ÇÖZÜME GENEL BAKIŞ

LIVEGUARD ADVANCED

Sıfır gün tehdidine ve daha önce görülmemiş tehdit türlerine karşı proaktif savunma

Progress. Protected.

Gelişmiş tehdit savunması nedir?

Hedefe yönelik saldırıların yanı sıra yeni, daha önce hiç görülmemiş tehdit türlerini, özellikle fidye yazılımlarını önlemek üzere gelişmiş uyarlanabilir tarama, son teknoloji makine öğrenimi, bulut sandbox ve derinlemesine davranışsal analizi kullanan proaktif bulut tabanlı teknoloji.

ESET LiveGuard Advanced; Mail Security, Endpoint ürünleri ve Cloud Office Security gibi ESET ürünleri için başka bir güvenlik katmanı sunar. Bulut tabanlı gelişmiş teknolojisi statik kod analizi gerçekleştiren, makine öğrenimini kullanarak örnekleri derinlemesine araştıran, bellek içi iç gözlem ve davranışa dayalı algılama kullanan birçok sensör türü içerir.

Proaktif bulut tabanlı tehdit savunması neden kullanılır?

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.

Proaktif bir bulut tabanlı tehdit algılama ürünü, fidye yazılımının üretim ortamında çalışmasını önlemek için şirket ağının dışında ek bir savunma katmanı sağlar.

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 saldırının tekrar gerçekleşmesini engellemek üzere çeşitli uygulamalara başvurur. Ancak bu, onları başka bir yepyeni vektör kullanabilecek bir sonraki saldırıdan korumaz.

Bulut güvenliği sandbox yaklaşımı, yalnızca olası tehdidin görünümüne bakmaktan çok daha etkilidir, çünkü yalnızca görünümün ötesine geçer ve bunun yerine olası tehdidin ne yaptığını gözlemler. Bu durum bir şeyin hedefe yönelik bir saldırı mı, gelişmiş sürekli tehdit mi veya iyi huylu mu olup olmadığını anlama konusunda yardımcı olur.

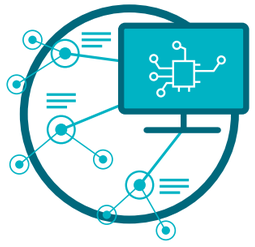
Statik ve dinamik analiz, derin öğrenme de dahil olmak üzere çeşitli teknikler kullanılarak bir dizi makine öğrenimi algoritması tarafından gerçekleştirilir.

Kullanıcı ağının dışındaki bir bulut güvenliği sandbox, yalnızca görünümü analiz etmenin ötesine geçebilir ve bunun yerine olası tehdidin gerçekte ne yaptığını gözlemleyebilir.

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.

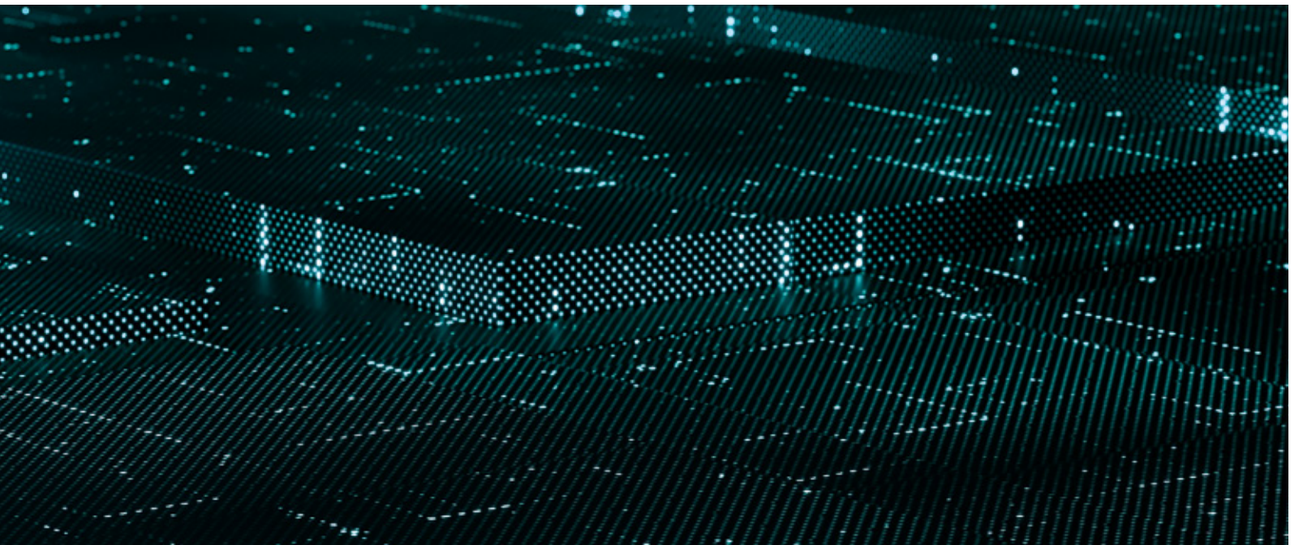


MAKİNE ÖĞRENİMİ

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

Günün her saati en iyi tehdit istihbaratını sağlamak için zengin bilgilerini ve istihbaratlarını paylaşan birinci sınıf güvenlik araştırmacıları.



ESET farkı

ÇOK KATMANLI KORUMA

ESET LiveGuard Advanced, istihbarat beslemeleri, ESET'in statik ve dinamik analiz için çok katmanlı iç araçları ve sıfır gün tehditlerini algılamak üzere itibar verileri kullanılarak gönderilen tüm şüpheli örneklerin davranışlarının değerlendirildiği ESET Genel Müdürlüğündeki güvenli test ortamına yürütülmek üzere tüm şüpheli örnekleri gönderen bir bulut tabanlı tehdit savunma çözümüdür. Ortaya çıkan sonuçlara bağlı olarak dinamik olarak dağıtılabilen örnekleri analiz etmek için dört katman kullanılır. ESET LiveGuard Advanced, algılama katmanlarından gelen tüm kararları birleştirir ve her örneğin durumunu değerlendirir. Sonuçlar önce kullanıcının ESET güvenlik ürününe ve şirketinin altyapısına iletilir.

TAM GÖRÜNÜRLÜK

Analiz edilen her örnek için nihai sonucu ESET PROTECT konsolunda görüntüleyebilirsiniz. Bunun da ötesinde, 100'den fazla lisansa sahip müşteriler, örnekler ve sandbox'ta analiz sırasında gözlemlenen davranışlar hakkında ayrıntılı bilgi içeren eksiksiz bir davranış raporu alır. Bu raporların tümü kolay anlaşılır bir biçimdedir. ESET LiveGuard Advanced'e gönderilen örneklerin yanı sıra ESET'in Bulut Kötü Amaçlı Yazılım Koruma Sistemi olan ESET LiveGrid®'e gönderilen her şeyi görüntülüyoruz.

HAREKETLİLİK

Günümüzde, kuruluşlardaki çalışanlar, şirket içinde değil, giderek daha fazla uzaktan çalışmaktadır. Bu nedenle ESET LiveGuard Advanced, kullanıcılar nerede olursa olsun dosyaları analiz edebilir. En iyi yanı ise kötü amaçlı herhangi bir şeyin algılanması durumunda tüm şirketin anında korunmasıdır.

GİZLİLİK

ESET, gizliliği ve düzenlemelerle uyum içerisinde olmayı oldukça ciddiye alır. Belirli ayarlar sayesinde kullanıcı, analizden sonra örnekleri derhal silecek şekilde ESET'i yapılandırabilir.

EŞİ OLMAYAN HIZ

Her dakika önemlidir, bu nedenle ESET LiveGuard Advanced, örneklerin çoğunu 5 dakikadan kısa sürede analiz edebilir. Örneğin daha önce analiz edilmiş olması durumunda, kuruluşunuzdaki tüm cihazların korunması sadece birkaç saniye sürer.

KANITLANMIŞ VE GÜVENİLİR

ESET, 30 yıldan fazla bir süredir güvenlik sektöründedir. Ayrıca, en yeni tehditlerin bir adım önünde olarak teknolojimizi geliştirmeye devam ediyoruz. Bunun sonucu olarak dünya genelinde 1 milyardan fazla internet kullanıcısı ESET tarafından korunuyor. Teknolojimiz, yaklaşımımızın en yeni tehditleri durdurma konusunda ne kadar etkili olduğunu gösteren üçüncü taraf test düzenleyiciler tarafından sürekli olarak dikkatle inceleniyor ve onaylanıyor.

PROAKTİF SAVUNMA

Bir örneğin şüpheli olduğu tespit edilirse, örneğin yürütülmesi engellenir ve örnek ESET LiveGuard Advanced tarafından analiz edilmeyi bekler. Bu, olası tehditlerin kullanıcının sisteminde hasara yol açmasını önler. Ayrıca analiz tamamlandığında ve bir uç noktada bir tehdit algılandığında, bu bilgi dakikalar içinde kuruluşun ağındaki her uç noktaya iletilir ve potansiyel olarak risk altında olabilecek tüm kullanıcılar derhal korunur.

Kullanım örnekleri

Fidye yazılımı

KULLANIM ÖRNEĞİ

Fidye yazılımı, e-posta yoluyla şüphelenmeyen kullanıcıların posta kutularına girmeye çalışıyor.

ÇÖZÜM

- ✓ ESET Mail Security, şüpheli e-posta eklerini otomatik olarak ESET LiveGuard Advanced'e yollar.
- ✓ ESET LiveGuard Advanced, örneği analiz eder ve ardından sonuçları genellikle 5 dakika içerisinde Mail Security'e iletir.
- ✓ ESET Mail Security, kötü amaçlı içeren bulunan ekleri algılar ve otomatik olarak ortadan kaldırır.
- ✓ Kötü amaçlı ek, alıcıya asla ulaşmaz.

Şirketteki farklı roller için ayrıntılı koruma

KULLANIM ÖRNEĞİ

Şirketteki her rol için farklı seviyede koruma gereklidir. Geliştiriciler veya BT çalışanları için ofis yöneticisinden veya CEO'dan farklı güvenlik kısıtlamaları gerekir.

ÇÖZÜM

- ✓ ESET LiveGuard Advanced'teki her bilgisayar veya her sunucu için benzersiz bir politika yapılandırın.
- ✓ Farklı statik kullanıcı grubuna veya Aktif Dizin grubuna bağlı olarak otomatik olarak farklı bir politika uygulayın.
- ✓ Kullanıcıyı bir gruptan bir diğerine geçirerek yapılandırma ayarlarını otomatik bir biçimde değiştirin.

Bilinmeyen veya sorgulanabilir dosyalar

KULLANIM ÖRNEĞİ

Bazen çalışanlar veya BT, güvenli olduğundan emin olmak için iki kere kontrol etmek istedikleri dosyalar alabilir.

ÇÖZÜM

- ✓ Tüm kullanıcılar, doğrudan tüm ESET ürünlerine analiz edilmek üzere örnek yollayabilir.
- ✓ ESET LiveGuard Advanced tarafından örnek hızlı bir şekilde analiz edilir.
- ✓ Dosyanın kötü amaçlı olduğuna karar verilmesi durumunda kuruluştaki tüm bilgisayarda korunur.
- ✓ BT yöneticisi, örneği gönderen kullanıcının bilgisayarıyla ilgili tam görünürlüğe sahiptir ve dosyanın temiz mi yoksa kötü amaçlı mı olduğunu görebilir.

ESET LiveGuard Advanced özellikleri

OTOMATİK KORUMA

Her şey ayarlandığında, yöneticinin veya kullanıcının yerine getirmesi gereken bir eylem yoktur. Uç nokta veya sunucu ürünü otomatik olarak örneğin iyi mi, kötü mü veya bilinmeyen mi olduğuna karar verir. Bilinmeyen bir örnekse, örnek analiz için ESET LiveGuard Advanced'e gönderilir. Analiz tamamlandığında, sonuçlar paylaşılır ve uç nokta ürünleri bu sonuçlara göre tepki verir.

SİZE UYGUN ÖZELLEŞTİRME

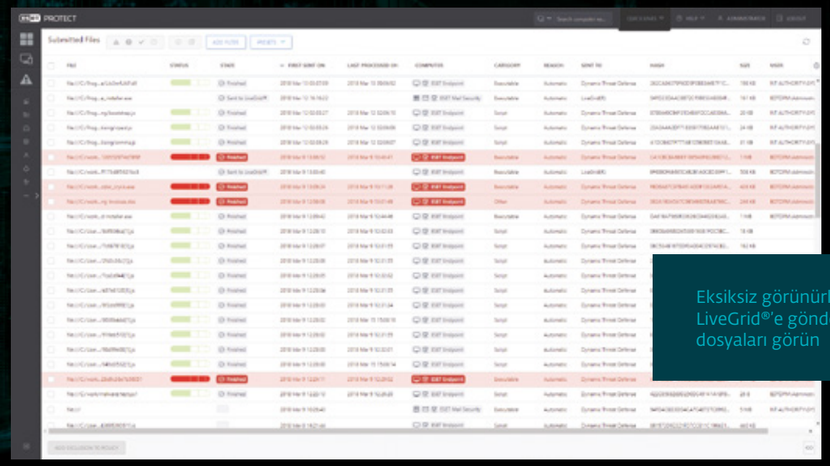
ESET, ESET LiveGuard Advanced için her bilgisayar için ayrıntılı politika yapılandırmasına izin verir, böylece yönetici, alınan sonuca göre neyin gönderildiğini ve ne olması gerektiğini kontrol edebilir. Ayrıca ayarlar sadece bilgisayar bazında değil, bilgisayar grubu bazında da uygulanabilir.

MANUAL GÖNDERME

Bir kullanıcı veya yönetici istediği zaman analiz için ESET uyumlu bir ürün aracılığıyla örnek gönderebilir ve tam sonucu alabilir. Yöneticiler, kimin neyi gönderdiğini ve sonucun ne olduğunu doğrudan ESET PROTECT konsolunda görebilir.

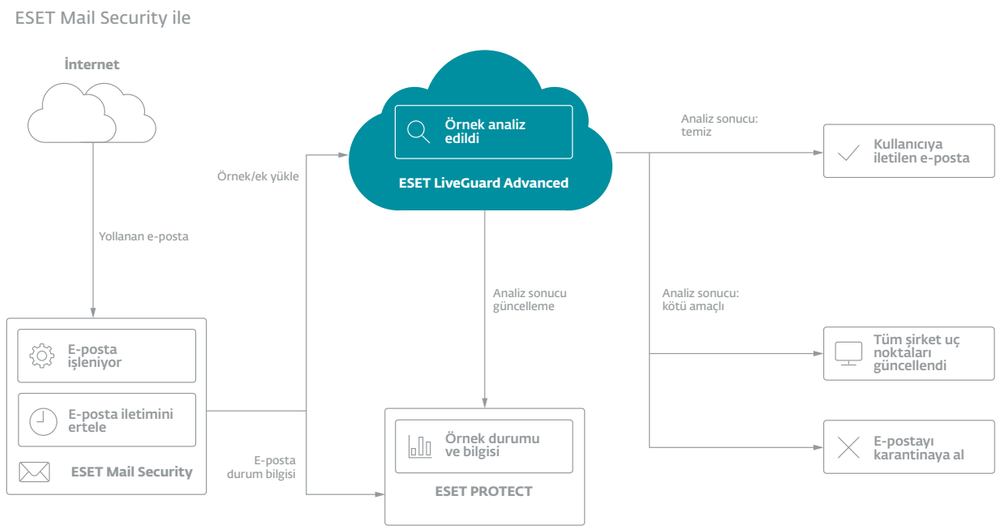
E-POSTA GÜVENLİĞİ KORUMASI

ESET LiveGuard Advanced, dosyalarla çalışmanın yanı sıra kötü amaçlı e-postaların kuruluşunuza teslim edilmemesini sağlamak için doğrudan ESET Mail Security ile de çalışır. İş sürekliliğini sağlamak amacıyla yalnızca kuruluş dışından gelen e-postalar inceleme için ESET LiveGuard Advanced'e gönderilebilir.



Eksiksiz görünürlük – ESET LiveGrid®'e gönderilen tüm dosyaları görün

ESET LiveGuard Advanced nasıl çalışır



ESET LiveGuard Advanced, ESET Endpoint, Server ve Cloud uygulama güvenliği (Microsoft 365) ürünleriyle uyumludur ve ESET yönetim konsollarına tamamen entegredir.

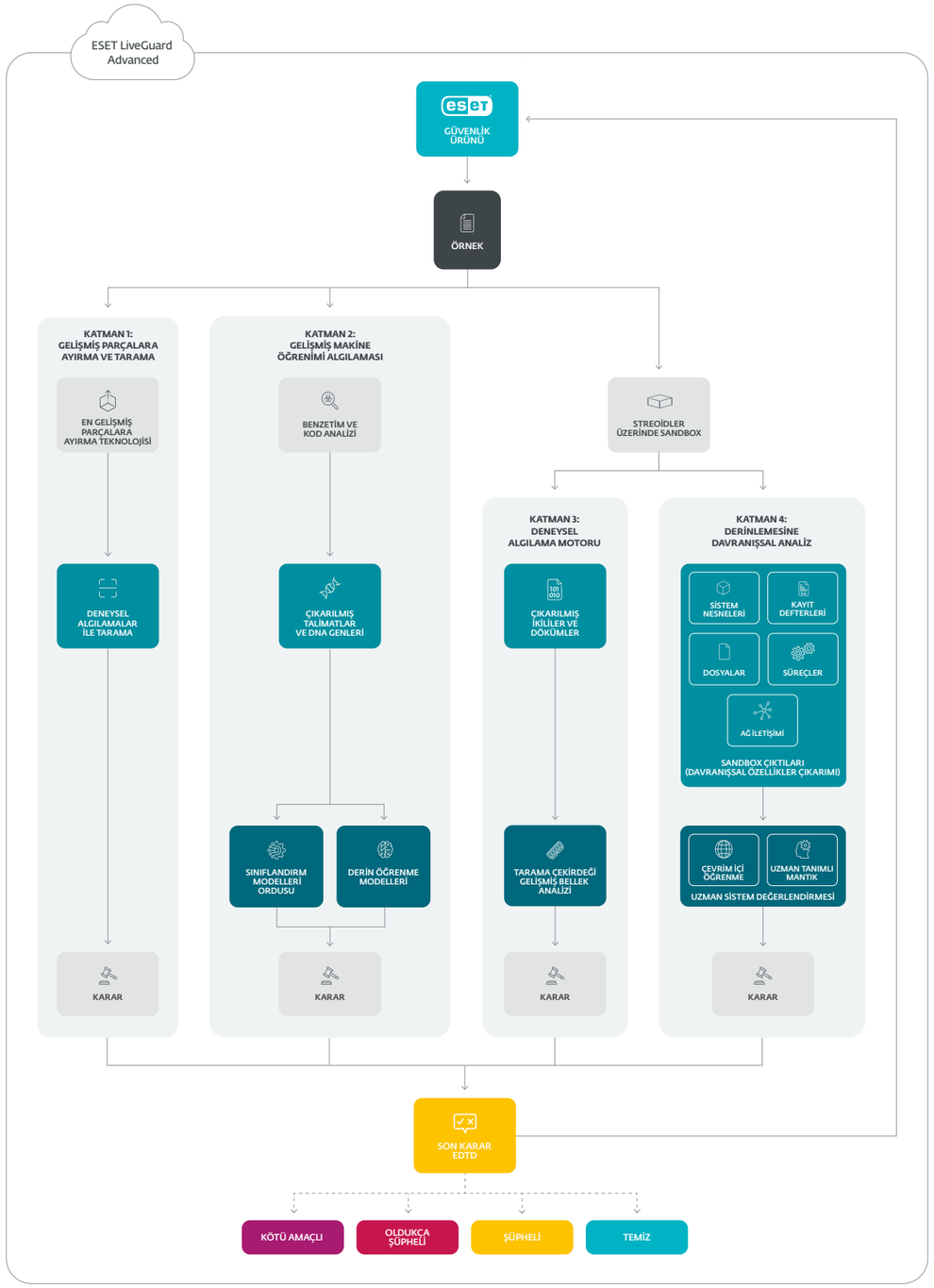
"Harika Ürün!"

En çok neyi seviyorsunuz?

"Tüm iş istasyonlarıma dağıtmanın kolay olmasını ve ağımı hızlı bir şekilde güvence altına almayı seviyorum. İstenmeyen yazılım buldum ve günlük e-postalar sayesinde ağ hataları can sıkıcı hale gelmiyor. Ağımın ESET tarafından korunduğunu bilerek daha rahat uyuyorum."

— Michael P./Ağ yöneticisi/Orta büyüklükte (51-1.000 çalışan)

Gelişmiş analizimiz nasıl çalışır



ESET LiveGuard Advanced, en yüksek algılama oranını sağlamak üzere 4 ayrı algılama katmanı kullanır. Her katman, farklı bir yaklaşıma sahiptir ve örnekle ilgili karar sunar. Nihai değerlendirme, örnekle ilgili tüm bilgilerin sonucuna göre yapılır.

KATMAN 1

Gelişmiş parçalama ayırma ve tarama

Örnekler statik analizden ve son teknoloji ürünü parçalara ayırma işleminden geçer ve ardından zenginleştirilmiş bir tehdit veritabanıyla eşleştirilir.

KATMAN 2

Gelişmiş makine öğrenimi algılaması

Statik ve dinamik analiz, derin öğrenme de dahil olmak üzere çeşitli teknikler kullanılarak bir dizi makine öğrenimi algoritması tarafından gerçekleştirilir.

KATMAN 3

Deneysel algılama motoru

Örnekler tam ölçekli kullanıcı cihazlarına çok benzeyen "steroidler üzerindeki sandbox'lara" yerleştirilir. Daha sonra herhangi bir kötü amaçlı davranış belirtisi için izlenirler.

KATMAN 4

Derinlemesine davranışsal analiz

Tüm sandbox çıktıları, bilinen kötü amaçlı modelleri ve eylem zincirlerini tanımlayan derinlemesine bir davranış analizine tabidir.

ÇÖZÜM, ALGILAMA KATMANLARINDAN GELEN TÜM KARARLARI BİRLEŞTİRİR VE HER ÖRNEĞİN DURUMUNU DEĞERLENDİRİR. SONUÇLAR ÖNCE KULLANICININ ESET GÜVENLİK ÜRÜNÜNE VE ŞİRKETİN ALTYAPISINA İLETİLİR.

EŞİ OLMAYAN HIZ

5 dakikadan kısa bir sürede bu işe ayrılan bulut sandbox analizi

ALGILAMA AVANTAJI

ESET LiveGuard AÇIK

ESET LiveGuard KAPALI **+ 135 dk**

Ortalama avantaj

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

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.