

ÇÖZÜME GENEL BAKIŞ



# PROTECT

Üst düzey ağ görünürlüğü sağlayan  
birleşik güvenlik yönetimi platformu.

Progress. Protected.

# Uç nokta güvenlik yönetim konsolu nedir?

**ESET PROTECT, çok yönlü bir UEM konsoldur. Şirket içerisinde veya bulutta dağıtılabilen bu konsol, tüm işletim sistemlerinde tam raporlama ve güvenlik yönetimi sunmanın yanı sıra şirket içinde ve dışında uç noktalara yönelik gerçek zamanlı görünürlük de sağlar.**

Ağda dağıtılan tüm ESET güvenlik çözümlerini tek bir panoda yönetme imkanı sunar. Masaüstü bilgisayarlar, sunucular, sanal makineler ve yönetilen mobil cihazlar dahil olmak üzere tüm platformlardaki uç nokta önleme, algılama ve yanıt katmanlarını kontrol eder.

# Neden uç nokta güvenlik yönetimi?

## GÖRÜNÜRLÜK

Sıfır gün tehditleri, gelişmiş kalıcı tehditler, hedefe yönelik saldırılar ve botnetler dünya genelinde tüm sektörler açısından sorun teşkil eder. Bu tehditleri gerçek zamanlı olarak görebilmek, BT personelinin bu tehditlere anında tepki vermesi ve ortaya çıkabilecek riskleri azaltması için oldukça önemlidir. Şirketlerin artan bir şekilde mobil iş gücüne geçmesiyle görünürlük yalnızca şirket içinde değil şirket dışında da gereklidir.

ESET PROTECT, BT personellerini şirket içindeki ve dışındaki tüm uç noktaların durumuyla ilgili bilgilendirmek üzere güncel bilgiler sağlar. Ayrıca, yalnızca birkaç sistemde değil, şirketteki tüm işletim sistemlerinde görünürlük sunar. Çoğu durumda, görünürlük durumun tam olarak farkına varılmasını sağlamak üzere donanım veya yazılım envanteri gibi cihaz seviyesinde bilgiler de sağlamak üzere geliştirilmiştir.

## YÖNETİM

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 keşfedildikten sonra ise kuruluşlar, cihaz tarama gibi belli görevleri tüm cihazlarda yürütmek isteyebilir. Bu durum, kuruluşların ileride yaşanabilecek bir saldırıya karşı daha iyi korunmak üzere yapılandırma politikalarını tamamen değiştirmeleriyle sonuçlanabilir.

ESET PROTECT, güçlü ve akıllı önceden tanımlı politikalar sunmanın yanı sıra kuruluşlara istedikleri zaman politikalarını yeniden düzenleme ve uç nokta güvenlik ürünlerinin yapılandırmalarını yeniden ayarlama imkanı da sunar. Ayrıca, görevler otomatikleştirilebilir. Bu sayede BT yöneticileri her bilgisayar için el ile görevleri yönetmek zorunda kalmadığından zaman kazanır.

## RAPORLAMA

Veri uyum yönetmeliklerinin karşılanması, çoğu kuruluşta raporlama ile ilgili gerekliliklerin en üst sırasında yer alır. Tüm kuruluşlarda, belirli aralıklarla oluşturulması gereken ve ilgili taraflara sunulan veya ileride kullanılmak üzere saklanan raporlar vardır.

ESET PROTECT, belirli aralıklarla rapor oluşturulabilir ve oluşturulan bu raporları belli dosyalarda saklayabilir veya istenen kişiye e-posta yoluyla doğrudan iletebilir. Düzinelerce işe yarar rapor şablonu bulunur ve bu şablonlar doğrudan kullanılabilir veya raporu talep eden kişinin ihtiyacına göre özelleştirilebilir. Devam eden raporlama ile ilgili olarak BT yöneticilerine zaman kazandırma konusunda büyük öneme sahiptir.

Gerçek zamanlı olarak bu tehditleri görebilmek, BT personelinin bu tehditlere anında tepki vermesi ve ortaya çıkabilecek riskleri azaltması için oldukça önemlidir.

Tüm kuruluşlarda, belirli aralıklarla oluşturulması gereken ve ilgili taraflara sunulan veya ileride kullanılmak üzere saklanan raporlar vardır.

*“ESET’in en büyük avantajı; tüm kullanıcıları tek konsolda görüntüleyebilmek, yönetebilmek ve tüm kullanıcıların güvenlik durumlarının tek konsoldan gözden geçirilebilmesidir.”*

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

# ESET farkı

## ÖNLEME AŞAMASINDAN YANITA

ESET PROTECT, ESET'in birçok güvenlik çözümününün yönetimini tek bir konsolda bir araya getirir. Kuruluşunuz için en iyi korumayı sunmak üzere tehdit önlemeden algılamaya ve yanıt vermeye kadar tüm kuruluşunuzda çok katmanlı bir çözüm sunar.

## TEK TIKLA OLAYIN DÜZELTİLMESİ

BT yöneticisi ana panodan durumu hızlı bir biçimde değerlendirebilir ve sorunları yanıtlayabilir. Tek bir tıklama hariç tutma listesi oluşturma, dosyaları daha ayrıntılı analiz etme veya tarama başlatma gibi eylemler gerçekleştirilebilir. Hariç tutmalar tehdit adı, URL, karma veya kombinasyona göre yapılabilir.

## GELİŞMİŞ RBAC

Çok faktörlü kimlik doğrulama (MFA) ile erişim sağlanan konsol, gelişmiş bir Rol Tabanlı Erişim Kontrolü (RBAC) sistemine sahiptir. Yöneticileri ve konsol kullanıcılarını belli ağ bölümlerine, nesne gruplarına atayabilir ve oldukça ayrıntılı bir şekilde ayarlayabileceğiniz izinler belirleyebilirsiniz.

## TAMAMEN ÖZELLEŞTİRİLEBİLEN BİLDİRİM SİSTEMİ

Bildirim sistemi tam olarak bir "ekranda ne görürsen onu alırsın" özelliğine sahiptir. Bu sayede tam olarak bildirim almak istediğiniz bilgiyle ilgili olarak uyarı alacak şekilde bildirimleri yapılandırabilirsiniz.

## DİNAMİK VE ÖZEL RAPORLAMA

ESET PROTECT, 170'ten fazla dahili raporlama sunar ve 1000'den fazla veri noktasıyla özel raporlar oluşturmanıza imkan tanır. Bu sayede kuruluşlar, tam olarak istedikleri şekilde raporlar oluşturabilir. Oluşturulan raporlar, belirli aralıklarla oluşturulmak ve e-posta ile gönderilmek üzere ayarlanabilir.

## OTOMASYON ÇERÇEVESİ

Dinamik gruplar, cihazın mevcut durumuna veya tanımlanan dahil etme kriterlerine göre bilgisayarları düzenleyebilir. Daha sonra görevler tarama, politika değişiklikleri veya yazılım kurma/kaldırma gibi dinamik grup üyeliği değişikliklerine bağlı eylemleri başlatmak üzere ayarlanabilir.

## TAM OTOMATİK VDI DESTEĞİ

Donanımına göre makineyi belirlemek üzere kapsamlı bir donanım algılama algoritması kullanılır. Bu sayede kalıcı olmayan donanım ortamlarının yeniden yüklenmesi ve kopyalanması otomatik olarak yapılır. Bu nedenle ESET'in VDI desteğine el ile müdahaleye gerek yoktur; tamamen otomatiktir.

## KANITLANMIŞ VE GÜVENİLİR

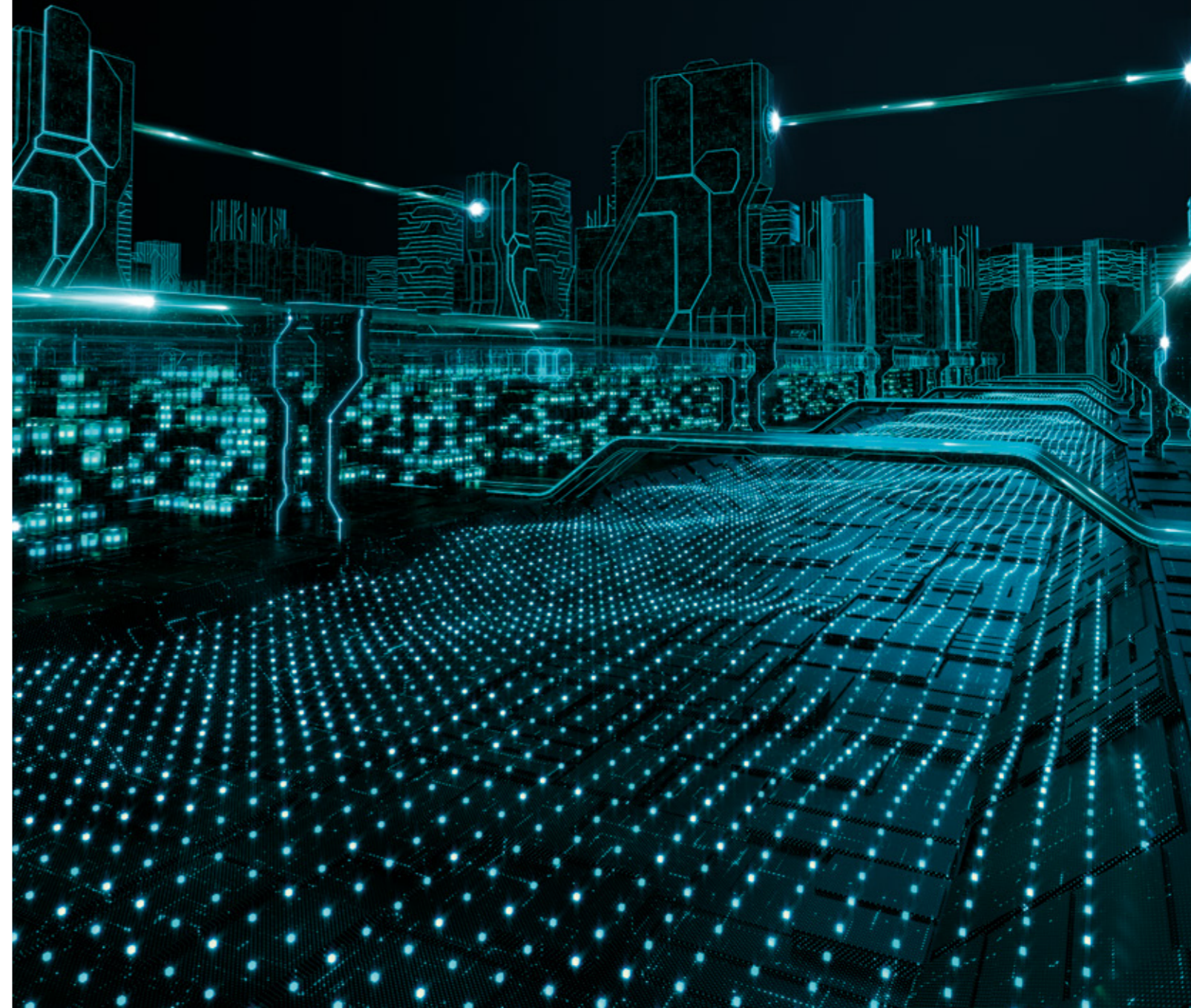
ESET, 30 yıldan fazla bir süredir güvenlik sektöründedir. Ayrıca, en yeni tehditlerin bir adım önünde olarak teknolojimizi geliştirmeye devam ediyoruz. Bu sayede dünya genelinde 110 milyondan fazla kullanıcı bize güveniyor. Teknolojimiz, yaklaşımımızın en yeni tehditleri durdurma konusunda ne kadar etkili olduğunu gösteren üçüncü taraf test düzenleyiciler tarafından sürekli olarak dikkatle inceleniyor ve onaylanıyor.

## MSP İÇİN HAZIR

Müşterilerinin ağırlarına önem veren bir Yönetilen Hizmet Sağlayıcı (MSP) iseniz, ESET PROTECT'in çok kullanıcı özelliklerini beğeneceksiniz. MSP lisansları otomatik olarak algılanır ve lisans sunucusuyla senkronize edilir. Ayrıca konsol, üçüncü taraf uygulamalarının kurulması/kaldırılması, komut dizilerinin ve uzaktan komutların çalıştırılması, yürütülen süreçlerin listelenmesi Donanım yapılandırılmaları gibi gelişmiş eylemleri gerçekleştirmenize olanak tanır.

*"Üstün teknik destek sağlayan bu olağanüstü şirket güçlü tehdit koruması ve merkezden yönetim imkanı sunuyor."*

— Dave, ABD, Deer Valley Birleşik Okul Bölgesi  
(15.500'den fazla üyelik), BT Sorumlusu



# Kullanım örnekleri

## Fidye yazılım

Bir kullanıcı, fidye yazılımının yeni bir biçimini içeren kötü amaçlı bir e-posta açıyor.

### ÇÖZÜM

- ✓ BT departmanı, belli bir bilgisayarda yeni bir tehdit algılandığına dair e-posta veya SIEM yoluyla bir bildirim alır.
- ✓ Virüs bulaşan bilgisayarda bir tıkla bir tarama başlatılır.
- ✓ Dosya, yine bir tıkla ESET LiveGuard Advanced'e yollarılır.
- ✓ Tehdidin sınırlandırıldığı onaylandıktan sonra, ESET PROTECT konsolundaki uyarılar otomatik olarak silinir.

## Kod geliştiriciler

İş bilgisayarlarında kod ile çalışan programcılar, derlenen yazılımlardan ötürü yanlış teşhisler oluşturabilir.

### ÇÖZÜM

- ✓ BT departmanı, yeni bir tehdit bulunduğu dair e-posta veya SIEM yoluyla bildirim alır.
- ✓ Bildirim tehdidin bir geliştiricinin bilgisayarından geldiğini gösteriyor.
- ✓ Dosyanın kötü amaçlı olmadığını onaylamak üzere dosya tek bir tıkla ESET LiveGuard Advanced'e yollarılır.
- ✓ BT departmanı tek bir tıkla ileride yanlış teşhislerin bu dosyada görüntülenmesini önlemek için bir hariç tutma oluşturur.

## VDI dağıtımları

Kalıcı olmayan donanım ortamları genellikle bir BT departmanından el ile etkileşim gerektirir, ayrıca raporlama ve görünürlükle ilgili de birçok sorun çıkarır.

### ÇÖZÜM

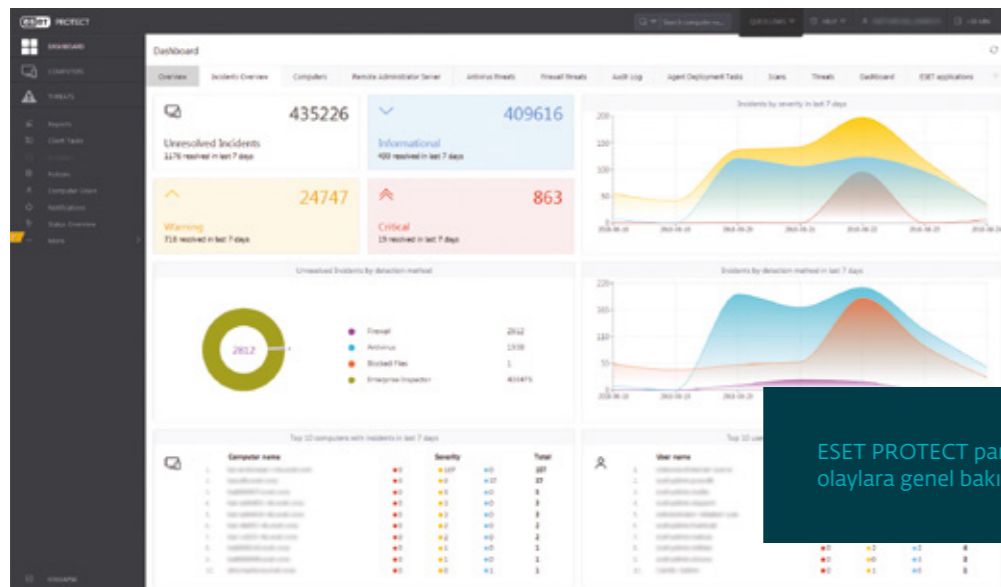
- ✓ ESET PROTECT'te bulunan bilgisayarlara ana imaj (master image) dağıttıktan sonra bilgisayarlar sistemin yeniden yüklenmesine rağmen önceki olayı raporlamaya devam eder.
- ✓ Çalışma süresinin sonunda ilk durumuna dönen makineler yeniden sayılmaz, aksine tek bir kayıt olarak kabul edilir.
- ✓ Kalıcı olmayan imajların dağıtımında, aracıyı da içeren bir imaj oluşturabilirsiniz. Bu sayede başka bir donanımın parmak iziyle yeni bir makine oluşturulduğunda, otomatik olarak ESET PROTECT'te yeni kayıtlar oluşturulur.

## Donanım ve yazılım envanteri

Kuruluşlar, her bir bilgisayarda hangi yazılımın kurulu olduğunu ve kaç yaşında olduğunu bilmelidir.

### ÇÖZÜM

- ✓ Sürüm numarası dahil olmak üzere bilgisayar kayıtlarında yüklenen her yazılımı görüntüleyin.
- ✓ Tüm bilgisayarların cihaz, üretici, model, seri numarası, işlemci, RAM, HD alanı ve buna benzer birçok donanım ayrıntısını görüntüleyin.
- ✓ Mevcut modellere ve yapımlara dayanarak ileriki yıllarda donanım yükseltmeleri ile ilgili bütçe kararlarını vermek üzere kuruluşla ilgili daha genel bir bakışa sahip olmak için raporlar oluşturun.



## Yazılımın düzeltilmesi

Kuruluşlar onaylanmayan bir yazılım kurulduğundan haberdar olmalı ve sonrasında yazılımı kaldırmalıdır.

### ÇÖZÜM

- ✓ Belli bir istenmeyen yazılımı bulmak üzere ESET PROTECT içerisinde dinamik bir grup belirleyin.
- ✓ Bir bilgisayar bu kriterleri karşıladığında BT departmanını bilgilendirecek bir bildirim oluşturun.

Dinamik grup kriterlerine uyan bir bilgisayar olması durumunda otomatik olarak yürütülmek üzere ESET PROTECT konsolunda bir yazılım kaldırma görevi kurun.

Kullanıcının ekranında söz konusu yazılımı yükleyerek, kullanıcının yazılım yüklemeye ilgili bir ihlaide bulunduğunu belirten bir kullanıcı bildirimini otomatik olarak belirmesini ayarlayın.

ESET PROTECT bulut konsolu olarak yürütülebilir, Windows'a veya Linux'a şirket içinde kurulabilir, sanal bir araç olarak dağıtılabilir.

Çoklu kullanıcı desteği ve 2FA ile güvenli girişler, büyük şirket ekiplerinde sorumlulukların tam anlamıyla düzenlenmesini sağlar.

*Tüm uç noktalarda, sunucularda ve mobil cihazlarda merkezi olarak yönetilen güvenlik, bizler için oldukça yararlıdır.”*

— Diamantis Masoutis S.A., Yunanistan,  
(6.000'den fazla üyelik)

# Teknik özellikler

## TEK BİR PANO

Tüm ESET uç nokta ürünleri, tek bir ESET PROTECT konsolundan yönetilebilir. Bu ürünlere iş istasyonları, mobil cihazlar ve sanal makineler dahildir. Ayrıca şu işletim sistemleri de dahildir: Windows, macOS, Linux ve Android.

## XDR DESTEĞİ

Durumun tam olarak farkına varılmasını arttırmak ve ağınızda görünürlüğü geliştirmek üzere ESET PROTECT, ESET PROTECT platformunun XDR etkinleştirme bileşeni olan ESET Inspect ile birlikte çalışır. ESET , birçok platformda (Windows, macOS ve Linux) kullanılabilir ve gelişmiş tehdit avı sunar. Tehdidin ortadan kaldırılmasını sağlar ve Güvenlik Operasyon Merkeziniz ile sorunsuz bir şekilde entegre olur.

## TAM DİSK ŞİFRELEMESİ (FDE)

Windows ve Mac (FileVault) uç noktalarındaki verinin şifrenmesini yöneten tam disk şifrelemesi ESET PROTECT'te özgü bir özelliktir. Bu özellik, veri güvenliğinin iyileştirilmesini sağlar ve kuruluşların veri yönetmelğine uyum sorunlarını çözmeye yardımcı olur.

## GELİŞMİŞ TEHDİT SAVUNMASI

Gelişmiş tehdit savunmasının desteklenmesi, şüpheli dosyaların güçlü ESET bulut sandbox'ta hızlı bir şekilde analiz edilerek fidye yazılım gibi sıfır gün tehditlerinin algılanmasını iyileştirir. Ayrıca, bulut detonasyonu dahil olmak üzere oldukça kapsamlı kötü amaçlı yazılım taramaları gerçekleştirir.

## DONANIM/YAZILIM ENVANTERİ

ESET PROTECT bir kuruluşta kurulmuş olduğu tüm yazılım uygulamaları ile ilgili rapor verir, ayrıca kurulduğu donanımlarla ilgili de rapor verir.

## TAMAMEN ÇOK KULLANICILI

ESET PROTECT konsolunun sınırlı bir kısmına erişim sağlamak üzere bir çok kullanıcı veya izin grupları oluşturulabilir. Bu sayede büyük şirket ekiplerinde sorumlulukların tam anlamıyla düzenlenmesini sağlar.

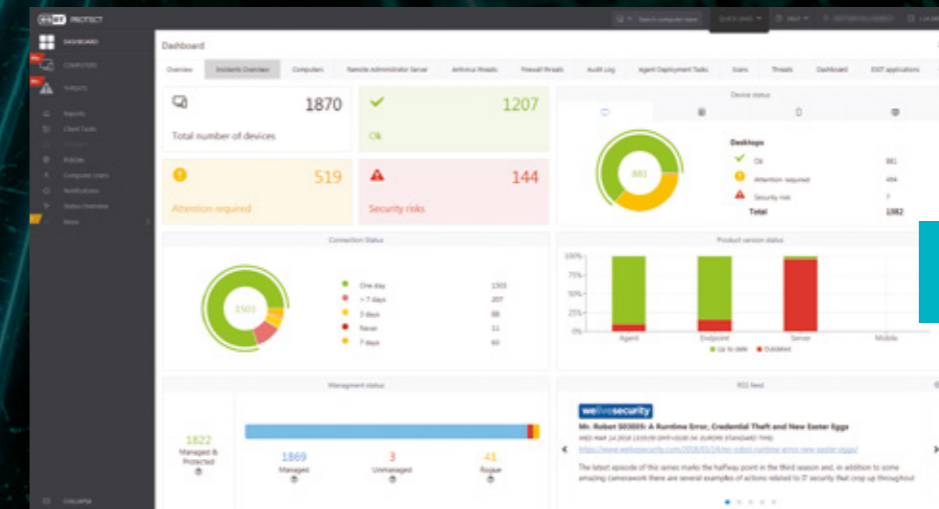
Bu durum bilgisayarların yapımına, modeline, işletim sistemine, işlemcisine, RAM'ına, HD alanına ve diğer birçok özelliğine göre dinamik olarak bilgisayarları gruplayarak tek bir konumdan daha fazla şey yapmanıza olanak tanır.

## AYRINTILI POLİTİKA KONTROLÜ

Kuruluşlar, aynı bilgisayar veya grup için birden çok politika belirleyebilir ve süregelen izinler için politikaları devam ettirebilir. Ayrıca kuruluşlar politika ayarlarını kullanıcının yapılandırabileceği şekilde belirleyebilir, bu sayede istediğiniz sayıda ayarı son kullanıcıların kullanmayacağı şekilde kısıtlayabilirsiniz

## SIEM VE SOC DESTEĞİ

ESET PROTECT, SIEM araçlarını tam anlamıyla destekler ve Güvenlik Operasyonları Merkezleri (SOC) ile entegrasyonu sağlamak üzere tüm giriş bilgilerinin yaygın kabul gören ISON veya LEEF biçiminde çıktısını alabilirsiniz.



ESET PROTECT Panosu

# Sonraki adımlarınız

## Nasıl satın alabilirsiniz:

İnternet sitemizden form doldurarak müşteri temsilcimizin sizinle iletişime geçmesini sağlayabilirsiniz.  
<https://www.eset.com/tr/business/contact-sales/>

## 30 günlük denemenize şimdi başlayın

Uç noktalar için koruma dahil olmak üzere tamamen işlevsel çözümü test etmek üzere 30 günlük ücretsiz denemeye sahip olun.

## Şirket içi ESET konsolundan geçiş:

Şu an ESET şirket içi konsolu mu kullanıyorsunuz? Geçişinize yardımcı olması için destek departmanımızla iletişime geçin.  
<https://www.eset.com/tr/support/business-support/>

# 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



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



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



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



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



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



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.





Digital Security  
Progress. Protected.

