kaspersky

Büyük Ölçekli İşletmeler için Kaspersky Güvenliği

Kaspersky Kurumsal Portföyü Hakkında

Doğru ürünü veya hizmeti seçerek kuruluşunuz için güvenliğin temelini atmak ilk adımdır. Ancak uzun vadeli başarının anahtarı ileriye dönük kurumsal bir siber güvenlik stratejisi geliştirebilmektir.

Kaspersky'nin Kurumsal Portföyü, günümüz işletmelerinin güvenlik taleplerini yansıtır ve kademeli yaklaşımıyla farklı büyüklük seviyelerindeki kuruluşların ihtiyaçlarını karşılar. Bu yaklaşım en karmaşık saldırıları bile tespit etmek, tüm olaylara hızlı ve gereğine uygun bir şekilde yanıt vermek ve gelecekteki tehditleri önlemek için tüm siber tehdit türleriyle mücadele eden farklı koruma katmanlarını bir araya getirir.

Uzun vadeli planlamada uç nokta güvenliğinin rolü

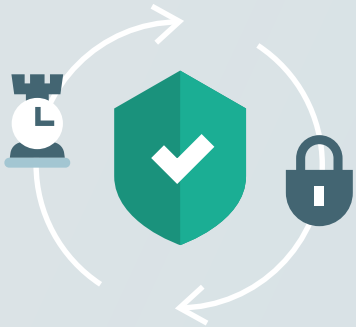
Geleneksel güvenlik evrimi süreci

Karar verme:

- Pazar trendleri
- Yalıtılmış güvenlik çözümü
- "Sorun çıktığında müdahale etme" yaklaşımı
- Uyumluluk odaklı

Geleneksel ürünleri kullanma:

- EPP (Uç Nokta Koruma Platformu)
- Güvenlik Duvarları/NGFW (Yeni Nesil Güvenlik Duvarı)
- Web Uygulaması Güvenlik Duvarları
- Veri Kaybını Önleme
- SIEM (Bilgi Güvenliği Tehdit ve Olay Yönetimi)

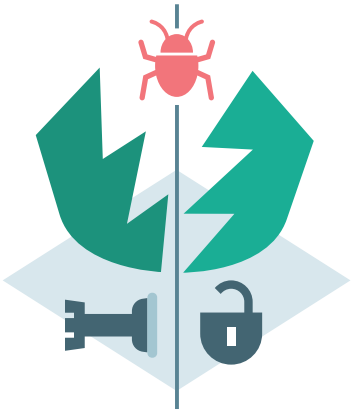


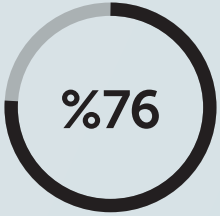
Nitelikler

- Kısa vadeli güvenlik planlaması
- Teknolojilere ve özelliklere bağımlılık
- Çevre tabanlı ağ savunması

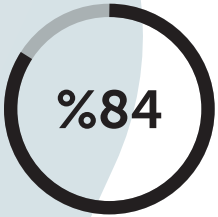
Geleneksel yaklaşımlar neden başarısız oluyor?

- Tehditlerin ve tehdit ortamının daha karmaşık hale gelmesi
- Siber güvenlik teknolojilerinin karmaşıklığı
- Uzun vadeli bir siber güvenlik stratejisine yönelik kurumsal gereklilikler





Uç noktalar tarafından oluşturulan alarmların oranı



Birden daha fazla uç noktayı içeren uç nokta sızıntılarının oranı

Uç noktalar, kuruluşların altyapılarına girmek için en yaygın olarak kullanılan giriş noktalarıdır, siber suçluların ana hedefleridir ve karmaşık olayların etkili bir şekilde araştırılması için gerekli verilerin ana kaynaklarıdır.

İşletmeler için gelişmiş siber güvenlik planlamasına yönelik 3 adım

2

Gelişmiş tehditler ve hedefli saldırılar — Uç Noktalar — Services

Gelişmiş savunma

Gelişmiş tespit ve önleyici koruma çözümleri tarafından kaçırılan karmaşık tehditlere hızla yanıt verme odaklı yaklaşım.

Kaspersky Endpoint Detection and Response

Kaspersky Targeted Attack Discovery Hizmeti

1

Daha Kapsamlı Tehdit Ortamı — Uç Noktalar — Ağ

Güvenlik Temelleri

Sistemleri güçlendirin ve mümkün olan maksimum sayıda tehdidi otomatik olarak engelleyin.

Kaspersky Endpoint Güvenlik for Business

Kaspersky Embedded Systems Security

Kaspersky Secure for Mail Server

Kaspersky Security for Internet Gateway

3

Hedefli saldırılar ve siber silahlar

Entegre siber güvenlik yaklaşımı

APT düzeyinde saldırılara hazırlık. Üst düzey uzmanlık, gelişmiş tehdit istihbaratı özellikleri ve sürekli tehdit avı.

Kaspersky Threat Management & Defense

Ağ

Kaspersky Anti Targeted Attack

Intelligence

Kaspersky Threat Intelligence

Çalışanlar

Kaspersky Cybersecurity Training

Gizlilik

Kaspersky Private Secutity Network

Cloud

Kaspersky Hybrid Cloud Security

Support

Kaspersky Premium Support and Professional Services

Veriler

Kaspersky Security for Storage

Çalışanlar

Kaspersky Security Awareness

Bu yaklaşımın 4 kurumsal avantajı

İşletmenin kendine özgü ihtiyaçlarını ve tehdit ortamındaki trendleri göz önünde bulundurarak uzun vadeli bir siber güvenlik stratejisinin geliştirilmesi için temel oluşturur.

Güvenlik teknolojisi yatırımlarının en uygun şekilde yapılmasını sağlar ve toplam sahip olma maliyetini (TCO) azaltır.

Siber suçlardan kaynaklanan finansal ve operasyonel zararlarda azalma.

ROI

Sorunsuz iş akışı otomasyonu ve iş süreçlerinde aksamanın ortadan kaldırılmasıyla daha yüksek yatırım getirisi

1 Güvenlik Temelleri

Otomatik önleyici teknolojiler ve güvenlik farkındalığı

Maksimum sayıda tehdidi engelleme

Özel bir güvenlik ekibi olmayan veya sınırlı siber güvenlik uzmanlığına sahip küçük şirketler için idealdir

- Alınıp satılabilen tehditlerden kaynaklanan yüksek sayıda olayın çok vektörlü ve otomatik olarak önlenmesi
- Orta-büyük ölçekli şirketlerin karmaşık tehditlere karşı entegre bir savunma stratejisi oluşturmasında temel adım

Uç Noktalar

- **Kaspersky Endpoint Security for Business**
- **Kaspersky Embedded Systems Security**

Cloud

- **Kaspersky Hybrid Cloud Security**

Ağ

- **Posta Ağ Geçidi için Kaspersky Koruması**
- **İnternet Ağ Geçidi için Kaspersky Güvenlik**

Çalışanlar

- **Kaspersky Security Awareness**

Veriler

- **Kaspersky Security for Storage**

Support

- **Kaspersky Premium Support**
- **Kaspersky Professional Services**

Kaspersky Endpoint Security for Business

Şirketlere yönelik siber saldırıların büyük bir kısmı uç noktalarda başlar. Sınırlı önleme ve otomasyon özellikleri, uzmanların güvenlik olaylarından başını kaldıramamasına neden olur. Her uç nokta, işlerin aksamasının temel nedeni olma potansiyeline sahiptir; Kaspersky Endpoint Security for Business, tehditleri önler ve uyarlanabilir güvenliği genişletilmiş kontrol araçlarıyla birleştirerek uç noktaları güçlendirir. Uç nokta kurumsal çevrenin dışında olsa bile tehditler, verilere zarar vermeden veya kullanıcı verimliliğini düşürmeden engellenir.

Şunlar için idealdir:

BT beklentileri artan ve çeşitlenen kuruluşlar

Güvenlik ihlallerine yol açan kullanıcı hatalarının yaşanmasına fırsat verecek durumları ve bu hataların sıklık derecesini azaltmak isteyen kuruluşlar

Kurumsal avantajlar

İşlerin aksamasını ve insan hatalarını önler

Dijital dönüşümü destekler ve mobil iş gücünün güvenliğini sağlar

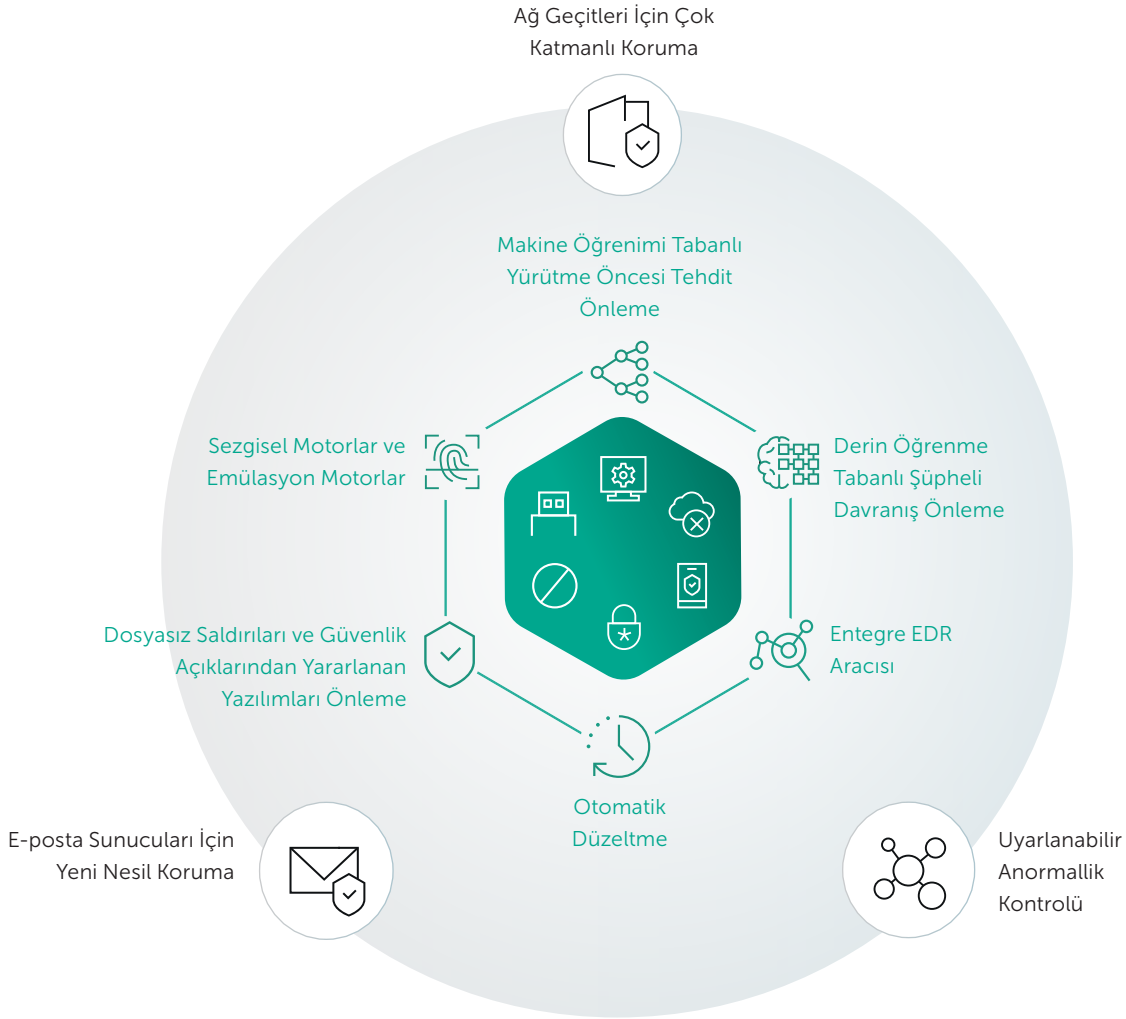
Denetimlere daha hazırlıklı olunmasını sağlar: Güvenlik açıklarını, "yapılandırma kaymalarını" ve şifrelenmemiş cihazları tespit eder ve onarır

Saldırı yüzeyini küçülterek ve yönetilecek olay sayısını azaltarak yatırım getirisini en üst düzeye çıkarır:

Entegre konsolu ve birleşik aracısı sayesinde tüm uç noktaların kontrol edilmesini sağlar

Kullanım senaryoları

- Uyarlanabilir güçlendirme uygulayarak; uç noktaları, e-posta ve dosya sunucularını ve internet ağ geçitlerini koruyarak saldırıya maruz kalma ihtimalini azaltır
- Uç noktaların düzenleyici gerekliliklere uygun olmasını sağlar
- Tespit, yanıt ve yazılım dağıtımı görevlerini otomatik hale getirerek güvenlik uzmanlarının başka görevlere zaman ayırmasını sağlar
- Diğer güvenlik teknolojilerinin entegrasyonunu ve kullanılmaya başlanmasını kolaylaştırır


Ağ Geçitleri İçin Çok Katmanlı Koruma
Makine Öğrenimi Tabanlı Yürütme Öncesi Tehdit Önleme
Sezgisel Motorlar ve Emülasyon Motorlar
Derin Öğrenme Tabanlı Şüpheli Davranış Önleme
Dosyasız Saldırıları ve Güvenlik Açıklarından Yararlanan Yazılımları Önleme
Entegre EDR Aracısı
Otomatik Düzeltme
E-posta Sunucuları İçin Yeni Nesil Koruma
Uyarlanabilir Anormallik Kontrolü

Kaspersky Hybrid Cloud Security

Hibrit Bulut Güvenliği, kuruluşların iş yüklerini sanallaştırması veya buluta taşıması sırasında dijital dönüşümü kolaylaştıran ve güvenliği sağlayan bir çözümdür. Patentli Hafif Aracı teknolojisi, güvenlik işlevinin merkezileştirilmesini ve akıllı optimizasyonunu sağlayarak hipervizör kaynak kullanımını önemli ölçüde azaltır. Çok çeşitli sanallaştırma, kapsayıcı ve herkese açık bulut platformlarıyla yerel entegrasyon sayesinde altyapının tamamında tutarlı görünürlük ve kontrol sağlanır. Aynı konsoldan yönetilen çok sayıda güvenlik teknolojisi, çeşitli ortamlarda günlük risk yönetimini kolaylaştırır.

Şunlar için idealdir:

Sunucu ve masaüstü iş yüklerini sanallaştıran şirketler

Altyapılarını herkese açık bulutlara taşıyan veya bu bulutlarda barındıran kuruluşlar

DevOps için herkese açık bulutları ve kapsayıcıları kullanan şirketler

Kurumsal avantajlar

Veri merkezinin ve bulut dağıtımlarının tamamı için tutarlı görünürlük ve kontrol sağlar
Yanal hareketi zorlaştırarak saldırı yüzeyini ve bekleme süresini azaltır
Hipervizör kaynaklarının %30'undan tasarruf eder ve oturum açma süresini dakikalardan saniyelere düşürür
Düzenlemelere uygunluğu destekler

Riski ve güvenlik boşluklarını kapatarak BT, Bilgi Güvenliği ve Geliştirme ekipleri arasında etkili iş birliği sağlar.

Kullanım senaryoları

- Sanal sunucu altyapıları için kaynakları dikkatli kullanan koruma
- VMWare ve Citrix VDI İçin Güvenlik
- Temel güvenlik gerekliliklerini karşılayarak düzenlemelere uygunluğu sağlar
- Otomatik dağıtım ve yerel API aracılığıyla tutarlı görünürlük sayesinde AWS ve Azure olayları için bulut iş yükü koruması sağlar
- Kapsayıcı koruması ve yönetim API'si sayesinde DevOps için güvenlik

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server, posta tabanlı tehditlere karşı koruma sağlar ve bu tehditlerin sosyal mühendislik ve kötü amaçlı yazılım saldırılarının çoğunlukla işe yaradığı uç noktalara ulaşmasını engeller. Fidye yazılımı ve madencilik yazılımları dahil olmak üzere her türlü kötü amaçlı yazılım ve kimlik avı saldırıları engellenir. Kurumsal E-Postaların Ele Geçirilmesi saldırılarının önlenmesine özel bir önem gösterilir. Bu çözüm, istenmeyen toplu postaları engeller ve istenmeyen verilerin iletilmesini önler.

Şunlar için idealdir:

Gelişmiş bir BT sistemine ve gizlilik ya da veri güvenliği konusunda endişelere sahip tüm işletmeler

Büyük ölçüde e-posta iletişimiyle gerçekleştiren ve granüler yönetim gerektiren işletmeler

APT tespit verilerini e-posta bağlamıyla zenginleştirmek ve e-postadan bulaşan APT bileşenlerini engellemek isteyen şirketler

Kurumsal avantajlar

Spam e-postalar dahil olmak üzere istenmeyen toplu e-postaları engelleyerek verimliliği artırır ve daha kullanışlı bir iletişim yönetimi için daha fazla posta kategorisi sunar

E-posta tabanlı tehditleri önleyerek işlerin aksamasını önlemeye yardımcı olur

İstenmeyen veri türlerinin aktarımını önleyerek veri güvenliğini artırır

Kullanıcı düzeyindeki olayları azaltarak servis masraflarını azaltmaya yardımcı olur

Üstün tespit özellikleriyle mevcut posta ağ geçidi güvenliğinin etkililiğini artırır ve hatalı pozitifleri çoğaltmaz

Kullanım senaryoları

- Çok çeşitli harici Posta Aktarım araçlarıyla birlikte ya da tüm özellikleri bir arada sunan sanal bir gereç olarak kullanılabilir.
- Microsoft Exchange sunucuları için, hem ağ geçidi hem de posta kutusu düzeylerinde çalışarak API entegre posta güvenliği sağlar

  İstenmeyen dosya türlerinin aktarımını engeller
- E-postadan bulaşan APT bileşenlerini engellemek için Kaspersky
- Anti Targeted Attack ile entegre edilir

Kaspersky Security for Internet Gateway

Kaspersky Security for Internet Gateway, web tabanlı tehditlere karşı kurumsal savunma çevresi düzeyinde koruma sağlar ve bu tehditlerin tüm saldırı türlerinin nihai hedefi olan uç noktalara ulaşmasını önler. Çözüm, sosyal mühendisliğe dayalı saldırıları önlemeye yardımcı olur ve kimlik avı girişimlerinin yanı sıra fidye ve madencilik yazılımları gibi tüm kötü amaçlı yazılım türlerini engeller. Daha yüksek performans için mevcut kurumsal ara sunucunuzla (proxy) eşleştirin ya da kullanıma hazır, hepsi bir arada sanal gereç olarak kullanıma sunun.

Şunlar için idealdir:

Gelişmiş bir BT sistemine ve gizlilik ya da veri güvenliği konusunda endişelere sahip tüm işletmeler

MSP'ler ve xSP'ler (Telekom sağlayıcıları dahil)

Kurumsal avantajlar

Birisi web tabanlı bir tehdide tıklayıp işletmenize sızmasına izin vermeden önce bu tehditleri engelleyerek işlerin aksamasını önler

Üstün tespit özellikleriyle mevcut web ağ geçidi güvenliğinin etkililiğini artırır ve hatalı pozitif sonuçları çoğaltmaz

Kullanıcı düzeyindeki olayların sayısını azaltarak servis masraflarını azaltmaya yardımcı olur
İnternet kullanımını ve belirli dosya türlerinin aktarımını yöneterek verimliliği artırır ve riski azaltır

Kullanım senaryoları

- Kimlik avı amaçlı, zararlı web kaynaklarını ve indirilen kötü amaçlı yazılımları engeller
- İstenmeyen web kaynaklarının kullanımını önler
- Kendine özgü kurallara sahip farklı çalışma alanlarının yönetimini sağlar
- Birden çok kritere bağlı olarak ağa giren ve ağdan çıkan istenmeyen dosya türlerini fitreler
- Web sensörü olarak Kaspersky Anti Targeted Attack ile entegre edilebilir ve gelişmiş tespit sonuçlarına göre hedefli saldırı bileşenlerini engeller

Kaspersky Security for Storage

Kolayca erişilebilen bağlı depolama alanları, tehditlerin tüm altyapıya yayılabileceği bir kaynak ve fidye yazılımı gibi tehditler için bir hedef haline gelebilir. Kaspersky Security for Storage, kurumsal verileri korur ve global tehdit istihbaratıyla desteklenen güçlü koruyucu teknolojilerle tehditlerin ağda yayılmasını önler. Depolama sistemi API'leriyle entegrasyon sayesinde etkinleştirilen Uzaktan Şifreleyici Yazılım Önleme gibi özellikleri içerir.

Şunlar için idealdir:

Gelişmiş bir BT sistemine ve gizlilik ya da veri güvenliği konusunda endişelere sahip tüm işletmeler

Büyük miktarda hassas/gizli veri ile çalışan bankacılık, e-ticaret ve sigortacılık gibi işletmeler

Kurumsal avantajlar

Depolama alanının yazılımına müdahale etmeden bağlı depolama alanlarındaki verileri korur

Tek bakış açısıyla yönetim konsolu sayesinde yönetimle ilgili zorlukları azaltır ve güvenliği artırır
Depolanan verileri uzaktan kontrol edilen fidye yazılımlarına ve kripto silme araçlarına karşı koruyarak iş devamlılığını sağlar

Düzenli Depolama Alanı olarak kullanılabilecek çok çeşitli modellerin güvenliğini sağlayarak düzenlemelere uygunluğu destekler

Kullanım senaryoları

- Hem ağa bağlı depolama alanlarını hem de bunların çalıştırıldığı sunucuları korur
- Güvenli depolama alanında yeni bir dosya oluşturulduğunda veya mevcut dosya değiştirildiğinde dosyanın kötü amaçlı olup olmadığını inceler. Talep üzerine tarama yapılması mümkündür
- Bu çözüm, dosyalar uzaktan şifrelenmeye başladığı anda ağdaki kaynağı tespit edip engelleyerek zararın artmasını önler*

* Yalnızca bazı depolama alanlarında kullanılabilen API entegrasyonu aracılığıyla gerçekleştirilebilir

Kaspersky Embedded Systems Security

Güçlü tehdit istihbaratı, gerçek zamanlı kötü amaçlı yazılım tespiti, kapsamlı uygulama ve cihaz kontrolleri ve esnek yönetim özelliklerine sahip Kaspersky Embedded Systems Security, özel olarak gömülü sistemler için tasarlanan hepsi bir arada bir güvenlik çözümüdür.

Şunlar için idealdir:

Finansal Hizmetler

Perakendecilik ve Taşımacılık

ATM ve POS hizmeti sağlayıcıları

Kurumsal avantajlar

Belirli finansal altyapıları hedef alan tehditlerle ilgili riskleri azaltır

PCI/DSS, SWIFT vb. gibi düzenlemelerin gerekliliklerine uyum sağlar

Tek bir yönetim konsolu aracılığıyla yönetim maliyetlerini optimize eder

Kullanım senaryoları

- Coğrafi olarak farklı bölgelere dağılmış, nadiren güncellenen ve kendine özgü belirli güvenlik özelliklerine sahip gömülü sistemlerin güvenliğini sağlar
- Düşük bütçeli donanımlarda hala yaygın olarak kullanılan ve desteklenmeyen Windows XP için koruma sağlar
- Verimli tasarımı sayesinde sistemlerde aşırı yüklenme olmadan güçlü koruma sağlanır.

Kaspersky Premium Support (MSA) hizmet

Bir güvenlik olayı meydana geldiğinde, nedeni belirlemek ve ortadan kaldırmak için geçen süre önemlidir. Sorunun hızla tespit edilip çözülmesi işletmelerin önemli maliyetlerden kurtulmalarını sağlayabilir. Bakım Hizmet Sözleşmesi (MSA) planlarımız, bu hedefi gerçekleştirmek için özel olarak tasarlanmıştır. 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 ürünlerini kullanan tüm kuruluşlar için idealdir

1 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

3 Maliyet

Kurumsal avantajlar

Sorununuzla ilgilenmek ve mümkün olan en hızlı çözümü sağlamak için 7/24/365 gün destek vermeye hazır olan size özel uzman grubuyla iş devamlılığını sağlar

Öncelikli destek hattı, garantili yanıt süreleri ve size özel yama hizmetleri sunarak güvenlik olayının maliyetini azaltır

Özel Teknik Hesap Yöneticisi, Kaspersky Lab içinde sizin temsilciliğinizi üstlenir ve sorunu çözmek için gerekli uzmanları harekete geçirme yetkisine sahiptir

Kullanım senaryoları

- Kritik sorunları, arka planda çalışan Kaspersky genel merkezindeki uzmanlara iletir. Bu uzmanlar size hızlı bir şekilde doğru çözümü sunmak için en iyi donanıma sahiptir.
- Hızlı düzeltmeler ve kişisel yamalar dahil olmak üzere sisteminiz için özel olarak hazırlanan koruyucu önlemlerle sizin için tam koruma sağlar
- Şirket içindeki değerli kaynaklarınızın bakım ve sorun giderme işlemleri için harcadığı zamanı azaltır

Kaspersky Professional Services hizmet

Siber güvenlik büyük bir yatırımdır. Şirketinizin benzersiz gereksinimlerini karşılamak için güvenliğinizi 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 Professional Services şunları içerir:

- Uygulama ve Yükseltme
- Yapılandırma
- Ürün Eğitimi

Kaspersky ürünlerini kullanan tüm kuruluşlar için idealdir

Kurumsal avantajlar

Güvenlik çözümlerinin %100 kapasiteyle çalışmasını sağlayarak çözümlerinizin yatırım getirisini en üst düzeye çıkarır

Şirket içi BT personeli maliyetlerini azaltır

Ürün yapılandırmalarının düzenli olarak denetlenmesiyle arıza süresi riskini en aza indirir ve en güncel savunma mekanizmalarının kullanılmasını sağlar

Ürünü benimseme süresini azaltarak uygulanan ürünün tüm avantajlarından hızlı bir şekilde yararlanılmasını sağlar

Kullanım senaryoları

- Korumayı azaltacak, verimliliği olumsuz olarak etkileyecek, hatta arıza süresine yol açabilecek ürün uygulama risklerini azaltır
- Yeni güvenlik çözümünüzü günlük çalışma faaliyetlerinize uygulamanın etkisini en aza indirir ve genel uygulama maliyetlerini azaltır
- Ürün eğitim programlarımızla personelinizi ürün bakım işlemlerini üstlenmeye hazırlar. Ürünün uyumluluklarını gösterip çalışma ilkelerini açıklayarak hata yapılmasını önler

Kaspersky Security Awareness

Bilgisayar tabanlı eğitim programlarımız, alışkanlıkları değiştirir ve farkındalık eğitimlerinin asıl hedefi olan yeni davranış biçimlerinin oluşturulmasını sağlar. Kaspersky Security Awareness eğitim portföyü şunları kapsar: Automated Security Awareness Platform (ASAP): Çalışanlar için farkındalık eğitimi. Çalışanların, her geçen gün sağlam siber hijyen becerileri kazanmasını sağlar; Cybersecurity for IT Online (CITO): Genel BT uzmanları için eğitim. Uzmanların, olası bir saldırı senaryosunu tanımak ve olay verilerini toplamak konusunda pratik beceriler geliştirmesini sağlar ve Kaspersky Interactive Protection Simulation (KIPS): Karar vericiler için siber güvenlik oyunu.

Şunlar için idealdir:

BT beklentileri artan ve çeşitlenen kuruluşlar

Güvenlik ihlallerine yol açan kullanıcı hatalarının yaşanmasına fırsat verecek durumları ve bu hataların sıklık derecesini azaltmak isteyen kuruluşlar

Kurumsal avantajlar

İşletmeleri içerideki tehditlere karşı korur

Kurumsal kültürde siber açıdan son derece güvenli bir zihniyetin yerleşmesini sağlar

İnsan hatalarını %80'e kadar azaltır

Kullanım senaryoları

- Tipik senaryolar ve durumlar, siber saldırı simülasyonları, farklı görevler ve açıklamalar aracılığıyla siber açıdan güvenli davranışların geliştirilmesini sağlar
- Olası tehditlerin anlaşılmasına yardımcı olur ve bu tehditlerle mücadele etmek için gerekli becerileri kazandırır
- Görünüşte herhangi bir tehlike içeremeyen bir bilgisayar olayında olası saldırı işaretlerini tanımak ve BT güvenliğine sunulacak olay verilerini toplamak için gerekli becerileri geliştirir
- Üst düzey yöneticilerin ve karar vericilerin güvenlik anlayışını geliştirir

2 Gelişmiş savunma

Gelişmiş tespit teknolojisi ve merkezi yanıt

Karmaşık tehditlerin tespiti ve yanıtlanması aşamasında maksimum otomasyon

- Saldırı yüzeyinin genişlediği ve gittikçe büyüyen ve daha karmaşık hale gelen BT ortamlarına sahip şirketler
- Sınırlı uzmanlığa sahip küçük bir güvenlik ekibine sahip şirketler
- Temel düzeyde olay yanıt becerilerine sahip şirketler

Büyük ve orta ölçekli şirketler için idealdir:

Uç Nokta

Kaspersky Endpoint Detection and Response

Çalışanlar

Kaspersky Cybersecurity Training

Hizmetler

Kaspersky Targeted Attack Discovery

Ağ

Kaspersky Anti Targeted Attack

Gizlilik

Kaspersky Private Security Network

İstihbarat

Kaspersky Threat Intelligence

Kaspersky Endpoint Detection and Response

İşletmenizi gelişmiş tehditlere karşı mümkün olan en erken aşamada savunmak için önleyici teknolojilerin uç nokta tespit ve yanıt özellikleriyle desteklenmesi büyük önem taşır. Kaspersky EDR, uç noktalarınızın hedef alındığı gelişmiş tehditlerle mücadele eden özel bir çözümdür. Bu çözüm, dünya lideri Kaspersky Endpoint Security koruma çözümümüzle aynı aracıyı paylaşır. Kaspersky EDR, kurumsal ağdaki tüm uç noktalarda kapsamlı görünürlük sağlar ve karmaşık tehditlerin hızlı bir şekilde keşfedilmesi, önceliklendirilmesi, araştırılması ve etkisiz hale getirilmesi için rutin görevleri otomatikleştirir.

Şunlar için idealdir:

Şirketler

Kaspersky Endpoint Security çözümünü kullanan kuruluşlar

Güvenlik İşlemleri Merkezleri ve olay yanıt ekipleri

4 Gerekli beceriler

3 Özelleştirme ve ölçeklenebilirlik

2 Maliyet

Kurumsal avantajlar

Gelişmiş tehditler ve hedefli saldırılarla ilgili riskleri azaltır
Görev otomasyonu ve iş odaklı basitleştirilmiş bir arayüz sayesinde yönetim maliyetlerini optimize eder

Olay işleme sürecinin hızını ve etkililiğini artırır ve bunun için ek bir maliyet gerektirmez

BT ve güvenlik ekiplerinizin zamanını diğer işlere ayırmasını sağlayarak
verimliliği artırır

Şirket içi güvenlik politikalarına ve
düzenlemelerde belirtilen gerekliliklere uygunluğu destekler

Kullanım senaryoları

- Otomatik tehdit engellemeden gelişmiş tehditlere karşı karmaşık olay yanıtına kadar uç nokta koruma döngüsünün tamamında tek bir aracıyla işlevlerini yerine getirir
- Ele geçirilen iş istasyonlarının kullanılamadığı veya verilerin şifrelendiği durumlarda bile uç nokta verilerine hızlı erişim sağlar
- Tehdit avı, IoA analizi ve MITRE ATT&CK eşleme özellikleriyle olay araştırmalarını destekler
- Geniş bir yelpazeyi kapsayan otomatik işlemler aracılığıyla dağıtık altyapılarda tehditlere etkili bir şekilde yanıt verilmesini sağlar

Kaspersky Anti Targeted Attack

Hedefli saldırıların sayısı ve kalitesi sürekli olarak artmaktadır. Yeni ortaya çıkan bu tehditlerle mücadele etmek için güvenlik sistemlerinizi sürekli olarak uyarlamanız gerekir. Kaspersky Anti Targeted Attack, tamamen otomatik veri toplama, analiz ve korelasyon özellikleriyle ağ düzeyinde gelişmiş tehdit tespitine odaklanır ve tehdit kapsamının detaylı olarak anlaşılmasını sağlar. Bunun sonucunda kurumsal altyapınız karmaşık tehditlere ve hedefli saldırılara karşı etkili bir şekilde korunur ve ek kaynaklara ihtiyaç duyulmaz.

Şunlar için idealdir:

Şirketler

Güvenlik İşlemleri Merkezi ekipleri

Yönetilen Güvenlik Hizmeti Sağlayıcıları

Düzenlemelere uygunluk şartına tabi kuruluşlar

4 Gerekli beceriler

3 Özelleştirme ve ölçeklenebilirlik

5 Maliyet

Kurumsal avantajlar

Gelişmiş tehditler ve hedefli saldırılarla ilgili riskleri a zaltır

Karmaşık tehditlere karşı koruma sağlamak için tek bir güvenli sistem sunarak finansal ve operasyonel zararı azaltır

Görev otomasyonu ve iş odaklı basitleştirilmiş bir arayüz sayesinde yönetim maliyetlerini optimize eder

Sorunsuz iş akışı otomasyonuyla görevleri düzenli hale getirir ve iş süreçlerinde aksamayı ortadan kaldırır

Kullanım senaryoları

- Altyapıya giriş noktalarının merkezi olarak izlenmesi ve kontrolü aracılığıyla, önleyici teknolojileri atlatmayı başaran siber suçluların hızlı bir şekilde tespiti
- Daha etkili bir araştırma için tehdit işaretlerinin tespiti ve bir saldırıdaki çok vektörlü olayların tek bir resimde birleştirilmesi
- Tespit edilen tehditlerle ilgili gerekli tüm bilgilerin olay yanıt ekibine zamanında sunulması

Kaspersky Private Security Network

Kaspersky Private Security Network, şirketlerin kontrollü çevrelerinin dışına hiçbir şekilde veri yayınlamadan global bulut tabanlı tehdit istihbaratından yararlanmalarını sağlar.

Bu ürün, Kaspersky Security Network'ün kuruma ait, yerel ve tamamen özel bir sürümüdür.

Şunlar için idealdir:

Sıkı veri erişimi kontrol gereklilikleri olan şirketler

Fiziksel olarak yalıtılmış ağlarda çalışan Kritik Altyapılar

Telekom, yönetilen güvenlik ve diğer hizmet sağlayıcıları

Kurumsal avantajlar

İşletmenizi hedef alan tehditlerin daha etkili bir şekilde tespit edilmesine yardımcı olur

Tehdit ve bilinirlik istatistiklerine gerçek zamanlı erişim sağlayarak yanıt sürelerini hızlandırır
Hatalı pozitif sonuçları en aza indirerek operasyonel verimliliği artırır

Yalıtılmış sistemlerin ve ortamların güvenliği için düzenleyici gerekliliklere tam uygunluğun sağlamasına yardımcı olur

Kullanım senaryoları

- Bilgilerinizi kontrollü altyapının dışında paylaşmanıza gerek kalmadan bulut tabanlı güvenliğin avantajlarından yararlanabilirsiniz
- Kendi "kararlarınızı" eklemenize izin vererek size özel bir koruma sistemi oluşturmanıza olanak tanır
- Yalıtılmış kritik ağlara göre uyarlanır

Kaspersky Targeted Attack Discovery hizmet

Kaspersky Targeted Attack Discovery, halihazırda saldırı altında olup olmadığınızı, saldırı sürecinde nelerin gerçekleştiğini ve tehdit aktörünü belirlemenizi sağlayan kapsamlı bir tehlike değerlendirme hizmetidir. Uzmanlarımız, devam etmekte olan ve geçmişte gerçekleşmiş olan olayları tespit eder, tanımlar ve analiz eder. Ayrıca saldırılardan etkilenen sistemlerin listesini oluşturur. Kötü amaçlı faaliyetleri açığa çıkarmanıza, olayların olası kaynaklarını belirlemenize ve en etkili iyileştirme işlemlerini planlamanıza yardımcı olur.

Şunlar için idealdir:

Güvenlik ekibi olmayan veya güvenlik ekibi yeterince gelmişmemiş şirketler

Devlet kurumları

Kritik altyapılar

1 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

3 Maliyet

Kurumsal avantajlar

Sistemlerin saldırıya uğramasından kaynaklanan hasarı önleyerek ve en aza indirerek maliyeti önemli ölçüde azaltır
Müşterileriniz, iş ortaklarınız ve yatırımcılarınız ile güven ilişkinizi sürdürmenize yardımcı olarak iş fırsatlarını artırmanızı sağlar

Düzenleyici gerekliliklere uymamaktan kaynaklanan cezalardan ve para cezalarından kaçınmanızı sağlar

İyileştirme önerileriyle gelecekteki olaylara karşı savunmanızı güçlendirir

Kullanım senaryoları

- Kuruluşunuzun dijital ayak izini ve ilgili riskleri anlamanızı sağlar
- BT altyapınız ve verileriniz (günlük dosyaları gibi) üzerinde kapsamlı incelemeler gerçekleştirerek ve şirket dışına giden ağ bağlantılarınızı analiz ederek riski değerlendirmenize yardımcı olur
- Ağlarınızda devam eden veya geçmişte gerçekleşen sızma girişimlerinin işaretlerini tespit eder
- Saldırının sistemlerinizi nasıl etkilediğini ve bu konuda neler yapabileceğinizi anlamanızı sağlar

Kaspersky Threat Intelligence

Günümüzün siber tehditleriyle mücadele etmek için tehdit aktörlerinin kullandığı 360 derece görüş açısı sağlayan taktikler ve araçlar gereklidir. Bu istihbaratın oluşturulması ve en etkili önlemlerin belirlenmesi ise sürekli tetikte olmayı ve üst düzey uzmanlığı gerektirir. Veri madenciliği için kullanılabilecek petabaytlarca veri, gelişmiş makine öğrenimi teknolojileri ve eşsiz küresel uzman havuzu ile Kaspersky Lab, dünyanın dört bir yanından en son tehdit istihbaratını sunarak sizleri daha önce hiç görülmemiş siber saldırılardan bile korumak için çalışır.

Şunlar için idealdir:

Şirketler

Devlet kurumları

Güvenlik İşlemleri Merkezleri ve olay yanıt ekipleri

Yönetilen Güvenlik Hizmeti Sağlayıcıları

Kurumsal avantajlar

İşletme faaliyetlerinin aksamasını önlemek için anında tehdit tespiti

Olaylardan kaynaklanan olası finansal zararları en aza indirir

Şirketinizi hedef alan tehditlerle ilgili zamanında sunulan bilgilere bağlı olarak belirli teknolojilere ve personele uygun maliyetli yatırımlar yapılmasını sağlar

Rakiplerinizin, fikri mülkiyet haklarınızı sızdırarak haksız avantaj sağlamasını önler

Proaktif ve uyarlanabilir bir savunma mekanizması oluşturmaya yardımcı olur

Kullanım senaryoları

- Sürekli güncellenen Tehdit Veri Akışı ağ güvenlik çözümlerini güçlendirin
- Çok sayıda güvenlik uyarısını etkili bir şekilde önceliklendirin. Tehdit Veri Akışı ve CyberTrace özellikleriyle olay yanıtı ekiplerine bildirilmesi gereken uyarıları derhal belirleyin
- Gerçek zamanlı "durum bilgileri"ni alın ve CyberTrace ile tehdit istihbaratı akışlarından daha etkili bir şekilde yararlanın
- Kuruluşunuzun dijital ayak izini belirleyin ve Size Özel Tehdit İstihbaratı Raporları sayesinde ilgili risklerin etkilerini en aza indirin

Kaspersky Cybersecurity Training: Olay Yanıtı

hizmet

Siber güvenlik eğitimi, sürekli gelişen tehditlerin günden güne artmasıyla karşı karşıya kalan şirketler için kritik önem taşır. BT güvenlik personeli, etkili kurumsal tehdit yönetiminin ve risk azaltma stratejilerinin temelini oluşturan gelişmiş teknikler konusunda becerili olmalıdır. Kaspersky Cybersecurity Training, şirket içi ekibinizin sürekli gelişen tehdit ortamıyla mücadele etmek için gerekli bilgileri kazanmasına yardımcı olur.

Şunlar için idealdir:

Şirketler

Devlet kurumları

Güvenlik İşlemleri Merkezleri ve olay yanıt ekipleri

Yönetilen Güvenlik Hizmeti Sağlayıcıları

3 Gerekli beceriler

3 Özelleştirme ve ölçeklenebilirlik

2 Maliyet

Kurumsal avantajlar

Güvenlik olayının olası zararlarını hızlı ve etkili bir şekilde en aza indirerek olayın maliyetini önemli ölçüde azaltır

Düzenleyici gerekliliklere uymamaktan kaynaklanan cezalardan ve para cezalarından kaçınmanızı sağlar

Müşterileriniz, iş ortaklarınız ve yatırımcılarınız ile güven ilişkinizi sürdürmenize yardımcı olarak iş fırsatlarını artırmanızı sağlar

Öğrenilen derslerle gelecekteki olaylara karşı savunmanızı güçlendirir

Kullanım senaryoları

- APT'leri diğer tehditlerden ayırt edin
- Çeşitli saldırgan tekniklerini ve hedefli saldırıların anatomilerini anlama
- Belirli izleme ve tespit yöntemlerini uygulayın
- Etkili tespit kuralları oluşturun
- Olayın kronolojisini ve mantığını yeniden oluşturma ve olay yanıt iş akışını takip etme

3 Entegre Siber Güvenlik Yaklaşımı

Tehdit Yönetimi ve Savunma

APT düzeyindeki saldırılara hazırlıklı olun

Tehdit istihbaratıyla çalışabilen ve tehdit avı işlemlerini gerçekleştirebilen şirketler için idealdir

- Karmaşık ve dağıtık ortamlar
- Şirket içi güvenlik ekibi veya Güvenlik İşlemleri Merkezi
- Olay ve veri sızıntısı maliyetlerinin yüksek olması
- Düzenlemelere uygunluk şartına tabi şirketler

Hizmetler

Kaspersky Managed Protection

Kaspersky Incident Response

Çalışanlar

Kaspersky Cybersecurity Training

Intelligence

Kaspersky Threat Intelligence

Kaspersky Threat Management and Defense

Kaspersky Threat Management and Defense, hızlı tehdit tespiti, olay araştırma, yanıt ve onarım işlemleri için kapsamlı bir sistem sunan özel bir çözümdür. Bu çözüm, global tehdit istihbaratı, gelişmiş tehdit tespit ve yanıt teknolojileri, siber güvenlik eğitimi yelpazesi, sürekli tehdit avı ve mevcut güvenlik engellerini atlatan tehditlere yanıt verme özelliklerini içerir.
Çözüm, karmaşık tehditlerle mücadele etmek için güncel kurumsal stratejinize dahil edilerek mevcut koruma teknolojilerinizi tamamlar ve ihtiyaç duyduğunuz anda sizi lider uzmanlık becerileriyle destekler.

Şunlar için idealdir:

Şirketler

Devlet kurumları

Güvenlik İşlemleri Merkezleri ve olay yanıt ekipleri

Yönetilen Güvenlik Hizmeti Sağlayıcıları

5 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

5 Maliyet

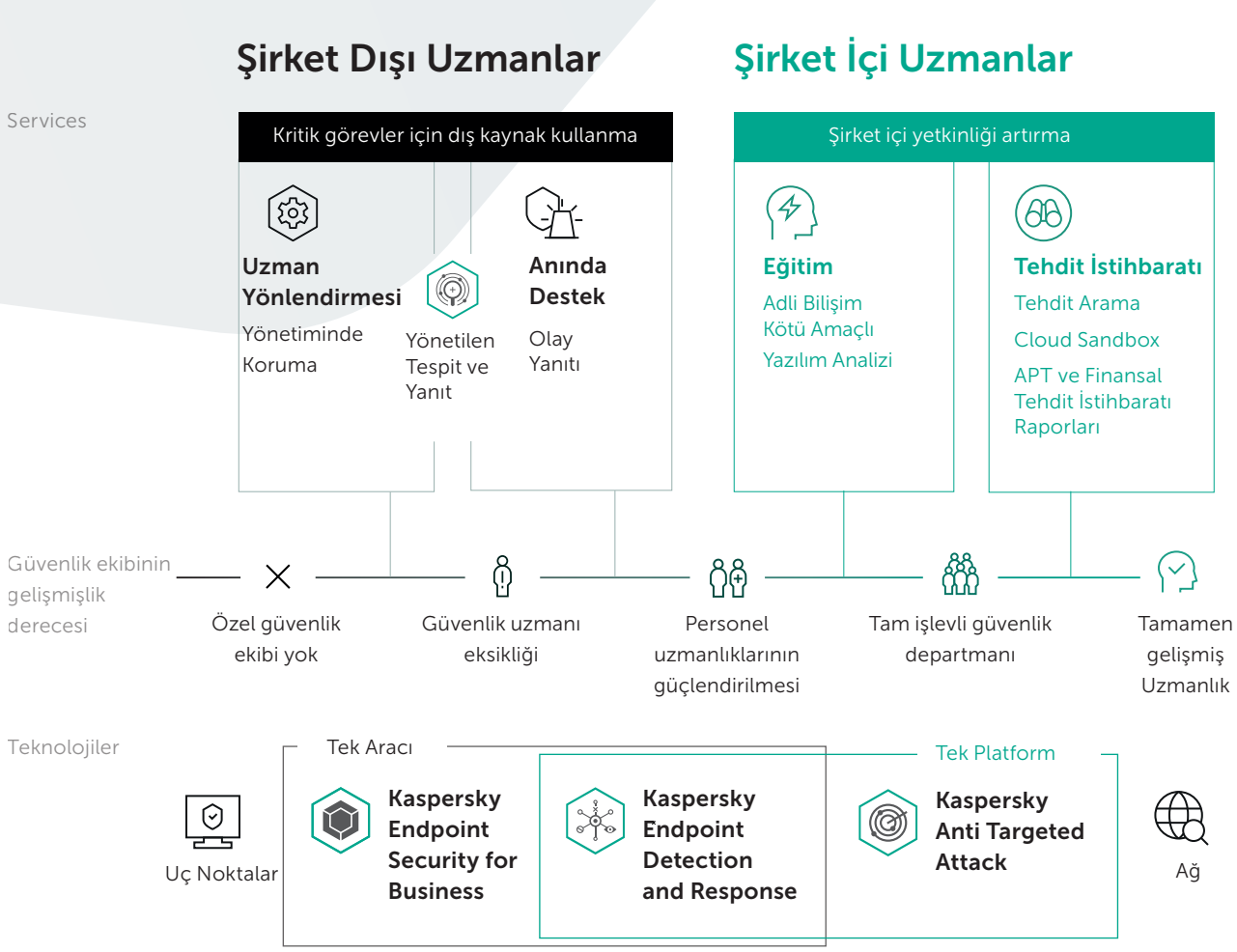
Kurumsal avantajlar

Siber suçların yol açtığı finansal ve operasyonel zararı en aza indirir ve işletme istikrarının korumasına yardımcı olur
Otomasyon ve iş süreçlerinin aksamasının önlenmesi sayesinde yatırım getirisini artırır

Şirket içi uzmanlığı geliştirerek personel değişim oranını azaltır ve operasyonel verimliliği artırır.
Özelleştirilmiş tehdit modellerine bağlı olarak bilinçli ve uygun maliyetli bilgi güvenlik stratejileri uygular

Kullanım senaryoları

- Gerekli tüm özellikleri bir arada sunan teknolojik platform, zaman alıcı delil toplama işlemlerini ve rutin manuel görevleri otomatikleştirir
- Proaktif tehdit istihbaratı, tehditleri tespit etme, önceliklendirme, araştırma ve yanıt verme için gerekli
- Gelişmiş becerilerin sağlanmasıyla kurumsal tehdit yönetim stratejisi
- Tehdit avı, önleyici teknolojileri atlatabilecek şekilde tasarlanan bilinmeyen ve gelişmiş tehditlerin tespitini sağlar
- Üçüncü taraf uzmanlara erişim, araştırmanın etkili bir şekilde yürütülmesini ve karmaşık olaylara yanıt verilmesini destekler


Şirket Dışı Uzmanlar
Şirket İçi Uzmanlar
Services
Kritik görevler için dış kaynak kullanma
Şirket içi yetkinliği artırma
Uzman Yönlendirmesi
Yönetiminde Koruma
Yönetilen Tespit ve Yanıt
Anında Destek
Olay Yanıtı
Eğitim
Adli Bilişim
Kötü Amaçlı Yazılım Analizi
Tehdit İstihbaratı
Tehdit Arama
Cloud Sandbox
APT ve Finansal Tehdit İstihbaratı Raporları
Güvenlik ekibinin gelişmişlik derecesi
Özel güvenlik ekibi yok
Güvenlik uzmanı eksikliği
Personel uzmanlıklarının güçlendirilmesi
Tam işlevli güvenlik departmanı
Tamamen gelişmiş Uzmanlık
Teknolojiler
Tek Aracı
Tek Platform
Uç Noktalar
Kaspersky Endpoint Security for Business
Kaspersky Endpoint Detection and Response
Kaspersky Anti Targeted Attack
Ağ

Uzun vadeli bir siber güvenlik stratejisi geliştirirken dikkat edilmesi gereken unsurlar

Siber güvenlik konusunda yalıtılmış bir yaklaşım izlemek işletmeleri riske atar

Ağ ve veri sızıntılarının artan maliyetleri, bir dönüşüm gerçekleştirmek isteyen işletmeler üzerinde ciddi finansal baskılar oluşturmaktadır. Bu nedenle siber güvenlik önemli bir unsurdur.

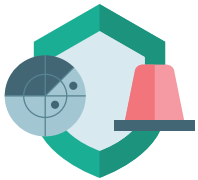
İşletmeler, bu ortamda başarıyı yakalamak için risk yönetiminde ve uzun vadeli planlamada kilit öneme shaip olan siber güvenliği genel işletme stratejilerinin bir parçası haline getirmelidir.

Siber güvenlik ulaşılabilecek bir nokta değil, hiç durmadan devam eden bir yolculuktur

Bir şirketin güvenlik planı, sürekli olarak gözden geçirilmeli ve ulaşılan yeni bilgiler ve araçlarla düzenlenmelidir. Tüm güvenlik olayları, gelecekte benzer olayların yaşanmasını önlemek için kapsamlı bir analizden geçirilmeli ve bu analiz sonucunda yeni saldırı yönetim prosedürleri ve önlemleri geliştirilmelidir. Mevcut savunma mekanizmalarının sürekli olarak geliştirilmesi gereklidir.

Hızla değişen siber tehdit dünyasında başarının anahtarı farkındalık, iletişim ve iş birliğidir.

Siber olayların %80'i insan hatalarından kaynaklanır. Her düzeyden personelin eğitimi, kurum genelinde güvenlik farkındalığını artırmak için çok önemlidir. Siber güvenlik, çalışanların görev tanımında olmasa bile bu eğitim, tüm çalışanları siber tehditlere ve önlemlere dikkat etme konusunda motive etmek açısından kritik önem taşır.



Proaktif bir "tespit ve yanıt" anlayışı, günümüzün hiç durmadan gelişen tehditleriyle mücadele etmek için en iyi yoldur.

Geleneksel önleme sistemleri gelişmiş tespit teknolojileri, tehdit analizleri, yanıt özellikleri ve önleyici güvenlik teknikleri ile uyum içinde çalışmalıdır. Bu sayede şirketlerin karşılaştığı yeni zorluklara karşı sürekli olarak uyarlanabilen ve yanıt verebilen bir siber güvenlik sistemi geliştirilebilir.

Neden Kaspersky'yi seçmelisiniz?

En Çok Test Edilen. En Çok Ödül Alan

Kaspersky, bağımsız testlerde diğer güvenlik satıcılarına kıyasla daha fazla birincilik elde etti.
Üstelik bu her yıl böyle oluyor.

www.kaspersky.com.tr/top3

En çok tavsiye edilen şirketlerden biri olan

Kaspersky, 2018'de Gartner Peer Insights'ta bir kez daha Customers' Choice for Endpoint Protection Platforms derecesini kazanmış ve müşteri memnuniyeti konusunda 5 üzerinden 4,6 gibi yüksek bir puan almıştır (28 Mayıs 2019 tarihi itibariyle).*

En şeffaf

Açtığımız ilk Şeffaflık Merkezimiz ve İsviçre'deki istatistiksel işleme sistemimiz sayesinde verilerinizin bağımsızlığı başka hiçbir satıcının yanına yaklaşamayacağı bir seviyede güvende.

*Gartner Peer Insights Customers' Choice, bireysel son kullanıcı yorumlarında belirtilen öznel fikirlerin, derecelendirmelerinin ve verilerin belgelendirilmiş bir metodolojiye göre değerlendirilmesini içerir; bunlar Gartner 'ın veya bağlı kuruluşlarının görüşlerini yansıtmaz veya onayını göstermez.

Bize ulaşın

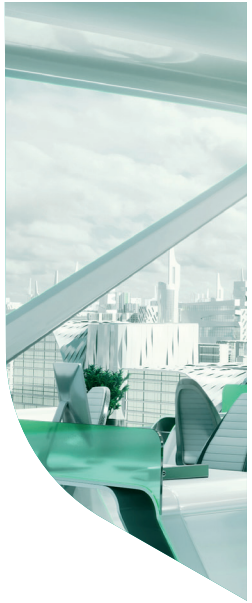
Size en yakın iş ortağımızı bulun: www.kaspersky.com/buyoffline
Kaspersky for Business: www.kaspersky.com/business
Kurumsal Siber Güvenlik: www.kaspersky.com/enterprise
BT Güvenliğiyle İlgili Haberler: business.kaspersky.com/
Benzersiz yaklaşımımız: www.kaspersky.com/true-cybersecurity

#bringonthefuture

www.kaspersky.com.tr

© 2019 AO Kaspersky Lab. Tüm hakları saklıdır. Tescilli ticari markalar ve hizmet markaları, ilgili sahiplerinin mülkiyetindedir.

kaspersky

Bring on the future

www.kaspersky.com.tr