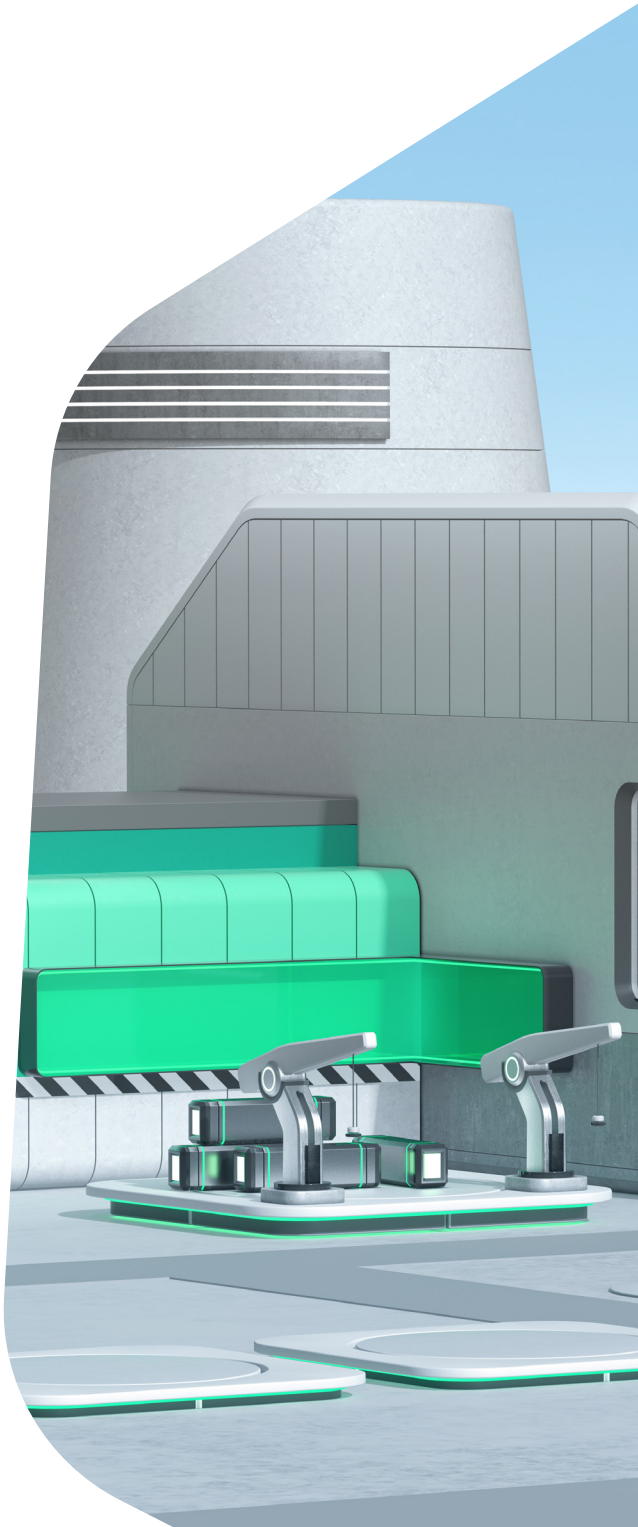
kaspersky

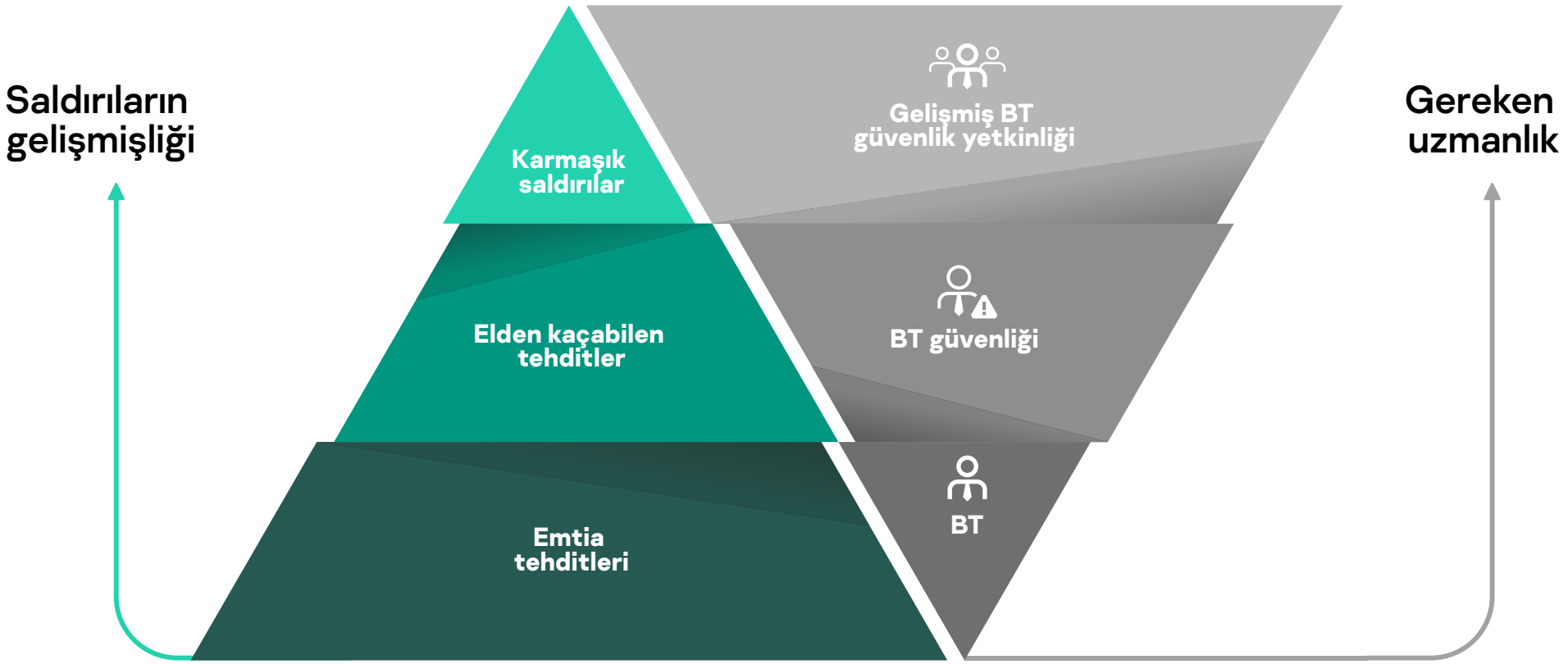
Kaspersky Security for Enterprise

Kaspersky'nin Kurumsal Ürün Portföyü Hakkında

Doğru ürünü veya hizmeti seçerek işletmeniz için güvenliğin temelini atmak yalnızca ilk adımdır. Uzun vadeli başarının anahtarı, ileriye dönük kurumsal bir siber güvenlik stratejisi geliştirmektir. Kaspersky'nin Kurumsal Ürün Portföyü, günümüz işletmelerinin güvenlik taleplerini yansıtır ve kademeli yaklaşımıyla farklı olgunluk 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.



Tehdit türleri ve bunlara karşı koymak için gereken uzmanlık



Uzun ve kısa dönem güvenlik planı karşılaştırması

Geleneksel güvenliğin evrim süreci:

Karar verme:

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

Nedenler

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

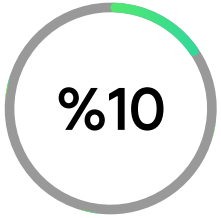
Geleneksel ürünleri kullanma:

- Uç Nokta Koruma Platformları (EPP)
- Güvenlik Duvarları / Yeni Nesil Güvenlik Duvarları (NGFW)
- Web Uygulaması Güvenlik Duvarları (WAF)
- Veri Kaybını Önleme (DLP)
- Bilgi Güvenliği ve Olay Yönetimi Sistemleri (SIEM)
- Ve diğerleri

Geleneksel yaklaşımların başarısız olma sebepleri:

- Tehdit ortamının daha karmaşık hale gelmesi
- Siber güvenlik teknolojilerinin karmaşıklığı
- İşletmenin başarılı bir dijital dönüşüm geçirebilmesi için uzun vadeli bir siber güvenlik stratejisi gerekmesi

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.

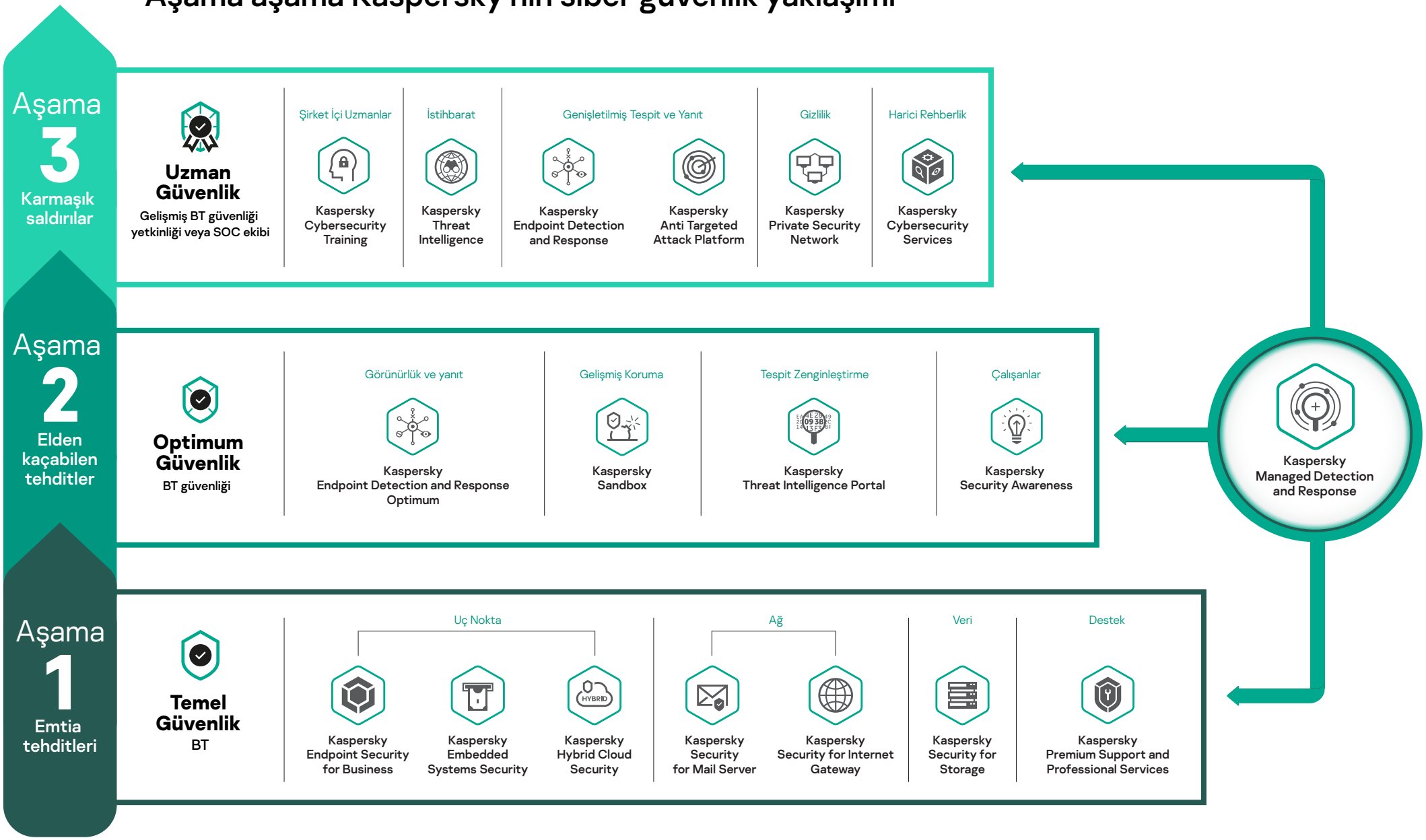


işletmelerin %10'u saldırıları neredeyse anında tespit ediyor

bir veri sızıntısının 7 gün sonra tespit edilmesinin yarattığı ilave maliyet

Kaynak: BT Güvenliği Ekonomisi 2020 Kaspersky raporu

Aşama aşama Kaspersky'nin siber güvenlik yaklaşımı



1. Aşama
Temel Güvenlik

Maksimum sayıda tehdidi otomatik engelleyin

- Her boyutta ve altyapı karmaşıklığındaki işletmeler için karmaşık tehditlere karşı entegre bir savunma stratejisi oluşturmadaki temel aşamadır
- Yalnızca BT ekipleri olan ve BT güvenlik uzmanları kullanmayan küçük kuruluşlar için genelde yeterlidir

Kaspersky Endpoint Security for Business

Ne pahasına olursa olsun işletmenizin itibarı her zaman korunmalıdır, bu nedenle tüm uç noktalarınızı "sadece" korumak ve kontrol etmekten fazlasını yapıyoruz. Kaspersky Endpoint Security for Business, işletmenizi BIOS'la ilişkili olanlardan dosyasız tehditlere kadar tüm tehditlere karşı korurken sunucu sağlamlaştırma, kişisel ve finansal bilgilerin kaybını önleyen özel kontroller sayesinde yüksek performanslı sunucu savunmanızı güçlendirir. Esnek güvenlik ve yönetim için buluttan veya şirket içinde yönetilebilir.

Hedefleriniz:

- Çalışanların kendilerini ve işletmenizi bir saldırıya maruz bırakmasını önlemek
- Manuel olarak işlenmesi gereken uç nokta olaylarının sayısını azaltmak
- Esnek ve başarısı kanıtlanmış savunmalar ile çeşitli ortamları güvence altına almaksa sizin için idealdir.

2 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

2 Yatırım düzeyi

Kurumsal avantajlar

- Hepsi bir arada bir ürünle farklı tehditlere karşı savunmalarınızı otomatikleştirerek TCO'yu (Toplam Sahip Olma Maliyeti) düşürür
- Her cihazı her yerde koruyarak iş sürekliliğini sağlar
- BT güvenlik yönetimi konusunda dış kaynak kullanımı için esneklik sağlarken uyumluluk gereksinimlerini karşılamaya yardımcı olur

Pratik Uygulamalar

- En çok ödüle sahip uç nokta koruma teknolojisi ile bir saldırının kurbanı olma riskinizi azaltır
- Bulut veya şirket içi konsoldan yönetimle BT varlığınızın yamalarının kurulduğundan emin olmanızı sağlar
- Üçüncü taraf çözümlerden kolay ve hızlı bir şekilde geçiş yapmanızı sağlar
- Uç noktalara yeniden kurulum yapmadan, EDR ve diğer özellikler de dahil olmak üzere yeni teknolojileri organik şekilde eklemenizi sağlar
- Uzaktan silme ve çeşitli işletim sistemleri için cihaz kontrolü dahil olmak üzere yerleşik şifreleme yönetimi aracılığıyla uyumluluk hedeflerini karşılarken verilerinizi korumanızı sağlar

Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security, işletmenizi sanallaştırırken veya iş yükünüzü buluta taşırken dijital dönüşümünüzü basitleştirir ve güvence altına alır. Patentli Light Agent teknolojisi, hipervizör kaynak kullanımını önemli ölçüde azaltır. Çok çeşitli sanallaştırma, kapsayıcılaştırma ve herkese açık bulut platformlarıyla yerel entegrasyon sayesinde altyapınızın tamamında tutarlı görünürlük ve kontrol sağlar. Aynı konsoldan yönetilen çok sayıda güvenlik teknolojisi, çeşitli ortamlarda günlük risk yönetimini kolaylaştırır.

Hedefleriniz:

- Sunucu ve masaüstü iş yüklerinizi sanallaştırmak
- Altyapıları herkese açık buluta taşımak veya sürekliliğini sağlamak
- Güvenlik adımlarını DevOps proje hattınıza entegre etmek
- Kapsayıcılaştırmadan güvenli şekilde faydalanmaksa sizin için idealdir.

2 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

2 Yatırım düzeyi

Kurumsal avantajlar

- Saldırı yüzeyinizi ve saldırganın bekleme süresini azaltarak finansal kaybı ve itibar kaybını en aza indirir
- Hipervizör kaynaklarından %30'a kadar tasarruf sağlayarak BT maliyetlerini optimize eder
- Temel güvenlik gerekliliklerini karşılayarak düzenlemelere uygunluğu destekler
- Riski ve güvenlik boşluklarını kapatarak BT, Bilgi Güvenliği ve Geliştirme (DevOps) ekipleri arasında etkili iş birliği sağlar

Pratik Uygulamalar

- Veri merkezlerinizin ve bulut dağıtımlarınızın tamamı için tutarlı görünürlük ve kontrol sağlar
- VMWare ve Citrix VDI'ın güvenliğini sağlar
- Yerel API entegrasyonu üzerinden sağlanan tutarlı görünürlük ve otomatik dağıtım ile AWS, Azure ve Google Cloud örneklerinde bulut iş yüklerinizi korur
- Kapsayıcı koruması, proje hattı entegrasyon arayüzleri ve yönetim API'si ile DevOps'un güvenliğini sağlar

Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security, Windows tabanlı gömülü cihazlarınızı ve artık yükseltme imkanınız olmayan, desteklenmeyen işletim sistemleri çalıştıran eski uç noktaları korumak için tasarlanmış çok katmanlı özel bir çözümdür. Uygulama Kontrolü, süreçlerinize ve cihaz yeteneklerinize göre uyarlanmış optimum koruma için açık suistimalini önleme, ağ tehdidi koruması, bütünlük izleme ve diğer güvenlik katmanları dahil olmak üzere isteğe bağlı kötü amaçlı yazılımdan koruma ile birleşir.

Hedefleriniz:

- ATM'leri, PoS sistemlerini, sağlık hizmeti ekipmanlarını veya diğer endüstriyel olmayan sınıf gömülü sistemleri korumak
- Eski uç noktalar dahil olmak üzere, eski donanım ve işletim sistemi çalıştıran sistemlerin güvenliğini optimize etmek
- Gömülü altyapınızın güvenliğini Kaspersky tabanlı güvenlik ekosisteminize entegre etmekse sizin için idealdir.

2 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

2 Yatırım düzeyi

Kurumsal avantajlar

- Bir saldırının finansal, yasal ve itibari etkisinin yıkıcı olabileceği alanlarda iş süreçlerinin sürekli, kesintisiz olmasını sağlar
- Yükseltmeye zorlanmaktan kaçınmanıza yardımcı olur - eski ve henüz yeri doldurulamaz, senaryoya özgü uç noktaları güvenli bir şekilde istediğiniz kadar kullanmaya devam edersiniz
- Düzenleyici kurumlar tarafından özellikle önerilenler dahil olmak üzere güvenilir koruma mekanizmaları aracılığıyla düzenlemelere tam uyumluluk sağlar

Pratik Uygulamalar

- Çeşitli güvenlik katmanları ve senaryoları arasından, kullanımına ve güç düzeyine göre sisteminiz için en etkili güvenlik senaryosunu yapılandırır
- Sık şekilde bakım yapılması imkansız olan yerlerde dayanıklı ve sorunsuz koruma sağlar
- E-posta veya web üzerinden saldırılamayan yerleşik cihazlar için büyük bir risk olan kötü niyetli çalışan kaynaklı saldırıları önler
- İnternet bağlantısı zayıf olan cihazları korur

Kaspersky Security for Mail Server

Kaspersky Security for Mail Server, suç yazılımı, fidye yazılımı, kimlik avı ve spam gibi e-posta tabanlı tehditlerin, çoğu kötü amaçlı yazılımın ve sosyal mühendislik dolandırıcılığının çalıştığı uç noktalarınıza ulaşmasını engeller. Bulut tabanlı yapay zeka uygulaması ve şirket içi makine öğrenimi tabanlı modeller, son derece düşük hatalı pozitiflerle yüksek algılama oranları sağlayarak, Kurumsal E-posta Dolandırıcılığı (BEC) da dahil olmak üzere gelişmiş posta tabanlı tehditleri ele alır. Kaynakların boşa harcanmasına neden olan spam, yayılmadan önce etkin bir şekilde engellenir.

Hedefleriniz:

- E-postayı bir teslim yöntemi olarak kullanan hem toplu hem de yüksek hedefli saldırılara karşı yeteneklerinizi güçlendirmek
- Farklı platformları ve dağıtım yöntemlerini içeren çok çeşitli e-posta güvenlik senaryolarını kapsamaksa sizin için idealdir.

Kurumsal avantajlar

- E-postadan bulaşan kötü amaçlı yazılımların ve sosyal mühendislik tabanlı saldırıların yıkıcı etkilerini azaltır
- Spam'in neden olduğu dikkat dağıtıcı unsurları ortadan kaldırarak çalışanların üretkenliğini artırır
- BT/BT güvenliğinin iş yüklerini azaltır ve operasyonel maliyetlerinizi optimize eder
- E-postayla gönderilen içerik paylaşımını kontrol ederek yasal ve itibar riskinizi en aza indirir

Pratik Uygulamalar

- Tehditleri hedeflerine, yani kullanıcılarınız ve uç noktalarınıza ulaşmadan önce engelleyerek, posta sunucusu düzeyinde altyapı savunmanızı ciddi anlamda güçlendirir
- Hatalı pozitiflere neden olmadan mevcut ağ geçidi güvenliğini artırır
- Kaspersky tabanlı gelişmiş tehdit algılama araçlarınızı, ek bağlam ve otomatik ağ geçidi düzeyinde yanıt yetenekleriyle güçlendirir

Kaspersky Security for Internet Gateway

Temel uygulaması Kaspersky Web Traffic Security ile birlikte Kaspersky Security for Internet Gateway, kötü amaçlı yazılımlar, fidye yazılımları, madencilik yazılımları, çevrimiçi kimlik avı ve kötü amaçlı web kaynakları dahil olmak üzere web tabanlı siber tehditlere karşı ağ geçidi düzeyinde sağlam koruma sunar. Ayrıca, global ağ (World Wide Web) kullanımını kontrol etmenize, kurumsal politikalarınızla uyumlu şekilde belirli web kaynaklarına erişimi kısıtlamanıza ve belirli dosya türlerinin aktarımını sınırlamanıza olanak tanır.

Hedefleriniz:

- Web tabanlı tehditlerin uç noktalarınızı etkilemesini önlemek
- İnternet kullanımına kontroller getirerek tehditlerin bulaşma riskini azaltmak ve genel verimliliği artırmak
- Web tabanlı tehditleri otomatik şekilde giriş noktasında engelleyerek BT/BT güvenlik ekiplerinizin iş yükünü azaltmaksa sizin için idealdir.

2 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

2 Yatırım düzeyi

Kurumsal avantajlar

- İşlerin aksaması ve ağ içi güvenlik sorunları nedeniyle ortaya çıkan etkileri en aza indirir
- BT/BT güvenliğinin verimliliğini artırır ve operasyonel maliyetlerinizi optimize eder
- İşletmenizi sosyal mühendislik tabanlı çevrimiçi tehditlere karşı korur
- Belirli web kaynaklarına çevrimiçi erişimi kontrol ederek çalışan verimliliğinin artmasını destekler

Pratik Uygulamalar

- Uç nokta tabanlı savunmalarınızı ağ geçidi düzeyinde güçlendirir
- Hatalı pozitiflere neden olmadan mevcut web ağ geçidi güvenliğinizi tamamlar ve güçlendirir
- İş veya kullanım nedeniyle uç nokta düzeyinde tam olarak güvenli hale getirilemeyen cihazları korur
- Kaspersky tabanlı gelişmiş tehdit algılama araçlarınızı, ek bağlam ve otomatik ağ geçidi düzeyinde yanıt araçları ile güçlendirir

Kaspersky Security for Storage

Kolayca erişilebilen bağlı depolama alanları, tehditlerin tüm altyapınıza yayılabileceği bir kaynak ve fidye yazılımı gibi tehditler için bir hedef haline gelebilir. Kaspersky Security for Storage, kurumsal verilerinizi 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.

Hedefleriniz:

- Bağlı depolama alanlarını harici saldırılara ve bulaşan tehditlerin yayılmasına karşı korumak
- Bağlı depolama alanlarındaki değerli verileri fidye yazılımı saldırılarına karşı korumak
- Kaspersky çözümleriyle korunan uç noktalar ve sunucuların yanı sıra veri depolama güvenliğinizi de yönetmekse sizin için idealdir.

3 Gerekli beceriler

4 Özelleştirme ve ölçeklenebilirlik

3 Yatırım düzeyi

Kurumsal avantajlar

- Depolama alanlarını yayılma noktalası olarak kullanan kötü amaçlı yazılım salgınlarını önleyerek iş sürekliliğini korur
- Düzenlemeye tabi veri depolama alanlarınız için güvenilir koruma araçları sunarak uyumluluğu korumaya yardımcı olur
- Diğer Kaspersky uç nokta ve sunucu koruma çözümleriyle birleşik bir yönetim deneyimi sunarak operasyonel zorlukları azaltır

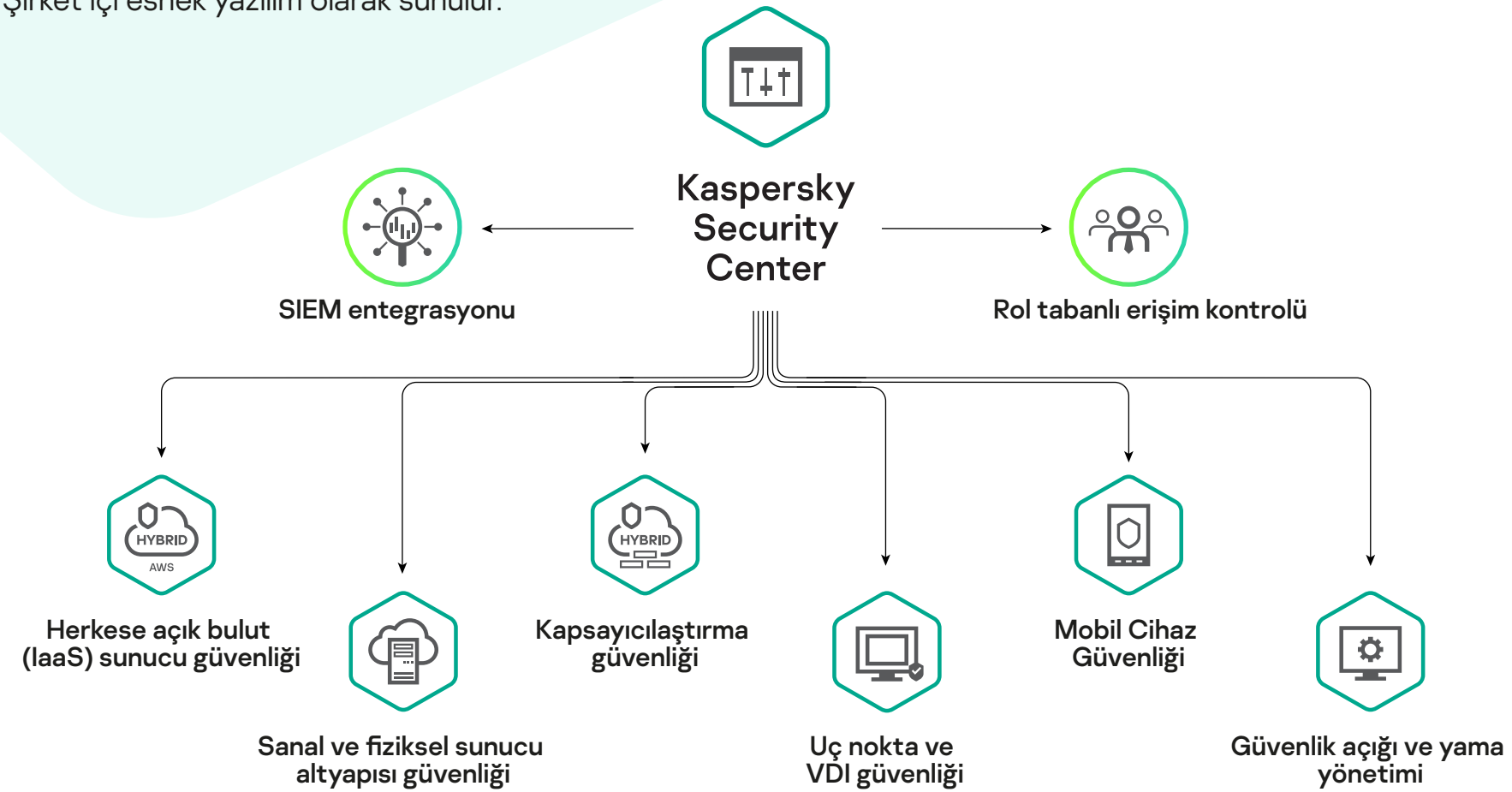
Pratik Uygulamalar

- NAS, DAS veya SAN'ı veya bunların altyapınızda kullanılan herhangi bir kombinasyonunu korur
- Hem depolama alanlarını hem de hepsi bir arada güvenlik çözümünü barındırmak için kullanılan sunucuyu korur
- Uzaktan çalıştırılan şifreleyici yazılımların neden olduğu veri kaybını önler

Tek bir pencereden güvenlik yönetimi

Birden çok görevin yönetimi ve ilke tabanlı kontrol için Kaspersky Security Center:

- Ölçeklenebilir SaaS hizmeti ve,
- Şirket içi esnek yazılım olarak sunulur.



Kaspersky Premium Support (MSA)

Bir güvenlik olayı meydana geldiğinde, nedeni belirlemek ve ortadan kaldırmak için geçen süre önemlidir. Sorunun hızla tespit edilip çözülmesi önemli maliyetlerden kurtulmayı sağlayabilir. Maintenance Service Agreement (MSA) planlarımız, bu hedefi gerçekleştirmek için özel olarak tasarlanmıştır. Uzmanlarımıza 7/24 erişim, garantili yanıt süreleriyle uygun ve bilinçli sorun önceliklendirme ve özel yamalar... Sorununuzun en kısa sürede çözülmesini sağlamak için gerekli her çözümü sunuyoruz.

Hedefiniz:

- BT sistemlerinizin, yalnızca sektör lideri güvenlik teknolojileri ile değil aynı zamanda uzman becerileri ve Kaspersky'nin dünyanın önde gelen uzmanlarının kararlılığı ile korunduğunun güvencesini yaşamaksa sizin için idealdir.

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 içinde sizin temsilciliğinizi üstlenir ve sorunu çözmek için gerekli uzmanları harekete geçirme yetkisine sahiptir

Pratik Uygulamalar

- Kritik sorunları, size hızlı bir şekilde doğru çözümü sunmak için en iyi donanıma sahip uzmanlara iletir
- Sisteminize uyarlanmış proaktif önlemlerle tam kapsamlı korunmayı sürdürmenizi sağlar
- Şirket içindeki değerli kaynaklarınızın bakım ve sorun giderme işlemleri için harcanan zamanı azaltır

1 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

3 Yatırım düzeyi

Kaspersky Professional Services

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 ürünlerini kurumunuzun BT altyapısında kullanma, yapılandırma ve yükseltme işlemlerine her açıdan yardımcı olmaya hazırdır.

Hedefiniz:

- En iyi siber güvenlik uygulama örneklerini karşılamak için Kaspersky çözümünüzü hızlandırmak, optimize etmek ve özelleştirmekse sizin için idealdir.

Kurumsal avantajlar

- Güvenlik çözümlerinin %100 kapasiteyle çalışmasını sağlayarak çözümlerinizin yatırım getirisini en üst düzeye çıkarır
- Şirket içi BT personeli maliyetlerini azaltır
- Herhangi bir yeni güvenlik çözümünün uygulanmasının günlük iş operasyonları üzerindeki etkisini en aza indirir ve genel uygulama maliyetlerini azaltır
- Ortaya çıkan kritik herhangi bir sorunun hızlı ve etkili bir şekilde çözülmesine yardımcı olur

Pratik Uygulamalar

- Korumanızı azaltabilecek, verimliliği etkileyebilen ve arıza süresine yol açabilecek, ürün uygulamalarından kaynaklanan riski azaltır
- En güncel savunma mekanizmalarının kullanılmasını sağlayan ürün yapılandırmalarının düzenli olarak denetlenmesiyle arıza süresi riskini en aza indirir
- Ürünün uyum süresini kısaltarak tüm faydaların hemen elde edilmesini sağlar

1 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

3 Yatırım düzeyi

2. Aşama
Optimum Güvenlik

Gelişmiş tespit ve merkezi yanıt

Temel Güvenlik tarafından organik şekilde oluşturulan kaynak bilinçli bir çözümle, daha küçük siber güvenlik ekiplerinin otomatik önlemeyi atlatan tehditlerle bile mücadele etmesini sağlar.

Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response (EDR) Optimum, temel düzeyde siber güvenlik uzmanlığına sahip işletmelerin bir dizi elden kaçabilen tehdidi ele almasına yardımcı olur. Kaspersky Endpoint Security for Business Advanced'in sahip olduğu koruma özelliklerini içerir ve Kaspersky Security Center'dan yönetilir. Kaspersky Endpoint Detection and Response (EDR) Optimum, basitleştirilmiş kök neden analizine, IoC (Risk Göstergesi) taramasına ve otomatikleştirilmiş veya 'tek tıkla' yanıt seçeneklerine dayalı, kullanımı kolay bir araç seti sağlar.

Hedefleriniz:

- Tüm uç noktalarınızda tehdit görünürlüğünü artırmak
- Ortalama yanıt sürenizi azaltmak
- BT güvenlik kaynaklarınızı optimize etmek ve verimliliği artırmaksa sizin için idealdir.

3 Gerekli beceriler

4 Özelleştirme ve ölçeklenebilirlik

3 Yatırım düzeyi

Kurumsal avantajlar

- Önleyici korumadan kaçan tehditlere ilişkin finansal, itibar risklerini ve diğer riskleri en aza indirir
- Kolaylaştırılmış iş akışı ve bir dizi otomasyon özelliği ile çalışanların iş yükünü ve kaynak kullanımını optimize etmeye yardımcı olur
- Derin bir uzmanlık ve uzmanlaşmak için çok zaman gerektirmeyen, düşük maliyetli, erişilebilir bir araçla verimliliği artırır

Pratik Uygulamalar

- Uç nokta güvenlik uyarılarının ayrıntılı görünürlüğünün keyfini yaşamanızı sağlar
- Ana bilgisayarda tespit edilen tehdidi daha ileri seviyede analiz ederek ölçeğini ve kök nedenini ortaya çıkarır
- Üçüncü taraf kaynaklardan içe aktarılan IoC'leri arayarak saldırı altında olup olmadığınızı öğrenmenizi sağlar
- Yalnızca birkaç tıklamayla, tehditlere keşfedildiği anda veya incelemeniz esnasında otomatik olarak yanıt vermeyi sağlar

Kaspersky Managed Detection and Response Optimum

Kaspersky Managed Detection and Response Optimum, ek personel veya uzmanlık yatırımı yapmanıza gerek kalmadan, hızlı ve ölçeklenebilir anahtar teslimi dağıtım yoluyla size anında kapsamlı bir BT güvenlik işlevi sunar. Patentli makine öğrenimi modelleri, benzersiz sürekli tehdit istihbaratı ve tescilli Saldırı Göstergeleri (IoA'lar) kullanan otomatik tehdit avı, işletmenizin bilinen taktikler, teknikler ve prosedürlerden yararlanarak karmaşık tehditlere karşı sürekli savunulmasını sağlar.

Hedefleriniz:

- 7/24 sürekli izleme kapsamı ile erken, etkili tehdit algılama ve yanıt oluşturmak ve geliştirmek
- BT güvenlik ekibinizin becerilerini artırma ve yeni çözümlerde uzmanlaşma konularında çok fazla zaman harcamadan, şirketinizin gelişmiş tehditlere karşı duyarlılığını hızla azaltmaksa sizin için idealdir.

Kurumsal avantajlar

- En yenilikçi tehditlere karşı bile sürekli korunmanızı sağlar
- Tüm olasılıkları karşılamak için şirket içi güvenlik uzmanı istihdam etmeye ve eğitmeye gerek kalmadan genel güvenlik maliyetlerini azaltır

Pratik Uygulamalar

- Ağlarınızı hedef alan tehditleri otomatik olarak önleyerek, tespit ederek, avlayarak ve bunlara yanıt vererek korumaya yönelik sistematik bir yaklaşım kullanmanızı sağlar
- Tüm yanıt eylemleri üzerinde tam kontrole sahip olurken, olaylara hızlı tepki vermenizi sağlar
- Tüm tespitlere, kapsam dahilindeki varlıklara ve mevcut koruma durumlarına tam gerçek zamanlı görünürlük elde etmenizi sağlar

Kaspersky Sandbox

Kaspersky Sandbox sizi, uç nokta korumasını atlamak için tasarlanmış yeni ve bilinmeyen tehditlerden otomatik olarak korur. Kaspersky Endpoint Security for Business'ı tamamlar ve işletmelerin yeni güvenlik personeli istihdam edilmesine gerek kalmadan, daha önceden bilinmeyen kötü amaçlı yazılımlar, yeni virüsler ve fidye yazılımları, sıfır gün açıkları ve diğer tehditlere karşı uç nokta ve sunucu koruma düzeylerini önemli ölçüde artırmalarına yardımcı olur.

Hedefleriniz:

- Elden kaçabilen tehditlere karşı savunmanızı güçlendirmek
- Gelişmiş algılamayı otomatikleştirmek
- Çalışanlarınızın iş yükünü ve uzmanlık gereksinimlerini optimize etmekse sizin için idealdir.

1 Gerekli beceriler

3 Özelleştirme ve ölçeklenebilirlik

2 Yatırım düzeyi

Kurumsal avantajlar

- BT güvenlik riskini azaltır ve iş sürekliliğini sağlar
- Uç nokta performansını veya kullanıcı verimliliğini etkilemeden yeni ve bilinmeyen tehditlere karşı korur
- Manuel işlemleri otomatikleştirerek iş gücü maliyetlerini en aza indirir
- Uzak ofislerin gelişmiş tehdit koruması için katlanılan maliyetleri optimize eder

Pratik Uygulamalar

- Bilinmeyen ve elden kaçabilen tehditlerin tespitini ve dinamik şekilde derinlemesine analiz edilmesini kolaylaştırır
- Korunan tüm uç noktalarda otomatik yanıt vermeyi sağlar
- Kaynak yoğun davranış analizinin yükünü korumalı alana aktararak çok fazla yüklenmiş olan uç noktaların güvenliğini artırır ve verimliliğin etkilenmemesini sağlar
- Bir API aracılığıyla üçüncü taraf çözümlerle entegre olur
- Basit kurulum ve korumalı alanınızın gelişmiş BT veya siber güvenlik personeli becerileri gerektirmeden tam otomatik şekilde çalışması sayesinde, mesai saatlerinden tasarruf etmenizi sağlar

Kaspersky Security for Enterprise

Kaspersky Threat Intelligence Portal

Kaspersky Threat Intelligence Portal, siber tehditler hakkında edindiğimiz tüm bilgileri tek ve güçlü bir web hizmetinde bir araya getiriyor. İster dosya, ister dosya karması, IP adresi veya URL olsun, şüpheli tehdit göstergelerini kontrol etmenizi sağlar. Portal, Kaspersky Security Network ile bilinirlik tespiti, yapısal makine öğrenimi modelleri ve Kaspersky Cloud Sandbox ile gelişmiş dinamik algılama gibi bir dizi gelişmiş tehdit algılama teknolojisiyle nesneleri analiz ederek bir nesnenin "İyi", "Kötü" veya "Kategorize Edilmemiş" bölgede olup olmadığını ortaya çıkarır. Sağlanan bağlamsal veriler, tehditleri daha etkili bir şekilde önceliklendirmenize ve yanıtlamanıza yardımcı olur.

Hedefiniz:

- Güvenilir bir tehdit istihbaratı kaynağına ücretsiz erişim kazanmak
- Olayları daha etkili bir şekilde önceliklendirmek
- İncelemeyi ve tehdit keşfini hızlandırmaksa sizin için idealdir.

Kurumsal avantajlar

- Ticari tehdit istihbaratının benimsenmesine yönelik yüksek maliyet engelini aşar
- %100 incelenmiş verilere zamanında erişmenizi sağlayarak ağlarınızın etkili bir şekilde korunmasına yardımcı olur

Pratik Uygulamalar

- Etki ve risk seviyelerine göre gerçek bir tehdit oluşturan uyarıları veya olayları doğrular ve önceliklendirir
- Olay müdahale ekibinize iletilmesi gereken uyarıları anında belirlemenizi sağlar
- Gerçek tehditleri anlamsız olanlardan ayırmanızı ve sınırlı olay müdahale kaynaklarınızı odaklayacağınız yerleri belirlemenizi sağlar
- Belirli bir gözlem veya saldırıya ait ayrıntılara ulaşmak için farklı veri tabanlarında karmaşık aramalar yapma ihtiyacını ortadan kaldırır
- Önceden tespit edilmemiş tehditleri keşfetmenizi sağlar

3 Gerekli beceriler

4 Özelleştirme ve ölçeklenebilirlik

0 Yatırım düzeyi

Kaspersky Security Awareness

Kaspersky Security Awareness, çalışanlarınızın siber hijyen becerilerini şekillendiren ve kurumsal yapının tüm seviyelerine hitap ederek güvenli uygulamaları sürdürmeleri yönünde motive eden, bilgisayar tabanlı oyunlaştırılmış eğitim ürünlerinden oluşan bir derlemedir. Bu çözüm,

- Katılım ve motivasyon için Kaspersky Interactive Protection Simulation ve CyberSafety Management Games,
- Doğru başlangıç noktasını belirlemek için Gamified Assessment Tool,
- Pratik beceriler kazanmak için Online Learning Platform ve Cybersecurity for IT Online,
- Yeni öğrenilen becerileri pekiştiren gündelik bir eğitici oyun olan [Dis]connected'tan oluşur.

Hedefleriniz:

- Çalışanların bilgisizliği veya ihmalini nedeniyle ortaya çıkan olayların sayısını azaltmak
- Her seviyedeki çalışanının doğru siber güvenlik önlemlerini konusunda bilgi sahibi olmasını sağlamak
- Kullanıma hazır çözümlerle işletmenize güçlü bir siber güvenlik kültürü kazandırmaksa sizin için idealdir.

Kurumsal avantajlar

- İnsanlarla kaynaklı güvenlik olaylarının sayısını azaltmaya, iş sürekliliğini sağlamaya ve bir olayın etkisini en aza indirmeye yardımcı olur
- İnsanları öğrenme konusunda teşvik ve motive eder ve yönetimi siber güvenlik önlemlerinin ve girişimlerinin destekçilerine dönüştürür
- İşletmeniz genelinde siber güvenlik kültürünü geliştirir

Pratik Uygulamalar

- Çalışanlarınızı, güvenli davranış şekillerini benimsemeleri ve sürdürmeleri için gereken beceriler ve bilgilerle donatır
- Siber güvenlik sorunlarına karşı sağlıklı bir kurumsal tutum geliştirir
- İşletmenizi siber risklere maruz bırakmadan, günlük sorumluluklarında daha iyi sonuçlar elde etmeleri konusunda çalışanlarınızı güçlendirir

3. Aşama
Uzman Güvenlik

Hedefli ve APT benzeri saldırılara hazırlık

Tehdit istihbaratı, uzman rehberliği ve bilgi aktarımıyla desteklenen genişletilmiş savunmalara odaklanır, gelişmiş BT güvenlik ekiplerini karmaşık tehditleri ve hedefli saldırıları yenmeleri konusunda güçlendirir.

Kaspersky Endpoint Detection and Response

Toplanan verilere hızlı erişim ile tam görünürlük, üst düzey tehdit algılama ve verimli analiz imkanı sunan, zengin özelliklere sahip, BT güvenlik uzmanları için güçlü bir EDR aracıdır. İnceleme süreciniz; geriye dönük analiz, tescilli Saldırı Göstergeleri (IoA) ve MITRE ATT&CK eşlemesinin yanı sıra proaktif tehdit avcılığı ve Kaspersky Tehdit İstihbaratı'na erişim ile desteklenir. Tüm saldırı dizisini ortaya çıkarır, uç noktaları hedefleyen çok aşamalı karmaşık saldırıları anlar, uygun ve hızlı yanıt verir!

Hedefleriniz:

- Uç nokta korumanızı güçlendirmek
- Ortalama algılama/yanıt verme sürenizi sürekli düşürerek, şirket içi olay müdahale yeteneklerinizi daha iyi hale getirmek
- Proaktif tehdit avlama işlemlerinizi artırmaksa sizin için idealdir.

4 Gerekli beceriler

3 Özelleştirme ve ölçeklenebilirlik

4 Yatırım düzeyi

Kurumsal avantajlar

- En değerli varlıklarınızı göz kulak olmanıza yardımcı olur
- Siber riski azaltır ve uç nokta olaylarının neden olduğu finansal ve operasyonel hasarı azaltır
- Uç nokta ile ilgili olay analizini ve yanıtını basitleştirerek operasyonel BT güvenliği maliyetlerinizi azaltır
- Yasal gereksinimlere uyum sağlanmasına yardımcı olur

Pratik Uygulamalar

- Uç nokta düzeyindeki gelişmiş saldırıların etkili bir şekilde tespit edilmesini (MITRE değerlendirmesiyle kanıtlanmış yeteneklerle) ve hızla yanıt verilmesini sağlar
- Merkezi olarak toplanmış veriler arasında geriye dönük analiz ve etkili araştırmalar yapılmasını sağlar
- Rehberli inceleme ve yanıtla olay yönetimini merkezileştirir
- Otomatik ve proaktif tehdit avlama yetenekleriyle gizli tehditleri avlar
- Kaspersky EDR, bir Extended Detection and Response çözümü oluşturarak Kaspersky Anti Targeted Attack Platform'un bir parçasını oluşturur

Kaspersky Security for Enterprise

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform, Threat Intelligence ve MITRE ATT&CK çerçevemiz tarafından desteklenen hepsi bir arada APT koruması sağlamak için Extended Detection and Response çözümü şeklinde davranarak ağ düzeyinde gelişmiş tehdit keşfi ve EDR yeteneklerini birleştirir. BT güvenlik uzmanlarınız, tek bir çözüm aracılığıyla, üstün çok boyutlu tehdit keşiflerini yönetmek, etkili incelemeler yapmak, proaktif olarak tehditleri avlamak ve hızlı, merkezi bir yanıt sunmak için ihtiyaç duydukları tüm araçlara sahip olur.

Hedefleriniz:

- Tek ve güçlü bir sistemle en karmaşık saldırılara karşı etkili genişletilmiş savunmalar oluşturmak
- Kurumsal çapta tam görünürlük elde etmek
- Ortalama algılama/yanıt verme sürenizi düşürmek
- Güvenlik Operasyon Merkezinizi güçlendirmek
- Gizliliğinizi korurken aynı zamanda güvenlik tutumunuzu geliştirmekse sizin için idealdir.

5 Gerekli beceriler

3 Özelleştirme ve ölçeklenebilirlik

5 Yatırım düzeyi

Kurumsal avantajlar

- Siber riski ve hedefli karmaşık saldırıların neden olduğu finansal ve operasyonel hasarı azaltır
- Olay yönetimi süreçlerini kolaylatırıp otomatikleştirerek operasyonel BT güvenliği maliyetlerini azaltır
- Yasal gereksinimlere uyum sağlanmasına yardımcı olur

Pratik Uygulamalar

- Hem ağ hem de uç nokta düzeyindeki birden çok potansiyel tehdit giriş noktasının güvenliğini sağlar
- Mevcut önleyici teknolojilerinizi atlatan gelişmiş tehditleri hızla keşfedilmesini sağlar
- Otomatik ve proaktif tehdit avlama yetenekleriyle gizli tehditleri avlamayı sağlar
- Daha derin bir inceleme yapmak için tespit edilen tehditler hakkında BT güvenlik ekibinize güncel bilgi sağlar
- Geniş kapsamlı otomatik senaryolar aracılığıyla karmaşık olaylara merkezi şekilde müdahale edilmesini sağlar

Managed Detection and Response Expert

Zaman alan ve kaynak tüketen olay önceliklendirme ve inceleme süreçlerinizin yönetimini bize devredin. Kaspersky Managed Detection and Response Optimum'un tüm özellikleri ve işlevselliği; bilinmeyen taktikler, teknikler ve prosedürleri (TTP'ler) kullanan tehditlere karşı yönetilen tehdit avlama, Kaspersky'nin SOC analistlerine doğrudan telefon üzerinden erişim, 3 aya kadar ham veri saklama, Kaspersky Threat Intelligence'a ayrıcalıklı erişim ve üçüncü taraf biletleme sistemleriyle entegrasyon sağlayan bir API ile bir araya gelerek, iş akışı yönetimi için harcamanız gereken zamanı önemli ölçüde azaltır.

Hedefleriniz:

- Şirket içi gelişmiş BT güvenlik ekibinizin sahip olduğu sınırlı süreden tasarruf etmek, böylece gerçekten müdahil olmalarını gerektiren kritik olaylara odaklanmalarını sağlamak
- Kaspersky'nin deneyimli uzmanlığıyla şirket içi en iyi uygulamalarınızı artırarak güvenlik ekibinizin verimliliğini artırmaksa sizin için idealdir.

2 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

5 Yatırım düzeyi

Kurumsal avantajlar

- Kendi Güvenlik Operasyon Merkezi'nizi oluşturmanıza gerek kalmadan bir Güvenlik Operasyon Merkezi'nin sunduğu önemli faydalara sahip olmanızı sağlar
- Kaspersky güvenlik çözümlerinizden elde ettiğiniz değeri en üst düzeye çıkarır
- Çeşitli şirket içi güvenlik uzmanlarını istihdam etmeye ve eğitmeye gerek kalmadan BT güvenlik kapasitesini anında artırarak genel güvenlik maliyetlerini ve bu alanda gelecekte ortaya çıkacak ek yatırım ihtiyacını azaltmaya yardımcı olur

Pratik Uygulamalar

- Kişiye özel uyarlanmış sürekli algılama, önceliklendirme, inceleme ve yanıt işlevi elde etmenizi sağlar
- Uzmanlarımıza danışarak ağlarınızda gözlemlendiğiniz tehditler hakkında destekleyici ek içerik edinmenizi sağlar
- Yeni edinilen tehdit istihbaratını kullanarak geriye dönük tehdit avı gerçekleştirmeyi sağlar
- Tehditler ve tehditlerin birbiriyle olan ilişkileri hakkında Kaspersky'nin sahip olduğu veri tabanında sorgulama yaparak olay incelemesini desteklemenizi sağlar

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence, olay yönetim döngüsü boyunca zengin ve anlamlı bağlam sağlar. Benzersiz ve hemen eyleme geçirilebilir bilgiler, mevcut güvenlik iş akışlarınızla sorunsuz entegrasyonu destekleyen farklı şekil ve biçimlerde sunulabilir. Portföy, tehdit istihbaratı akışları, sektöre ve tehdide özgü insanların okuyabildiği raporlar ve tehditler, meşru nesneler ve bunların çeşitli ilişkileri hakkında petabaytlarca veri içeren arama yapılabilir bir havuzdan oluşur.

Hedefleriniz:

- Önleme ve algılama yeteneklerinizi optimize etmek
- Reaktiften proaktif bir güvenlik tutumuna geçmek
- Tehdit istihbaratı programınızı geliştirmek
- Daha iyi bilgilendirilmiş stratejik güvenlik karar verme sürecini etkinleştirmekse sizin için idealdir.

4 Gerekli beceriler

5 Özelleştirme ve ölçeklenebilirlik

5 Yatırım düzeyi

Kurumsal avantajlar

- Analistlerin tükenmişlik sendromu yaşamasını önleyerek BT güvenlik personeli değişim oranını azaltmaya yardımcı olur
- Güvenliğin operasyonel verimliliklerini artırır, işlerin aksamasını ve olayların neden olduğu etkileri en aza indirir
- BT güvenlik yatırımınızı, tehdit ortamınızla uyumlu hale getirerek yatırım getirinizi optimize etmeye yardımcı olur

Pratik Uygulamalar

- Güvenlik çözümlerini sürekli güncellenen, makine tarafından okunabilen siber tehdit verileriyle güçlendirir
- Olay müdahale ekiplerine iletilmesi gerektiren kritik uyarıları belirleyerek uyarı önceliklendirmesini geliştirir
- Tespit edilen tehditler arasındaki ilişkileri ortaya çıkararak insan tarafından gerçekleştirilen incelemeleri destekler
- Net ve ilgili risk senaryoları sunarak BT güvenlik bütçenizi optimize eder

Kaspersky Cybersecurity Training

Sayıları sürekli artan gelişen tehditler karşısında beceri geliştirmek kuruluşlar için kritik önem taşır. BT güvenlik personeli; tersine mühendislik, YARA kuralları oluşturma ve dijital kanıtlarla çalışma gibi etkili kurumsal tehdit yönetimi ve risk azaltma stratejileri için merkezi olan gelişmiş teknikler konusunda gerekli becerilere sahip olmalıdır. Kaspersky Cybersecurity Training, şirket içi güvenlik ekibinizin sürekli gelişen tehdit ortamıyla mücadele etmek için gerekli uzmanlığı kazanmasına yardımcı olur.

Hedefleriniz:

- Şirket içi BT güvenlik uzmanlığı seviyenizi yükseltmek
- Güvenlik Operasyon Merkezi uygulamalarınızı güçlendirmek
- Dahili tehdit araştırma yetenekleri geliştirmekse sizin için idealdir.

4 Gerekli beceriler

3 Özelleştirme ve ölçeklenebilirlik

4 Yatırım düzeyi

Kurumsal avantajlar

- Güvenlik olaylarından kaynaklanan olası hasarı daha hızlı ve daha etkili bir şekilde azaltmak için SOC ekibinizin becerilerini güçlendirir
- Bulunması zor, alanında uzman personeli istihdam etme ve sonrasındaki şirketinizin tüm özelliklerini öğrenmesi süreci konusunda zaman ve para tasarrufu sağlar
- Beceriye dayalı kariyer gelişimini teşvik ederek şirket bünyesindeki personeli içeride tutmaya ve motive etmeye yardımcı olur.

Pratik Uygulamalar

- Tehdidin ve en etkili müdahale planını geliştirmenin tam olarak anlaşılması için kötü amaçlı yazılım analizi ile olay müdahalenizi destekler
- Bir olayın kök nedenini ortaya çıkarmak, gelecekte benzer olayları önlemek ve yasal yaptırımlardan kaçınmak için ana bilgisayar veya ağ sistemlerinde kanıt izinin sürülmesini sağlar
- Kurumsal ağlardaki çok çeşitli tehditlere karşı başarılı bir kurtarma sağlamak için ölçeklenebilir, hızlı ve etkili olay müdahale süreçlerini etkinleştirir

Kaspersky Cybersecurity Services

Kaspersky Cybersecurity Services, bilgi güvenliği olaylarına yanıt verme, geçmişteki ve devam eden ihlal girişimlerini açığa çıkarmanın yanı sıra, güvenlik açıklarını istismar edilmeden önce kapatma ve gelecekteki saldırıları önlemek için kurumsal çapta ve sektöre özel gerçekleştirdiği güvenlik değerlendirmeleri konusunda Kaspersky'nin sahip olduğu uzmanlığa erişim sağlar. Kaspersky uzmanlarıyla işbirliği yapmak, dahili BT güvenlik ekiplerinizin giderek karmaşıklaşan tehditlerle mücadele konusunda daha yüksek verimliliğe ulaşmasına olanak sağlar.

Hedefleriniz:

- Bir olayın yaşanması halinde arkanızı kollayan uzman bir ortağa sahip olmak
- Mevcut tespit ve önleme sistemlerinizin yeterli olup olmadığını anlamak
- Proaktif bir güvenlik yaklaşımı uyguladığınızdan emin olmaksa sizin için idealdir.

Kurumsal avantajlar

- Kanıtlanmış BT güvenlik uzmanlığına sürekli erişim sayesinde, ne kadar karmaşık olursa olsun olaylardan kaynaklanan hasarın en aza indirilmesini sağlar
- Olası arıza süresinin sebep olduğu masrafları önemli ölçüde azaltır ve olumsuz bir üne sahip olmaktan kaçınmayı sağlar
- Mevzuata tam uyumu destekler, cezalardan ve para cezalarından kaçınmaya yardımcı olur

Pratik Uygulamalar

- Sistemlerinizi ve işletme faaliyetlerinizi daha hızlı şekilde yoluna koymanızı sağlar
- İhlal girişimlerinin tespit edilmesini ve olayın etkisinin, ortaya çıkmadan önce azaltılmasını sağlar
- Sektöre özgü altyapıların güvenliğini artırır
- Savunma yeteneklerinizi değerlendirir ve ele alınması gereken zayıf noktaları belirler

Kaspersky Private Security Network

Kaspersky Private Security Network, kontrollü çevrenizin dışına hiçbir şekilde veri yayınlamadan küresel bulut tabanlı tehdit istihbaratından yararlanmanızı sağlar. Bu ürün, Kaspersky Security Network'ün işletmenize ait, yerel ve tamamen özel bir sürümüdür.

Hedefleriniz:

- Gizliliğe duyarlı bir şirketi uygulanacak katı politikalarla, herhangi bir verinin BT altyapısının sınırlarını terk etmesine karşı korumak
- En katı veri koruma düzenlemelerini karşılamak
- İşletmenizin korumasını güçlendirmek ve yanıt sürelerini kısaltmak için işletmeniz içinde tehdit istihbaratı paylaşımını kolaylaştırmaksa sizin için idealdir.

Kurumsal avantajlar

- Dahili bilgi paylaşımıyla desteklenen verimli algılama ve yanıtlama yoluyla iş sürekliliğini korur
- Hatalı pozitiflerin uzak tutulmasına yardımcı olarak operasyonel verimliliği artırır
- Yalıtılmış sistemlerin ve ortamların güvenliği için düzenleyici gerekliliklere uygunluğun sağlamasına yardımcı olur

Pratik Uygulamalar

- Tehdit algılama etkinliğinden ödün vermeden izole, hatta hava aralığına sahip altyapınızı korur
- Ulusal bir tehdit veri değişim aracı düzenlemeyi sağlar
- Mevcut Kaspersky gelişmiş tehdit algılama çözümlerinizi, kendi dahili tehdit istihbaratı ağınız aracılığıyla diğer Kaspersky B2B çözümleriyle entegre etmenizi sağlar

5 Gerekli beceriler

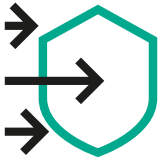
5 Özelleştirme ve ölçeklenebilirlik

5 Yatırım düzeyi

Uzun vadeli bir siber güvenlik stratejisi geliştirirken dikkat edilmesi gereken faktörler

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



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

Bir kuruluşun 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 çalışanın 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 etme 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 kuruluşların 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 başarı, her yıl tekrarlanıyor. www.kaspersky.com/top3

MITRE ATT&CK değerlendirmesi ile onaylanmış Kaspersky kalitesi

MITRE | ATT&CK®

Kaspersky bir kez daha Gartner Peer Insights Customers' Choice ödüllerinin Uç Nokta Koruma Platformları kategorisinde müşterilerin tercihi seçildi.

Kaspersky, "Gartner Peer Insights 'Voice of the Customer': EDR Solutions"da Customers' Choice (Müşterilerin Tercihi) seçilmiştir.

Kaspersky 2020 yılı Gartner Peer Insights Customer's Choice ödüllerinin Web Ağ Geçitleri kategorisinde müşterilerin tercihi seçildi.

Başarısını Kanıtlamış.
Şeffaf.
Bağımsız.

En şeffaf

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

kaspersky