ESET NOD32 Antivirus

Kullanıcı Kılavuzu

Bu belgenin yardım sürümünü görüntülemek için burayı tıklayın

Digital Security
Progress. Protected.

ESET NOD32 Antivirus, 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

ESET NOD32 Antivirus

ESET NOD32 Antivirus tamamen tümleşik bilgisayar güvenliğinde yepyeni bir yaklaşımın temsilcisidir. En yeni ESET LiveGrid® tarama altyapısı sürümü 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 NOD32 Antivirus, 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 NOD32 Antivirus 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 izler. 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 NOD32 Antivirus 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 NOD32 Antivirus ürününün özelliklerinin çalışması için aboneliğin etkin olması gerekir. ESET NOD32 Antivirus için aboneliğinizin süresi dolmadan birkaç hafta önce aboneliğinizi yenilemenizi öneririz.

Yenilikler

ESET NOD32 Antivirus 17.1 sürümündeki yenilikler

- Ağ Denetçisi'nde küçük iyileştirmeler
- Diğer küçük hata düzeltmeleri ve iyileştirmeler

> **Yenilikler ile ilgili bildirimleri** devre dışı bırakmak için:
> 1. Gelişmiş ayarlar > **Bildirimler** > **Masaüstü bildirimleri** öğesini açın.
> 2. **Masaüstü bildirimleri** öğesinin yanındaki **Düzenle** seçeneğine tıklayın.
> 3. **Yenilikler ile ilgili bildirimleri göster** onay kutusunun işaretini kaldırın ve **Tamam**'a tıklayın.
> Daha fazla bilgi için Bildirimler bölümüne bakın.

> ESET NOD32 Antivirus Ürünündeki değişikliklerin ayrıntılı bir listesi için ESET NOD32 Antivirus değişiklik günlüklerine 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**
- **ESET Security Ultimate**

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	ESET Security Ultimate
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		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Ağ Denetçisi		✔	✔	✔
Web Kamerası Koruması		✔	✔	✔
Ağ Saldırısına Karşı Koruma		✔	✔	✔
Botnet Koruması		✔	✔	✔
Güvenli Bankacılık ve Gezinme		✔	✔	✔
Tarayıcı Gizliliği ve Güvenliği		✔	✔	✔
Ebeveyn Kontrolü		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Yukarıdaki ürünlerdne bazıları sizin dilinizde / bölgenizde mevcut olmayabilir.

Sistem gereksinimleri

ESET NOD32 Antivirus 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

İşletim Sistemleri destekleniyor

Microsoft® Windows® 11

Microsoft® Windows® 10

Temmuz 2023'ten sonra piyasaya sürülen ESET ürünlerini yüklemek veya yükseltmek için tüm Windows işletim sistemlerine Azure Kod İmzalama desteği yüklenmelidir. Daha fazla bilgi.

İşletim sisteminizi daima güncel halde tutun.

ESET NOD32 Antivirus özellik gereksinimleri

Aşağıdaki tabloda belirli ESET NOD32 Antivirus özellikleri için sistem gereksinimlerine bakın:

Özellik	Gereklilikler
Intel® Threat Detection Technology	Desteklenen işleyicilere bakın.

Özellik	Gereklilikler
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.

Diğer

Etkinleştirme işlemi ve ESET NOD32 Antivirus 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 NOD32 Antivirus ürününü Windows 7, Windows 8 (8.1) veya Windows Home Server 2011'e sahip bir bilgisayara yüklemek istiyorsunuz
- ESET NOD32 Antivirus yükleme sırasında **Eski işletim sistemi** şeklinde bir hata görüntüler

Ayrıntılar

En son ESET NOD32 Antivirus sürümü, Windows 10 veya Windows 11 işletim sistemleri gerektirir.

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.

ESET NOD32 Antivirus 16.0 sürümünü yükleyin

Windows'u yükseltemiyorsanız ESET NOD32 Antivirus 16.0 sürümünü yükleyin. Daha fazla bilgi için ESET NOD32 Antivirus 16.0 sürümü çevrim içi yardım bölümüne bakın.

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 NOD32 Antivirus kullanım kılavuzuna hoş geldiniz. Burada sağlanan bilgiler, ürününüzü tanımanızı ve bilgisayarınızı daha güvenli hale getirmenizi sağlayacaktır.

Başlarken

ESET NOD32 Antivirus aracını kullanmaya başlamadan önce, bilgisayarınızı kullanırken karşılaşabileceğiniz çeşitli tespit türleri ve uzaktan saldırılar hakkında bilgi edinebilirsiniz. Ayrıca ESET NOD32 Antivirus ürününde sunulan yeni özelliklerin bir listesini de derledik.

Önce ESET NOD32 Antivirus aracını yükleyin. Zaten ESET NOD32 Antivirus uygulamasını yüklediyseniz ESET NOD32 Antivirus ile çalışma bölümüne bakın.

ESET NOD32 Antivirus Yardım sayfalarını kullanma

Online Yardım, çeşitli bölümlere ve alt bölümlere ayrılmıştır. Halihazırda açılan pencereyle ilgili bilgileri görüntülemek için ESET NOD32 Antivirus 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 NOD32 Antivirus 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 NOD32 Antivirus 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 NOD32 Antivirus ürününü yüklemek için gereken ek dosyalar otomatik olarak indirilir.

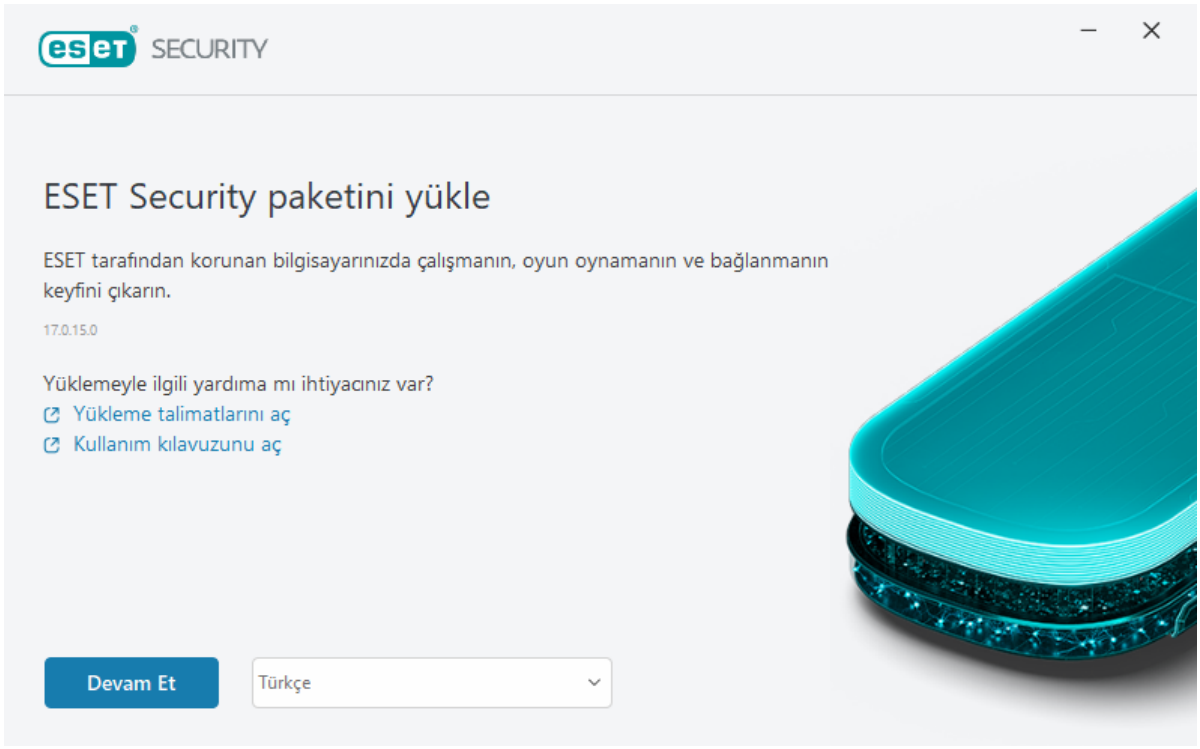
- Çevrim dışı yükleme - Live installer dosyasından daha büyük bir .exe dosyası kullanır ve yükleme işleminin tamamlanması için internet bağlantısı veya ek dosyalar gerektirmez.

ESET NOD32 Antivirus 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

Live installer yükleme paketini indirdiğinizde yükleme dosyasına çift tıklayın ve Yükleme Sihirbazı'ndaki adım adım açıklamalı 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. Önceki sürümün üzerine daha yeni bir sürümü yüklüyorsanız **etkinleştirme anahtarınız** otomatik olarak girilir.

5. Yükleme Sihirbazı, aboneliğinize bağlı olarak hangi ESET ürününün yükleneceğini 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.

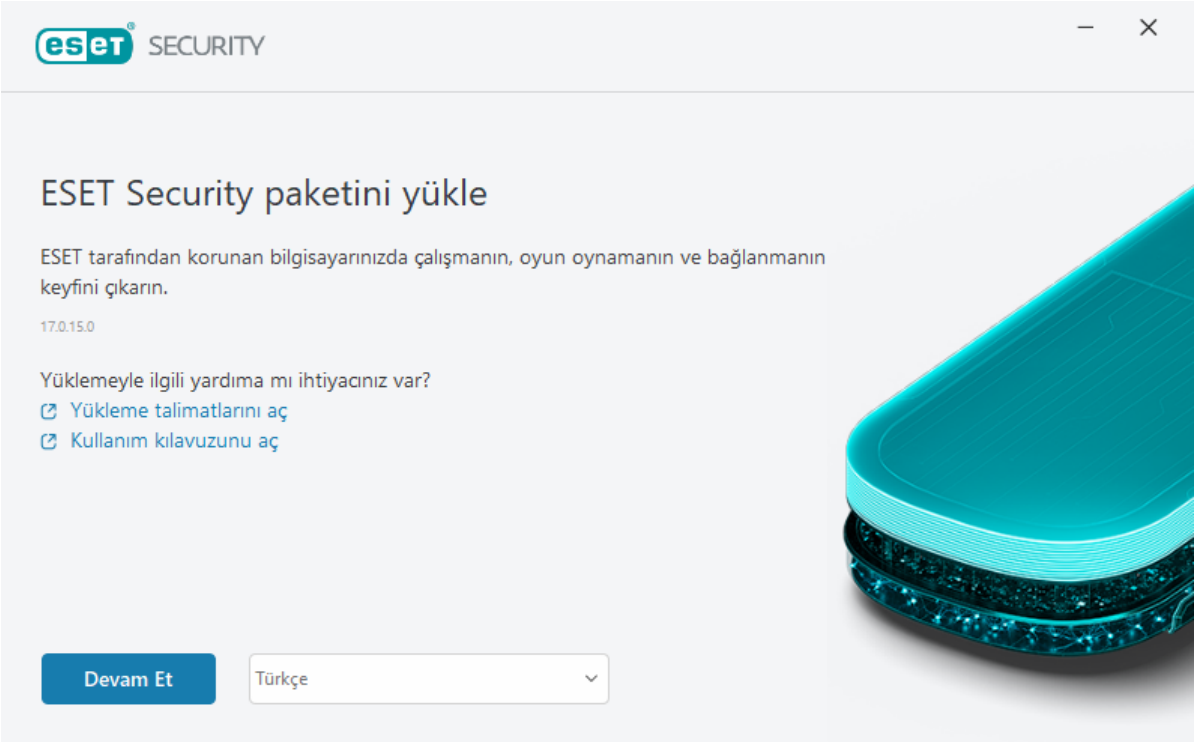
Çevrimdışı yükleme

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	ESET Security Ultimate
64 bit indir 32 bit indir ARM İndirme	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 NOD32 Antivirus 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.

Abonelik yükseltildi

Bu bildirim penceresi, ESET ürününüzü etkinleştirmek için kullanılan abonelik değiştirildiğinde görüntülenir. Değiştirilen aboneliğiniz, daha fazla güvenlik özelliğine sahip bir ürünü etkinleştirmenize olanak tanır. Hiçbir değişiklik yapılmamışsa ESET NOD32 Antivirus, 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 aboneliği hakkında daha fazla bilgi için Aboneliğe İlişkin SSS bölümüne bakın.

Aşağıdaki tabloda her spesifik üründe bulunan özelliklerin detayları verilmektedir.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
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		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Web Kamerası Koruması		✔	✔	✔
Ağ Saldırısına Karşı Koruma		✔	✔	✔
Botnet Koruması		✔	✔	✔
Güvenli Bankacılık ve Gezinme		✔	✔	✔
Tarayıcı Gizliliği ve Güvenliği		✔	✔	✔
Ebeveyn Kontrolü		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

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	ESET Security Ultimate
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		✔	✔	✔
Güvenli Bankacılık ve Gezinme		✔	✔	✔
Tarayıcı Gizliliği ve Güvenliği		✔	✔	✔
Ebeveyn Kontrolü		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Abonelik alt düzeydeki bir sürüme geçirildi

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

ESET aboneliği hakkında daha fazla bilgi için Aboneliğe İlişkin SSS bölümüne bakın.

Aşağıdaki tabloda her spesifik üründe bulunan özelliklerin detayları verilmektedir.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
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		✔	✔	✔
Güvenli Bankacılık ve Gezinme		✔	✔	✔
Tarayıcı Gizliliği ve Güvenliği		✔	✔	✔
Ebeveyn Kontrolü		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Ürünü eski sürüme düşürme

Şu anda yüklü olan ürün, etkinleştirmek üzere olduğunuz üründen daha fazla güvenlik özelliğine sahip.

Aşağıdaki tabloda her spesifik üründe bulunan özelliklerin detayları verilmektedir.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
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		✔	✔	✔
Güvenli Bankacılık ve Gezinme		✔	✔	✔
Tarayıcı Gizliliği ve Güvenliği		✔	✔	✔
Ebeveyn Kontrolü		✔	✔	✔
Anti-Theft		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

Yükleme sorun giderici

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

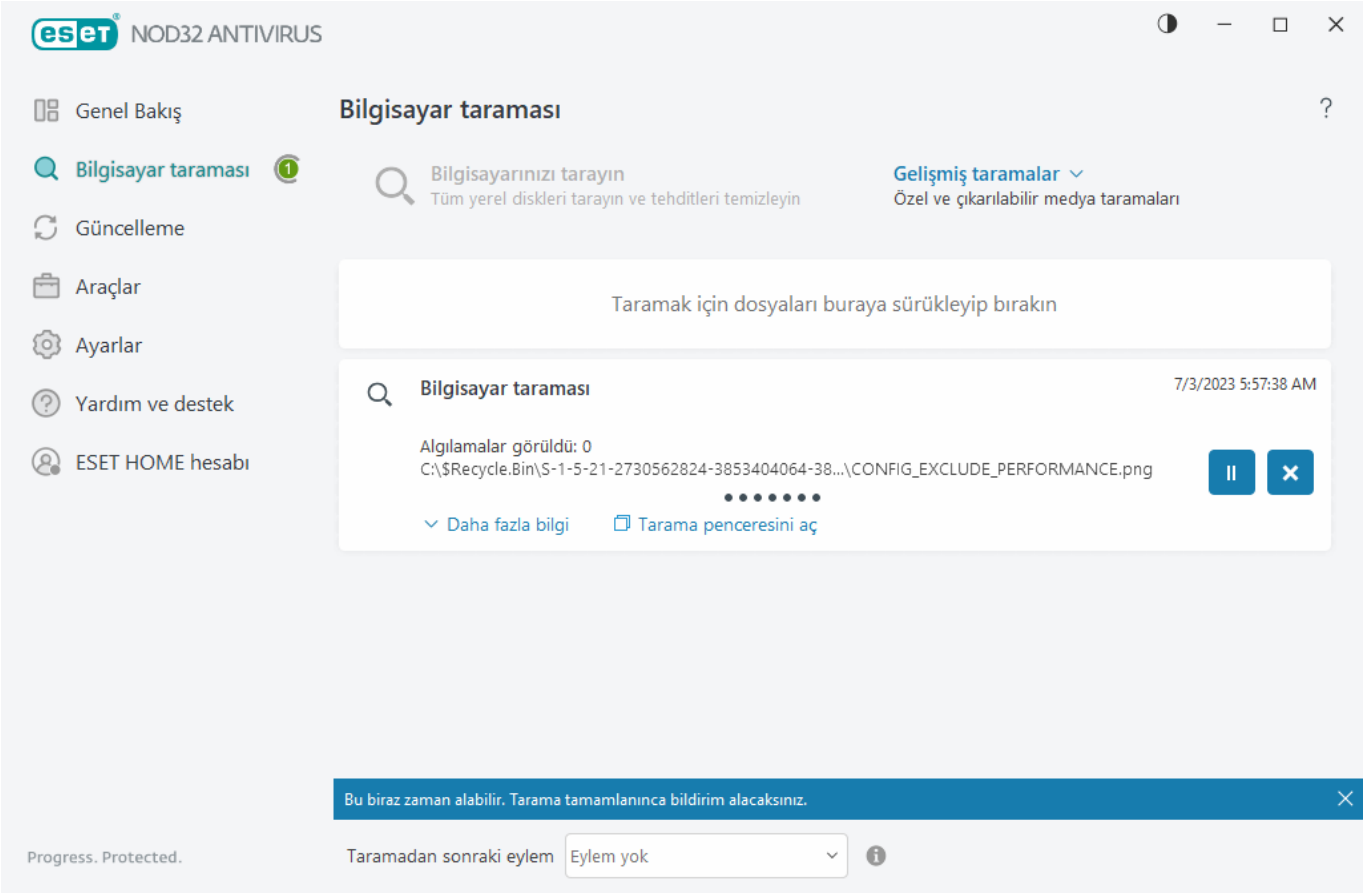
Sorun gidericiyi başlatmak için **Sorun gidericiyi çalıştır**'ı tıklayın. Sorun giderici sona erdiğinde önerilen çözümü izleyin.

Sorun devam ederse genel yükleme hataları ve çözüm listesine bakın.

Yüklemeden sonra ilk tarama

ESET NOD32 Antivirus 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 NOD32 Antivirus 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 > 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 aboneliğe 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 etkinleştirme anahtarınızla etkinleştirdikten sonra Genel Bakış sayfası görüntülenir. Abonelik bilgileriniz bulunamazsa ücretsiz deneme sürümü ile devam edin. Önceki üründe kullanılan aboneliğiniz geçerli değilse ESET ürününüzü etkinleştirin.

4. Yüklemeyi tamamlamak için cihazın yeniden başlatılması gerekir.

ESET NOD32 Antivirus yüklenecek

Şu iletişim penceresi görüntülenebilir:

- Yükleme işlemi sırasında - ESET NOD32 Antivirus ürününü yüklemek için **Devam**'ı tıklayın.
- ESET NOD32 Antivirus ürünündeki bir aboneliği değiştirme sırasında: Aboneliği değiştirmek ve ESET NOD32 Antivirus ürününü etkinleştirmek için **Etkinleştir** öğesine tıklayın.

Ürünü değiştir seçeneği, ESET aboneliğinize 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 aboneliğinize göre farklı ESET Windows ev ürünleri arasında geçiş yapabilirsiniz. Daha fazla bilgi için Benim ürünüm hangisi? bölümüne bakın.

Kayıt

Kayıt formundaki alanları tamamlayıp **Etkinleştir** seçeneğine tıklayarak aboneliğinizi kaydedin. Parantez içinde gerekli olarak işaretlenen alanlar zorunludur. Bu bilgiler yalnızca ESET aboneliğinizle 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.

Birkaç saniye içinde modül güncellemesi başlatılır. ESET NOD32 Antivirus için düzenli güncellemeler hemen başlar.

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

> Teklif ESET HOME hesabıyla ilişkilendirilmemişse etkinleştirme işlemi kesintiye uğrayabilir. ESET HOME hesabınıza giriş yapın veya hesap oluşturun.

Yeni Başlayanlara yönelik kılavuz

ESET NOD32 Antivirus ve temel ayarları hakkında genel bir ilk bakış sağlar.

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.

Gelişmiş ayarlar - ESET NOD32 AntivirusGelişmiş 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 NOD32 Antivirus Ürününü aç - ESET NOD32 Antivirus ana program penceresini açar.

Pencere düzenini sıfırla – ESET NOD32 Antivirus 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 NOD32 Antivirus günde birkaç kez otomatik olarak güncellemeleri denetler.

Hakkında - Sistem bilgilerini, ESET NOD32 Antivirus ürününün yüklü sürümüyle ilgili bilgileri ve yüklenen program modüllerinin yanı sıra işletim sistemi ile sistem kaynakları hakkındaki bilgileri de sağlar.

Klavye kısayolları

ESET NOD32 Antivirus 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 aboneliğiyle 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.

Profiller

Profil yöneticisi ESET NOD32 Antivirus ürününde iki yerde kullanılır: **İsteğe bağlı tarama** bölümünde ve **Güncelleme** bölümünde.

Bilgisayar taraması

ESET NOD32 Antivirus 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 > **Tespit altyapısı** > **Zararlı yazılım taramaları** > **İsteğe bağlı tarama** > **Profil listesi** > **Düzenle**'yi açın. **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 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.

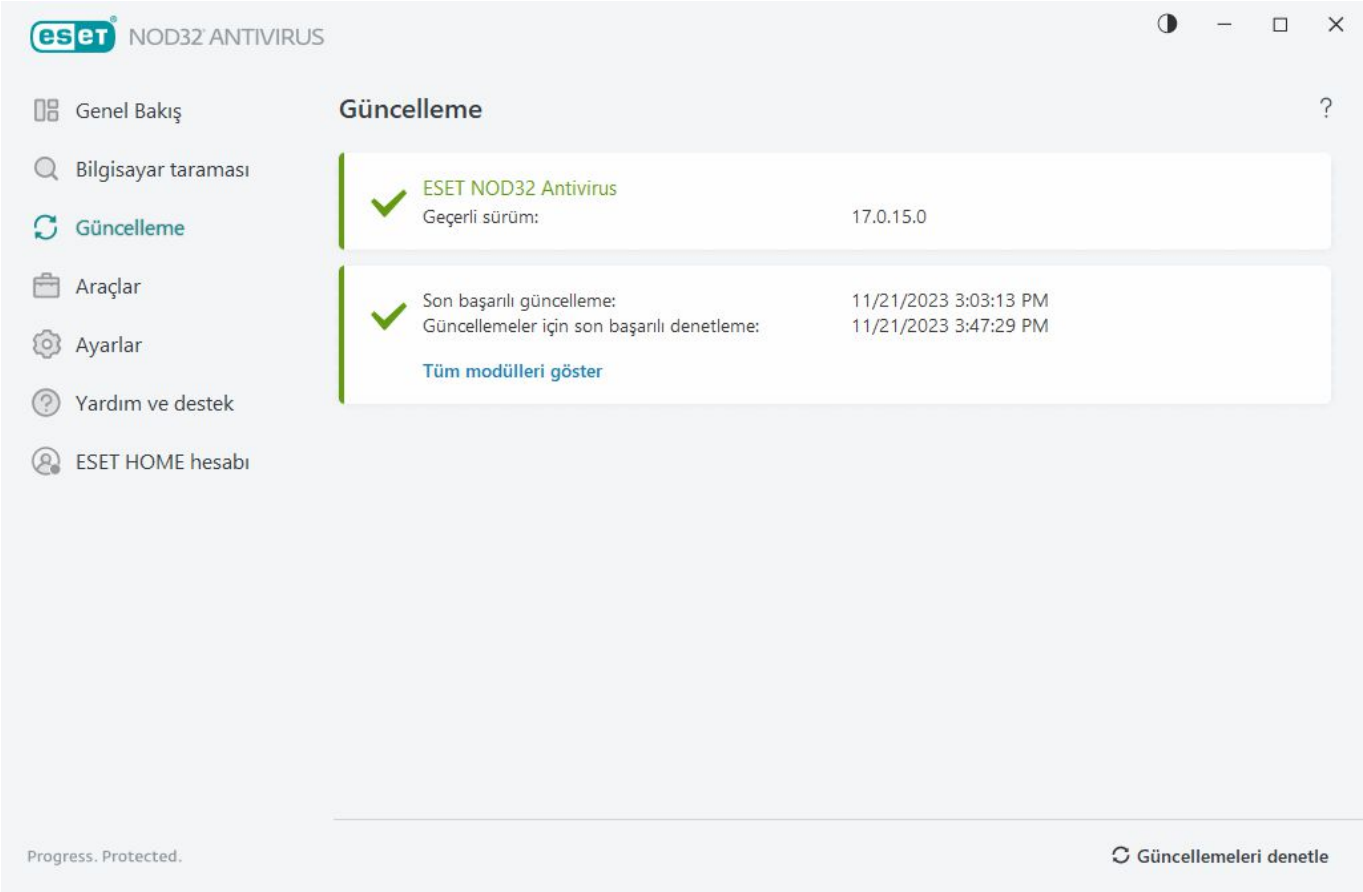
Güncellemeler

ESET NOD32 Antivirus 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

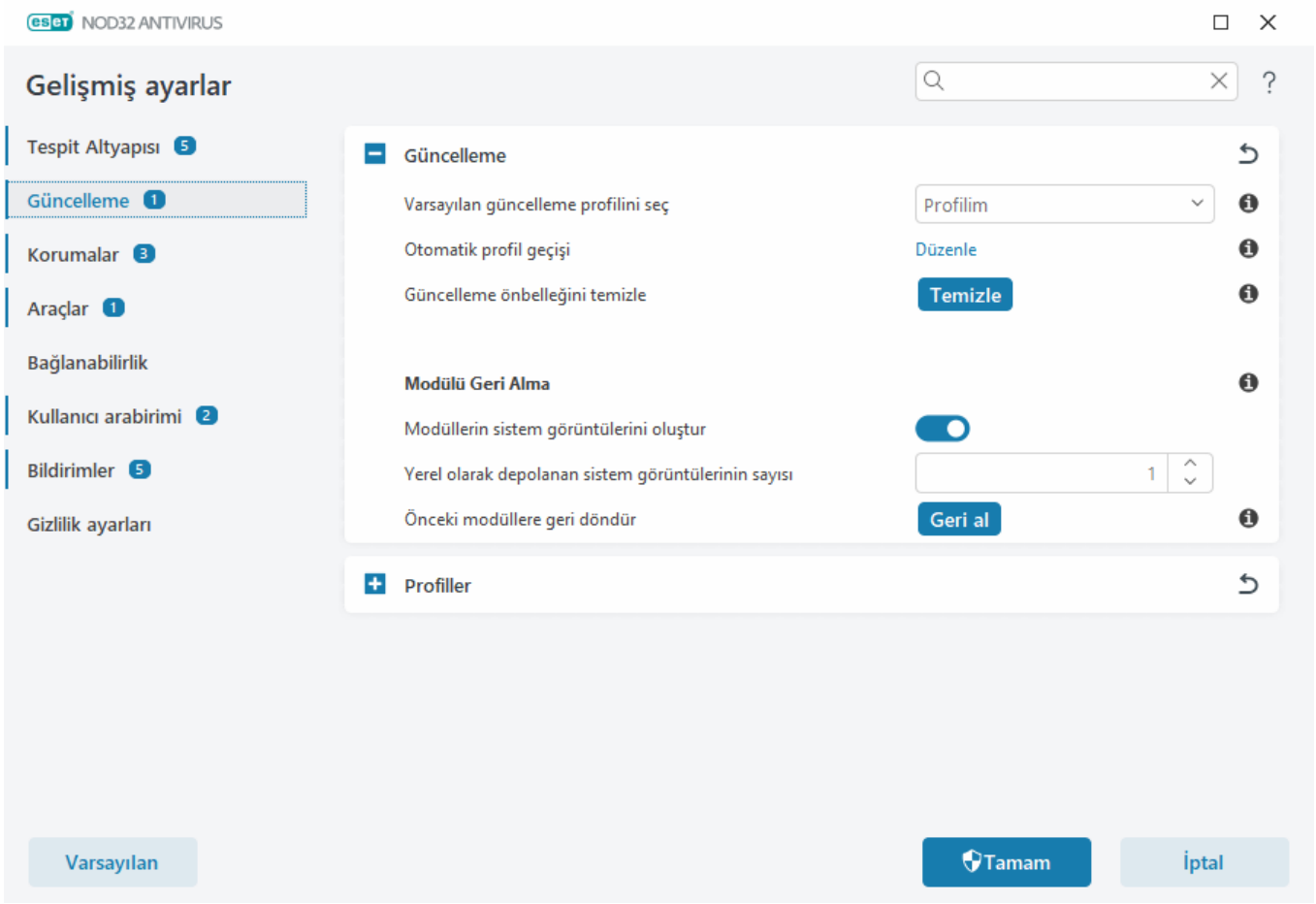
gerekip gerekmediği de dahil olmak üzere geçerli güncelleme durumunu görüntüleyebilirsiniz.

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



Gelişmiş ayarlar > **Güncelleme** güncelleme modu, proxy sunucu erişimi ve LAN bağlantıları gibi ek güncelleme seçenekleri içerir.

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.



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 abonelik bilgilerini içeren bir e-posta aldıysanız **Satın alınmış bir etkinleştirme anahtarını kullanın**'a tıklayarak ürününüzü etkinleştirin. Etkinleştirmenin başarılı olabilmesi için etkinleştirme anahtarı sağlandığı şekilde girilmelidir. Etkinleştirme anahtarı, abonelik sahibinin tanımlanması ve aboneliğin etkinleştirilmesi için kullanılan XXXX-XXXX-XXXX-XXXX-XXXX veya XXXX-XXXXXXXX biçimindeki benzersiz bir dizidir. Etkinleştirme anahtarı genellikle ürün paketinin içinde veya arka tarafında bulunur.

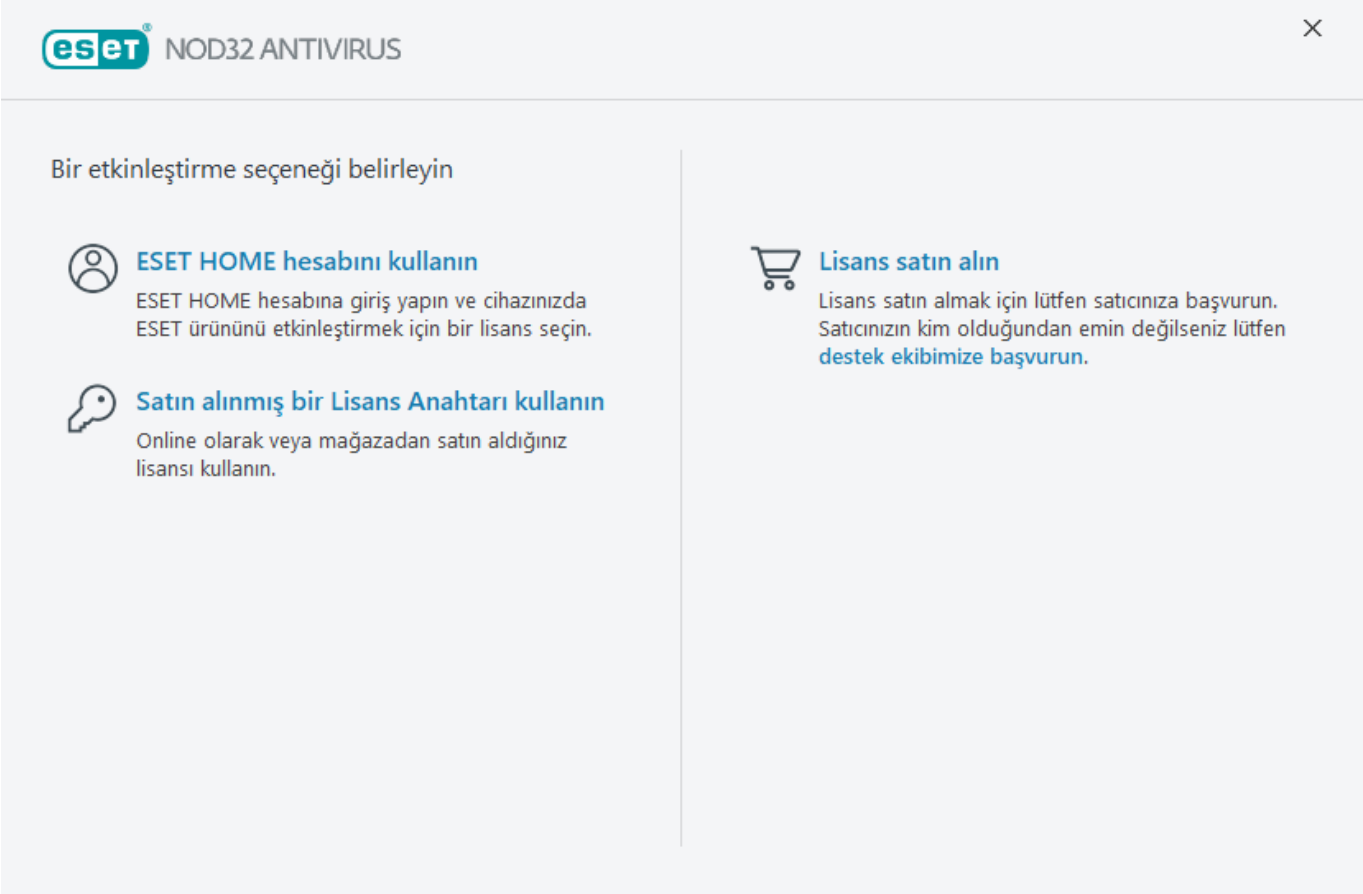
- ESET HOME Hesabını kullan'ı seçtikten sonra ESET HOME hesabınıza giriş yapmanız istenir.

- Satın alma işlemini gerçekleştirmeden önce ESET NOD32 Antivirus ürününü değerlendirmek istiyorsanız Ücretsiz deneme sürümü seçeneğini belirleyin. ESET NOD32 Antivirus Ürününü sınırlı bir süre için etkinleştirmek üzere e-posta adresinizi ve ülkenizi girin. Ücretsiz deneme sürümünüz size e-posta ile gönderilecektir. Ücretsiz deneme sürümü her müşteri için yalnızca bir kez etkinleştirilebilir.

- Aboneliğiniz yoksa ve satın almak istiyorsanız **Abonelik satın alın** öğesine tıklayın. Bu, sizi yerel ESET dağıtımcısının web sitesine yönlendirir. ESET Windows ev ürünü abonelikleri ücretsiz değildir.

Ürün aboneliğinizi dilediğiniz zaman değiştirebilirsiniz. Bunun için ana program penceresinde **Yardım ve destek** > **Aboneliği değiştir** öğesine tıklayın. Aboneliğinizi ESET Destek bölümüne tanıtmak için kullanılan genel kimliğinizi görürsünüz.

Ürün etkinleştirme işlemi başarısız mı oldu?



Etkinleştirme sırasında etkinleştirme anahtarını girme

Otomatik güncellemeler, güvenliğiniz için önemlidir. ESET NOD32 Antivirus yalnızca etkinleştirildikten sonra güncellemeleri alır.

Etkinleştirme anahtarınızı girerken tam olarak yazıldığı gibi girmeniz önemlidir. Etkinleştirme anahtarınız, abonelik sahibinin tanımlanması ve aboneliğin etkinleştirilmesi için kullanılan XXXX-XXXX-XXXX-XXXX-XXXX biçiminde benzersiz bir dizidir.

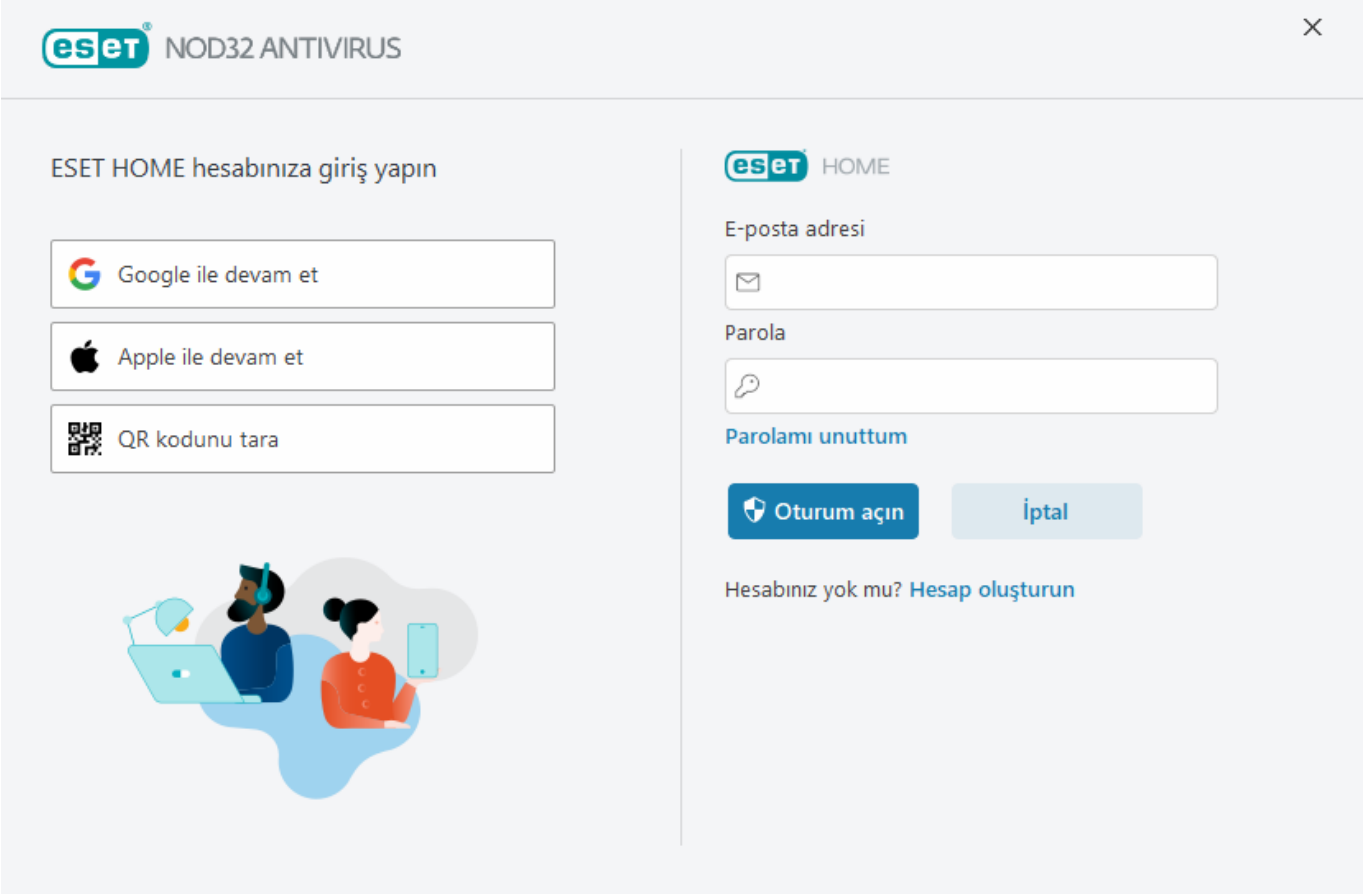
Doğruluğunu garantilemek adına etkinleştirme anahtarınızı kayıt e-postanızdan kopyalayıp yapıştırmanızı öneririz.

Yüklemenin ardından etkinleştirme anahtarınızı girmediyseniz ürününüz etkinleştirilmez. Ana program penceresinde **Yardım ve Destek** > **Aboneliği etkinleştir** seçeneğini kullanarak ESET NOD32 Antivirus ürününü etkinleştirebilirsiniz.

ESET Windows ev ürünü abonelikleri ücretsiz değildir.

ESET HOME hesabını kullanma

Etkinleştirilen tüm ESET aboneliklerinizi ve cihazlarınızı görüntüleyip yönetmek için cihazınızı ESET HOME portalına bağlayın. Aboneliğinizi yenileyebilir, yükseltebilir veya uzatabilir ve önemli abonelik ayrıntılarını görüntüleyebilirsiniz. ESET HOME yönetim portalında veya mobil uygulamada farklı abonelikler ekleyebilir, ürünleri cihazlarınıza indirebilir, ürün güvenlik durumunu kontrol edebilir ya da e-posta üzerinden abonelikleri 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 abonelik seçin veya yeni bir abonelik ekleyin. ESET NOD32 Antivirus ürününü etkinleştirmek için **Devam'ı** tıklayın.

Ücretsiz Deneme Sürümünü Etkinleştir

ESET NOD32 Antivirus Deneme sürümünüzü etkinleştirmek için **E-posta adresi** ve **E-posta adresini onaylayın** alanına geçerli bir e-posta adresi girin. Etkinleştirmeden sonra ESET aboneliğiniz 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. Ücretsiz deneme sürümü yalnızca bir kez etkinleştirilebilir.

ESET NOD32 Antivirus ürününü, teknik destek sağlayacak olan yerel dağıtımcınıza kaydettirmek için **Ülke** açılır menüsünden ülkenizi seçin.

Ücretsiz ESET etkinleştirme anahtarı

ESET NOD32 Antivirus ürünü için abonelik ücretsiz değildir.

ESET etkinleştirme anahtarı, ESET NOD32 Antivirus ürününün Son Kullanıcı Lisans Sözleşmesi gereğince yasal olarak kullanılmasına izin vermek için ESET tarafından sağlanan, kısa çizgiyle ayrılan harf ve rakamlardan oluşan benzersiz bir dizidir. Her Son Kullanıcı, etkinleştirme anahtarını ESET tarafından verilen lisans sayısına göre ESET NOD32 Antivirus ürününü kullanma hakkının kapsamıyla sınırlı olacak şekilde kullanabilecektir. Etkinleştirme anahtarı gizli kabul edilir ve paylaşılamaz ancak ESET HOME portalını kullanarak bir abonelik paylaşabilirsiniz.

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

- Bir "Ücretsiz ESET aboneliği" reklamına 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 aboneliği devre dışı bırakabilir ve bırakır.
- Korsan bir etkinleştirme anahtarına sahip olmak, ESET NOD32 Antivirus ürününü yüklemek için kabul etmeniz gereken Son Kullanıcı Lisans Sözleşmesi'ne uygun değildir.
- ESET aboneliğini yalnızca www.eset.com, ESET dağıtıcıları veya satıcıları gibi resmi kanallardan satın alın (eBay gibi resmi olmayan üçüncü taraf web sitelerinden lisans satın almayın veya üçüncü taraflara ait ortak lisansları kullanmayın).
- ESET NOD32 Antivirus ürünü ücretsiz olarak indirilir ancak yükleme sırasında etkinleştirme işlemi, geçerli bir ESET etkinleştirme anahtarı gerektirir. Ürünü indirip yükleyebilirsiniz ancak etkinleştirmeden kullanamazsınız.
- Aboneliğinizi internette veya sosyal medyada paylaşmayın çünkü yayılabilir.

Korsan ESET aboneliği tespit edip bildirmek için talimatları uygulamak üzere Bilgi Bankası makalemizi ziyaret edin.

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

1. ESET NOD32 Antivirus ürününü ücretsiz deneme sürümüyle etkinleştirin
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 NOD32 Antivirus ürününün etkinleştirilmesi başarılı olmadıysa en yaygın nedenler şu şekildedir:

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

Doğru etkinleştirme anahtarını girdiğinizi ve internet bağlantınızın etkin olduğunu doğrulayın. ESET NOD32 Antivirus ürününü yeniden etkinleştirmeyi deneyin. Etkinleştirme için ESET HOME hesabı kullanıyorsanız ESET HOME Aboneliği ve abonelik yönetimi - Çevrimiçi Yardım bölümüne bakın.

Belirli bir hata alırsanız (örneğin, askıya alınan abonelik veya aşırı kullanılmış abonelik) abonelik durumu bölümündeki 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).

Abonelik durumu

Aboneliğinizde farklı durumlar bulunabilir. Abonelik durumunuzu ESET HOME üzerinde bulabilirsiniz. Aboneliğinizi ESET HOME hesabınıza eklemek için Abonelik ekleme bölümüne bakın.

ESET HOME hesabınız yoksa Yeni bir ESET HOME hesabı oluşturabilirsiniz.

Abonelik durumu **Etkin** haricindeki bir durumsa etkinleştirme sırasında bir hata veya ana program penceresinde bir bildirim alırsınız.

Abonelik durumu bildirimlerini devre dışı bırakmak için Gelişmiş ayarlar > **Bildirimler** > **Uygulama durumları** öğesini 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 abonelik durumları için açıklamaları ve önerilen çözümleri aşağıdaki tabloda görebilirsiniz:

Abonelik durumu	Açıklama	Çözüm
Etkin	Abonelik geçerli. Herhangi bir etkileşimde bulunmanıza gerek yok. ESET NOD32 Antivirus etkinleştirilebilir ve abonelik ayrıntılarını ana program penceresi > **Yardım ve destek** bölümünde bulabilirsiniz.	
Aşırı kullanıldı	Bu aboneliği izin verilenden daha fazla cihaz kullanıyor. Bir etkinleştirme hatası alırsınız.	Daha fazla bilgi için Aşırı kullanılmış abonelik nedeniyle etkinleştirme gerçekleştirilemedi bölümüne bakın.

Abonelik durumu	Açıklama	Çözüm
Askıya alındı	Aboneliğiniz ödeme sorunları nedeniyle askıya alındı. Aboneliği kullanmak için ESET HOME portalındaki ödeme bilgilerinizin güncel olduğundan emin olun veya abonelik satıcınızla iletişime geçin. Bu hatayı etkinleştirme sırasında veya ana program penceresinden alabilirsiniz.	Yüklenen ürün: ESET HOME hesabınız varsa ana program penceresinde gösterilen bildirimde **Aboneliğinizi ESET HOME portalından yönetin** öğesine tıklayın ve ödeme ayrıntılarınızı gözden geçirin. Aksi takdirde, abonelik satıcınızla iletişime geçin. Etkinleştirme hatası - ESET HOME hesabınız varsa etkinleştirme hatası penceresinde **ESET HOME portalını aç**'ı tıklayın ve ödeme bilgilerinizi gözden geçirin. Aksi takdirde, abonelik satıcınızla iletişime geçin.
Sona erdi	Aboneliğinizin süresi doldu ve ESET NOD32 Antivirus ürününü etkinleştirmek için bu aboneliği kullanamazsınız. Bu hatayı etkinleştirme sırasında veya ana program penceresinden alabilirsiniz. ESET NOD32 Antivirus ürününü zaten yüklediyseniz bilgisayarınız korunmuyor ve güncellenmiyor.	Yüklenmiş ürün: Ana program penceresinde görüntülenen bildirimde, **Aboneliği yenile** öğesine tıklayın ve Aboneliğimi nasıl yenilerim? bölümündeki talimatları uygulayın veya **Ürünü etkinleştir** seçeneğine tıklayın ve etkinleştirme yönteminizi seçin. Etkinleştirme hatası: Etkinleştirme hatası penceresinde **Aboneliğinizi yenileyin** öğesine tıklayın ve Aboneliğimi nasıl yenilerim? bölümündeki talimatları uygulayın veya yeni ya da yenilenmiş bir etkinleştirme anahtarı yazıp **Aboneliği yenile** seçeneğine tıklayın.
İptal edildi	Aboneliğiniz ESET veya abonelik satıcınız tarafından iptal edildi.	Bir hata alırsanız: Ana program penceresinde veya etkinleştirme sırasında aboneliğinizin iptal edildiğini görüyorsanız ve aboneliğinizin düzgün çalışması gerekiyorsa abonelik satıcınızla iletişime geçin.

Aşırı kullanılmış abonelik nedeniyle etkinleştirme gerçekleştirilemedi

Sorun

- Aboneliğiniz aşırı kullanılmış veya kötüye kullanılmış olabilir
- Aşırı kullanılmış abonelik nedeniyle etkinleştirme gerçekleştirilemedi

Çözüm

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

Abonelik sahibiyseniz ve e-posta adresinizi girmeniz istenmemişse:

1. ESET aboneliğinizi 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 Abonelik aşırı kullanıldığında ne olur? bölümüne bakın.

2. Korsan ESET aboneliğini tespit edip bildirmek için talimatları uygulamak üzere Korsan ESET aboneliğini tespit etme ve bildirme makalemizi ziyaret edin.

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

Abonelik sahibi değilseniz bu aboneliğin sahibiyle, aboneliğin 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 NOD32 Antivirus ürününüzü satın almak veya etkinleştirmek için kullandığınız e-posta adresini girin.

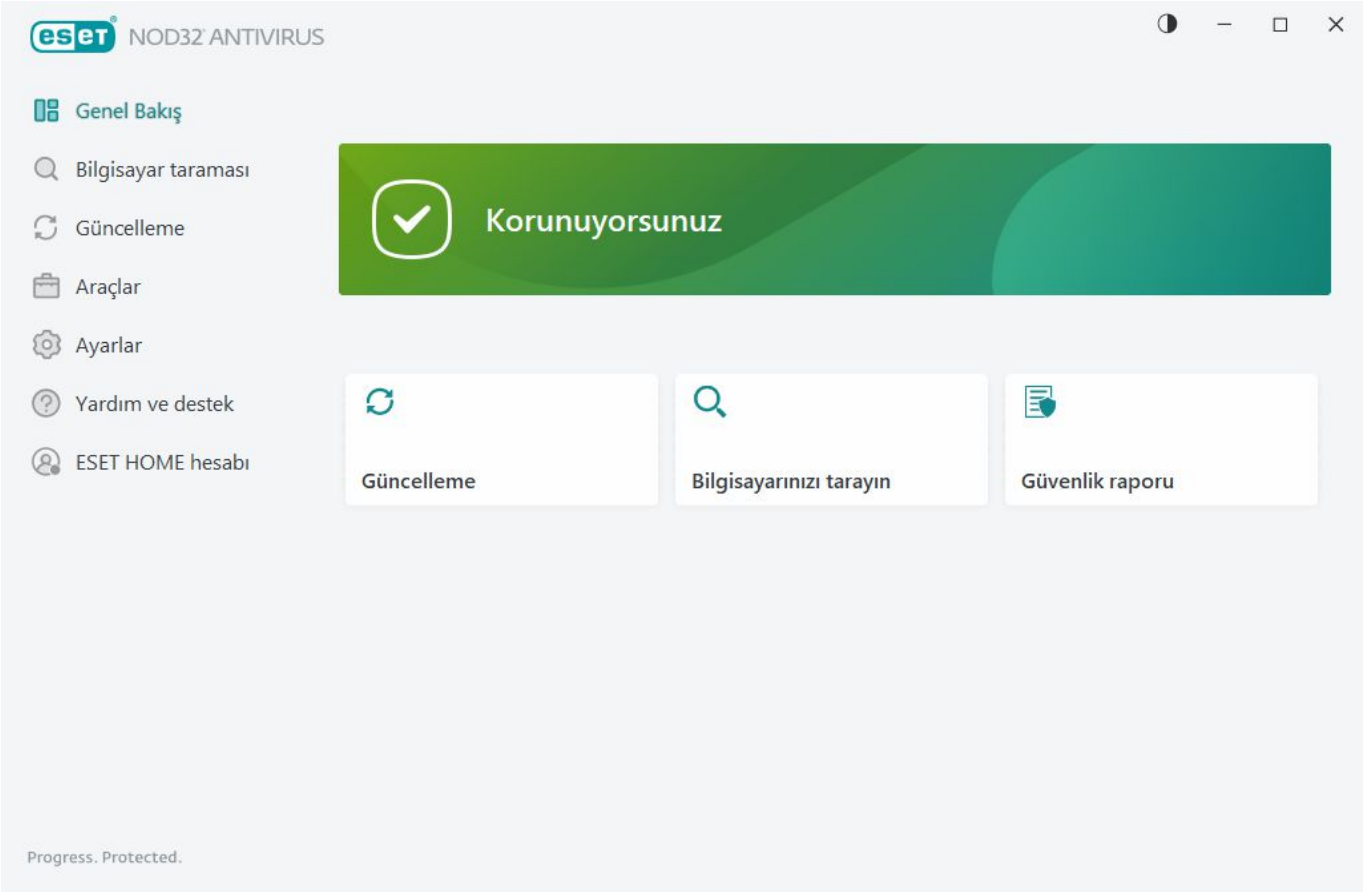
ESET NOD32 Antivirus ile çalışma

ESET NOD32 Antivirus 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 program penceresinin sağ üst köşesinden ESET NOD32 Antivirus GUI için renk düzenini seçebilirsiniz. **Simge durumuna küçült** simgesinin yanındaki **Renk şeması** simgesini tıklayın (simge seçili renk düzenine göre değişir) ve açılır menüden renk düzenini seçin:

- **Sistem rengiyle aynı** - İşletim sistemi ayarlarınıza göre ESET NOD32 Antivirus renk düzenini ayarlar.
- **Koyu mod** - ESET NOD32 Antivirus koyu renk düzeni (koyu mod) sahip olur.
- **Açık** - ESET NOD32 Antivirus standart, açık renk düzenine sahip olur.



Ana menü seçenekleri:

Genel bakış – ESET NOD32 Antivirus 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 - özelliklere erişim sağlar.

Ayarlar - ESET NOD32 Antivirus koruma özellikleri için yapılandırma seçenekleri (Bilgisayar koruması ve İnternet koruması) ve Gelişmiş ayarlara erişim sunar.

Yardım ve destek: Aboneliğiniz ve yüklenmiş ESET ürünüyle ilgili bilgilerin yanı sıra Çevrimiçi Yardım, ESET Bilgi Bankası ve Teknik Destek ile ilgili bağlantıları gösterir.

ESET HOME hesabı - Cihazınızı ESET HOME portalına bağlayın veya ESET HOME hesabının bağlantı durumunu inceleyin. ESET HOME Kullanarak etkin ESET aboneliği ile cihazlarını görüntüleyip yönetebilirsiniz.

Genel Bakış

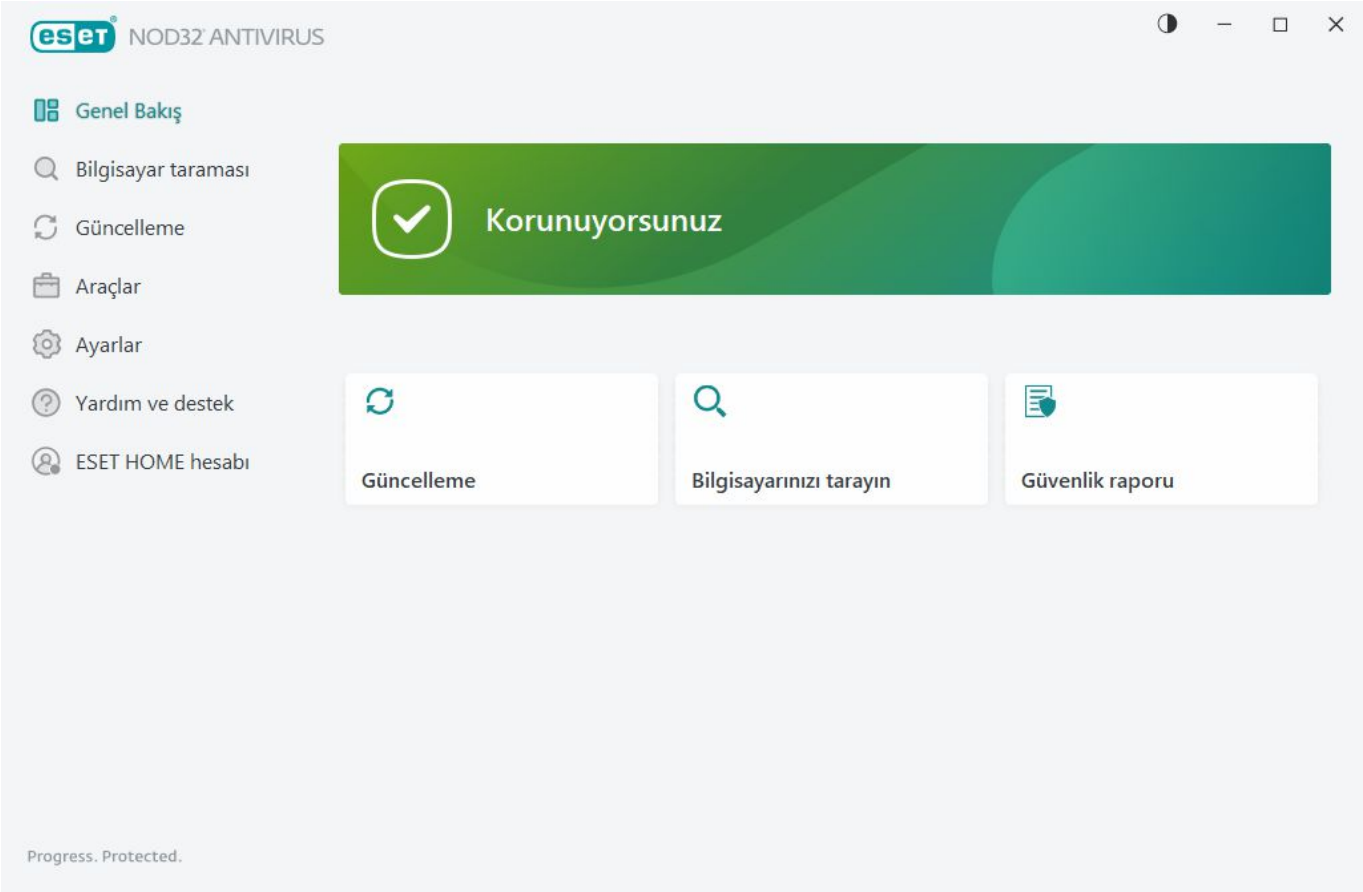
Genel Bakış penceresi, bilgisayarınızın mevcut korumasıyla ilgili bilgilerin yanı sıra ESET NOD32 Antivirus ürünündeki güvenlik özelliklerine hızlı bağlantıları gösterir.

Genel Bakış penceresinde, ESET NOD32 Antivirus 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.

Güncelleme - Güncelleme sayfasını açar ve güncellemeleri denetler.

Bilgisayarınızı tarayın - Bilgisayar taraması sayfasını açar ve standart bir bilgisayar taraması başlatır.

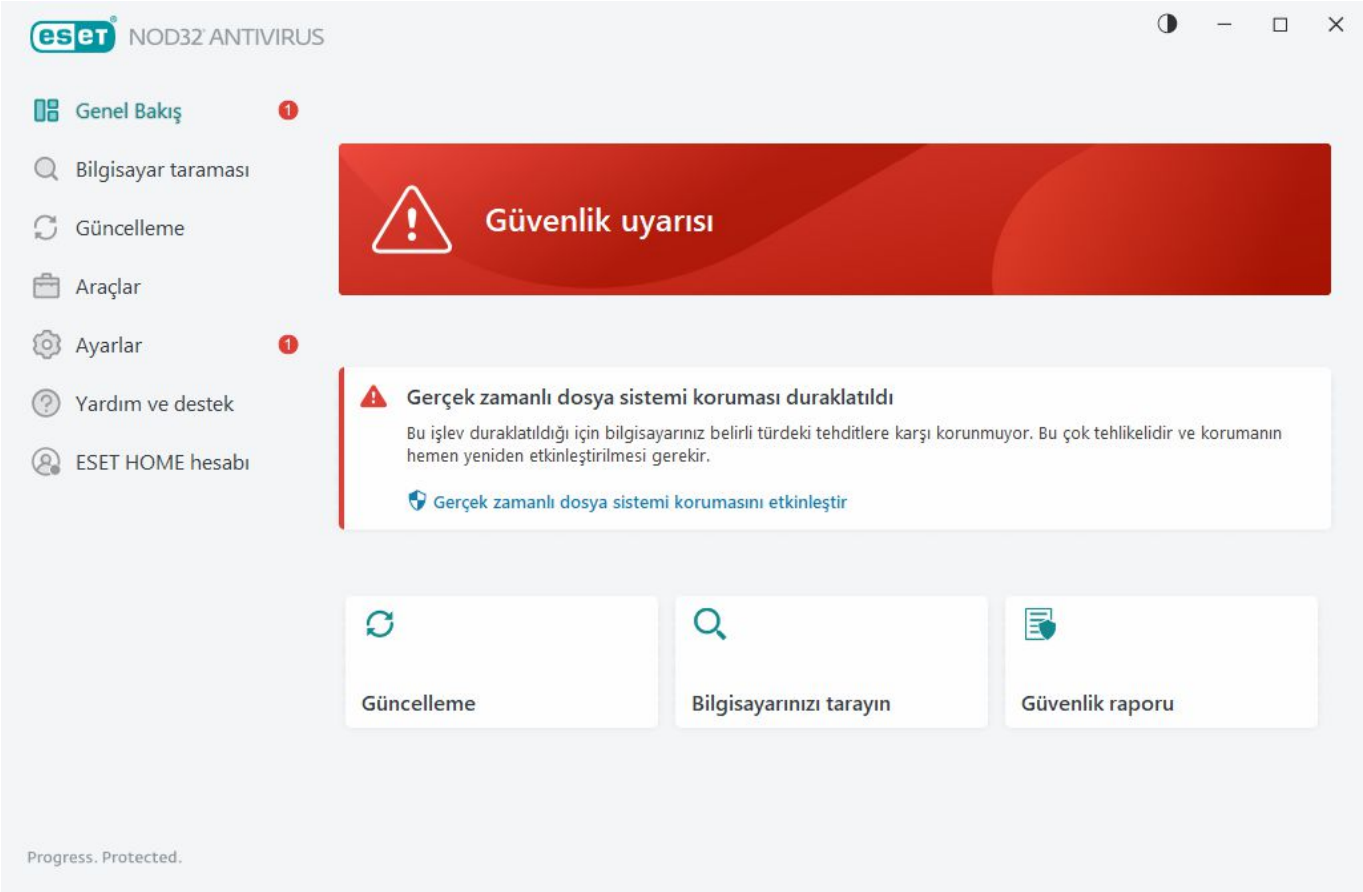
Güvenlik raporu - Güvenlik raporunu açar.



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 **Aboneliğin süresi doldu**: Bu durum, kırmızı koruma durumu simgesiyle belirtilir. Aboneliğinizin süresi dolduktan sonra program güncellenemez. Aboneliğinizi 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.

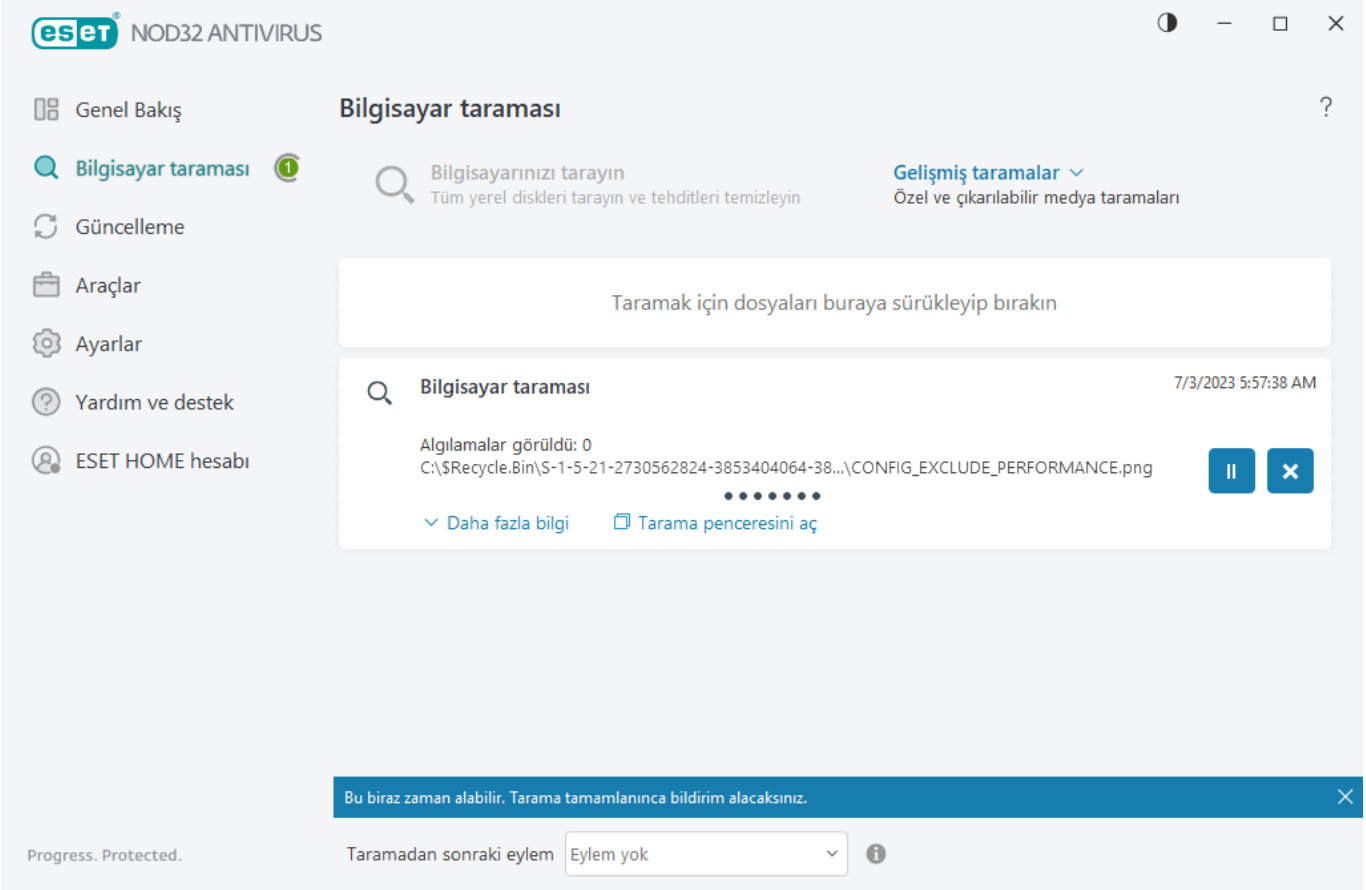
Turuncu simge sınırlı koruma anlamına gelir. Örneğin, program güncellenirken bir sorun oluşmuştur veya aboneliğinizin süresi yakında dolacaktır.
Bu durumun görüntülenmesinin birkaç nedeni olabilir, örneğin:

- **Oyun modu etkin** – Oyun modunun etkinleştirilmesi olası bir güvenlik riskidir. Bu özellik etkinleştirildiğinde tüm bildirim/uyarı pencereleri devre dışı kalır ve zamanlanan tüm görevler durur.
- **Aboneliğinizin süresi yakında doluyor/Aboneliğinizin süresi bugün sona eriyor**: Bu durum koruma durumu simgesinin, sistem saatinin yanında bir ünlem işareti görüntülemesiyle belirtilir. Aboneliğinizin 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.

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 NOD32 Antivirus 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** > **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 > **Tespit altyapısı** > **Zararlı yazılım taramaları** > **İsteğe bağlı tarama** > ThreatSense bölümünde açıklanmaktadır.

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

• **İşletim belleği** - İşletim belleği tarafından halihazırda kullanılan tüm işlemleri ve verileri tarar.

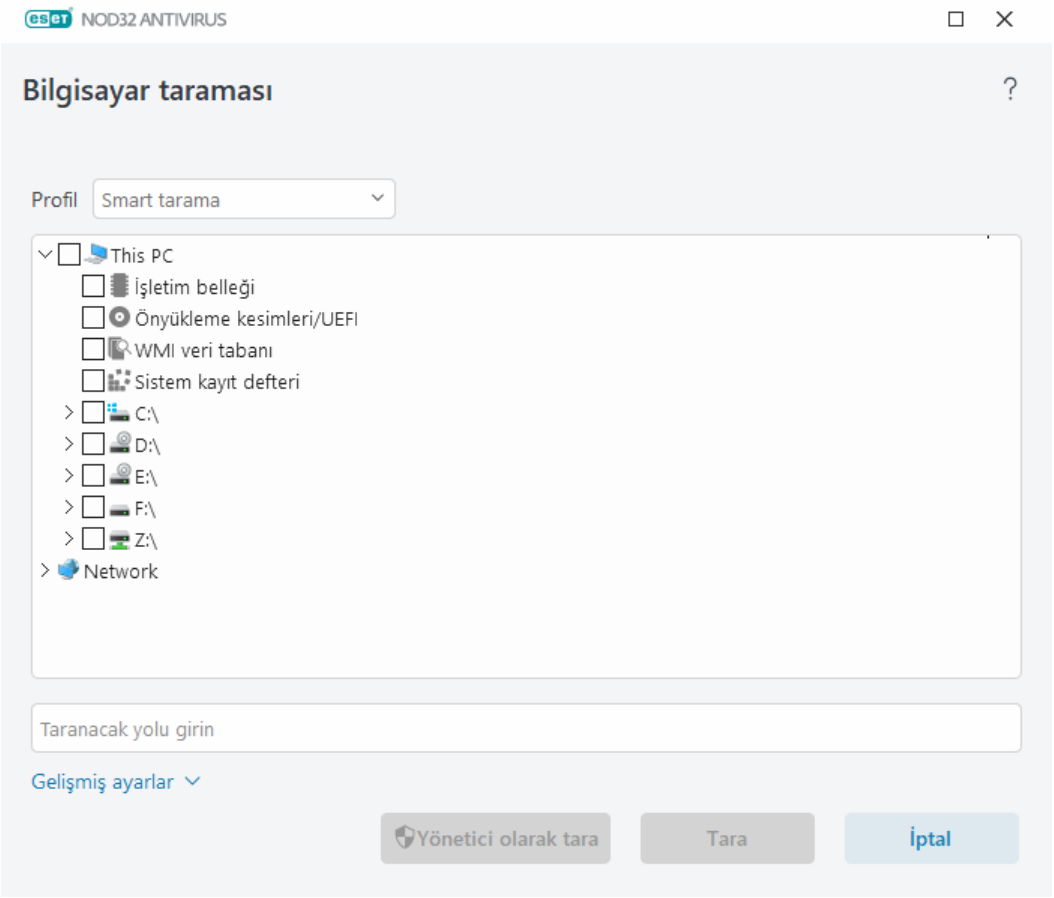
• **Önyükleme kesimleri/UEFI** - Önyükleme kesimlerini ve UEFI'yi zararlı yazılımlara karşı tarar. UEFI tarayıcı ile ilgili daha fazla bilgi için sözlükten yararlanın.

• **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 bölümüne bakın.



Gelişmiş ayarlar > **Tespit altyapısı** > **Zararlı yazılım taramaları** > **İsteğe bağlı tarama** > **ThreatSense** > **Temizleme** altında tarama için temizleme parametrelerini yapılandırabilirsiniz. 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.

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. Bilgi Bankası makalemizde daha fazla ayrıntı bulabilirsiniz.

Haftalık bir bilgisayar taraması zamanlama

Normal bir görev zamanlamak için Haftalık bilgisayar taraması planlama bölümüne bakın.

Tarama ilerleme durumu - İlerleme çubuğu, çalışan taramanın durumunu gösterir.

Hedef – Taranmakta olan nesnenin ve konumunun adı.

Bulunan tespitler - Taranan dosyaların, bulunan tehditlerin ve tarama sırasında temizlenen tehditlerin toplam sayısını gösterir.

Aşağıdaki bilgileri görüntülemek için Daha fazla bilgi'yi tıklayın:

- **Kullanıcı** - Taramayı başlatan kullanıcı hesabının adı.
- **Taranan nesneler** - Halihazırda taranmış nesnelerin sayısı.
- **Süre** - Geçen süre.

Duraklat simgesi - Bir taramayı duraklatır.

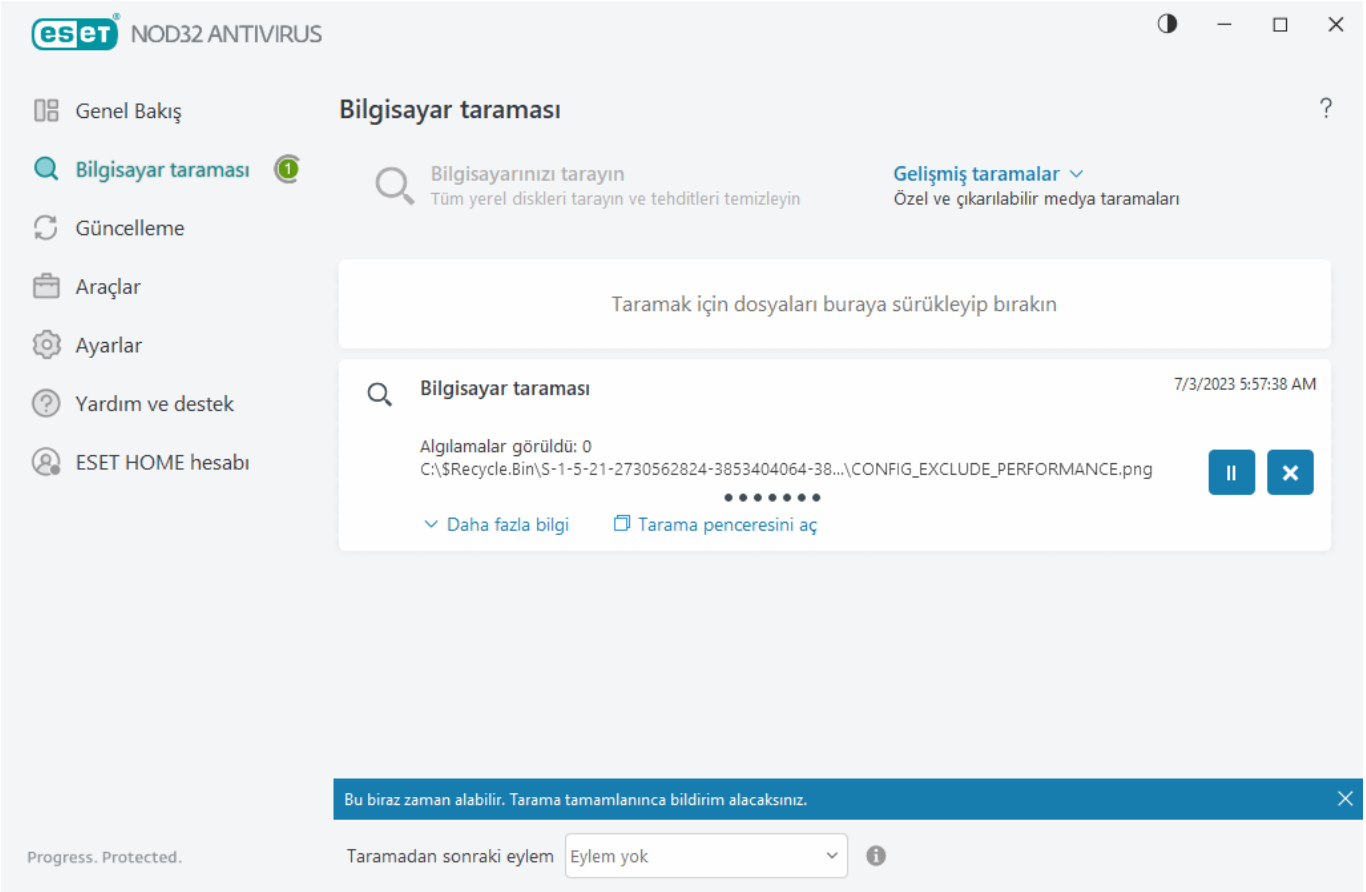
Sürdür simgesi – Tarama ilerlemesi duraklatıldığında bu seçenek görünür. Taramaya devam etmek için simgeyi tıklayın.

Durdur simgesi - Taramayı sonlandırır.

Tarama hakkında daha fazla ayrıntı içeren Bilgisayar taraması günlüğünü açmak için **Tarama penceresini aç**'ı tıklayın.

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).

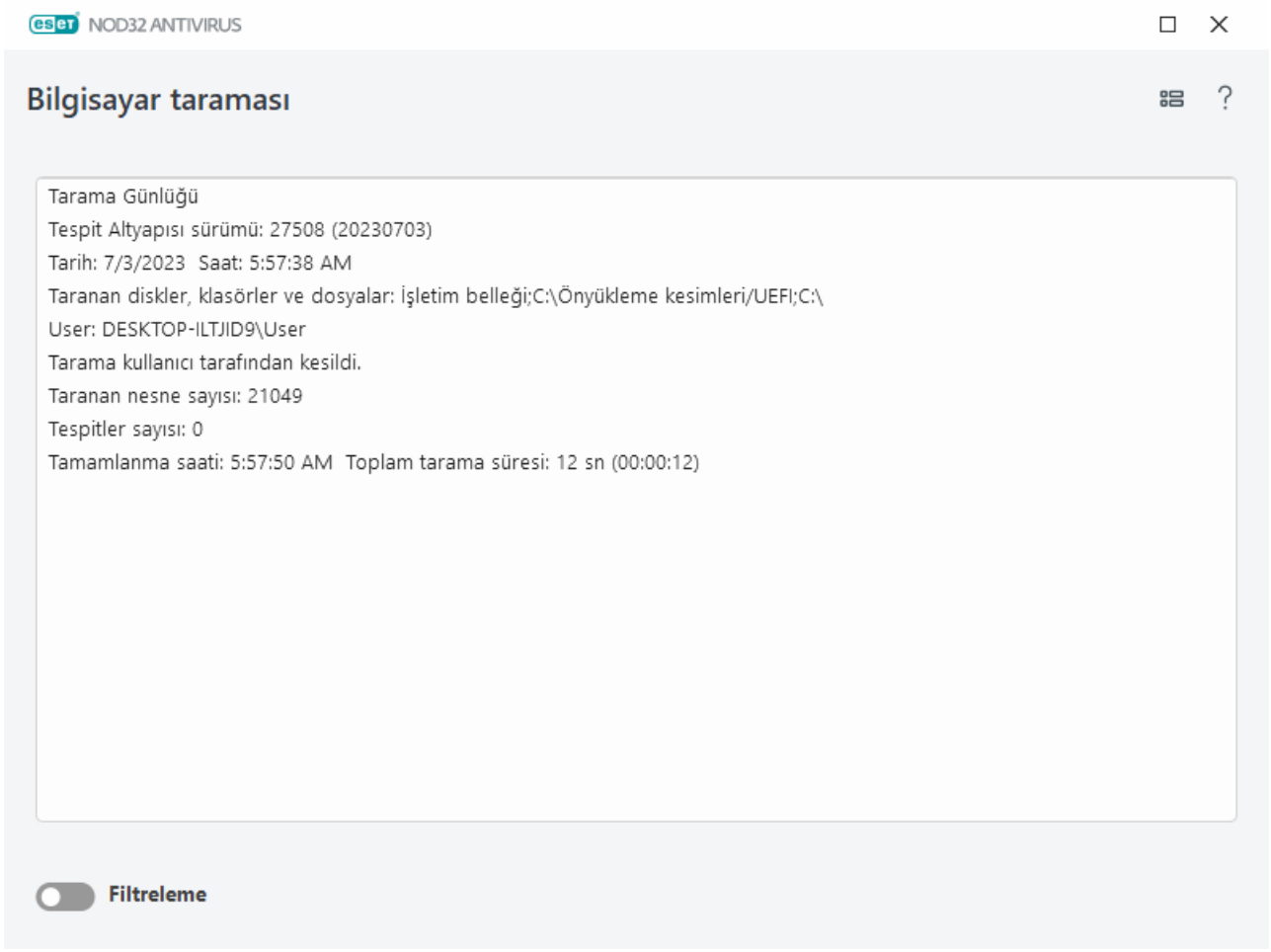
Bilgisayar tarama günlüğü

Belirli bir taramayla ilgili ayrıntılı bilgileri Günlük dosyaları'nda görüntüleyebilirsiniz. Tarama günlüğü aşağıdaki bilgileri içerir:

- Algılama altyapısı sürümü
- Başlama tarihi ve saati
- Taranan diskler, klasörler ve dosyalar
- Zamanlanan tarama adı (yalnızca zamanlanan tarama)
- Taramayı başlatan kullanıcı.
- 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** > **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.

Aramanızı daraltmak için özel kriterler tanımlayabileceğiniz Günlük filtreleme penceresini açmak için **Filtreleme** açma/kapama düğmesini tıklayın. Bu pencerede aramanızı özel kriterlere göre daraltabilirsiniz. İçerik menüsünü görmek için belirli bir günlük girişini sağ tıklayın:

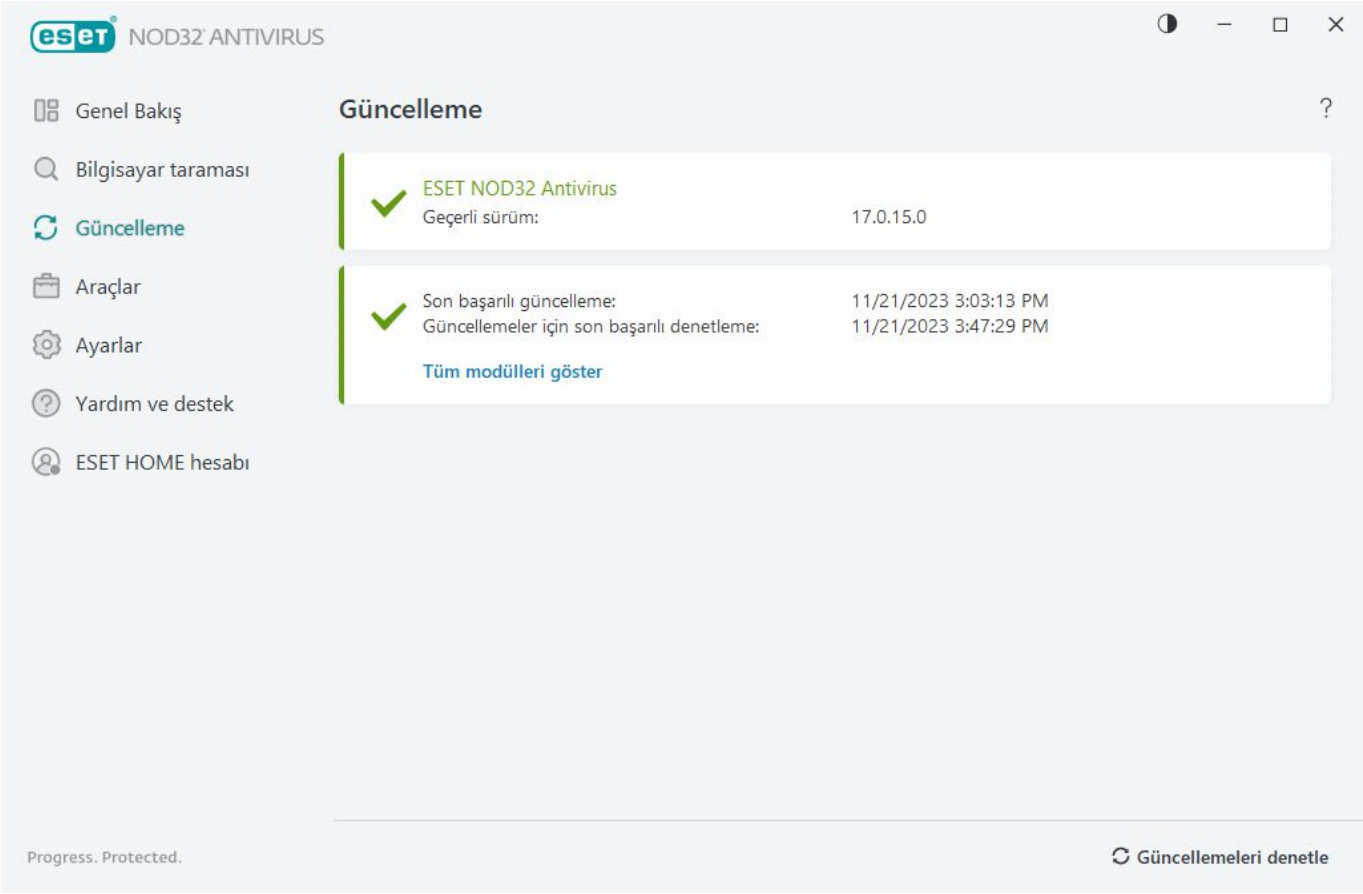
Eylem	Kullanım
Aynı kayıtları filtrele	Günlük filtreleme özelliğini etkinleştirir. Günlük, yalnızca seçilenle aynı türdeki kayıtları gösterir.
Filtrele...	Bu seçenek, Günlük filtreleme penceresini açar ve belirli günlük girişleri için kriterleri tanımlamanıza olanak tanır. Kısayol: `Ctrl+Shift+F`
Filtreyi 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`
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.

Güncelleme

ESET NOD32 Antivirus 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 etkinleştirme anahtarınızı kullanarak ürününüzü etkinleştirmeniz gerekir. Kurulum esnasında bunu yapmadıysanız ESET güncelleme sunucularına erişmek için ESET NOD32 Antivirus ürününü etkinleştirmeniz gerekir. Etkinleştirme anahtarınız ESET NOD32 Antivirus ürününü satın aldıktan sonra ESET tarafından bir e-posta ile size gönderilir.



Mevcut sürüm – Yüklediğiniz mevcut ürün sürümünün numarasını gösterir.

Son başarılı güncelleme – Son başarılı güncelleme tarihini gösterir. Yakın bir tarih göremezseniz, ürün modülleriniz güncel olmayabilir.

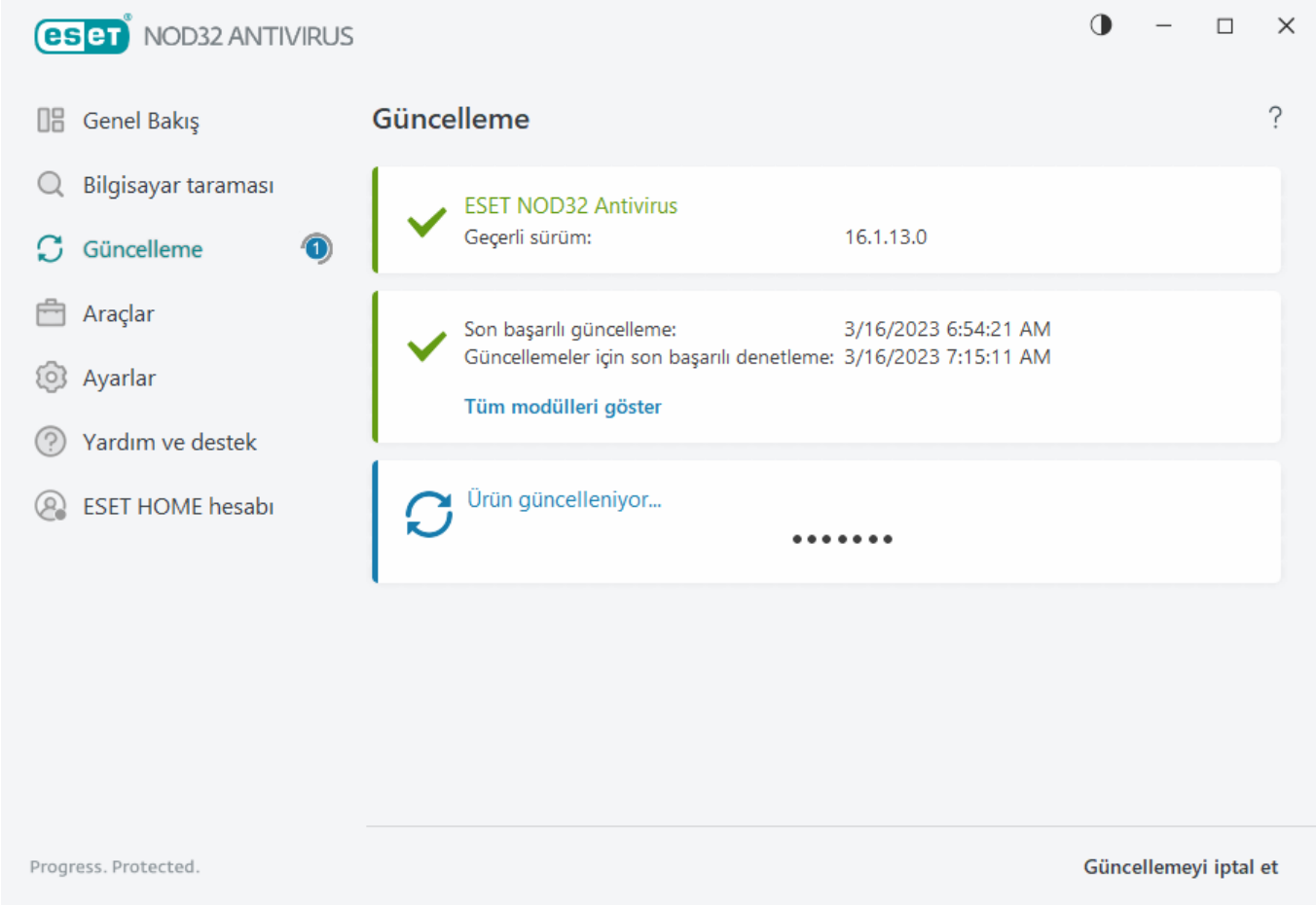
Güncellemeler için son başarılı kontrol – Güncellemeler için son başarılı kontrolün tarihini gösterir.

Tüm modülleri göster – Yüklenmiş olan program modüllerinin listesini gösterir.

Kullanılabilir en yeni ESET NOD32 Antivirus 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.



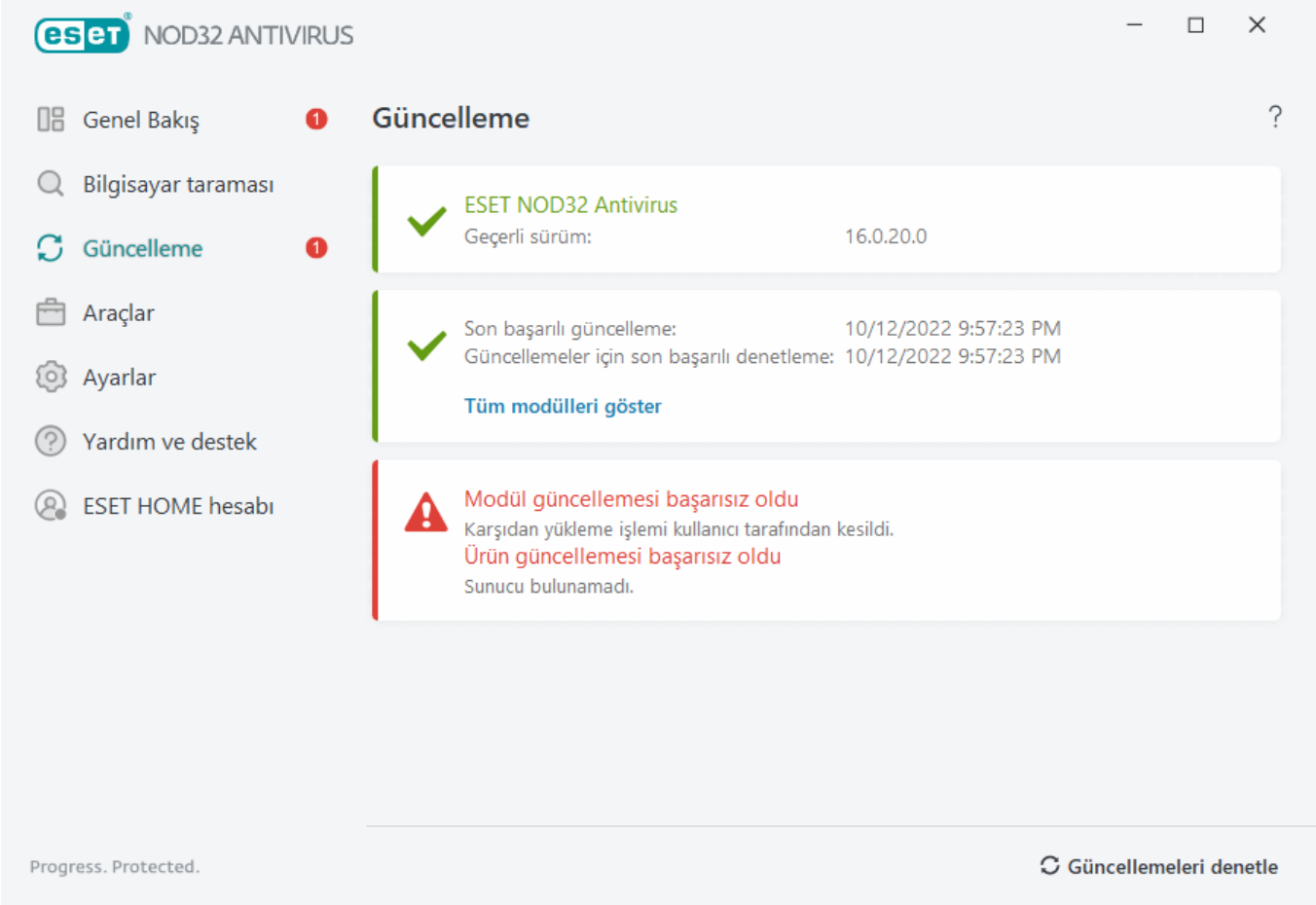
Normal şartlarda **Güncelleme** penceresinde programın güncel olduğunu belirten yeşil onay işaretini görürsünüz. Yeşil onay işaretini görmezseniz, program güncel değildir ve virüslere açıktır. Lütfen program modüllerini en kısa zamanda güncelleyin.

Başarısız güncelleme

Modül güncellemesinin başarısız olduğuyla ilgili bir ileti alırsanız nedeni şunlardan biri olabilir:

1. **Geçersiz abonelik**: Etkinleştirme için kullanılan abonelik geçersiz veya süresi dolmuş. Ana program penceresinde, **Yardım ve destek** > **Aboneliği değiştir** öğesine 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 ESET NOD32 Antivirus aracını yeni ürün sürümüne başarıyla güncelledikten sonra bilgisayarınızı yeniden başlatmanız gerekir. Normal modül güncellemelerinin ardından bilgisayarınızın yeniden başlatılması gerekmez.

Daha fazla bilgi için lütfen "Modül güncellemesi başarısız oldu" iletisi için sorun giderme bölümüne bakın.

İletişim penceresi - Yeniden başlatma gerekli

ESET NOD32 Antivirus ürününü yeni bir sürüme güncelledikten sonra bilgisayarın yeniden başlatılması gerekir. ESET NOD32 Antivirus yeni sürümleri, iyileştirmeleri uygulayacak veya program modüllerinin otomatik güncellemelerinin çözemediği sorunları düzeltecek şekilde tasarlanmıştır.

ESET NOD32 Antivirus 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.

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** > **Zamanlayıcı**'yı tıklatın. Varsayılan olarak, ESET NOD32 Antivirus içinde aşağıdaki güncelleme görevleri etkindir:

- **Düzenli 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.

Araçlar

Araçlar menüsü, ek güvenlik sunan ve ESET NOD32 Antivirus yönetimini basitleştirmeye yardımcı olan özellikler içerir. Aşağıdaki araçlar kullanılabilir:

 Günlük dosyaları

 Çalışan işlemler (ESET NOD32 Antivirus ürününde ESET LiveGrid® etkinse)

 Güvenlik raporu

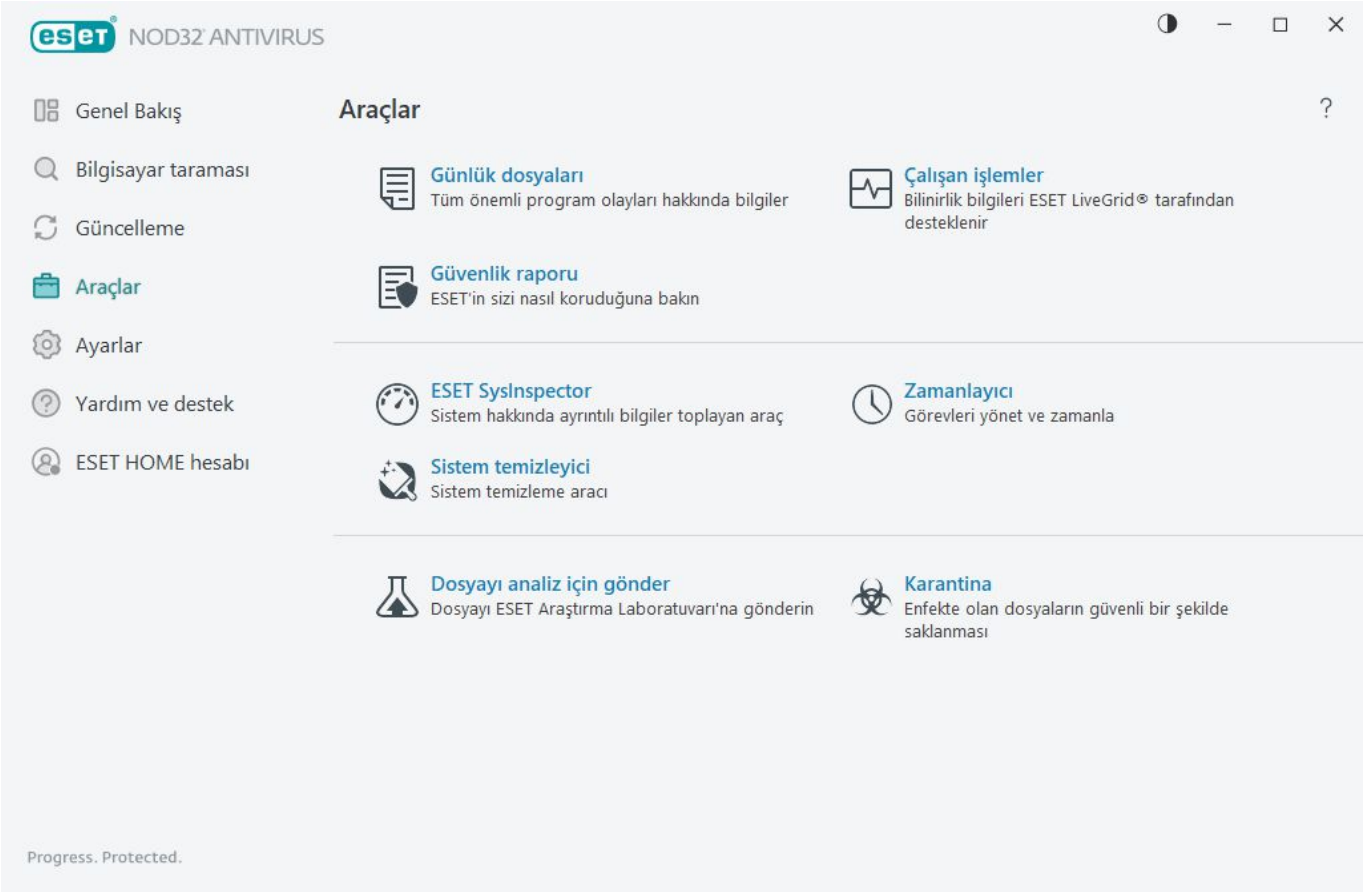
 ESET SysInspector

 Zamanlayıcı

 Sistem temizleyici

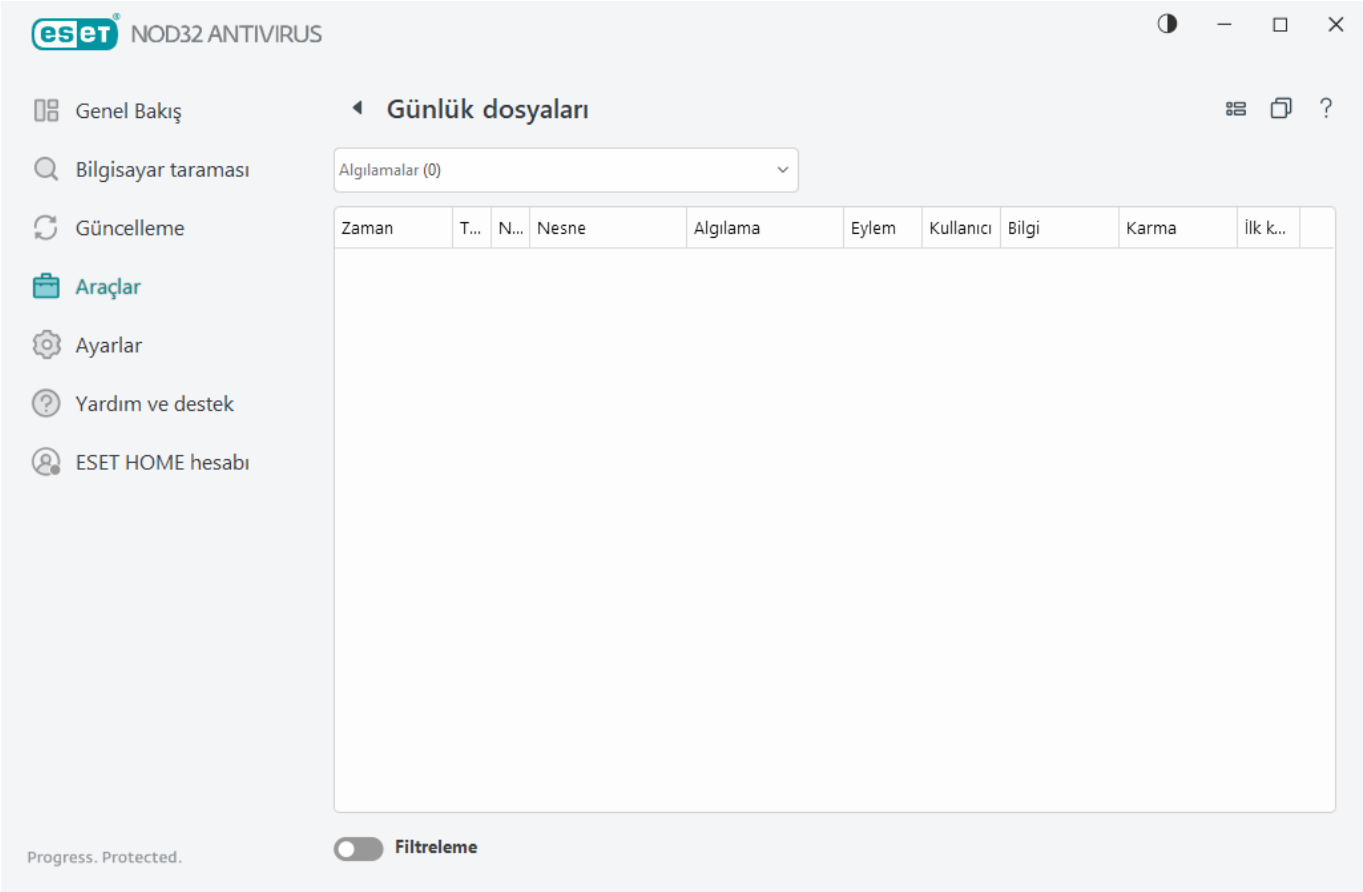
 Örneği analiz için gönder (ESET LiveGrid® yapılandırmanıza bağlı olarak kullanılamıyor olabilir).

 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 NOD32 Antivirus içinden metin iletileri ile günlükleri görüntülemek ve günlükleri arşivlemek mümkündür.



Günlük dosyalarına, ana program menüsünden **Araçlar** > **Günlük dosyaları** tıklatılarak erişilebilir. Günlük açılır menüsünden istediğiniz günlük türünü seçin.

- **Tespitler** – Bu günlük, ESET NOD32 Antivirus 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 NOD32 Antivirus 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.

- **Filtrelenen web siteleri** -Bu liste, Web Erişimi Koruması tarafından engellenen web sitelerinin listesini görüntülemek istediğinizde kullanışlıdır. Her günlük saat, URL adresi, kullanıcı ve belirli bir web sitesi ile bağlantı kuran uygulamayı içerir.

- **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.

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).
- **Tarayıcı koruması izin verilenler listesine ekle** - Tarayıcı koruması izin verilenler listesi penceresi açılır ve öğe listeye eklenir.

Günlük filtreleme

Filtreleme simgesini tıklayarak (**Araçlar** > **Günlük dosyaları**) filtreleme kriterlerini tanımlayın.

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

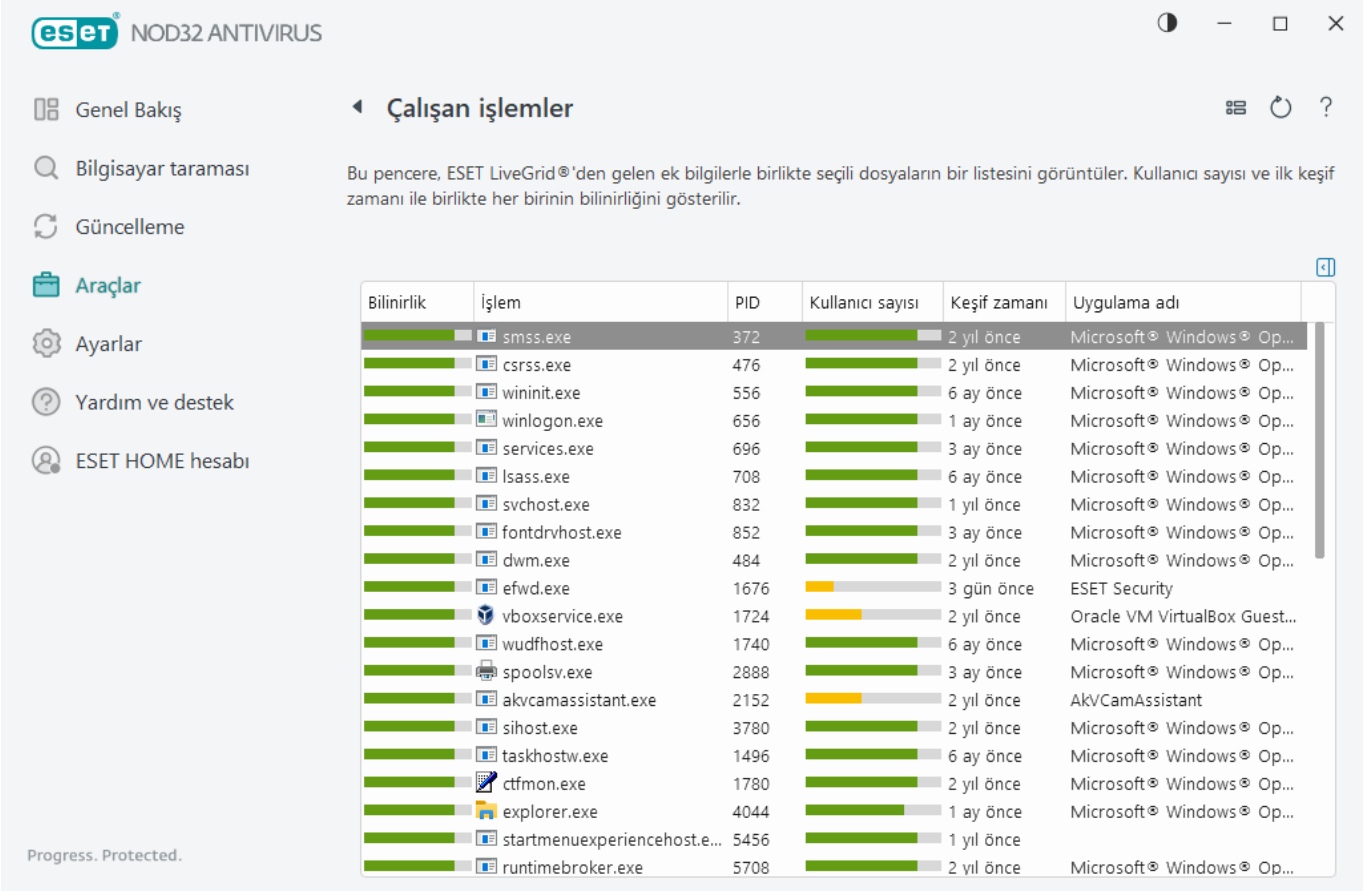
Daha hassas sonuçlar için tam sözcükleri aramak istiyorsanız onay kutusunu işaretleyin.

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.

Çalışan işlemler

Çalışan işlemler, bilgisayarınızda çalışan programları veya işlemleri görüntüler ve ESET'i hemen ve sürekli olarak yeni sızıntılarla ilgili bilgilendirir. ESET NOD32 Antivirus, kullanıcıları ESET LiveGrid® teknolojisiyle korumak için çalışan işlemlerle ilgili ayrıntılı bilgi sağlar.



Bilinirlik – Çoğu durumda, ESET NOD32 Antivirus 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.

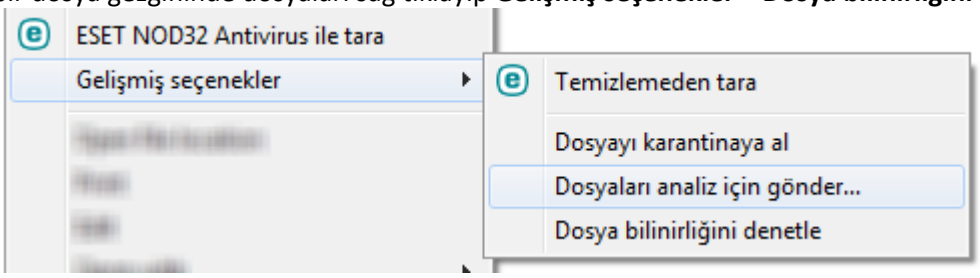
Keşif zamanı – Uygulamanın ESET LiveGrid® teknolojisi tarafından tespit edilmesinden o ana kadar geçen süre.

> 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.
- **PUA algılandı** – İstenmeyen türden olabilecek uygulamaların (PUA) sayısını gösterir.
- **Taranan belgeler**: Taranan belge nesnelerinin sayısını gösterir.

- **Taranan uygulamalar** – Taranan yürütülebilir nesnelerinin sayısını gösterir.
- **Taranan 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.

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 NOD32 Antivirus 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.

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. Günlük C:\ProgramData\ESET\ESET Security\SysInspector hedefine kaydedilir.
- **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.

Zamanlayıcı

Zamanlayıcı, zamanlanan görevleri önceden tanımlanmış yapılandırma ve özelliklerle başlatır ve yönetir.

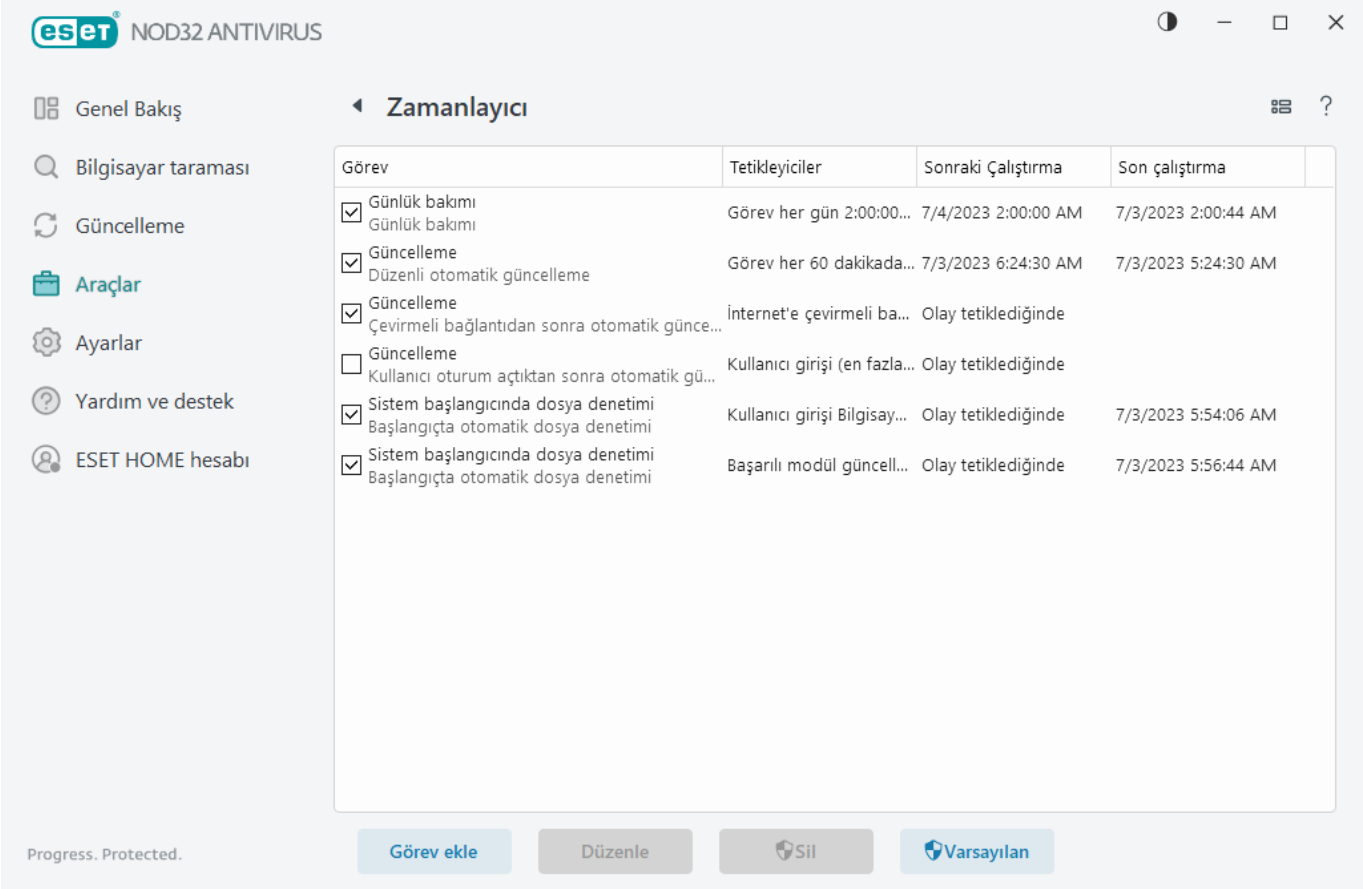
Zamanlayıcıya **Araçlar** > **Zamanlayıcı** öğeleri tıklanarak ESET NOD32 Antivirus ana program penceresinden erişilebilir. **Zamanlayıcı**, tüm zamanlanan görevlerin ve önceden tanımlı tarih, saat ve kullanılan tarama profili gibi yapılandırma özelliklerinin listesini içerir.

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**
- **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 açma/kapama düğmesini tıklayın (zamanlanan görevler listesinden onay kutusunu işaretleyerek/işaretini kaldırarak bu işlemi daha sonra yapabilirsiniz), **Sonraki**'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.

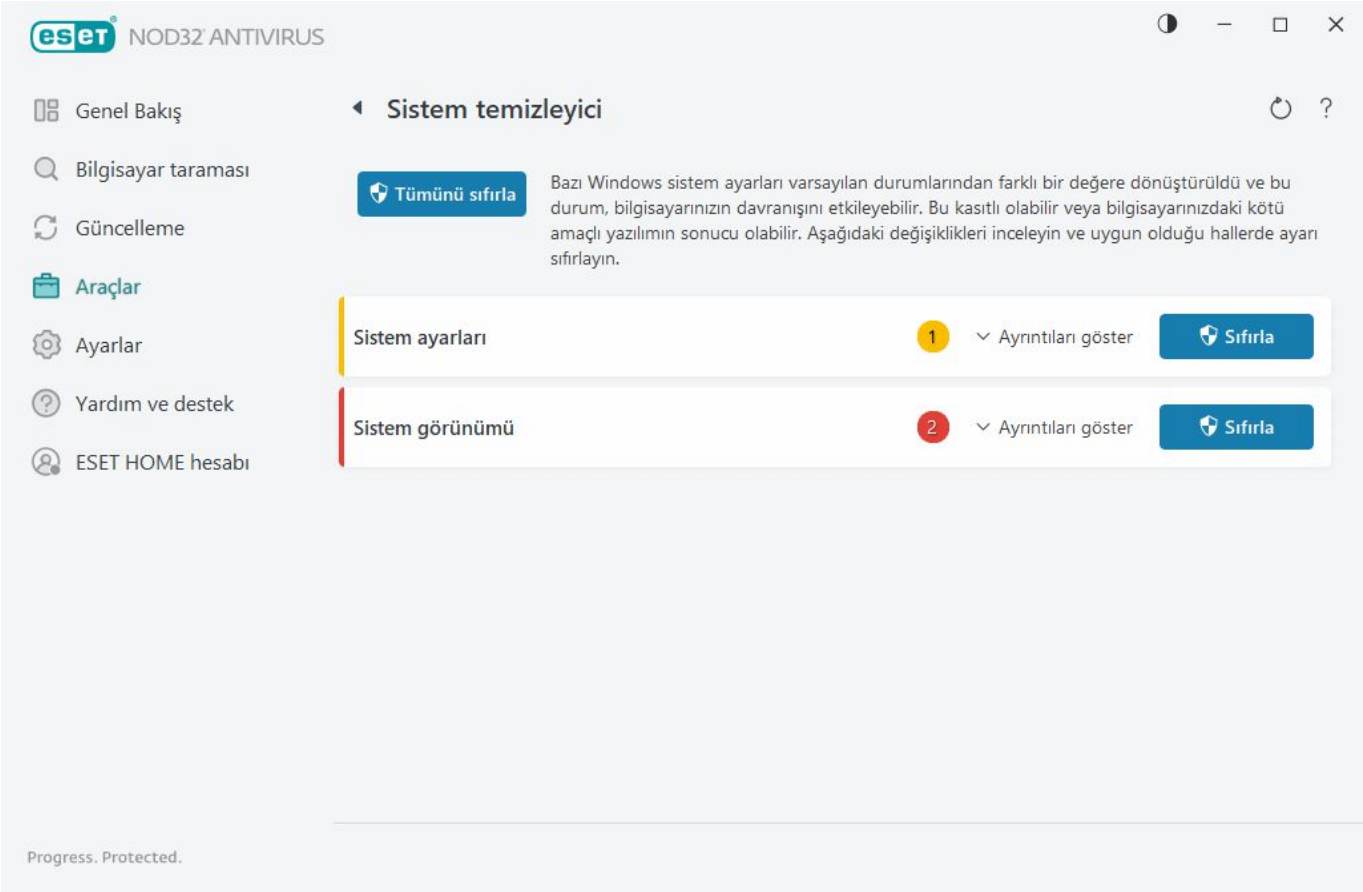
Sistem temizleyici beş ayar kategorisi için sorunları bildirir:

- **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.

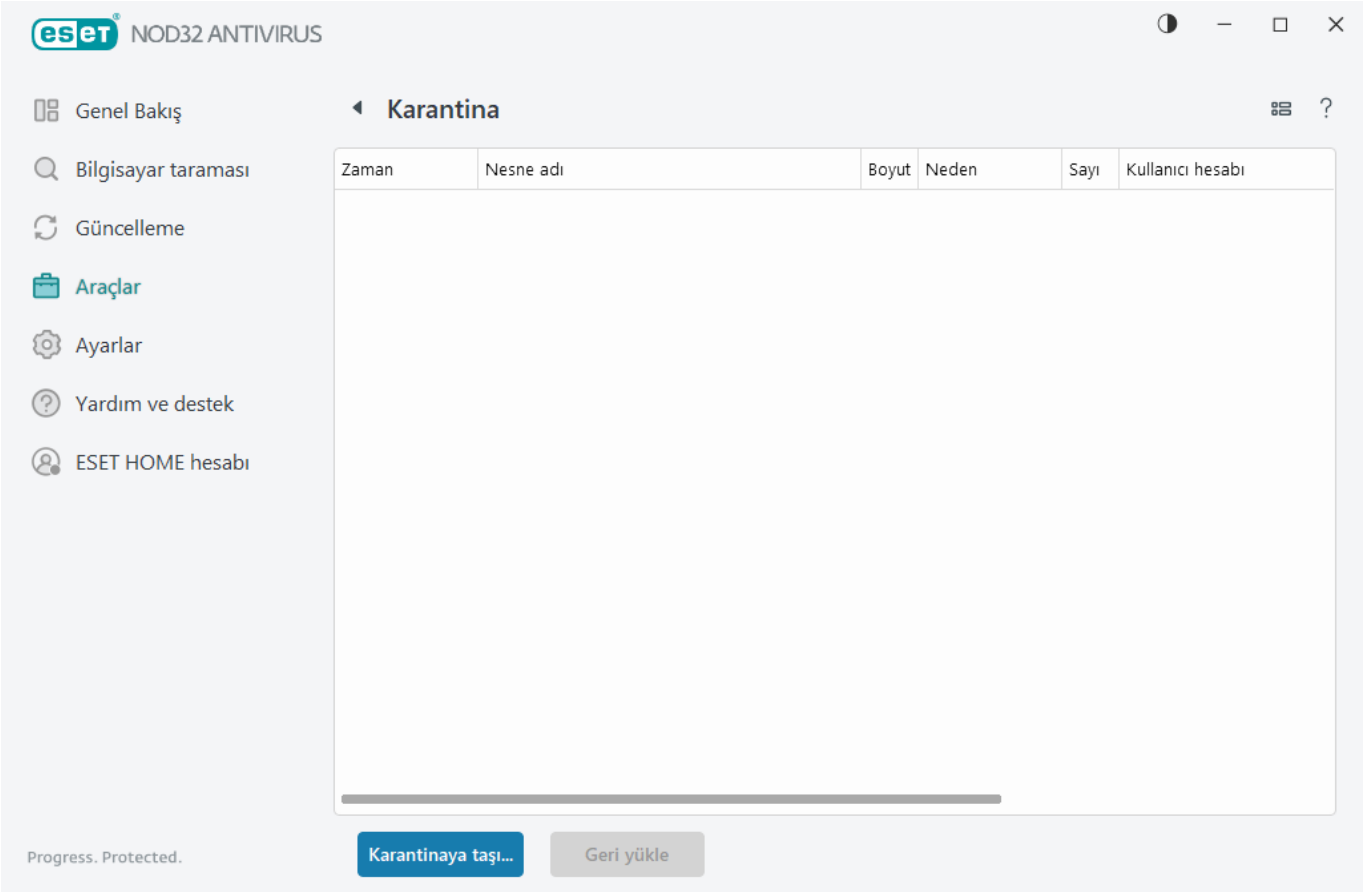
Karantina

Karantinanın temel işlevi, bildirilen nesneleri (kötü amaçlı yazılım, enfekte olan dosyalar veya istenmeyen türden olabilecek uygulamalar gibi) güvenli bir şekilde depolamaktır.

Karantinaya ESET NOD32 Antivirus ana program penceresinden **Araçlar** > **Zamanlayıcı** 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 NOD32 Antivirus, 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 NOD32 Antivirus tarafından hatalı bir şekilde tespit edilirse

d.veya bir dosya şüpheli bir şekilde davranırsa ancak Korumalar 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. Karantinadaki tüm öğeleri seçmek ve silmek istiyorsanız klavyenizdeki **Ctrl + A** ve **Delete** tuşlarına basabilirsiniz. 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 NOD32 Antivirus ürününde karantinaya alınmış bir dosyayı geri yükleme
> - ESET NOD32 Antivirus 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.

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 veya spam yanlış tespitlerini 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.

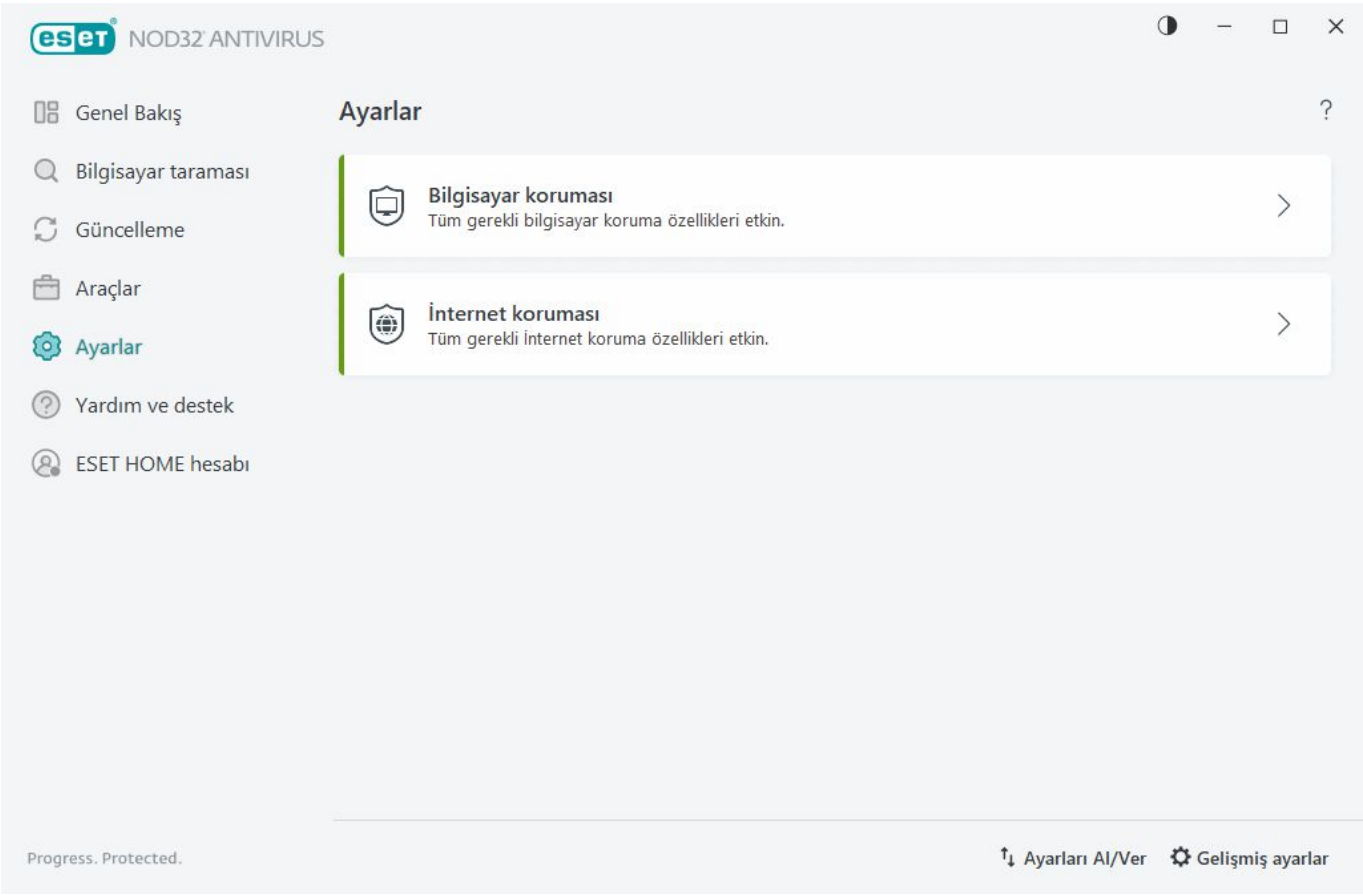
Analiz için örnek seçin - Diğer

Şüpheli dosya veya **Hatalı pozitif** olarak sınıflandırılamayacak dosyalar için bu formu kullanın.

Dosyayı gönderme nedeni - Lütfen detaylı bir açıklama ve dosyanın neden gönderildiğini girin.

Ayarlar

Kullanılabilir koruma özellikleri gruplarını ana program penceresi > **Ayarlar**'da bulabilirsiniz.



Ayarlar menüsünde aşağıdaki gruplar bulunur:

 Bilgisayar koruması

 İnternet koruması

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 modüllerine genel bir bakış için ana program penceresi > **Ayarlar** bölümünden **Bilgisayar koruması**'nı tıklayın:

- 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.

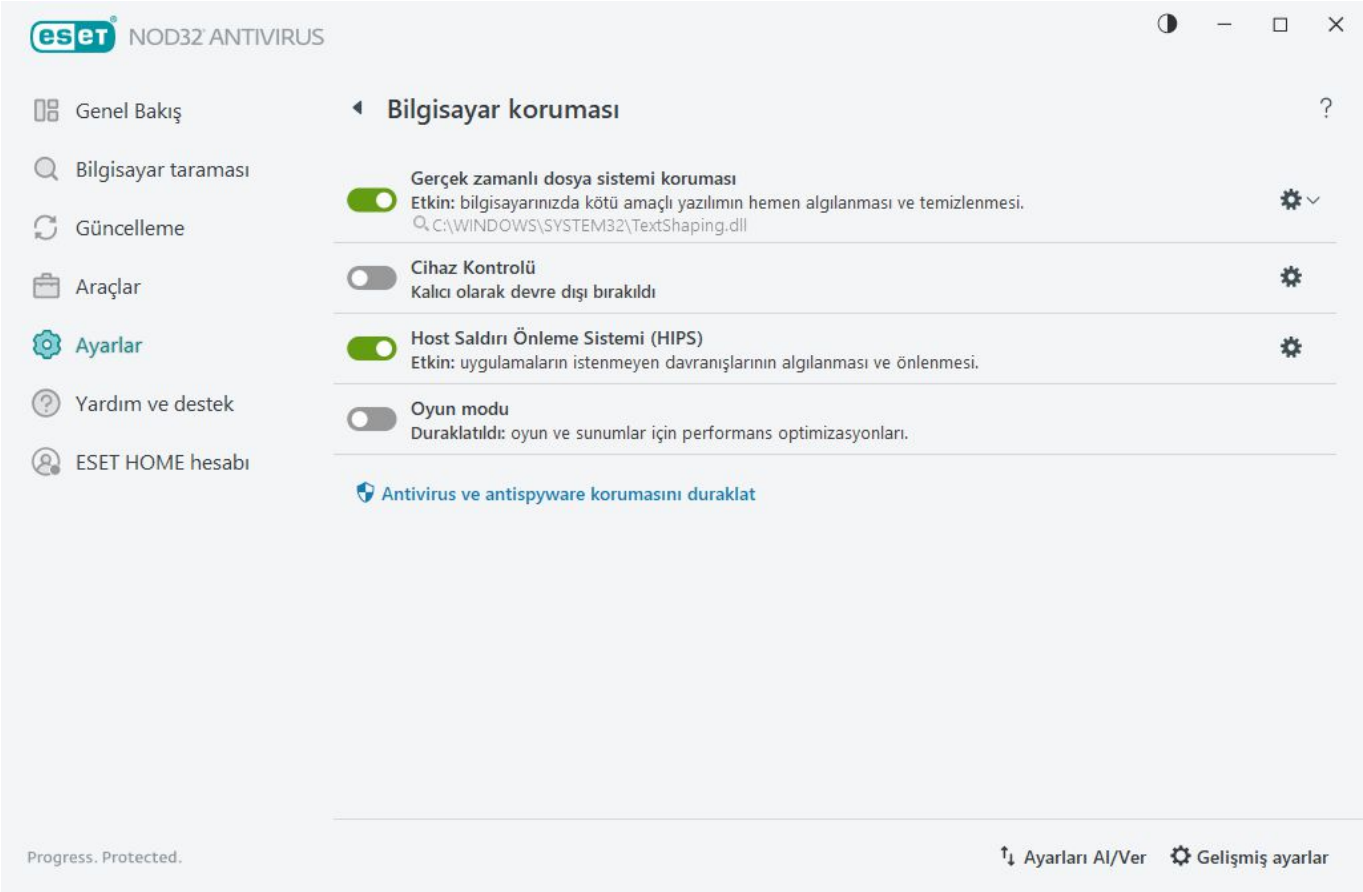
Koruma modüllerini tek tek duraklatmak veya devre dışı bırakmak için  açma/kapama simgesini tıklayın.

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.



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.

Sızıntı algılandı

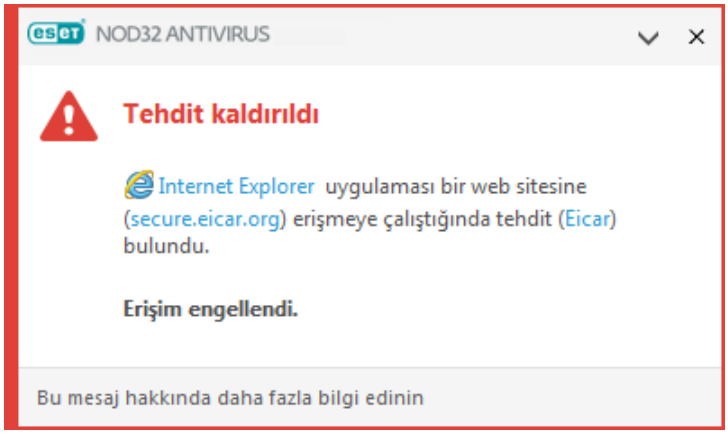
Sızıntılar sisteme web sayfaları, paylaşılan klasörler, e-posta veya çıkarılabilir aygıtlar (USB, harici diskler, CD, DVD, vb.) gibi çeşitli giriş noktalarından ulaşabilir.

Standart davranış

Sızıntıların, ESET NOD32 Antivirus 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 NOD32 Antivirus uygulamasını açıp **Bilgisayar taraması**'nı tıklatın.

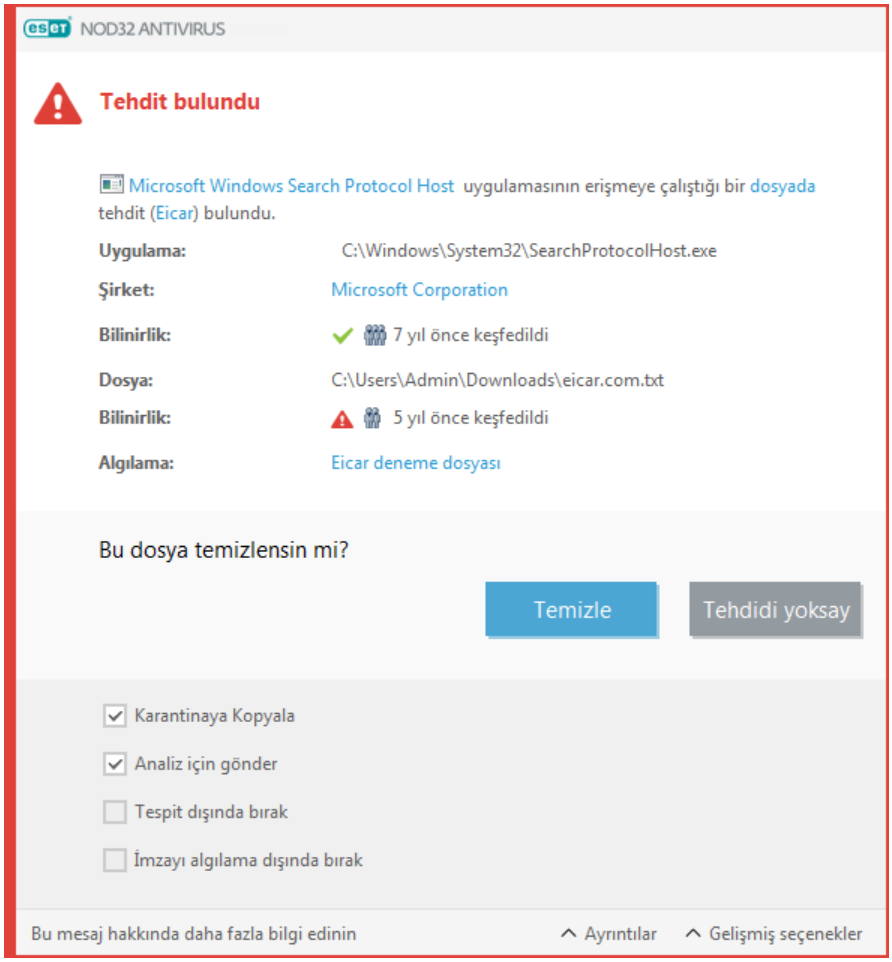
2.**Bilgisayarınızı tarayın**'ı tıklatın (daha fazla bilgi için Bilgisayar taraması bölümüne bakın).

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 NOD32 Antivirus ana program penceresinden **Araçlar** > **Zamanlayıcı** 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

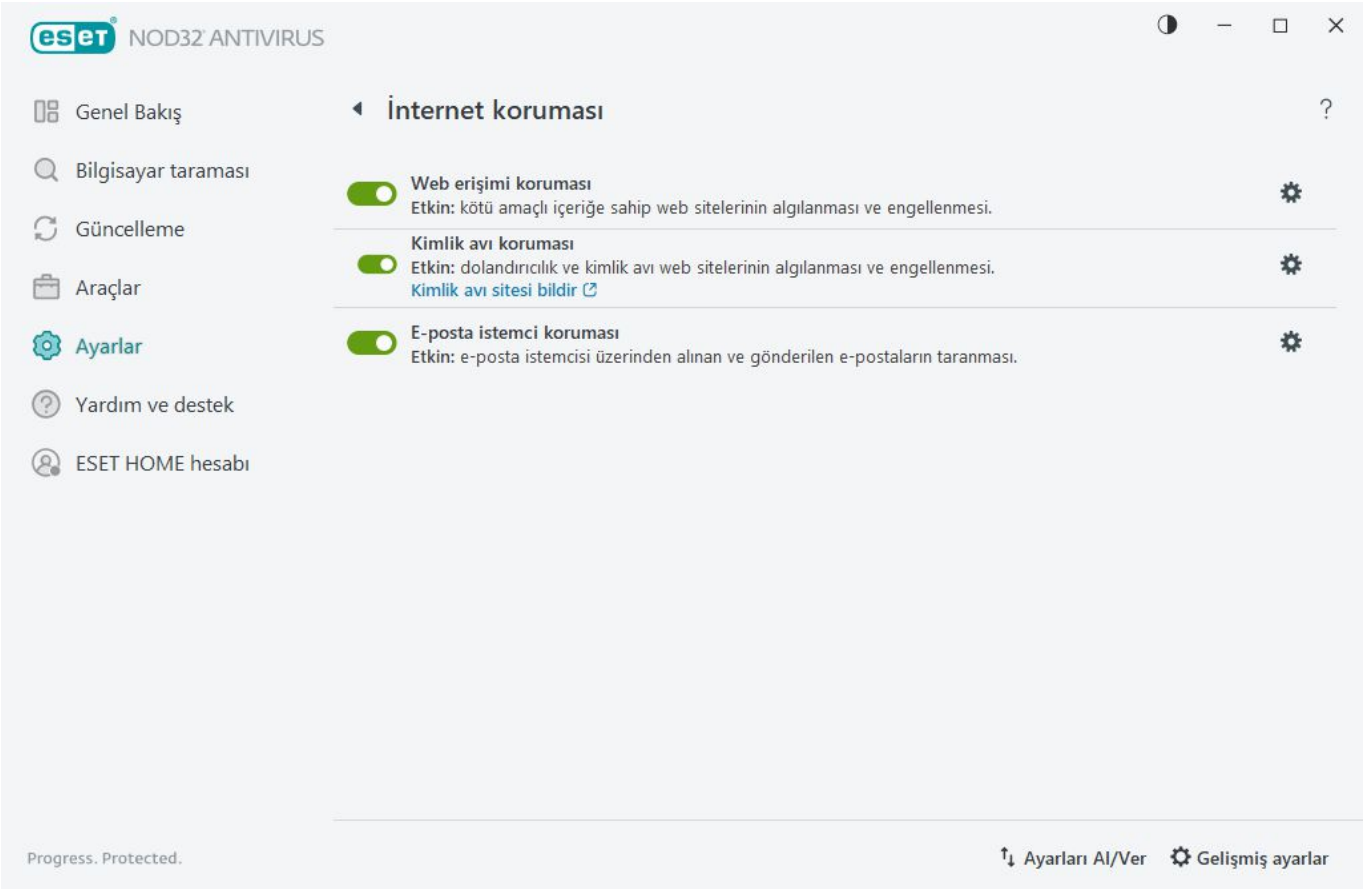
Varsayılan temizleme modunda, arşiv ancak yalnızca etkilenen dosyalar içeriyor ve temiz dosya içermiyorsa tümüyle silinir. Başka bir deyişle, arşivler zararsız temiz dosyalar da içeriyorsa silinmez. Katı kurallı temizleme taraması gerçekleştirirken dikkatli olun; Katı kurallı temizleme etkinken arşivde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

İnternet koruması

Internet'e bağlanabilirlik bir kişisel bilgisayardaki standart özelliktir. Ne yazık ki aynı zamanda kötü amaçlı kod aktarımının gerçekleştirildiği ana ortam haline gelmiştir. ESET NOD32 Antivirus ürününde internet korumanızı artıran özellikleri yapılandırmak için ana program penceresi > **Ayarlar** > **İnternet koruması**'nı açın.

Koruma modüllerini tek tek duraklatmak veya devre dışı bırakmak için açma/kapama simgesini tıklayın.

Koruma modüllerini kapatmak, bilgisayarınızın koruma düzeyini düşürebilir.



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

Web erişimi koruması, HTTP/HTTPS iletişimini zararlı yazılımlara ve kimlik avına karşı tarar. Web erişimi koruması yalnızca sorun giderme amacıyla kapatılmalıdır.

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

Bir kimlik avı sitesini bildirin - Kimlik avı/kötü amaçlı web sitesini analiz için ESET'e bildirin.

> 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.

E-posta istemci koruması POP3(S) ve IMAP(S) protokolleri üzerinden alınan e-posta iletişiminin denetimini sağlar. ESET NOD32 Antivirus, e-posta istemcinize yönelik olan eklenti programını kullanarak e-posta istemcisinden yapılan tüm iletişimler üzerinde denetim sağlar.

Kimlik Avı koruması

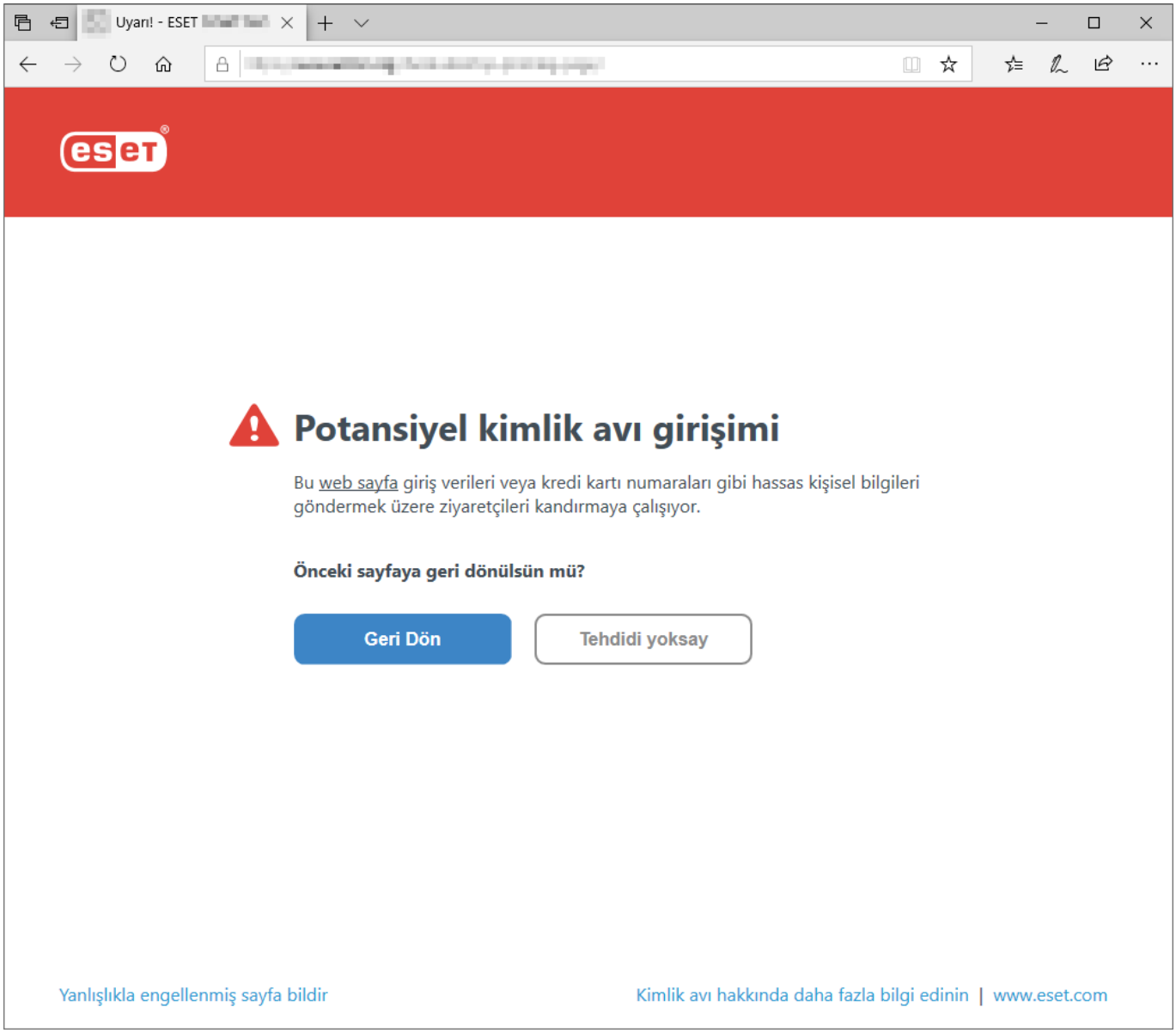
Kimlik avı, sosyal mühendisliği (kullanıcıları gizli bilgilerini elde etmek için manipüle etmek) kullanan bir suç faaliyetidir. Kimlik avı; banka hesap numaraları, PIN kodları gibi hassas verilere erişmek için kullanılır. Daha fazla bilgi için sözlüğe bakabilirsiniz. ESET NOD32 Antivirus, bu tür içeriği dağıttığı bilinen web sayfalarını engelleyen kimlik avı koruması sağlar.

Kimlik Avı koruması varsayılan olarak etkindir. Bu ayar, Gelişmiş ayarlar > **Korumalar Web erişimi koruması**'nda yapılandırılabilir.

ESET NOD32 Antivirus 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 > **Korumalar** > **Web erişimi koruması** > **URL adresi yönetimi** > **Adres listesi** > **Düzenle** bölümünde düzenlemek istediğiniz web sitesini listeye ekleyin.

Kimlik avı sitesi bildir

Hatalı bir şekilde engellenmiş bir sayfayı bildir bağlantısı, hatalı bir şekilde tehdit olarak algılanan bir web sitesini bildirmenizi sağlar.

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.

Ayarları al ve ver

Özelleştirilmiş ESET NOD32 Antivirus.xml yapılandırma dosyanızı **Ayarlar** menüsünde alabilir veya verebilirsiniz.

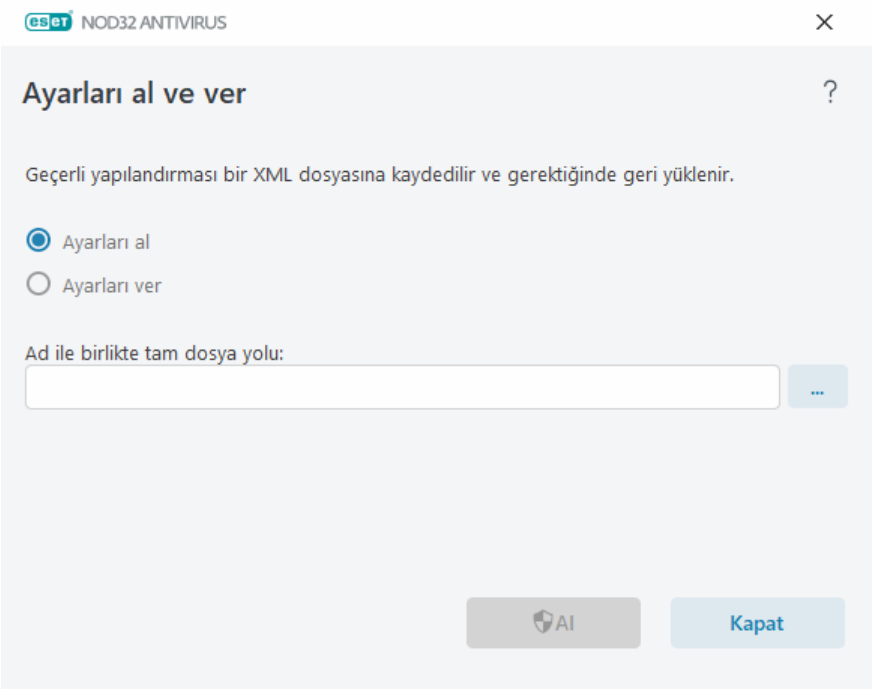
> **Resimli talimatlar**
> İngilizce ve diğer bazı dillerde mevcut olan resimli talimatlar için bir .xml dosyası kullanarak ESET yapılandırma ayarlarını içe veya dışa aktarma bölümüne bakın.

Geçerli ESET NOD32 Antivirus 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.



Yardım ve destek

Karşılaşabileceğiniz sorunları çözmenize yardımcı olacak destek bilgilerini ve sorun giderme araçlarını görüntülemek için ana program penceresinde **Yardım ve destek**'i tıklayın.

Abonelik

- Abonelikle ilgili sorun giderme: Etkinleştirme veya abonelik değişikliğiyle ilgili sorunlara çözüm bulmak için bu bağlantıya tıklayın.
- Aboneliği değiştirme: Etkinleştirme penceresini başlatmak ve ürününüzü etkinleştirmek için tıklayın.

Cihazınız ESET HOME ürününe bağlıysa ESET HOME hesabınızdan bir abonelik seçin veya yeni bir abonelik ekleyin.

Yüklenen ürün

- Yenilikler - Yeni ve geliştirilmiş özelliklerle ilgili bilgi penceresini açmak için bunu tıklayın.
- ESET NOD32 Antivirus Hakkında – ESET NOD32 Antivirus ürününüzün kopyası hakkındaki bilgileri görüntüler.
- Ürünle ilgili sorun giderme - En sık karşılaşılan sorunlara çözüm bulmak için bu bağlantıyı tıklayın.
- **Ürünü değiştirme**: ESET NOD32 Antivirus ürününü mevcut abonelik ile farklı bir ürün serisine dönüştürme imkanı olup olmadığını anlamak için tıklayın.

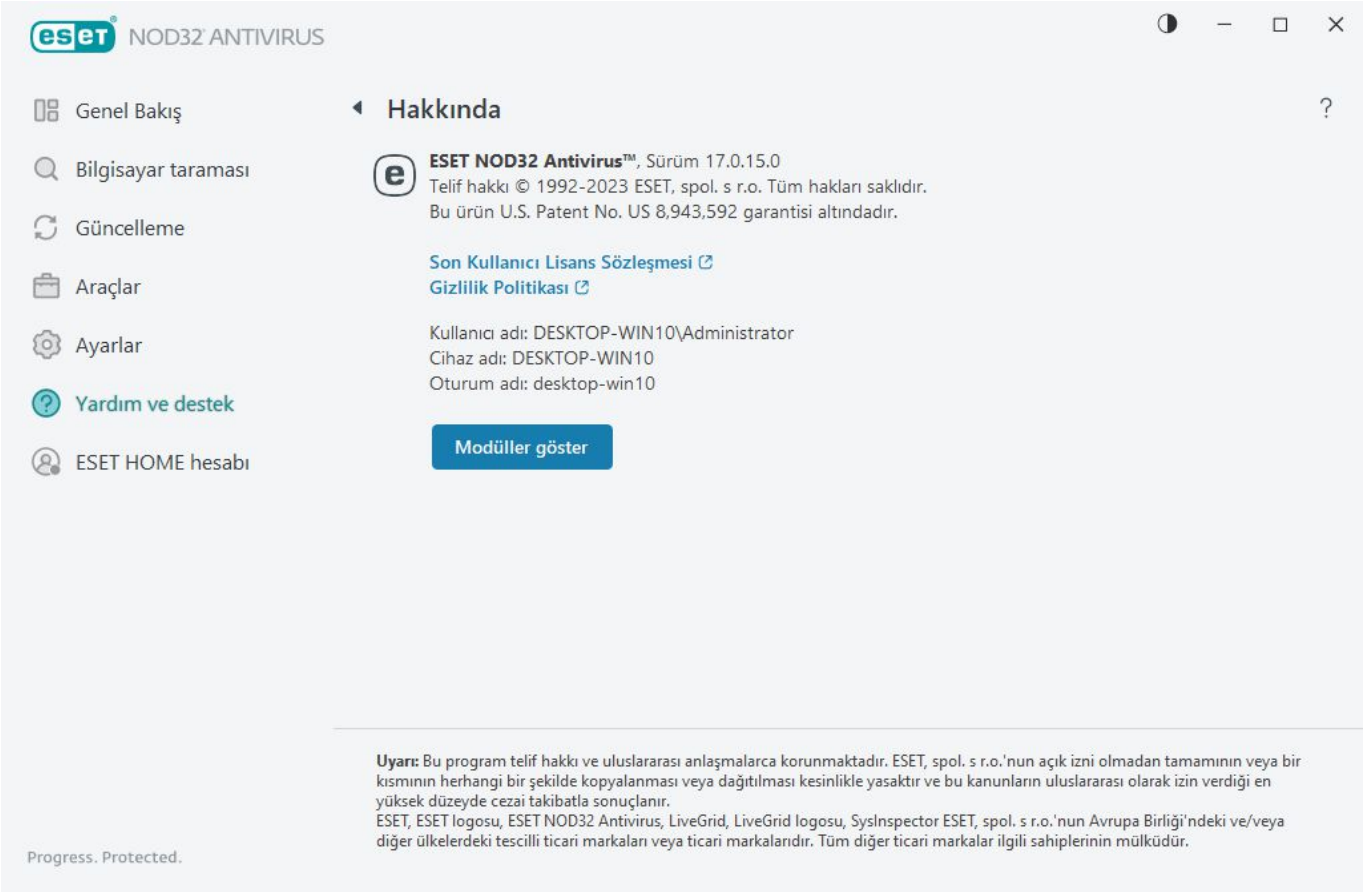
Yardım sayfası – ESET NOD32 Antivirus yardım sayfalarını açmak için bu bağlantıyı tıklatın.

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 NOD32 Antivirus Hakkında

Bu pencerede, ESET NOD32 Antivirus 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 NOD32 Antivirus, ESET haberleri hakkında sizi düzenli olarak bilgilendirir.

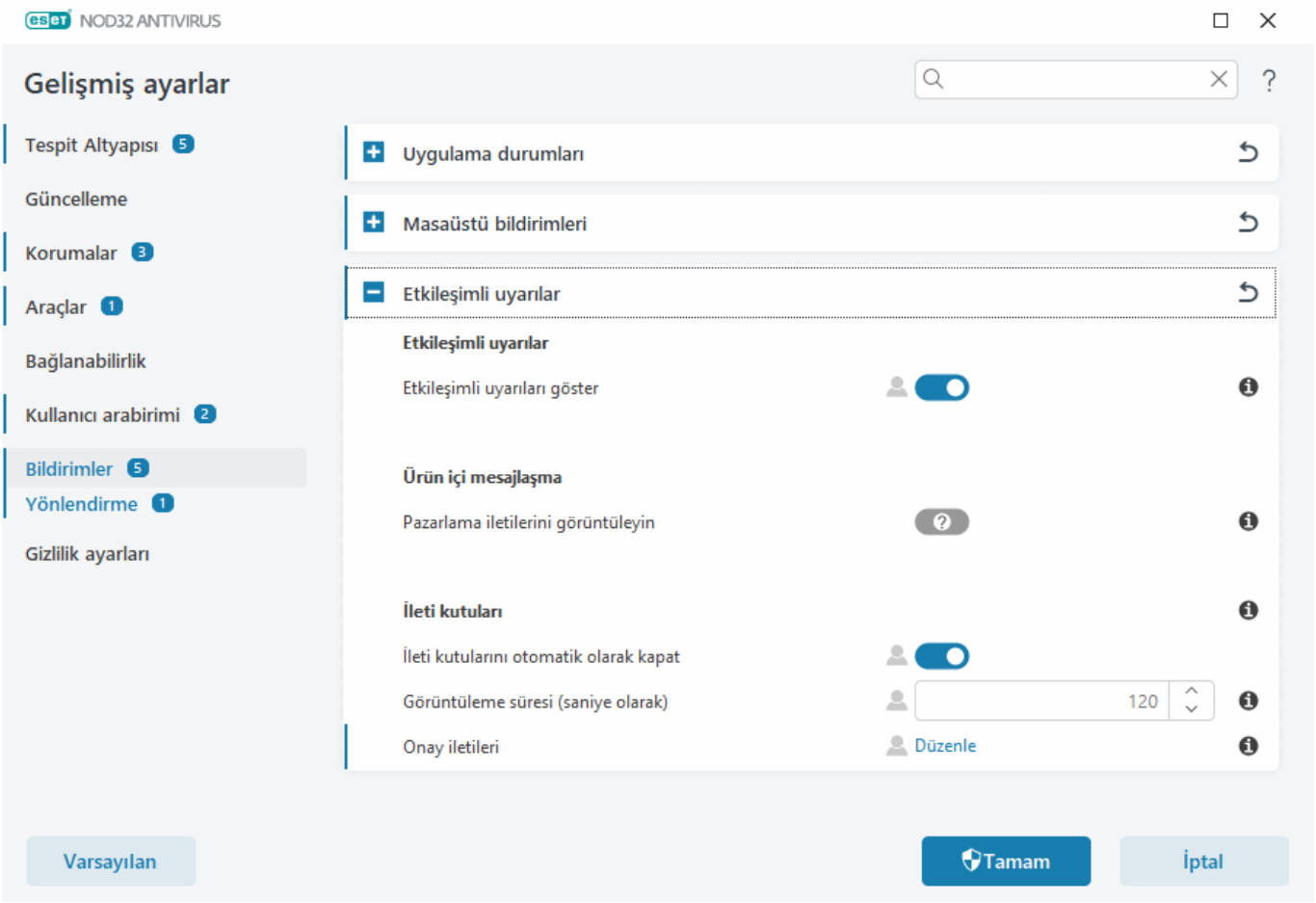
Ürün içi mesajlaşma, ESET haberleri ve diğer iletişimler hakkında kullanıcıları bilgilendirmek üzere tasarlanmıştır. Pazarlama iletileri göndermek için kullanıcının onayı gerekir. Bu nedenle, pazarlama iletileri varsayılan olarak kullanıcıya gönderilmez (soru işaretiyle gösterilir). Bu seçeneği etkinleştirerek ESET pazarlama iletilerini almayı kabul edersiniz. ESET pazarlama malzemelerini almak istemiyorsanız **Pazarlama iletilerini göster** seçeneğini devre dışı bırakın.

Bildirim penceresi üzerinden pazarlama mesajları almayı etkinleştirmek veya devre dışı bırakmak için aşağıdaki talimatları uygulayın.

1. Gelişmiş ayarları açar

2. **Bildirimler** > **Etkileşimli Uyarıları** tıklayın.

3. **Pazarlama iletilerini göster** seçeneğini değiştirin.



Sistem konfigürasyon verilerini gönder

ESET, mümkün olduğu kadar çabuk ve doğru bir şekilde destek sağlamak amacıyla ESET NOD32 Antivirus yapılandırması hakkındaki bilgilere, ayrıntılı sistem bilgilerine ve çalışan işlemler (ESET SysInspector günlük dosyası) ile 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. Web formunu herhangi bir veri göndermeden, **Verileri gönderme**'yi tıklayın ve devam edin.

Sistem yapılandırma verilerinin gönderilmesini Gelişmiş ayarlar > **Araçlar** > **Tanılamalar** > Teknik destek bölümünde yapılandırabilirsiniz.

Sistem yapılandırma verilerini göndermeye karar verdiyseniz web formunu doldurmanız ve göndermeniz gerekir. Aksi takdirde, biletiniz oluşturulmaz ve sistem yapılandırma verileriniz kaybolur. Sistem yapılandırma verileri gönderilemiyorsa web formunu doldurun ve Teknik Destek'ten gelecek talimatları bekleyin.

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

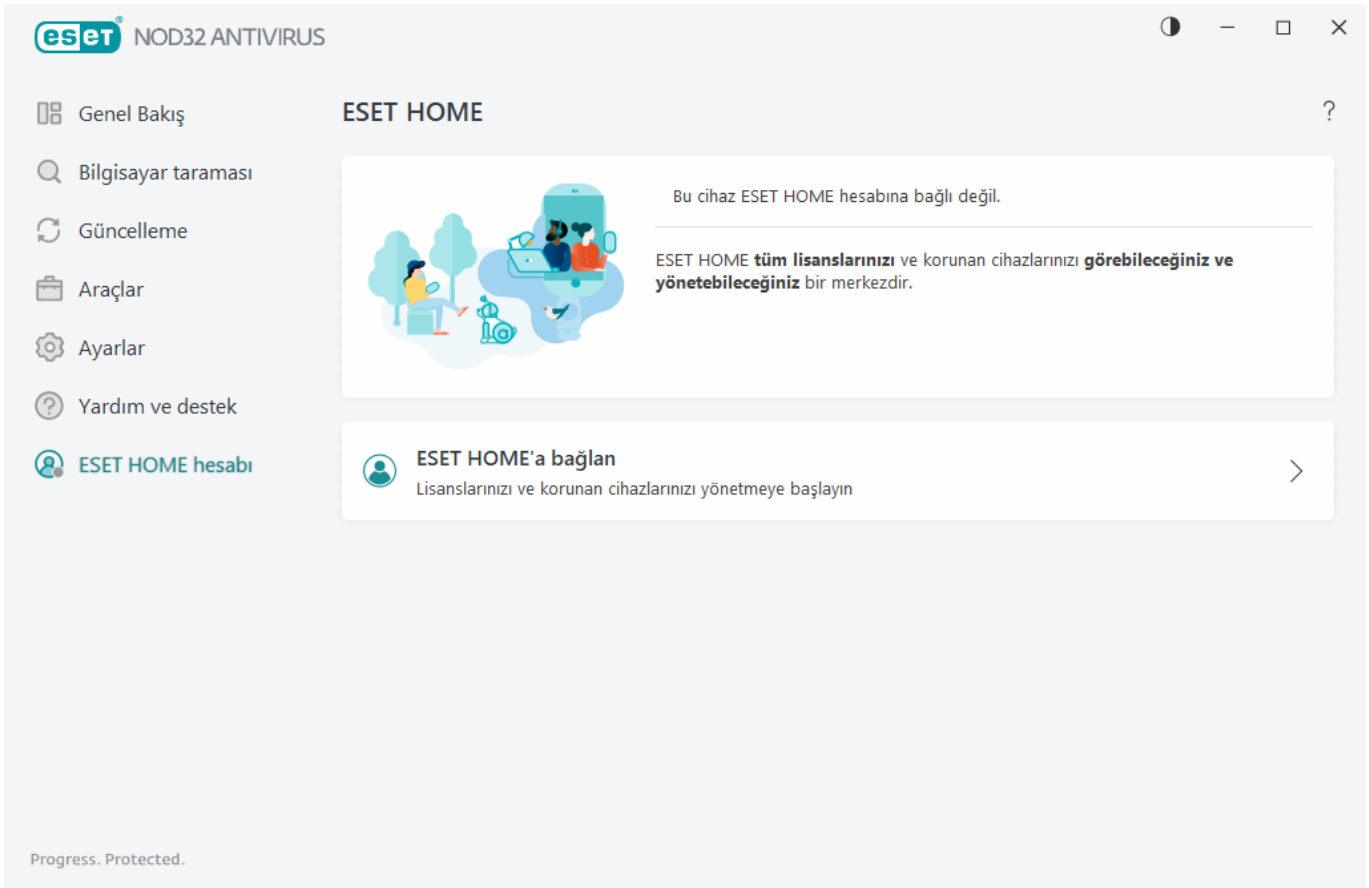
Teknik Destek Ayrıntıları: İstendiğinde bilgileri (örneğin abonelik bilgileri, ürün adı, ürün sürümü, işletim sistemi ve bilgisayar bilgileri) kopyalayıp ESET Teknik Destek bölümüne gönderebilirsiniz.

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 ve aboneliklerinizi ile korunan cihazlarınızı yönetmek için ESET HOME portalına bağlan'a tıklayın. Aboneliğinizi yenileyebilir, yükseltebilir veya uzatabilir ve önemli ayrıntıları görüntüleyebilirsiniz. ESET HOME Yönetim portalında veya mobil uygulamada farklı abonelikler ekleyebilir, ürünleri cihazlarınıza indirebilir, ürün güvenlik durumunu kontrol edebilir veya e-posta üzerinden abonelik 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.

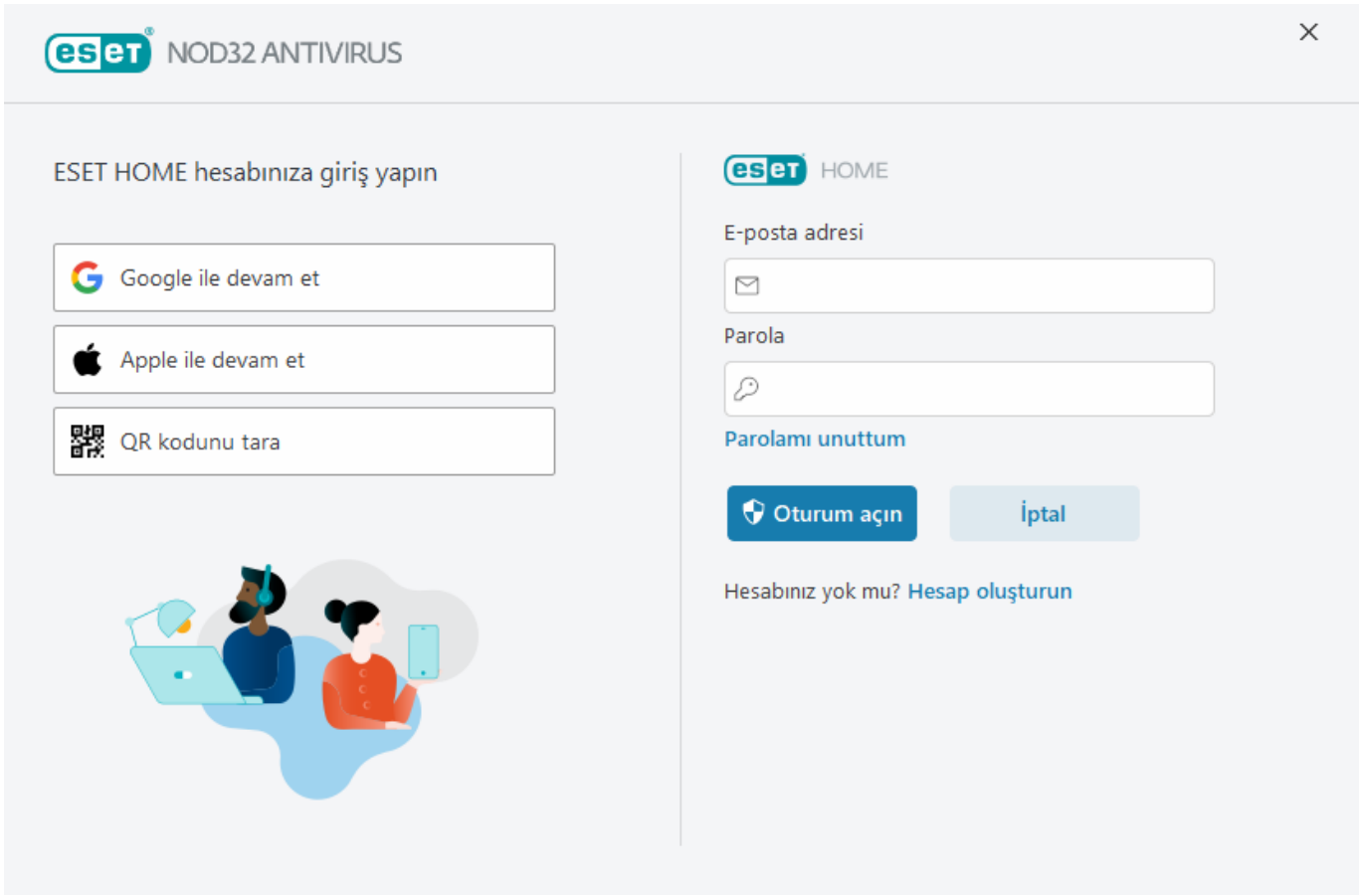
Cihaz adı - Bu cihazın ESET HOME hesabında gösterilen adı.

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 abonelik etkin halde kalır ve cihazınız korunur.

ESET HOME Hesabınıza bağlanın

Etkinleştirilen tüm ESET aboneliklerinizi ve cihazlarınızı görüntüleyip yönetmek için cihazınızı ESET HOME portalına bağlayın. Aboneliğinizi yenileyebilir, yükseltebilir veya uzatabilir ve önemli abonelik ayrıntılarını görüntüleyebilirsiniz. ESET HOME yönetim portalında veya mobil uygulamada farklı abonelikler ekleyebilir, ürünleri cihazlarınıza indirebilir, ürün güvenlik durumunu kontrol edebilir ya da e-posta üzerinden abonelikleri 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 NOD32 Antivirus ürünü zaten yüklenmişse ve ESET HOME hesabınıza eklenmiş bir abonelikle etkinleştirilmişse cihazınızı ESET HOME portalını kullanarak ESET HOME aracına bağlayabilirsiniz. ESET HOME Online Yardım kılavuzundaki talimatları uygulayın ve ESET NOD32 Antivirus 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:

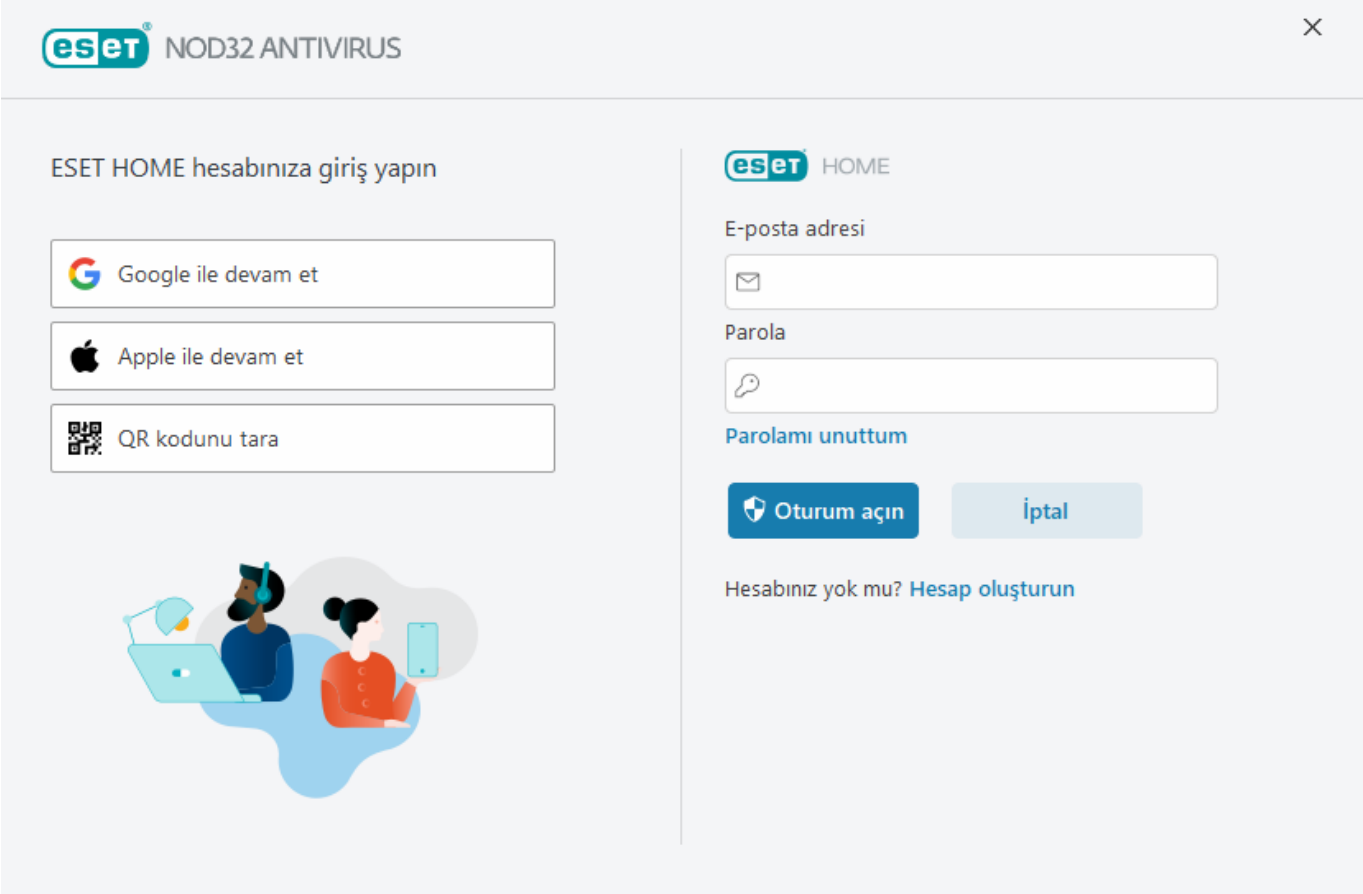
• **ESET HOME E-posta adresinizi ve parolanızı kullanarak** - ESET HOME hesabınızı oluşturmak için kullandığınız **E-posta adresini** ve **Parolayı** yazın ve **Giriş yap**'ı tıklayın.

• **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 yazın ve yazılan e-posta adresinin doğru olduğunu onaylayın. Yine de oturum açamazsanız **Geri** > **Parolamı unuttum**'u tıklayarak parolanızı sıfırlayın ve ekran adımlarını takip edin veya ESET HOME parolamı unuttum bölümüne bakın.

Seçilen giriş 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 NOD32 Antivirus 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 NOD32 Antivirus ürünü zaten yüklenmişse ve ESET HOME hesabınıza eklenmiş bir abonelikle etkinleştirilmişse cihazınızı ESET HOME portalını kullanarak ESET HOME aracına bağlayabilirsiniz:

1. Cihazınıza bir bağlantı isteği gönderin.

2. ESET NOD32 Antivirus, 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.

Gelişmiş ayarlar

Gelişmiş ayarlar, ayrıntılı ESET NOD32 Antivirus ayarlarını gereksinimlerinize uyacak şekilde yapılandırmanıza olanak tanır.

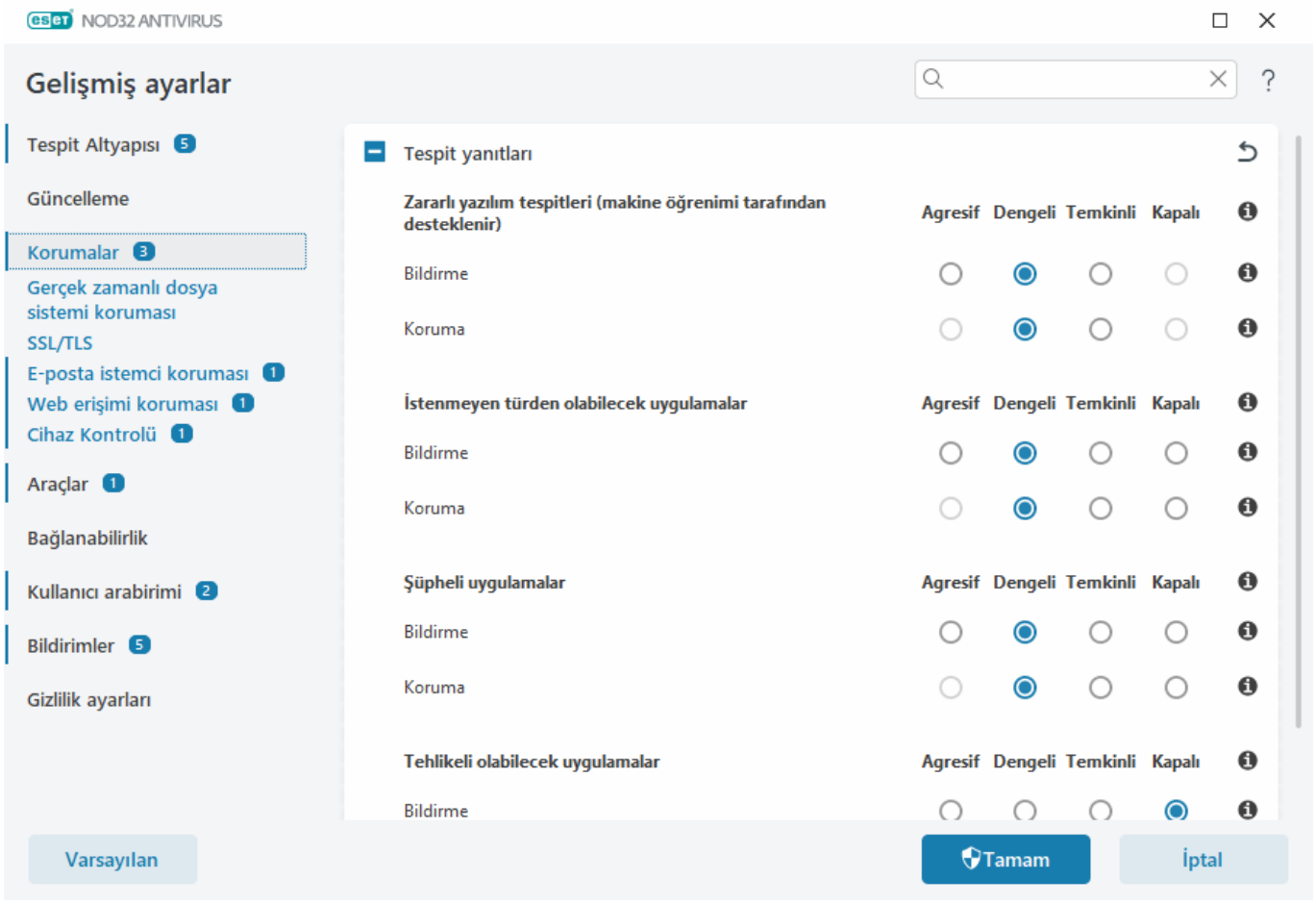
Gelişmiş ayarlar'ı açmak için ana program penceresini açın ve klavyenizdeki **F5** tuşuna basın veya **Ayarlar** > **Gelişmiş ayarlar**'ı tıklayın.

Access ayarlarınıza bağlı olarak, Gelişmiş ayarlar'ı açmak için bir parola yazmanız istenebilir.

Gelişmiş ayarlarda, aşağıdaki ayarları yapılandırabilirsiniz:

- Algılama altyapısı

- Güncelleme
- Korumalar
- Araçlar
- Bağlanabilirlik
- Kullanıcı arabirimi
- Bildirimler
- Gizlilik ayarları



Algılama altyapısı

Gelişmiş ayarlar > **Tespit altyapısı** aşağıdaki seçenekleri yapılandırmanızı sağlar:

- Tarama Dışı Bırakılanlar
- Gelişmiş seçenekler
- Ağ trafiği tarayıcısı

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

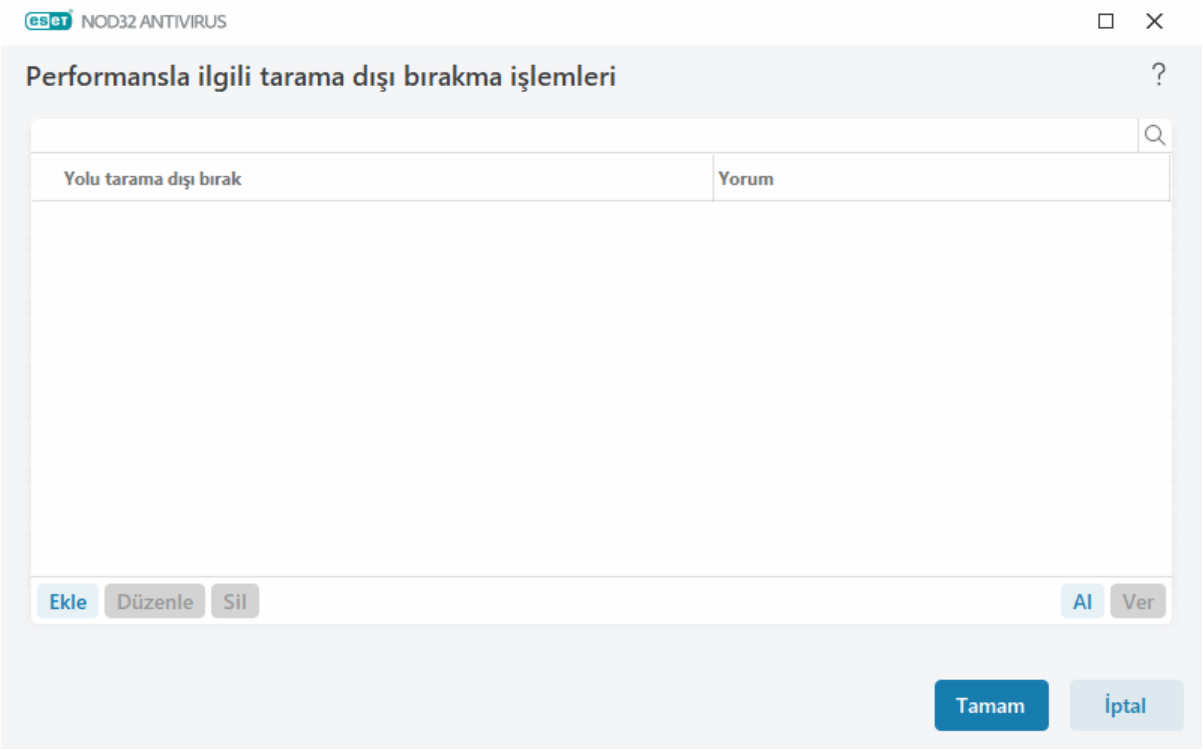
Performansla ilgili tarama dışı bırakma işlemleri, dosya ve klasörleri tarama dışı bırakmanıza olanak tanır.

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 > **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

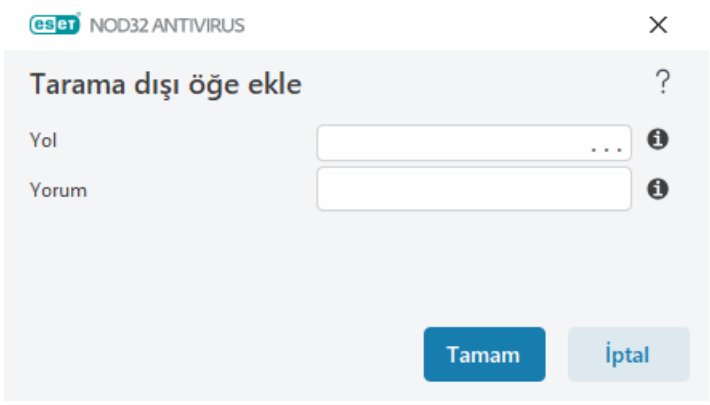
- **Ekle** – Nesneleri algılama dışında bırakır.
- **Düzenle** – Seçili girişleri düzenlemenize olanak tanır.
- **Sil** - Seçilen girişleri kaldırır (birden çok giriş seçmek için CTRL tuşuna basıp tıklayın).

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

- Üst/alt düğmeler kullanılarak tarama dışı öğelerin öncelik düzeyini ayarlama seçeneği yoktur.
- 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.

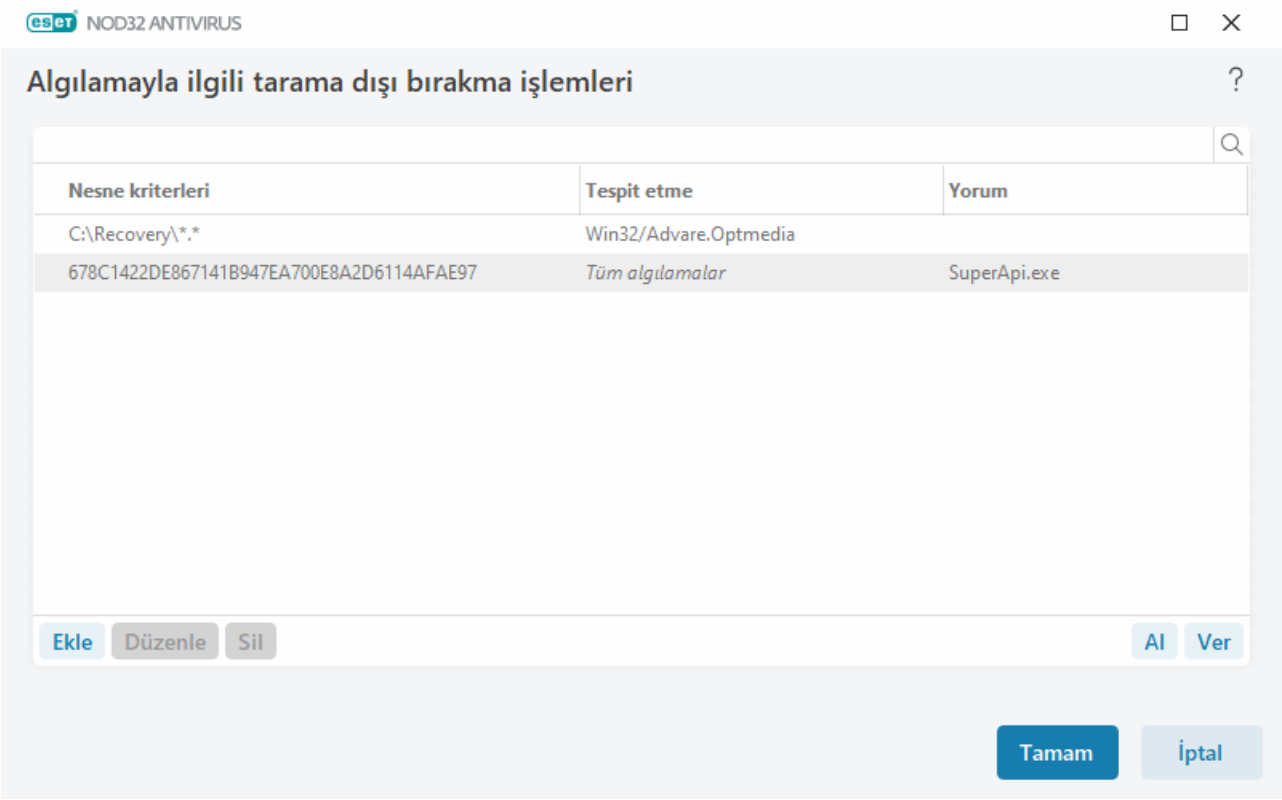
Algılamayla ilgili tarama dışı bırakma işlemleri

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 > **Algılama altyapısı** > **Tarama Dışı Bırakılanlar** > **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** > **Karantina**'yı tıkladıktan sonra karantinaya alınan dosyayı çift tıklayarak ve içerik menüsünden **Geri yükle ve tarama dışında bırak**'ı seçerek.

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

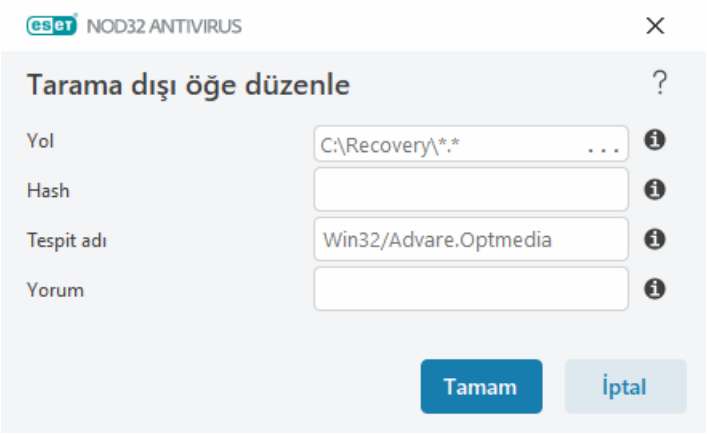
hariç tutar.

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 NOD32 Antivirus 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.

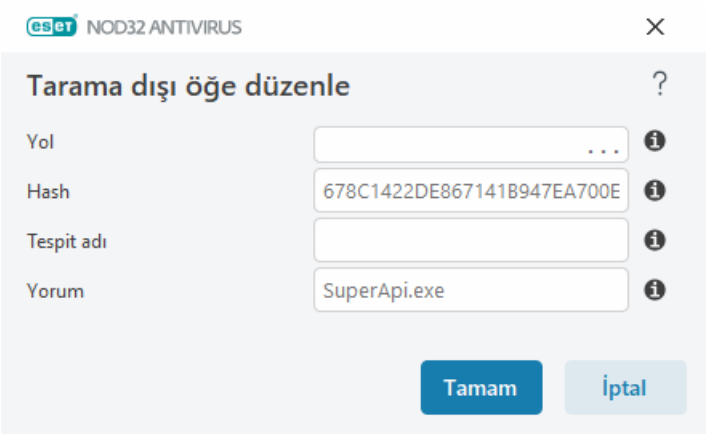
Tarama dışı bırakılan yol biçimi bölümüne de bakın.



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 NOD32 Antivirus 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 **Araçlar** > **Günlük dosyaları**'nı tıklayın.
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.

Algılama altyapısı gelişmiş seçenekleri

AMSI üzerinden gelişmiş taramayı etkinleştir; PowerShell komut dosyalarının, Windows Script Host tarafından yürütülen komut dosyalarının ve AMSI SDK'sı kullanılarak taranan verilerin taranmasını sağlayan Microsoft Antimalware Scan Arabirimi aracıdır.

Ağ trafiği tarayıcısı

Ağ trafiği tarayıcısı, birden çok gelişmiş zararlı yazılım tarama tekniğini entegre eden uygulama protokolleri için zararlı yazılım koruması sağlar. Ağ trafiği tarayıcısı, internet tarayıcısından veya e-posta istemcisinden bağımsız olarak HTTP(S), POP3(S) ve IMAP(S) protokollerini otomatik olarak tarar. Ağ trafiği tarayıcısını Gelişmiş ayarlar > **Tespit altyapısı** > **Ağ trafiği tarayıcısı**'nda etkinleştirebilir/devre dışı bırakabilirsiniz.

Ağ trafiği tarayıcısını etkinleştir - Bu seçeneği devre dışı bırakırsanız HTTP(S), POP3(S) ve IMAP(S) protokolleri taranmaz. Aşağıdaki ESET NOD32 Antivirus özelliklerin Ağ trafiği tarayıcısının etkinleştirilmesini gerektirdiğini unutmayın:

- Web erişimi koruması
- SSL/TLS
- Kimlik Avı koruması
- E-posta istemci koruması

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 NOD32 Antivirus, 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 NOD32 Antivirus 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 NOD32 Antivirus 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® gelişmiş ayarlarına erişmek için Gelişmiş ayarlar > **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 NOD32 Antivirus 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) – Otomatik olarak gönderilen 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.

Kötü amaçlı yazılım taramaları

Tarama profilleri için tarama parametrelerini yapılandırmanıza olanak tanıyan **Zararlı yazılım taramaları** bölümüne Gelişmiş ayarlar > **Tespit altyapısı** > **Zararlı yazılım taramaları** bölümünden erişilebilirsiniz.

İsteğe bağlı tarama

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 profilini seçtikten sonra aşağıdaki seçenekleri yapılandırabilirsiniz:

Tarama hedefleri - Yalnızca belirli bir hedefi veya hedef grubunu taramak isterseniz **Tarama hedefleri**'nin yanındaki **Düzenle**'yi tıklayabilir ve klasör (ağaç) yapısından bir seçenek belirleyebilirsiniz. Daha fazla bilgi için Tarama hedefleri'ne bakın.

İsteğe bağlı koruma ve makine öğrenimi koruması - Her tarama profili için raporlama ve koruma düzeylerini yapılandırabilirsiniz. Varsayılan olarak, tarama profilleri Gerçek zamanlı dosya sistemi koruması'nda tanımlananla aynı ayarları kullanır. Özel raporlama ve koruma düzeylerini yapılandırmak için **Gerçek zamanlı koruma ayarlarını kullan** seçeneğinin yanındaki açma/kapama düğmesini devre dışı bırakın. Raporlama ve koruma düzeylerinin ayrıntılı bir açıklaması için Korumalar'a bakın.

ThreatSense - Kontrol etmek istediğiniz dosya uzantıları ve kullanılan tespit yöntemleri gibi gelişmiş ayar seçenekleri. Daha fazla bilgi için ThreatSense bölümüne bakın.

Tarama profilleri

ESET NOD32 Antivirus 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 > **Tespit altyapısı** > **Zararlı yazılım taramaları** > **İsteğe bağlı tarama** > **Profil listesi** > **Düzenle**'yi açın. **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 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.

Boşta durumu taraması

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

Boşta durumu taraması

Bu özelliği etkinleştirmek için **Boşta durumu taramasını etkinleştir** seçeneğinin yanındaki açma/kapama düğmesini 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 açma/kapama düğmesini etkinleştirerek geçersiz kılabilirsiniz.

Bilgisayar tarama çıktısını Günlük dosyaları bölümüne kaydetmek için Gelişmiş Ayarlar'da **Günlük kaydını etkinleştir** seçeneğinin yanındaki açma/kapama düğmesini etkinleştirin (ana program penceresinden **Araçlar** > **Günlük dosyaları** seçeneğini tıklayın, **Günlük** açılır menüsünden **Bilgisayar taraması**'nı seçin).

Boşta durumunun algılanması

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

ThreatSense - Kontrol etmek istediğiniz dosya uzantıları ve kullanılan tespit yöntemleri gibi gelişmiş ayar seçenekleri. Daha fazla bilgi için ThreatSense bölümüne bakın.

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 tetiklemelerini etkinleştirmek veya devre dışı bırakmak için her bir ilgili durumun açma/kapama düğmesini kullanın.

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** > **Zamanlayıcı** bölümüne gidin, **Başlangıçta otomatik dosya denetimi**'ni ve **Düzenle**'yi tıklayın. Son adımda Başlangıçta otomatik dosya denetimi penceresi görünür. Zamanlayıcı görevi oluşturma ve yönetme ile ilgili ayrıntılı talimatlar için bkz.Yeni görev oluşturma.

ThreatSense - Kontrol etmek istediğiniz dosya uzantıları ve kullanılan tespit yöntemleri gibi gelişmiş ayar seçenekleri. Daha fazla bilgi için ThreatSense bölümüne bakın.

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:

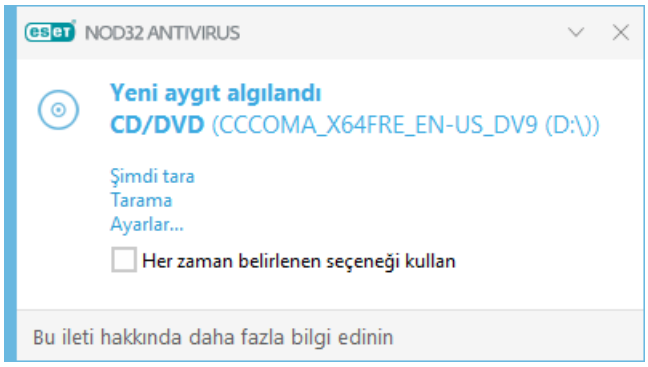
- **Boştayken** – Görev yalnızca sistem boştayken gerçekleştirilir,
- **En düşük** – sistem yüklemesi olası en düşük düzeyde olduğunda,
- **Düşük** – düşük sistem yüklemesinde,

- **Normal** – ortalama sistem yüklemesinde.

Çıkarılabilir medya

ESET NOD32 Antivirus, 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 Gelişmiş ayarlar > **Tespit altyapısı** > **Zararlı yazılım taramaları** > **Çıkarılabilir medya** bölümünde **Tarama seçeneklerini göster** ayarı seçildiğinde aşağıdaki iletişim kutusu gösterilir:



Bu iletişim kutusu için seçenekler:

- **Şimdi tara** – Bu seçenek, çıkarılabilir medyanın taranması işlemini başlatır.
- **Tarama** - Çıkarılabilir medya taranmayacak.
- **Ayarlar** – Gelişmiş ayarları açar.
- **Her zaman belirlenen seçeneği kullan** – Bu seçenek belirlendiğinde, çıkarılabilir medyanın her takılışında aynı eylem gerçekleştirilir.

Ayrıca, ESET NOD32 Antivirus, 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> **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.

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 > **Tespit altyapısı** > **Zararlı yazılım taramaları** > **Belge koruması**'na gidin ve **Belge korumasını etkinleştir**'in yanındaki açma/kapama düğmesini tıklayın.

ThreatSense - Kontrol etmek istediğiniz dosya uzantıları ve kullanılan tespit yöntemleri gibi gelişmiş ayar seçenekleri. Daha fazla bilgi için ThreatSense bölümüne bakın.

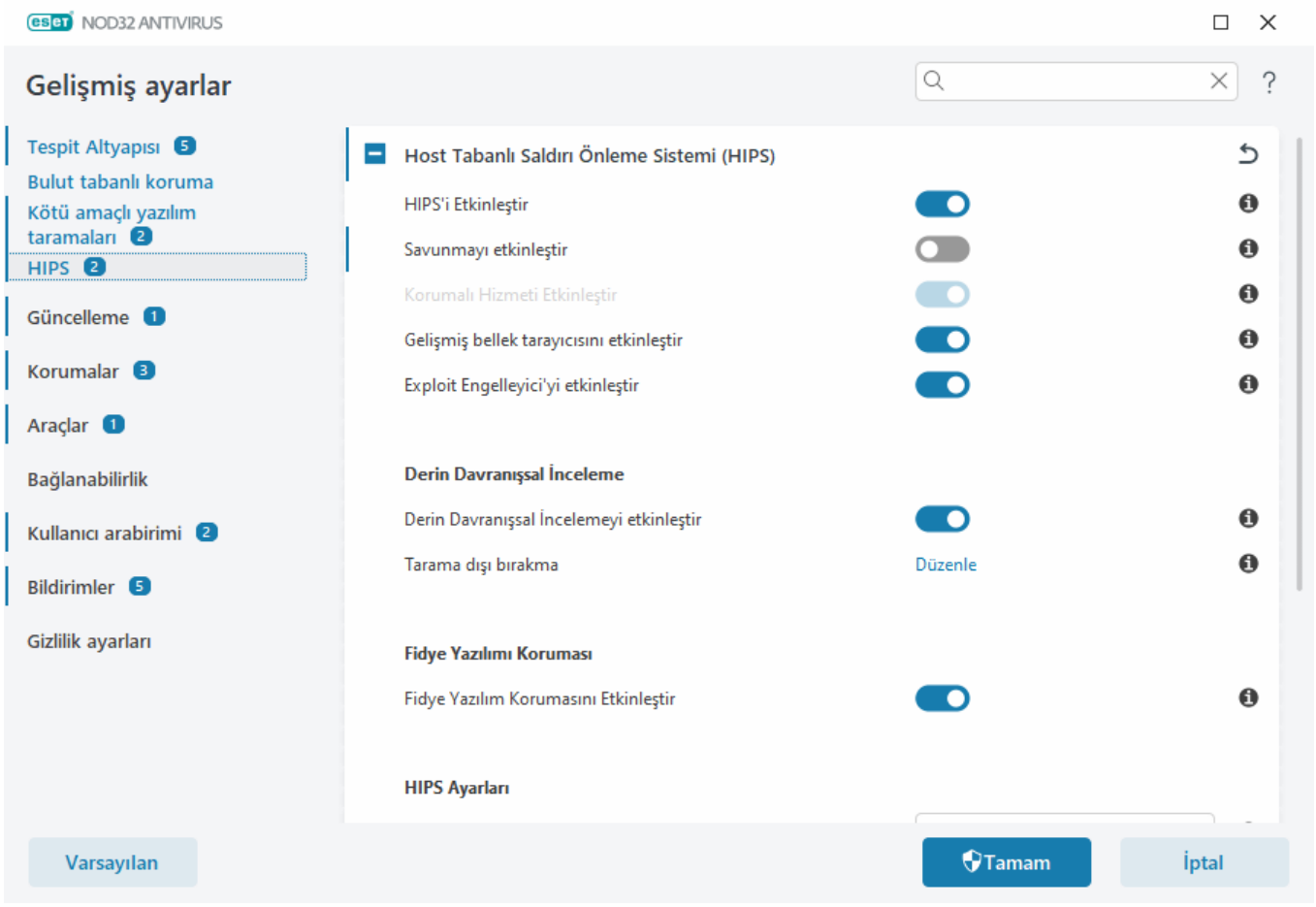
Bu özellik, Microsoft Antivirus API kullanan uygulamalar (ör. Microsoft Office 2000 ve üzeri veya Microsoft Internet Explorer 5.0 ve üzeri) tarafından etkinleştirilir.

HIPS - Host Tabanlı Saldırı Önleme Sistemi (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.

Host Tabanlı Saldırı Önleme Sistemi (HIPS) ayarlarını Gelişmiş ayarlar > **Tespit altyapısı** > **Host Tabanlı Saldırı Önleme Sistemi (HIPS)** > **Host Tabanlı Saldırı Önleme Sistemi (HIPS)** bölümünde yapılandırabilirsiniz. HIPS durumu (etkin/devre dışı), ESET NOD32 Antivirus ana program penceresinde > **Ayarlar** > **Bilgisayar koruması** içinde gösterilir.



Host Tabanlı Saldırı Önleme Sistemi (HIPS)

HIPS'i etkinleştir – HIPS, ESET NOD32 Antivirus ürününde varsayılan olarak etkindir. HIPS'i kapatmak Exploit Engelleyici gibi diğer HIPS özelliklerini devre dışı bırakır.

Kendini Korumayı etkinleştir – ESET NOD32 Antivirus, 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.

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 taraması dışında bırakılan öğeler

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

Host Tabanlı Saldırı Önleme Sistemi (HIPS) tarama dışı bırakma işlemlerini düzenlemek için Gelişmiş ayarlar > **Tespit altyapısı** > **Host Tabanlı Saldırı Önleme Sistemi (HIPS)** > **Host Tabanlı Saldırı Önleme Sistemi (HIPS)** > **Tarama dışı öğeler** > **Düzenle**'yi açın.

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.

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.

Yüklemenin ardından sürücü listesi boş olur. ESET NOD32 Antivirus listeyi zaman içinde otomatik olarak doldurur.

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).

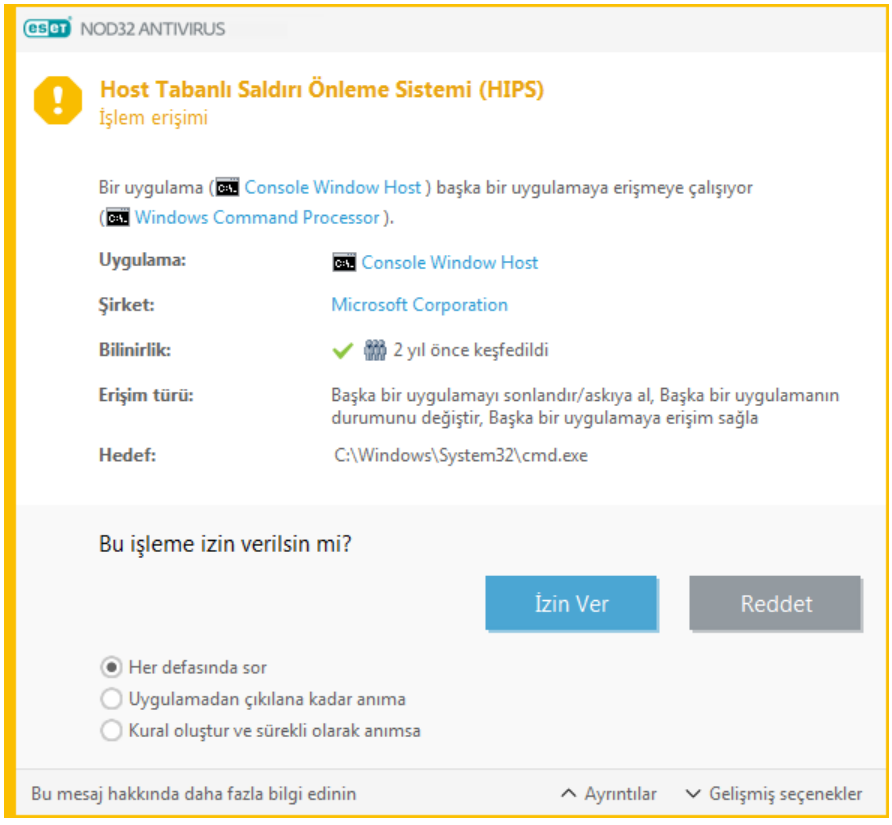
İşlemi hangi uygulamanın tetiklediğini, dosyanın bilinirliğini veya ne tür bir işleme izin vermeniz ya da reddetmeniz istendiğini görmek için aşağıdaki **Ayrıntılar**'ı tıklayın.

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 filtreleme modunu Gelişmiş ayarlar > **Tespit altyapısı** > **Host Tabanlı Saldırı Önleme Sistemi (HIPS)** > **Host Tabanlı Saldırı Önleme Sistemi (HIPS)** bölümünde **Otomatik** olarak değiştirin.



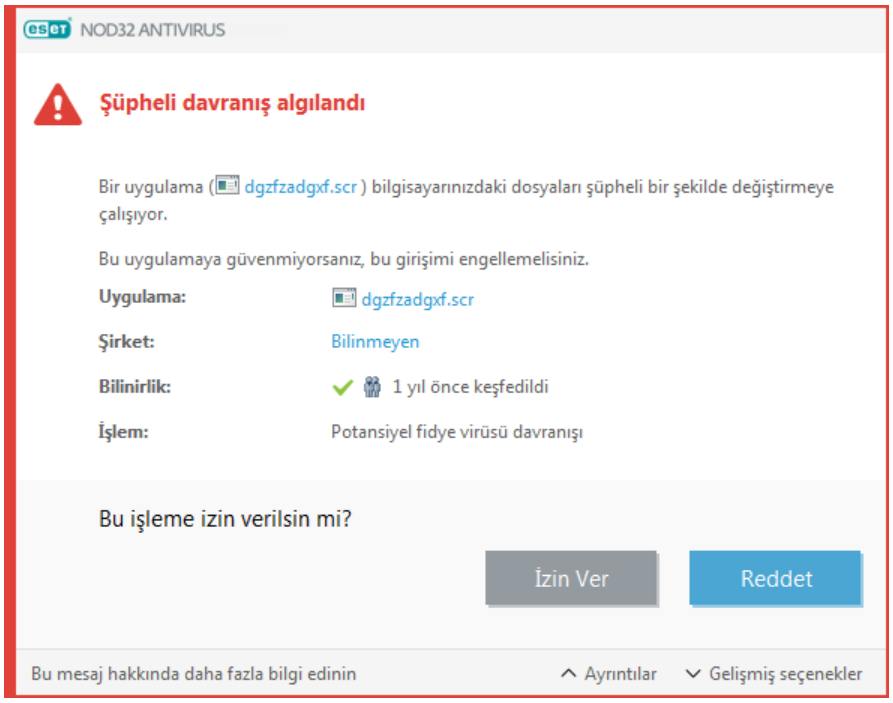
Öğrenme modu sona erdi

Öğrenme modu otomatik olarak kural oluşturur ve kaydeder. Oluşturulan tüm kuralları Host Tabanlı Saldırı Önleme Sistemi (HIPS) kural ayarları bölümünden kontrol edebilirsiniz. Bu mod özellikle HIPS'in ilk yapılandırması için uygundur ancak yalnızca kısa bir süreliğine açık tutulmalıdır. ESET NOD32 Antivirus Kuralları önceden tanımlı parametrelere göre kaydettiği için herhangi bir kullanıcı müdahalesi gerekmez. İşletim sistemi içinde yürütülen gerekli işlemler için tüm kurallar oluşturulduktan sonra güvenlik risklerini önlemek amacıyla **etkileşimli** veya **ilke tabanlı mod** seçeneklerinden birine geçiş yapın.

Ayarları değiştirmek istemiyorsanız bu kararı erteleyebilirsiniz.

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 Host Tabanlı Saldırı Önleme Sistemi (HIPS) işlemleriyle ilgili daha fazla ayrıntı için Host Tabanlı Saldırı Önleme Sistemi (HIPS) kuralı ayarları bölümüne bakın. 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 açma/kapama düğmesini 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.

Bildir - Bir olay tetiklenirse sağ alt köşede küçük bir bildirim penceresi 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 Host Tabanlı Saldırı Önleme Sistemi (HIPS) kurallarının öncelik düzeyini ayarlama seçeneği yoktur.

- 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 açma/kapama düğmesini 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 bildirim penceresi 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 açma/kapama düğmesini etkinleştirin.

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

4. **İleri**'yi tıklayın.

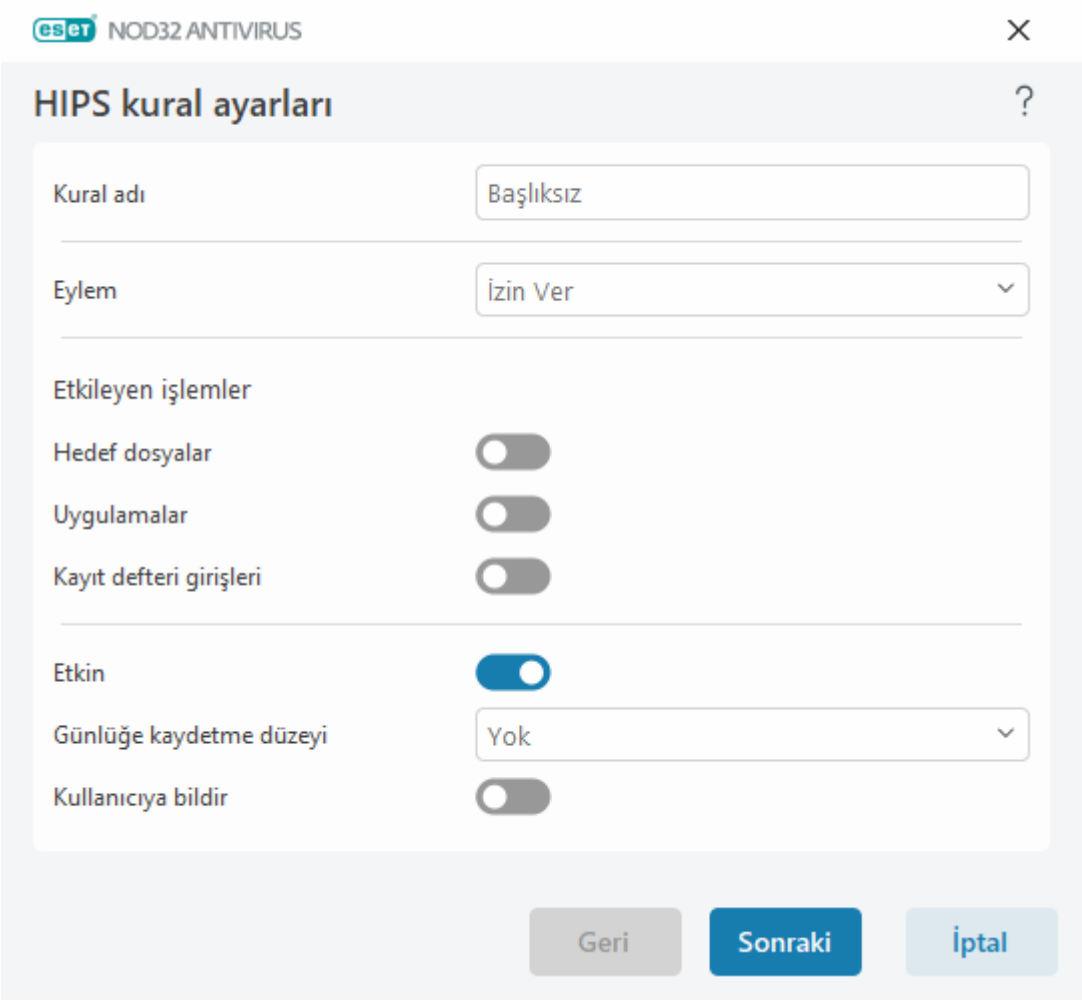
5. Yeni kuralınızı belirlediğiniz uygulamalar üzerinde, seçili uygulama işlemlerinden herhangi birini gerçekleştirmeye çalışan tüm uygulamalar için geçerli kılmak üzere **Kaynak uygulamaları** penceresinde, açılır menüden **Belirli uygulamalar**'ı seçin.

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*

Güncelleme

Güncelleme ayarları seçenekleri Gelişmiş ayarlar > **Güncelleme** bölümünde bulunabilir. Bu bölüm, kullanılan güncelleme sunucuları gibi güncelleme kaynağı bilgilerini ve bu sunucular için kimlik doğrulama verilerini belirtir.

Güncelleme

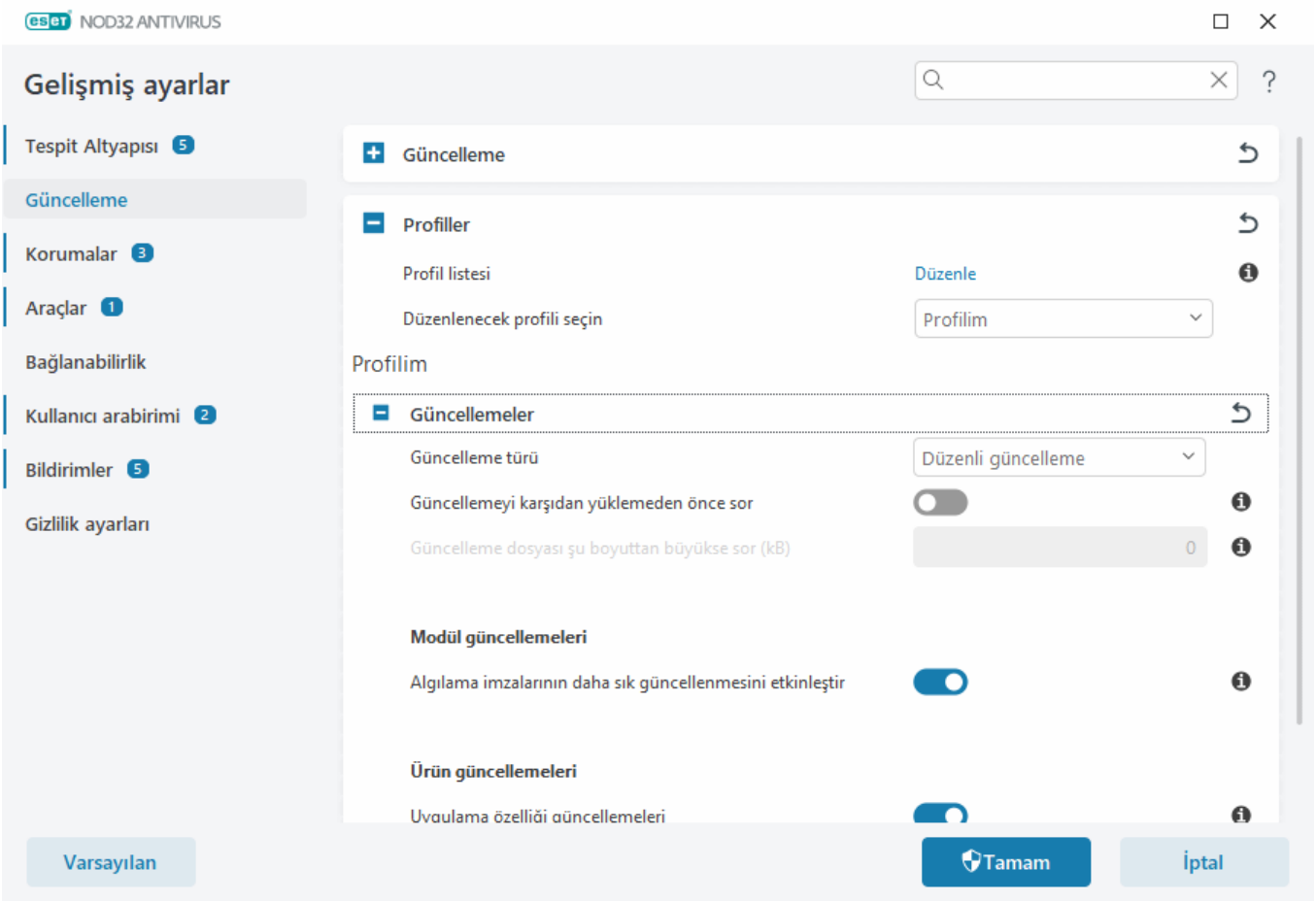
Şu anda kullanımda olan güncelleme profili **Varsayılan güncelleme profilini seç** açılır menüsünde gösterilir.

Yeni bir profil oluşturmak için Güncelleme profilleri bölümüne bakın.

Tespit altyapısını veya modül güncellemelerini indirmek istediğinizde sorun yaşıyorsanız geçici güncelleme dosyalarını/ön belleği temizlemek için **Güncelleme önbelleğini temizle**'nin yanındaki **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 NOD32 Antivirus ürününün yeni sürümlerini otomatik olarak yükler.

Bağlantı seçenekleri

Güncellemeleri indirmek için proxy sunucusu kullanmak üzere Bağlantı seçenekleri bölümüne bakın.

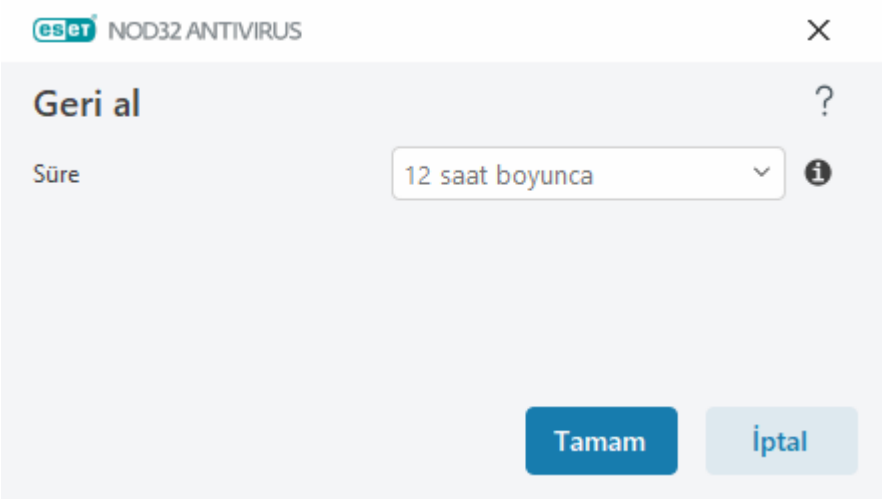
Geri almayı güncelle

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 NOD32 Antivirus, 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.

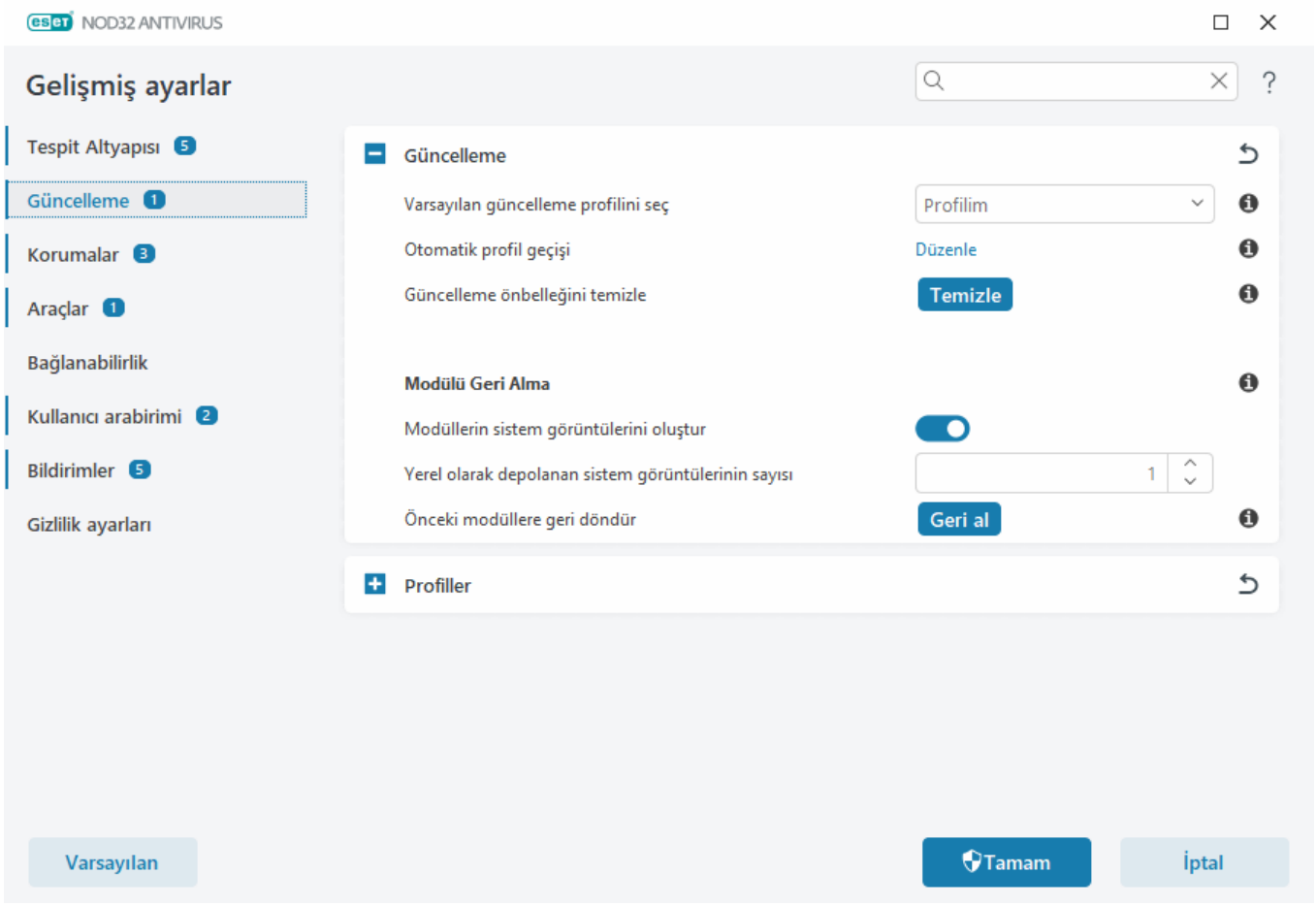
Maksimum sistem görüntüsü sayısına ulaşıldıysa (örneğin üç), en eski sistem görüntüsü 48 saatte bir yeni bir sistem görüntüsüyle değiştirilir. ESET NOD32 Antivirus, tespit altyapısı ve program modülü güncelleme sürümlerini en eski sistem görüntüsüne döndürür.

Gelişmiş ayarlar > **Güncelleme** > **Güncelleme** bölümünde **Geri al** seçeneğini tıklarsanız **Süre** açılır menüsünden tespit 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.

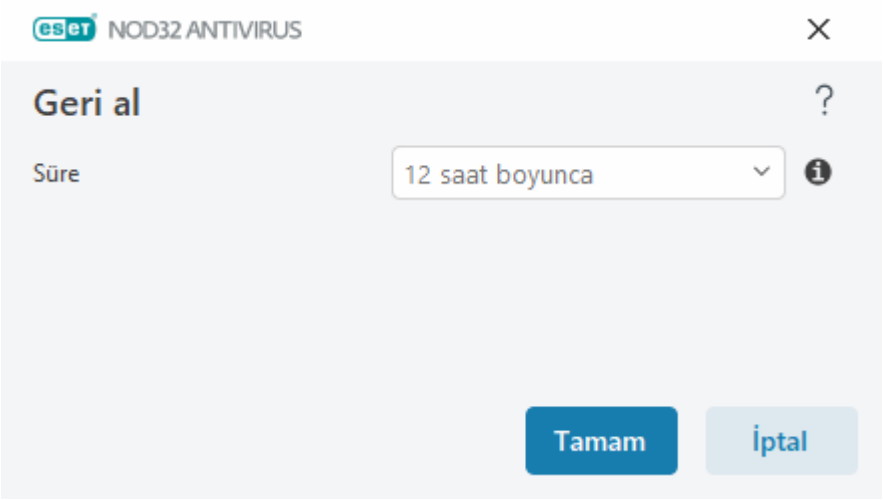
Geri alma gerçekleştirilirse **Geri al** düğmesi **Güncellemelere izin ver** olarak değişir. **Güncellemeleri askıya al** açılır menüsünden seçilen zaman aralığı süresince hiçbir güncellemeye izin verilmez. Tespit altyapısı sürümü kullanılabilir en eski sürüme geri döndürülür ve yerel bilgisayar dosya 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

Gelişmiş ayarlar > **Güncelleme** > **Güncelleme** bölümünde **Geri al** seçeneğini tıklarsanız **Süre** açılır menüsünden tespit 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 profilinin proxy sunucusu kurulum seçeneklerine erişmek için Gelişmiş ayarlar > **Güncelleme** > **Profiller** > **Güncellemeler** > **Bağlantı seçenekleri**'ni açın. Açılır menüden **Proxy modu**'nu tıklayın ve aşağıdaki üç seçenekten birini belirleyin:

- Proxy sunucu kullanma
- Proxy sunucuyla bağlan
- Genel proxy sunucu ayarlarını kullan

Halihazırda Gelişmiş ayarlar > **Bağlanabilirlik** > **Proxy sunucu**'da belirtilmiş olan proxy sunucu yapılandırması seçeneklerini kullanmak için **Genel proxy sunucu ayarlarını kullan**'ı işaretleyin.

ESET NOD32 Antivirus uygulamasını güncellemek için proxy sunucusu kullanılmayacağını belirtmek üzere **Proxy sunucu kullanma** seçeneğini belirleyin.

Şu durumlarda **Proxy sunucu üzerinden bağlan** seçeneği belirlenmelidir:

- ESET NOD32 Antivirus ürünü Gelişmiş ayarlar > **Bağlanabilirlik** bölümünde tanımlanandan farklı bir proxy sunucu kullanılarak 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 NOD32 Antivirus 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.

Korumalar

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

Korumaları ayrıntılı olarak yapılandırmak için Gelişmiş ayarlar > **Korumalar**'ı açın.

Korumalar'da yapılacak değişiklikler yalnızca deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. Ayarların yanlış yapılandırılması, koruma düzeyinin düşmesine neden olabilir.

Bu bölümde:

- Tespit yanıtları
- Raporlama ayarları
- Koruma ayarları

Tespit yanıtları

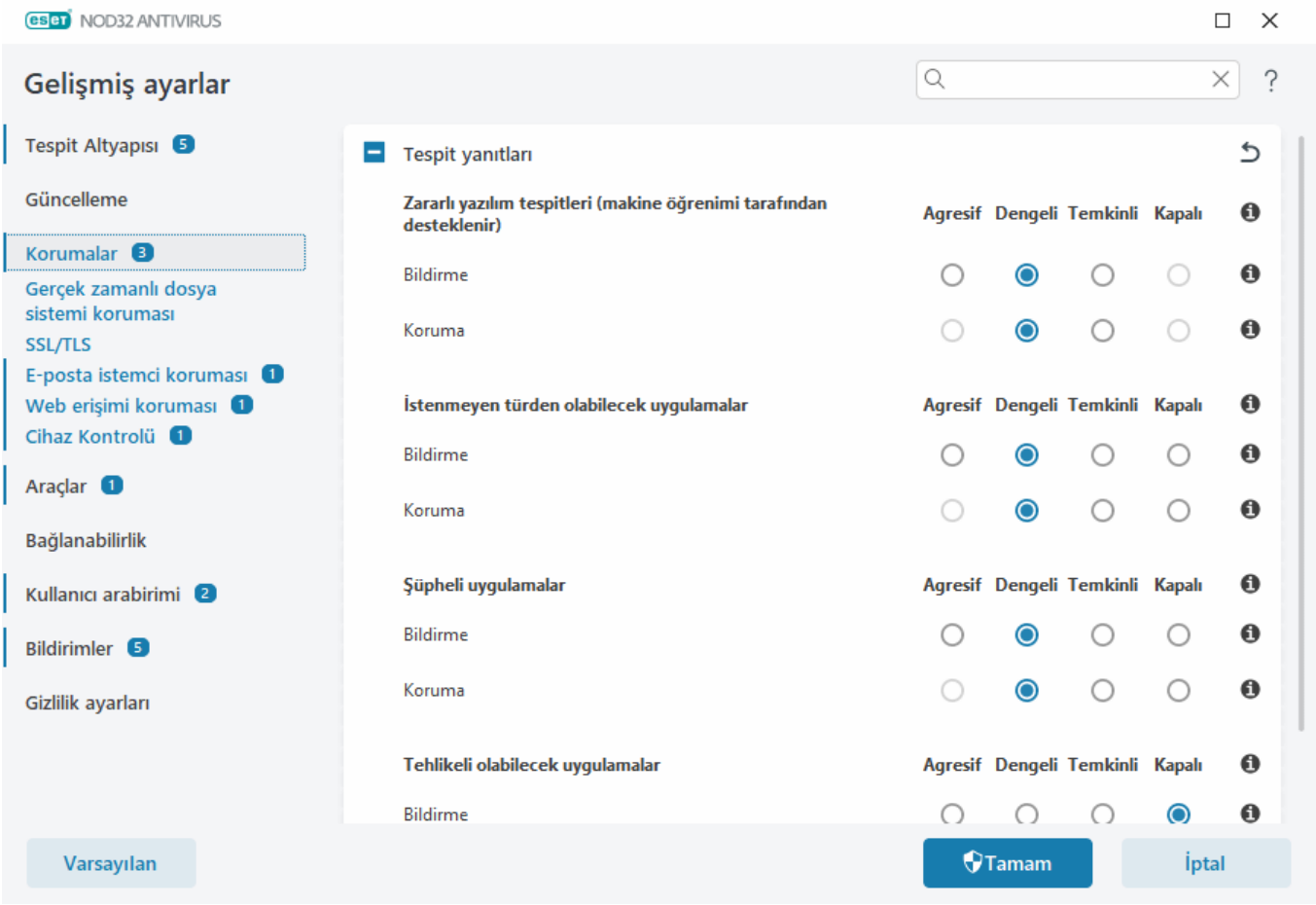
Tespit yanıtları, aşağıdaki kategoriler için raporlama ve koruma düzeylerini yapılandırmanıza olanak tanır:

- **Zararlı yazılım tespitleri (makine öğrenimi tarafından desteklenir** - Bir bilgisayar virüsü, bilgisayarınızda mevcut olan dosyaların önüne veya sonuna eklenen kötü amaçlı kodun bir 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 artık, makine öğrenimine dayalı olarak tespiti iyileştiren gelişmiş bir koruma katmanı olarak tespit altyapısının bir parçası olarak sunulmaktadır. Bu koruma türüyle ilgili daha fazla bilgi için Sözlüğe başvurun.

Raporlama ayarları

Bir algılama görüldüğünde (ör. bir tehdit bulunduğunda ve kötü amaçlı yazılım olarak sınıflandırıldığında), bilgiler Algılama günlüğüne kaydedilir ve ESET NOD32 Antivirus ürününde yapılandırılmış olması halinde Masaüstü bildirimleri gösterilir.

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

1.Zararlı yazılım tespitleri

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 NOD32 Antivirus 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

*Önerilmez.

Ürün sürümü, program modülü sürümleri ve yapı tarihlerini belirleyin

1. **Yardım ve destek** > **ESET NOD32 Antivirus 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.

• 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 NOD32 Antivirus 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

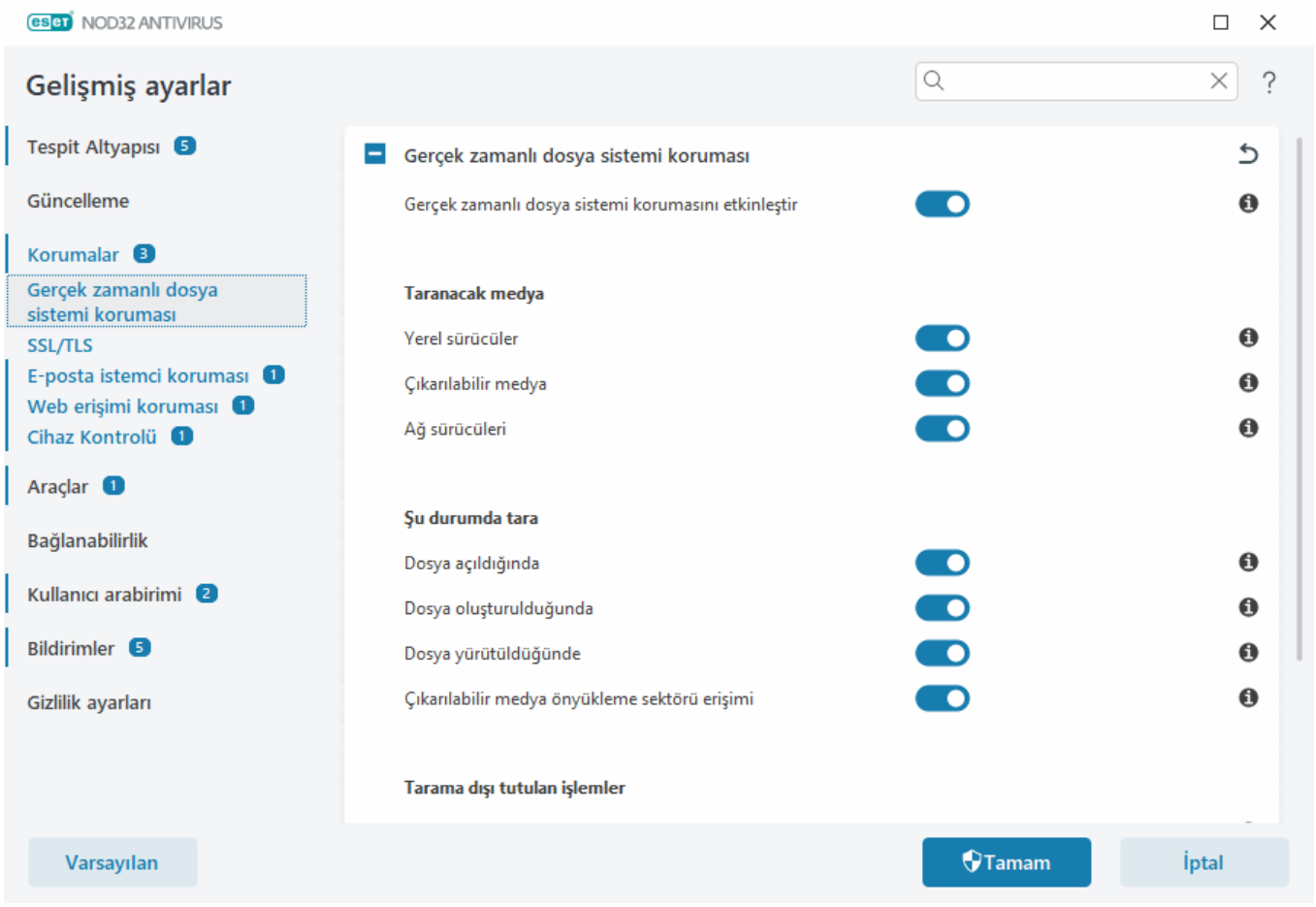
CATEGORY olarak sınıflandırılan bir nesne bildirildiğinde program nesneyi engeller ve ardından temizler, siler ya da Karantinaya alır.

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.

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. **Gerçek Zamanlı Dosya Sistemi Korumasını etkinleştir** seçeneğinin Gelişmiş ayarlar > **Korumalar** > **Gerçek zamanlı dosya sistemi koruması** > **Gerçek zamanlı dosya sistemi koruması**'nda 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 aracında **Önyükleme kesimleri/UEFI** seçeneğini etkin halde bırakın.

Tarama dışı tutulan işlemler

Tarama dışı bırakılan işlemler'e bakın.

ThreatSense

Gerçek zamanlı sistem koruması her medya türünü kontrol eder ve bir dosyaya erişme gibi çeşitli sistem olayları tarafından tetiklenir. **ThreatSense** teknolojisi tespit yöntemleri kullanıldığında (ThreatSense 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 ayarı değiştirmek için Gelişmiş ayarlar > **Korumalar** > **Gerçek zamanlı dosya sistemi koruması**'nı açın. **ThreatSense** > **Diğer** öğesine tıklatın ve **Akıllı optimizasyonu etkinleştir** seçeneğinin işaretini seçin veya seçimini kaldırın.

Gerçek zamanlı dosya sistemi koruması, Ek ThreatSense parametreleri'ni yapılandırmanıza da olanak tanır.

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.

Gelişmiş ayarlar > **Korumalar** > **Gerçek zamanlı dosya sistemi koruması** > **Gerçek zamanlı dosya sistemi koruması** > **Tarama dışı tutulan işlemler**'de tarama dışında bırakılan işlemlerin listesine yürütülebilir dosyalar

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 NOD32 Antivirus 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 NOD32 Antivirus 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**.

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 NOD32 Antivirus Yüklendikten sonra, kullanıcılara en üst düzeyde sistem güvenliği sağlamak için tüm ayarlar en iyi duruma getirilir. Varsayılan ayarları geri yüklemek için, Gelişmiş ayarlar > **Korumalar** > **Tespit yanıtları**'nın yanındaki simgesini tıklayın.

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 > **Korumalar** > **Gerçek zamanlı dosya sistemi koruması**'nı açın.

Gerçek zamanlı koruma sızıntıları algılamıyor ve temizlemiyorsa

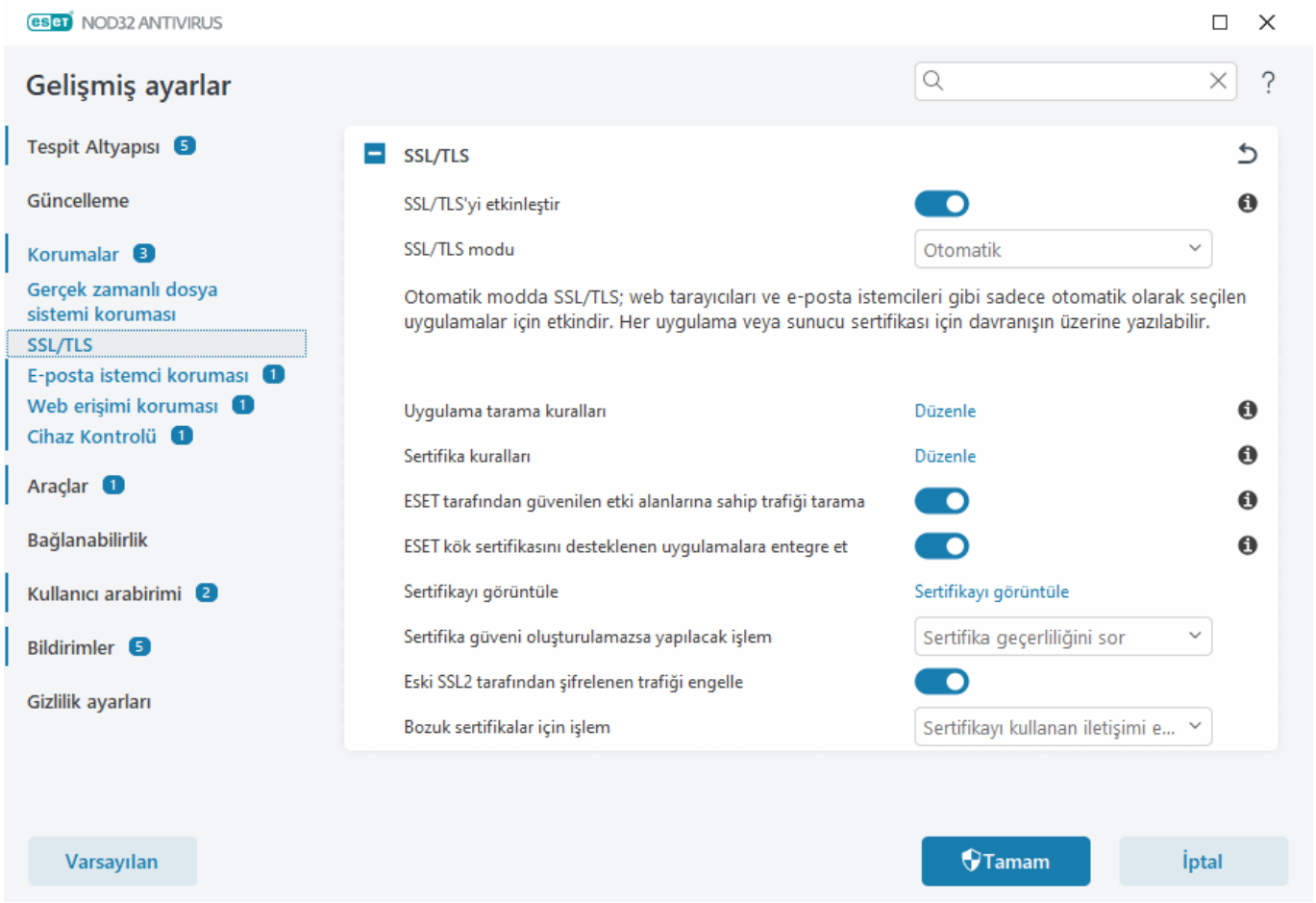
Bilgisayarınızda başka antivirüs programları yüklü olmadığından emin olun. İki antivirus programı aynı anda yüklüyse birbirleriyle çakışabilir. ESET'i kurmadan önce sisteminizdeki diğer antivirüs programlarını kaldırmanızı öneririz.

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.

SSL/TLS

ESET NOD32 Antivirus, SSL protokolünü kullanan iletişim tehditlerini 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 ayarlarını düzenlemek için Gelişmiş ayarlar > **Korumalar** > **SSL/TLS**'yi açın.



SSL/TLS'yi **etkinleştir** - Devre dışı bırakılırsa ESET NOD32 Antivirus SSL/TLS üzerinden iletişimi taramaz.

SSL/TLS modu aşağıdaki seçeneklerde kullanılabilir:

Filtreleme modu	Açıklama
Otomatik	Varsayılan mod sadece, web tarayıcıları ve e-posta istemcileri gibi ilgili uygulamaları tarar. İletişimin tarandığı uygulamaları seçerek bunu geçersiz kılabilirsiniz.
Etkileşimli	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 tabanlı	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 bir sertifikası olduğu halde güvenilir olarak işaretlenmiş (güvenilir sertifikalar listesindedir) bir sunucuya erişim sağladığınızda sunucuyla iletişime izin verilir ve iletişim kanalı içeriği filtrelenir.

Uygulama tarama kuralları - Belirli uygulamalar için ESET NOD32 Antivirus davranışını özelleştirmenize olanak tanır.

Bilinen sertifikalar listesi - Belirli SSL sertifikaları için ESET NOD32 Antivirus davranışını özelleştirmenizi sağlar.

ESET tarafından güvenilen alanları içeren trafiği tarama - Etkinleştirildiğinde, güvenilen etki alanlarıyla iletişim tarama dışında bırakılır. ESET tarafından yönetilen yerleşik bir beyaz liste, bir etki alanının güvenilirliğini belirler.

ESET kök sertifikasını desteklenen uygulamalara entegre et – SSL iletişiminin tarayıcılarınızda/e-posta istemcilerinizde düzgün bir şekilde çalışması için ESET kök sertifikasının bilinen kök sertifikalar (yayımcılar) listesine eklenmesi önemlidir. Etkinleştirildiğinde ESET NOD32 Antivirus, 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 güveni oluşturulamazsa yapılacak işlem - Bazı durumlarda, bir web sitesi sertifikası Güvenilen Kök Sertifika Yetkilileri (TRCA) deposu kullanılarak doğrulanamaz (örneğin, süresi dolmuş sertifika, güvenilmeyen sertifika, ayrıştırılabilen ancak sertifikayı doğru şekilde imzalamayan belirli bir etki alanı veya imza için geçerli olmayan sertifika). Yasal web siteleri her zaman güvenilir sertifikalar kullanır. Güvenilir sertifika sağlamıyorlarsa bu, bir saldırganın iletişiminizin şifresini çözdüğü veya web sitesinin teknik sorunlar yaşadığı anlamına gelebilir.

Sertifika geçerliliğini sor seçeneği (varsayılan olarak seçilidir) işaretlenirse şifreli bir iletişim kurulduğunda kullanıcıdan yapılacak işlemi seçmesi istenir. 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 işaretleyerek güvenilmeyen sertifikayı kullanan siteyle olan şifreli bağlantıyı her zaman sonlandırabilirsiniz.

Eski SSL2 ile şifrelenen trafiği engelle - SSL protokolünün eski bir sürümünü kullanan iletişim otomatik olarak engellenir.

Bozuk sertifikalar için yapılacak işlem - Bozuk sertifika, sertifikanın ESET NOD32 Antivirus tarafından tanınmayan veya zarar görmüş olarak kabul edilen bir biçim kullandığı anlamına gelir (örneğin, rastgele verilerle üzerine yazılır). Bu durumda **Sertifikayı kullanan iletişimi engelle** öğesini seçili bırakmanızı öneririz. **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"

Uygulama tarama kuralları

Uygulama taraması kuralları; belirli uygulamalar için ESET NOD32 Antivirus davranışını özelleştirmek ve **SSL/TLS modu Etkileşimli modda** olduğunda seçilen işlemleri hatırlamak için kullanılabilir. Liste, Gelişmiş ayarlar > **Korumalar** > **SSL/TLS** > **Uygulama taraması kuralları** > **Düzenle**'de görüntülenebilir ve düzenlenebilir.

Uygulama taraması kuralları penceresi şunlardan oluşur:

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.

Sertifika kuralları

Sertifika kuralları, belirli SSL sertifikaları için ESET NOD32 Antivirus davranışını özelleştirmek ve **SSL/TLS modu Etkileşimli moddayken**seçilen eylemleri hatırlamak üzere kullanılabilir. Liste, Gelişmiş ayarlar > **Korumalar** > **SSL/TLS** > **Sertifika kuralları** > **Düzenle**'de görüntülenebilir ve düzenlenebilir.

Sertifika kuralları penceresi şunlardan oluşur:

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.

Şifrelenmiş ağ trafiği

Sisteminiz SSL/TLS 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 NOD32 Antivirus 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.

İkinci olarak, **SSL/TLS modu Etkileşimli mod** olarak ayarlandıysa her web sitesi için bir iletişim kutusunda trafiği **Tara** veya **Yoksay** seçeneklerinden birini belirlemeniz istenir. Bazı uygulamalar kendi SSL trafiğinin değiştirilmediğini ya da herhangi biri tarafından denetlenmediğini doğrular; bu durumlarda ESET NOD32 Antivirus 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 Sertifika kuralları'nda depolanır.

E-posta istemcisi koruması

E-posta istemci korumasını yapılandırmak için Gelişmiş ayarlar > **Korumalar** > **E-posta istemcisi koruması**'nı açın ve aşağıdaki yapılandırma seçeneklerinden birini belirleyin:

- Posta aktarımı koruması
- Posta kutusu koruması
- ThreatSense

Posta aktarımı koruması

IMAP(S) ve POP3(S) 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 NOD32 Antivirus, 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.
MAPI protokolü taranmaz. Ancak, Microsoft Exchange sunucusuyla iletişim Microsoft Outlook gibi e-posta istemcilerinde entegrasyon modülü tarafından taranabilir.

ESET NOD32 Antivirus, IMAPS (585, 993) ve POP3S (995) protokolleri taramasını da destekler. Bu protokoller sunucu ve istemci arasında bilgilerin aktarılması için şifreli kanal kullanılır. ESET NOD32 Antivirus, iletişimi SSL (Güvenli Yuva Katmanı) ve TLS (Aktarım Katmanı Güvenliği) protokollerini kullanarak denetler.
Şifreli iletişim varsayılan olarak taranır. Tarayıcı ayarlarını görüntülemek için Gelişmiş ayarlar > **Korumalar** > SSL/TLS'yi açın.

Posta aktarımı korumasını yapılandırmak için Gelişmiş ayarlar > **Korumalar** > **E-posta istemci koruması** > **Posta aktarımı koruması**'nı açın.

Posta aktarımı korumasını etkinleştir - Etkinleştirildiğinde, posta aktarımı iletişimi ESET NOD32 Antivirus tarafından taranır.

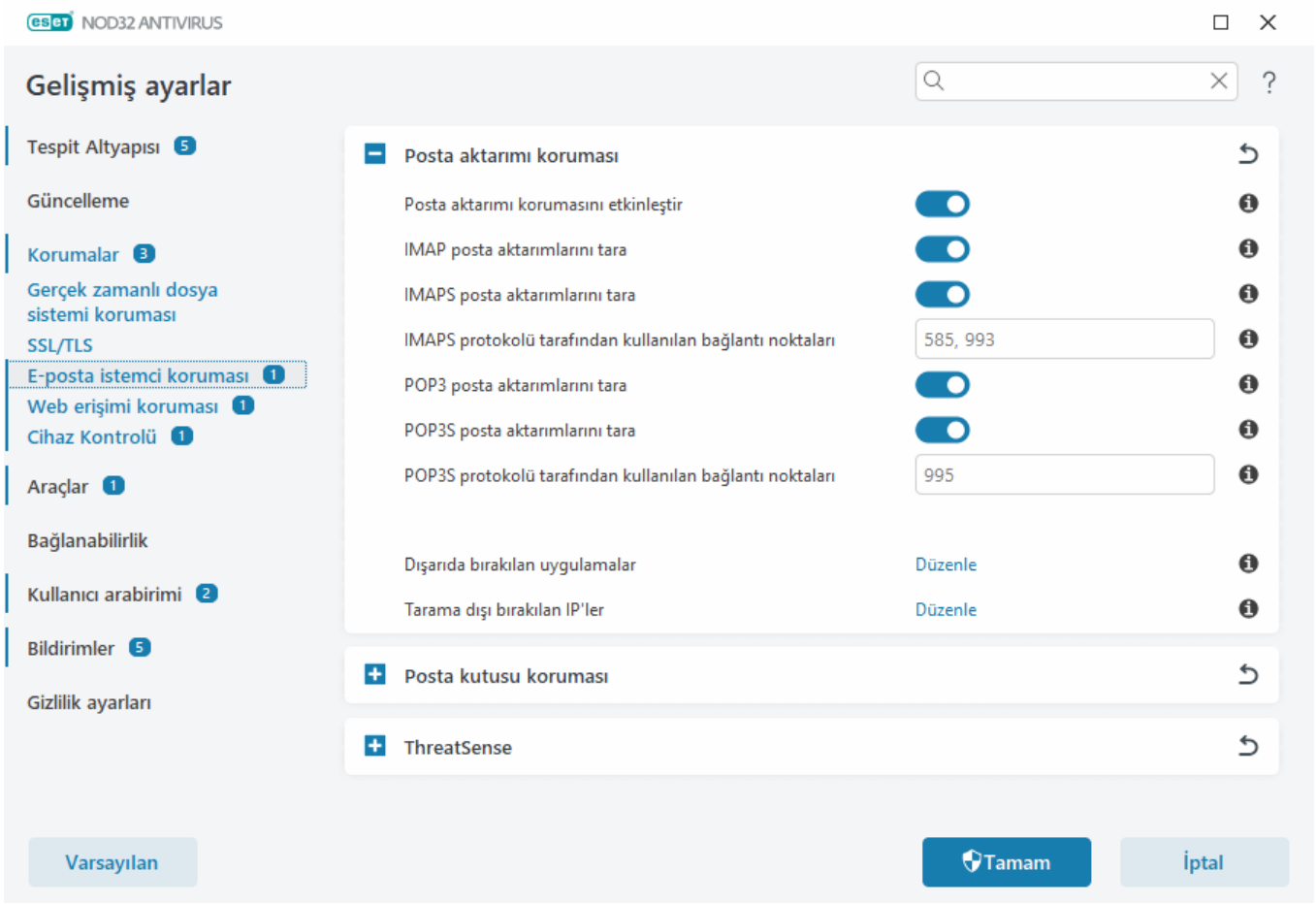
Aşağıdaki seçeneklerin yanındaki açma/kapama düğmesini tıklayarak hangi posta aktarımı protokollerinin taranacağını seçebilirsiniz (varsayılan olarak, tüm protokollerin taranması etkindir):

- **IMAP posta aktarımlarını tara**
- **IMAPS posta aktarımlarını tara**
- **POP3 posta aktarımlarını tara**
- **POP3S posta aktarımlarını tara**

Varsayılan olarak, ESET NOD32 Antivirus standart bağlantı noktalarında IMAPS ve POP3S iletişimini tarar. IMAPS ve POP3S protokolleri için özel bağlantı noktaları eklemek üzere, bunları **IMAPS protokolü tarafından kullanılan bağlantı noktaları** veya **POP3S protokolü tarafından kullanılan bağlantı noktaları**'nın yanındaki metin alanına ekleyin. Birden fazla bağlantı noktası numaraları virgülle ayrılmalıdır.

Tarama dışı bırakılan uygulamalar - Belirli uygulamaların Posta aktarımı koruması tarafından taranmasını engellemenizi sağlar. Web erişimi koruması uyumluluk sorunlarına neden olduğunda bu seçenek kullanışlıdır.

Tarama dışı bırakılan IP'ler - Belirli uzak adresleri Posta aktarımı koruması taramasından hariç tutmanıza olanak tanır. Web erişimi koruması uyumluluk sorunlarına neden olduğunda bu seçenek kullanışlıdır.



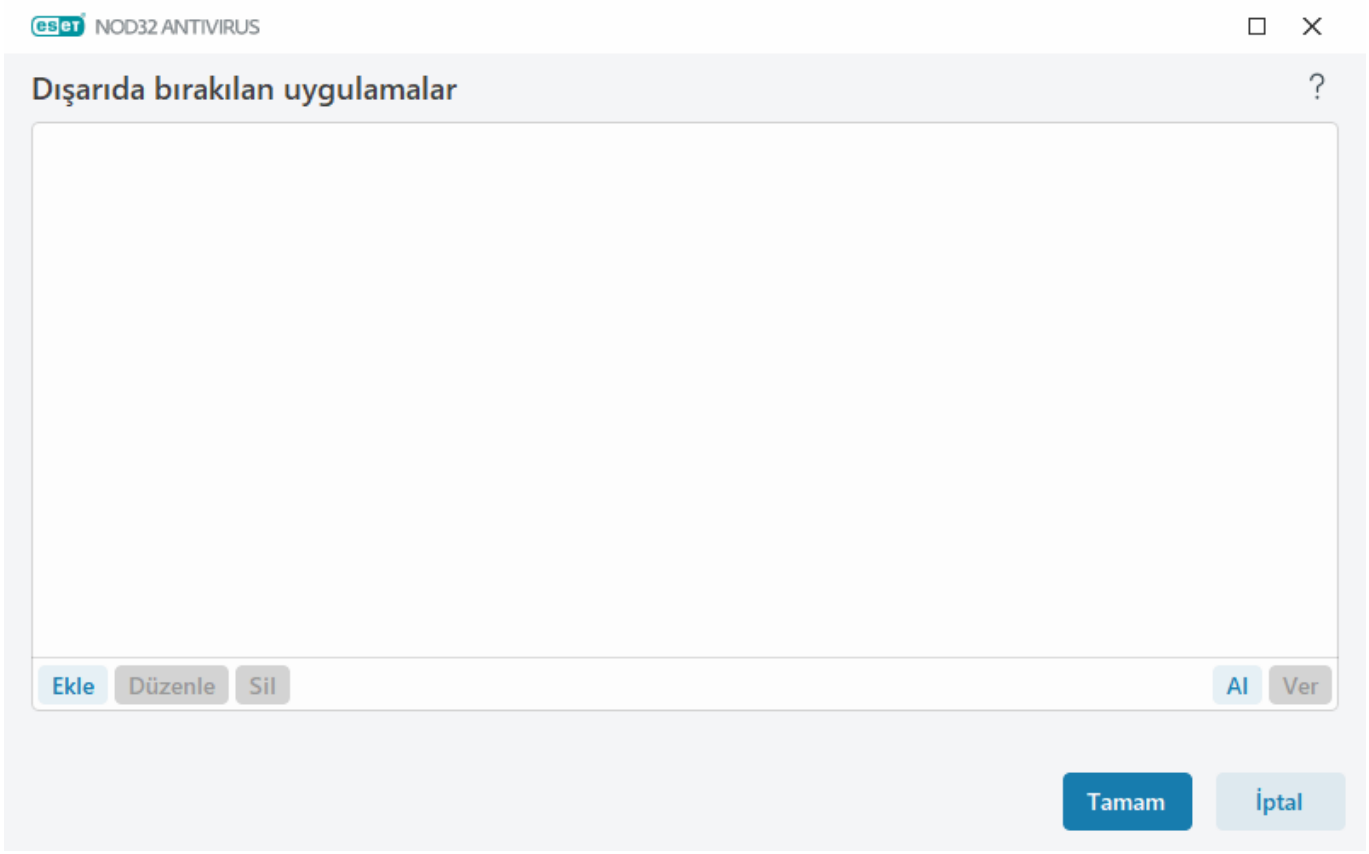
Dışarıda bırakılan uygulamalar

Belirli uygulamalar için iletişim taramasını hariç tutmak üzere bunları listeye ekleyin. Seçili uygulamaların HTTP(S)/POP3(S)/IMAP(S) iletişimi tehditlere karşı denetlenmeyecektir. Bu seçeneğin yalnızca, taranmakta olan iletişimleri düzgün şekilde çalışmayan uygulamalar için kullanılmasını öneririz.

Çalışan uygulama ve hizmetler **Ekle** seçeneğini tıkladığınızda otomatik olarak burada olacaktır. Tarama dışı öğeyi manuel olarak eklemek için **...** seçeneğine tıklayın ve bir uygulamaya gidin.

Düzenle - Listeden seçilen girişleri düzenleyin.

Kaldır - Seçili girişleri listeden kaldırır.



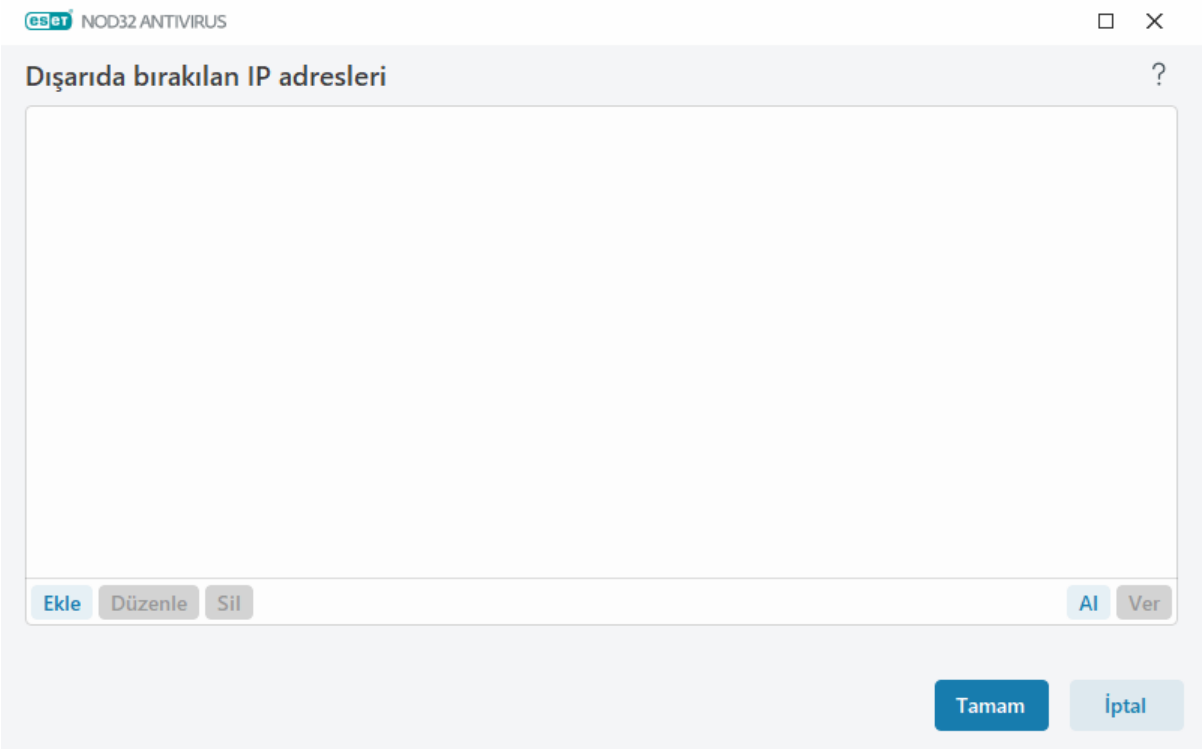
Tarama dışı bırakılan IP'ler

Listedeki girişler tarama dışında bırakılır. Seçili adreslerden/adreslere HTTP(S)/POP3(S)/IMAP(S) iletişimi tehditlere karşı denetlenmez. Bu seçeneği yalnızca güvenilir olduğu bilinen adresler için kullanmanızı öneririz.

Uzak bir noktanın IP adresi/adres aralığı/alt ağını tarama dışı bırakmak için **Ekle** seçeneğini tıklayın.

Seçilen IP adresini değiştirmek için **Düzenle**'yi tıklayın.

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



IP adresleri örnekleri

IPv4 adresi ekle:

Tek adres - Tek bir bilgisayarın IP adresini ekler (örneğin, *192.168.0.10*).

Adres aralığı - Birkaç bilgisayarın IP aralığını belirtmek için başlangıç ve bitiş IP adresini girin (örneğin *192.168.0.1-192.168.0.99*).

Alt ağ - IP adresi ve maske tarafından tanımlanan alt ağ (bilgisayar grubu). Örneğin, 255.255.255.0, 192.168.1.0 alt ağının ağ maskesidir. *192.168.1.0/24* adresindeki tüm alt ağ türünü tarama dışı bırakmak için.

IPv6 adresi ekle:

Tek adres - 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*).

Posta kutusu koruması

ESET NOD32 Antivirus uygulamasının posta kutunuzla entegre edilmesi, e-posta mesajlarındaki kötü amaçlı kodlara karşı etkin koruma düzeyini artırır.

Posta kutusu korumasını yapılandırmak için Gelişmiş ayarlar > **Korumalar** > **E-posta istemci koruması** > **Posta kutusu koruması**'nı açın.

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

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. Entegrasyon etkin veya işlevsel olmasa bile e-posta iletişimi Posta aktarımı koruması (IMAP/IMAPS ve POP3/POP3S) ile korunmaya devam eder.

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

Entegrasyonlar - Posta kutusu korumasını e-posta istemcinize entegre etmenizi sağlar. Daha fazla bilgi için Entegrasyonlar bölümüne bakın.

Yanıt - Spam mesajların işlenmesini özelleştirmenizi sağlar. Daha fazla bilgi için Yanıt bölümüne bakın.

Entegrasyonlar

ESET NOD32 Antivirus Uygulamasının e-posta istemcilerinizle entegre edilmesi, e-posta iletilerindeki kötü amaçlı kodlara karşı gerçekleştirilen etkin koruma düzeyini artırır. E-posta istemciniz destekleniyorsa ESET NOD32 Antivirus aracında entegrasyonu etkinleştirebilirsiniz. E-posta istemcinizle entegre edildiğinde, ESET NOD32 Antivirus araç çubuğu, daha etkili e-posta koruması için doğrudan e-posta istemcisine eklenir. Entegrasyon ayarlarını düzenlemek için Gelişmiş ayarlar > **Korumalar** > **E-posta istemci koruması** > **Posta kutusu koruması** > **Entegrasyon**'u açın.

Microsoft Outlook'a entegre et - 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.

Gelişmiş e-posta istemcisi işleme - - Ek Outlook Messaging API (MAPI) olaylarını işler: Nesne değiştirildi (`fnevObjectModified`) ve Nesne oluşturuldu (`fnevObjectCreated`). E-posta istemcinizle çalışırken sistem yavaşlaması yaşıyorsanız bu seçeneği devre dışı bırakın.

Microsoft Outlook araç çubuğu

Microsoft Outlook koruması bir eklenti modülü olarak çalışır. ESET NOD32 Antivirus Yüklendikten sonra antivirus koruması seçeneklerini içeren bu araç çubuğu Outlook Express'e eklenir:

ESET NOD32 Antivirus - ESET NOD32 Antivirus 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 Posta kutusu koruması bölümüne bakın.

Tarayıcı ayarları - Posta kutusu koruması ayar seçeneklerini görüntüler.

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 NOD32 Antivirus 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.

Yanıt

Mesaj tarama sonuçlarına dayanarak ESET NOD32 Antivirus, taranan mesajları taşıyabilir veya konuya özel metin ekleyebilir. Bu ayarları Gelişmiş ayarlar > **Korumalar** > **E-posta istemci koruması** > **Posta kutusu koruması** > **Yanıt** bölümünde yapılandırabilirsiniz.

Tespit içeren bir mesaj varsa varsayılan olarak ESET NOD32 Antivirus mesajı temizlemeye çalışır. Mesaj temizlenemiyorsa **Temizleme mümkün değilse gerçekleştirilecek işlemi** seçebilirsiniz:

- **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 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.

Alınan ve okunan e-postanın konusunu güncelle/Gönderilen e-postanın konusunu güncelle - Mesaja aşağıda belirtilen özel metni eklemek için bu seçeneği etkinleştirin.

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.

ThreatSense

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 ThreatSenseteknolojisini kullanan herhangi bir modülün Gelişmiş ayarlar penceresinde **ThreatSense** seçeneğini tıklayın. 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 NOD32 Antivirus aracının davranışını belirler. 4 temizleme düzeyi vardır:

ThreatSense aşağıdaki düzeltme (veya temizleme) düzeylerine sahiptir.

ESET NOD32 Antivirus 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.

Temizleme düzeyi	Açıklama
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.

Tarama dışı bırakma

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

Diğer

İsteğe bağlı bilgisayar taraması için ThreatSense altyapısı parametrelerini 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.

Web erişimi koruması

Web erişimi koruması, gelişmiş İnternet koruması modülü ayarlarını yapılandırmanıza olanak tanır. Aşağıdaki seçenekler Gelişmiş ayarlar > **Korumalar** > **Web erişimi koruması** > **Web erişimi koruması**'nda bulunabilir:

Web erişimi korumasını etkinleştir - Bu seçenek devre dışı bırakıldığında Web erişimi koruması ve Kimlik avı koruması çalışmaz.

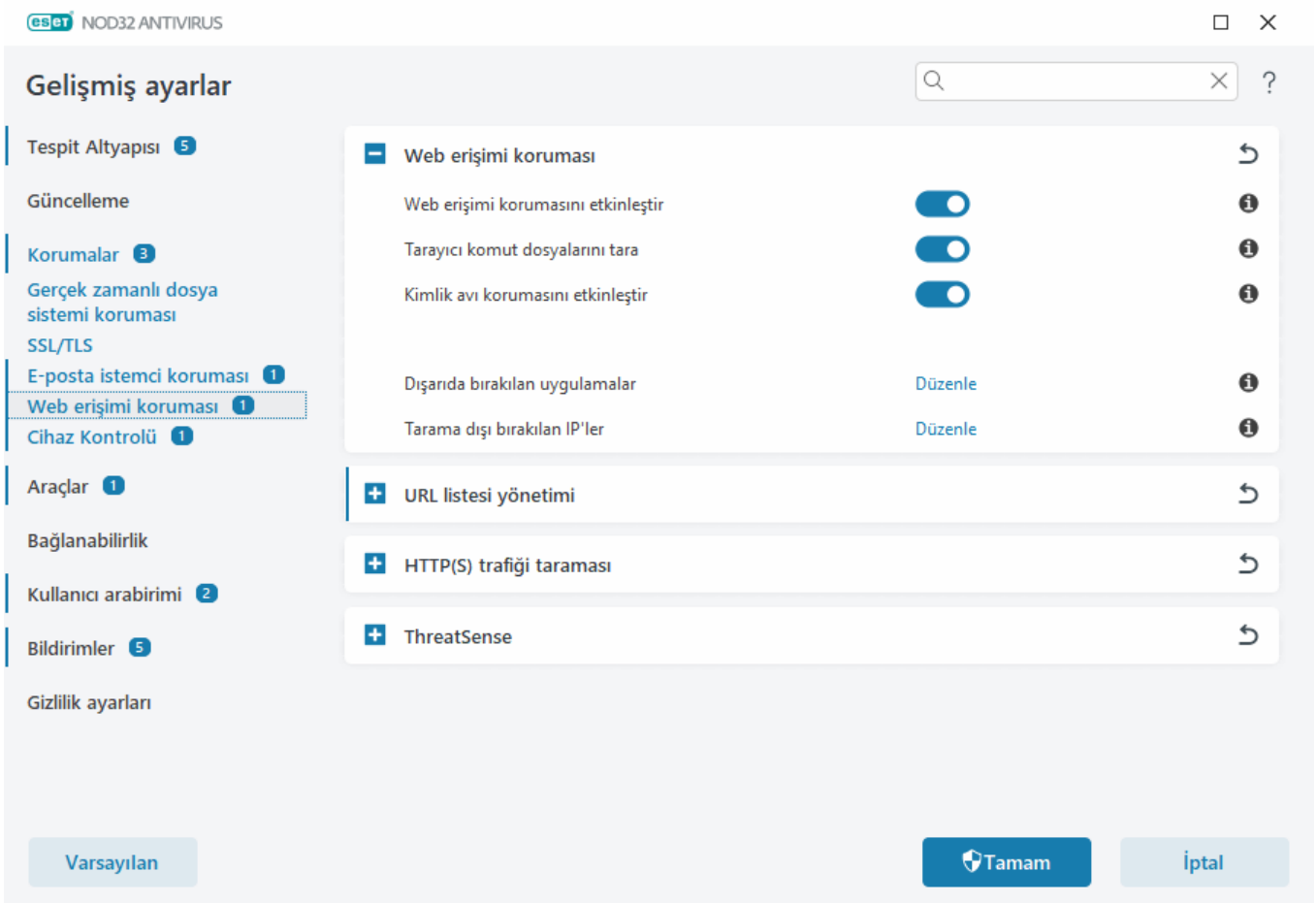
> Web erişimi korumasını etkin halde bırakmanızı ve varsayılan olarak hiçbir uygulamayı veya IP adresini tarama dışı bırakmamanızı kesinlikle öneririz.

Tarayıcı komut dosyalarını tara - Etkinleştirildiğinde, tespit altyapısı web tarayıcıları tarafından yürütülen tüm JavaScript programlarını kontrol eder.

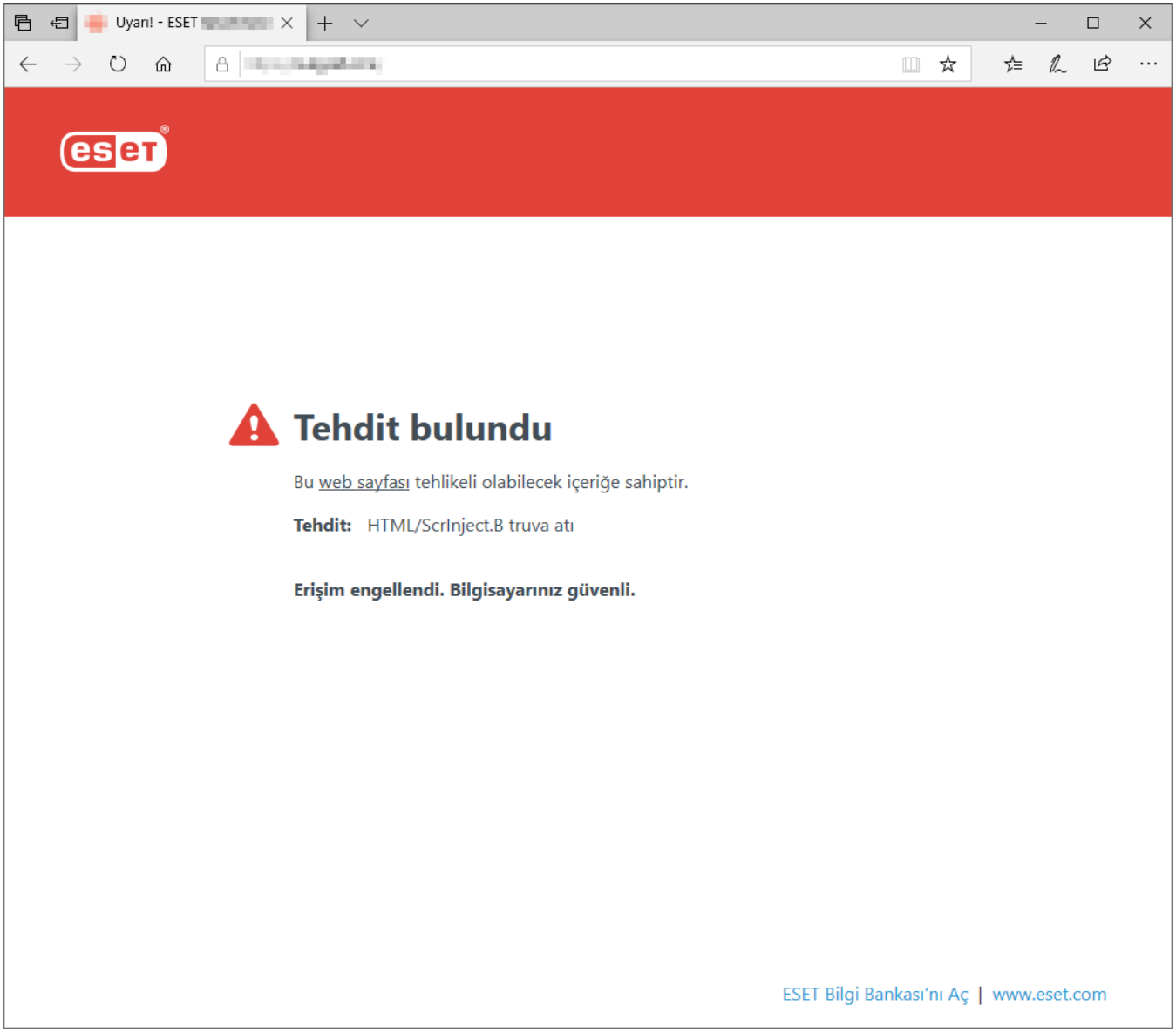
Kimlik Avı korumasını etkinleştir - Etkinleştirildiğinde kimlik avı web sayfaları engellenir. Daha fazla bilgi için Kimlik Avı koruması öğesine bakın.

Tarama dışı bırakılan uygulamalar - Belirli uygulamaların Web Erişimi Koruması tarafından taranmasını engellemenizi sağlar. Web erişimi koruması uyumluluk sorunlarına neden olduğunda bu seçenek kullanışlıdır.

Tarama dışı bırakılan IP'ler - Belirli uzak adresleri Web Erişimi Koruması taramasından hariç tutmanıza olanak tanır. Web erişimi koruması uyumluluk sorunlarına neden olduğunda bu seçenek kullanışlıdır.



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 NOD32 Antivirus aracını kullanarak engelleme

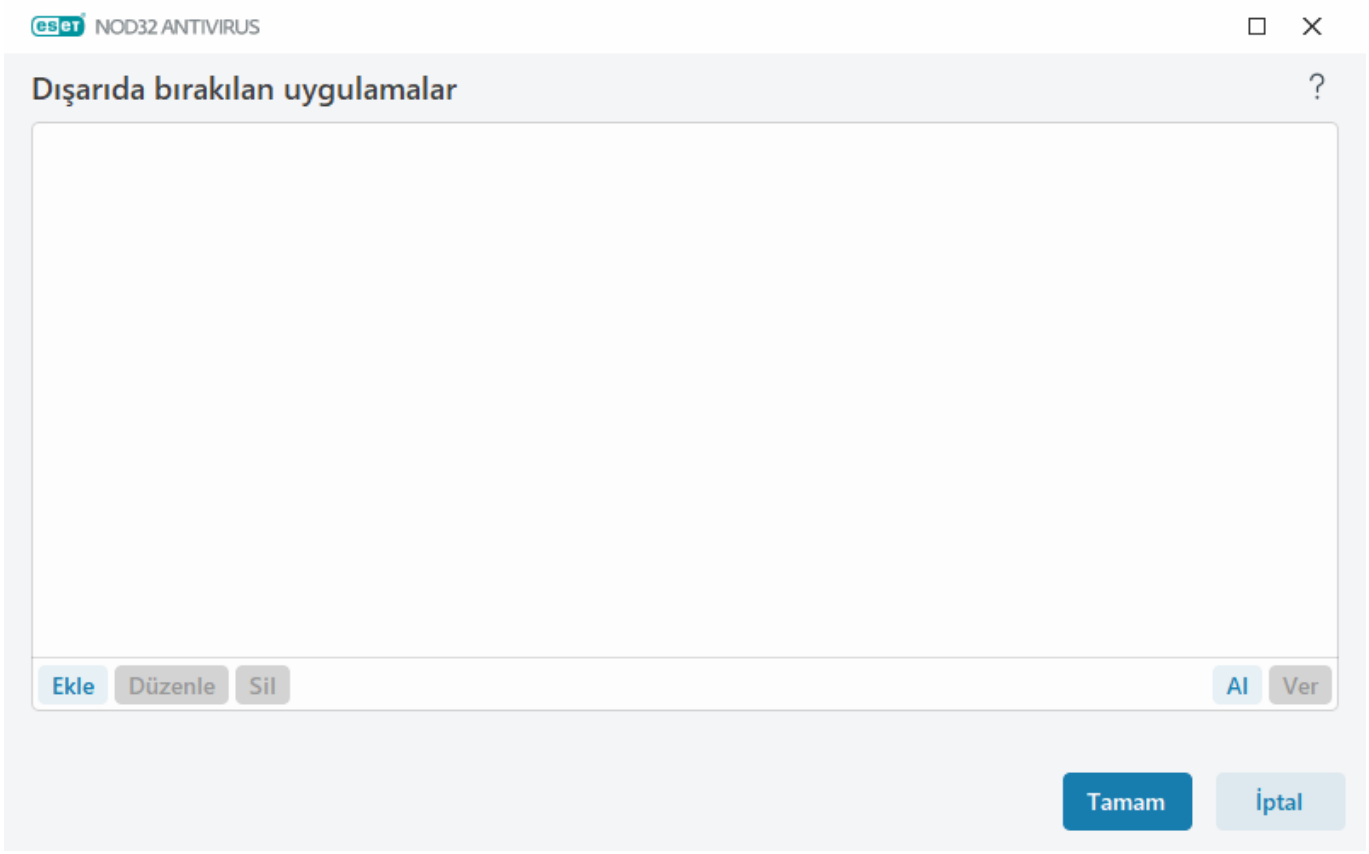
Dışarıda bırakılan uygulamalar

Belirli uygulamalar için iletişim taramasını hariç tutmak üzere bunları listeye ekleyin. Seçili uygulamaların HTTP(S)/POP3(S)/IMAP(S) iletişimi tehditlere karşı denetlenmeyecektir. Bu seçeneğin yalnızca, taranmakta olan iletişimleri düzgün şekilde çalışmayan uygulamalar için kullanılmasını öneririz.

Çalışan uygulama ve hizmetler **Ekle** seçeneğini tıkladığınızda otomatik olarak burada olacaktır. Tarama dışı öğeyi manuel olarak eklemek için **...** seçeneğine tıklayın ve bir uygulamaya gidin.

Düzenle - Listeden seçilen girişleri düzenleyin.

Kaldır - Seçili girişleri listeden kaldırır.



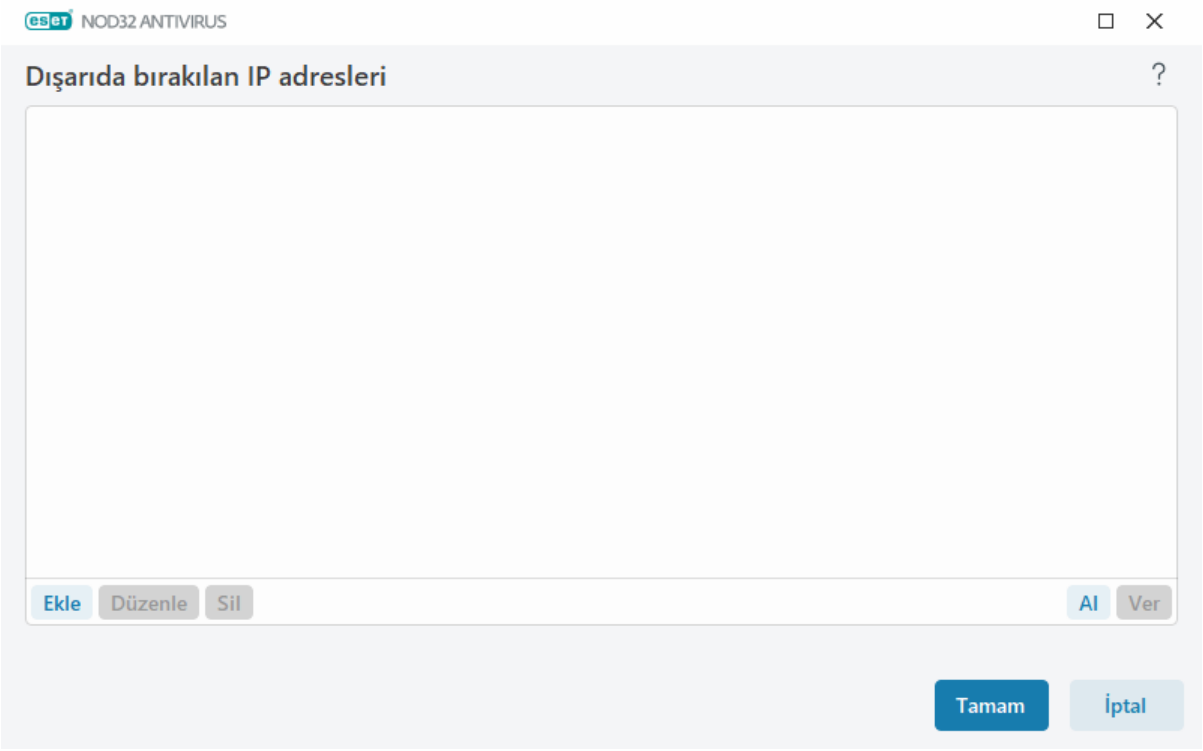
Tarama dışı bırakılan IP'ler

Listedeki girişler tarama dışında bırakılır. Seçili adreslerden/adreslere HTTP(S)/POP3(S)/IMAP(S) iletişimi tehditlere karşı denetlenmez. Bu seçeneği yalnızca güvenilir olduğu bilinen adresler için kullanmanızı öneririz.

Uzak bir noktanın IP adresi/adres aralığı/alt ağını tarama dışı bırakmak için **Ekle** seçeneğini tıklayın.

Seçilen IP adresini değiştirmek için **Düzenle**'yi tıklayın.

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



IP adresleri örnekleri

IPv4 adresi ekle:

Tek adres - Tek bir bilgisayarın IP adresini ekler (örneğin, *192.168.0.10*).

Adres aralığı - Birkaç bilgisayarın IP aralığını belirtmek için başlangıç ve bitiş IP adresini girin (örneğin *192.168.0.1-192.168.0.99*).

Alt ağ - IP adresi ve maske tarafından tanımlanan alt ağ (bilgisayar grubu). Örneğin, 255.255.255.0, 192.168.1.0 alt ağının ağ maskesidir. *192.168.1.0/24* adresindeki tüm alt ağ türünü tarama dışı bırakmak için.

IPv6 adresi ekle:

Tek adres - 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*).

URL listesi yönetimi

Gelişmiş ayarlar > **Korumalar** > **Web erişimi koruması**'ndaki **URL listesi yönetimi**, engellenecek, izin verilecek veya içerik taraması dışında bırakılacak HTTP adreslerini belirtmenize olanak tanır.

HTTPS adreslerini filtrelemek istiyorsanız SSL/TLS'nin HTTP'ye ek olarak etkinleştirilmesi gerekir. Aksi takdirde yalnızca ziyaret ettiğiniz HTTPS sitelerinin etki alanları eklenir, tam URL eklenmez.

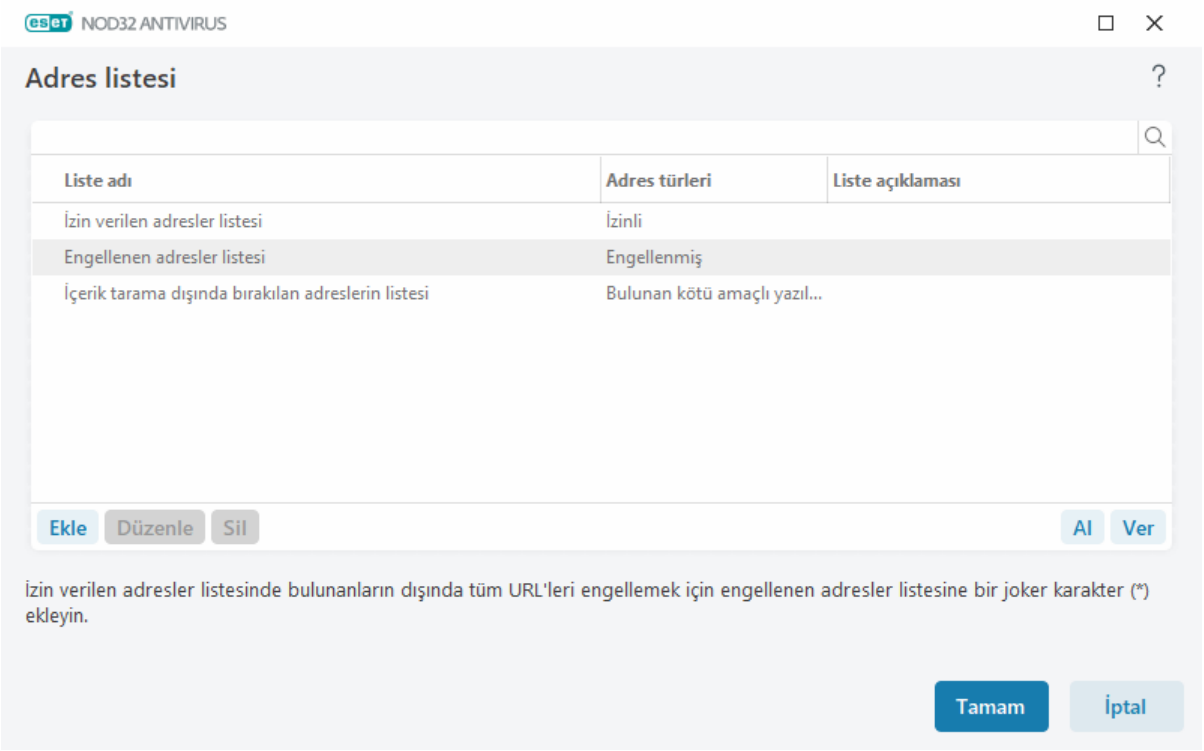
Engellenen adresler listesindeki web siteleri **İzin verilen adresler listesine** dahil edilmedikçe bunlara erişilemez. **İçerik taraması dışında bırakılan adresler listesindeki** web sitelerine erişildiğinde bunlar üzerinde kötü amaçlı kod taraması yapılmaz.

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.

> **ESET Tarafından Güvenilen Adresler**
> SSL/TLS bölümünde **ESET tarafından güvenilen etki alanlarını içeren trafiği tarama** seçeneği etkinse ESET tarafından yönetilen beyaz listedeki etki alanları URL listesi yönetimi yapılandırmasından etkilenmez.



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.

Adres listesi

Bu bölümde; engellenecek, izin verilecek veya denetleme dışında bırakılacak HTTP(S) adreslerinin listelerini belirleyebilirsiniz.

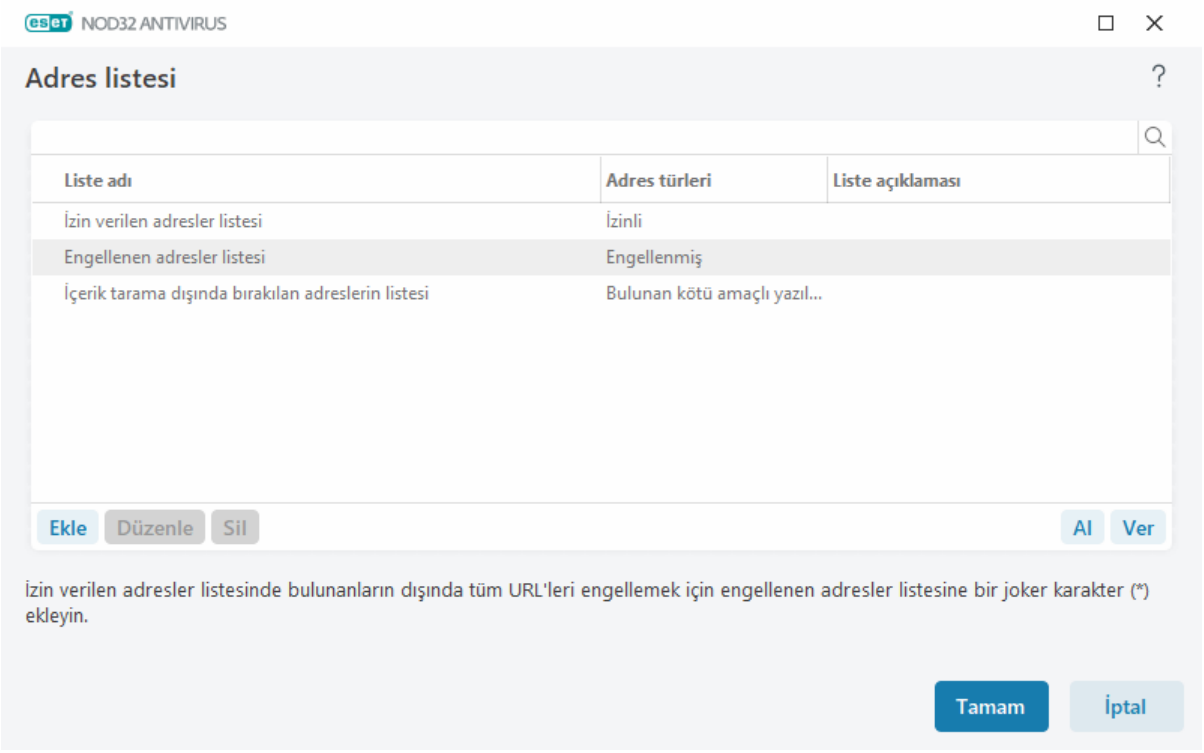
Varsayılan olarak aşağıdaki üç liste kullanılabilir:

- **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 listesi yönetimi'ne bakın.

Yeni 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 NOD32 Antivirus, 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.

HTTP(S) trafiği taraması

Varsayılan olarak, ESET NOD32 Antivirus internet tarayıcıları ve diğer uygulamalar tarafından kullanılan HTTP ve HTTPS trafiğini tarayacak şekilde yapılandırılmıştır. Trafik taramasını yalnızca 3. taraf bir yazılımla ilgili sorunlar yaşıyorsanız ve sorunun ESET NOD32 Antivirus uygulamasından kaynaklanıp kaynaklanmadığını öğrenmek istiyorsanız devre dışı bırakmalısınız.

HTTP trafiği taramasını etkinleştir - HTTP trafiği, tüm uygulamalar için tüm bağlantı noktalarında her zaman izlenir.

HTTPS trafiği taramasını etkinleştir - HTTPS iletişimi, sunucu ile istemci arasında bilgi aktarmak için şifreli bir kanal kullanır. ESET NOD32 Antivirus, 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 noktalarında trafiği tarar (önceden tanımlı 443 ve 0-65535'e bağlantı noktaları ekleyebilirsiniz).

ThreatSense

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 ThreatSenseteknolojisini kullanan herhangi bir modülün Gelişmiş ayarlar penceresinde **ThreatSense** seçeneğini tıklayın. 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 NOD32 Antivirus aracının davranışını belirler. 4 temizleme düzeyi vardır:

ThreatSense aşağıdaki düzeltme (veya temizleme) düzeylerine sahiptir.

ESET NOD32 Antivirus 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.

Tarama dışı bırakma

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

Diğer

İsteğe bağlı bilgisayar taraması için ThreatSense altyapısı parametrelerini 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.

Aygıt denetimi

ESET NOD32 Antivirus otomatik cihaz (CD/DVD/USB vb.) kontrolü 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 Cihaz (medya oynatıcılar, akıllı telefonlar, tak ve çalıştır cihazlar gibi pil destekli cihazlar)
- Tüm aygıt türleri

Cihaz kontrolü ayarları seçenekleri Gelişmiş ayarlar > **Korumalar** > **Cihaz Kontrolü** içinde değiştirilebilir.

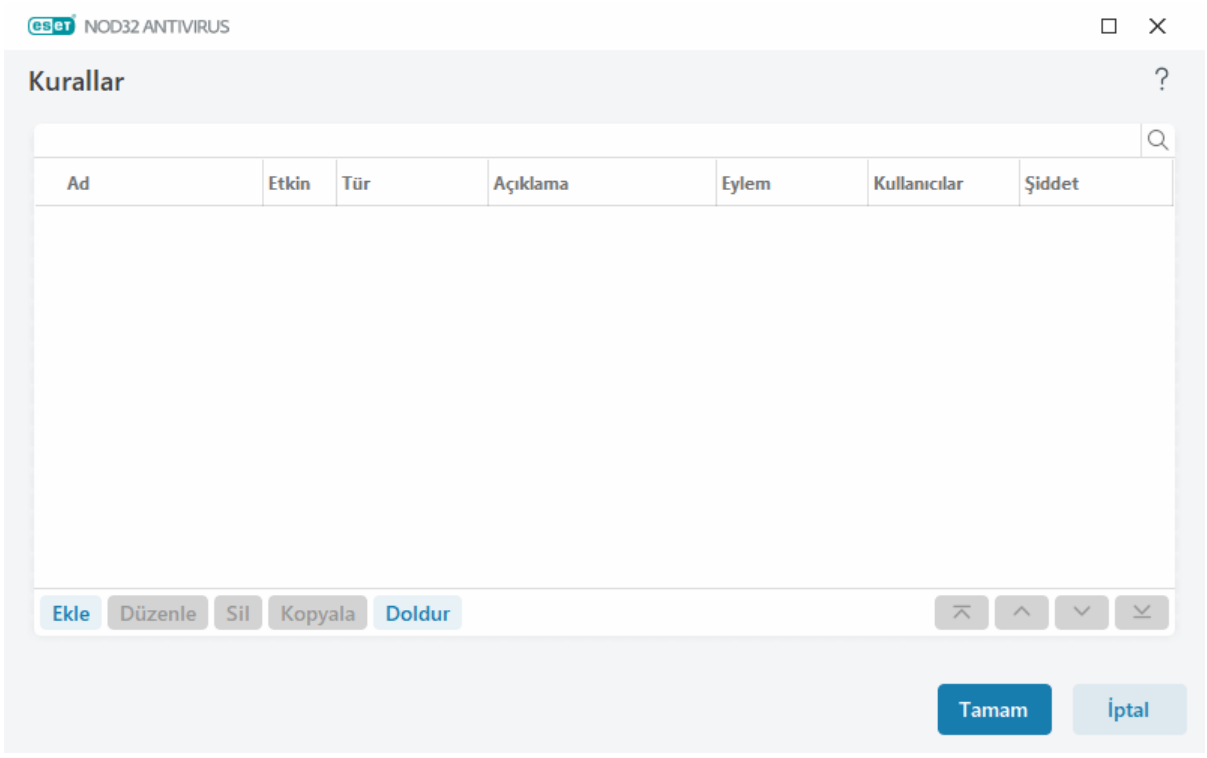
ESET NOD32 Antivirus aracında Cihaz Kontrolü özelliğini etkinleştirmek için **Cihaz Kontrolü'nü etkinleştir** açma/kapama düğmesini tıklayın. Bu değişikliğin etkili olması için bilgisayarınızı yeniden başlatmanız gerekir. Cihaz Kontrolü'nü etkinleştirdikten sonra Kural düzenleyici penceresinde **Kurallar**'ı tanımlayabilirsiniz.

> Farklı kuralların uygulanacağı cihazlardan 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.

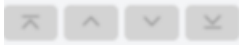


Kullanıcı veya kullanıcı grubu başına ve kural yapılandırmasında belirlenebilen ek cihaz parametrelerine göre belirli cihazlara izin verilebilir ya da bu cihazlar engellenebilir. Kural listesi, bir kuralın çeşitli açıklamalarını içerir: ad, harici cihaz türü, bir harici cihazın bilgisayarınıza bağlanmasının 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.

Bilgisayarınıza bağlı aygıtlar için çıkarılabilir medya aygıt parametrelerini otomatik olarak doldurmak için **Doldur** seçeneğini tıklatın.

Kurallar yüksek önceliğe sahip olanlar en yukarıda olacak şekilde, önceliklerine göre sıralanır. Kurallar,  **Üst/Yukarı/Alt/Aşağı**'yı tıklayarak taşınabilir ve ayrı ayrı ya da gruplar halinde hareket ettirilebilir.

Günlük girişleri, ana program penceresinde > **Araçlar** > Günlük dosyaları'nda 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). Tüm gizli cihazları görmek istiyorsanız **Gizli cihazları göster**'i seçin.

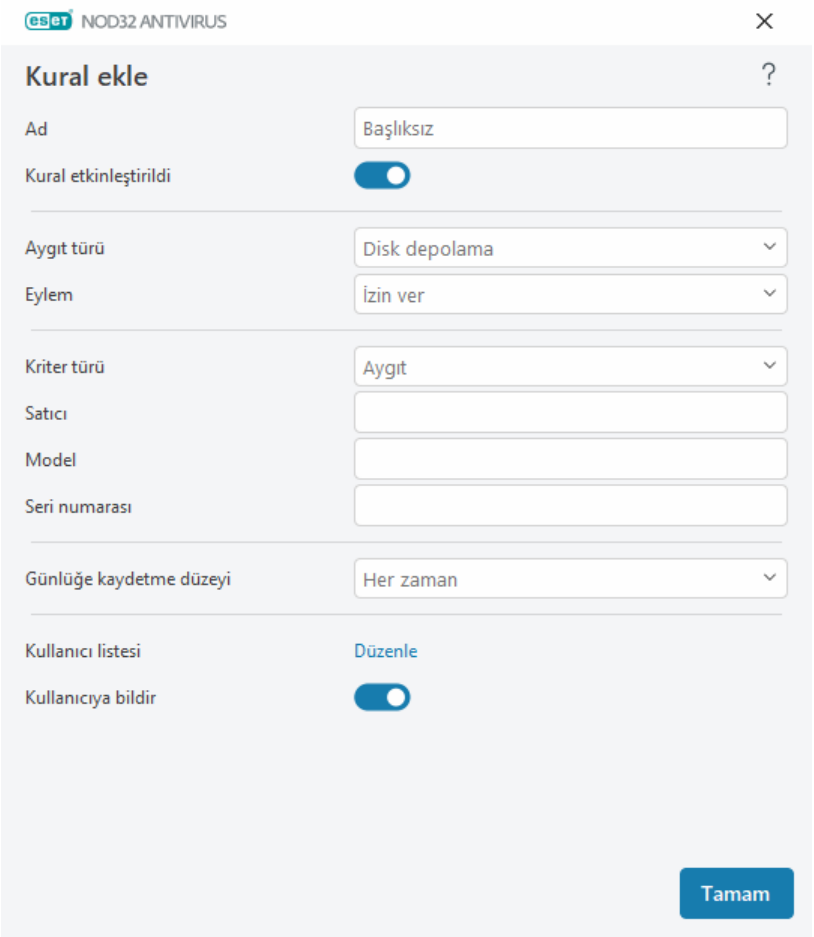
Algılanan cihazlar listesinden bir cihaz seçin ve önceden tanımlı bilgilere sahip bir cihaz kontrolü kuralı eklemek için **Tamam**'ı tıklayın (tüm ayarlar yapılabilir).

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 NOD32 Antivirus tüm önemli olayları ana menüden doğrudan görüntülenebilen bir günlük dosyasına kaydeder. **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).

ThreatSense

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 ThreatSenseteknolojisini kullanan herhangi bir modülün Gelişmiş ayarlar penceresinde **ThreatSense** seçeneğini tıklayın. 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 NOD32 Antivirus aracının davranışını belirler. 4 temizleme düzeyi vardır:

ThreatSense aşağıdaki düzeltme (veya temizleme) düzeylerine sahiptir.

ESET NOD32 Antivirus 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.

Tarama dışı bırakma

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

Diğer

İsteğe bağlı bilgisayar taraması için ThreatSense altyapısı parametrelerini 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.

Temizleme düzeyleri

İstediğiniz koruma modülünün temizleme düzeyi ayarlarını değiştirmek için **ThreatSense** seçeneğini genişletin (örneğin, **Gerçek zamanlı dosya sistemi koruması**) ve ardından açılır menüden bir **Temizleme düzeyi** seçin.

ThreatSense aşağıdaki düzeltme (veya temizleme) düzeylerine sahiptir.

ESET NOD32 Antivirus 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.

Tarama dışında bırakılan dosya uzantıları

Tarama dışı bırakılan dosya uzantıları, ThreatSense aracının bir parçasıdır. Tarama dışı bırakılan dosya uzantılarını yapılandırmak için ThreatSense teknolojisini kullanan herhangi bir modül için Gelişmiş ayarlar penceresinde **ThreatSense** seçeneğini tıklayın.

Uzantı, dosya adının nokta ile ayrılmış olan parçasıdır. Uzantı bir dosyanın türünü ve içeriğini tanımlar. ThreatSense 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 sisteminde bir dosyanın tam uzantısını (varsa) görmek için **Windows Explorer** > **Görünüm**'de (sekme) **Dosya adı uzantıları** onay kutusunu işaretlemeniz gerekir.

Ek ThreatSense parametreleri

Bu ayarları düzenlemek için Gelişmiş ayarlar > **Korumalar** > **Gerçek zamanlı dosya sistemi koruması** > **Ek ThreatSense parametreleri**'ni açın.

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 NOD32 Antivirus, 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.

Araçlar

Ek güvenlik sunan ve ESET NOD32 Antivirus yönetimini basitleştirmeye yardımcı olan özellikler için gelişmiş ayarları Gelişmiş ayarlar > **Araçlar**'da yapılandırabilirsiniz.

- Microsoft Windows® güncellemesi
- ESET CMD
- Günlük dosyaları
- Oyun modu
- Tanılamalar

Microsoft Windows® güncellemesi

Windows update özelliği, kullanıcıları kötü amaçlı yazılımlardan korumaya yönelik önemli bir bileşendir. Bu nedenle, Microsoft Windows güncellemelerini kullanılabilir oldukları anda yüklemeniz büyük önem taşır. ESET NOD32 Antivirus, Gelişmiş ayarlar > **Araçlar**'da 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.

İletişim penceresi - Sistem güncellemeleri

İşletim sisteminiz için güncellemeler varsa ESET NOD32 Antivirus 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 bilgiler içeren yeni bir pencere görüntülemek için bir güncelleme satırını sağ tıklayın ve **Bilgileri göster**'i tıklayın.

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 NOD32 Antivirus 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 NOD32 Antivirus 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.

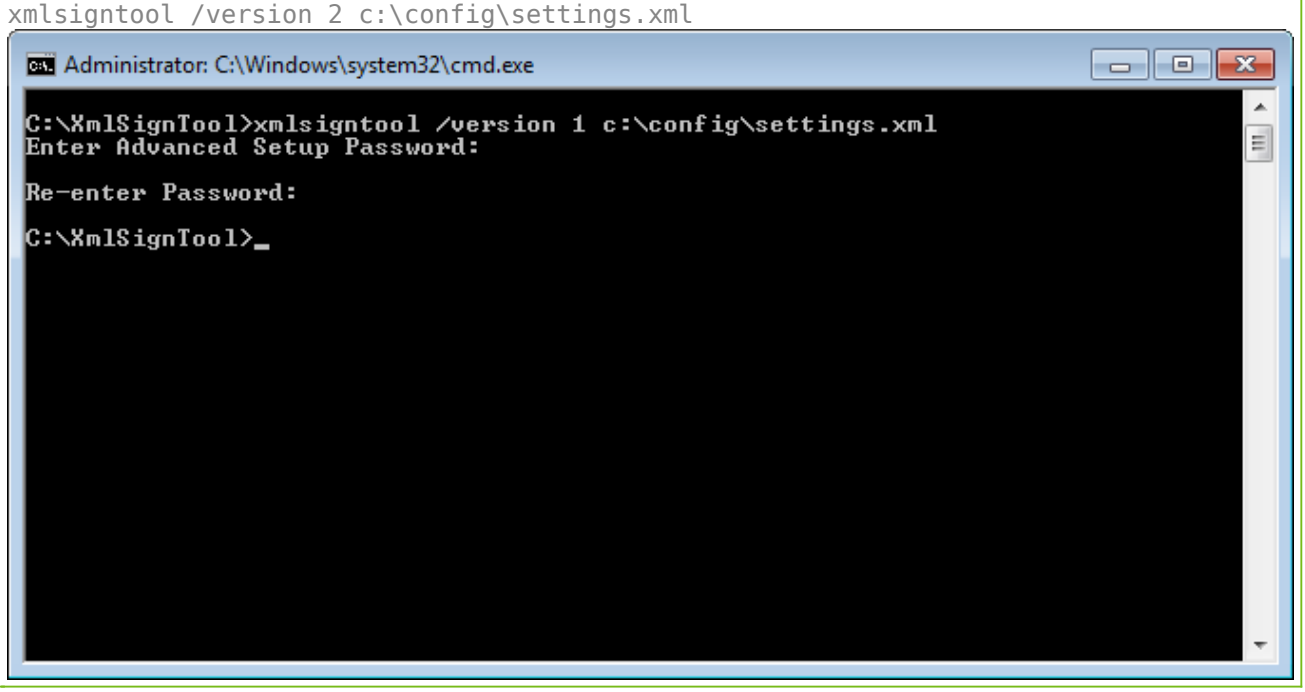
.xml yapılandırma dosyasını imzalama:

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 NOD32 Antivirus sürümüne bağlıdır. ESET NOD32 Antivirus 11.1'den daha eski sürümler için `/version 1` kullanın. Geçerli ESET NOD32 Antivirus 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 NOD32 Antivirus 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 NOD32 Antivirus 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.

Günlük dosyaları

ESET NOD32 Antivirus ürününün günlük kaydı yapılandırmasını Gelişmiş ayarlar > **Araçlar** > **Günlük dosyaları**'nda bulabilirsiniz. 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 günlüğe kaydedilir (Antivirus korumasını vs. başlatırken hata...).

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.

Oyun modu

Oyun modu; yazılımlarını kesintisiz olarak kullanabilmeyi talep eden, bildirim/uyarı pencereleriyle rahatsız edilmek istemeyen ve CPU kullanımının en düşük düzeye 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** > 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.

Tanılamalar

Tanılamalar, ESET işlemleri için uygulamanın kilitlendiği durumların dökümünü sağlar (örneğin: ekrn). Bir uygulama kilitlendiğinde döküm oluşturulur. Bu, geliştiricilerin hataları düzeltmesine ve ESET NOD32 Antivirus 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.

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 trafiği tarayıcısı gelişmiş günlük kaydını etkinleştir - Geliştiricilerin ağ trafiği tarayıcısıyla ilgili sorunları tanılamasına ve düzeltmesine yardımcı olmak için Ağ trafiği tarayıcısından geçen tüm verileri PCAP biçiminde kaydedin.

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.

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 NOD32 Antivirus 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.

Bağlanabilirlik

Belirli ağlarda, bir proxy sunucusu bilgisayarınız ile internet arasındaki iletişime aracılık edebilir. Bir proxy sunucu kullanıyorsanız aşağıdaki ayarları tanımlamanız gerekir. Aksi takdirde, ESET NOD32 Antivirus ve modülleri otomatik olarak güncellenemez. ESET NOD32 Antivirus aracında proxy sunucu ayarları Gelişmiş ayarlar'ın iki farklı bölümünde bulunabilir.

Genel proxy sunucu ayarları Gelişmiş ayarlar > **Bağlanabilirlik** > **Proxy sunucu**'da yapılandırılabilir. Proxy sunucunun bu düzeyde belirtilmesi, tüm ESET NOD32 Antivirus için global proxy sunucu ayarlarını belirler. Buradaki parametreler İnternet bağlantısının gerekli olduğu tüm modüller tarafından kullanılır.

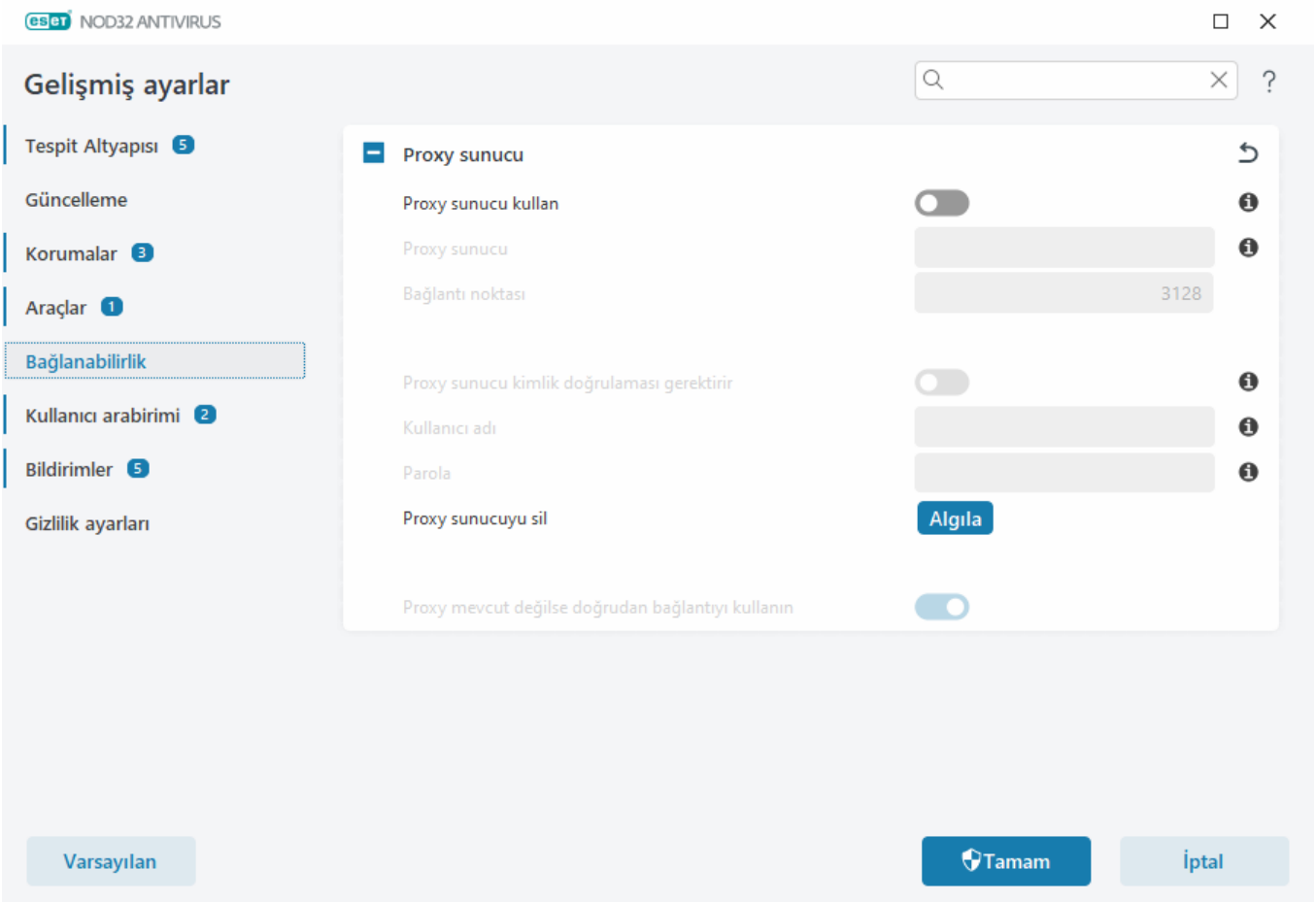
Genel proxy sunucu ayarlarını belirtmek için, **Proxy sunucu kullan**'ı etkinleştirin ve **Proxy sunucu** adresini, proxy sunucunun **bağlantı noktası** numarasıyla birlikte yazın.

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 tespit etmek ve doldurmak için **Proxy sunucuyu tespit et**'i tıklayın. ESET NOD32 Antivirus, Internet Explorer veya Google Chrome için internet seçeneklerinde belirtilen parametreleri kopyalar.

Proxy sunucu ayarlarında Kullanıcı Adı ve Parolanızı manuel olarak girmeniz gerekir.

Proxy kullanılamıyorsa doğrudan bağlantı kullan – ESET NOD32 Antivirus ürünü proxy kullanacak şekilde yapılandırılmışsa ancak proxy'e ulaşılamıyorsa ESET NOD32 Antivirus, proxy'i atlayarak doğrudan ESET sunucularıyla iletişim kurar.

Proxy sunucu ayarları, Gelişmiş ayarlar > **Güncelleme** > **Profiller** > **Güncellemeler** > **Bağlantı seçenekleri** bölümünde, **Proxy modu** açılır menüsünden **Proxy sunucu üzerinden bağlantı** seçilerek yapılabilir. Bu yapılandırma yalnızca güncellemeler için geçerlidir ve modül güncellemelerini uzak konumlardan alan dizüstü bilgisayarlar için önerilir. Daha fazla bilgi için Gelişmiş güncelleştirme ayarları konusuna bakın.



Kullanıcı arabirimi

Programın grafik kullanıcı arabirimi (GUI) davranışını yapılandırmak için, Gelişmiş ayarlar > **Kullanıcı arabirimi**'ni açın.

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 NOD32 Antivirus Çalışma ortamını (GUI) Gelişmiş ayarlar > **Kullanıcı arabirimi** > **Kullanıcı arabirimi öğeleri**'nde ihtiyaçlarınızı karşılayacak şekilde ayarlayabilirsiniz.

Renk modu - Açılır menüden ESET NOD32 Antivirus GUI'sinin renk düzenini seçin:

- **Sistem rengiyle aynı** - İşletim sistemi ayarlarınıza göre ESET NOD32 Antivirus renk düzenini ayarlar.
- **Koyu mod** - ESET NOD32 Antivirus koyu renk düzeni (koyu mod) sahip olur.
- **Açık** - ESET NOD32 Antivirus standart, açık renk düzenine sahip olur.

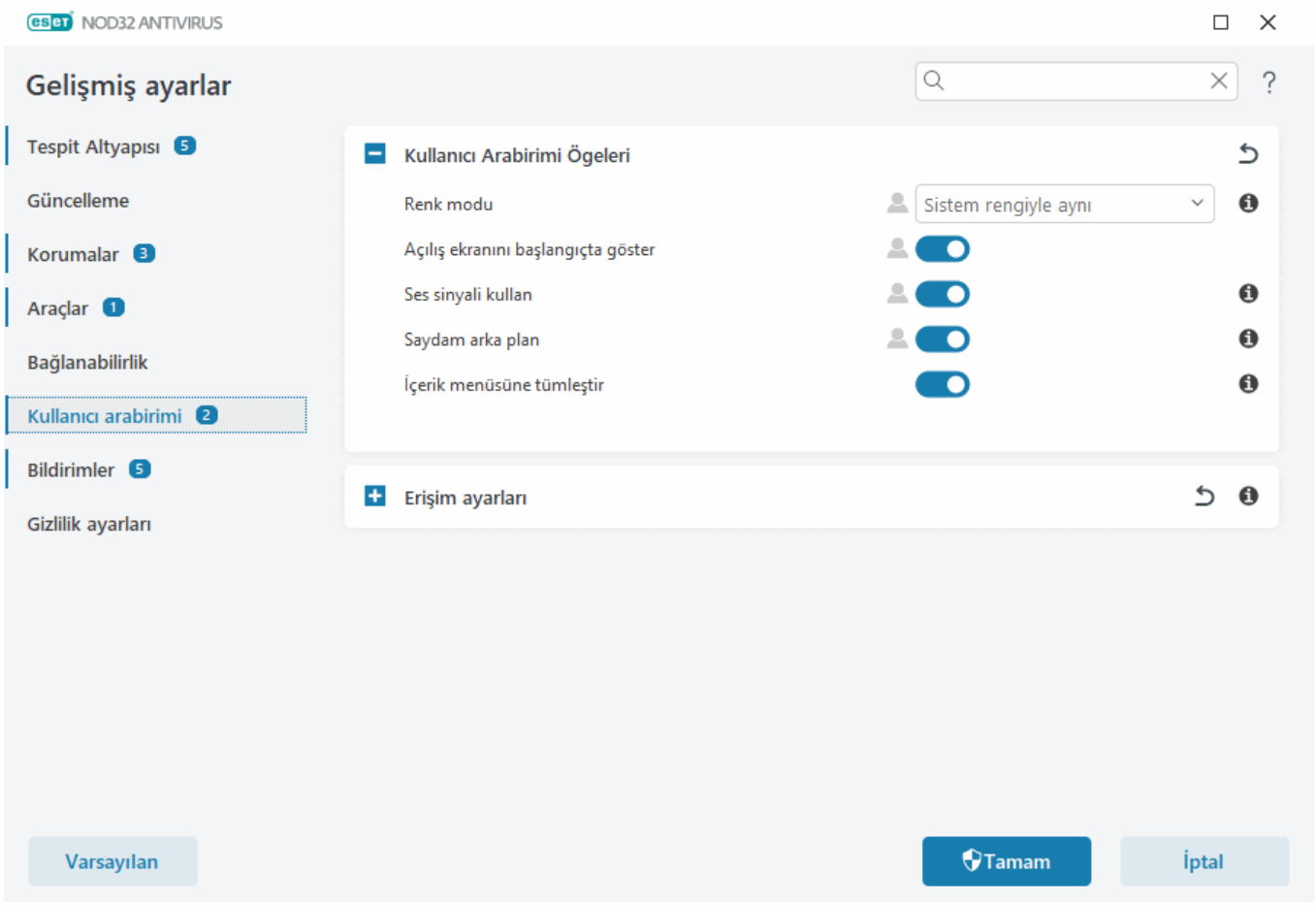
Ayrıca ana program penceresinin sağ üst köşesindeki ESET NOD32 Antivirus GUI renk şemasını da seçebilirsiniz.

Başlangıçta giriş ekranını göster - Başlatma sırasında ESET NOD32 Antivirus 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 NOD32 Antivirus denetim öğelerini içerik menüsüne dahil eder.



Erişim ayarları

ESET NOD32 Antivirus ayarları, güvenlik politikanızın önemli bir parçasıdır. Yetkisiz olarak yapılabilecek değişiklikler sisteminizin kararlılığını ve korunmasını tehlikeye atma olasılığı taşır. Yetkisiz değişiklikleri engellemek için ESET NOD32 Antivirus ürününün ayar parametreleri ve kaldırılması parola korumalı hale getirilebilir. Erişim ayarları Gelişmiş ayarlar > **Kullanıcı arabirimi** > **Erişim ayarları**'nda yapılandırılabilir.

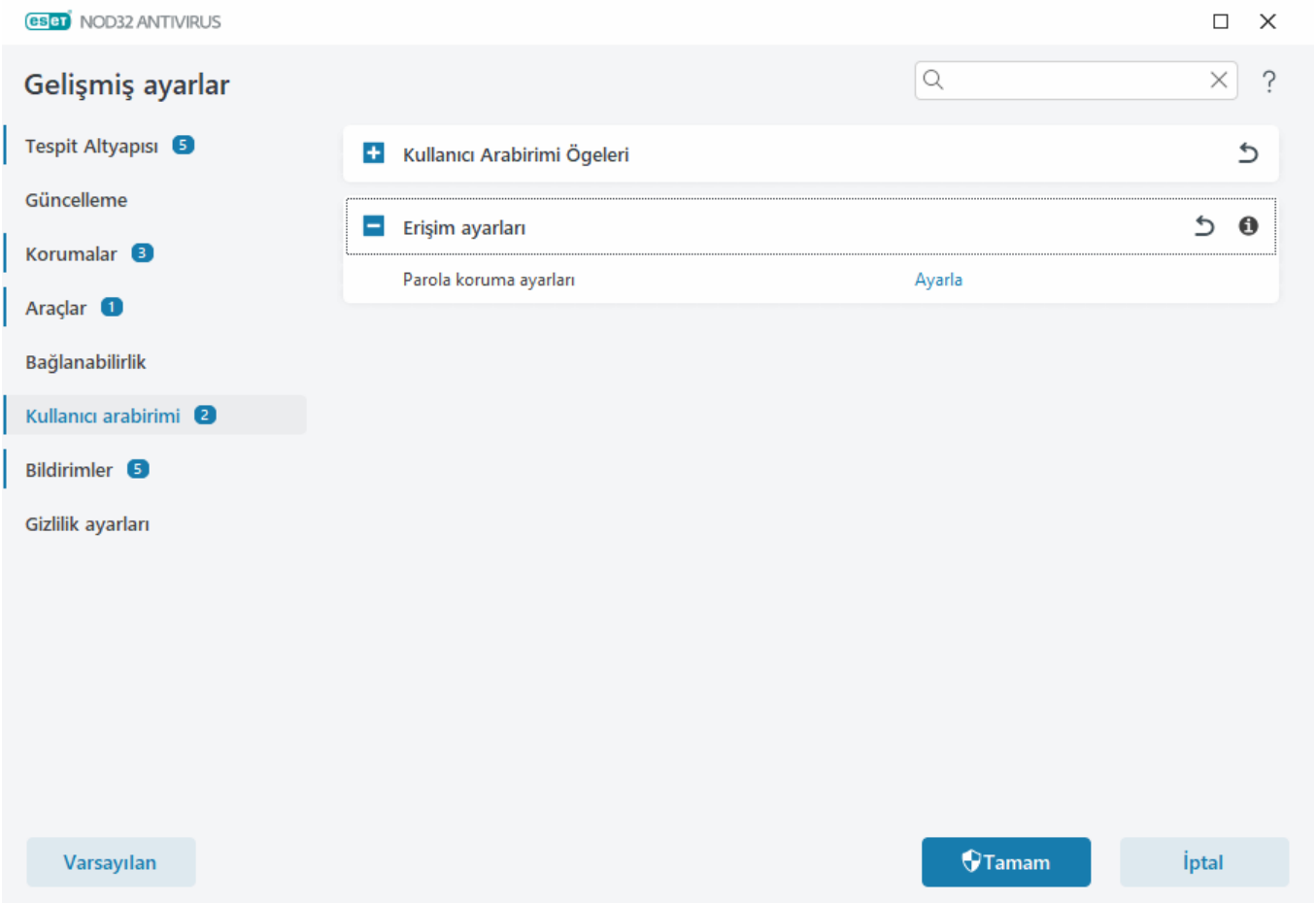
Kurulum parametrelerini korumak ve ESET NOD32 Antivirus yüklemesini kaldırmayı korumak için **Parola koruma ayarlarının** yanındaki **Ayarla**'yı tıklayın.

Korumalı Gelişmiş ayarlara erişmek istediğinizde parola girişi için bir pencere görüntülenir. Parolanızı unutur veya kaybederseniz alt taraftaki **Parolayı geri yükle** seçeneğine tıklayın ve abonelik 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 NOD32 Antivirus 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 etkinleştirme anahtarınızı kurtarmak veya aboneliğinizin sona erme tarihini ya da ESET NOD32 Antivirus ürünü için diğer abonelik bilgilerini görmek üzere Etkinleştirme anahtarımı kaybettim bölümüne bakın.

Ekran okuyucusu desteği

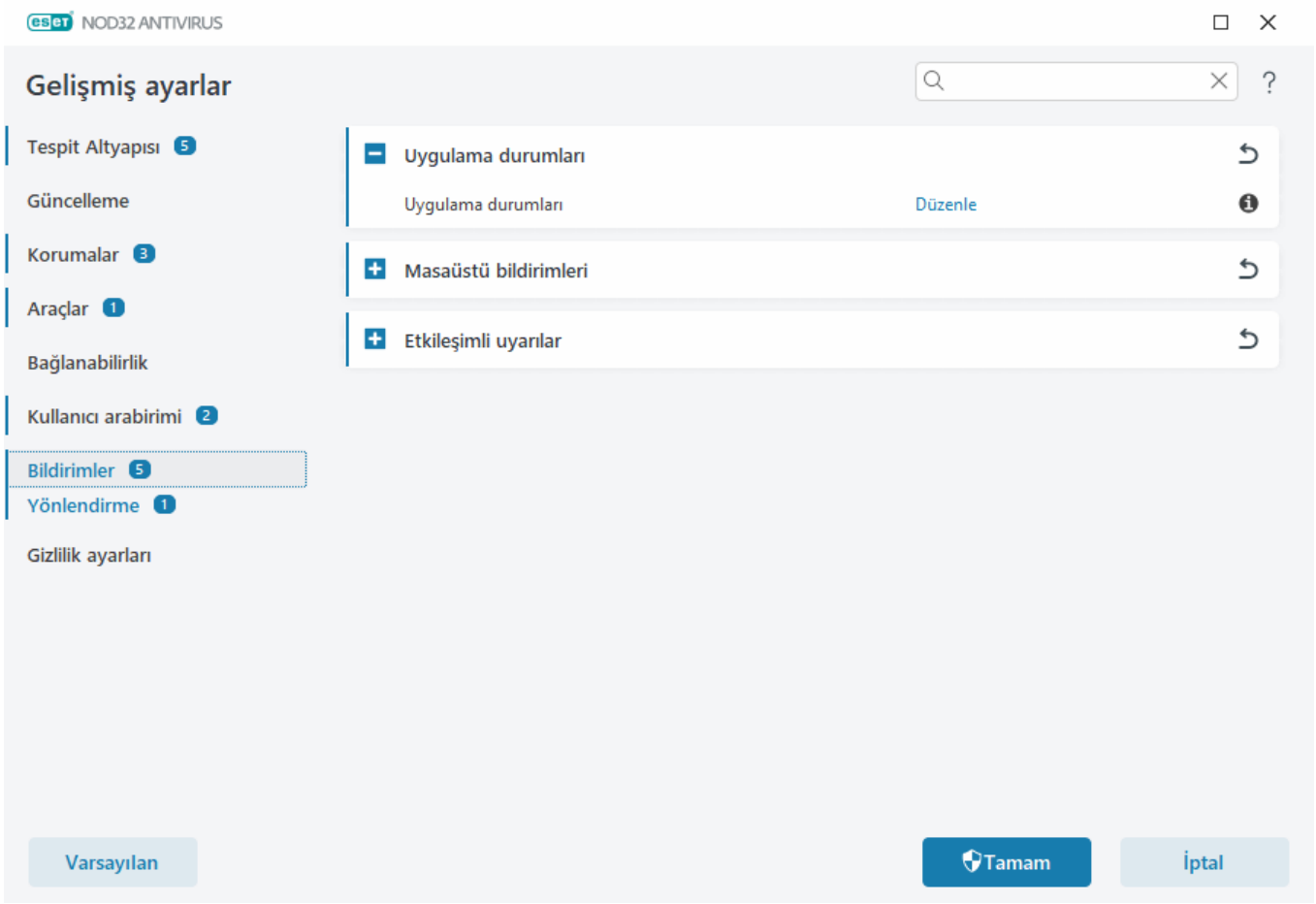
ESET NOD32 Antivirus, görme bozukluğu olan ESET kullanıcılarının üründe gezinmelerine veya ayarları yapılandırmalarına olanak sağlamak için ekran okuyucularla birlikte kullanılabilir. Aşağıdaki ekran okuyucular desteklenmektedir: (JAWS, NVDA, Narrator) .

Ekran okuyucu yazılımının ESET NOD32 Antivirus GUI'sine doğru şekilde erişebilmesini sağlamak için Bilgi Bankası makalemizdeki talimatları izleyin.

Bildirimler

ESET NOD32 Antivirus bildirimlerini yönetmek için Gelişmiş ayarlar > **Bildirimler**'i açın. Aşağıdaki bildirim türlerini yapılandırabilirsiniz:

- Uygulama durumları - Ana program penceresi > **Genel bakış** bölümünde gösterilen bildirimler.
- Masaüstü bildirimleri - Sistem görev çubuğunun yanındaki küçük bildirim pencereleri.
- 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.

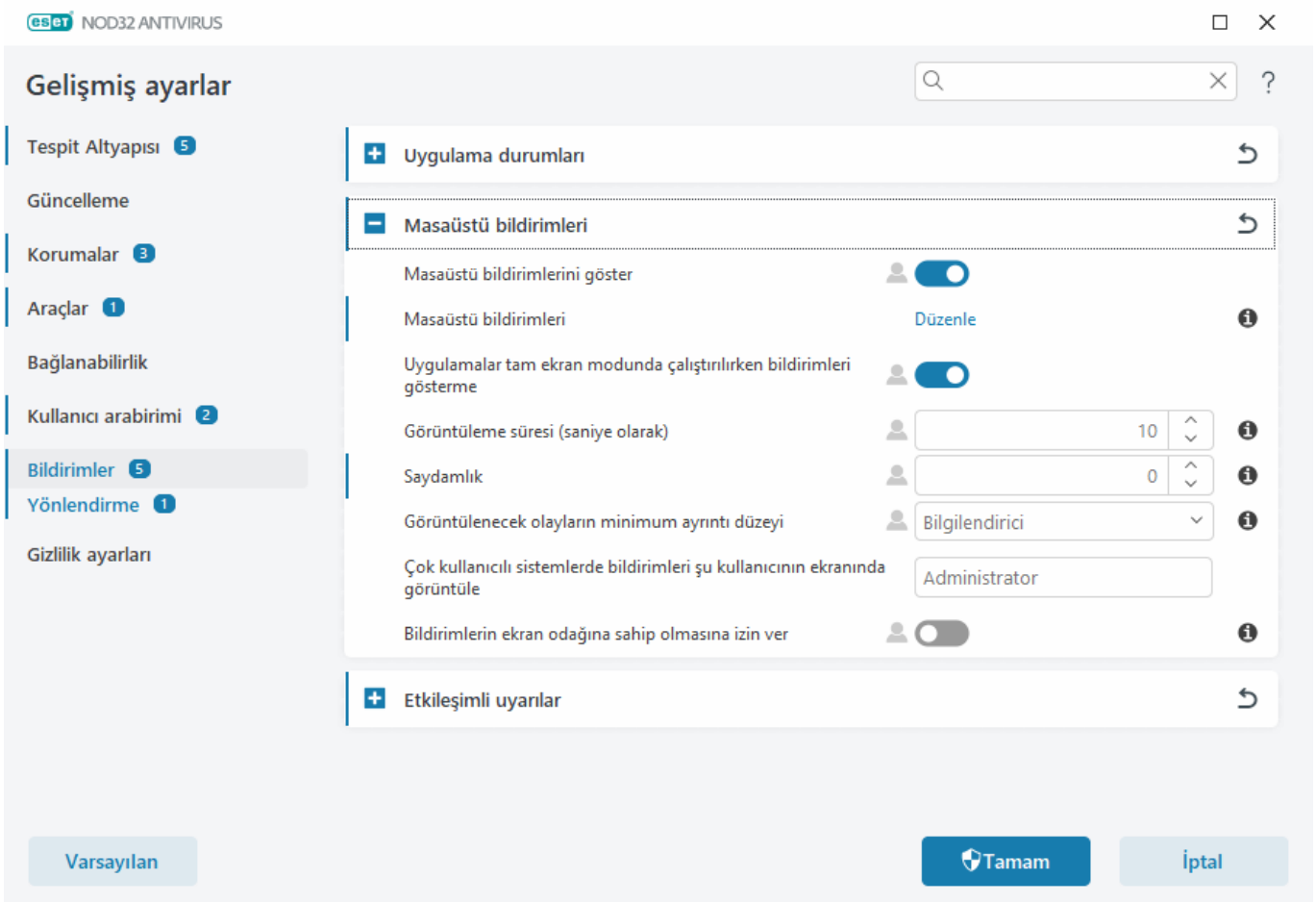
İletişim penceresi - Uygulama durumları

Bu iletişim penceresinde, hangi uygulama durumlarının görüntüleneceğini seçebilirsiniz. Örneğin, Antivirus ve antispyware korumasını duraklattığınızda veya Oyun modunu etkinleştirdiğinizde.

Ayrıca uygulama durumu, ürününüz etkinleştirilmediğinde veya aboneliğinizin süresi dolduğunda da gösterilir.

Masaüstü bildirimleri

Masaüstü bildirimleri sistem görev çubuğunun yanında küçük bir bildirim penceresiyle 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 görüntüleme süresi: Bildirim görünürlüğü süresini ayarlar. 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 (örneğin, güncelleme başarısız).
- **Hatalar** - Hataları (örneğin, belge koruması başlatılmadı) ve kritik hataları görüntüler.

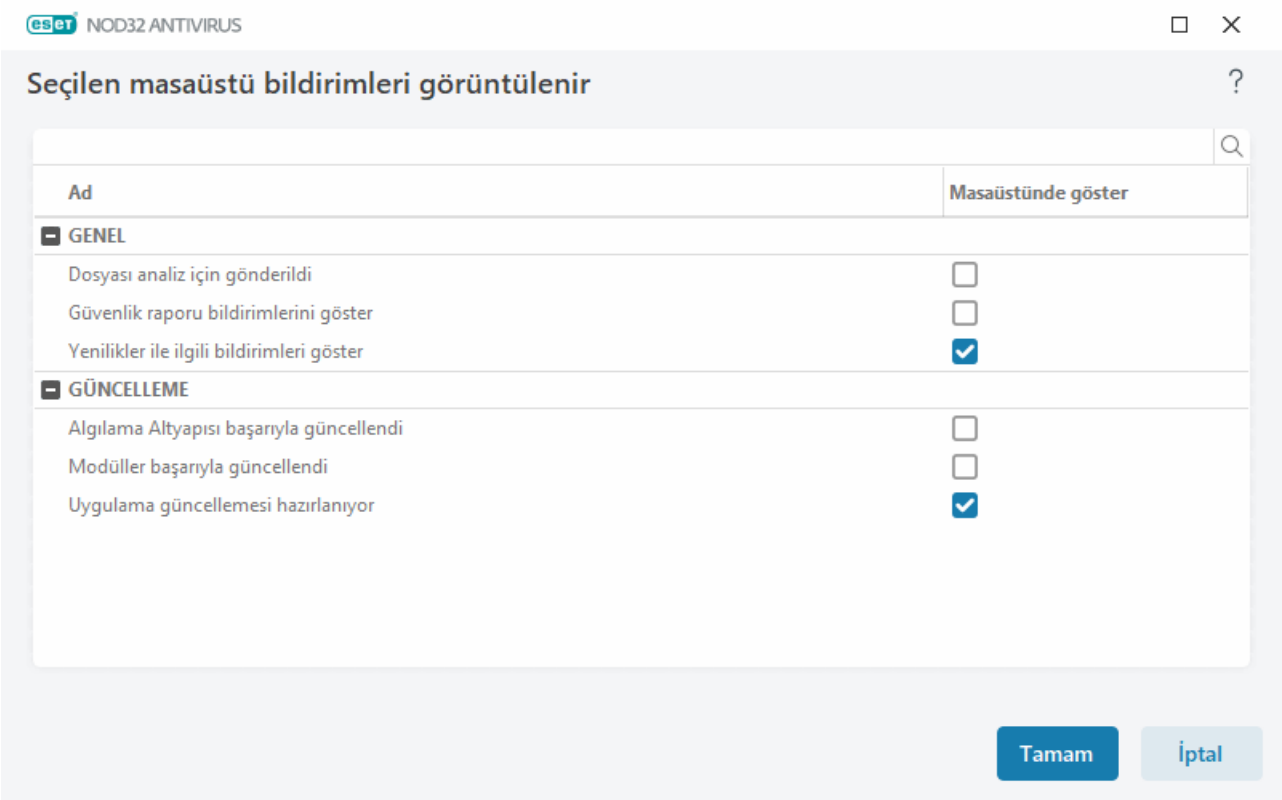
- **Kritik** - Yalnızca kritik hataları gösterir (Antivirus korumasının veya virüs bulaşmış sistemin başlatılmasıyla ilgili hata).

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 > **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 NOD32 Antivirus ürününün analiz için dosya gönderdiği her seferinde bir bildirim alırsınız.

Ağ Denetçisi

Yeni bulunan ağ cihazları hakkında bilgilendir - Ağa yeni bir cihaz bağlandığında bildirim alırsınız.

Ağ koruması

Ağ profili değiştirildi - Ağ profili değiştirildiğinde bildirim alırsınız.

Wi-Fi koruma uyarıları - Parolası zayıf olan veya parolası olmayan bir Wi-Fi ağına bağlanmaya çalıştığınızda bildirim alırsınız.

Güncelleme

Uygulama güncellemesi hazırlanıyor - Hazırlanacak yeni ESET NOD32 Antivirus 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.

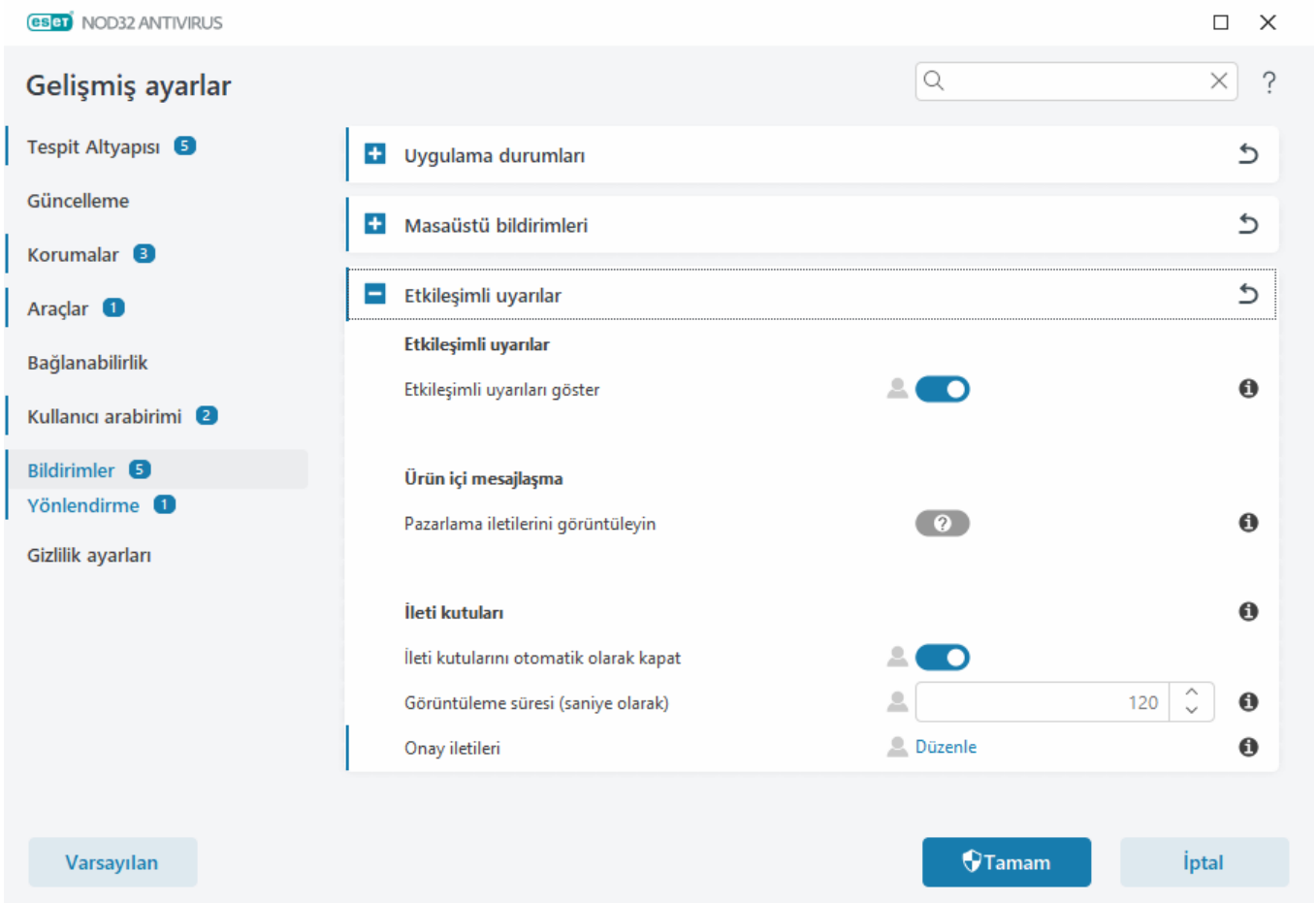
Masaüstü bildirimleri için genel ayarları yapmak üzere (örneğin bir mesajın ne kadar süre gösterileceği veya gösterilecek olayların en düşük ayrıntı düzeyi gibi) Gelişmiş ayarlar > **Bildirimler**'de Masaüstü bildirimleri bölümüne bakın.

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
- Web sitesi sertifikası iptal edildi

Gelişmiş ayarlar > 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 NOD32 Antivirus 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. Bu seçeneğin etkin halde kalmasını öneririz.

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

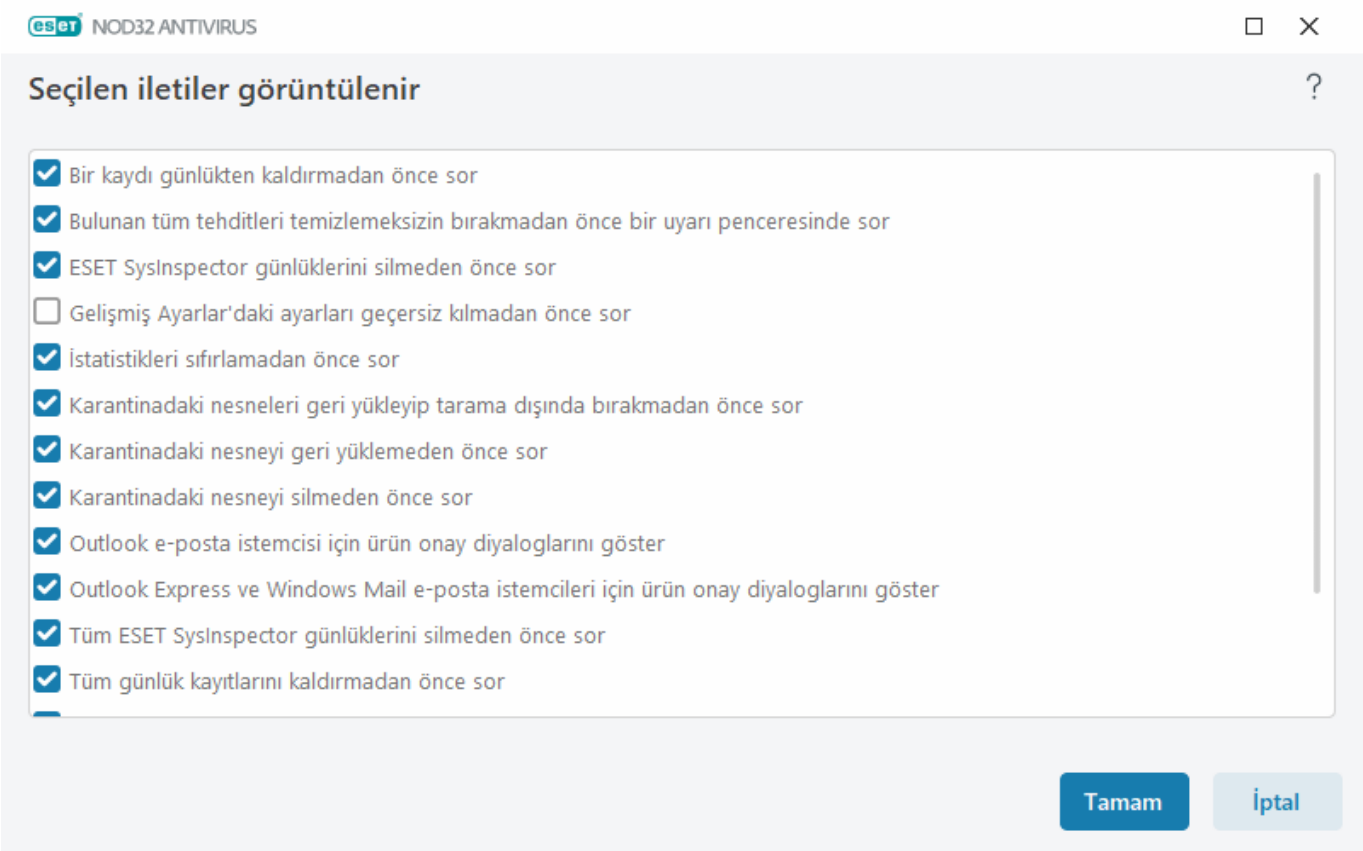
Mesaj kutularını belirli bir sürenin ardından otomatik olarak kapatmak için **Mesaj kutularını otomatik olarak kapat**'ı seçin. Kutular manuel olarak kapatılmazlarsa belirtilen süre geçtikten sonra uyarı pencereleri otomatik olarak kapatılır.

Saniye cinsinden görüntüleme süresi: Uyarı 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 > **Bildirimler** > **İnteraktif uyarılar**'a gidin ve **Onay mesajları**'nın yanındaki **Düzenle**'yi tıklayın.



Bu iletişim penceresi herhangi bir eylem gerçekleştirilmeden önce ESET NOD32 Antivirus tarafından gösterilecek onay iletilerini görüntüler. İzin vermek veya devre dışı bırakmak için her bir onay iletisinin yanındaki kutuyu işaretleyin veya işaretini kaldırın.

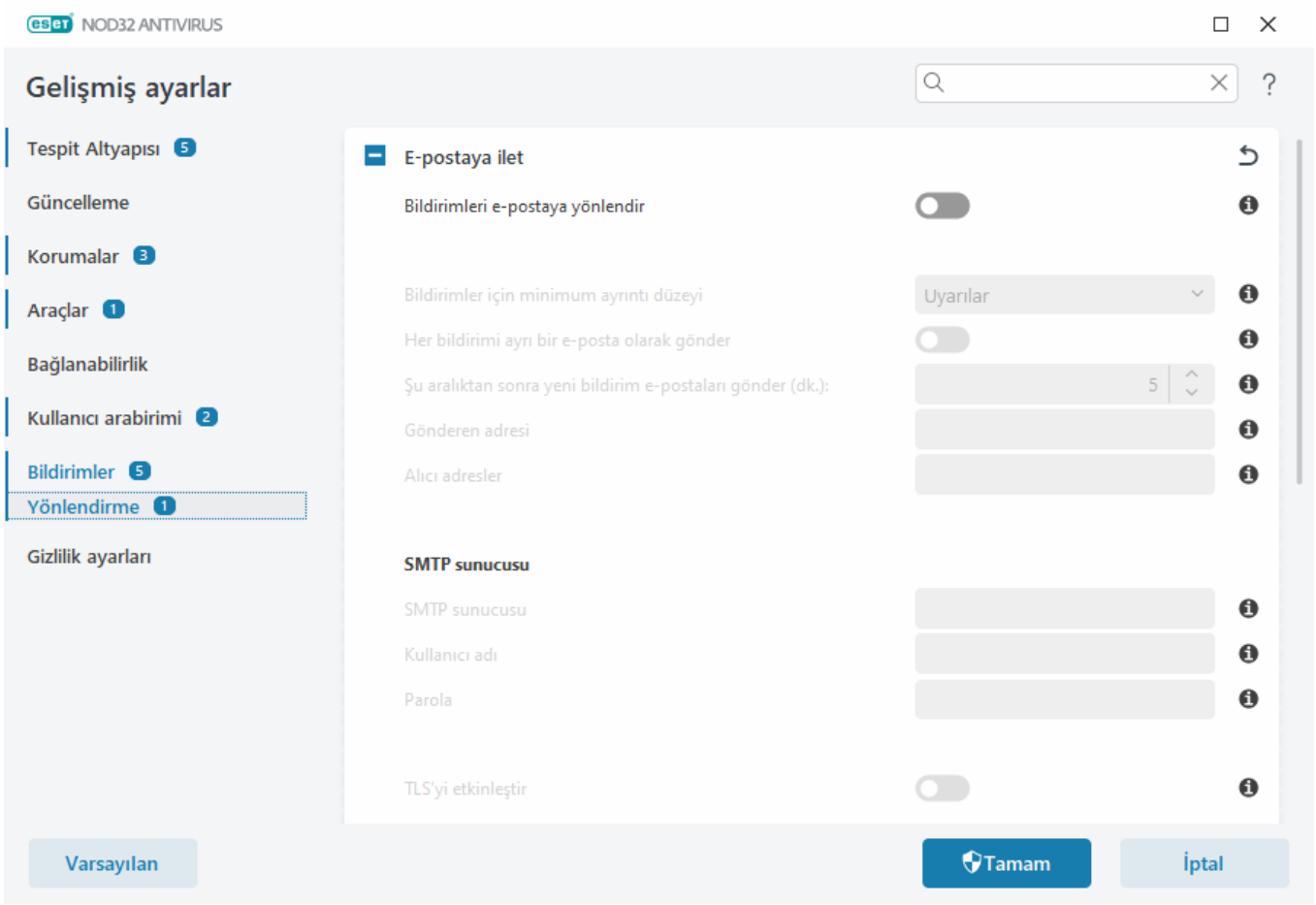
Onay iletileriyle ilgili belirli özellik hakkında daha fazla bilgi:

- 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
- 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

Yönlendirme

ESET NOD32 Antivirus, seçili ayrıntı düzeyine sahip bir olay meydana gelirse otomatik olarak bildirim e-postaları gönderebilir. Gelişmiş ayarlar > **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 (örneğin, güncelleme başarısız) kaydeder.
- **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 NOD32 Antivirus 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. Önceden tanımlı biçimi değiştirmemenizi öneririz. 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

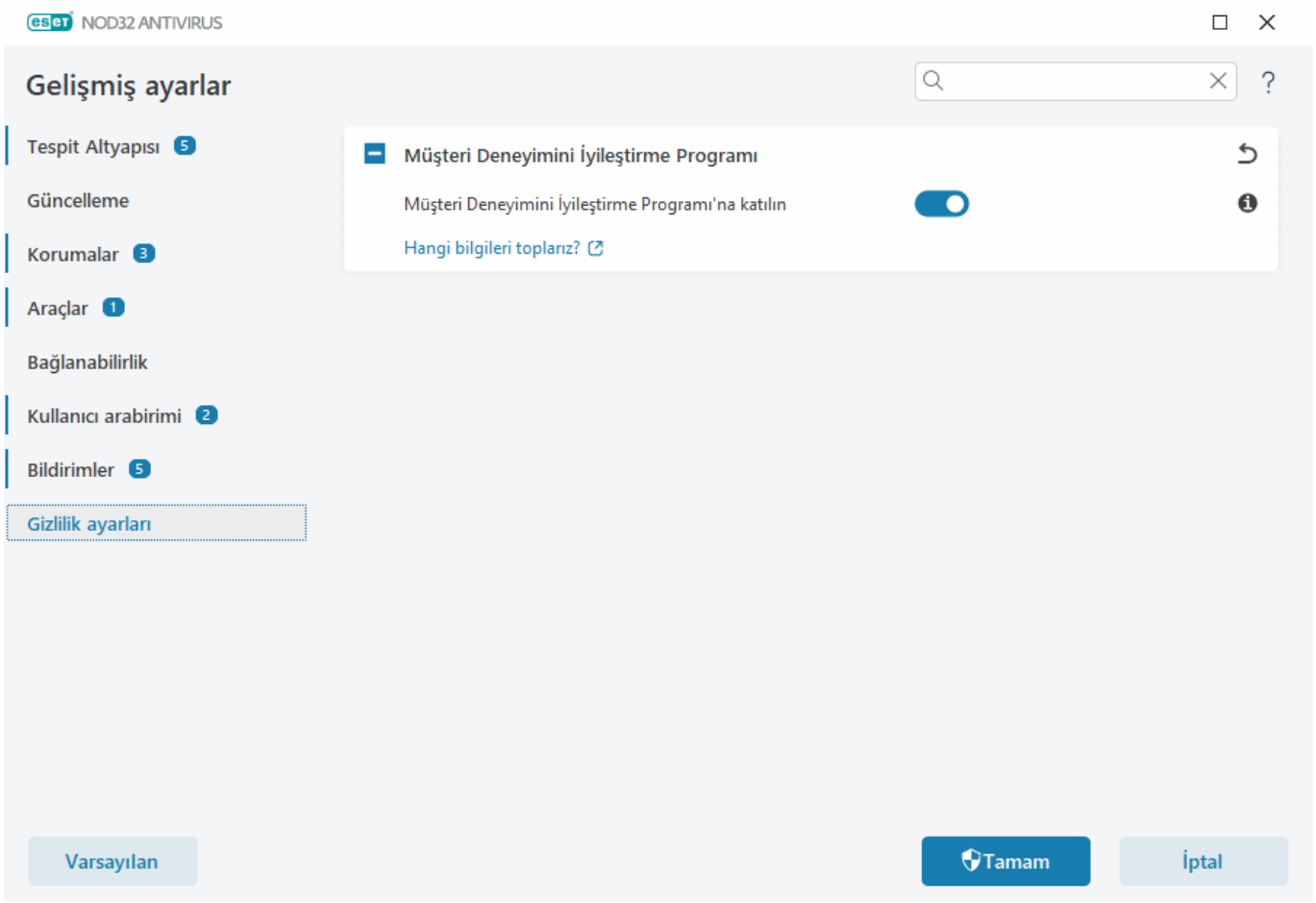
kodlanır.

- **%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

Gelişmiş ayarlar > **Gizlilik ayarları**'nı açın.



Müşteri Deneyimini İyileştirme Programı

Müşteri Deneyimini İyileştirme Programı'na katılmak için **Müşteri Deneyimini İyileştirme Programı'na katıl** seçeneğinin yanındaki açma/kapama düğmesini 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?

Varsayılan ayarlara döndür

Tüm program ayarları, tüm modüller için sahip oldukları durumlara döndürmek amacıyla **Gelişmiş ayarlar'da** Varsayılan'ı tıklayın. Bu, ayarları yeni bir yüklemenin ardından sahip olacakları değerlere sıfırlar.

Ayarları içe ve dışa aktarma bölümüne de bakın.

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.

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 NOD32 Antivirus 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.

SSS

En sık sorulan soruların ve karşılaşılan sorunların bazılarını aşağıda bulabilirsiniz. Sorununuzu nasıl çözebileceğinizi bulmak için konu başlığını tıklatın:

- ESET NOD32 Antivirus nasıl güncellenir?
- ESET NOD32 Antivirus bir tehdit algıladı
- Bilgisayarımdaki virüsü nasıl kaldırırım
- Zamanlayıcıda yeni bir görev oluşturulması
- Tarama görevini (haftalık olarak) zamanlama
- Gelişmiş ayarların kilidi nasıl açılır?
- Ürünün ESET HOME üzerinden devre dışı bırakılması nasıl çözümlenir?

Sorununuz yukarıdaki listede yer almıyorsa ESET NOD32 Antivirus Online Yardım'da aramayı deneyin.

Sorununuzun çözümünü veya sorunuzun yanıtını ESET NOD32 Antivirus Online Yardım'da bulamazsanız düzenli olarak güncellenen online ESET Bilgi Bankası'nı ziyaret edebilirsiniz. En popüler Bilgi Bankası makalelerimizin bağlantıları aşağıda yer almaktadır:

- Aboneliğimi nasıl yenileyeceğim?
- ESET ürünümü yüklerken bir etkinleştirme hatası aldım. Bunun anlamı nedir?
- Etkinleştirme anahtarını kullanarak ESET Windows ev ürünümü etkinleştirme
- ESET ev ürünümü kaldır veya yeniden yükle
- ESET yüklememin zamanından önce sona erdiğine ilişkin ileti aldım
- Aboneliğimi 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 NOD32 Antivirus nasıl güncellenir?

ESET NOD32 Antivirus 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 **Araçlar** > Zamanlayıcı'ya gidin.

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.

Daha fazla bilgi için şu bölüme bakın:

- ESET Bilgi Bankası makalesi
- Karantina

Zamanlayıcıda yeni bir görev oluşturulması

Araçlar > **Zamanlayıcı** içinde yeni bir görev oluşturmak için **Görev ekle** seçeneğini tıklatın veya sağ tıklatıp 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** > **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.

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** seçeneğine tıklayın ve abonelik 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 abonelik 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

Abonelik sahibi ESET HOME portalından ESET NOD32 Antivirus hesabınızı devre dışı bıraktığında veya ESET HOME hesabınızla paylaşılan abonelik artık paylaşılmadığında bu hata mesajı görüntülenir. Bu sorunu çözmek için:

- **Etkinleştir**'i tıklayın ve ESET NOD32 Antivirus ürününü etkinleştirmek için Etkinleştirme yöntemlerinden birini kullanın.

- ESET NOD32 Antivirus ürününüzün abonelik sahibi tarafından devre dışı bırakıldığı veya aboneliğin artık sizinle paylaşılmadığı bilgisiyle abonelik 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 NOD32 Antivirus ürününü etkinleştirmek için Etkinleştirme yöntemlerinden birini kullanın.

- ESET NOD32 Antivirus Ürününüzün devre dışı bırakıldığı ve cihazın ESET HOME üzerinden bağlantısının kesildiği bilgisiyle beraber abonelik sahibiyle iletişime geçin.

- Abonelik sahibi sizseniz ve bu değişikliklerden haberiniz yoksa ESET HOME Etkinlik feed'inizi gözden geçirin. 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 NOD32 Antivirus ürününü etkinleştirmek için Etkinleştirme yöntemlerinden birini kullanın.

- ESET NOD32 Antivirus Ürününüzün devre dışı bırakıldığı ve cihazın ESET HOME üzerinden bağlantısının kesildiği bilgisiyle beraber abonelik sahibiyle iletişime geçin.

- Abonelik sahibi sizseniz ve bu değişikliklerden haberiniz yoksa ESET HOME Etkinlik feed'inizi gözden geçirin. Şüpheli bir aktivite bulursanız hesap ESET HOME hesabına ait parolanızı değiştirin ve ESET Teknik Destek ekibiyle iletişime geçin.

Ürün etkinleştirilmedi

Abonelik sahibi ESET HOME portalından ESET NOD32 Antivirus hesabınızı devre dışı bıraktığında veya ESET HOME hesabınızla paylaşılan abonelik artık paylaşılmadığında bu hata mesajı görüntülenir. Bu sorunu çözmek için:

- **Etkinleştir**'i tıklayın ve ESET NOD32 Antivirus ürününü etkinleştirmek için Etkinleştirme yöntemlerinden birini kullanın.

- ESET NOD32 Antivirus ürününüzün abonelik sahibi tarafından devre dışı bırakıldığı veya aboneliğin artık sizinle paylaşılmadığı bilgisiyle abonelik sahibiyle iletişime geçin. Lisans sahibi bu sorunu ESET HOME çözebilir.

0

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 İlkesi

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