ESET Cyber Security

Kullanıcı Kılavuzu

Bu belgenin yardım sürümünü görüntülemek için burayı tıklayın

Digital Security
Progress. Protected.

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

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

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

REVİZE. 12.04.2024

ESET Cyber Security

ESET Cyber Security tamamen tümleşik bilgisayar güvenliğinde yepyeni bir yaklaşımın temsilcisidir. ESET LiveGrid® tarama motorunun en son sürümü, bilgisayarınızı güvende tutmak için hız ve hassasiyetten yararlanır.Sonuç, bilgisayarınızı saldırılara ve kötü amaçlı yazılımlara karşı koruyan, sürekli tetikte olan akıllı bir sistemdir.

ESET Cyber Security, maksimum koruma ve sistem kaynaklarının minimum kullanımını birleştirecek uzun soluklu bir çaba sonucunda oluşturulan tam bir güvenlik çözümüdür. Yapay zekayı temel alan, ESET Cyber Security ürününü oluşturan ileri teknolojiler; virüs, solucan, truva atı, casus yazılım, reklam yazılımı, kök seti ve diğer İnternet kaynaklı saldırıların neden olduğu sızıntıları sistem performansını engellemeksizin proaktif olarak engelleme yeteneğine sahiptir.

Sürüm 7›deki yenilikler

ESET Cyber Security sürüm 7 aşağıdaki güncellemeleri ve geliştirmeleri sunar:

- **Yüksek performanslı ve daha istikrarlı** - Her bileşeni daha yalıtılmış olan daha hafif bir yapıya sahiptir, yalnızca gerektiğinde başlatılır ve bir hata olması halinde uygulamanın tamamının kilitlenmesini önler. Daha iyi optimizasyon işlemleri daha hızlı ve etkili taramaya olanak sağlar.
- **ARM uyumluluğu** - ARM Mimarisine dayalı olarak Apple çip yerel desteğini içerir. Önceki sürümler ARM'i desteklemek için Rosetta 2'yi kullanıyordu.
- **Grafik kullanıcı arabirimi için yeni tasarım** - Koyu mod desteği içerir.
- **Çok dilli yükleyici** - Tüm dilleri tek bir yükleme dosyası halinde kapsar.
- **Otomatik güncellemeler** - Güncellemeleri arar ve yeni sürümleri otomatik olarak indirir, her güncelleme hakkında sizi bilgilendirir.
- **Uygulama Tercihleri** - Yeniden tasarlandı ve iyileştirildi.

ESET Cyber Security yeni özellikleri hakkında daha fazla bilgi için bu ESET Bilgi Bankası makalesine bakın.

Ayarları taşıma

7.2 ve üzeri sürümlerde,ESET Cyber Security sürüm 6'daki ayarlarınız yükseltme işlemi sırasında yeni sürüme otomatik olarak taşınır.

Taşıma işleminin ardından ESET Cyber Security ana ekranda başarılı ayarların başarıyla taşındığını belirten bir bildirim gösterir: **Ayarlarınız yeni sürüme aktarıldı**.

ESET Cyber Security Sürüm 6'dan sürüm 7 veya 7.1'e halihazırda yükselttiyseniz daha yeni bir sürüme yükselttiğinizde yine de ayarlarınızı taşıyabilirsiniz. Talimatlar için taşıma ile ilgili ESET Bilgi Bankası makalesine bakın.

7.X sürümünde mevcut olan tüm ayarlar sürüm 6'dan taşınacaktır, şunlar hariç tutulur:

- Ayrıcalık ayarları (sürüm 7'de desteklenmiyor)

- Güncellemeler için özel proxy sunucu (Özel proxy sürüm 7'de desteklenmiyor)
- İçeriği karantinaya alma
- Taramalar için temizleme düzeyleri
- İsteğe bağlı tarama için hedef profiller

Aşağıdaki özellikler için ayarlar .xml taşıma dosyasında depolanır ve özellikler ESET Cyber Security ürününün gelecek sürümlerinde mevcut olduğunda yüklenebilir:

- Aygıt denetimi
- Günlükler
- Web erişimi koruması
- Sunum modu

Sistem gereksinimleri

Ürününde en iyi performansı elde etmek için sisteminizin aşağıdaki donanım ve yazılım gereksinimlerini karşılaması gerekir:

	Sistem gereksinimleri:
İşlemci mimarisi	Intel 64-bit, M1, M2
İşletim sistemi	macOS Big Sur (11.0) ve üzeri
Bellek	300 MB
Boş disk alanı	600 MB
Diğer	İnternet bağlantısı, ürünü etkinleştirmek veya yükseltmek için gereklidir

ESET Cyber Security sürüm 7, ARM mimarisine sahip Apple çipleri için yerel destek sunuyor.

Yükleme

Yükleme işlemini başlatmadan önce açık olan tüm bilgisayar programlarınızı kapatın. ESET Cyber Security, bilgisayarınızda yüklü olan diğer antivirus programlarıyla çakışabilecek bileşenler içerir. Bu nedenle, olası sorunları önlemek için tüm diğer antivirus programlarının kaldırılmasını kesinlikle öneririz.

Yükleme sihirbazını başlatmak için ESET web sitesinden indirdiğiniz dosyayı açın ve **ESET Cyber Security ürününü yükle** simgesini tıklayın. Yükleme sihirbazı, size kurulumda yol gösterir.

ESET Cyber Security yükleme dosyası da ESET HOME ürününden indirilebilir. Daha fazla bilgi için ESET Bilgi Bankası makalesini okuyun.

Ekleme

ESET Cyber Security yüklemesinin ardından, **ekleme sihirbazı** görüntülenir. Bu sihirbaz, ESET Cyber Security ürününü tüm işlevleriyle kullanmanız için önerilen ve zorunlu adımlarla sizi yönlendiren bir ekran kümesidir.

1. **Önerilen Koruma Ayarları**'nı etkinleştirin, tercih ettiğiniz seçenekleri belirleyin ve **Devam**'ı tıklayın. **ESET LiveGrid®** veya **İstenmeyen türden olabilecek uygulamalar** ile ilgili daha fazla bilgi için sözlüğümüze bakın.

2. Zorunlu adım: **ESET Sistem Uzantılarını** Etkinleştir. Kuruluma devam etmek için ekrandaki talimatları uygulayın.

3. Zorunlu adım: **Proxy yapılandırmasına** izin verin. Uyarı penceresinde **İzin ver**'i tıklayın.

4. Zorunlu adım: ESET Cyber Security **Tam Disk Erişimi**'ne izin verin. Ekrandaki talimatları uygulayarak tam disk erişimine izin verin.

5. Bunun ardından sihirbaz, **ESET Cyber Security** ürününü etkinleştirmenizi ister. Etkinleştirme bölümünde birden çok etkinleştirme seçeneği bulabilirsiniz.

6. **Bildirimlere izin ver** Sisteminize yönelik tespit edilen tüm tehditler hakkında bilgi sahibi olmanız için bildirimlere izin vermenizi öneririz.

ESET Cyber Security Ekleme sihirbazını atlama.
Daha sonra ayarla'yı tıklayarak zorunlu ayarları atlayabilirsiniz, ancak korumanın yalnızca kısmen işlevsel olacağını unutmayın.

Ekleme sihirbazını yeniden başlatma
Finder > **Uygulamalar**'ı açın > Control tuşuna basarak **ESET Cyber Security** simgesini tıklayın (veya sağ tıklayın) > kısayol menüsünden **Paket içeriklerini göster**'i seçin > **Contents** > **Helpers** > **Kullanmaya başlayın**'ı açın. Ayrıca zorunlu güvenlik ayarlarını, Sistem uzantılarına izin ver ve Tam disk erişimine izin ver bölümlerini takip ederek manuel olarak da yapabilirsiniz.

ESET Cyber Security Ürününü yükledikten sonra kötü amaçlı kod için bilgisayarınızda bir tarama işlemi yapmalısınız. Ana program penceresinden, **Tarama** > **Şimdi tara**'yı tıklayın. İsteğe bağlı bilgisayar taramaları hakkında daha fazla bilgi için İsteğe bağlı bilgisayar taraması bölümüne bakın.

Sistem uzantılarına izin verilmesi

ESET Cyber Security ürününü ilk kez yüklüyorsanız **sistem uzantılarının** ESET Cyber Security tarafından korunmasına izin vermeniz gerekir. Bu, Katılım işleminin bir parçası olarak yapılabilir veya aşağıdaki adımları kullanarak **Sistem uzantılarına izin ver** işlemini manuel olarak tamamlayabilirsiniz:

macOS Ventura (13.x) ve üzeri bir sürüm kullanıyorsanız buradaki adımları izleyin

1. **Sistem Ayarları**'nı açın.
2. Soldaki menüden **Gizlilik ve Güvenlik**'i seçin.
3. **Güvenlik** bölümüne gidin ve "Bazı sistem yazılımları kullanılmadan önce ilgilenmenizi gerektirir" notunun altındaki **Ayrıntılar** düğmesini tıklayın.

"Bazı sistem yazılımları kullanılmadan önce ilgilenmenizi gerektiriyor" notu ve **Ayrıntılar** düğmesi kullanılamıyorsa sistem uzantılarına önceden izin verilmiştir ve başka bir işlem gerekmez.

4. **Touch ID**'nizi kullanın veya **Parolayı kullan**'ı tıklayın, **Kullanıcı adınızı** ve **Parolanızı** yazıp **Kilidi aç**'ı tıklayın.
5. Hem **ESET Gerçek Zamanlı Dosya Sistemi Koruması**'nı hem de **ESET Web ve E-posta Koruması**'nı açma-kapama düğmelerini tıklayarak etkinleştirin.
6. **Tamam**'ı tıklayın.
7. **ESET Web ve E-posta Koruması** uyarısını gösterilerek **proxy yapılandırması eklemeniz** istenir. Burada **İzin Ver**'i seçin. Uyarı gösterildiğinde proxy yapılandırmasına izin vermezseniz uyarıyı başlatmak ve proxy yapılandırmasına yeniden izin verme seçeneğini görüntülemek için bilgisayarınızı yeniden başlatmanız gerekir.
Ayrıntılı bir adım adım açıklamalı kılavuz için Bilgi Bankası makalemizi ziyaret edin. (Bilgi Bankası makaleleri tüm dillerde mevcut değildir.)

macOS Monterey (12.x) veya önceki bir sürümü kullanıyorsanız buradaki adımları izleyin

1. **Sistem Tercihleri**'ni açın.
2. **Güvenlik ve Gizlilik** seçeneğini belirleyin.
3. Ayarlar penceresinde değişikliklere izin vermek için sol alttaki kilit simgesini tıklayın.
4. **Touch ID**'nizi kullanın veya **Parolayı kullan**'ı tıklayın**,** Kullanıcı adınızı ve Parolanızı yazıp **Kilidi aç**'ı tıklayın.
5. **Ayrıntılar**'ı tıklayın.
6. Tüm **ESET Cyber Security** seçeneklerini işaretleyin.
7. **Tamam**'ı tıklayın.

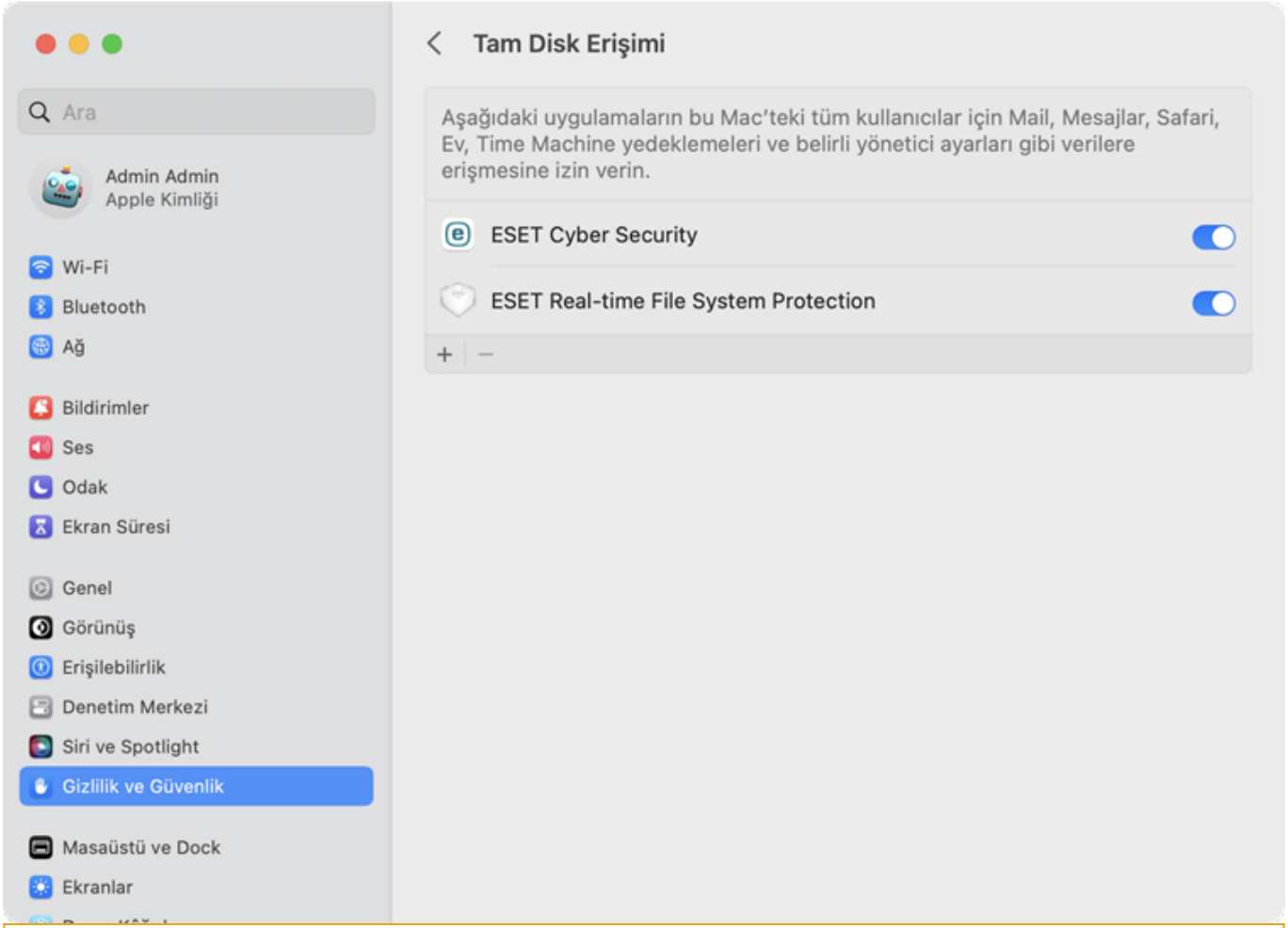
Ekleme sihirbazını yeniden başlatma
Finder > **Uygulamalar**'ı açın > Control tuşuna basarak **ESET Cyber Security** simgesini tıklayın (veya sağ tıklayın) > kısayol menüsünden **Paket içeriklerini göster**'i seçin > **Contents** > **Helpers** > **Kullanmaya başlayın**'ı açın. Ekleme sihirbazı, ESET Cyber Security tam korumasından yararlanmanız için gerekli adımlarla sizi yönlendirecektir.

Tam disk erişimine izin verin.

ESET Cyber Security ürününü ilk kez yüklüyorsanız ESET Cyber Security tarafından korunmak için **Tam Disk Erişimi**'ne izin vermeniz gerekir. Bu, Katılım işleminin bir parçası olarak yapılabilir veya aşağıdaki adımları kullanarak **Tam Disk Erişimi'ne izin ver** işlemini manuel olarak tamamlayabilirsiniz:

macOS Ventura (13.x) veya üzeri bir sürümü kullanıyorsanız buradaki adımları izleyin

1. **Sistem Ayarları**'nı açın.
2. Soldaki menüden **Gizlilik ve Güvenlik**'i seçin.
3. **Tam Disk Erişimi** seçeneğini tıklayın ve etkinleştirmek için ESET Cyber Security açma/kapama düğmesini tıklayın.
4. **Touch ID**'nizi kullanın veya **Parolayı Kullan**'ı tıklayın ve Kullanıcı Adınızı ve Parolanızı yazıp **Kilidi Aç**'ı tıklayın.
5. ESET Cyber Security aracını yeniden başlatma istemi görüntülenirse **Daha Sonra**'yı tıklayın.
6. Etkinleştirmek için **ESET Gerçek Zamanlı Dosya Sistemi Koruması**'nın düğmesini açıp tıklayın.



Gerçek Zamanlı Dosya Sistemi Koruması seçeneği kullanılamıyorsa ESET ürününüz için sistem uzantılarına izin vermeniz gerekir.

7. Sistem uzantılarını ve Tam Disk Erişimini etkinleştirdikten sonra bilgisayarınızı yeniden başlatın. Daha ayrıntılı bilgi için Bilgi Bankası makalemizi ziyaret edin.

macOS Monterey (12.x) veya önceki bir sürümü kullanıyorsanız buradaki adımları izleyin

1. **Sistem Tercihleri**'ni açın.
2. **Gizlilik** sekmesine gidin ve soldaki menüden **Tam Disk Erişimi**'ni seçin.
3. Ayarlar penceresinde değişikliklere izin vermek için sol alttaki kilit simgesini tıklayın.
4. **Touch ID**'nizi kullanın veya **Parolayı Kullan**'ı tıklayın ve Kullanıcı Adınızı ve Parolanızı yazıp **Kilidi Aç**'ı tıklayın.
5. Listeden **ESET Cyber Security** ürününü seçin.
6. ESET Cyber Security Ürününü yeniden başlatma bildirimi görüntülenir. Daha **Sonra'yı tıklayın.**
7. Listeden **ESET Gerçek Zamanlı Dosya Sistemi Koruması**'nı seçin.

Gerçek Zamanlı Dosya Sistemi Koruması seçeneği kullanılamıyorsa ESET ürününüz için sistem uzantılarına izin vermeniz gerekir.

8. ESET Cyber Security ürününü yeniden başlatmak için uyarı iletişim penceresinde **Yeniden başlat**'ı tıklayın veya bilgisayarınızı yeniden başlatın. Daha ayrıntılı bilgi için Bilgi Bankası makalemizi ziyaret edin.

Ekleme sihirbazını yeniden başlatma
Finder > **Uygulamalar**'ı açın > Control tuşuna basarak **ESET Cyber Security** simgesini tıklayın (veya sağ tıklayın) > kısayol menüsünden **Paket içeriklerini göster**'i seçin > **Contents** > **Helpers** > **Kullanmaya başlayın**'ı açın. Ekleme sihirbazı, ESET Cyber Security tam korumasından yararlanmanız için gerekli adımlarla sizi yönlendirecektir.

Ürün etkinleştirme

Ürün Etkinleştirme penceresi, başlama adımlarından biri olarak gösterilir. Ürün etkinleştirme işlemi, başlama sürecinde yapılmamışsa ESET Cyber Security uygulamasında herhangi bir zamanda erişilebilir. Uygulamayı başlatmak için macOS menü çubuğunda bulunan ESET Cyber Security simgesini (ekranın üst kısmında) tıklayın ve ESET Cyber Security aracını göster'i seçin. **Ürün Etkinleştirme** uyarısı **Genel Bakış** bölümünde gösterilir. Uyarı, **etkinleştirme iletişim kutusuna** bir bağlantı içerir. Etkinleştirme iletişim kutusu açıldıktan sonra şunları belirtin:

- **Etkinleştirme Anahtarı ile etkinleştir** - Abonelik sahibini tanımlayan ve aboneliği etkinleştiren etkinleştirme anahtarınızı yazın. Etkinleştirme anahtarı şu biçimdeki benzersiz bir dizedir: XXXX-XXXX-XXXX-XXXX-XXXX veya XXXX-XXXXXXXX.
- **Ücretsiz deneme** - Satın almadan önce ESET Cyber Security ürününü değerlendirmek için bu seçeneği belirleyin. Bilgilerinizi yazın ve ESET Cyber Security ürününü sınırlı bir süre etkinleştirmek için **Kaydolun**'u tıklayın. Deneme lisansları yalnızca her bir müşteri için etkinleştirilebilir.
- **Abonelik satın alın** - Abonelik satın almak için bu seçeneği tıklayın. Bu sizi yerel ESET distribütörünüzün web sitesine yönlendirir.
- **ESET HOME** hesabınızı kullanın - ESET HOME hesabınıza giriş yapın ve ESET ürününü cihazınızda etkinleştirmek için bir abonelik seçin.
- **Daha sonra etkinleştir** - Etkinleştirme işlemini hemen yapmak istemiyorsanız bu seçeneği tıklayın.

Etkinleştirme anahtarının nerede bulunacağı hakkında daha fazla bilgi için aşağıdaki ESET Bilgi Bankası makalesini ziyaret edin.

Aboneliğimi nerede bulabilirim?

Çevrim içi olarak bir abonelik satın aldıysanız ESET'ten etkinleştirme anahtarınızı (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX), genel kimliğinizi (xxx-xxx-xxx), ürün adını (veya ürün listesini) ve miktarını içeren bir e-posta almış

olmalısınız. Ürünün kutulu bir sürümünü satın aldıysanız etkinleştirme anahtarı ürün paketinin içinde veya arka yüzünde yer alır.

Etkinleştirme anahtarınız çalışmıyorsa aşağıdaki ESET Bilgi Bankası makalesini ziyaret edin.

Kaldır

ESET Cyber Security aracını kaldırmak için aşağıdaki adımları uygulayın:

1. **Finder**'ı başlatın
2. Sabit sürücüdeki **Uygulamalar** klasörünü açın.
3. **ESET Cyber Security** simgesini Control tuşuna basarak tıklayın (veya sağ tıklayın).
4. Kısayol menüsünden **Paket içeriklerini göster**'i seçin.
5. **Contents** > **Helpers** klasörünü açın ve **Uninstaller** simgesini çift tıklayın.

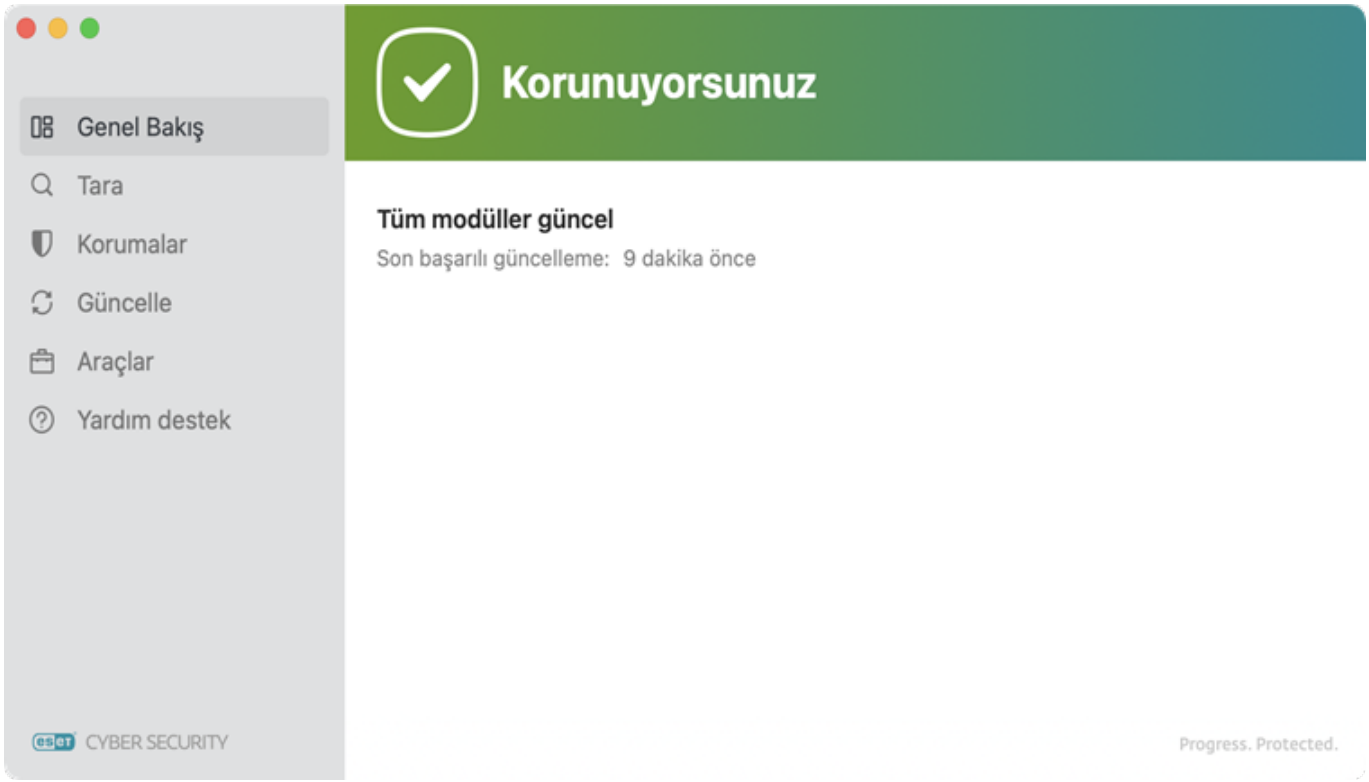
ESET Cyber Security Yükleme dosyasını (.dmg) sakladıysanız açın ve **Yüklemeyi** kaldır'ı çift tıklayın.

ESET Cyber Security ile çalışma

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

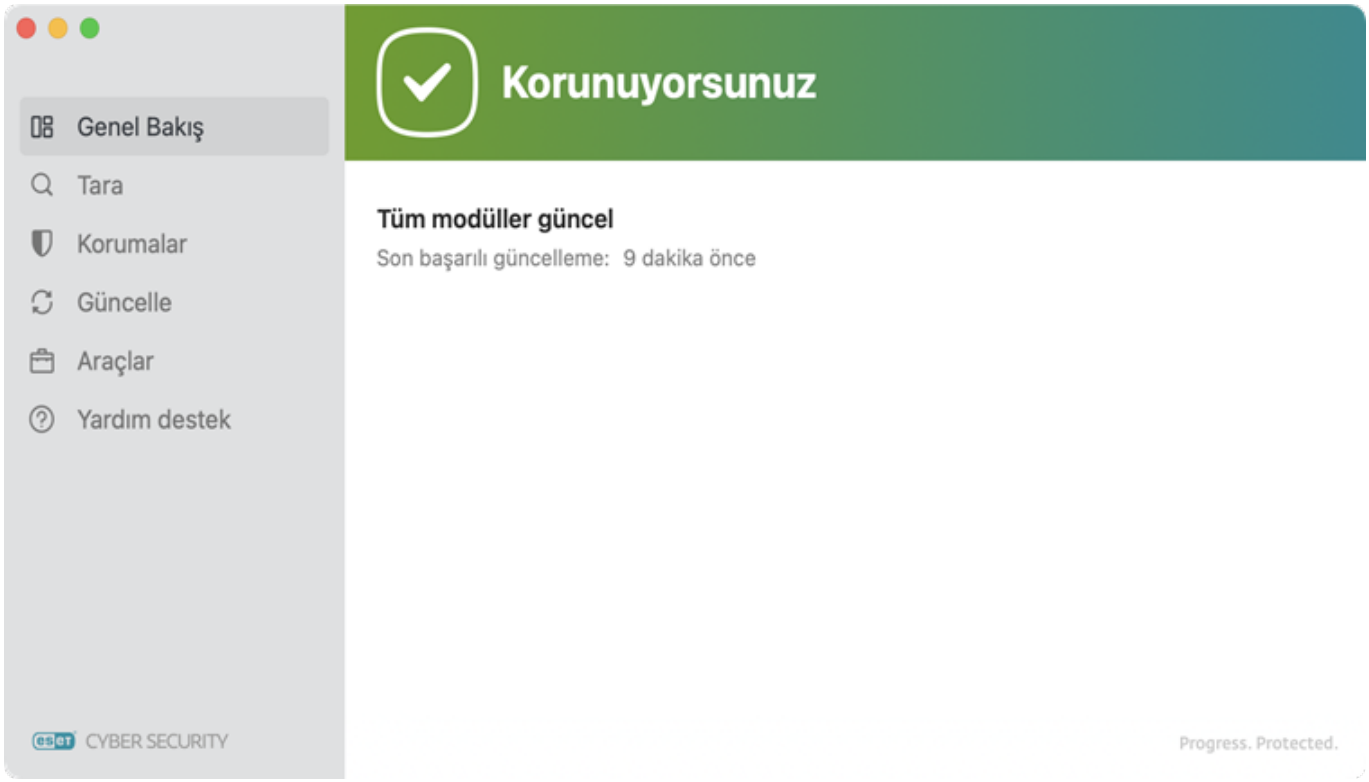
Ana menüden şu bölümlere erişebilirsiniz:

- **Genel Bakış** - ESET Cyber Security modüllerinin işleyişi hakkında durum özeti bilgilerini sağlar.
- **Tarama** - Tüm yerel diskleri taramanızı veya özel tarama çalıştırmanızı sağlar.
- **Korumalar** - Bilgisayarınızın güvenlik düzeyinin ayarlanmasına izin verir.
- **Güncelleme** – Algılama modülleri hakkındaki bilgileri görüntüler.
- **Araçlar** - Günlük dosyalarına ve karantinaya erişim sağlar.
- **Yardım ve Destek** - Yardım dosyalarına, ESET Bilgi Bankası'na, destek isteği formuna ve ek program bilgilerine erişim sağlar.



Koruma durumunu denetleme

Koruma durumunuzu görüntülemek için ana menüden **Genel Bakış** seçeneğini belirleyin. Birincil pencerede, ESET Cyber Security modüllerinin çalışması hakkında bir durum özeti görüntülenir.



Yardım ve destek

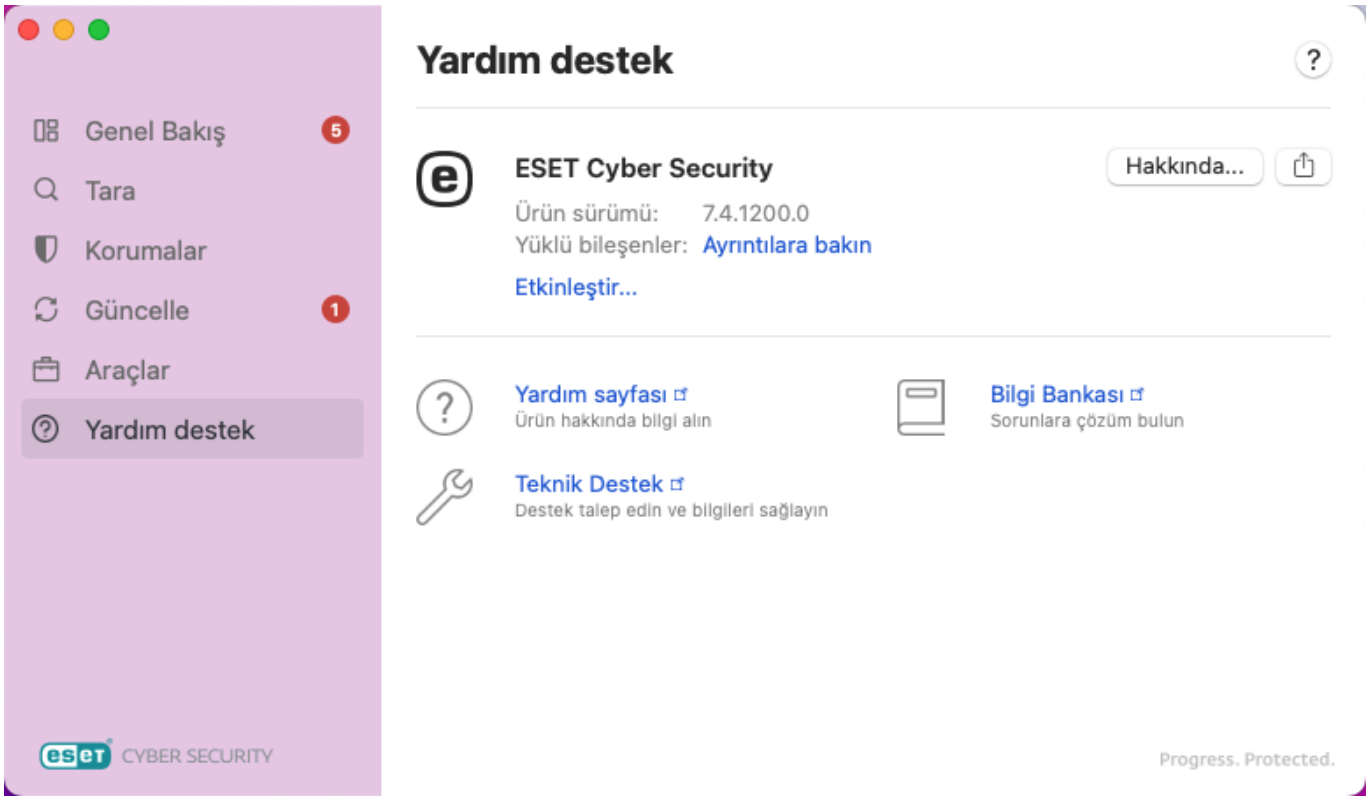
ESET Cyber Security, karşılaşabileceğiniz sorunları çözmede size yardımcı olacak sorun giderme araçlarını ve destek bilgilerini içerir. Ana uygulama penceresinde Yardım ve Destek bölümünü bulabilirsiniz. Yüklü bileşenlerin listesini göstermek için **Yüklü bileşenler**'in yanındaki **Ayrıntılara bakın**'ı tıklayın. Listeyi panoya kopyalamak için Yüklü bileşenler penceresinde herhangi bir yeri sağ tıklayıp **Tümünü kopyala**'yı tıklayın. Bu özellik Teknik Destekle iletişim kurarken veya sorun giderme sırasında faydalı olabilir.

ESET Cyber Security Ürün sürümü ve Ürün Abonelik Kimliği gösterilir. Aboneliğinizi değiştirme seçeneği vardır. Etkinleştirme penceresini başlatmak ve ürününüzü etkinleştirmek için bu seçeneği tıklayın. **Hakkında** düğmesini tıklayarak daha fazla ESET Cyber Security ayrıntısı görüntüleyebilirsiniz.

Yardım sayfası – ESET Cyber Security yardım sayfalarını açmak için bu bağlantıyı tıklatın.

Teknik Destek - Yardım sayfalarımızı kullanarak sorunu çözebiliyorsanız ESET Teknik Destek ekibiyle iletişime geçin.

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.



Ayarları al ve ver

Mevcut bir yapılandırmayı içe veya aktarmak veya ESET Cyber Security yapılandırmanızı dışa aktarmak için ESET Cyber Security ana uygulama penceresini açın, ekranın sol üstündeki macOS menü çubuğunda bulunan **Dosya** > **Ayarları içe veya dışa aktar**'ı tıklayın.

Geçerli ESET Cyber Security yapılandırmasını ileri bir tarihte kullanmak için yedeklemeniz gerekiyorsa alma ve

verme işlemleri kullanışlıdır. Ayarları ver seçeneği de, tercih ettikleri ESET Cyber Security yapılandırmasını birden fazla sistemde kullanmak isteyen kullanıcılar için uygundur. İstediğiniz ayarları aktarmak için bir yapılandırma dosyasını kolayca alabilirsiniz.

Yapılandırmayı içe aktarmak için **Ayarları içe aktar**'ı seçin ve içe aktarmak istediğiniz yapılandırma dosyasına gidin. Vermek için **Ayarları içe aktar** seçeneğini belirleyin ve yapılandırma dosyasını kaydetmek için bilgisayarınızda konum belirlemek üzere tarayıcıyı kullanın.

Klavye kısayolları

ESET Cyber Security ürününde aşağıdaki klavye kısa yollarını kullanabilirsiniz:

- cmd+, - ESET Cyber Security tercihlerini görüntüler,
- cmd+Q - ESET Cyber Security ana GUI penceresini gizler. Bunu macOS menü çubuğundaki ekranın üst tarafında yer alan ESET Cyber Security simgesini tıklayarak ve **ESET Cyber Security ürününü göster**'i seçerek açabilirsiniz,
- cmd+W - ESET Cyber Security ana GUI penceresini kapatır.

Program düzgün çalışmadığında yapılacaklar

Tüm modüller doğru şekilde işlev gösterdiğinde **Genel Bakış** bölümünde yeşil renkli **Korunuyorsunuz** başlığı görüntülenir. Bir modül arızalı olduğunda kırmızı bir **Güvenlik uyarısı** başlığı veya turuncu bir **İlgilenmenizi gerektiriyor** başlığı görüntülenir. ESET Cyber Security modülle ilgili ek bilgileri ve sorunları düzeltmek için önerilen çözümü gösterir. Modüllerin durumunu tek tek değiştirmek için, her bildirim iletisinin altındaki mavi bağlantıyı tıklatın.

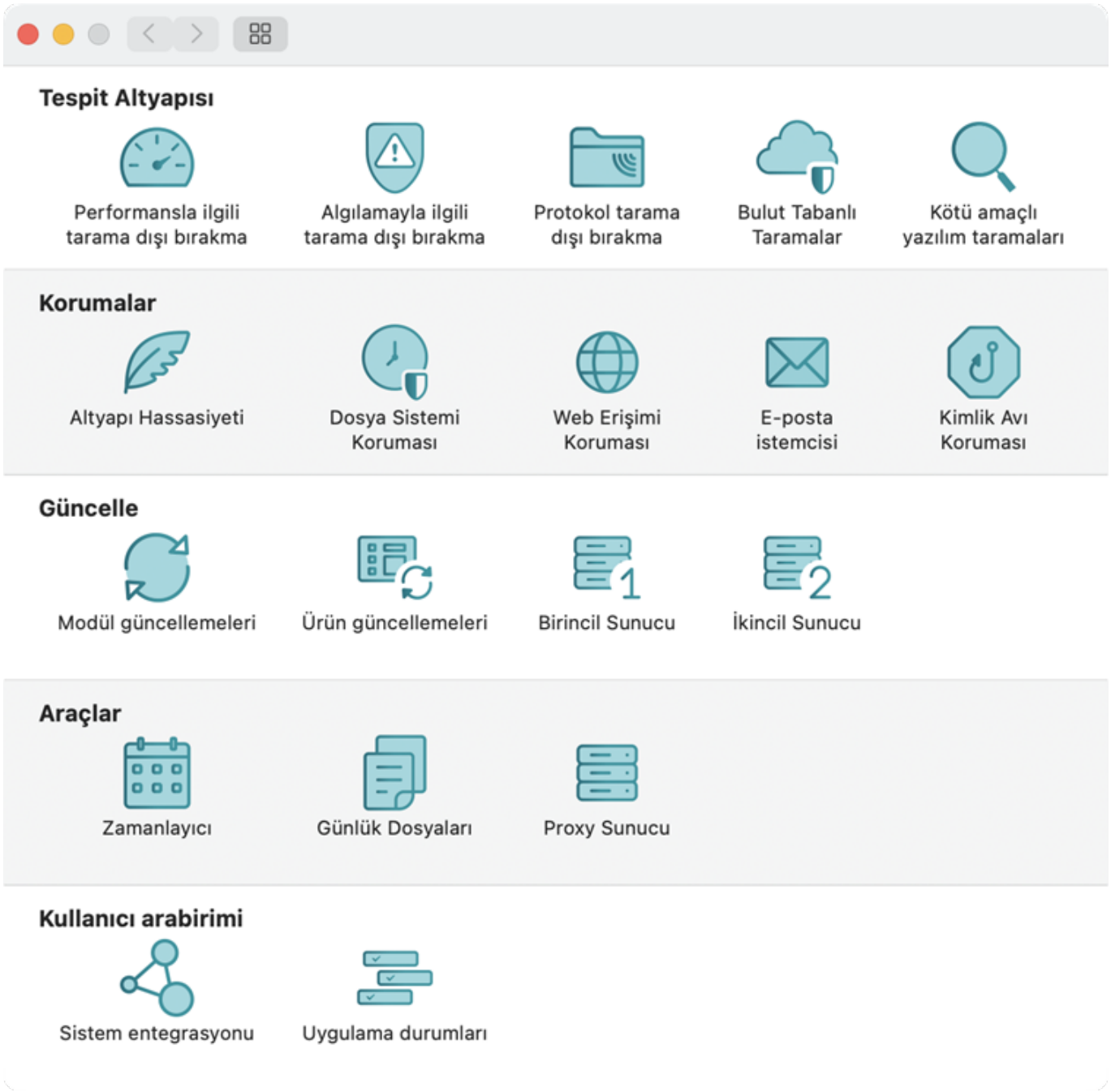
Önerilen çözümleri kullanarak sorunu çözemiyorsanız ESET Bilgi Bankası'nda arama yapın veya ESET Teknik Destek ekibiyle iletişime geçin.

Uygulama Tercihleri

ESET Cyber Security ürününün gelişmiş ayarlarını değiştirmek için cmd+, kombinasyonunu kullanarak **Uygulama Tercihleri**'ni açın veya macOS menü çubuğundan ESET Cyber Security öğesini tıklayıp **Tercihler**'i (Ayarlar) seçin.

Aşağıdaki kategorilerdeki modüllerin ayarlarını yapılandırabilirsiniz:

- Algılama altyapısı
- Korumalar
- Güncelleme
- Araçlar
- Kullanıcı arabirimi



Algılama altyapısı

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

ESET Cyber Security **Tespit Altyapısı** gelişmiş ayarlarını değiştirmek için cmd+, kombinasyonunu kullanarak **Uygulama Tercihleri**'ni açın veya macOS menü çubuğundan ESET Cyber Security öğesini tıklayıp **Tercihler**'i (Ayarlar) seçin.

Performansla ilgili tarama dışı bırakma işlemleri

Performansla ilgili tarama dışı bırakma işlemleri bölümünde, belirli dosyaları/klasörleri, uygulamaları veya IP/IPv6 adreslerini tarama dışında bırakabilirsiniz. Yolları (klasörleri) tarama dışı bırakarak zararlı yazılımlara karşı dosya sistemini taramak için gereken süre önemli ölçüde azaltılabilir.

-  – yeni bir tarama dışı öğe oluşturur. Nesnenin yolunu girin.
-  – Seçilen girişleri kaldırır.

Dosyaları yalnızca gerçek zamanlı korumayla ilgili ciddi sorunlar yaşadığınızda taramadan hariç tutmalısınız, aksi halde dosyaları taramanın dışında tutmak genel korumayı azaltır.

Algılamayla ilgili tarama dışı bırakma işlemleri

Bu işlev tespit adını, nesne yolunu veya hash'ini filtreleyerek nesneleri temizleme işleminin dışında bırakmanıza olanak tanır.

Tespit dışında bırakma işlemlerini ayarlarken belirli tarama dışı bırakma ölçütlerinin belirtilmesi gerekir. Geçerli bir tespit adı veya SHA-1 hash'i sağlanmalıdır. Geçerli tespit adı veya SHA-1 hash'i için Günlük dosyaları'na bakın ve Günlük dosyaları açılır menüsünden Tespitler'i seçin. ESET Cyber Security ürününde hatalı pozitif bir örnek algılandığında bu seçenek kullanılır. Gerçek sızıntılar için tarama dışı öğeler çok tehlikeli olduğundan, yalnızca etkilenen dosyaları veya klasörleri geçici bir süreliğine tarama dışı bırakmanız önerilir. Tarama dışı bırakma İstenmeyen türden olabilecek uygulamalar, tehlikeli olabilecek uygulamalar ve şüpheli uygulamalar için de geçerlidir.

Aşağıdaki türde **tarama dışı bırakma kriterleri** vardır:

- **Spesifik dosya** – Bir dosyayı; dosya türü, konumu, adı veya uzantısı ne olursa olsun belirtilen hash'e SHA-1 göre hariç tutar.
- **Algılama** – Her dosyayı algılama adına göre tarama dışı bırakın.
- **Yol ve Algılama** – Her dosyayı dosya adı da dahil olmak üzere (ör. `file:///Users/documentation/Downloads/eicar_com.zip`) algılama adına ve yoluna göre tarama dışı bırakın.

Zararlı yazılımları tarama dışında bırakmak genel korumayı azalttığından, tespitlerin tarama dışı bırakılmasını yalnızca zararlı yazılım gibi bir şeyi tespitle ilgili ciddi sorunlar yaşıyorsanız kullanmalısınız.

Protokol tarama dışı bırakma işlemleri

Tarama dışı bırakma listelerindeki girişler protokol içeriği filtreleme dışında bırakılır. Bu seçeneği yalnızca güvenilir olduğu bilinen uygulamalar ve adresler için kullanmanızı öneririz.

Bulut Tabanlı Taramalar

ESET LiveGrid® bilinirlik sistemini etkinleştirin (önerilir)

ESET LiveGrid® itibar sistemi, taranan dosyaları bulutta yer alan beyaz ve kara listelerden oluşan bir veri tabanıyla karşılaştırarak ESET anti-malware çözümlerinin etkililiğini geliştirir.

ESET LiveGrid® Geri bildirim sistemini etkinleştirebilirsiniz

Veriler, daha ayrıntılı inceleme için ESET Virus Lab'a gönderilir.

Örneklerin gönderimi

Tespit edilen örneklerin otomatik gönderimi: Tercih edilen seçeneğe dayalı olarak bu, etkilenen örnekleri analiz etmek ve gelecekte daha iyi tespit edilebilmesini sağlamak için ESET Research Lab'a gönderilebilir.

- Algılanan tüm örnekler
- Belgeler dışındaki tüm örnekler
- Gönderme

Şüpheli örneklerin otomatik gönderimi: Tehditlere benzeyen şüpheli örnekler ve sıra dışı özellikleri ya da davranışları olan örnekler analiz için ESET Research Lab'a gönderilir.

- Yürütülebilir - .exe, .dll, .sys gibi yürütülebilir dosyaları içerir
- Arşivler - Arşiv dosya türlerini içerir: .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- Komut dosyaları - Komut dosyası türlerini içerir: .bat, .cmd, .hta, .js, .vbs, .ps1
- Belgeler - Microsoft Office, Libre Office veya başka bir ofis aracında oluşturulan belgeleri ya da etkin içerikli PDF'leri içerir.
- Diğer - Şu dosya türlerini içerir: .jar, .reg, .msi, .swf, .lnk

Otomatik gönderimleri tarama dışı bırakma: Tarama dışı bırakılan dosyalar, şüpheli kod içerse bile ESET Research Lab'a gönderilmez.

Kilitlenme raporlarını ve tanılama verilerini gönder

Kilitlenme raporları, modüller veya bellek dökümleri gibi verileri gönderin.

Anonim kullanım istatistikleri göndererek ürünü iyileştirmemize yardımcı olun

ESET'in yeni tespit edilen tehditler hakkında tehdit adı, tespit tarihi ve saati, tespit yöntemi ve ilgili meta veriler, taranan dosyalar (hash, dosya adı, dosyanın kaynağı, telemetri), engellenen ve şüpheli URL'ler, sisteminizle ilgili bilgiler de dahil olmak üzere ürün sürümü ve yapılandırması gibi bilgileri toplamasına izin verin.

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.

Kötü amaçlı yazılım taramaları

İsteğe bağlı tarayıcı, antivirus çözümünüzün önemli bir parçasıdır ve bilgisayarınızda dosya ve klasörlerin taramalarını gerçekleştirmek için kullanılır. Güvenlik açısından, güvenlik taramalarının yalnızca enfeksiyondan şüphelenildiğinde değil, rutin güvenlik önlemlerinin parçası olarak düzenli şekilde yapılması önemlidir. **Zararlı yazılım taramaları** bölümünde, İsteğe bağlı tarama profilleri için seçenekleri yapılandırabilirsiniz:

Profil listeleri - Yeni bir profil oluşturmak veya mevcut bir profili kaldırmak için  ya da  öğesini seçin. Yeni bir profil eklerken profil için bir ad yazıp **Tamam'ı** tıklayın. Yeni profil, mevcut tarama profillerini listeleyen Seçili profil açılır menüsünde görüntülenir.

ThreatSense parametreleri – Denetlemek istediğiniz dosya uzantıları, kullanılan algılama yöntemleri vb. gibi gelişmiş ayar seçenekleri bu bölümde bulunabilir.

Korumalar

ESET Cyber Security için gelişmiş **koruma** ayarlarını değiştirmek üzere cmd+, kombinasyonunu kullanarak **Uygulama Tercihleri**'ni açın veya macOS menü çubuğundan ESET Cyber Security öğesini tıklayıp **Tercihler**'i (Ayarlar) seçin.

Altyapı Hassasiyeti

Altyapı hassasiyeti, tüm koruma modülleri için aşağıdaki kategorilerin raporlama ve koruma düzeylerini yapılandırmaya olanak sağlar.

- **Zararlı yazılım** - Bilgisayarınızda bulunan dosyaların bir parçası olan kötü amaçlı kod parçası

- **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 yükleyebilir, dijital cihazın 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. Paketleyici, çeşitli kötü amaçlı yazılım türlerini tek bir pakette birleştiren, çalışma zamanında kendi kendini ayıklayan yürütülebilir bir dosyadır. En yaygın paketleyiciler arasında UPX, PE_Compact, PKLite ve ASPack yer alır. Aynı zararlı yazılım, farklı bir paketleyici kullanılarak sıkıştırıldığında farklı şekilde tespit edilebilir. Ayrıca paketleyiciler "imzalarını" zaman içinde mutasyona uğratarak zararlı yazılımların tespit edilip kaldırılmasını zorlaştırabilirler.

- **Tehlikeli olabilecek uygulamalar** - Bu uygulamalar, kullanıcının izni olmadan yüklendiyse saldırganlar

tarafından kötü amaçla kullanılabilecek ticari ve yasal yazılımlardır. Bu sınıflandırma, uzaktan erişim araçları gibi programları içerir. Bu seçenek varsayılan olarak devre dışıdır.

Dosya Sistemi Koruması

ESET LiveGrid® teknolojisini kullanan (ThreatSense altyapı parametre ayarlarında açıklanmaktadır), gerçek zamanlı dosya sistemi koruması yeni oluşturulan dosyalar ve mevcut dosyalar için değişiklik gösterebilir. Yeni oluşturulan dosyalar daha kesin olarak kontrol edilebilir.

Aşağıdaki medya türlerini Real-time tarayıcısı dışında bırakabilirsiniz:

- **Yerel sürücüler** - sistem sabit sürücüleri
- **Çıkarılabilir medya** - USB medyası, Bluetooth cihazları gibi
- **Ağ medyası** - tüm eşlenen sürücüler

Varsayılan olarak, tüm dosyalar **dosya açma** ve **dosya oluşturma** sırasında taranır. Bilgisayarınız için en üst düzeyde gerçek zamanlı koruma sağladığından, ESET bu varsayılan ayarları korumanızı önerir.

Ayrıca belirli işlemleri de tarama dışı bırakabilirsiniz.

Varsayılan ayarları kullanmanızı ve yalnızca belirli durumlarda dışarıda bırakılan tarama öğelerini değiştirmenizi (ör; bazı medyaları tarama işlemi veri aktarımını önemli derecede yavaşlattığında) öneririz.

Web erişimi koruması

Web erişimi koruması, HTTP (Köprü Metni Aktarım Protokolü) kurallarına uygunluk için web tarayıcıları ile uzak sunucular arasındaki iletişimi izler.

HTTP iletişimi ve URL adresleri için bağlantı noktası numaralarını tanımlayarak web filtrelemesini gerçekleştirebilirsiniz.

Web protokolleri

Web protokolleri bölümünde, HTTP protokolü denetlemesini etkinleştirebilir veya devre dışı bırakabilirsiniz ve HTTP iletişimi için kullanılan bağlantı noktası numaralarını tanımlayabilirsiniz. Bağlantı noktası numaraları 80, 8080 ve 3182 varsayılan olarak önceden tanımlanmıştır.

URL adresi yönetimi

Bu bölüm, engellenecek, izin verilecek veya denetleme dışında bırakılacak HTTP adreslerini belirtmenizi sağlar. Engellenen adresler listesindeki web sitelerine erişilemez. Dışarıda bırakılan adresler listesindeki web sitelerine, bu sitelere kötü amaçlı kod taraması yapılmaksızın erişilebilir.

İzin verilen, engellenen veya hariç tutulan adreslerin listesini etkinleştirmek için bir adres seçin ve **Etkin olarak listele** seçeneğini etkinleştirin. Geçerli listedeki bir adrese girilirken bildirim almak istiyorsanız **Uygulanırken bildirim gönder** seçeneğini etkinleştirin.

Herhangi bir listede *(yıldız) ve ?(soru işareti) özel sembollerini kullanabilirsiniz. Yıldız işareti herhangi bir

karakter dizesinin, soru işareti de herhangi bir sembolün yerine geçer. Hariç bırakılan adresler listesinin yalnızca güvenilir ve güvenli adresleri içermesi gerektiğinden, hariç bırakılan adresleri belirlerken çok dikkatli olmak gerekir. Benzer şekilde * ve ? sembollerinin bu listede doğru kullanıldığından emin olmalısınız.

E-posta istemcisi koruması

E-posta koruması, POP3 ve IMAP protokolleri ile alınan e-posta iletişimlerinin denetimini sağlar. Program, gelen iletileri incelerken ESET Cyber Security, ThreatSense tarama altyapısında bulunan tüm gelişmiş tarama yöntemlerini kullanır. POP3 ve IMAP protokolü iletişimlerinin taranması, kullanılan e-posta istemcisinden bağımsızdır. Şu ayarlar kullanılabilir:

E-posta protokolleri

Burada POP3 ve IMAP protokolleri aracılığıyla alınan e-posta iletişimlerinin denetimini etkinleştirebilir veya devre dışı bırakabilirsiniz.

POP3 protokol denetimi

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

Bu denetimi sağlayan koruma modülü, sistem başlatıldığında otomatik olarak başlatılır ve bellekte etkin halde kalır. Protokol filtrelemenin düzgün çalışması için modülün etkin olduğundan emin olun. POP3 protokol denetimi, e-posta istemcinizi yeniden yapılandırmaya gerek olmadan otomatik olarak gerçekleştirilir. Varsayılan olarak, bağlantı noktası 110 üzerindeki tüm iletişim taranır ancak gerekirse başka iletişim bağlantı noktaları da ekleyebilirsiniz. Birden çok bağlantı noktası virgülle ayrılmalıdır.

POP3 protokol denetimi seçeneğini etkinleştirirseniz tüm POP3 trafiği zararlı yazılımlara karşı izlenir.

IMAP protokol denetimi

Internet İleti Erişim Protokolü (IMAP), e-posta alımına yönelik başka bir Internet protokolüdür. IMAP protokolünün POP3'e göre bazı avantajları vardır. Örneğin, birden fazla istemci aynı posta kutusuna aynı anda bağlanabilir ve iletinin okunup okunmadığı, yanıtlanıp yanıtlanmadığı veya silinip silinmediği gibi ileti durumu bilgilerini koruyabilir. ESET Cyber Security, kullanılan e-posta istemcisi dikkate alınmaksızın bu protokol için koruma sağlar.

Bu denetimi sağlayan koruma modülü, sistem başlatıldığında otomatik olarak başlatılır ve bellekte etkin halde kalır. Modülün düzgün çalışması için IMAP protokol denetlemesinin etkinleştirildiğinden emin olun. IMAP protokol denetimi, e-posta istemcinizi yeniden yapılandırmaya gerek olmadan otomatik olarak gerçekleştirilir. Varsayılan olarak, bağlantı noktası 143 üzerindeki tüm iletişim taranır ancak gerekirse başka iletişim bağlantı noktaları da ekleyebilirsiniz. Birden çok bağlantı noktası virgülle ayrılmalıdır.

IMAP protokol denetimini etkinleştirirseniz IMAP üzerindeki tüm trafik zararlı yazılımlara karşı izlenir.

E-posta etiketleri

E-posta etiketlerini kullanmak, etiket mesajını e-posta dipnot bölümüne eklemenizi sağlar. Bir e-posta tarandıktan sonra tarama sonuçlarını içeren bir bildirim iletiye eklenebilir. Etiket mesajları faydalı bir araç olsa da mesaj güvenliğinin nihai belirleyicisi olarak kullanılmamalıdır. Aksi halde, sorunlu HTML mesajlarında göz ardı edilebilir ve belirli tehditler tarafından taklit edilebilirler. Aşağıdaki seçenekler kullanılabilir:

- **Bir tespit olduğunda alınan ve okunan e-posta için** - Yalnızca zararlı yazılım içeren e-posta "denetlendi" olarak etiketlenir.
- **Taranan tüm e-postalar için** - Taranan tüm e-postalara etiket mesajları eklenir.
- **Hiçbir zaman** - Etiket mesajları herhangi bir e-postaya eklenmez.

Alınan e-postanın konusunu güncelleyin – E-posta korumasının etkilenen e-postalara bir tehdit uyarısı eklemesini istiyorsanız bu onay kutusunu işaretleyin. Bu özellik, etkilenen e-postalara yönelik basit filtrelemeye olanak sağlar. Ayrıca, alıcı için güvenilirlik düzeyini artırır ve sızıntı algılanması durumunda, belirtilen e-posta veya gönderenin tehdit düzeyi ile ilgili değerli bilgiler sağlar.

Tespit edilen e-postanın konusuna ekle – Etkilenen bir e-postanın konu ön eki biçimini değiştirmek isterseniz bu şablonu düzenleyin.

ThreatSense Parametreleri

Gelişmiş tarayıcı ayarları, tarama dışında bırakılan temizleme düzeylerini, tarama seçeneklerini ve dosya uzantılarını yapılandırmanıza olanak sağlar.

Kimlik Avı Koruması

Kimlik Avı koruması parolaları ve diğer hassas bilgileri edinmeye çalışan, yasal olmayan web sitelerine karşı korumayı artırmayı sağlayan başka bir koruma katmanıdır. Kimlik Avı Koruması varsayılan olarak etkindir ve etkin durumda bırakılması önerilir.

Güncelleme

Bu bölüm, kullanılan güncelleme sunucuları gibi güncelleme kaynağı bilgilerini ve bu sunucular için kimlik doğrulama verilerini belirtir. ESET Cyber Security ürününün gelişmiş **güncelleme** ayarlarını değiştirmek için cmd+, kombinasyonunu kullanarak **Uygulama Tercihleri**'ni açın veya macOS menü çubuğundan ESET Cyber Security öğesini tıklayıp **Tercihler**'i (Ayarlar) seçin.

Modül ve Ürün Güncellemeleri

Modül güncellemeleri

Güncelleme türü

- **Düzenli güncelleme**. Bu, varsayılan güncelleme türüdür ve tespit imza veri tabanının ve ürün modüllerinin ESET güncelleme sunucularından otomatik olarak güncellenmelerini sağlar.
- **Sürüm öncesi güncellemeler**, kısa bir süre içinde kullanıma sunulacak olan en son hata düzeltmelerini ve tespit yöntemlerini içerir. Ancak, her zaman istikrarlı olmayabilirler; bu nedenle, bunların bir üretim ortamında kullanılması önerilmez.
- **Gecikmeli güncellemeler**, özel güncelleme sunucularından güncelleme gerçekleştirilmesine olanak tanır

ve en az X saat gecikme ile virüs veri tabanlarının yeni sürümlerini sağlar (ör. gerçek bir ortamda test edilmiş ve istikrarlı olarak görülen veri tabanları).

Modül geri alımı

Tespit altyapısının veya program modüllerinin yeni güncellemesinin istikrarsız veya bozuk olduğundan şüpheleniyorsanız önceki sürüme geri alabilir ve güncellemeleri geçici olarak devre dışı bırakabilirsiniz.

Modüllerin sistem görüntülerini oluştur

ESET Cyber Security, geri alma özelliğiyle birlikte kullanılmak üzere tespit altyapısının ve program modüllerinin sistem görüntülerini kaydeder. Modül 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 (örneğin üç) ulaşıldıysa en eski sistem görüntüsü 48 saatte bir yeni bir sistem görüntüsüyle değiştirilir. macOS için ESET Cyber Security, tespit altyapısı ve program modülü güncelleme sürümlerini en eski sistem görüntüsüne döndürür.

Ürün güncellemeleri

Ürün güncellemeleri, her zaman en son ürün sürümünü kullanmanızı sağlar. Ürün güncellemelerinin bir sonraki yeniden başlatmada otomatik olarak yüklenmesi ve en son özelliklere sürekli erişim ve mümkün olan en yüksek korumayı sürdürmek için **Otomatik Güncellemeler** düğmesini etkinleştirin.

Birincil Sunucu ve İkincil Sunucu

Birincil ve ikincil güncelleme sunucularını otomatik olarak seçme seçeneği varsayılan olarak etkindir. Otomatik olarak seçmek için kullanılan açma-kapama düğmesi devre dışı bırakıldıktan sonra her iki sunucu da belirtilebilir.

Araçlar

ESET Cyber Security **Araçları**'nın gelişmiş ayarlarını değiştirmek için cmd+, kombinasyonunu kullanarak **Uygulama Tercihleri**'ni açın veya macOS menü çubuğundan ESET Cyber Security öğesini tıklayıp **Tercihler**'i (Ayarlar) seçin.

Zamanlayıcı

Belirli bir zamanda otomatik olarak yürütülen isteğe bağlı tarama görevleri ayarlayabilirsiniz. Yeni bir zamanlanmış görev oluşturmak veya mevcut bir görevi kaldırmak için + ya da − simgesini seçin. Ayrıca, görevin hangi gün veya günlerde tekrarlanması gerektiğini de tanımlayabilirsiniz.

Günlük dosyaları

Günlük Ayrıntı Düzeyi

Günlüğe kaydetme ayrıntı düzeyi, günlük dosyalarının barındırdığı ayrıntıların düzeyini tanımlar.

- **Kritik uyarılar** - Yalnızca kritik hatalar içerir (örneğin: **Antivirus koruması başlatılamadı**).
- **Hatalar** - **"Dosya indirme hatası"** gibi hatalar kritik uyarılara ek olarak kaydedilir.
- **Uyarılar** - Kritik hatalar ve uyarı mesajları hatalara ek olarak kaydedilir.
- **Bilgilendirici** – Başarılı güncelleme iletileri dahil olmak üzere bilgilendirici iletileri ve yukarıdaki tüm kayıtları kaydeder.
- **Tanılama kayıtları** - Programla ilgili hassas ayarlama gerektiren bilgileri ve yukarıdaki tüm kayıtları içerir.

Günlük Dosyaları Temizliği

(Gün) günden eski **kayıtları otomatik olarak sil** - Belirtilen gün sayısından daha eski günlük girişleri otomatik olarak silinir.

Günlük Dosyaları Optimizasyonu

Günlük dosyalarını otomatik olarak optimize et – Bağlanıldığında bölümlere ayırma yüzdesi **Kullanılmayan kayıt sayısı şu değeri aşarsa (%)**: alanında belirtilen değerden daha büyükse günlük dosyaları otomatik olarak birleştirilir. Tüm boş günlük girişleri performansı ve günlük işleme hızını artırmak için silinir. Bu iyileştirme özellikle çok sayıda girdi içeren günlüklerde gözlenebilir.

Proxy sunucu ayarları

Burada proxy sunucu ayarlarını belirtebilirsiniz. Buradaki parametreler İnternet bağlantısının gerekli olduğu tüm modüller tarafından kullanılır.

Proxy sunucuyu yapılandırmak için:

1. **Proxy sunucu kullan'ı** etkinleştirin ve proxy sunucu alanına proxy sunucunun adresini ve proxy sunucunun bağlantı noktası numarasını girin.
2. Proxy kullanılamıyorsa proxy'yi atlamak ve ESET sunucularıyla doğrudan iletişim kurmak için **Doğrudan bağlantıyı kullan** seçeneğini etkinleştirin.
3. **Proxy sunucu ile iletişim için kimlik doğrulaması gerekliyse** proxy sunucu kimlik doğrulaması gerektirir seçeneğini etkinleştirip ilgili alanlara geçerli **kullanıcı adı** ve **parolayı** girin.

Kullanıcı arabirimi

ESET Cyber Security **Kullanıcı arabirimi** gelişmiş ayarlarını değiştirmek için cmd+, kombinasyonunu kullanarak **Uygulama Tercihleri**'ni açın veya macOS menü çubuğundan ESET Cyber Security öğesini tıklayıp **Tercihler**'i (Ayarlar) seçin.

Sistem entegrasyonu

Kullanıcı arabirimi öğeleri

Kullanıcının grafik kullanıcı arabirimini açmasına izin ver - Kullanıcıların GUI'ye erişmesini önlemek için bu ayarı devre dışı bırakın. Bu mod, yönetilen ortamlarda veya sistem kaynaklarınızı korumanız gereken durumlarda yararlıdır.

Simgeyi menü çubuğu ekstralarında göster - macOS menü çubuğunun Menü Çubuğu Ekstraları bölümündeki (ekranın üst kısmında) ESET Cyber Security simgesini kaldırmak için bu ayarı devre dışı bırakın.

Bildirimler

Bildirimleri masaüstünde görüntüle - Masaüstü bildirimleri (başarılı güncelleme mesajları, virüs tarama görevlerinin tamamlanması veya yeni tehditler bulundu gibi) macOS menü çubuğunun yanında bulunan küçük bir açılır pencereyle temsil edilir. Etkinleştirilirse ESET Cyber Security yeni bir olay meydana geldiğinde sizi bilgilendirilebilir.

Uygulama durumları

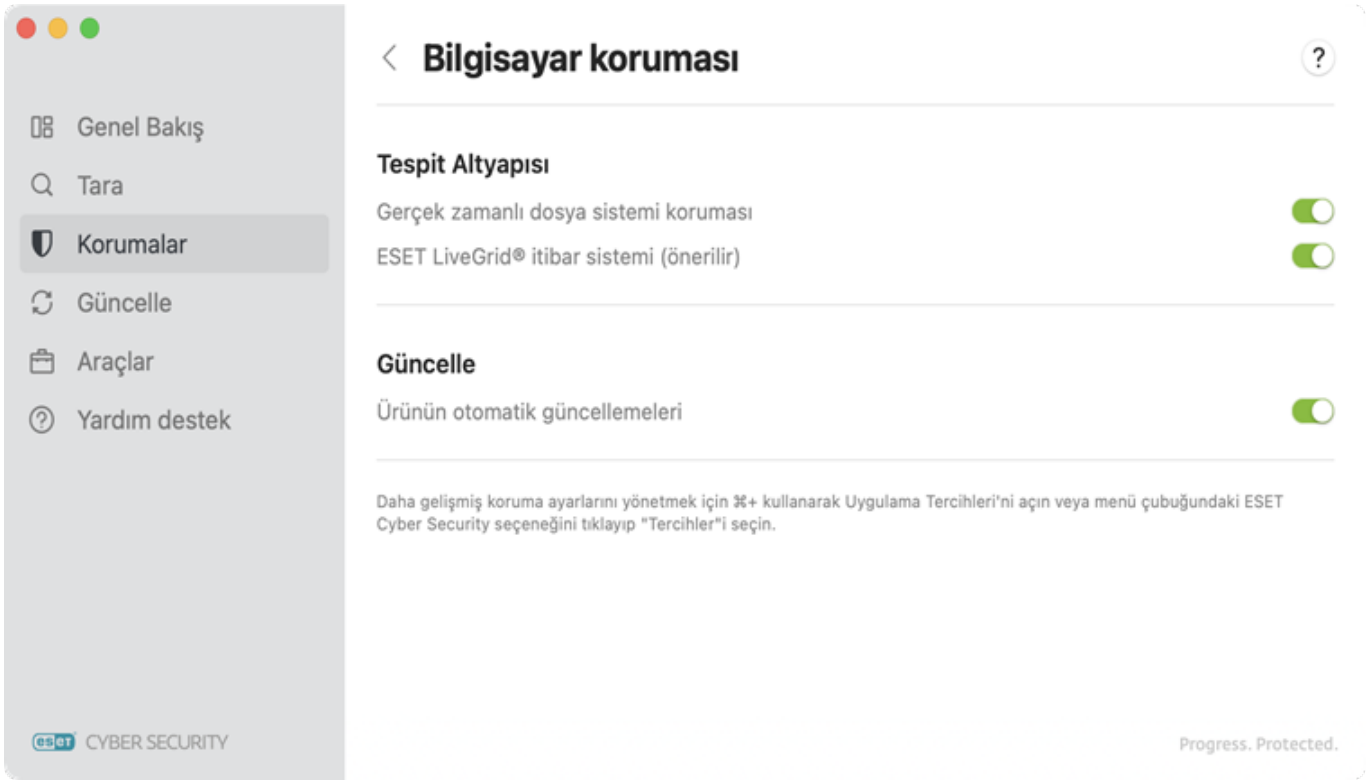
Burada, ESET Cyber Security ürününüzde hangi uygulama durumlarının gösterileceğini seçebilirsiniz. **Durumu göster** anahtarı devre dışı bırakıldığında ve bir sorun bildirildiğinde ESET Cyber Security uygulamanız yeşil renkli **Korunuyorsunuz** durumunu devam ettirir.

Korumalar

Ana uygulama penceresindeki **Korumalar** seçeneği bilgisayarınız, web ve e-postanız için koruma düzeyini ayarlamanıza olanak sağlar. Hem Bilgisayar koruması hem de Web/E-posta koruması bölümleri etkinleştirilebilen veya devre dışı bırakılabilen koruma modülleri içerir. ESET Cyber Security aracından en iyi şekilde yararlanmak ve bilgisayarınızı güvende tutmak için tüm modülleri etkin durumda bırakmanızı kesinlikle öneririz.

Bilgisayar koruması

Bilgisayar koruması yapılandırmasını **Korumalar** > **Bilgisayar** altında bulabilirsiniz. Bu pencere, **Gerçek zamanlı dosya sistemi korumasının** ve **ESET LiveGrid® bilinirlik sistemi** modüllerinin durumunu gösterir. Her iki modülü de etkin durumda tutmanızı öneririz. Bunlardan birini kapatmanız bilgisayarınızın koruma düzeyini düşürebilir.



Güncelleme bölümünde **Otomatik güncelleme** özelliğini etkinleştirmek veya devre dışı bırakmak için açma/kapama anahtarını tıklayabilirsiniz. Otomatik güncelleme etkinleştirildiğinde ESET Cyber Security en son ürün güncellemelerini bulup bunları otomatik olarak indirir.

Web ve E-posta koruması

Web ve Posta korumasına erişmek için ana menüde **Korumalar** > **Web ve E-posta** seçeneklerini tıklayın. Her modül için daha gelişmiş ayarları yönetmek üzere cmd+, kombinasyonunu kullanarak **Uygulama Tercihleri**'ni açın veya macOS menü çubuğundan ESET Cyber Security öğesini tıklayıp **Tercihler**'i (Ayarlar) seçin. Aşağıdaki koruma modülleri web ve e-posta koruması içerisinde mevcuttur:

- **Web** - Web tarayıcıları ve uzak sunucular arasındaki HTTP iletişimini izler.
- **Kimlik Avı Koruması** - Web siteleri veya etki alanlarından gelen potansiyel kimlik avı saldırılarını engeller.
- **E-posta** - POP3 ve IMAP protokolleri aracılığıyla alınan e-posta iletişiminin denetimini sağlar.

Özel durumları tarama
ESET Cyber Security şifrelenen protokoller (HTTPS, POP3S ve IMAPS) taramaz.

Kimlik Avı koruması

Kimlik avı, sosyal mühendisliği (kullanıcıları gizli bilgilerini elde etmek için manipüle etmek) kullanan bir suç faaliyetidir. Kimlik avının amacı genellikle banka hesap numaraları, kredi kartı numaraları, PIN kodları, kullanıcı adları veya parolalar gibi hassas verilere erişim kazanmaktır. Kimlik avı hakkında ESET Sözlüğü'nde daha fazla bilgi edinebilirsiniz.

Kimlik avı korumasını etkin durumda tutmanızı öneririz (Korumalar > Web ve E-posta > Kimlik Avı Koruması).

Tehlikeli web sitelerinden veya etki alanlarından gelen tüm olası kimlik avı saldırıları engellenir ve sizi söz konusu saldırı konusunda bilgilendiren bir uyarı bildirimi görüntülenir.

Kimlik Avı Koruması'nın çalışıp çalışmadığını test etmek için AMTSO test sayfasına başvurun.

Antivirus ve antispyware koruması

Antivirus koruması, olası tehdit oluşturan dosyaları değiştirerek kötü amaçlı sistem saldırılarına karşı koruma sağlar. Kötü amaçlı kod içeren bir tehdit algılanırsa, Antivirus modülü bu tehdidi engelleyerek, sonra da temizleyerek, silerek veya karantinaya taşıyarak yok edebilir.

Gerçek zamanlı dosya sistemi koruması

Gerçek zamanlı dosya sistemi koruması tüm medya türlerini denetler ve çeşitli olaylara dayalı olarak bir taramayı tetikler. ESET LiveGrid® teknolojisini kullanan (ThreatSense altyapı parametre ayarlarında açıklanmaktadır), gerçek zamanlı dosya sistemi koruması yeni oluşturulan dosyalar ve mevcut dosyalar için değişiklik gösterebilir. Yeni oluşturulan dosyalar daha kesin olarak kontrol edilebilir.

Gerçek zamanlı dosya sistemi koruması için gelişmiş ayarları değiştirmek üzere cmd+, kombinasyonunu kullanarak **Uygulama tercihleri**'ni açın veya macOS menü çubuğundan **ESET Cyber Security** öğesini tıklayın ve **Tercihler** > **Gerçek Zamanlı Koruma**'yı seçin.

Varsayılan olarak, tüm dosyalar **dosya açma** ve **dosya oluşturma** sırasında taranır. Bilgisayarınız için en üst düzeyde gerçek zamanlı koruma sağladığından, ESET bu varsayılan ayarları korumanızı önerir. Varsayılan olarak koruma, sistem başlatılırken başlatılır ve kesintisiz tarama sağlar. Özel durumlarda (örneğin, başka bir gerçek zamanlı tarayıcıyla çakışma varsa) ana program penceresinden gerçek zamanlı korumayı durdurabilirsiniz (**Korumalar** > **Bilgisayar**'ı tıklayın ve **Gerçek zamanlı dosya sistemi koruması**'nı kapatın).

Aşağıdaki medya türlerini Real-time tarayıcısı dışında bırakabilirsiniz:

- **Yerel sürücüler** - sistem sabit sürücüleri
- **Çıkarılabilir medya** - CD'ler, DVD'ler, USB medyası, Bluetooth cihazlar vb.
- **Ağ medyası** - tüm eşlenen sürücüler

Ayrıca belirli işlemleri de tarama dışı bırakabilirsiniz.

Varsayılan ayarları kullanmanızı ve yalnızca belirli durumlarda dışarıda bırakılan tarama öğelerini değiştirmenizi (ör; bazı medyaları tarama işlemi veri aktarımını önemli derecede yavaşlattığında) öneririz.

Gerçek zamanlı koruma yapılandırması ne zaman değiştirilir?

ESET Cyber Security ile güvenli bir sistem sağlamak için gerçek zamanlı koruma gereklidir. Gerçek zamanlı koruma parametrelerini değiştirirken dikkatli olun. Bu parametreleri yalnızca belirli durumlarda (örneğin, belirli bir uygulamayla çakışmanın olduğu bir durumda) değiştirmenizi öneririz.

ESET Cyber Security Yüklendikten sonra, kullanıcılara en üst düzeyde sistem güvenliği sağlamak için tüm ayarlar en iyi duruma getirilir.

Gerçek zamanlı korumayı denetleme

Gerçek zamanlı korumanın çalıştığını ve virüsleri algıladığını doğrulamak için eicar.com test dosyasını indirip ESET Cyber Security ürününün bu dosyayı bir tehdit olarak algılayıp algılamadığını kontrol edin. Bu sınama dosyası tüm antivirus programları tarafından algılanabilen özel bir zararsız dosyadır. Avrupa Bilgisayar Antivirus Araştırmaları Enstitüsü (EICAR enstitüsü), antivirus programlarının işlevselliğini test etmek için dosyayı oluşturdu.

Gerçek zamanlı koruma çalışmıyorsa neler yapılabilir

Burada, gerçek zamanlı koruma kullanılırken oluşabilecek sorunları ve bunların nasıl çözümleneceğiyle ilgili bilgiler yer almaktadır.

Gerçek zamanlı koruma devre dışı bırakılmış

Gerçek zamanlı koruma kullanıcı tarafından yanlışlıkla devre dışı bırakılırsa korumayı yeniden etkinleştirmeniz gerekir. Gerçek zamanlı korumayı ana menüden yeniden etkinleştirmek için **Gerçek zamanlı dosya sistemi korumasını** açma/kapama düğmesini tıklayın. Alternatif olarak, uygulama tercihleri penceresine gidin ve gerçek zamanlı dosya sistemi korumasını etkinleştirmek için **Gerçek Zamanlı Koruma**'yı tıklayın.

Gerçek zamanlı koruma sızıntıları algılamıyor ve temizlemiyor

Bilgisayarınızda başka antivirus programları yüklü olmadığından emin olun. İki gerçek zamanlı koruma kalkanı aynı anda etkinleştirilirse, birbirleriyle çakışabilirler. Sisteminizde bulunabilecek diğer antivirus programlarını kaldırmanızı öneririz.

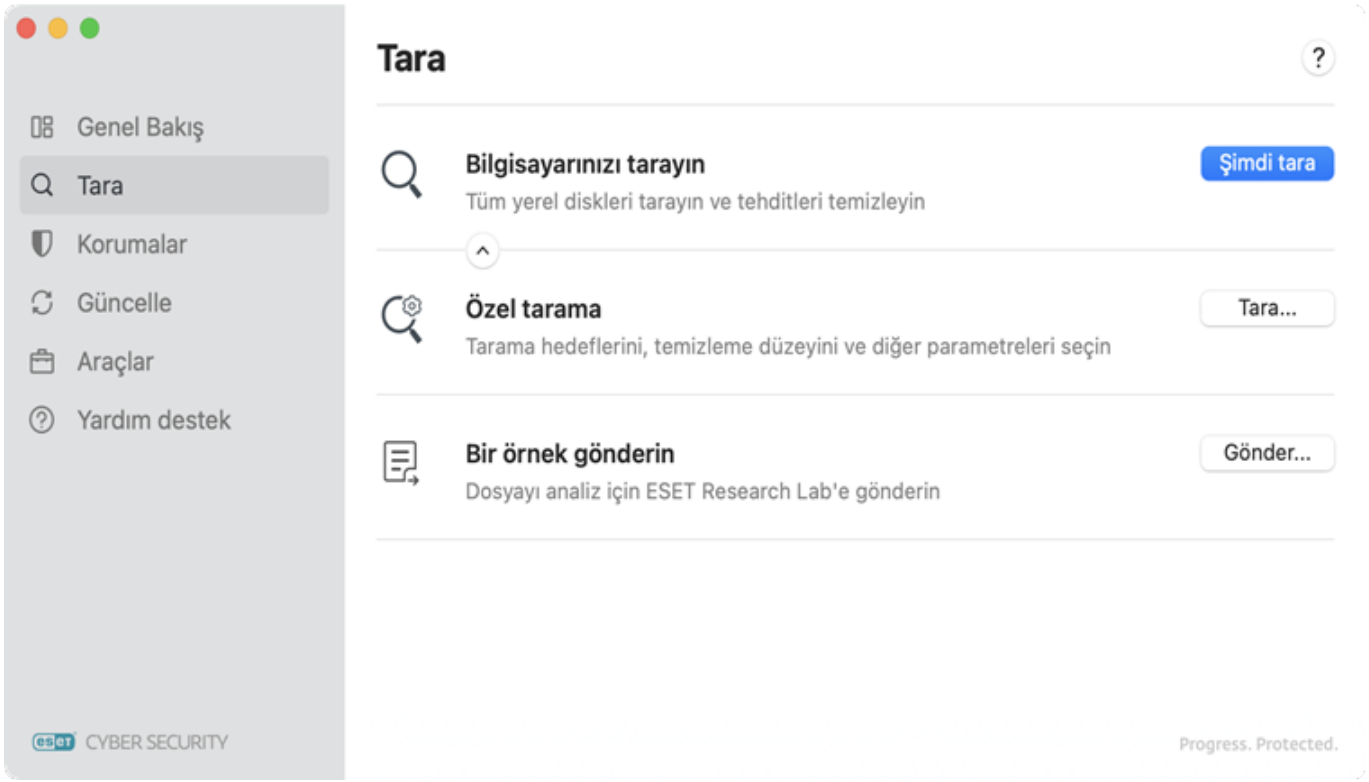
Gerçek zamanlı koruma başlamıyor

Gerçek zamanlı koruma, sistem başlatılırken başlamazsa diğer programlarla çakışmalar olabilir. Gerçek zamanlı koruma başlamazsa ESET Teknik Destek ekibiyle iletişime geçin.

İsteğe bağlı bilgisayar taraması

Bilgisayarınızın enfekte olduğundan şüpheleniyorsanız (bilgisayarınız anormal şekilde davranıyorsa) ana uygulama penceresinden **Tarama**'nı seçin ve bilgisayarınızı sızıntılara karşı incelemek için **Şimdi tara**'yı tıklayın. Maksimum koruma için yalnızca bir enfeksiyondan şüphelendiğinizde değil, rutin güvenlik önlemlerinin parçası olarak bilgisayar taramalarını düzenli aralıklarla çalıştırın. Düzenli tarama, diske kaydedildiğinde gerçek zamanlı tarayıcı tarafından tespit edilmeyen sızıntıları bulabilir. Sızıntı sırasında Gerçek zamanlı tarayıcı devre dışıysa veya algılama modülleri güncel değilse, bu durum gerçekleşebilir.

ESET ayda en az bir defa isteğe bağlı bilgisayar taraması çalıştırmanızı önerir.



Taramayı, uygulama tercihlerinde **Araçlar** > **Zamanlayıcı** bölümünden zamanlanan bir görev olarak yapılandırabilirsiniz.

Özel tarama

Ana uygulama penceresinde **Tarama** bölümüne gidin, ok simgesini tıklayarak **Özel tarama** ve **Bir örnek gönderin** seçeneğini görüntüleyin.

Özel tarama

Tarama hedefleri ve tarama yöntemleri gibi tarama parametreleri belirtmek istiyorsanız bu seçenek idealdir. Özel tarama çalıştırmanın avantajı, parametreleri ayrıntılı biçimde yapılandırabilme özelliğidir.

Özel tarama penceresini açmak için **Özel Tarama** bölümünde **Tara**'yı tıklayın. Taramak istediğiniz dosyaları pencere içindeki ilgili alana sürükleyip bırakın. Ayrıca **Gözat** düğmesini tıklayarak ve dahil etmek istediğiniz klasöre veya dosyalara giderek bir **tarama hedefi** de belirtebilirsiniz.

Üç nokta menü simgesini tıklayarak daha fazla seçenek elde edersiniz: **Tarama profilini** ve **Tarama dışı bırakılacak ayarlar**'ı **seçin**.

Tarama profilini seç

Burada tercih edilen **tarama profilini** seçin ve **temizleme düzeyini** ayarlayın.

Tarama profilleri

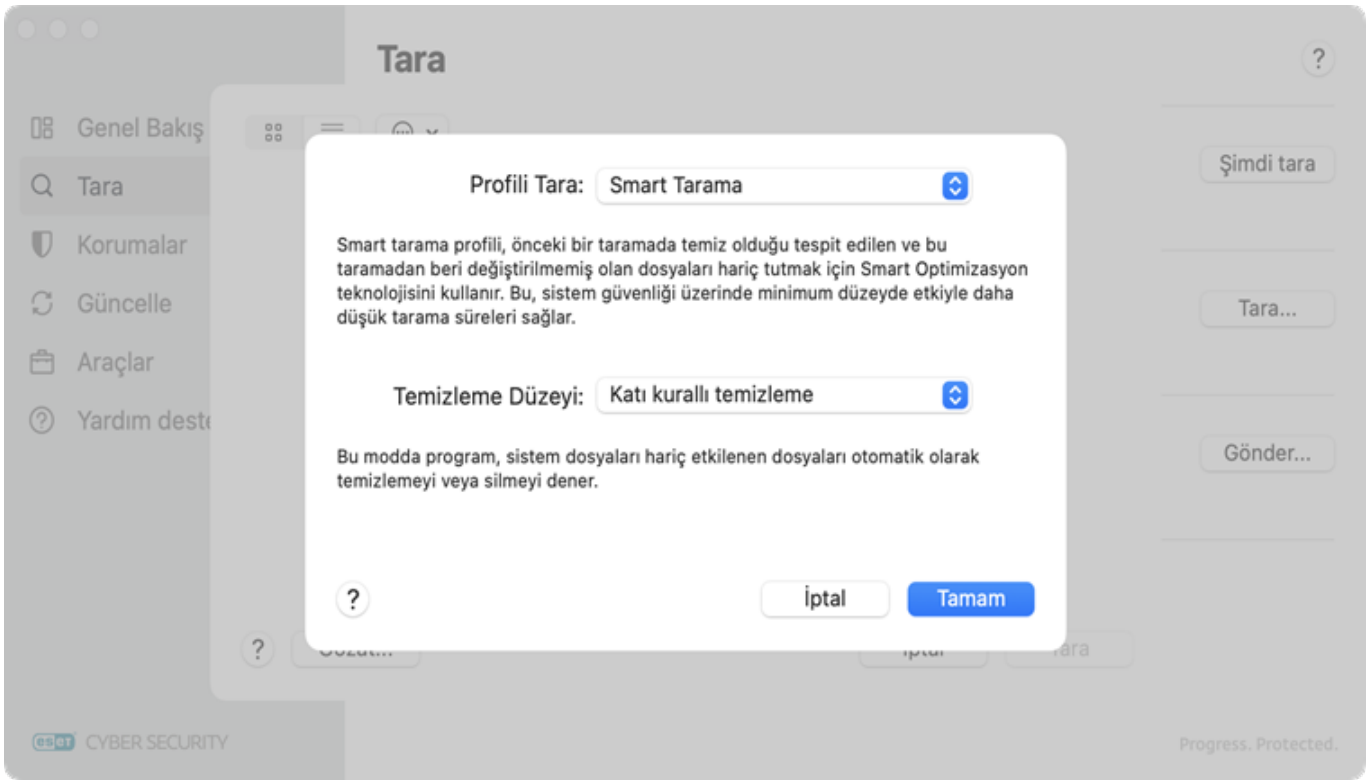
Smart tarama, hızlı bir şekilde bilgisayar taraması başlatmanıza ve etkilenen dosyaları kullanıcı müdahalesine gerek kalmadan temizlemenize olanak verir. Temel avantajı, ayrıntılı tarama yapılandırması gerektirmeden kolay işlem yapılmasını sağlamasıdır. Smart tarama, tüm klasörlerdeki tüm dosyaları denetler ve algılanan sızıntıları

otomatik olarak temizler veya siler. Smart tarama profili, önceki bir taramada temiz olduğu tespit edilen ve bu taramadan beri değiştirilmemiş dosyaları hariç tutan Smart Optimizasyon teknolojisini kullanır.

Kapsamlı tarama profili Akıllı Optimizasyon teknolojisini kullanmadığından hiçbir dosya taramadan hariç tutulmaz.

Temizleme düzeyi

Burada, tarayıcının etkilenen dosyaları nasıl işleyeceğini seçebilirsiniz. Temizleme düzeyleri hakkında daha fazla bilgi edinmek için Temizleme bölümüne bakın.



Tarama dışı öğeleri ayarla

Tarama dışı bırakılacak dosyaları veya klasörleri ekleyin. Tarama dışı bırakmak istediğiniz dosyaları gösterilen penceredeki ilgili alana sürükleyin.

> Önceden antivirus programları kullanmış olan ileri düzey kullanıcılar için **özel tarama** ile bilgisayar taramaları gerçekleştirilmesi önerilir.

Bir örnek gönderin

Bu seçenek, analiz için ESET Araştırma Laboratuvarı'na bir dosya göndermenizi sağlar. Örnek dosya gönderme hakkında daha fazla bilgi için Örnek Gönderme başlıklı makaleye bakın.

ThreatSense altyapısı parametre ayarları

ThreatSense, çeşitli karmaşık tehdit algılama yöntemlerinden oluşan, ESET'e ait bir teknolojidir. Bu teknoloji proaktiftir; başka bir deyişle, yeni bir tehdidin ilk yayılmaya başladığı saatlerde de koruma sağlar. ThreatSense sistem güvenliğini önemli ölçüde yükseltmek üzere birlikte çalışan birkaç yöntemin (kod analizi, kod öykünmesi, genel imzalar vs.) bir bileşimini kullanır. Bu tarama altyapısı birkaç veri akışını aynı anda denetleme, böylece verimliliği ve algılama hızını azamiye çıkarma yeteneğindedir. ThreatSense teknolojisi de kök setlerini başarıyla

önler.

ThreatSense teknolojisi ayar seçenekleri birkaç tarama parametresi belirtmenize olanak tanır:

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

Uygulama Tercihleri'nde ThreatSense yapılandırmalarını değiştirebilirsiniz (cmd+, kombinasyonunu kullanarak veya macOS menü çubuğundaki ESET Cyber Security öğesini tıklayıp **Tercihler**'i [Ayarlar] seçerek açın). 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
- Kötü amaçlı yazılım taramaları
- Web erişimi koruması
- E-posta istemcisi koruması

ThreatSense parametreleri her modül için özel olarak en iyi duruma getirilmiştir ve bu parametrelerin değiştirilmesi sistemin çalışmasını önemli ölçüde etkileyebilir. Örneğin, ayarların her zaman çalışma zamanı paketleyicileri taranacak şekilde değiştirilmesi veya Gerçek zamanlı dosya sistemi koruma modülünde gelişmiş sezgisel taramanın etkinleştirilmesi, sistemin yavaşlamasına neden olabilir. Bilgisayar taraması dışındaki tüm modüller için varsayılan ThreatSense parametrelerini değiştirmeden bırakmanızı öneririz.

Tarama seçenekleri

Tarama seçenekleri, bu koruma modülleri için Uygulama Tercihleri'nde yapılandırılabilir: Gerçek zamanlı dosya sistemi koruması, zararlı yazılım taramaları, web erişimi koruması ve e-posta istemci koruması. Koruma modüllerinin her biri için, sistem taraması sırasında kullanılan yöntemleri seçebilirsiniz. Aşağıdaki seçenekler kullanılabilir:

- **Sezgisel tarama** - Sezgisel tarama, programların etkinliğini (kötü amaçlı) analiz eden bir algoritma kullanır. Sezgisel algılamanın başlıca avantajı, daha önceden mevcut olmayan yeni kötü amaçlı yazılımları algılama becerisidir.

- **Gelişmiş sezgisel tarama** – Gelişmiş sezgisel tarama, yüksek düzey programlama dillerinde yazılmış bilgisayar solucanlarının ve truva atlarının algılanması için ESET tarafından geliştirilmiş, en iyi duruma getirilmiş benzersiz bir sezgisel tarama algoritmasından oluşur. Gelişmiş sezgisel tarama sonucunda programın algılama yeteneği çok daha yüksektir.

- **Akıllı Optimizasyon** - Etkinleştirildiğinde Akıllı Optimizasyon, en yüksek tarama hızlarını korurken en etkili tarama düzeyini sağlar. Çeşitli koruma modülleri, belirli dosya türlerine farklı tarama yöntemleri uygulayarak akıllıca tarama yapar.

Temizleme düzeyi

Temizleme düzeyleri, bu koruma modülleri için Uygulama Tercihleri'nde yapılandırılabilir: Gerçek zamanlı dosya sistemi koruması, zararlı yazılım taramaları, web erişimi koruması ve e-posta istemci koruması. Tek tek düzeyler, tarayıcının etkilenen dosyaları nasıl temizleyeceğini belirler. Aşağıdaki temizleme düzeyleri kullanılabilir:

- **Temizleme yok** - Etkilenen dosyalar otomatik olarak temizlenmez. Program bir uyarı penceresi görüntüler ve bir eylem seçmenize olanak sağlar.
- **Varsayılan düzey** - Program virüsten etkilenen dosyayı otomatik olarak temizlemeye veya silmeye çalışır. Doğru eylem otomatik olarak seçilemiyorsa, program izleme eylemlerinden oluşan bir seçim listesi sunar. Takip işlemleri, önceden tanımlanmış bir işlem tamamlanamadığında da görüntülenir.
- **Katı kurallı temizleme** - Program etkilenen tüm dosyaları (arşivler dahil) temizler veya siler. Yalnızca sistem dosyaları bu işlemin dışında tutulur. Bir dosyanın temizlenmesi mümkün değilse bununla ilgili bildirim alırsınız; burada gerçekleştirilecek eylemin türünü belirlemeniz istenir.
- **Ayrıntılı temizleme** – Bu modda program, etkilenen tüm dosyaları otomatik olarak temizlemeyi veya silmeyi dener.
- **Sil** - Etkilenen tüm dosyaları silin.

Arşiv taraması
Normal temizleme modunda, yalnızca arşivdeki tüm dosyalar etkilenmişse bütün arşiv dosyaları silinir. Bir arşivde etkilenmiş dosyaların yanı sıra temiz dosyalar da yer alıyorsa arşiv silinmez. Katı kurallı temizleme modunda etkilenen bir arşiv dosyası algılanırsa içinde temiz dosyalar olsa bile arşiv tümüyle silinir.

Tarama Dışı Bırakılanlar

Uzantı, dosya adının nokta ile ayrılmış olan parçasıdır. Uzantı, dosya türünü ve içeriğini tanımlar. Bu koruma modülleri için Uygulama Tercihleri'nde tarama dışında bırakılacak dosya türlerini tanımlayabilirsiniz:

- Gerçek zamanlı dosya sistemi koruması
- Kötü amaçlı yazılım taramaları
- Web erişimi koruması
- E-posta istemcisi koruması

Varsayılan olarak, uzantıları ne olursa olsun tüm dosyalar taranır. Tarama dışında bırakılan dosyalar listesine herhangi bir uzantı ekleyebilirsiniz. Artı + ve eksi − düğmelerini kullanarak belirli uzantıların taramasını etkinleştirebilir veya taramayı yasaklayabilirsiniz.

Bazen belirli dosya türlerinin taranması, programın düzgün şekilde çalışmasını önlüyorsa dosyaların tarama dışında bırakılması gerekir. Örneğin, log, cfg ve tmp dosyalarının hariç tutulması tavsiye edilebilir. Dosya uzantılarının girilmesine ilişkin doğru biçim şu şekildedir:

- log

- cfg
- tmp

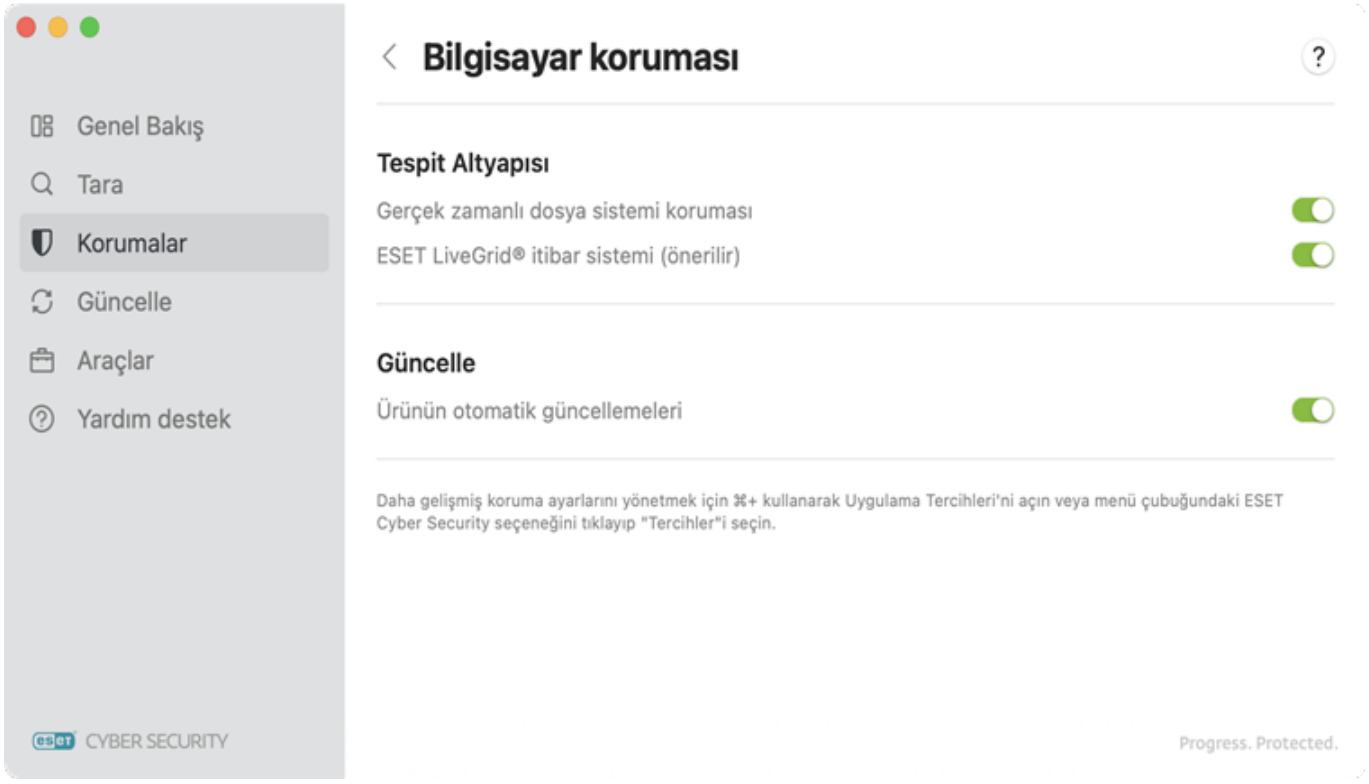
Güncelleme

Maksimum güvenlik düzeyini korumak için ESET Cyber Security ürününün düzenli olarak güncellenmesi gerekir. Güncelleme modülü, en son algılama modüllerini yükleyerek programın her zaman güncel olmasını sağlar.

Ana menüden **Güncelle**'yi tıklatarak, son başarılı güncellemenin tarih ve saati ile güncelleme gerekip gerekmediği de dahil olmak üzere ESET Cyber Security ürününün geçerli güncelleme durumunu görüntüleyin. Yeni güncellemeler için denetimi başlatmak üzere **Güncellemeleri denetle** düğmesini tıklayın. Bir ürün güncellemesinin mevcut olması durumunda, güncelleme boyutu ve çıkış tarihi ile birlikte geçerli ve kullanılabilir sürüm hakkındaki bilgiler gösterilir. **Şimdi güncelle** veya **Yeniden başlatıldığında güncelle** seçeneklerinden birini tercih edebilirsiniz. Tek tek ürün sürümleri hakkında daha fazla ayrıntı görmek için **Değişiklik günlüğüne bakın** bağlantısını tıklayın.

ESET Cyber Security Ürününü yeni bir sürüme yükseltme

Maksimum koruma için, en son ESET Cyber Security sürümünün kullanılması önemlidir. Her zaman en son sürümü sahip kullandığınızdan emin olmak için **Ürünün otomatik güncellemelerinin** açılması önerilir (ana uygulama menüsünde **Korumalar** > **Bilgisayar**).



Araçlar

Araçlar menüsü, program yönetimini basitleştirmeye yardımcı olan ve ileri düzey kullanıcılar için ek seçenekler sunan modüller içerir. Bu menüde şu araçlar bulunur:

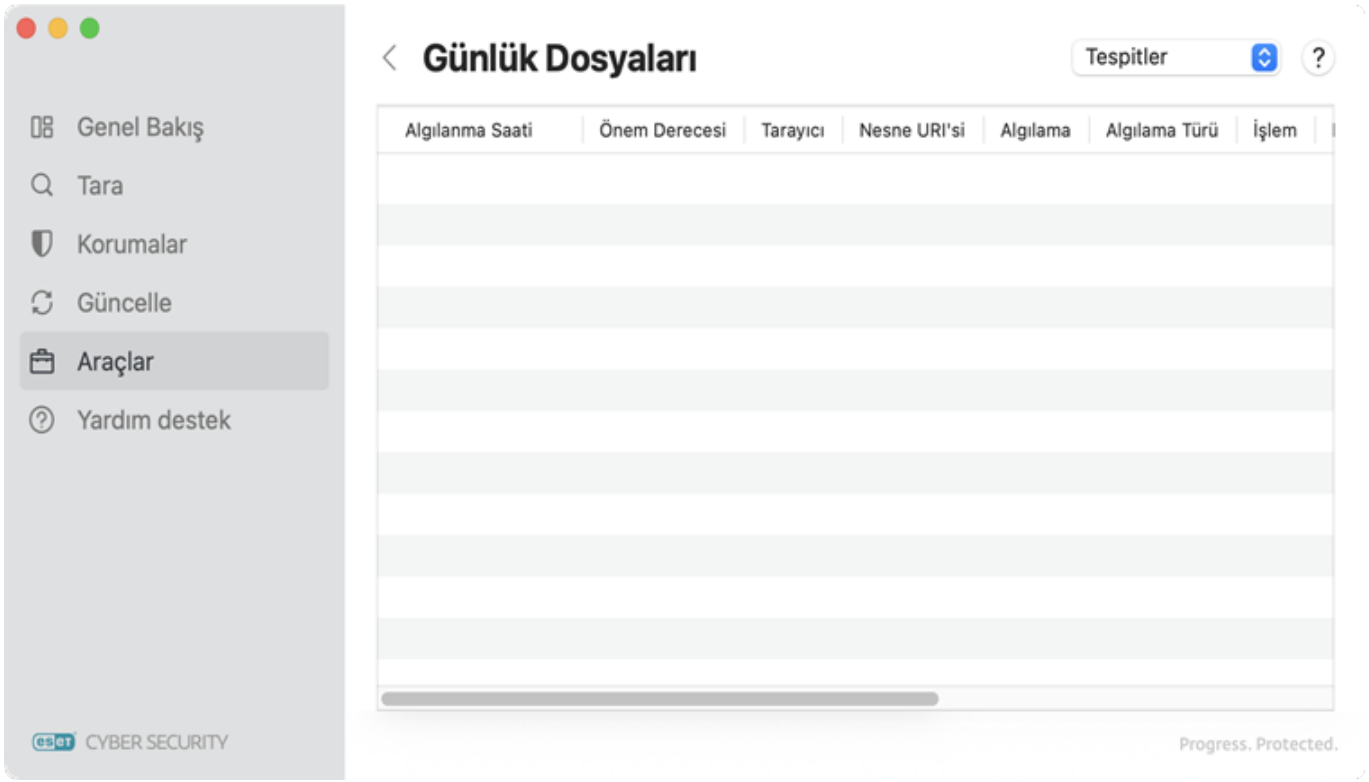
- Günlük dosyaları
- Karantina

Günlük dosyaları

Günlük dosyaları, gerçekleşen önemli program olayları hakkında bilgi içerir ve algılanan tehditlere genel bir bakış sağlar. Günlüğe kaydetme; sistem analizi, tehdit tespiti ve sorun giderme için gereklidir. Günlüğe kaydetme işlemi herhangi bir kullanıcı müdahalesi olmadan arka planda etkin biçimde gerçekleşir. Bilgiler, geçerli günlük ayrıntı ayarlarına göre kaydedilir. Doğrudan ESET Cyber Security ortamından metin mesajları ile günlükleri görüntüleyebilir ve günlükleri arşivleyebilirsiniz.

Günlük dosyalarına, ESET Cyber Security ana menüsünden **Araçlar** > **Günlük dosyaları** seçeneği tıklatılarak erişilebilir. Pencerenin sağ üst kısmındaki açılır menüyü kullanarak istenen günlük türünü seçin. Şu günlükler görüntülenebilir:

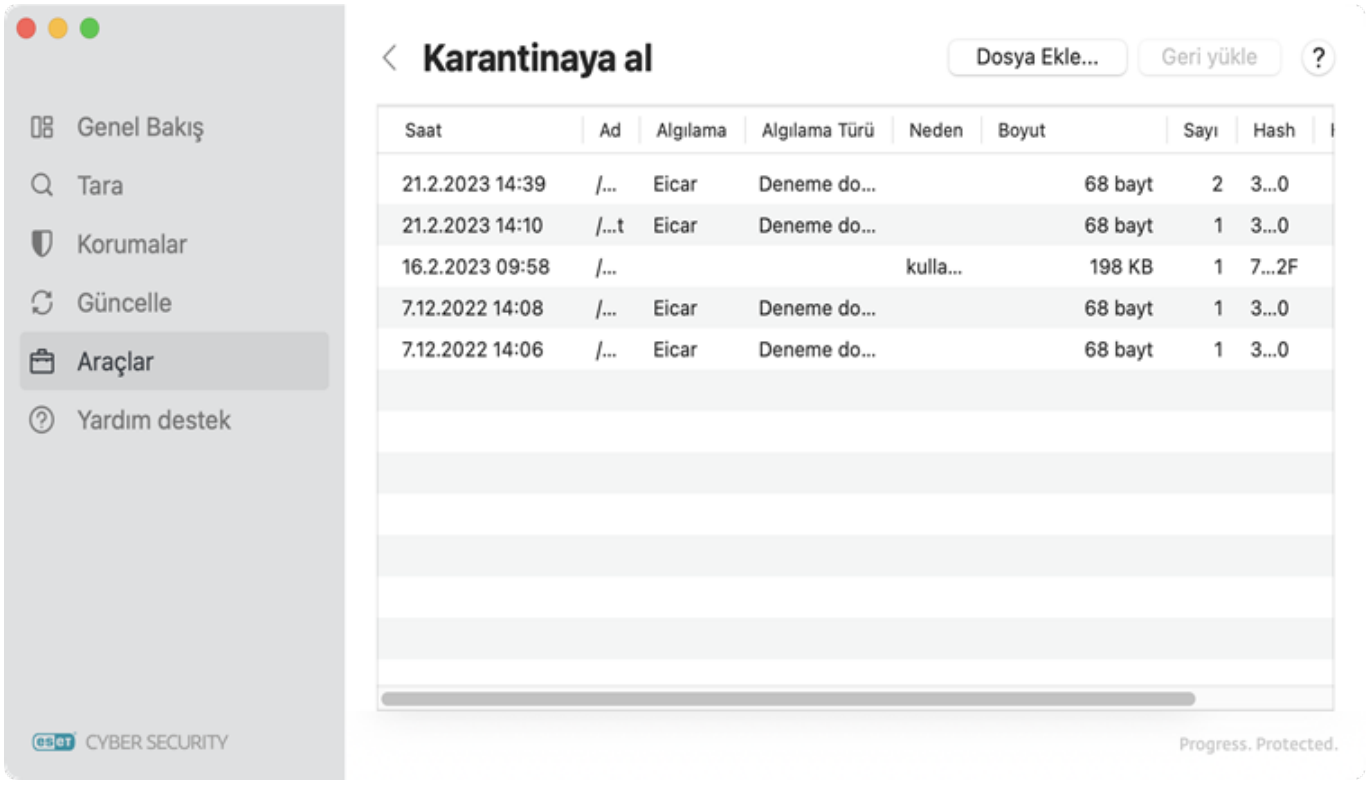
- **Tespitleri** - Sızıntıların tespitiyle ilgili olaylar hakkındaki tüm bilgileri gösterir.
- **Bilgisayar taraması** - Tüm tamamlanan taramaların sonuçları bu günlükte görüntülenir. İlgili İsteğe bağlı bilgisayar taramasının ayrıntılarını görüntülemek için girişi çift tıklatın.
- **Olaylar** - Sistem yöneticilerinin ve kullanıcıların sorunları çözmesine yardımcı olur. ESET Cyber Security Tarafından gerçekleştirilen tüm önemli işlemler, olay günlüklerine kaydedilir.
- **Filtrelenmiş web siteleri** - Web erişimi koruması tarafından engellenen web sitelerinin listesini gösterir. Bu günlüklerde; zamanı, URL'yi, durumu, IP adresini, belirli web sitesine bağlantı sağlayan kullanıcı ve uygulamayı görebilirsiniz.
- **Gönderilen dosyalar** - Analiz için gönderilen örneklerin kayıtlarını içerir.



Karantina

Karantinanın ana görevi etkilenen dosyaları güvenli bir şekilde saklamaktır. Dosyalar temizlenemiyorsa, silinmeleri güvenli değilse ya da önerilmiyorsa veya ESET Cyber Security tarafından hatalı bir şekilde algılanıyorsa, bunların karantinaya alınmaları gerekir.

Karantina klasörüne depolanmış dosyaları; karantinanın tarih ve saatini, etkilenen dosyanın orijinal konumunun yolunu, bayt olarak boyutunu, nedenini (örneğin, kullanıcı tarafından eklenen nesne) ve tehdit sayısını (örneğin, birden çok sızıntıyı içeren bir arşiv olup olmadığını) görüntüleyen bir tabloda görebilirsiniz. ESET Cyber Security kaldırıldıktan sonra bile karantinaya alınan dosyaları içeren karantina klasörü (*/Kitaplık/Uygulama Desteği/Eset/güvenlik/önbellek/ karantina*) sistemde kalır. Karantinaya alınan dosyalar, güvenli olarak şifrelenmiş şekilde depolanır ve ESET Cyber Security yüklendikten sonra geri yüklenebilir.



Dosyaları karantinaya alma

ESET Cyber Security silinen dosyaları otomatik olarak karantinaya alır (bu seçeneği uyarı penceresinde iptal etmediyseniz). Şüpheli dosyaları karantinaya almak için **Dosya ekle**'yi tıklayın. Ayrıca bir dosya veya klasörü tıklayarak, fare düğmesini basılı tutarken fare imlecini işaretli alana taşıyıp düğmeyi serbest bırakarak ilgili dosya veya klasörü sürükleyip bırakabilirsiniz.

Karantinadan geri yükleme

Karantinaya alınan bir dosya seçin ve orijinal konuma **geri yüklemek** için Geri Yükle'yi tıklayın. Bu özellik, **Karantina** penceresinde belirli bir dosyayı Control tuşuna basarak tıkladığınızda (veya sağ tıkladığınızda) ve **Geri Yükle**'yi tıkladığınızda da kullanılabilir. Bağlam menüsü aynı zamanda dosyayı silinmiş olduğu konumdan farklı bir konuma geri yüklemenize olanak tanıyan **Geri yükleme konumu...** seçeneğini de sunar.

Karantinadan dosya gönderme

Program tarafından algılanmayan şüpheli bir dosyayı karantinaya aldıysanız veya bir dosya yanlışlıkla etkilenmiş olarak değerlendirilmiş (örn., kodun sezgisel tarama analizi tarafından) ve sonra da karantinaya alınmışsa, lütfen dosyayı ESET Tehdit Laboratuvarı'na gönderin. Dosyayı karantinadan göndermek için, dosyayı Control tuşuna basarak tıklayın (veya sağ tıklayın) ve içerik menüsünden **Örneği gönder**'i seçin. Örnek dosya gönderme hakkında daha fazla bilgi için Örnek Gönderme başlıklı makaleye bakın.

Örneği analiz için gönderin

Ana uygulama penceresinde sol menüden **Tarama** bölümüne gidin,  ok simgesini tıklayarak **Bir örnek gönderin** seçeneğini görüntüleyin.

Bu seçenek, bilgisayarınızda bulunan şüpheli davranan bir dosyayı veya çevrim içi bulunan şüpheli bir siteyi seçmenize ve analiz için ESET Araştırma Laboratuvarı'na göndermenize olanak tanır.

Örnekleri ESET'e göndermeden önce
Gönderdiğiniz örnek aşağıdaki ölçütlerden en az birini karşılamalıdır:
- Örnek ESET ürününüz tarafından algılanmıyor
- Örnek hatalı bir şekilde tehdit olarak algılandı
- Örnek kişisel bir dosya değildir. ESET kişisel dosyalarınızı (zararlı yazılımlara karşı ESET tarafından taranmasını istediğiniz dosyalarınızı) örnek olarak kabul etmez ve ESET Araştırma Laboratuvarı, kullanıcılar için isteğe bağlı taramalar gerçekleştirmez

Analiz için göndermek istediğiniz dosyayı belirtmek üzere **Gönder**'i tıklayın. **Analiz için örnek gönderme** formunda aşağıdakileri belirtin:

- **Gönderim nedeni** - İçerik menüsünden seçin.
- **Örnek** - Göndermek istediğiniz dosyanın yolunu belirtin veya dosyayı işaretli alana sürükleyip bırakın.
- **İletişim** - Dosya hakkında daha fazla bilgiye ihtiyaç duymamız durumunda sizinle iletişim kurabilmemiz için sağlanmış olan iletişim bilgileridir. Anonim olarak gönder açma/kapama düğmesini etkinleştirerek e-postanızı dahil etme adımını atlayabilirsiniz

Sonraki'ni tıkladığınızda örnek dosya hakkında zararlı yazılım bulaşmasının gözlemlenen işaretleri veya belirtileri ve dosya kaynağı gibi ek bilgiler sağladığınız son adıma yönlendirilirsiniz. Ek bilgi sağlamak, laboratuvarlarımızın örnekleri tanımlamasına ve işlemesine önemli ölçüde yardımcı olacaktır.

ESET'ten yanıt almayabilirsiniz
Daha fazla bilgi gerekmedikçe ESET'ten yanıt almazsınız. Sunucularımıza her gün on binlerce dosya geldiğinden tüm bu gönderimleri yanıtlamamız olanaksızdır.
Örneğin kötü amaçlı bir uygulama veya web sitesi olduğu belirlenirse, bu örneğin algılanması yaklaşan bir ESET güncellemesine eklenir.

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 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.

EULAID: EULA-PRODUCT-LG; 3537.0

Gizlilik Politikası

Kişisel verilerin korunması bir Veri Denetleyicisi ("ESET" veya "Biz") olan ve Einsteinova 24, 851 01 Bratislava, Slovak Republic adresinde mukim ve Bratislava I. Bölge Mahkemesinin Ticari Sicil Kaydında Bölüm Sro, Giriş No 3586/B, İşyeri Sicil Numarası: 31333532 olan ESET, spol. s r. o. için özellikle önemlidir. AB Genel Veri Koruma Yönetmeliği ("GDPR") altında yasal olarak standartlaştırılan şeffaflık gereksinimine uymayı istiyoruz. Bu amaçla, bu Gizlilik Politikasını yalnızca veri öznesi olarak müşterimizi ("Son Kullanıcı" veya "Siz") şu kişisel veri koruma konuları hakkında bilgilendirmek için yayınlamaktayız:

- Kişisel Verilerin İşlenmesi İçin Yasal Dayanak,
- Veri Paylaşımı ve Gizlilik,
- Veri Güvenliği,
- Veri Öznesi Olarak Haklarınız,
- Kişisel Verilerinizin İşlenmesi
- İletişim bilgileri.

Kişisel 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:

- Güncelleme ve yükleme işlemi ve ürünümüzün yüklendiği platform dahil olmak üzere bilgisayarınız ile ilgili bilgileri kapsayan istatistikler ve işletim sistemi, donanım bilgileri, yükleme kimlikleri, lisans kimlikleri, IP adresi, MAC adresi, ürünün yapılandırma ayarları gibi işlemler ve işlevler ile ilgili bilgiler.
- ESET LiveGrid® itibar sistemi kapsamında sızıntılarla ilişkili tek yönlü karmalar, taranan dosyaları buluttaki beyaz ve kara listelerde yer alan öğelerden oluşan veri tabanıyla karşılaştırarak anti-malware çözümlerimizin etkisini artırır.
- 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;
    - tür, satıcı, model ve/veya cihaz adı gibi, yerel ağda bulunan cihazlar hakkındaki bilgiler;
    - 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.

- Lisans kimliği gibi lisans bilgileri ve ad, soyadı, adres, e-posta adresi gibi kişisel veriler faturalandırma amaçları, lisans orijinalliğini doğrulama ve hizmetlerimizin sunulması için gereklidir.
- İletişim bilgileri ve destek isteklerinizde yer alan veriler, destek hizmetleri için gereklidir. 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.

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 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.

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