KASPERSKY lab

Kaspersky Kurumsal Güvenlik Çözümleri 2018

#TrueCybersecurity

Kaspersky
Kurumsal Güvenlik Çözümleri
2018

Dijital Dönüşüm Çağında Siber Güvenlik Riskini Azaltma

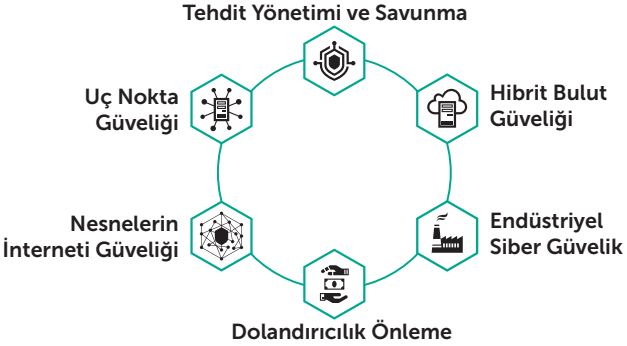
Siber saldırıların sayısı giderek artmaya devam ederken kurumsal altyapılara yönelik saldırılar, her geçen gün daha profesyonel ve hazırlıklı hale gelmektedir. Artık saldırıya uğrayıp uğrayamayacağınız sorusu geride kalmıştır. Önemli olan şey saldırıya ne zaman uğrayacağınız ve saldırı sonrasında ne kadar hızlı ve eksiksiz iyileşebileceğinizdir.

Ayrıca kurumsal BT altyapısı mobil cihazlara, herkese açık bulutlara ve üçüncü taraf sağlayıcılara kadar genişlediği için hiç olmadığı kadar karmaşık hale gelmiştir. Dijital dönüştürme iş verimliliği ve hızı açısından büyük avantajlar sağlamasına rağmen güvenlik açısından yeni zorlukları da beraberinde getirir. Kurumsal verileri ve müşteri verilerini korumanın yanı sıra iş sürekliliğini sağlamak ve finansal performansı korumak BT güvenlik ekibiniz ve bütçeniz üzerince ciddi bir yük oluşturur.

Kaspersky Lab'in yeni Kurumsal Portföyü günümüzün kurumsal işletmelerinin güvenlik taleplerini yansıtır. Bu portföy, statik ve mobil uç noktalar, sunucular, ağlar ve özel donanımlar ve yazılımlar dahil olmak üzere fiziksel, sanal ve bulut tabanlı sistemler için tamamen ölçeklenebilir koruma özelliklerini birleştiren eksiksiz bir siber güvenlik platformu oluşturmaktadır.

Lider teknolojilerin ve hizmetlerin benzersiz birleşimi, güvenlik ekibinizin saldırıların çoğunu önlemesini, yeni ve gelecekteki tehditleri tespit etmesini ve ortaya çıkan olayları yanıtlamasını sağlayarak operasyonel sürekliliğin ve yasal uyumluluğun elde edilmesine yardımcı olur.

Portföyümüz, aşağıdaki çözümlerden oluşur. Bu çözümlerin tamamı çok çeşitli uzman hizmetleri, güvenlik eğitimleri ve profesyonel destek ile tamamlanır:



Bu çözümler ve bileşen teknolojileri, uyarlanabilir bir güvenlik çerçevesi oluşturmak için birbirlerine sıkıca entegre edilmiştir. Bu özellik, en gelişmiş siber güvenlik tehditlerinin ve hedefli saldırıların tahmin edilmesini, önlenmesini, tespit edilmesini ve düzeltilmesini sağlar. Böylece performans üzerinde minimum etkiyle iş sürekliliği ve esnekliği geliştirilir.

Makine öğrenimi ve insan uzmanlığının yanı sıra sektör lideri tehdit istihbaratıyla desteklenen gerçek siber güvenlik, üstün performanslı koruma ve birleşik görünürlük ve yönetim sağlar. Ayrıca dijital dönüşümünüzü tam olarak destekler.

Dijital Özgürlüğünüz İçin Mücadele Etme

Verileriniz ve gizliliğiniz siber suçlular ve casuslar tarafından saldırıya uğramaktadır. Bu nedenle kurumsal varlıklarınızı savunma mücadelesinde yanınızda durmaktan korkmayacak bir ortağa ihtiyacınız vardır. Kaspersky Lab, 20 yıldır saldırılar kimden (basit hacker'lar, siber suçlular veya devletler) veya dünyanın neresinden gelirse gelsin her türlü siber tehdidi açığa çıkarır ve engeller. İnternet dünyasında saldırıların ve devlet destekli casusluk faaliyetlerinin olmaması gerektiğine inanıyoruz ve gerçekten özgür ve güvenli bir dijital dünya için mücadele etmeye devam edeceğiz.

Başarısını Kanıtlamış

Kaspersky Lab, bağımsız derecelendirmelerde ve araştırmalarda sürekli olarak en yüksek puanları alır.

- Sektördeki **80 tanınmış satıcıyla** birlikte değerlendirilmiştir
- **2017 yılında 86 testte 72 kez** birincilik elde edilmiştir
- **Tüm ürün testlerinin %90'ından fazlasında ilk üçe girilmiştir***
- Kaspersky Lab, 2017 yılında Uç Nokta Koruma Platformları pazarı için Gartner's Peer Insight** Customer Choice Awards ödüllerinde **Platinum Status** ödülünü almıştır

Global Araştırma ve Analiz Ekibimiz hükümetler ve devlet kurumlarıyla ilgili bazı önemli kötü amaçlı yazılım saldırılarının keşfedilmesinde ve açığa çıkarılmasında etkin bir rol oynamıştır.

Şeffaf

Tamamen şeffaf bir politikaya sahibiz ve yaptıklarımızı anlamayı daha kolay hale getiriyoruz:

- Şirketin kaynak kodunun, yazılım güncellemelerinin ve tehdit tespit kurallarının bağımsız incelemesi
- Şirket içi süreçlerin bağımsız incelemesi
- 2020 yılına kadar üç şeffaflık merkezi
- Keşfedilen her güvenlik açığı için 100 bin USD'ye varan bug bounty (ödül avcılığı) ödülleri

Bağımsız

Özel bir şirket olarak, kısa vadeli iş fırsatlarından ve kurumsal etkilerden bağımsızız.

Uzmanlığımızı, bilgi birikimimizi ve teknik bulgularımızı dünya güvenlik topluluğu, BT güvenlik satıcıları, uluslararası kuruluşlar ve emniyet teşkilatları ile paylaşırız.

Araştırma ekibimiz dünyanın her yerine dağılmıştır ve dünya çapında en saygın güvenlik uzmanlarından bazılarını içerir. Kaynaklarına veya amaçlarına bakmadan her türlü gelişmiş APT'yi tespit eder ve etkisiz hale getiririz.

---

* www.kaspersky.com/top3
** https://www.gartner.com/reviews/customerchoice-awards/endpoint-protection-platforms

Uç Nokta Güvenliği

Yeni Nesil siber güvenlik teknolojilerine dayanan çok katmanlı lider uç nokta güvenlik platformu

Tehdit ortamı sürekli gelişerek; kritik iş süreçlerini, gizli verileri ve finansal kaynakları sıfır gün açıklarından dolayı daha fazla riske sokmaktadır. Kurumunuzdaki riski azaltmak için sizi hedef alan siber suçlulardan daha akıllı, daha donanımlı ve daha bilgili olmanız gerekir. Ancak şirketlere yapılan siber saldırıların çoğu uç noktalar aracılığıyla başlatılır. Statik ve mobil uç noktalar dahil olmak üzere tüm kurumsal uç noktalarınızın, güvenliğini yeterli bir şekilde sağlarsanız genel güvenlik stratejiniz için sağlam bir temel atmış olursunuz.

2017 yılında Uç Nokta Koruma Platformları İçin Gartner Peer Insights Customer Choice Awards ödüllerinde **Platin Ödülü'nü kazanan tek sağlayıcıyız***.

*Gartner Peer Insights Customer Choice Logo'su; Gartner, Inc., ve/veya bağlı kuruluşlarının ticari markası ve hizmet markasıdır ve bu belgede izin alınarak kullanılmıştır. Tüm hakları saklıdır. Gartner Peer Insights Customer Choice Awards (https://www.gartner.com/reviews/customer-choice-awards/endpointprotection-platforms); bireysel son kullanıcı müşterilerinin kendi deneyimlerinden yola çıkarak beyan ettiği öznel fikirlerine, Gartner Peer Insights'ta yayınlanan yorumların sayısına, piyasadaki belirli bir satıcının genel derecesine ve http://www.gartner.com/reviews-pages/peer-insights-customer-choice-awards/ adresinde açıklanan diğer kriterlere göre belirlenir ve hiçbir şekilde Gartner ya da bağlı kuruluşlarının görüşlerini yansıtma amacı taşımaz.

Dijital Dönüşüm Beraberinde Ek Riskler Getirir

Birçok kurumsal BT ağının artan karmaşıklığı, tehditlerin gizlenebileceği "görünürlük boşlukları" yaratabilir.

Hedefli bir saldırı, hedef alınan sistemlerde ortalama 214 gün boyunca hiçbir şekilde tespit edilmeden gizlenebilir.

Bu süre boyunca tehdit, çeşitli kötü amaçlı etkinlikler gerçekleştirmeye devam edebilir. Bu nedenle hızlı bir şekilde tespit etme, kaldırma ve düzeltme sağlayabilen etkili araçların kullanılması çok önemlidir.

Maalesef bazı satıcıların gösterişli iddialarına rağmen her türlü riske karşı %100 koruma sağlayabilen Mucizevi bir güvenlik ürünü yoktur. Aynı şekilde "tek seferde onarım" sağlayan bir ürün de yoktur. BT güvenliği, sürekli olarak tehlikelerin nasıl geliştiğini değerlendiren bir süreçtir. Daha sonra;

- Güvenlik ilkeleri uyarlanır ve güncellenir
- Yeni güvenlik teknolojileri piyasaya sürülür

Bunlar sayesinde yeni risklerle mücadele edilir.

Kaspersky Endpoint Security, güvenilir, başarısını kanıtlamış ve çok katmanlı bir güvenlik platformuyla

bu ihtiyaçları giderir ve aynı zamanda şirketinizin kârını korur. Bu son derece sıkı bir şekilde entegre edilen çözüm, olağanüstü koruma, tespit ve olay yanıt özelliklerini bir araya getirir. Bu özellikler, Güvenlik İşlem Merkeziniz'i otomatik olarak zenginleştirmek ve risk azaltma becerinizi artırmak için benzersiz bir global güvenlik istihbaratı ve Yeni Nesil makine öğrenimi teknolojisi ile desteklenir. Her fiziksel, sanal ve bulut tabanlı uç nokta için koruma bir konsol aracılığıyla yönetilir. Böylece verimlilik artar ve toplam mülkiyet maliyeti azalır.

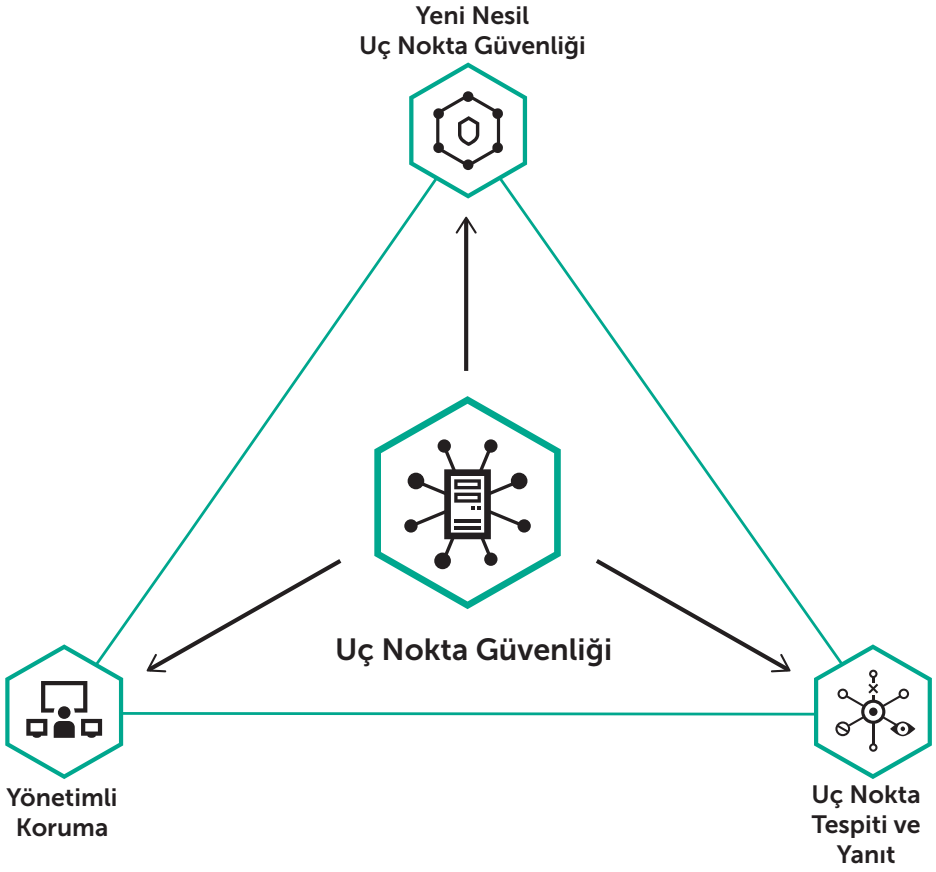
Bu platform şunları içerir:

- **Yeni Nesil Uç Nokta Güvenliği**
  Ödüllü tehdit istihbaratı motorumuzu temel alan ve granüler kontroller, fidye yazılımlarına karşı koruma ve açıklardan yararlanan yazılımları önleme teknolojilerimizi içeren tamamen ölçeklenebilir koruma.

- **Uç Nokta Tespiti ve Yanıtı**
  Saldırganlar ve tehditler, pahalı hasarlara yol açmadan saldırganları proaktif olarak bulma ve tehditleri durdurma; olaylara ve veri ihlallerine hızlı ve etkili bir şekilde yanıt verme.

- **Yönetilen Koruma**
  APT'leri araştırma konusunda dünya lideri olan ve kuruluşunuza yönelik siber tehditleri bulmaya odaklanan bir şirketten sürekli izleme ve olay yanıt hizmeti.

Uç Nokta Güvenlik Çözümü



Saldırılar nasıl gerçekleşir?

Saldırıların birçoğunda, dört farklı aşama bulunur:

- **Keşif**: saldırı için uygun giriş noktalarını belirleme
- **İzinsiz Giriş**: kurumsal ağdaki bir uç noktaya izinsiz giriş
- **Bulaşma**: genellikle kurumsal ağdaki birçok konuma yayılma
- **Uygulama**: siber suçluların kötü amaçlı eylemlerini uygulaması

Aşama aşama savunma

Saldırılarla mücadele etmenin en önemli yollarından biri, saldırının dört aşamasına karşı koruma sağlayabilen savunma araçlarına sahip olmaktır.

Keşiflere Maruz Kalmayı Önleme
Olası giriş noktalarına erişimi engelleme

İzinsiz Giriş Ön Yürütme İşlemine Karşı Koruma
Tehditler, bulaşmadan önce onları tespit etme

Bulaşma Yürütme Sonrası Süreçler
Şüpheli davranışları tespit etme ve bulaşan kötü amaçlı nesnenin kötü amaçlı eylemler gerçekleştirmesini önleme

Uygulama Otomatik Yanıt
Saldırıya maruz kalan işletmenin sistemlerini ve verilerini kurtarmasına yardımcı olma ve gelecekte benzer saldırılardan nasıl kaçınılabileceğini belirleme

Tek bir sağlayıcıdan çok katmanlı koruma

Saldırının her aşaması için savunma sağlarız ve her aşamada tek bir savunma katmanı değil birden çok savunma tekniği sunarız. Böylece müşterilerimiz saldırının her aşamasında çok katmanlı korumadan yararlanabilir.

1. Savunma Aşaması: Maruz Kalmayı Önleme
Saldırıları olası giriş noktalarında önlemeye yardımcı oluruz.

Koruma katmanlarımız şunları içerir:

- Ağ filtreleme
- Bulut destekli içerik filtreleme
- Bağlantı noktası kontrolleri

2. Savunma Aşaması: Ön Yürütme Güvenliği
"Sızan nesnenin" başlatılmasını durdurmaya yardımcı oluruz.

Koruma katmanlarımız ve hizmetlerimiz şunları içerir:

- Uç nokta güçlendirmesi
- Bilinirlik hizmetleri
- Makine öğrenimini dayalı ön yürütme tespiti
-

3. Savunma Aşaması: Çalışma Zamanı Kontrolü
Çalışanlarınızın kendi mobil cihazları dahil olmak üzere, şirket ağınıza bağlı tüm cihazlarda şüpheli davranış olup olmadığını proaktif olarak inceleriz.

Koruma katmanlarımız şunları içerir:

- Aşağıdakiler dahil olmak üzere makine öğrenimine dayalı davranış analizi:
  – Açıklardan yararlanan yazılımları önleme
  – Fidye yazılımlarına karşı koruma
- Yürütme ayrıcalık kontrolü

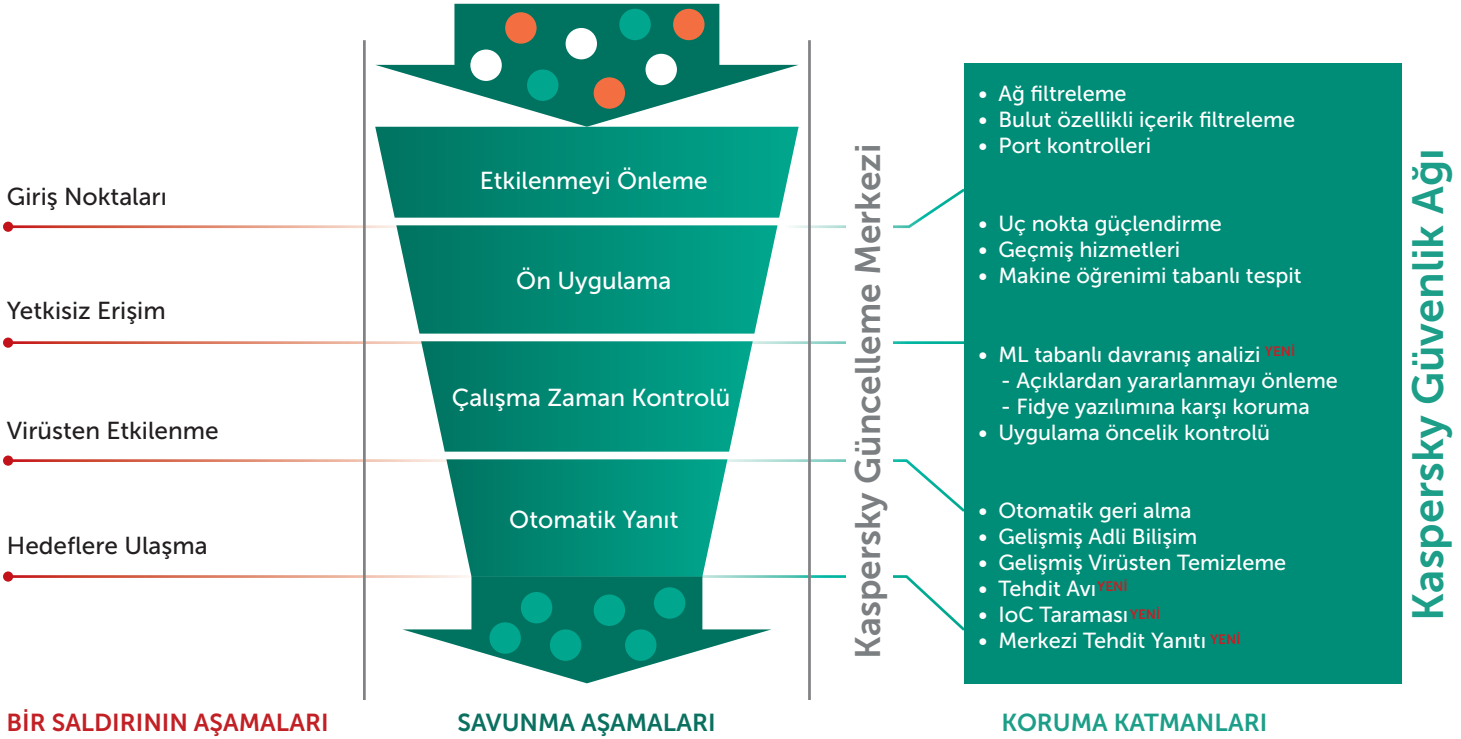
4. Savunma Aşaması: Otomatik Yanıt
İşletmeniz bir saldırıya maruz kaldıysa saldırı sonrası işlemlerle daha hızlı bir şekilde ilgilenmenize yardımcı oluruz.

Teknolojilerimiz ve hizmetlerimiz şunları içerir:

- Otomatik geri alma: Sistemlerin saldırıdan önceki durumlarına geri dönmelerine yardımcı olur
- Gelişmiş adli bilişim
- Gelişmiş temizleme
- Tehdit avı
- Risk Göstergesi (IoC) tarama
- Merkezi istihbarat yanıtı

Meta Katmanımız, ayrı savunma katmanlarının bulgularını birbirleriyle ilişkilendirerek ve ayrı savunma araçlarından kaçmayı başarabilen tehditleri belirleyerek şirketlerin tehlikeli Hedefli Saldırılara ve APT'lere karşı kendilerini korumak için daha fazla önlem almasına yardımcı olur.

Saldırı Zinciri



Mobil Güvenlik

Mobil güvenlik stratejinizi destekleyen entegre güvenlik ve yönetim

2017 yılında düzenlenen araştırmamıza göre kurumsal şirketlerin %38'i, mobil cihazların temel saldırı vektörü olarak kullanıldığı saldırılar nedeniyle suistimale veya kayba maruz kalmıştır.

1.700.000 USD

Mobil cihazlar aracılığıyla suistimalleri veya veri kayıplarını içeren bir güvenlik olayının Şirket için ortalama maliyeti

Mobil cihazlara yönelik kötü amaçlı yazılımlar, web siteleri ve kimlik avı saldırıları çoğalmaya devam ederken mobil cihazların özellikleri de gelişmeye devam etmektedir. Evde ve iş yerinde üretkenlik açısından verimli olan mobil cihazlar siber suçlular için cazip hedeflerdir. Kişisel cihazların iş amaçlı kullanılması (Kendi Cihazını Getir) kurumsal ağdaki cihaz ve platform çeşitliliğini artırmaktadır. Bu da BT altyapılarını yönetmeye ve kontrol etmeye çalışan BT yöneticileri için ek zorluklara neden olur.

Çalışanların Kişisel Cihazları Şirketler İçin Risk Oluşturur

Mobil cihazlarını hem iş hem de kişisel amaçları için kullanan çalışanlar BT altyapınızda güvenlik ihlâli yaşanma olasılığını arttırır. Hacker'lar, korunmasız bir mobil cihazdaki kişisel bilgilere erişim sağladığı andan itibaren kullanıcıların kurumsal sistemlerine ve iş verilerine ulaşması da kolaylaşır.

Hiçbir Platform Güvenli Değildir

Siber suçlular, mobil cihazlara yetkisiz erişim sağlamak için çeşitli yöntemler kullanır. Buna virüslü uygulamalar, düşük güvenlik düzeyine sahip ortak Wi-Fi ağları, kimlik avı saldırıları ve virüslü metin mesajları da dahildir. Bir kullanıcı yanlışlıkla kötü amaçlı bir web sitesini (veya kötü amaçlı kod bulaşmış yasal bir siteyi) ziyaret ettiğinde cihazlarının ve cihazda toplanan verilerin güvenliği risk altına girer. iPhone marka bir telefonu Mac bilgisayara bağlamak bile kötü amaçlı tehditlerin Mac'ten iPhone'a geçmesine neden olabilir (Bu tehditler Android, iOS ve Windows Phone gibi tüm yaygın mobil platformlar için geçerlidir.)

Çözüm: Kaspersky Security for Mobile

Kaspersky Security for Mobile, çok katmanlı Mobil Tehdit Savunması (MTD) ve mobil yönetim işlevleri sağlayarak bu sorunları çözer. Bu özelliklerin birleşmesi, güvenlik ekiplerinin mobil tehdit yönetimi için proaktif bir yaklaşım benimsemesini sağlar.

Hem uç noktalar hem de mobil cihazlar için tüm işlevler, aynı konsoldan yönetilerek kurumsal siber suçla etkili bir şekilde mücadele edilebilir.

Kötü amaçlı yazılımlara karşı fonksiyonel şifreleme ve korumanın bir araya gelmesi sayesinde, Kaspersky Security for Mobile çözümü yalnızca cihazı ve verileri izole etmek yerine mobil cihazlar için proaktif koruma sağlar.

Mobil Cihazlar için Gelişmiş Koruma

Kötü amaçlı yazılımlara karşı koruma teknolojisi, gelişmiş mobil tehditlere karşı koruma sağlamak için bulut destekli tehdit zekası ve makine öğrenimi ile bir araya gelir.

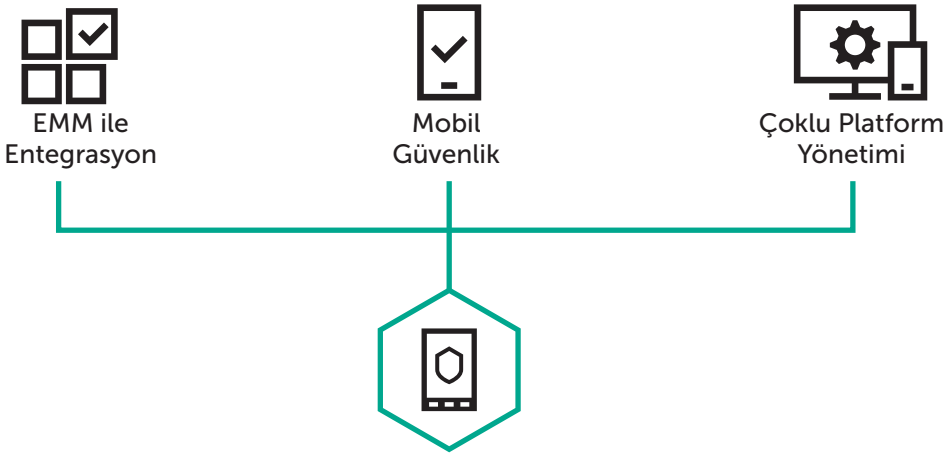
Web Kontrolü, Kimlik Avı ve İstenmeyen E-Postalara Karşı Koruma

Güçlü web kontrolü, kimlik avı ve istenmeyen e-postalara karşı koruma teknolojileri, kimlik avı saldırılarının yanı sıra istenmeyen web sitelerine, çağrılara ve iletilere karşı koruma sağlar.

EMM Platformları ile Entegrasyon

Mobil güvenliği tamamen EMM konsolunuz (VMware AirWatch, Citrix XenMobile) aracılığıyla uygulama ve yönetme

Mobil Cihazlar için Gelişmiş Koruma



Hibrit Bulut Güvenliği

Çoklu bulut ortamları için geliştirilmiş sınırsız güvenlik

Hibrit Bulut Güvenliği çözümümüz bulut tabanlı ortamlar için birleştirilmiş ve çok katmanlı koruma sağlar. Önemli iş verilerini ister özel ister herkese açık bir bulutta veya her ikisinde birden işleyin ve depolayın, hızlı ve sürekli güvenlik ile üstün verimliliğin mükemmel bir şekilde dengelenmiş birleşiminden faydalanabilirsiniz. Böylece verileriniz, günümüzdeki ve gelecekteki en gelişmiş tehditlere karşı korunu ve sistem performansınızdan taviz verilmez.

Yerel API entegrasyonu aracılığıyla basitleştirilmiş tedarik hizmeti sunulur. Çoklu bulut ortamlarınızı her türlü siber tehditten korumak için kaynaklar üzerinde mümkün olan en düşük etki bırakılır ve hassas özellikler sağlanır. Bu özelliklerin tümü, birleşik güvenlik düzenlemesi ve yönetimi kapsamında sunulur.

Tüm Bulutlar İçin Yeni Nesil Siber Güvenlik

Ortak güvenlik sorumluluğunuzun bir parçası olarak, herkese açık bulutlara yüklediğiniz nesneleri koruma ihtiyacını karşılar. Bulut API'larıyla entegrasyon, her bulut iş yükü için ödüllü siber güvenlik teknolojilerimizi sunmamızı sağlar.

Birleşik Düzenleme ve Şeffaflık

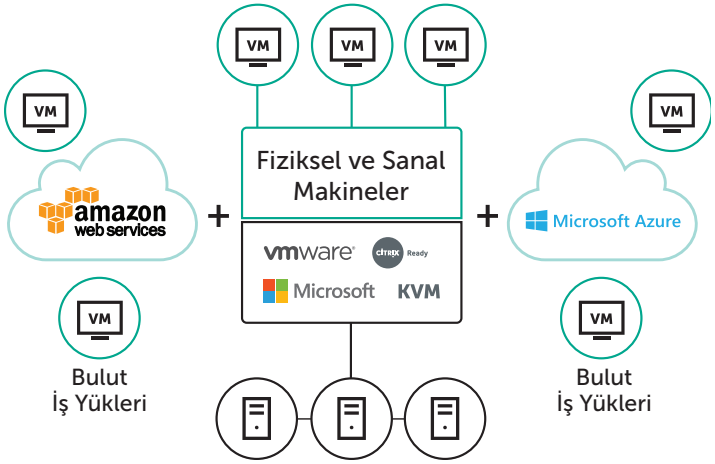
Sınırsız yönetilebilirlik, esneklik ve görünürlük kurumsal düzeyde güvenlik düzenleme konsolu aracılığıyla sağlanır. Sıra dışı şeffaflık, tüm hibrit bulut ortamınızın güvenlik katmanında tam olarak neler olduğunu bilmenizi sağlar. Siber güvenlik özelliklerinin tamamen otomatik olarak sağlanması özelliğiyle birlikte bu görünürlük avantajı, bulut varlığınızın tamamında daha iyi ve hızlı güvenlik için sorunsuz düzenleme sağlar.

Elastik ve Güvenli Bulut Ortamları İçin

Sanal ve fiziksel sunucular, VDI dağıtımı, depolama sistemleri ve hatta veri kanalları için başarısını kanıtlamış güvenlik. Patentli mimari ve entegrasyon özellikleri, BT ortamınızın merkezinde siber güvenliğin sağlanmasına yardımcı olurken iş açısından kritik sistemlerin operasyonel verimliliğini korur.

Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security, mükemmel bir şekilde düzenlenmiş ve uyarlanabilir siber güvenlik ekosistemi oluşturmak için gerekli her şeyi sağlar. Bu çözüm, çoklu bulut iş yüklerinizin gerektirdiği hassas özellikleri sağlarken kaynak verimliliği ve sorunsuz düzenleme üstün avantajlarını sunmaya devam eder. Kaspersky Hybrid Cloud Security, fiziksel, sanal ve bulut iş yüklerinizdeki uygulamaları ve verileri korumak için geliştirilmiştir. Çözüm, iş sürdürülebilirliği sağlar ve hibrit bulut ortamınızın tamamında standartlara uyumu hızlandırır.



Başarılı bir dijital dönüşüm stratejisinin parçası olarak kurumsal iş yüklerinizin fiziksel veya sanal sunucularda ya da VDI ortamlarında çalıştırıldığı Özel Veri Merkezi'niz için bazı konulara dikkat edilmesi gerekir:

- **Güvenli veri erişimi ve işleme** iş yüklerinizin hangi sanallaştırma platformunda veya fiziksel ortamda çalıştığına bakılmaksızın sağlanır
- **BT ve Güvenlik katmanları arasında birlikte çalışma özelliği** gelişmiş tehditlere karşı neredeyse sıfıra yakın yanıt süreleri sağlamak için yerel API'lar kullanılır
- **Kaynaklar açısından verimli çalışma** BT performansı geliştirilir ve kritik iş sistemlerinin verimliliği sağlanır

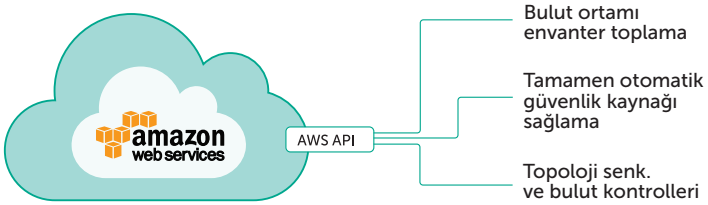
Kaspersky Hybrid Cloud Security; VMware NSX, Citrix XenServer and XenDesktop, MS Hyper-V ve KVM sanallaştırma platformlarına entegre edilen yazılım tanımlı veri merkezlerini koruma konusunda mükemmel bir başarı sunar ve kurumsal düzeydeki ortamları yönetme karmaşıklığını ortadan kaldırır. Yerel API'lar aracılığıyla BT merkezi ile entegrasyon sağlanması, güvenlik ihtiyaçlarını değerli sistem performansını neredeyse hiç etkilemeden karşılamaya yardımcı olur.

- VMware NSX for vSphere için entegre aracısız güvenlik, daha fazla koruma için güvenlik ve BT katmanlarının birlikte çalışmasına olanak tanır.
- Sanal sunucular ve VDI platformları için Patentli Hafif Aracılı koruma, kaynak açısından verimli ve hataya dayanıklı çalışma sağlar.
- Fiziksel sunucular için geleneksel çok katmanlı güvenlik, fidye yazılımlarına karşı koruma, açıklardan yararlanan yazılımları önleme ve davranış tespit teknolojilerini içerir.

Herkese Açık Bulutlar İçin Otomatik Siber Güvenlik

Özel veri merkezi kaynaklarının talep üzerine ve ihtiyaca göre harici bulutlara genişletilebildiği bir bulut hizmetleri modelinin benimsenmesi, benzersiz esneklik, çeviklik ve belirgin ekonomik avantajlar sunar. Ancak Ortak Güvenlik Sorumluluğu Modeli, bazı ek özelliklerin olmasını şart koşar. Bu özellikler, bulut ortamınızın tamamını kapsayan elastik bir siber güvenlik katmanı oluşturmalı ve Amazon Web Services (AWS) ya da Microsoft Azure iş yüklerinizi korumalıdır.

Amazon Web Services (AWS) teknolojisine entegre edilebilir



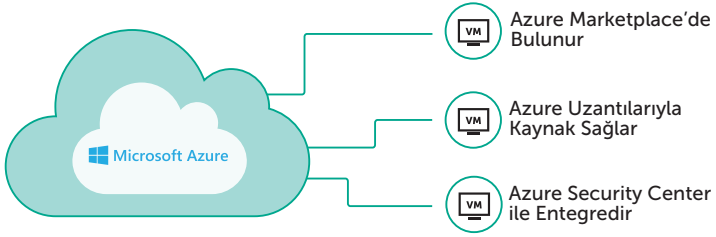
Kaspersky Hybrid Cloud Security, ortak güvenlik sorumluluğunuzun bir parçası olarak ortak buluta yüklenen her şeyi koruma ihtiyacınızı gidererek bulut varlıklarını korumaya yardımcı olur. Kaspersky Hybrid Cloud Security, bulut API'ı ile entegre olan çok katmanlı koruma sağlar. Bu çözüm, üstün bir çoklu bulut siber güvenlik düzenleme deneyimi sağlamak için daha fazla çeviklik ve sınırsız yönetim özellikleriyle ödüllü siber güvenlik tekniklerini tüm bulut iş yüklerinize sunmak üzere MarketPlaces aracılığıyla edinilebilir.

- Herkese açık bulutlardaki iş yüklerinizi koruyan sektör lideri siber güvenlik, bulut API aracılığıyla Amazon Web Services (AWS) ve Microsoft Azure Extensions ile yerel entegrasyondan faydalanır.
- Buluta özgü güvenlik özelliklerini tamamlar, buluttaki uygulamaların, işletim sistemlerinin, verilerin ve kullanıcıların korunmasına yardımcı olur ve GDPR standartlarına uyumluluğu destekler.
- Akıllı mimari ve API entegrasyonu bulut kaynakları üzerindeki etkiyi azaltarak envanter ve güvenlik sağlama özelliklerini otomatikleştirir.

Daha Fazla Koruma Sağlar

Buluta özgü araçları proaktif siber güvenlik, açıklardan yararlanan yazılımları önleme, bütünlük izleme, günlük denetimleri, uygulama kontrolleri, Yapay Zeka destekli çalışma zamanı koruması ve fidye yazılımlarına karşı koruma özellikleriyle tamamlarız. Her türlü siber tehditle mücadele edecek bir ürün.

Microsoft Azure için geliştirilmiştir



Tüm Bulutlar İçin Durdurulamaz Güvenlik

Buluta geçiş, hiçbir zaman bu kadar kolay ve güvenli olmamıştı. Kaspersky Hybrid Cloud Security çözümünde yerel API'lar ile entegrasyon, herkese açık bulut altyapı envanterinin daha kolay hazırlanmasının yanı sıra AWS ve Microsoft Azure bulutlarındaki tüm olaylarda otomatik güvenlik sağlama özelliğini sunar.

Kaspersky Hybrid Cloud Security, BT ortamınızın dönüşümünü desteklemek ve kolaylaştırmak için sektörde saygın birçok güvenlik teknolojisi sunar ve fiziksel ortamdan sanal ortama ve buluta geçişinizin güvenliğini sağlar. Ayrıca görünürlük ve şeffaflık özellikleri, kusursuz bir güvenlik düzenleme deneyimi sunar.

Kaspersky Security for Storage

Kaspersky Security for Storage, ağa bağlı kurumsal depolama cihazlarında (NAS) ve dosya sunucularında bulunan tüm değerli ve hassas veriler için sağlam, yüksek performanslı ve ölçeklenebilir koruma sağlar.

ICAP ve RPC dahil olmak üzere hızlı protokoller aracılığıyla sorunsuz entegrasyon; güvenilir ve kaynak açısından verimli korumanın yanı sıra optimize edilmiş son kullanıcı deneyimi sağlamak için depolama sistemlerinin verimliliğini korur. Depolama için güvenilir ve gerçek zamanlı koruma, optimum düzeyde süreklilik için kendi kendini savunma özellikleri içerir.

Güvenilir ve Şeffaf Veri Koruması

- Yerel entegrasyon, veri depolama sistemlerinin performansı ve üretkenliği üzerinde hiçbir olumsuz etki bırakmadan esneklik, ölçeklenebilirlik ve olağanüstü operasyonel verimlilik sağlar.
- Yenilikçi teknolojiler, en gelişmiş koruma özellikleri, hatalara karşı sıra dışı dayanıklılık ve fidye yazılımlarına karşı koruma sağlar.

Verileriniz Nerede Depolanırsa Depolansın Korur

- En yeni NAS ile yerel olarak entegre olur ve kurumsal dosya sunucularında çalışır
- Uç noktalardaki veya mobil cihazlardaki kötü amaçlı yazılımlara karşı koruma teknolojilerini kontrol etmeye gerek kalmadan veri depolarınızdaki tüm dosyaların güvenliği sağlanır
- Erişim veya talep üzerine kötü amaçlı yazılımlara karşı tarama görevleri için esnek ve granüler yapılandırma
- Optimum düzeyde çalışma sürekliliği için kendi kendini savunma özellikleri

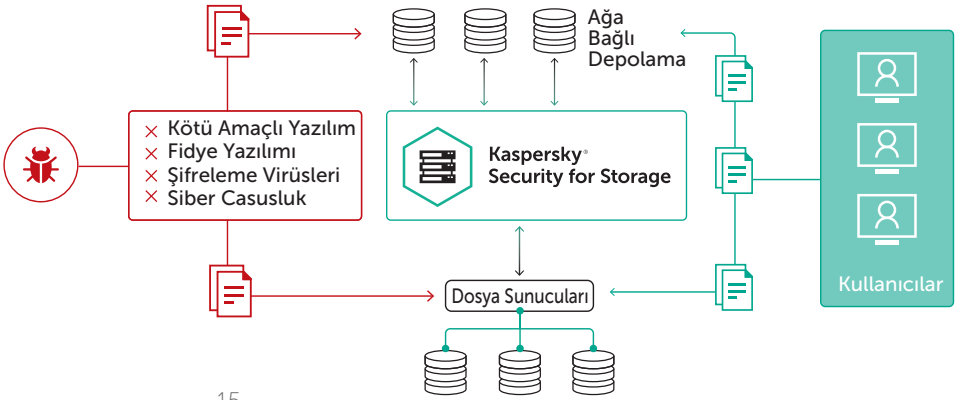
Kötü Amaçlı Yazılımlar ve Fidye Yazılımları ile Mücadele

- Ödüllü kötü amaçlı yazılımlara karşı tarama motorumuz, tüm dosyaları en gelişmiş saldırılara karşı savunur
- FPolicy aracılığıyla NetApp NAS cihazları için fidye yazılımlarına karşı gerçek zamanlı koruma (Kaspersky Lab tarafından başlatılmıştır
- Birden çok protokol aracılığıyla entegrasyon sayesinde geniş bir depolama cihazı yelpazesi desteği
-

Hafif ve Güvenilir Güvenlik Sağlar

- Yerel API ile entegrasyon, son kullanıcının verimliliğine daha az etki eden daha fazla güvenlik anlamına gelir
- Yük dengeleme ve hatalara karşı dayanıklılık, kesintisiz koruma sağlar
- Tüm depolama altyapınızda veri dosyası siber güvenliğinin tam görünürlüğünün sağlanması

Kaspersky Security for Storage, Kaspersky Hybrid Cloud Security çözümü ile birleştirilebilir. Böylece kurumsal veri merkezinizin hem fiziksel hem de sanal bileşenleri üzerinde sınıfının en iyisi koruma sağlanır.



Kaspersky DDoS Protection

Tek bir DDoS saldırısının finansal etkisi, işletmenin büyüklüğüne bağlı olarak 106.000 USD ila 1.600.000 USD arasında değişir. DDoS saldırısı organize etmenin maliyeti ise yaklaşık 20 USD'dir.

Dağıtılmış Hizmet Engelleme (DDoS) saldırısı başlatmanın maliyeti azaldığı için bu tür saldırıların sayısı artmıştır. Saldırılar gittikçe daha karmaşık ve korunması daha zor hale gelmektedir. Bu tür saldırıların değişen yapısı daha sıkı bir koruma gerektirir.

Otomatik olarak yayılmaya eğilimli kötü amaçlı yazılım saldırılarından farklı olarak, DDoS saldırıları insan uzmanlığına ve bilgilerine dayanır. Saldırgan, güvenlik açıklarını belirleyerek ve amaçlarına ulaşmak için en uygun saldırı araçlarını özenle seçerek hedef aldığı işletmeyi araştırır. Siber suçlular, saldırı sırasında gerçek zamanlı çalışarak zararı en üst dereceye çıkarmak için sürekli olarak taktiklerini değiştirir ve farklı araçları seçer.

Şirketlerin, DDoS saldırılarına karşı korunabilmesi için saldırıları mümkün olduğunca hızlı bir şekilde tespit eden çözümlere ihtiyacı vardır.

Çözüm: Kaspersky DDoS Protection

Kaspersky DDoS Protection, işletmenizi DDoS saldırılarına karşı korumak için her aşamayla ilgilenen DDoS saldırısına karşı tam koruma ve risk azaltma çözümüdür. Üç dağıtım seçeneği: Connect, Connect+ ve Control seçenekleri kullanılabilir.

Olası bir saldırı senaryosu fark edildiği anda Kaspersky Lab'in Güvenlik İşlemleri Merkezi (SOC) uyarılır. Kaspersky DDoS Protection Connect ve Connect+ kullanım senaryolarında, risk azaltma otomatik olarak başlatılır. Bu sırada mühendislerimiz DDoS saldırısının büyüklüğü, türü ve karmaşıklığına göre risk azaltma işlemini optimize etmek için ayrıntılı kontrollere başlar. Kaspersky DDoS Protection Control senaryosunda ise siber güvenlik ilkeleriniz, işletme amaçlarınız ve altyapı ortamınıza uygun olarak risk azaltma işlemine ne zaman başlayacağımıza siz karar verirsiniz.

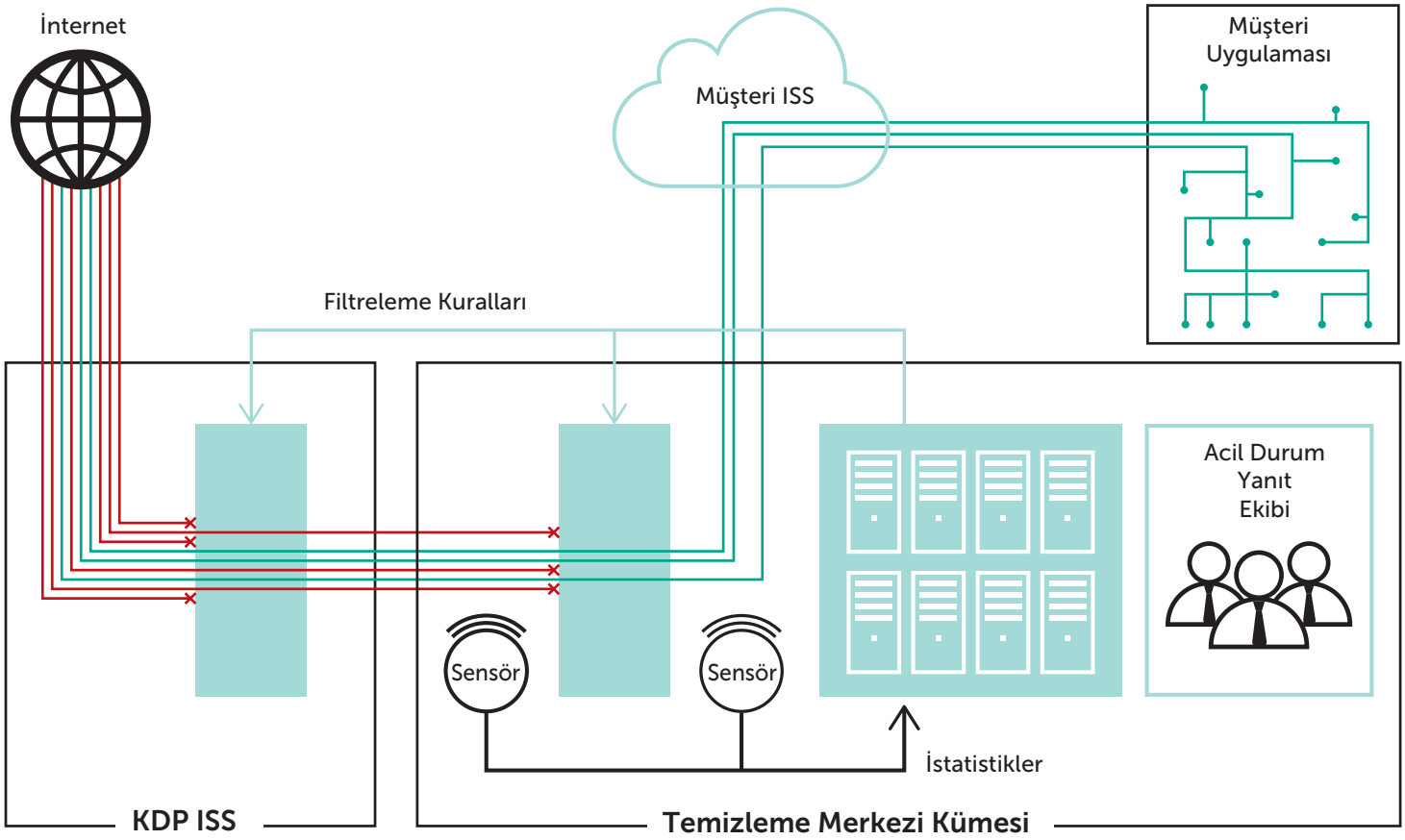
Farklı yapılandırmalara uyum sağlayacak esnekliğini sunan çözümümüzle işletmenizin ve çevrimiçi varlıklarının ihtiyaçlarını tam olarak karşılayabiliriz.

Kaspersky DDoS Protection Mimarisi

Bu tam savunma çözümü şunları sağlar:

- İş açısından önemli çevrimiçi kaynaklar ve ağ altyapıları için kapsamlı koruma
- Esnek dağıtım seçenekleri: Kaspersky DDoS Protection Connect, Connect+ ve Control
- Avrupa genelinde son derece büyük temizlik merkezleri
- Büyük veri güvenlik analizine dayalı gerçek zamanlı global DDoS istihbaratı
- 7/24 hızlı koruma ve Acil Yanıt Ekiplerinden destek.

Kaspersky DDoS Protection



Tehdit Yönetimi ve Savunma

Gelişmiş koruma ve tehdit istihbaratı

Yüksek oranda dijitalleştirilmiş altyapılar, kuruluşlar için yeni zorluklar anlamına gelir:

- Olay yanıtı için gereken büyük hacimli manuel görevler
- BT Güvenlik ekibinde personel eksikliği ve yüksek düzeyde uzmanlık eksikliği
- Sınırlı bir zaman dilimi içinde etkili bir şekilde işlemek, analiz etmek, çoğaltmak ve yanıtlamak için çok fazla güvenlik olayı
- Dijital altyapı kapsam olarak büyüdükçe güven sorunları ve veri paylaşımı uyumluluk sorunları.
- İhlal sonrası analiz için yetersiz görünürlük ve kanıt toplama zorluğu

Tehdit Yönetimi ve Savunma çözümlerine yatırım yapmanın işletme için değeri:

- Siber suçlardan kaynaklanan finansal ve operasyonel zararlarda azalma
- Basit, işletme odaklı yönetim arabirimi sayesinde daha az karmaşıklık
- Görev otomasyonu ve basitleştirilmiş güvenlik uyumluluğu süreçleri sayesinde daha düşük yönetim maliyetleri
- Sorunsuz iş akışı otomasyonu ve iş süreçlerinde aksamanın ortadan kaldırılmasıyla daha yüksek yatırım getirisi
- Hızlı tespit ile gelişmiş tehdit riskini azaltma

Dijital Dönüşüm: Siber Güvenlik İçin Yeni Bir Rol

Dijital dönüşüm, kurumsal büyümede önemli bir faktördür ve kuruluşlara birçok yeni fırsat sağlar. Ancak uyumluluk ve güvenli veri kullanımının yanı sıra BT altyapısının güvenliğini sağlamayla ilgili risklere de sahiptir. Gelişmiş Kalıcı Tehditler (APT'ler) dahil olmak üzere hedefli saldırılar ve karmaşık tehditler, artık şirketlerin mücadele etmesi gereken en tehlikeli risklerden birisidir. Dijital dönüşümde hızlandırılmış yeniliklerin desteklenmesine yardımcı olmak için birleşik bir çözüm olarak geliştirilen **Kaspersky Threat Management and Defense**, kuruluşun kendine özgü özelliklerine ve devam eden süreçlerine uyum sağlar. Bu çözüm, lider güvenlik teknolojileri ve siber güvenlik hizmetlerinin birleşimiyle, gelişmiş tehditlere ve benzersiz hedefli saldırılara karşı eksiksiz bir kurumsal koruma sağlamak için birleşik bir yöntem geliştirmenize yardımcı olur.

Kaspersky Threat Management and Defense, kuruluşun tehdit yönetim stratejisinin geliştirilmesini veya büyütülmesini destekleyerek bilgilerin ve dijital kanıtların otomatik olarak toplanmasını sağlar, manuel tespit işlemini kolaylaştırır ve makine öğrenimi destekli olay analizini otomatikleştirir. Sağlanan zengin veri havuzu, karmaşık olay incelemesine yardımcı olur ve en karmaşık tehditleri bile engellemek için gerekli desteği ve uzmanlığı sağlar.

Kaspersky Threat Management and Defense, lider teknolojilerden ve hizmetlerden oluşan benzersiz bir birleşim sunarak Uyarlanabilir Güvenlik Stratejisi'nin uygulanmasını destekler. Böylece saldırıların birçoğunun Önlenmesine, benzersiz yeni tehditlerin hızla Tespit Edilmesine, canlı olaylara Yanıt Verilmesine ve gelecekteki tehditlerin Öngörülmesine yardımcı olur. Kaspersky Threat Management and Defense aşağıdaki bileşenleri içerir:

- **Kaspersky Anti Targeted Attack** Ağ ve uç nokta izleme, gelişmiş korumalı alan teknolojisi ve tehdit istihbaratı odaklı analiz ile birleştirilmiş lider güvenlik istihbaratı ve gelişmiş makine öğrenimi teknolojilerine dayalıdır. Kaspersky Anti Targeted Attack, kuruluşların hedefli saldırıları, gelişmiş tehditleri ve halihazırda ele geçirilmiş sistemleri tespit etmelerine yardımcı olmak için farklı olayları ilişkilendirir ve olayların öncelik sırasını belirler.

- **Kaspersky Endpoint Detection and Response** adli bilişim verilerinin otomatik olarak toplanmasını ve merkezi olarak depolanmasını sağlayarak uç nokta tehdit görünürlüğü elde edilmesine yardımcı olur. Kaspersky Endpoint Detection and Response, Kaspersky Anti Targeted Attack ile aynı arayüzü ve Kaspersky Endpoint Security ile aynı aracıyı kullanır. Bu çözüm, karmaşık hedefli saldırıları ortaya çıkarmak, tanımlamak ve açığa çıkarmak için çok yönlü bir yaklaşım sağlar. Gelişmiş teknolojiler kullanarak tehditleri tespit etmeye, saldırılara zamanında yanıt vermeye ve uç noktalardaki tehditleri bularak kötü amaçlı eylemleri önlemeye odaklanır.

- **Kaspersky Siber Güvenlik Hizmetleri**, devam eden bir olay sırasında hızlı ve profesyonel destek sunar. Olay sonrasında ise gizliliği ihlal edilen verilerin risklerini azaltmaya ve olası finansal kayıpları ve itibar kaybını en aza indirmeye yardımcı olur. Siber Güvenlik Hizmetleri portföyümüz geniş bir Güvenlik Eğitimi müfredatı, güncel Tehdit İstihbaratı, hızlı Olay Yanıtı, proaktif Güvenlik Değerlendirmeleri, tamamen dış kaynaklı Tehdit Avı hizmetleri ve 7/24 Üst Düzey Destek avantajlarını içerir.

Müşterinin gelişmiş önleme becerileri gereksinimlerine ve şirket verilerinin tam izolasyonu dahil olmak üzere şirket altyapısının kendine özgü taleplerine bağlı olarak Threat Management and Defense çözümümüzü aşağıdaki ürünlerle zenginleştirebiliriz. Bu ürünler sayesinde risk azaltmanın yanı sıra gelişmiş tehditler ve hedefli saldırılar konusunda gerçekten entegre ve stratejik bir yaklaşım elde edilebilir:

- **Kaspersky Endpoint Security**, HuMachine İstihbaratı'na dayanan Yeni Nesil siber güvenlik teknolojilerini temel alan çok katmanlı bir uç nokta koruma platformudur. Bu platform makine öğrenimi motorları, şüpheli davranış tespiti, kontroller ve veri koruma gibi özellikler aracılığıyla dosyasız saldırılar ve kötü amaçlı yazılımlar dahil olmak üzere en gelişmiş bilinen ve bilinmeyen tehditlere karşı esnek ve otomatik koruma sağlar.

- **Kaspersky Secure Mail Gateway**, hedefli saldırılara karşı önleyici yaklaşımın bir parçasıdır. Bu çözüm posta sunucularından geçen trafik için istenmeyen e-postalara, kimlik avı saldırılarına, genel ve gelişmiş kötü amaçlı yazılım tehditlerine karşı otomatik e-posta tehdit önleme özelliği sunar ve olağanüstü bir koruma sağlar. Kaspersky Secure Mail Gateway; hangi posta gönderme yolunun (bulut, şirket içi, şifreli) kullanıldığına bakılmaksızın en karmaşık heterojen altyapılarda bile etkili bir şekilde çalışır.

- **Kaspersky Private Security Network**, sıkı veri paylaşım kısıtlamalarına sahip izole ağlar ve ortamlar için kapsamlı bir tehdit istihbarat veritabanı sunar. Böylece işletmelerin, verilerini kontrollü çevre dışına çıkarmalarına gerek kalmadan bulut destekli güvenliğin avantajlarından faydalanması sağlanır. Bu ürün, Kaspersky Security Network'ün şirkete ait, yerel ve tamamen özel bir sürümüdür. Kaspersky Private Security Network, en küçük verilerin dahi yerel ağdan çıkmasına gerek kalmadan kritik siber güvenlik endişelerini giderir.

Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack çözümü; ağ, uç noktalar ve global tehdit ortamı gibi birçok katmandan gelen olayları ilişkilendirerek karmaşık tehditlerin neredeyse gerçek zamanlı olarak tespit edilmesini sağlar. Ayrıca soruşturma sürecini güçlendirmek için önemli adli bilişim verileri sunar.

Kaspersky Anti Targeted Attack kuruluşlara aşağıdaki avantajları sağlar:

- Başlangıçtan itibaren yeni süreçlerin güvenliğini ve uyumluluğunu sağlayarak entegre iş sürekliliği
- Gölge BT ve gizli tehditlerin üzerinde görünürlük
- Görünürlük ve kontrolün gerekli olduğu her yerde, hem fiziksel hem de sanal ortamlarda dağıtım sağlayan maksimum esneklik
- İnceleme ve yanıt görevlerinin otomasyonu ile güvenliğinizin, olay yanıtının ve Güvenlik İşlem Merkezi ekiplerinizin maliyetini optimize hale getirme
- Mevcut güvenlik ürünleriyle sıkı ve doğrudan entegrasyon, genel güvenlik düzeylerini artırma ve eski güvenlik yatırımını koruma

Kaspersky Endpoint Detection and Response

Geleneksel uç nokta güvenlik ürünleri (örneğin Kaspersky Endpoint Security), fidye yazılımları, kötü amaçlı yazılımlar ve botnetler gibi çeşitli tehditlere karşı koruma sağlama konusunda önemli bir rol oynamaktadır. Ancak, daha geniş bir yelpazedeki gelişmiş siber saldırılara ve akıllı saldırganlara karşı koruma sağlamak için kuruluşlar, artık uç nokta tespit ve yanıt çözümü dahil olmak üzere uç nokta düzeyinde ek koruma düzeyleri uygulamak zorundadır.

Kaspersky Endpoint Detection and Response, kuruluşlara aşağıdaki konularda yardımcı olur:

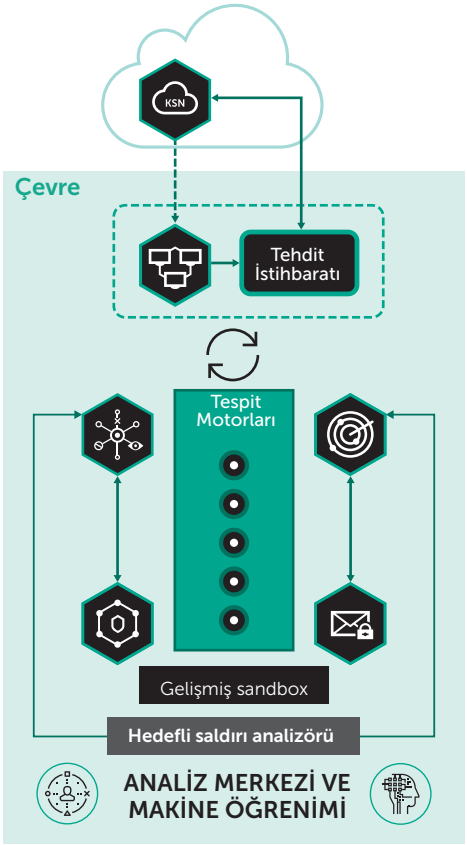
- İş kesintisi olmadan tehditlerin belirlenmesini ve tehditlere yanıt verilmesini otomatikleştirme
- Makine öğrenimi, korumalı alan, risk Göstergesi taraması ve tehdit istihbaratı dahil olmak üzere gelişmiş teknolojiler aracılığıyla uç nokta görünürlüğünü artırma
- Olay Yanıtına yönelik kullanımı kolay kurumsal bir çözümle siber güvenliği güçlendirme
- Birleştirilmiş ve etkili Tehdit Avı, Olay Yönetimi ve Yanıt süreçleri oluşturma.

Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway, hedefli saldırıların tespiti ve önlenmesine yönelik tek yaklaşımın parçası olarak her türlü posta trafiğini korumak için gelişmiş teknolojiler sunan bir otomatik e-posta tehdit önleme çözümüdür. Kaspersky Secure Mail Gateway, e-posta güvenliğine çok katmanlı ve otomatik bir yaklaşım getirmek için tehdit istihbaratı, makine öğrenimi ve gelişmiş korumalı alan teknolojileriyle desteklenir. İstenmeyen e-postalara karşı yenilikçi bulut destekli koruma, kimlik avı saldırılarına karşı koruma ve sıfır gün ve açıklardan yararlanan yazılımlara karşı koruma özelliklerine sahip gelişmiş ve çok katmanlı kötü amaçlı yazılımlara karşı koruma sağlar.

Kaspersky Secure Mail Gateway kuruluşlara şunları sağlar:

- Bilinen, bilinmeyen ve gelecekteki tehditleri otomatik olarak önleme
- İmza tabanlı, bulut destekli dosya analizi
- Makine öğrenimi yöntemleriyle dosya analizi
- Hızlı olay bildirimi
- Kurumsal siber güvenliğin sorunsuz gelişimi



Kaspersky Private Security Network

Kaspersky Private Security Network, Kaspersky Security Network'ün (KSN) yerel ve tamamen özel bir sürümüdür. Bu çözüm, kontrollü çevresinin dışına veri aktarmak istemeyen kuruluşların global bulut tabanlı tehdit istihbaratının birçok avantajından faydalanmasını sağlar.

Patentli bir teknoloji olarak Kaspersky Private Security Network:

- URL'lerin ve Dosyaların global istatistiklerine erişim imkânı sunar
- URL'ler, ve dosyaları, kötü amaçlı ve güvenli nesnelere göre özel kararlar vererek sınıflandırır
- Gerçek zamanlı tehdit farkındalığı sayesinde siber güvenlik olaylarının neden olduğu hasarı en aza indirir
- Benzersiz, müşteriye özgü ve üçüncü taraf tehdit kaynaklı kararların (dosya karmaları) eklenmesini sağlar
- Sıkı mevzuat, güvenlik ve gizlilik standartlarına uyum sağlar.

Siber Güvenlik Hizmetleri

Yeni bir siber bağışıklık düzeyi sağlayan istihbarat ve uzmanlık

Tehdit İstihbarat Portalı

Kaspersky Lab, müşterileriyle güncel istihbaratını paylaşarak kuruluşların, tehdit unsurları tarafından kullanılan yöntemleri, taktikleri ve araçları 360 derece görmelerini sağlar ve modern siber tehditlere karşı önlem almalarına yardımcı olur. Geniş kapsamlı tehdit istihbaratı hizmetlerimiz, Güvenlik İşlemleri Merkezi'nizin (SOC) ve/veya BT güvenlik ekibinizin, işletmenizi en gelişmiş tehditlere karşı korumak için yeterli donanıma sahip olmasını sağlar.

- **Tehdit Veri Akışları.** Güvenlik kontrollerinizi geliştirir (SIEM, IDS, güvenlik duvarları vb.) ve çok çeşitli biçimlerde ve gönderme yöntemleriyle paylaşılan güncel siber tehdit verilerimizle adli bilişim becerilerini artırır
- **APT İstihbarat Raporları**, Risk Göstergeleri (IOC) ve YARA kuralları dahil olmak üzere üst düzey siber casusluk faaliyetleri hakkındaki açıklamalara özel ve proaktif erişim imkânı sunar.
- **Finansal Tehdit İstihbarat Raporları**; hedefli saldırılar, belirli altyapılara yönelik saldırılar (ör. ATM/POS) ve siber suçlular tarafından bankalara, ödeme işleme şirketlerine, ATM'lere ve POS sistemlerine saldırmak için geliştirilen veya satılan araçlar dahil olmak üzere özellikle finansal kuruluşları hedef alan tehditlere odaklanır.
- **Özel Hazırlanmış Tehdit Raporları.** Hem deep hem de dark web'i kapsayan özel ve açık kaynaklardan elde edilen kuruluşunuza veya ülkenize göre özel olarak hazırlanmış tehdit istihbaratı.
- **Tehdit Arama.** Kaspersky Lab tarafından tehdit göstergeleri ve birbirleriyle ilişkileri konusunda edinilen tüm bilgilere tam erişim sağlayan web portalı.
- **Bulut Korumalı Alan teknolojisi, şüpheli dosyaları Kaspersky Lab'e göndermenizi, dünya lideri teknolojimizin yardımıyla dosyanın davranışının ayrıntılı bir açıklamasını almanızı ve Kaspersky Threat Lookup çözümüyle sıkı entegrasyona dayalı kapsamlı ve derin incelemeler yürütmenizi sağlar.**
- **Kimlik Avı Takibi.** Sizi veya müşterilerinizi hedef almakta olan kimlik avı saldırıları hakkında gerçek zamanlı bildirimler.
- **Botnet Takibi.** Müşterilerinizi ve itibarınızı tehdit eden ve devam etmekte olan botnet saldırıları hakkında gerçek zamanlı bildirimler.

Güvenlik Değerlendirmesi

Kaspersky Security Assessment Services: Uzman düzeyinde güvenlik analizi ve ileri teknolojili araştırmalar, bilgi sistemlerini gerçek hayat ortamlarında her türlü karmaşıklık düzeyinde test etmek için bir araya getirilir.

Sızma Testleri
Tehdit İstihbaratı temelli saldırgan simülasyonu, olası saldırı vektörlerini gösterir ve saldırganın bakış açısından kurumsal güvenlik durumunuzu genel hatlarıyla görmenizi sağlar.

Uygulama Güvenliği Değerlendirmesi
Derinlemesine bir araştırma ile işletme mantık hataları ve büyük bulut tabanlı çözümlerden gömülü ve mobil uygulamalara kadar her türlü uygulamadaki güvenlik açıkları aranır.

Ödeme Sistemleri Güvenlik Değerlendirmesi
Ödeme sistemlerinin donanım ve yazılım bileşenlerinin kapsamlı analiziyle, olası dolandırıcılık senaryolarının ve finansal işlem manipülasyonlarına neden olan güvenlik açıklarının ortaya çıkartılması hedeflenir.

ICS Güvenlik Değerlendirmesi
Endüstriyel Kontrol Sistemleri'nin ve bileşenlerinin vakaya özel tehdit modellemesi ve güvenlik açığı değerlendirmesi, geçerli saldırı yüzeyiniz ve bir saldırının işletmeniz üzerindeki olası etkileri hakkında bilgiler sağlar.

Taşımacılık Sistemleri Güvenlik Değerlendirmesi
Otomotiv sektöründen Uzay-Havacılık sektörüne kadar modern taşımacılık altyapılarının görev açısından kritik bileşenleriyle ilgili güvenlik sorunlarının belirlenmesine odaklanan özel araştırmalar.

Akıllı Teknolojiler ve Nesnelerin İnterneti Güvenlik Değerlendirmesi
Günümüzün birbirine bağlı cihazlarının ve arka uç altyapılarının ayrıntılı değerlendirmesi; ürün yazılımı, ağ ve uygulama katmanlarındaki güvenlik açıklarını ortaya çıkarır.

Tehdit Avı

Son derece nitelikli ve deneyimli güvenlik uzmanları tarafından gerçekleştirilen proaktif tehdit avı teknikleri, kuruluşun içinde gizlenen gelişmiş tehditlerin ortaya çıkarılmasına yardımcı olur.

- **Kaspersky Managed Protection**
  Kaspersky Lab uzmanları tarafından siber tehdit verilerinizin sürekli olarak izlenmesi ve analiz edilmesi.

- **Hedefli Saldırı Keşfi**
  Mevcut veya geçmişteki risklerin belirtilerinin proaktif olarak bulunmasını sağlayan ve daha önce kaçırılan saldırılara yanıt vermeyi içeren kapsamlı bir hizmet.

Olay Yanıtı

Kaspersky Lab'in Olay Yanıt Hizmetleri, son derece deneyimli siber saldırı tespiti analistleri ve araştırmacıları tarafından yürütülür. Global uzmanlığımız, güvenlik olayınızın çözümü için kullanılabilir.

- **Olay Yanıtı.** Kuruluşunuza yönelik tehdidi tamamen ortadan kaldırmak için tüm olay inceleme döngüsünü kapsar.
- **Adli Bilişim.** Bir siber suç ile ilgili dijital kanıtların analizi ve ilgili tüm bulguları ayrıntılı olarak açıklayan kapsamlı bir raporun hazırlanması.
- **Kötü Amaçlı Yazılım Analizi.** Belirli kötü amaçlı yazılım dosyalarının davranışlarını ve işlevselliğini tam olarak görmenizi sağlar.

Güvenlik Eğitimi

Temel düzeydeki bilgilerden adli bilişim, kötü amaçlı yazılım analizi ve olay yanıtı için kullanılan gelişmiş araç ve tekniklere kadar her düzeyi kapsayan geniş bir kurs portföyü sunuyoruz. Bu sayede kuruluşların bu alanlarda siber güvenlik bilgi havuzunu geliştirmelerine yardımcı oluyoruz.

- **Adli Bilişim:** Kurslar, saldırı zaman dilimlerini ve kaynaklarını geri getirmek için dijital siber suç kanıtlarını arama ve farklı türlerdeki verileri analiz etme konusundaki pratik becerileri geliştirerek ve ilerleterek deneyim boşluğunu kapatmak için tasarlanmıştır.
- **Kötü Amaçlı Yazılım Analizi ve Tersine Mühendislik:** Kurslar, kötü amaçlı yazılımları analiz etmek, IOC'leri (Risk Göstergeleri) toplamak, virüslü makinelerde tespit edilen kötü amaçlı yazılımlar için imza yazmak ve virüslü/şifreli dosyaları ve belgeleri kurtarmak için gerekli bilgileri öğretir.
- **Olay Yanıtı:** Kurslar, şirket içindeki ekibinize olay yanıt sürecinin tüm aşamalarından geçme konusunda rehberlik eder ve ekibinizi başarılı olay düzeltme çalışmaları için gerekli kapsamlı bilgilerle donatır.
- **YARA ile Verimli Tehdit Tespiti:** Katılımcılar, en etkili YARA kurallarını nasıl yazacaklarını, bunları nasıl test edeceklerini ve bu kuralları diğer yöntemler tarafından keşfedilemeyen tehditleri açığa çıkaracak kadar geliştirme yöntemini öğrenir.

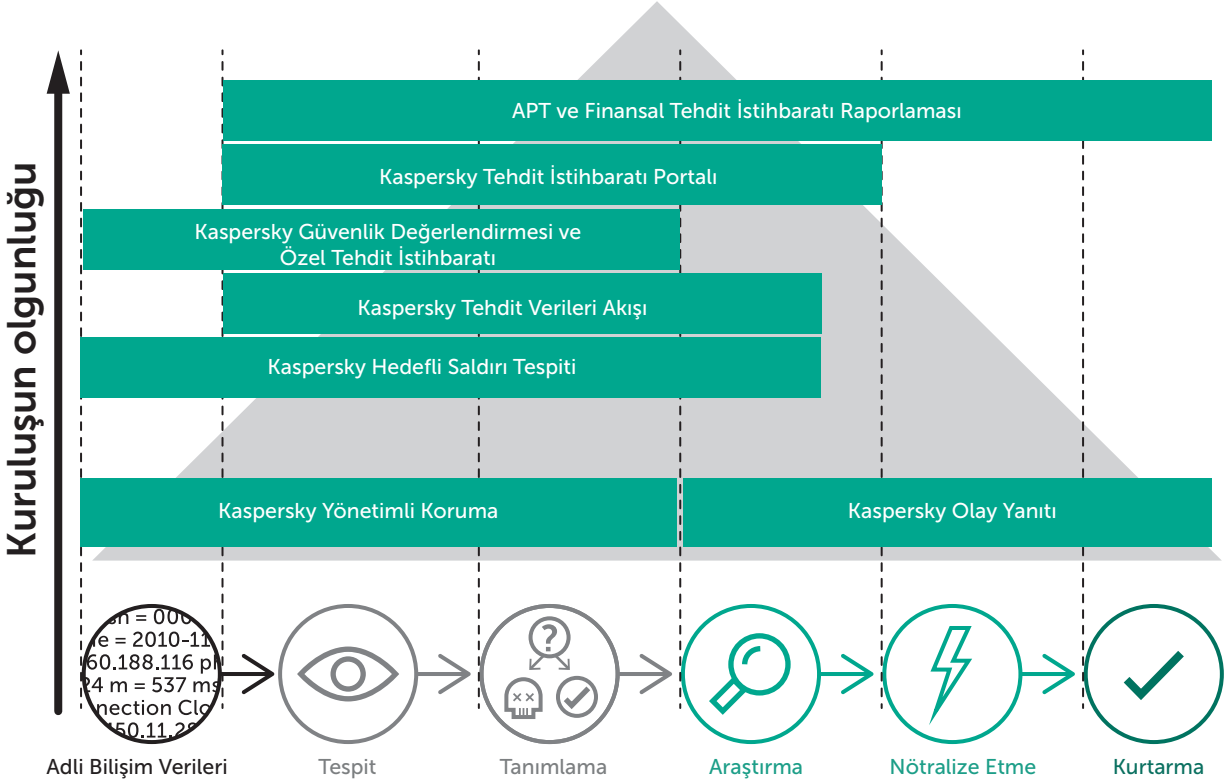
Kaspersky Siber Güvenlik Hizmetleri

Kaspersky Güvenlik Eğitimi Programı

Gelişmiş Dijital Adli Bilişim ve Gelişmiş Kötü Amaçlı Yazılım Analizi

Adli Bilişim ve Kötü Amaçlı Yazılım Analizi

Siber Güvenlik Farkındalığı



Siber Güvenlik Farkındalığı

Oyunlaştırılmış eğitimlerle güvenli bir kurumsal siber ortam oluşturma

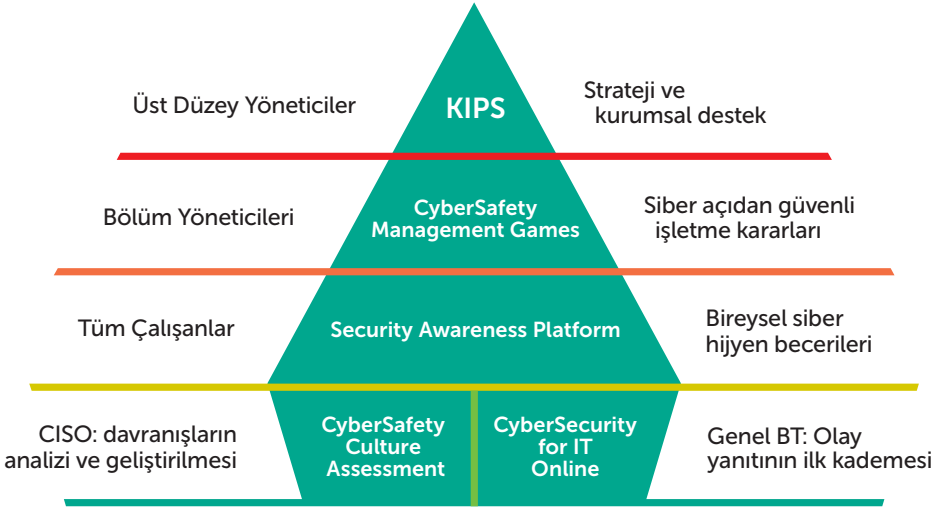
Şirketler, dikkatsiz/bilgisiz çalışanlar nedeniyle gerçekleşen saldırılardan sonra toparlanmak için ortalama 1.155.000 USD civarında harcama yaparken bu rakam KOBİ'ler için 83.000 USD civarındadır. Siber olayların %80'i insan hatalarından kaynaklanır. Yalnızca kimlik avı saldırılarının çalışan başına maliyeti bile yılda 400 USD'dir.

Şirketler, personelleriyle ilgili güvenlik olaylarını düzeltmek için milyonlarını kaybeder. Ancak bu sorunları önlemeyi amaçlayan geleneksel eğitim programlarının etkisi sınırlıdır ve genellikle istenen davranışı ve motivasyonu oluşturma konusunda başarısız olurlar.

Kaspersky Lab, modern eğitim teknikleri kullanan ve kurum yapısındaki her düzeye hitap eden bilgisayar tabanlı eğitim ürünleri ailesini sunar. Eğitim programımız, hem müşterilerimiz hem de Kaspersky Lab iş ortaklarımız için başarısını çoktan kanıtlamıştır:

- Olay sayısında %90'a varan azalma görülmüştür
- Siber risklerle ilgili olası parasal kayıplarda %50-60 azalma görülmüştür
- Bilgilerin günlük hayatta kullanılma ihtimali %93'tür
- Katılımcıların %86'sı aldıkları kursu iş arkadaşlarına önerir.

Kaspersky Güvenlik Farkındalığı Eğitimi Ürünleri



Kazandıran Yaklaşım

- **Sadece bilgileri sıralamaz, davranış oluşturur**: Öğrenme yaklaşımı oyunlaştırma, yaparak öğrenme, grup dinamikleri, saldırı simülasyonları, öğrenme yolları ve becerilerin otomatik olarak pekiştirilmesi gibi yöntemleri içerir. Bu yaklaşım sonucunda güçlü davranış modelleri oluşur ve bunlar kalıcı siber güvenlik gelişmelerine öncülük eder;

- **Programın ciddi ve kullanışlı içeriği**, üst düzey yöneticiler, bölüm yöneticileri ve ortalama çalışanlar dahil olmak üzere kurum içindeki farklı düzeylerin zaman/biçim tercihlerine ve işletme ihtiyaçlarına göre ayarlanmış interaktif alıştırmalar halinde sunulur;

- **Gerçek zamanlı ölçüm, sorunsuz program yönetimi**: Amaca yönelik eğitim yazılımları otomatikleştirilmiş eğitim ödevleri, beceri değerlendirmeleri, tekrarlanan kimlik avı simülasyonları aracılığıyla pekiştirme ve eğitim modüllerine otomatik kayıt olanağı sunar. Kurslar Kaspersky Lab ortakları veya müşterinin kendi Eğitim ve Gelişim ekipleri tarafından yönetilebilir ve sunulabilir (Eğitmeni Eğit programları ve destek, Kaspersky Lab tarafından sağlanır).

Nasıl Çalışır?

- Eğitim, veri sızıntısı, fidye yazılımı, internet tabanlı saldırılar, güvenli sosyal ağ oluşturma ve mobil güvenlik dahil olmak üzere çok çeşitli güvenlik konularını kapsar.

- Devamlı öğrenme metodolojisi, becerilerin sürekli olarak pekiştirilmesini teşvik eder ve kurumda her düzeyden çalışanın motive edilmesini sağlar.

- Farklı kurumsal düzeylere ve işlevlere hitap eden eğitim kursları, en üst düzeyden en alt düzeydeki çalışanlara kadar herkes tarafından paylaşılan ortak bir Siber Güvenlik kültürü oluşturur.

- Eğitimde, programın kurumsal düzeydeki verimliliğinin yanı sıra çalışan becerilerini ve öğrenim gelişimlerini ölçen analiz ve raporlama araçları kullanılır.

- Kaspersky Lab tarafından sağlanan eğitim planları ve en iyi alıştırmalar, programın uygulanmasını kolaylaştırır ve müşterinin BT Güvenliği ekipleri ve Eğitim ve Dokümantasyon ekiplerinin Güvenlik Farkındalığı girişimlerinden en iyi derecede yararlanmasını sağlar.

Endüstriyel Siber Güvenlik

Endüstriyel kontrol sistemleri için özel koruma

Geçmişte endüstriyel üretim bölümleri ve dış dünya arasındaki boşluklar iyi düzeyde koruma sağlarken artık durum değişmiştir. Kritik olmayan birçok endüstriyel ağa isteğe bağlı olarak veya olmayarak internet üzerinden erişilebildiği Endüstri 4.0 çağında bu yöntemler yeterli değildir.

Endüstriyel ortamlardaki kötü amaçlı saldırılar son yıllarda büyük oranda artmıştır. Tedarik zincirlerine yönelik riskler ve ticari faaliyetlerin aksaması son üç yıldır global olarak en çok endişe duyulan risktir. Siber olay riskinden duyulan endişe ise gittikçe artmaktadır. Endüstriyel ve kritik altyapı sistemleri kullanan işletmeler için risk hiç bu kadar fazla olmamıştır.

Endüstriyel güvenlik, işletmenin ve saygınlığın korunmasından çok daha fazla önem taşır. Endüstriyel sistemler siber tehditlere karşı korunurken birçok önemli ekolojik, sosyolojik ve makro ekonomik faktör göz önünde bulundurulmalıdır. Her kritik altyapı, çeşitleri sürekli olarak artan tehditlere karşı en üst koruma düzeyine ihtiyaç duyar.

Aynı zamanda endüstriyel ortamlar, önemli hizmetleri kesintiye uğratabilecek veya durdurabilecek eylemleri (kasıtlı veya kazara) tespit ederek ve engelleyerek endüstriyel süreçlerin kullanılabilirliğini koruyan entegre bir çözüme ihtiyaç duyar.

Çözüm: Kaspersky Industrial Cybersecurity

Kaspersky Industrial CyberSecurity, operasyonel devamlılığı ve endüstriyel süreçlerin uyumunu etkilemeden SCADA sunucuları, HMI panelleri, mühendislik iş istasyonları, PLC'ler, ağ bağlantıları ve kişiler dahil olmak üzere her endüstriyel katmanın güvenliğini sağlamak için tasarlanmış teknoloji ve hizmetlerden oluşan bir portföydür. Çözüm, esnek ve çok yönlü ayarları sayesinde her endüstriyel tesisin benzersiz ihtiyaçlarını ve gereksinimlerini karşılayacak şekilde yapılandırılabilir.

Bu çözüm, birçok farklı endüstriyel kontrol sistemine dayanan kritik altyapıları korumak için geliştirilmiştir. Kaspersky Industrial CyberSecurity'nin esnekliği ve kapsamı sayesinde kurumlar, çözümlerini belirli ICS ortamlarının gereksinimlerine tam olarak uyacak şekilde yapılandırabilir. Güvenlik teknolojilerinin ve hizmetlerinin optimum düzeyde yapılandırılması, Kaspersky Lab tarafından gerçekleştirilen bir tam altyapı denetimi ile sağlanır.

Kaspersky Lab'in endüstriyel sistemleri korumaya yaklaşımı, dünyadaki en karmaşık ve endüstriyel tehditleri açığa çıkarma ve analiz etme konusundaki on yıllık uzmanlığına dayanır. Sistemlerdeki güvenlik açıklarının özellikleri konusundaki derin bilgimiz ve anlayışımız; Interpol, Endüstriyel İnternet Konsorsiyumu, çeşitli ICS tedarikçileri ve düzenleyicileri gibi dünyada lider emniyet teşkilatları, devletler ve endüstriyel ajanslar ile yakın işbirliğimizle birleşerek, bizi endüstriyel siber güvenliğin gereksinimlerini karşılama konusunda liderliğe taşımıştır.
Bu son derece özel çözüm:

- Endüstriyel ortamlara bütünsel siber güvenlik yaklaşımı sunar
- Siber güvenlik değerlendirmesinden olay yanıtına kadar güvenlik hizmetlerinin tamamını kapsar
- Endüstriyel sistemler için özel olarak geliştirilen benzersiz güvenlik teknolojileri sağlar

- Arıza süresini ve endüstriyel süreç gecikmelerini en aza indirir.

Kaspersky Industrial Cybersecurity

Teknolojiler

Anormallik Tespiti (DPI)

Diğer sistemlerle entegrasyon

Kötü Amaçlı Yazılımlara Karşı Koruma

Bütünlük Kontrolü

Merkezi Yönetim

Olay İncelemesi

İzinsiz Giriş Tespit Sistemi

Hizmetler

Eğitim ve İstihbarat

- Siber güvenlik eğitimi
- Farkındalık programları
- Tehdit İstihbaratı

Uzman Hizmetleri

- Siber güvenlik değerlendirmesi
- Çözüm entegrasyonu
- Bakım
- Olay yanıtı

Dolandırıcılık Önleme

Sorunsuz bir kullanıcı deneyimi ve dolandırıcılığın gerçek zamanlı ve proaktif olarak önlenmesi için gelişmiş çözüm

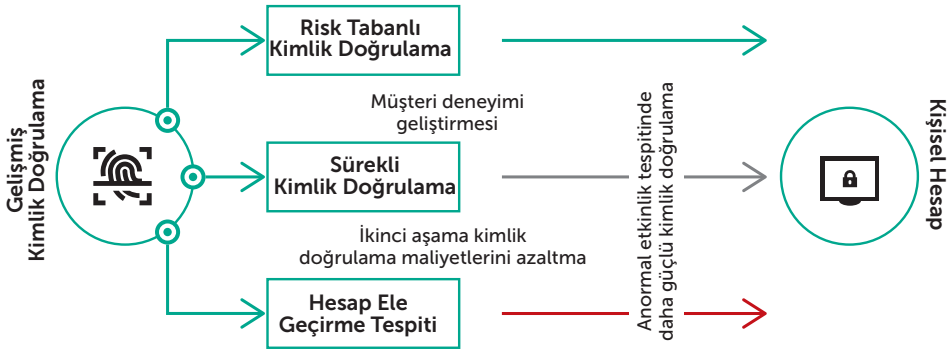
Dijital hayata geçiş yalnızca bir eğilim değil bir gerekliliktir. Günümüzde birçok müşteri, günlük ihtiyaçlarında çevrimiçi ve mobil kanalları kullandığı için işletmeler maksimum işlevselliğe sahip yüksek seviyeli hizmetler sunmalıdır. Aynı anda, çevrimiçi güvenliğin sorunsuz müşteri deneyimiyle dengelenmesi gereklidir. Kaspersky Fraud Prevention ürünü de tam olarak bu ihtiyaçlarınızı karşılar. Bu çözüm, güvenlik konularının ve çevrimiçi kullanılabilirlik sorunlarının ek stresi olmadan çevrimiçi ve mobil kanallarınızı büyütmenize ve geliştirmenize yardımcı olur.

Kaspersky Fraud Prevention davranış analizi ve biyometrik verilerin yanı sıra Kaspersky Fraud Prevention Cloud çözümünde bir araya getirilen cihaz ve ortam analizi dahil olmak üzere çok çeşitli gelişmiş teknolojilere dayalıdır. Makine öğrenimi, web ve mobil kanallardaki karmaşık dolandırıcılık planlarının proaktif tespiti için uygulanır. Bu sayede, dolandırıcılık izleme sistemleriniz daha akıllı ve uyarlanabilir aşamalı doğrulama kullanımının yanı sıra daha doğru ve daha proaktif karar alma süreci için ek bir bağlamdan yararlanabilir.

Çözüm, ilgili iş sorunlarını çözmek için ayrı olarak veya birlikte kullanılabilen iki tam özellikli üründen oluşur. Bu ürünler, kullanıcı deneyimini geliştirmenin yanı sıra güvenlik düzeylerini ve korumayı önemli ölçüde artırır.

Gelişmiş Kimlik Doğrulama özelliği, kullanıcı deneyimini geliştirmek, iki aşamalı kimlik doğrulamasının maliyetini azaltmak ve sürekli olarak şüpheli etkinlikleri tespit etmek için geliştirilmiştir. Bunların yanı sıra işinizin büyümesine ve daha üst düzey güvenlik elde etmenize yardımcı olur.

Gelişmiş Kimlik Doğrulama özelliği, ilk oturum açma anından itibaren, olayları sürekli olarak analiz eder. Böylece risk seviyelerinin hesaplanmasını ve uygun önerilerin yapılmasını sağlar.



Otomatik Dolandırıcılık Analizleri, global tehdit istihbaratı ve insan uzmanlığı ile ileri teknolojileri mükemmel bir şekilde dengeleyerek bir araya getirir. Bu özellik, olası dolandırıcılık faaliyetlerini önceden belirler ve kuruluşu uyarır. Ayrıca doğru kararların zamanında verilebilmesi için önemli verileri analiz eder ve karmaşık dolandırıcılık vakalarının açığa çıkmasını sağlar.

Kullanıcı oturumları sırasında kullanıcıları, cihazlarını ve ortamlarını etkileyen olaylar, dolandırıcılık yönetim sistemlerini zamanında ve doğru karar verilebilmesi için gerekli verilerle besler. Kaspersky Fraud Prevention Cloud çözümü içinde oluşturulan kullanıma hazır olaylar, gerçek dolandırıcılık vakalarına ilişkin bilgiler sağlayarak sorunun köküne ulaşır.

Kaspersky Fraud Prevention, gelişmiş teknolojiler ve uzmanlığın yanı sıra aşağıdaki özellikleri sunar:

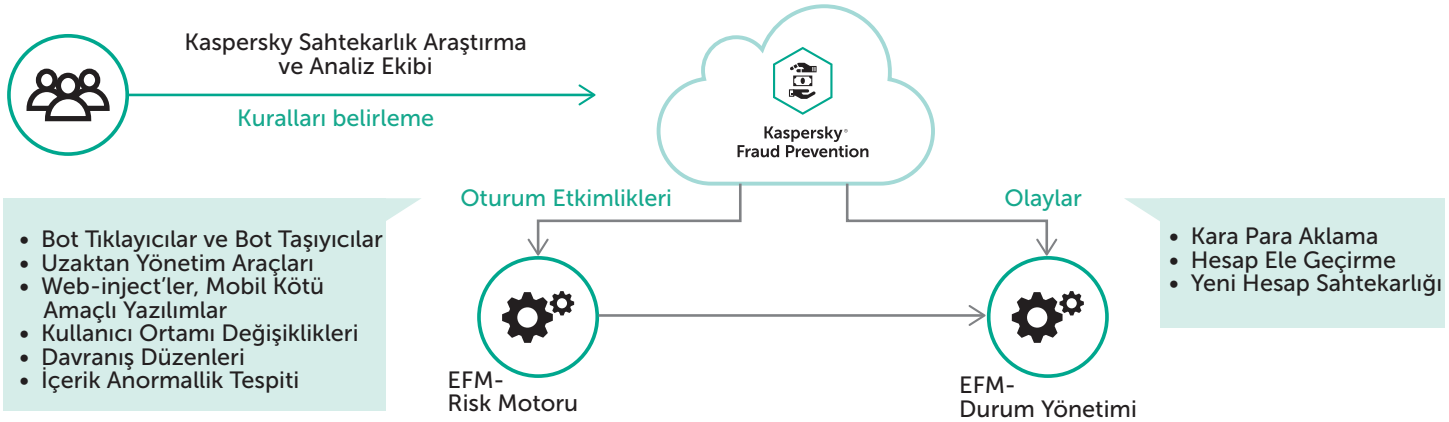
Maintenance Service Agreement: tüm güvenlik ihtiyaçlarınız için üstün destek ve sertifikalı mühendislerden oluşan yerel ekiplerimizden birinci sınıf destekle işletmenizi koruma hizmeti.

Uygulama hizmetleri: ürün serimizi mevcut güvenlik ve dolandırıcılık önleme çözümleriyle birbirine bağlayan özel uygulama mühendisleri.

Dolandırıcılık Önleme danışmanlığı: uzman becerilerine ve farklı endüstrilerde uzmanlığa sahip uzmanlardan oluşan bir ekipten doğru dolandırıcılık önleme stratejisinin oluşturulması için işletme danışmanlığı.

Kaspersky Fraud Prevention çözümünün en önemli avantajları:

- Ek güvenlik endişeleri ve kullanılabilirlik sorunları olmadan çevrimiçi ve mobil kanalların büyümesi
- Dolandırıcılık önleme maliyetlerinin kontrolü ve dolandırıcılık kayıplarının bitmesi
- Herhangi bir işlem gerçekleşmeden önce gelişmiş dolandırıcılığın gerçek zamanlı olarak tespiti
- Kurumsal Dolandırıcılık İzleme çözümlerinin ek verilerle zenginleştirilmesi



Nesnelerin İnterneti Güvenliği

Müşterilerinizin gizliliğini güvence altına alarak size olan güvenlerini artırma

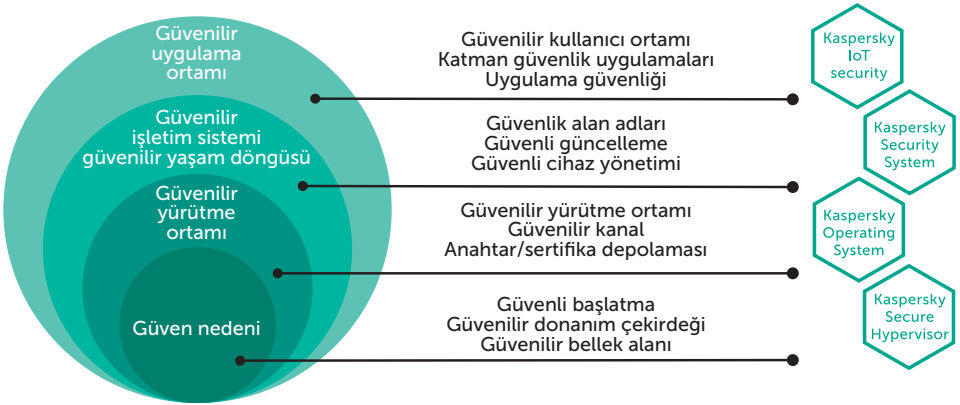
Nesnelerin İnterneti (IoT) dünyayı değiştiren yeni bir akımdır. Bu teknoloji, dünyamızı daha güvenli hale getirebilir, sağlığımızı iyileştirebilir, zaman ve paradan tasarruf etmemize yardımcı olabilir, atıkları azaltabilir ve üretim kontrolüne ve genel olarak hayatımıza yeni bir boyut katabilir.

Siber güvenlik, geleneksel olarak kişisel verilerin güvenliği ile ilişkilendirilmiştir. Ancak Nesnelerin İnterneti çağında bu durum gizliliğin güvenliği şeklinde dönüşmüştür. Akıllı ev kameraları, multimedya araçları veya bebek monitörleri ile uzaktan izleme gibi kullanıcı gizliliği ihlalleri; ev cihazlarının çalışmasına müdahale etme; günlük hizmetlerin beklenmedik bir şekilde kapanması ve arızalanması... Bunların tamamı, son kullanıcı için kabul edilemez durumlardır.

Ayrıca, Nesnelerin İnterneti teknolojisi cihaz üreticileri (donanım bileşenleri ve yazılımları dahil olmak üzere), telekom hizmeti sağlayıcıları ve sistem entegrasyonu pazarı için çok önemli fırsatlar sağlar. Son kullanıcıların Nesnelerin İnterneti çözümlerine güvenmemesi, bu potansiyel fırsatların kullanılmasını engelleyebilir veya önemli ölçüde yavaşlatabilir. Bu nedenle, Nesnelerin İnterneti çözümlerinin uçtan uca güvenliği bu teknolojiden faydalanan herkes için en önemli önceliktir.

Mevcut duruma göre müşterilere sunulan Nesnelerin İnterneti teknolojisine sahip cihazlar ve telekom ekipmanları, kolaylıkla siber güvenlik ihlalleri içerebilir. Donanım, ürün yazılımının bütünlüğünü denetleyemeyebilir ve cihazlar, bazen yönetici parolaları dahil olmak üzere önceden belirlenmiş parolalarla birlikte gelir. Zayıf ağ güvenlik ayarları veya eski ve güvenlik açığı bulunan yazılımların kullanımı da sorunlara neden olabilir. Ayrıca yazılım güncelleme süreçlerinin eksikliği, güvenlik açığı bulunan cihazların güncelleştirilmeden yıllarca kullanılabilmeleri anlamına gelir. Bu tür cihazların, başarılı bir saldırıya uğraması an meselesidir.

Cihaz düzeyinde güven garantisi



Güven zinciri ilkesi, Nesnelerin İnterneti cihazının güvenli bir şekilde çalışması garantisinin temelini oluşturur. Buna uç cihazları ve altyapı unsurları (ağ geçitleri) dahildir. Bu ilke, donanım düzeyinde güvenilir kök kullanımı ile başlar.

Bu teknoloji işletim sistemi görüntüsünün bütünlüğünü kontrol etme, şifreleme uygulama ve anahtar bilgiler için donanım destekli güvenli depolama mekanizmaları dahil olmak üzere işletim sisteminin güvenilir bir şekilde ön yüklemesini gerçekleştirir. Güvenilir önyükleme, ağ geçitleri gibi temel IoT altyapı cihazları için çok önemlidir. Bu işlem, işletim sisteminin ekipman belirli bütünlük kontrollerini başarıyla geçtikten sonra önceden tanımlanmış ortamdan yüklendiğini gösterir.

Güven zincirindeki bir sonraki önemli unsur, güvenilir olarak kabul edilmeyen yazılımların düzgün bir şekilde yürütülmesini sağlayabilen güvenli bir işletim sistemidir. Bilgisayar teknolojisindeki son gelişmeler, işletim sistemi düzeyinde güvenilir kabul edilemeyecek uygulamaların davranışlarını kısıtlayan bir ortamın uygulanmasını mümkün kılar.

IoT kavramı, çok çeşitli cihazları, araçları, teknolojileri, yazılımları ve iletişim protokollerini kapsar. Ancak bu heterojen ortam, IoT teknolojisine bağlı olan yaşamımızın her yönünü ciddi bir şekilde etkileyebilecek birçok güvenlik riski oluşturur. Kaspersky Lab, ilgili riskleri en aza indiren bir dizi ürün geliştirmiştir:

- **Gömülü Sistem Güvenliği**
  Sürekli bakım veya internet bağlantısı gerektirmeyen sınırlı bellek kapasitesine sahip alt uç sistemlerin güvenliğini optimize etmek için geliştirilmiş bir çözümle Microsoft Windows tabanlı gömülü cihazlarınızı ve bilgisayarınızı koruyun.

- **KasperskyOS**
  KasperskyOS işletim sistemi, güçlü bir ayırma ve ilke uygulama yoluyla çok çeşitli ve karmaşık gömülü sistemleri zararlı kodların, virüslerin ve hacker saldırılarının sonuçlarından korumak için tasarlanmıştır. KasperskyOS, bir güvenlik açığının veya kötü bir kodun büyük bir sorun yaratmadığı bir ortam oluşturur. Kaspersky Security System koruma bileşeni, tüm sistemdeki etkileşimleri kontrol eder ve bu sayede güvenlik açıklarından yararlanılmasını engeller.

- **Kaspersky Security System**
  Kaspersky Security System, eş zamanlı olarak farklı güvenlik ilkeleri türleri (rol tabanlı ve zorunlu erişim kontrolü, geçici mantık, kontrol akışı, tip uygulama vb.) ile çalışabilen ve istemcinin gereksinimlerini karşılayabilecek şekilde özelleştirilebilen bir güvenlik ilkesi karar hesaplama motorudur. İlkeler ne kadar kesin olursa tüm sistem için o kadar çok kontrol ve güvenlik sağlanır.

  Kaspersky Security System, KasperskyOS (en güvenli yapılandırma) ve Linux tabanlı bir çözümle (güvenli olmayan bir sistemde güvenli eylemler) birlikte kullanılabilir.

- **Kaspersky Secure Hypervisor**
  Kaspersky Secure Hypervisor (KSH), KasperskyOS mikro çekirdeği üzerinde çalışır. KSH ile güvenilir olmama riski olan sanallaştırılmış misafir işletim sistemleri, fiziksel olarak aynı donanım platformunda çalıştırılsa bile birbirlerinden ayrılabilir ve bunlar arasındaki bütün iletişimler kontrol edilebilir ve güvenilir hale getirilebilir. KSH'nin ek bir avantajı, donanım bakım maliyetlerini azaltma özelliğidir.

- **Kaspersky Transportation Security Service**
  KasperskyOS teknolojisine dayalı entegre" Emniyet İçin Güvenlik" yaklaşımı. Elektronik Kontrol Üniteleri (ECU) için tek bir güvenli ağ geçidinin yanı sıra günümüzün ve geleceğin bağlı taşıtlarının ihtiyaçlarını karşılayan geniş bir güvenlik değerlendirme hizmetleri yelpazesi.

- **Güvenli İletişim Birimi**
  Güvenli İletişim Birimi (SCU), birden çok alt ağa ve/veya araç ağı içindeki alt ağlar için ağ geçidi kontrolörlerine bağlı iletişim ağ geçidi kontrol ünitesidir. Dolayısıyla SCU, harici iletişimlere yönelik tek ağ geçididir. Dahili cihazlar ise SCU hizmetlerini kullanmadan bir etki alanı içinde veya etki alanları arasında iletişim kurabilir.
  SCU, KasperskyOS tarafından desteklenir ve Kaspersky Security System tarafından güçlendirilir. Kaspersky OS, SCU içindeki tüm etkileşimleri en düşük seviyede kontrol eder ve Kaspersky Security System çözümünün ilke kararlarını uygular. Yalnızca açıkça izin verilen etkileşimler mümkündür.

Gömülü Sistem Güvenliği

Gömülü sistemler için özel olarak tasarlanan ve tüm özellikleri bir arada içeren güvenlik teknolojisi

Gerçek para ve kredi kartı kimlik bilgileriyle çalışan Gömülü sistemler, siber suçluların tercih ettiği hedeflerdir. Bu nedenle en yüksek düzeyde odaklı ve akıllı koruma gerektirir. Artık, Cihaz Kontrolü ve Baştan Yasaklı (Default Deny) gibi başarısını kanıtlamış teknolojilerin ilk savunma hattı olarak kullanılmasının zamanı gelmiştir.

Günümüzde bilet makineleri, ATM'ler, kiosklar, Satış Noktası (POS) sistemleri ve medikal ekipmanlar gibi birçok alanda gömülü sistemler kullanılmaktadır.

Gömülü sistemler genellikle coğrafi olarak farklı bölgelerde bulunduğu, yönetimi zor olduğu ve nadiren güncellendiği için güvenlik açısından özel bir önem taşır. Ayrıca nakit para ve müşteri kimlik bilgileri ile çalışan sistemler hatalardan etkilenmemeli ve dayanıklı olmalıdır. Gömülü sistemlerin yalnızca tehditlere karşı korunuyor olması yeterli değildir. Aynı zamanda siber suçlular ve içerideki saldırganlar tarafından kurumsal ağa giriş noktası olarak kullanılamaz olmalıdır.

Gömülü cihazlar için standart güvenlik düzenlemeleri, genellikle yalnızca virüsten koruma tabanlı güvenlik ve sistem güçlendirmesini kapsar, bu da yeterli değildir. Tamamen virüsten koruma tabanlı bir yaklaşım, mevcut gömülü sistem tehditleri karşısında yeterince etkili değildir. yakın zamanda gerçekleştirilen saldırılarda da bu durum fazlasıyla görülmüştür.

Cihaz Kontrolü işleviyle güçlendirilen Uygulamalar, Sürücüler ve Kitaplıklar için Baştan Yasaklı özelliği, hala kullanılmakta olan eski kritik sistemlerin güvenliğini sağlayabilecek tek yaklaşımdır.

Çözüm: Kaspersky Embedded Systems Security

Kaspersky Lab, gömülü sistemler kullanan kuruluşlar için özel olarak tasarlanmış bir çözüm geliştirdi. Bu çözüm, gömülü sistemlerin benzersiz işlevlerini, işletim sistemini, kanal ve donanım gerekliliklerini göz önüne almanın yanı sıra bu sistemlerin karşılaştığı özel tehdit ortamına odaklanmaktadır. Ayrıca Windows XP ailesindeki tüm ürünleri tam olarak destekler.

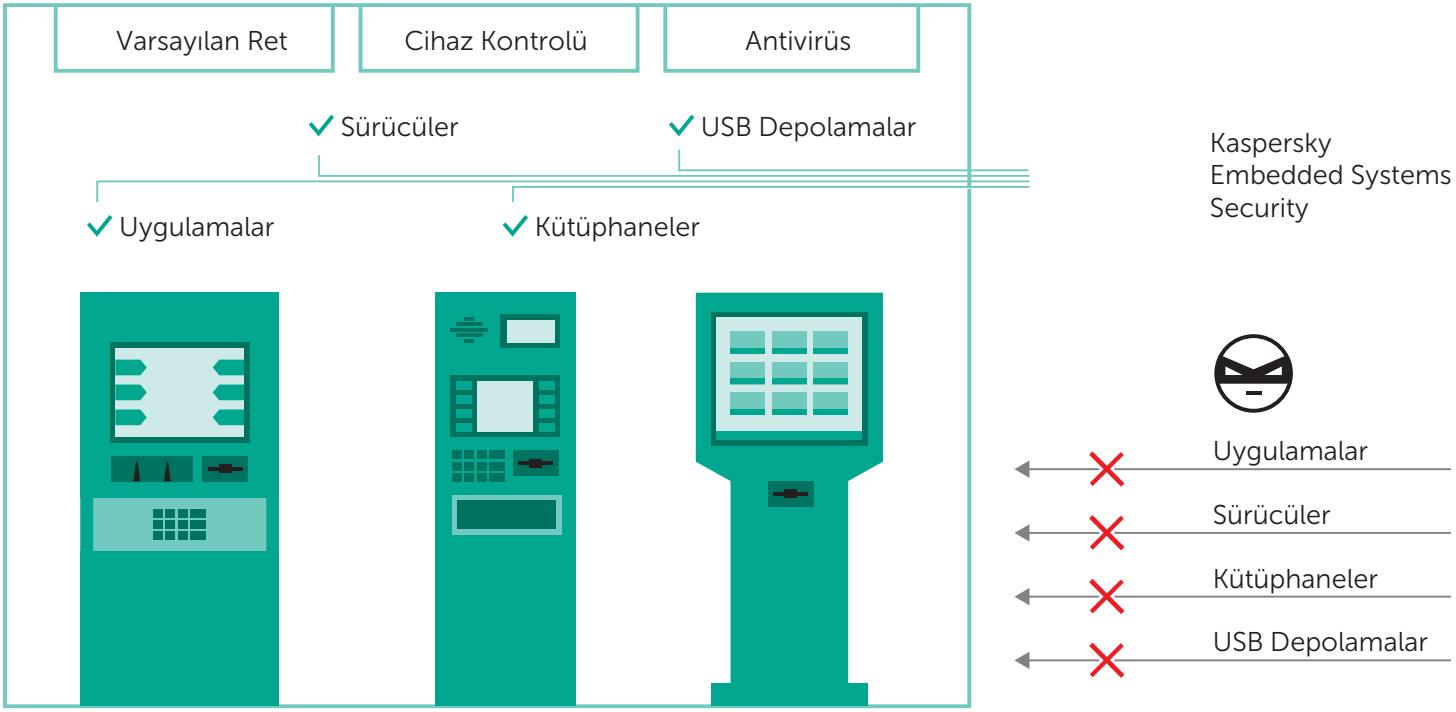
Kaspersky Embedded Systems Security, düşük bütçeli donanım sistemleri için sistem gerekliliklerinin Windows XP'de 256 Mb RAM ve 50 mb sabit disk sürücü alanından başladığı "Yalnızca Baştan Yasaklı" çalışma modunu sunar.

Ayrıca opsiyonel bir Antivirüs modülünün sağladığı istek üzerine tarama modu bulunur. Buna ek olarak koruma duvarı yönetimi özelliği vardır. Bu modül, gerektiği takdirde yama yönetimi olanaklarıyla Kaspersky Security Network tarafından desteklenir.

Yani bu tek çözüm şu üç temel ihtiyacı karşılar:

- "Yönetimi zor" sistemler için etkili güvenlik
- PCI DSS gereklilikleri 5.1, 5.1.1, 5.2, 5.3 ve 6.2 ile uyum
- Eski sistemler ve donanım değişimi için esnek zaman çizelgesi

Bu çözüm, Gömülü işletim sistemlerine dayalı sistemlerdeki siber güvenlik risklerini azaltmak için özel olarak tasarlanmıştır. Ürün, bu sistemlerin mimarisine özgü saldırı alanlarını korurken aynı zamanda ilgili donanıma ve verimlilik etkenlerine uyum sağlar. Tek bir sezgisel konsol, uç noktalarınızın, kritik sistemlerinizin ve tüm BT altyapınızın etkili ve çok katmanlı güvenliğini yönetmek için ihtiyacınız olan kontrolü ve görünürlüğü sunar



Üst Düzey Destek ve Profesyonel Hizmetler

Şirketlerin Kaspersky Lab ürünlerinden en üst düzeyde yararlanmasını sağlayan hizmet seçenekleri

Üst Düzey Destek

Bir güvenlik olayı meydana geldiğinde, nedeni belirlemek ve ortadan kaldırmak için geçen süre önemlidir. Bir sorunu hızlı bir şekilde tespit etmek ve çözmek, işletmelere yüksek miktarda tasarruf sağlayabilir. Üst düzey destek planlarımız tam olarak bu hedefe ulaşmaya odaklanmıştır. Uzmanlarımıza 7/24 erişim, garantili yanıt süreleriyle uygun ve bilinçli sorun önceliklendirme ve özel düzeltme ekleri... Sorununuzun en kısa sürede çözülmesini sağlamak için gerekli her şeyi sunarız.

Kaspersky Lab, BT güvenlik sorunlarınızı her zaman yüksek öncelikli olarak değerlendiren üstün destek programları seçenekleri sunar. Bu programlar, işletmenizin sorunsuz bir şekilde çalışmaya devam etmesini sağlamaya ve yeniden tam performansla güvenli bir şekilde çalışmanız için en hızlı ve etkili yolu bulmak amacıyla tüm uzmanlarımızın tam kadro çalışmasına odaklanır.

Üst düzey destek planlarımız şunları kapsar:

- Özel Teknik Hesap Yöneticisi
- Özel telefon hattı üzerinden 7/24 destek
- Olay yanıtı SLA'ları
- Yeni tehditler için proaktif uyarılar

Profesyonel Hizmetler

Siber güvenlik büyük bir yatırımdır. Şirketinizin benzersiz gereksinimlerini karşılamak için yatırımınızı tam olarak nasıl optimize edebileceğinizi anlayan uzmanlarla görüşerek onlardan en iyi şekilde yararlanın.

En iyi uygulamalarımıza ve metodolojilerimize uygun olarak çalışan güvenlik uzmanlarımız, Kaspersky Lab ürünlerini şirketinizin BT altyapısında kullanma, yapılandırma ve yükseltme işlemlerine her açıdan yardımcı olmaya hazırdır.

Kaspersky Lab Professional Services, değişiklik veya geçiş sürecinizin sorunsuz ve etkili olmasını ve çalışmalarınızda gereksiz kesintilere yol açmamasını sağlar.

Kaspersky Professional Services şunları içerir:

- Uygulama ve Yükseltme
- Yapılandırma
- Sağlık Kontrolü
- Ürün Eğitimi

Kaspersky Lab Hakkında

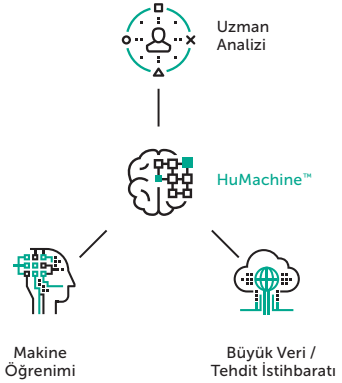
Kaspersky Lab, dünyanın en hızlı büyüyen siber güvenlik şirketlerinden birisi olmasının yanı sıra en büyük özel siber güvenlik şirketidir.

Bağımsız bir kuruluş olmamız daha çevik olmamızı, daha farklı düşünmemizi ve daha hızlı hareket etmemizi sağlar. Sürekli olarak yenilikler yapar ve etkili, kullanılabilir ve erişilebilir koruma sağlarız. Şirketimizin, 400 milyon kullanıcımızın ve 270.000 kurumsal müşterimizin olası tehditlerden bir adım önde olmasını sağlayan dünya lideri güvenlik çözümlerini geliştirmekten gurur duyarız.

İnsanlara ve gelişmiş teknolojiye bağlı olmamız, rakiplerimizin önüne geçmemizi sağlar.

Kaspersky Lab'in benzersiz uzmanlığı ve Kurumsal Güvenlik Çözümlerimiz hakkında daha fazla bilgi edinmek için kaspersky.com/enterprise adresini ziyaret edin.

Notlar



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com.tr/**

#truecybersecurity
#HuMachine

www.kaspersky.com