ÇÖZÜME GENEL BAKIŞ

ENDPOINT SOLUTIONS

Masaüstü bilgisayarlar, dizüstü bilgisayarlar ve akıllı telefonlar için güçlü, çok katmanlı koruma

Progress. Protected.

Uç Nokta Kóruma Platformu nedir?

Uç nokta koruma platformu (EPP), uç nokta cihazlarda dağıtılan çok platformlu ve çok katmanlı bir çözümdür. Dosya tabanlı kötü amaçlı yazılım saldırılarını önlemeye, kötü amaçlı etkinliği algılamaya yardımcı olur. Ayrıca, dinamik güvenlik olaylarına ve uyarılarına tepki vermek üzere araştırma ve ortadan kaldırma özellikleri de sunar.

ESET'in uç nokta koruma çözümleri, sürekli olarak performans, algılama ve yanlış teşhisler arasında denge kurma özelliği ile birlikte çalışan birçok teknolojiden yararlanan çok katmanlı bir yaklaşıma sahiptir.

Neden **Uç Nokta Koruma Çözümleri?**

FİDYE YAZILIMI

Fidye yazılımı, 2013'teki Cryptolocker'dan beri dünya genelindeki birçok sektör için sürekli bir endişedir. Fidye yazılımı çok daha uzun süredir var olmasına rağmen, hiçbir zaman şirketlerin endişe duyduğu büyük bir tehdit olmadı. Ancak, artık tek bir fidye yazılımı olayı, önemli veya gerekli dosyaları şifreleyerek bir şirketi kolayca çalışamaz hale getirebilir.

Bir şirket bir fidye yazılımı saldırısıyla karşılaştığında, sahip olduğu yedeklerin yeterince yeni olmadığını hemen anlar ve bu nedenle şirket fidyeyi ödemesi gerektiğini düşünür.

ESET'in uç nokta koruma çözümleri, fidye yazılımı önlemenin yanı sıra fidye yazılımın bir kuruluşta görülmesini engellemek üzere fidye yazılımı engellemek üzere birçok savunma katmanı sunar. Fidye yazılımı önlemek ve algılamak,fidye ödendiğinde suçlular bu saldırı modunu kullanmaya devam edebileceğinden önemlidir.

HEDEFE YÖNELİK SALDIRILAR VE VERİ İHLALLERİ

Günümüz siber güvenlik ortamı yeni saldırı yöntemleri ve daha önce görülmemiş tehditler ortaya çıktıkça sürekli olarak değişmektedir. Bir saldırı veya veri ihlali meydana geldiğinde, kuruluşlar savunmalarına nasıl sızıldığı veya saldırıdan tamamen habersiz olmaları konusunda şaşkınlık yaşar. Saldırı nihayetinde keşfedildikten sonra kuruluşlar, bu benzer bir saldırının tekrar gerçekleşmesini engellemek üzere çeşitli önlemlere başvurur. Ancak bu, onları başka bir yepyeni vektör kullanabilecek bir sonraki saldırıdan korumaz.

ESET'in uç nokta koruma çözümleri, en yeni tehditleri dünyanın herhangi bir yerine kullanılmaya başlanmadan önce önceliklendirmek ve etkili bir şekilde engellemek üzere dünya genelinde bulundukları yerle ilgili tehdit istihbaratıyla ilgili bilgileri kullanır. Ayrıca, çözümlerimiz, normal bir güncellemeyi beklemek zorunda kalmadan, kaçırılan bir algılama durumunda hızlı yanıt vermek için bulut tabanlı güncelleme özelliğine sahiptir.

DOSYASIZ SALDIRILAR

Dosyasız kötü amaçlı yazılım olarak adlandırılan daha yeni tehditler, yalnızca bilgisayar belleğinde bulunur ve bu nedenle dosya tarama tabanlı korumaların bunları algılamasını imkansızdır.

Ayrıca, bazı dosyasız saldırılar, kötü amaçlı bir yükün algılanmasını daha da zorlaştırmak için işletim sistemine dahil olan uygulamalardan yararlanır. Örneğin bu saldırılarda PowerShell kullanımı oldukça yaygındır.

ESET uç nokta koruma platformlarında, dosyasız saldırılara karşı koruma sağlamak için yanlış biçimlendirilmiş veya ele geçirilmiş uygulamaları algılamak için azaltıcı önlemler bulunur. ESET şüpheli herhangi bir şey için belleği sürekli olarak kontrol etmek üzere özel tarayıcılara da sahiptir. Bu çok katmanlı yaklaşımı kullanarak, en yeni kötü amaçlı yazılımlardan her zaman bir adım önde olduğumuzdan emin oluyoruz.

ESET'in uç nokta koruma çözümleri, fidye yazılımı önlemenin yanı sıra fidye yazılımın bir kuruluşta görülmesini engellemek üzere fidye yazılımı engellemek üzere birçok savunma katmanı sunar.

Bir saldırı veya veri ihlali meydana geldiğinde, kuruluşlar savunmalarına nasıl sızıldığı veya saldırıdan tamamen habersiz olmaları konusunda şaşkınlık yaşar.

Dosyasız kötü amaçlı yazılım olarak adlandırılan daha yeni tehditler, yalnızca bilgisayar belleğinde bulunur ve bu nedenle dosya tarama tabanlı korumaların bunları algılamasını imkansızdır.

"ESET yıllardır sağlam güvenlik çözümümüz. Yapması gerekeni yapıyor, endişelenmenize gerek yok. Kısaca ESET güvenlik, nitelik ve hizmet sunuyor."

— Jos Savelkoul, Bilişim ve İletişim Teknolojileri Departmanı, Ekip Lideri, Zuyderland Hastanesi, Hollanda, 10.000'den fazla üyelik

ESET uç nokta koruma çözümleri

ESET Endpoint Security for Windows/macOS/Android
ESET Endpoint Antivirus for Windows/macOS/Linux
ESET Server Security for Windows Server/Linux/Azure
ESET MDM for iOS and iPadOS

İşletim sistemine bağlı olarak ürün özellikleri ve işlevleri değişiklik gösterebilir.

ESET farkı

ÇOK KATMANLI KORUMA

ESET, müşterilerimize mümkün olan en iyi düzeyde koruma sağlamak için çok katmanlı teknolojiyi, makine öğrenimini ve insan uzmanlığını birleştirir. Teknolojimiz sürekli olarak performans, algılama ve yanlış teşhisler arasında denge kurmak üzere ayarlanıyor ve değişiyor.

EŞİ OLMAYAN PERFORMANS

Uç nokta koruma çözümlerinin performansa etkisi, birçok kuruluş için önemli bir endişe kaynağıdır. ESET ürünleri performans alanında üstünlüğünü kanıtlamaya ve uç noktalarımızın sistemleri ne kadar az etkilediğini gösteren üçüncü taraf testlerini kazanmaya devam ediyor.

PLATFORMLAR ARASI DESTEK

ESET uç nokta koruma ürünleri Windows (Windows on ARM dahil), macOS, Linux ve Android tüm işletim sistemlerini destekler. Tüm uç nokta ürünlerimiz, tek bir panodan tamamen yönetilebilir. Ayrıca iOS ve Android için mobil cihazdan yönetim de mümkündür.

DÜNYA GENELİNDE HİZMET

Dünya çapında 22 ülkede ofisi, 13 ülkede ise Ar-Ge laboratuvarı olan ESET, 200'den fazla ülke ve bölgede faaliyet gösterir. Bu sayede kötü amaçlı yazılımları dünya genelinde görülmeden önce durdurmak için veri elde ediyor ve en son tehditlere veya olası yeni vektörlere dayanan yeni teknolojilere öncelik veriyoruz.

"En iyi kanıt mı? Yardım masamızdaki istatistikler: ESET'i kullanmaya başladıktan sonra, destek ekiplerimiz herhangi bir aramayı günlüğe kaydetmiyor - herhangi bir virüsten koruma veya kötü amaçlı yazılımla ilgili sorunlarla uğraşmak zorunda kalmıyor!

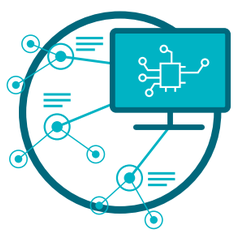
— Adam Hoffman, BT Altyapı Yöneticisi; Mercury Engineering, İrlanda
1.300 üyelik

Teknoloji

Ürünlerimiz ve teknolojilerimiz üç temele dayanır

ESET LIVEGRID®

Fidye yazılımı gibi bir sıfır gün tehdidi görüldüğünde, dosya bulut tabanlı kötü amaçlı yazılım koruma – LiveGrid®'e gönderilir ve burada tehdit etkisiz hale getirilir ve davranış izlenir. Bu sistemden elde edilen sonuçlar, birkaç dakika içerisinde, herhangi bir güncellemeye gerek olmadan dünya genelindeki tüm uç noktalara iletilir.



MAKİNE ÖĞRENİMİ

Gelen örnekleri temiz, potansiyel olarak istenmeyen veya kötü amaçlı olarak doğru şekilde etiketlemek üzere sinir ağlarının ve özenle seçilmiş algoritmaların birleşik gücünü kullanır.

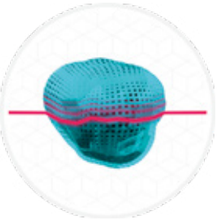
İNSAN UZMANLIĞI

ESET'in birinci sınıf güvenlik araştırmacıları, günün her saati en iyi tehdit istihbaratını sağlamak için zengin bilgilerini ve istihbaratlarını paylaşır.

Sürekli değişen tehdit ortamı için tek bir savunma kalkanı yeterli değildir. Tüm ESET Uç Nokta Güvenlik ürünleri, yürütülmeden önce, sonra ve yürütüldüğü sırada kötü amaçlı yazılımı algıma özelliğine sahiptir. Kötü amaçlı yazılımın yaşam döngüsünün yalnızca bir kısmına değil, tümüne odaklanarak mümkün olan en yüksek seviyede korumayı sunuyoruz.

MAKİNE ÖĞRENİMİ

Tüm ESET uç nokta güvenlik ürünlerinde 1997'den beri kullandığımız savunma katmanlarına ek olarak makine öğrenimine de yeri veriyoruz. Özellikle makine öğrenimi, birleştirilmiş çıktı ve sinir ağları biçiminde kullanılır. Ağın derinlemesine incelenmesi için yöneticiler, internet bağlantısı olmasa bile çalışan özel bir agresif makine öğrenimi modunu açabilir.



GELİŞMİŞ BELLEK TARAYICI

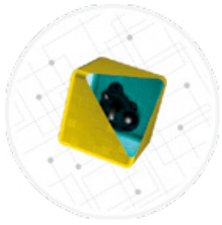
ESET Gelişmiş Bellek Tarayıcı, kötü amaçlı yazılım sürecinin davranışını izler ve bu kötü amaçlı yazılım bellekte gizlendikten sonra onu tarar. Dosyasız kötü amaçlı yazılım, dosya sisteminde geleneksel olarak algılanabilen kalıcı bileşenlere ihtiyaç duymadan çalışır. Yalnızca bellek taraması, bu tür kötü amaçlı saldırıları keşfetmede ve durdurmada başarılı olabilir.

FİDYE YAZILIMI KALKANI

ESET Fidye Yazılımı Kalkanı, kullanıcıları fidye yazılımdan koruyan ek bir katmandır. Bu teknoloji, davranışına ve itibarına bağlı olarak yürütülen tüm uygulamaları izler ve değerlendirir. Davranışına benzeyen süreçleri tespit etmek ve engellemek üzere tasarlanmıştır.

SUİSTİMAL ENGELLEYİCİ

ESET Suistimal Engelleyici, tipik olarak suistimal edilebilir uygulamaları (tarayıcılar, belge okuyucular, e-posta istemcileri, Flash, Java ve daha fazlası) izler ve yalnızca belirli CVE tanımlayıcılarını hedeflemek yerine, suistimal tekniklerine odaklanır. Tetiklendiğinde, tehdit makinede hemen engellenir.



ÜRÜN İÇİ SANDBOX

Günümüzün kötü amaçlı yazılımları genellikle oldukça karmaşıktır ve algılanmaktan mümkün olduğunca kaçınmaya çalışır. Bu kötü amaçlı yazılımları anlamak ve gizlenen gerçek davranışı belirlemek için ürün içi sandbox kullanıyoruz. Bu teknolojinin yardımıyla ESET çözümleri, izole edilmiş bir sanallaştırılmış ortamda şüpheli bir örneği çalıştırmak için bilgisayar donanımının ve yazılımının farklı bileşenlerini taklit eder.

BOTNET KORUMASI

ESET Botnet Koruması, botnet'ler tarafından kullanılan kötü amaçlı iletişimi algılar ve aynı zamanda kuralları ihlal eden süreçleri tanımlar. Algılana tüm kötü amaçlı iletişimler engellenir ve kullanıcıya bildirilir.

AĞ SALDIRISI KORUMASI

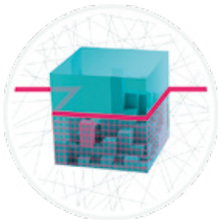
Bu teknoloji, ağ düzeyinde bilinen güvenlik açıklarının daha iyi algılanmasını sağlar. Kötü amaçlı yazılımın yayılmasına, ağ tarafından yürütülen saldırılara ve henüz bir yamanın yayınlanmadığı veya dağıtılmadığı güvenlik açıklarından yararlanılmasına karşı başka bir önemli koruma katmanı oluşturur.

GÜVENLİ TARAYICI

Intranet çevresi içindeki ve buluttaki kritik verilere erişmek için kullanılan ana araç olarak tarayıcıya odaklanan özel bir koruma katmanıyla kuruluşun varlıklarını korumak için tasarlanmıştır. Güvenli Tarayıcı, klavye korumasıyla birlikte tarayıcı işlemi için gelişmiş bellek koruması sağlar ve yöneticilerin, güvenli tarayıcı tarafından korunacak URL'ler eklemesine olanak tanır.

HIPS

ESET'in Ana Bilgisayar Tabanlı Saldırı Önleme Sistemi (HIPS), sistem etkinliğini izler ve şüpheli sistem davranışını fark etmek üzere önceden tanımlı kurallar kümesini kullanır. Ayrıca HIPS kendini savunma mekanizması, kuralları ihlal eden süreçlerin zararlı etkinliği yürütmesini engeller.



UEFI TARAYICI

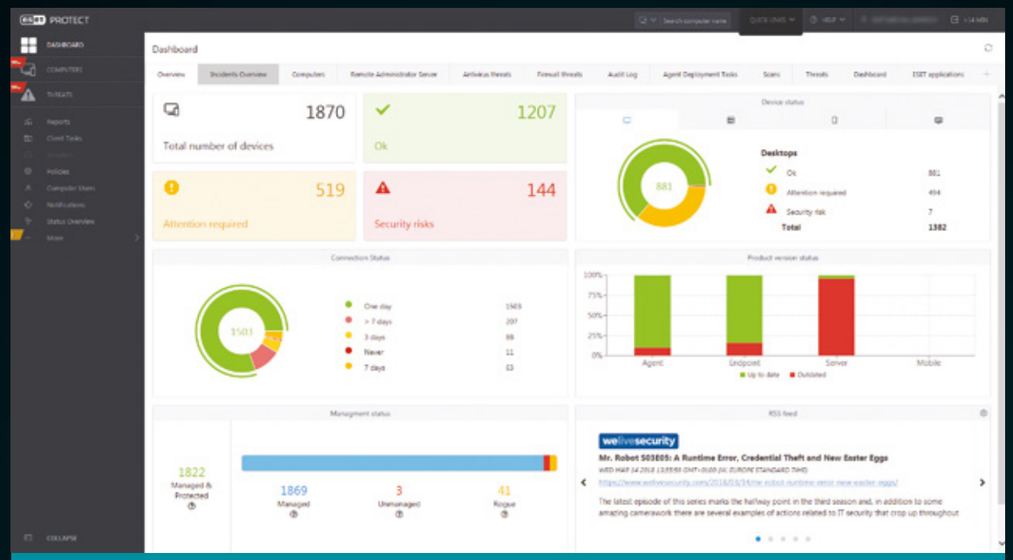
ESET, çözümüne Birleşik Genişletilebilir Ürün Yazılımı Arayüzü'nü (UEFI) koruyan özel bir katman ekleyen ilk uç nokta güvenlik sağlayıcısıdır. ESET UEFI Tarayıcı, önyükleme öncesi ortamın güvenliğini kontrol eder ve sağlar. Ayrıca, donanımın bütünlüğünü izlemek için tasarlanmıştır. Değişiklik tespit edilirse, kullanıcıyı bilgilendirir.

KABA KUVVET SALDIRISINA KARŞI KORUMA

Cihazları, kimlik bilgilerinin olası tahmin edilmesine ve yasal olmayan uzaktan bağlantı kurulmasına karşı koruyan bir güvenlik özelliği. Koruma, doğrudan konsoldan bir politika yoluyla kolayca yapılandırılabilir ve engellenmemesi gereken bir şey engellendiğinde hariç tutmalar oluşturulabilir.

"Öne çıkan en büyük şey, pazardaki diğer ürünlere göre güçlü teknik avantajıdır. ESET bize sağlam bir güvenlik sunuyor, yani bilgisayarlarımızın %100 korunduğunu bilerek herhangi bir zamanda herhangi bir proje üzerinde çalışabilirim."

— Fiona Garland, Şirket Analist Grubu BT; Mercury Engineering, İrlanda; 1.300 üyelik



Kullanım örnekleri

Fidye yazılımı

Bazı şirketler, fidye yazılımı saldırılarından korunacaklarına dair ekstra güvence istiyor.

ÇÖZÜM

- ✓ Ağ Saldırısı Koruması, ağ düzeyinde suistimalleri durdurarak fidye yazılımlarının sisteme bulaşmasını önleyebilir.
- ✓ Çok katmanlı savunmamız, kod gizlemeyi kullanarak algılamadan kaçmaya çalışan kötü amaçlı yazılımları algılama yeteneğine sahip bir ürün içi sandbox'a sahiptir.
- ✓ Bir sonraki algılama güncellemesini beklemeye gerek duymadan yeni tehditlere karşı otomatik olarak koruma sağlamak için ESET'in bulut kötü amaçlı yazılım koruma sisteminden yararlanın.
- ✓ Tüm ürünler, ESET kullanıcılarının kötü amaçlı dosya şifrelemesinden korunmasını sağlamak için Fidye Yazılımı Kalkanı biçiminde koruma içerir.

Dosyasız kötü amaçlı yazılım

Dosyasız kötü amaçlı yazılım nispeten yeni bir tehdittir ve yalnızca bellekte bulunduğundan geleneksel dosya tabanlı kötü amaçlı yazılımlara göre farklı bir yaklaşım gerektirir.

ÇÖZÜM

- ✓ Eşsiz bir ESET Teknolojisi olan Gelişmiş Bellek Tarayıcı, kötü amaçlı yazılım sürecinin davranışını izleyerek ve bu kötü amaçlı yazılım bellekte gizlendikten sonra onu tarayarak bu tür tehditlere karşı koruma sağlar.
- ✓ Nasıl çalıştığı hakkında bilgi edinmek için tehdidi ESET Tehdit İstihbaratı'na yükleyerek veri toplama ve soruşturma süresini azaltın.
- ✓ Çok katmanlı teknoloji, makine öğrenimi ve insan uzmanlığı ile müşterilerimize mümkün olan en iyi düzeyde koruma sağlıyoruz.

Çalıntı kimlik bilgileri

Kimlik bilgilerini ve finansal verileri çalmak amacıyla gerçek kuruluşları taklit eden sahte web siteleri ve kimlik avı hırsızlığı saldırıları oldukça popülerdir.

ÇÖZÜM

- ✓ ESET uç nokta ürünleri, intranet çevresi içindeki ve buluttaki kritik verilere erişmek için kullanılan ana araç olarak tarayıcıya odaklanan özel bir koruma katmanıyla kuruluşun varlıklarını korumak için tasarlanmıştır.
- ✓ Güvenli Tarayıcı özelliği, çevrim içi arama esnasında hassas bilgileri korur.
- ✓ Tek tıkla yöneticiler, tüm bankacılık ve ödeme portallarını dahil etmeyi seçebilir ve tarayıcının belli web sitelerine karşı korunup korunmayacağına karar verebilir.

Şifre tahmin saldırıları

Uzaktan Masaüstü Protokolü (RDP) ve Sunucu İleti Bloğu (SMB), saldırganın sistemin tüm kontrolünü uzaktan ele geçirmesine izin veren, ilgi çekici saldırı vektörleridir.

ÇÖZÜM

- ✓ Kaba Kuvvet Saldırısına Karşı Koruma, parola korumalı uzaktan erişim noktalarındaki saldırılara karşı etkili bir savunma sağlar.
- ✓ Cihazları, kimlik bilgilerinin tahmin edilmesi olasılığına ve yasal olmayan uzaktan bağlantı kurulmasına karşı korur.
- ✓ Doğrudan konsoldan bir politika yoluyla kolayca yapılandırılabilir ve engellenmemesi gereken bir şey engellendiğinde hariç tutmalar oluşturulabilir.
- ✓ Çok Yönlü: Kullanıcılar kendi kurallarını ekleyebilir veya mevcut kuralları değiştirebilir.

"ESET'i bulduğumuzda bunun doğru seçim olduğunu biliyorduk; güvenilir teknoloji, güçlü algılama, yerel olarak bulunması ve mükemmel teknik destek, ihtiyacımız olan her şey."

— Ernesto Bonhoure, BT Altyapı Yöneticisi; Hospital Alemán, Arjantin, 1.500'den fazla üyelik

ESET hakkında

ESET® dünya çapında 30 yılı aşkın bir süredir işletmeler ve tüketiciler için sektör lideri BT güvenliği yazılımları ve hizmetleri geliştiriyor, ayrıca siber güvenlik tehditlerine kapsamlı ve çok katmanlı koruma sağlar.

ESET kötü amaçlı yazılımı önlemek, algılama ve kötü amaçlı yazılıma tepki vermek üzere makine öğreniminde ve bulut teknolojilerinde öncüdür. ESET, dünya genelinde bilimsel araştırmayı ve gelişmeyi destekleyen özel bir şirkettir.

SAYILARLA ESET

1 milyar+
küresel kullanıcı

400 bin+
kurumsal müşteri

200+
ülke ve bölge

13
küresel AR&GE merkezi

MÜŞTERİLERİMİZDEN BAZILARI

MITSUBISHI MOTORS
Drive your Ambition

9.000'den fazla uç nokta 2017'den beri ESET tarafından korunuyor

Allianz Suisse

4.000'den fazla posta kutusu 2016'dan beri ESET tarafından korunuyor

Canon Marketing Japan Group

32.000'den fazla uç nokta 2016'dan beri ESET tarafından korunuyor

T

2 milyon müşteri tabanı 2008'den beri ISP güvenlik ortağı

YÜKSEK SEKTÖR STANDARTLARINA BAĞLILIK

AV comparatives APPROVED Business Security DEC 2021

ESET, 2021 Aralık'ta AV - Comparatives tarafından düzenlenen Kurumsal Güvenlik Testi'nde ONAYLI Kurumsal Güvenlik Ürünü ödülüne layık görüldü.

G2 Leader WINTER 2022

ESET, sürekli olarak küresel G2 kullanıcı yorumu platformunda en yüksek sıralarda yer alıyor ve çözümleri dünya genelinde tüketiciler tarafından takdir görüyor.

FORRESTER®

ESET çözümleri, "The Forrester Tech Tide(TM): Sıfır Güven Tehdit Algılama ve Yanıt, 2021 ikinci çeyrek" dahil olmak üzere önde gelen analiz firmaları tarafından sürekli örnek satıcı olarak gösteriliyor.


eset
Digital Security
Progress. Protected.