcı tarafından gönderilen dosyaları ve analiz sonuçlarını yalnızca Gizlilik Politikasına ve ilgili yasal düzenlemelere uygun olarak kullanacaktır.

ESET LiveGuard için geçerli olan ek hükümler münhasır olarak ESET Smart Security Premium Son Kullanıcıları için geçerlidir.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Gizlilik Politikası

Kişisel verilerin korunması bir Veri Denetleyicisi ("ESET" veya "Biz") olan ve Einsteinova 24, 851 01 Bratislava, Slovak Republic adresinde mukim ve Bratislava I. Bölge Mahkemesinin Ticari Sicil Kaydında Bölüm Sro, Giriş No 3586/B, İşyeri Sicil Numarası: 31333532 olan ESET, spol. s r. o. için özellikle önemlidir. AB Genel Veri Koruma Yönetmeliği ("GDPR") altında yasal olarak standartlaştırılan şeffaflık gereksinimine uymayı istiyoruz. Bu amaçla, bu Gizlilik Politikasını yalnızca veri öznesi olarak müşterimizi ("Son Kullanıcı" veya "Siz") şu kişisel veri koruma konuları hakkında bilgilendirmek için yayınlamaktayız:

- Kişisel Verilerin İşlenmesi İçin Yasal Dayanak,
- Veri Paylaşımı ve Gizlilik,
- Veri Güvenliği,
- Veri Öznesi Olarak Haklarınız,
- Kişisel Verilerinizin İşlenmesi
- İletişim bilgileri.

Kişisel Verilerin İşlenmesi İçin Yasal Dayanak

Veri işleme için yalnızca birkaç yasal dayanak vardır ve Biz, bu dayanakları kişisel verilerin korunması ile ilgili geçerli yasal çerçeveye uygun olarak kullanırız. ESET'te kişisel verilerin işlenmesi, genel olarak, Son Kullanıcı ile yapılan Son Kullanıcı Lisans Sözleşmesi ("EULA") (Madde 6 (1) (b) GDPR), şartlarının uygulanması için temel olarak gereklidir ve aşağıdaki örnekteki gibi başka bir şekilde belirtilmediği takdirde ESET ürün ve hizmetlerinin sağlanması için geçerlidir:

- Kullanıcılarımıza sunabileceğimiz en iyi korumayı, desteği ve deneyimi sağlamak için müşterilerimizin Hizmetlerimizi nasıl kullandığıyla ve memnuniyetiyle ilgili verileri işlememize olanak sağlayan kanuni menfaatlere ilişkin yasal zemin (Madde 6 (1) (f) GDPR). Pazarlama bile geçerli kanunlar tarafından meşru bir menfaat olarak görülmektedir. Bu nedenle, genellikle müşterilerimizle pazarlama iletişimimiz için bu zemine güveniriz.

- Bu yasal zemini en uygun zemin olarak kabul ettiğimizde veya yasalarca gerekli görüldüğünde belirli durumlarda Sizden talep ettiğimiz onay (Madde. 6 (1) (a) GDPR).

- Bir yasal yükümlülükle, örneğin elektronik iletişim, faturanın saklanması veya faturalandırma belgeleri için gereksinimlere uygunluk (Madde 6 (1) (c) GDPR).

Veri Paylaşımı and Gizlilik

Verilerinizi üçüncü taraflarla paylaşmayız. Ancak ESET; satış, hizmet ve destek ağımızın bir parçası olarak bağlı şirketler veya iş ortakları üzerinden global olarak faaliyet gösteren bir şirkettir. ESET tarafından işlenen lisanslar, faturalandırma ve teknik destek bilgileri, Son Kullanıcı Lisans Sözleşmesi (EULA) şartlarının (örneğin hizmetleri sağlama veya destek sunma) yerine getirilmesi amacıyla, bağlı kuruluşlar veya iş ortaklarına ya da bu kurumlardan tarafımıza aktarılabilir.

ESET, verilerini Avrupa Birliği'nde (AB) işlemeyi tercih eder. Ancak konumunuza (ürünlerimizin ve/veya hizmetlerimizin AB dışında kullanımına) ve/veya seçtiğiniz hizmete bağlı olarak, verilerinizin AB dışında bir ülkeye aktarılması gerekebilir. Örneğin, bulut bilgi işlemle bağlantılı olarak üçüncü taraf hizmetlerini kullanırız. Bu durumlarda, hizmet sağlayıcılarımızı dikkatlice seçer ve sözleşme yoluyla, teknik ve organizasyonel önlemlerle birlikte uygun bir veri koruması düzeyine sahip olduğumuzdan emin oluruz. Kural olarak, gerekirse, ek sözleşme düzenlemeleriyle birlikte AB standart sözleşme maddeleri üzerinde anlaşmaya varırız.

AB dışındaki bazı ülkelerde (örneğin Birleşik Krallık ve İsviçre) AB, halihazırda karşılaştırılabilir bir veri koruması düzeyi belirlemiştir. Karşılaştırılabilir veri koruması düzeyine bağlı olarak, verilerin bu ülkelere aktarımı için özel yetkilendirme veya sözleşme gerekmemektedir.

Veri Güvenliği

ESET, potansiyel risklere uygun bir güvenlik düzeyi sağlamak için uygun teknik ve organizasyonel önlemleri alır. Gizlilik, doğruluk, sistemlerin ve hizmetlerin kullanılabilirliği ve dayanıklılığını sürekli olarak sağlamak için elimizden gelenin en iyisini yaparız. Ancak haklarınız ve özgürlüklerinize yönelik bir riskle sonuçlanan veri ihlali durumunda ilgili yetkili kurumu ve veri özneleri olarak etkilenen Son Kullanıcıları bilgilendirmeye hazırız.

Veri Öznesinin Hakları

Her Son Kullanıcının hakları önemlidir ve (herhangi bir AB ülkesindeki veya AB olmayan herhangi bir ülkedeki) tüm Son Kullanıcıların aşağıdaki haklarının ESET tarafından garanti edildiğini size bildirmek isteriz. Veri öznesi olarak haklarınızı kullanmak için destek formu üzerinden veya dpo@eset.sk e-posta adresinden e-posta göndererek bizimle iletişime geçebilirsiniz. Tanımlama amaçlarına yönelik olarak sizden şu bilgiler istenir: Ad, e-posta adresi ve (varsa) lisans anahtarı veya müşteri numarası ve şirket ilişikliği. Lütfen bize doğum tarihi gibi diğer kişisel verileri göndermekten kaçının. İsteğinizi işleyebilmenin yanı sıra tanımlama amaçlarına yönelik olarak da kişisel verilerinizi işleyeceğimizi belirtmek isteriz.

Onayı Geri Çekme Hakkı. Onayı geri çekme hakkı, yalnızca onaya dayalı olarak işleme durumunda geçerlidir. Kişisel verilerinizi onayınıza dayalı olarak işlersek herhangi bir zamanda herhangi bir neden belirtmeksizin onayı geri çekme hakkınız vardır. Onayınızı geri çekmek, yalnızca gelecekte geçerli olur ve onayın geri çekilmesinden önce işlenen verilerin yasallığı bu durumdan etkilemez.

İtiraz Hakkı. İşlemeye itiraz etme hakkı, ESET'in veya üçüncü tarafların yasal çıkarına dayalı olarak işleme durumunda geçerlidir. Yasal bir çıkarı korumak için kişisel verilerinizi işlersek veri öznesi olarak Sizin, tarafımızca belirtilen yasal çıkara ve kişisel verilerinizin işlemesine herhangi bir zamanda itiraz etme hakkınız vardır. İtirazınız yalnızca gelecek için etkilidir ve itirazdan önce işlenen verilerin yasallığı bu durumdan etkilenmez. Kişisel

verilerinizi doğrudan pazarlama amaçlarına yönelik olarak işlersek itirazınız için neden belirtmek gerekli değildir. Bu aynı zamanda, ilgili doğrudan pazarlama ile bağlantılı olduğu sürece, profil oluşturma için de geçerlidir. Tüm diğer durumlarda, kişisel verilerinizi işlememiz için ESET'in yasal çıkarına yönelik şikayetlerinizi bize kısaca bildirmenizi rica ederiz.

Onayınızı geri çekmenize rağmen bazı durumlarda, kişisel verilerinizi başka bir yasal temele dayanarak, örneğin bir sözleşmenin yerine getirilmesi amacıyla işlemeye devam etme hakkına sahip olduğumuzu lütfen unutmayın.

Erişim Hakkı. Bir veri öznesi olarak ESET tarafından depolanan verilerinizle ilgili bilgileri herhangi bir zamanda ücretsiz olarak alma hakkınız vardır.

Düzeltme Hakkı. Sizinle ilgili hatalı kişisel verileri yanlışlıkla işlememiz halinde bunun düzeltilmesini isteme hakkınız vardır.

Silme Hakkı ve İşlemenin Kısıtlanması Hakkı. Bir veri öznesi olarak, kişisel verilerinizin silinmesini veya bu verilerin işlenmesinin kısıtlanmasını talep etme hakkınız vardır. Kişisel verilerinizi örneğin onayınız ile işlememiz, onayı geri çekmeniz ve sözleşme gibi başka bir yasal dayanak olmaması halinde kişisel verilerinizi hemen sileriz. Ayrıca kişisel verileriniz, saklama süremizin sonunda bu veriler için belirtilen amaçlara yönelik olarak artık gerekli olmadığı anda silinir.

Kişisel verilerinizi yalnızca doğrudan pazarlama amacına yönelik olarak kullanırsak ve onayınızı geri çekerseniz veya ESET'in temel yasal menfaatine itiraz ederseniz, istenmeyen iletişimleri önlemek için iletişim verilerinizi dahili kara listemize ekler ve bunun dışında kişisel verilerinizin işlenmesini kısıtlarız. Aksi halde, kişisel verileriniz silinecektir.

Verilerinizi, kanuni veya denetleyici yetkililer tarafından belirtilen saklama yükümlülükleri ve dönemlerinin sona erme tarihine kadar saklamamız gerekebileceğini lütfen unutmayın. Elde tutma yükümlülükleri ve dönemleri Slovak kanunlarından da kaynaklanabilir. Bunun ardından ilgili veriler rutin olarak silinir.

Veri taşınabilirliği hakkı. Bir veri öznesi olarak Size, ESET tarafından işlenen kişisel verileri xls biçiminde sunmaktan memnuniyet duyarız.

Şikayette Bulunma Hakkı. Bir veri öznesi olarak, yetkili kuruluşa herhangi bir zamanda şikayette bulunma hakkınız vardır. ESET Slovak kanunlarının yürütülmesine tabidir ve Avrupa Birliği'nin parçası olarak veri koruma mevzuatına tabiyiz. İlgili veri denetim yetkilisi Slovakya Cumhuriyeti Kişisel Verileri Koruma Müdürlüğü'dür ve şu adreste bulunmaktadır: Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Kişisel Verilerinizin İşlenmesi

ESET tarafından sağlanan ve ürünümüze eklenen hizmetler, Son Kullanıcı Lisans Sözleşmesi EULAaltında sağlanmaktadır, ancak hizmetlerimizden bazıları özel dikkat gerektirmektedir. Hizmetlerimizin sağlanmasıyla bağlantılı veri toplama hakkında size daha fazla detay sunmak istiyoruz. Son Kullanıcı Lisans Sözleşmesi (EULA) ve ürünle ilgili dokümanlardaaçıklandığı şekilde çeşitli hizmetler sağlarız. Bunu yapabilmek için aşağıdaki bilgileri toplamamız gerekmektedir:

Lisans ve Faturalandırma Verileri. Ad, e-posta adresi, lisans anahtarı ve (varsa) adres, şirket ilişkisi ve ödeme verileri, lisansın etkinleştirilmesi, lisans anahtarının sağlanması, son kullanma tarihiyle ilgili hatırlatmalar, destek istekleri, lisansın orijinalliğinin doğrulanması, hizmetimizin sağlanması ve geçerli mevzuat ya da Sizin onayınıza uygun olarak pazarlama mesajları dahil olmak üzere diğer bildirimlerin iletilmesi amacıyla ESET tarafından toplanır ve işlenir. ESET, faturalandırma bilgilerini 10 yıllık süre boyunca yasal olarak tutmakla yükümlüdür, ancak lisans bilgileri lisans süresinin dolmasının ardından 12 ayın sonunda anonim hale getirilir.

Güncelleme ve Diğer İstatistikler. İşlenen bilgiler arasında yükleme işlemi ve ürünümüzün yüklenmiş olduğu platform dahil olmak üzere bilgisayarınızla ilgili bilgiler yer alır ve işletim sistemi, donanım bilgileri, yükleme kimlikleri, lisans kimlikleri, IP adresi, MAC adresi, ürünün yapılandırma ayarları gibi ürünlerimizin işlemleri ve işlevleri ile ilgili bilgiler, sağlama güncellemesi ve yükseltme hizmetleri ve bakım, güvenlik ve arka uç altyapımızın iyileştirilmesi amacına yönelik olarak işlenir.

Bu bilgiler, Son Kullanıcının tanımlanmasını gerektirmeyen lisans ve faturalandırma amaçları için gerekli olan kimlik bilgilerinden ayrı olarak tutulur. Saklama süresi 4 yıla kadardır.

ESET LiveGrid® Bilinirlik Sistemi. Sızıntılarla ilgili tek yönlü hash'ler ESET LiveGrid® Bilinirlik Sistemi amaçlarına yönelik olarak işlenir. Bu, taranan dosyaları buluttaki beyaz ve kara listelerde yer alan öğelerden oluşan veri tabanıyla karşılaştırarak zararlı yazılıma karşı koruma çözümlerimizin etkisini iyileştirir. Son Kullanıcı bu işlem sırasında tanımlanmaz.

ESET LiveGrid® Geri Bildirim Sistemi. ESET LiveGrid® İtibar Sistemi kapsamında dağınık haldeki ortamdan alınan şüpheli örnekler ve meta veriler, ESET'in son kullanıcılarımızın ihtiyaçlarına hemen yanıt vermesine ve en son tehditlere anında tepki verebilmemize olanak tanır. Hizmetlerimizi sağlamamız Sizin bize şu bilgileri iletmenize bağlıdır:

- Potansiyel virüs örnekleri ve diğer kötü amaçlı yazılım programları gibi sızıntılar; sorunlu, istenmeyen türden olabilecek veya tehlikeli olabilecek güvenilir olmayan nesneler (örneğin yürütülebilir dosyalar, Sizin tarafınızdan spam olarak bildirilen veya ürünümüz tarafından işaretlenen e-posta iletileri;

- IP adresi ve coğrafi bilgiler, IP paketleri, URL'ler ve ethernet çerçeveleri gibi internet kullanımı ile ilgili bilgiler;

- Kilitlenme bilgi döküm dosyaları ve içindeki bilgiler.

Bu kapsamın dışındaki verilerinizi toplamayı istemeyiz, ancak kimi zaman bunu önlemek mümkün olmamaktadır. Yanlışlıkla toplanan veriler kötü amaçlı yazılıma dahil edilebilir (bilginiz veya onayınız olmadan toplanabilir) veya dosya adlarının ya da URL'lerin bir parçası olarak gelebilir ve bu Gizlilik Politikası'nda açıklanan amaca yönelik olarak bu bilgilerin sistemlerimizin parçası haline gelmelerini veya bu bilgileri işlemeyi amaçlamayız.

ESET LiveGrid® Geri Bildirim Sistemi üzerinden elde edilen ve işlenen tüm bilgiler, Son Kullanıcı tanımlanmaksızın kullanılır.

Ağ Bağlantılı Cihazlar İçin Güvenlik Değerlendirmesi. Güvenlik değerlendirmesi işlevini sağlamak için yerel ağ adının yanı sıra lisans bilgileriyle bağlantılı olarak yerel ağınızda bulunan cihazın varlık, tür, ad, cihazın IP adresi ve MAC adresi gibi, yerel ağınızdaki cihazlarla ilgili bilgileri işleriz. Bu bilgiler aynı zamanda yönlendirici cihazlar için kablosuz güvenlik türü ve kablosuz şifreleme türünü de içerir. Son Kullanıcının kimliğini tanımlayan lisans bilgileri, lisansın süresi dolduktan sonra en fazla 12 ay sonra anonim hale getirilir.

Teknik destek. İletişim ve lisans bilgileri ve destek isteklerinizde yer alan veriler destek hizmeti için gerekli olabilir. Bizimle iletişim kurmak için seçtiğiniz kanala bağlı olarak e-posta adresinizi, telefon numaranızı, lisans bilgilerinizi, ürün ayrıntılarını ve destek olayınızın açıklamasını toplayabiliriz. Destek hizmetini kolaylaştırmak için bize başka bilgiler sağlamanız da istenebilir. Teknik destek için işlenen veriler 4 yıl boyunca saklanır.

Verilerin Kötüye Kullanılmasına Karşı Koruma. https://home.eset.com adresinde ESET HOME hesabı oluşturulursa ve işlev bilgisayarın çalınmasıyla bağlantılı olarak Son Kullanıcı tarafından etkinleştirilirse, şu bilgiler toplanır ve işlenir: konum verileri, ekran görüntüleri, bilgisayarın yapılandırmasıyla ilgili veriler ve bilgisayarın kamerası tarafından kaydedilen veriler. Toplanan veriler sunucularımızda veya hizmet sağlayıcılarımızın sunucularında 3 aylık saklama süresiyle saklanır.

Password Manager. Password Manager işlevini etkinleştirmeyi seçerseniz, giriş bilgileriniz ile ilgili veriler yalnızca

bilgisayarınızda veya atanan başka bir cihazda şifreli biçimde depolanır. Senkronizasyon hizmetini etkinleştirirseniz şifrelenen veriler sunucularımızda veya hizmet sağlayıcılarımızın sunucularında bu tür hizmetin sunulmasını sağlamak için saklanır. ESET'in ve hizmet sağlayıcının şifrelenen verilere erişimi yoktur. Verilerini şifresini açmak için yalnızca Sizin anahtarınız vardır. Veriler, işlevin devre dışı bırakılmasıyla kaldırılır.

ESET LiveGuard. ESET LiveGuard İşlevini etkinleştirmeyi seçerseniz Son Kullanıcı tarafından önceden tanımlanmış ve seçilmiş dosyalar gibi örneklerin gönderilmesi gerekir. Uzaktan analiz için seçtiğiniz örnekler ESET hizmetine yüklenir ve analiz sonucu Bilgisayarınıza geri gönderilir. Tüm şüpheli örnekler, ESET LiveGrid® Geri Bildirim Sistemi tarafından toplanan bilgilerle aynı şekilde işlenir.

Müşteri Deneyimini İyileştirme Programı. Şu programı etkinleştirmeyi seçerseniz: Müşteri Deneyimini İyileştirme Programı Ürünlerimizin kullanımıyla ilgili anonim telemetri bilgileri Onayınıza dayanarak toplanır ve kullanılır.

Ürünlerimizi ve hizmetlerimizi kullanan kişinin, ürünü veya hizmeti satın alan ve bizimle Son Kullanıcı Lisans Sözleşmesi (EULA) imzalamış olan Son Kullanıcı, aile üyesi veya Son Kullanıcı tarafından Son Kullanıcı Lisans Sözleşmesi'ne (EULA) uygun olarak başka bir şekilde yetkilendirilen bir kişi değilse verilerin işlemesi, ESET'in yasal çıkarları doğrultusunda gerçekleştirilir ve bu durumda, GDPR Madde 6 (1) f) uyarınca Son Kullanıcı tarafından yetkilendirilen kullanıcının Son Kullanıcı Lisans Sözleşmesi'ne (EULA) uygun olarak Bizim tarafımızdan sağlanan ürün ve hizmetleri kullanması mümkün olur.

İletişim bilgileri

Veri öznesi olarak hakkınızı kullanmak istemeniz halinde veya sorunuz ya da endişeniz varsa bize şu adresten mesaj gönderebilirsiniz:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk