Kaspersky Endpoint Detection and Response Optimum

Uç nokta savunmalarınızı bir sonraki seviyeye taşıyın ve sinsi tehditlerle doğrudan ve zahmetsizce mücadele edin.

kaspersky 25 years

Kaspersky Endpoint Detection and Response Optimum

Bir seviye atlama zamanı. Kuruluşunuzu yalnızca temel kötü amaçlı yazılımdan koruma teknolojileriyle korumaya değil, aynı zamanda geleneksel korumadan kaçmak ve kendilerini sistemlerinizin derinliklerine gömmek için kasıtlı olarak tasarlanmış ve en kötüsünü yapmaya hazır olan tehditleri belirlemeye, analiz etmeye ve etkili bir şekilde etkisiz hale getirmeye hazırsınız.

Zorluklar

Tehditlerin tespitten kaçması

Kaçınma amaçlı kötü amaçlı yazılımlar, fidye yazılımları, casus yazılımlar ve diğer tehditler, saldırmak için meşru sistem araçları ve diğer gelişmiş teknikleri kullanarak geleneksel algılama mekanizmalarından kaçınmada daha akıllı hale geliyor.

Hizmet Olarak Fidye Yazılımı

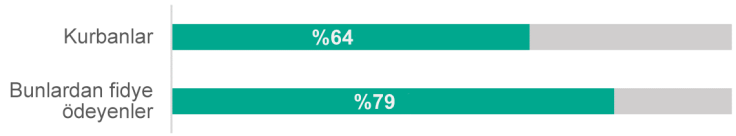
Bilgisayar korsanları, ucuza hazır araçlar satın alabilir ve herkese saldırabilir – veri çalabilir, altyapınıza zarar verebilir ve sürekli artan miktarlarda fidye talep edebilir.

Sınırlı kaynaklar

Altyapılar giderek daha karmaşık ve yaygın hale gelirken, kaynaklar – zaman, para ve dikkat süreleri – yetersiz kalıyor. Burada kullanıma hazır yazılım için yer yok.

Kurumların %64'ü halihazırda fidye yazılımı saldırılarının kurbanı olmuştur. Bunların %79'u fidyeyi saldırganlarına ödedi.

Kaspersky, Mayıs 2022



"Kaspersky'nin kapsamlı çözümlerine, güvenilirliğine ve hızlı servis ve desteğine değer veriyoruz. BT ortamımızın kullanılabilirliğini garanti ediyorlar."

Marcelo Mendes CISO, NEO
örnek olay incelemesini okuyun

Kaspersky Endpoint Detection and Response (EDR) Optimum, kullanımı kolay gelişmiş algılama, basitleştirilmiş araştırma ve otomatik yanıt sağlayarak kaçamak tehditleri belirlemenize, analiz etmenize ve etkisiz hale getirmenize yardımcı olur.

Gelişmiş koruma

Gelişmiş algılama mekanizmalarımız makine öğrenimi, davranış analizi ve bulut kum havuzu gibi teknolojileri içerir.

Basit görsel analiz araçları, tehdidi ve kapsamını tam olarak anlayabileceğiniz anlamına gelir – ve hızlı müdahale eylemleri, herhangi bir hasar oluşmadan önce saldırıyı durdurur.

Tek çözüm

Yeni nesil uç nokta güvenliği, dizüstü bilgisayarların, iş istasyonlarının, sunucuların, bulut iş yüklerinin ve sanal ortamların daha iyi korunması için kullanımı kolay EDR ile bir araya getirilmiştir.

Tüm bu dağıtım ve yönetim tek bir yerde, tek bir bulut veya şirket içi konsol aracılığıyla gerçekleşir.

Basit ve etkili

EDR Optimum'u daha küçük siber güvenlik ekiplerini düşünerek oluşturduk – olay müdahale yeteneklerini yükseltmek ve uzmanlık geliştirmek isteyen ancak ayıracak çok fazla zamanı olmayanlar için.

Çoğu görevi otomatikleştirir ve optimize ederiz, böylece gerçekten önemli şeylere harcayacak daha fazla zamanınız olur.

Temel avantajlar

- **Birden fazla tehdit** türünü önleyin
- **Sistemlerinizi ve verilerinizi sinsi tehditlere** karşı koruyun
- **Hareket** etmeden önce mevcut tehditleri yakalayın
- **Uç noktalarınızdaki sinsi** tehditleri tanıyın
- **Tehdidi anlayın** ve hızlı bir şekilde analiz edin
- **Hızlı bir otomatik müdahale** ile hasarı önleyin
- **Basit bir** araçla zaman ve kaynak tasarrufu sağlayın
- **Her son noktayı savunma:** dizüstü bilgisayarlar, sunucular, bulut iş yükleri

Temel özellikler

- Doğal **yeni nesil uç nokta güvenliği**
- **Makine öğrenimine** dayalı gelişmiş algılama
- **Uzlaşma Göstergesi** (IoC) taraması
- **Görsel inceleme ve analiz** araçları
- Gerekli tüm veriler **tek bir uyarı kartında**
- **Yerleşik müdahale** kılavuzu ve otomasyonu
- **Tek bulut veya şirket içi konsol** ve otomasyon
- İş istasyonlarını, sanal ve fiziksel sunucuları, VDI dağıtımlarını ve genel bulut iş yüklerini destekler

Temel kullanım durumları

Saldırı altında mıyım?

- **Bulut kum havuzu da dahil olmak üzere makine öğrenimine dayalı gelişmiş algılama**, tehditleri otomatik olarak algılar.
- **Gelişmiş tehditleri bulmak için securelist.com'dan veya diğer kaynaklardan IoC'leri** indirin ve tarayın.

Onu etkisiz hale getirebilir miyim?

- **Birden fazla yanıt seçeneği** kullanın – ana bilgisayarı izole edin, dosyanın yürütülmesini önleyin veya kaldırın.
- **Analiz edilen tehdidin işaretleri** için diğer ana bilgisayarları tarayın.
- **Bir tehdit keşfedildiğinde ana bilgisayarlar arasında otomatik bir yanıt** uygulayın (IoC).

Bazı beceri eğitimlerini nasıl alırım?

- **Uyarı kartındaki yanıt** kılavuzuna bakın.
- **Tehdit İstihbarat Portalı'na** ve en son TI'ye erişin.
- **Tehditleri analiz** ederken ve bunlara yanıt verirken uzmanlığınızı geliştirin.

Bu nasıl oldu?

- **Görsel bir süreç ağacındaki tehdidi analiz edin.**
- Eylemlerini **drill-down bir grafikte izleyin.**
- **Temel nedenini ve altyapıya** giriş noktasını anlayın.

Bunun tekrar olmasını nasıl durdururum?

- **Hangi IP'lerin ve web sitelerinin engelleneceğini, politikaların değiştirileceğini ve çalışanların eğitileceğini** bilerek öğrenilen bilgileri kullanın.
- **Gelecekte** bu tür tehditleri önlemek için kurallar oluşturun, örneğin dosya yürütmeyi önleyin.

Peki ya tüm emtia tehditleri?

- **Yeni nesil uç nokta güvenliği**, çoğu tehdidi anında durdurmak için hazır.
- **Güvenlik Açığı ve Yama Yönetimi** ile yama işlemlerinizi hızlandırın.
- **Uç nokta kontrolleri ile saldırı yüzeyini azaltma** ve ilke ayarlama işlemlerinizi otomatikleştirin.

Nasıl çalışır?

Hızlı bir demo için **bu videoyu inceleyin**.

Nereden geliyorsunuz?

Kötü amaçlı yazılımdan koruma yazılımınız var ama yeterli değil mi?

Uç nokta korumanızı artırın

İster Kaspersky ister 3. taraf uç nokta koruması kullanıyor olun, EDR'yi uygulamayı düşünmek için doğru zaman.

Bu sadece gelişmiş tespit ve önleme yetenekleriyle ilgili değil, aynı zamanda kaçamak tehditlere karşı hazırlıklı olmakla – onları tanımlamak, analiz etmek ve etkisiz hale getirmekle ilgili.

Optimum Seviye güvenlik kılavuzu ile kaçamak tehditlere karşı nasıl korunacağınız hakkında daha fazla bilgi edinin.

Halihazırda Kaspersky kullanıyor musunuz?

Güvenliğinizi optimize edin

Ürünlerimizi sürekli olarak geliştiriyoruz, bu nedenle bir yükseltme ile bizi tam olarak kullandığınızdan emin olun – veya buluta geçin ve sinir bozucu rutin görevleri tamamen unutun.

Kaspersky EDR Optimum'un son sürümünde:

- Uyarı kartında yönlendirmeli yanıt!
- Sistem Kritik Nesneleri yanıtı uygulamadan önce kontrol edin!
- Tehdit İstihbaratı dosya itibarı uyarı kartında!
- Sınırsız derinlikte süreç ağacı analizi!

Yeni özellikler hakkında buradan daha fazla bilgi edinebilirsiniz.

Kaspersky'de yeni misiniz?

Güvenliğinizi optimize edin

Dünya çapında binlerce işletme Kaspersky EDR Optimum'u kullanıyor, çünkü Kaspersky EDR Optimum güven veriyor:

- Tek bir üründe güçlü EPP ve temel EDR
- Daha küçük siber güvenlik ekipleri için tasarlanmış kullanımı kolay EDR yetenekleri
- Bulut veya şirket içi dağıtım ile hafif ve esnek bir çözüm

Kaçamak tehditlere karşı EDR ve MDR teknolojisine dayalı bileşik bir çözüm olan Kaspersky Optimum Security'yegöz atın.

Aşamalı bir yaklaşımla ilerleyin

Kullandığınız araçlar, siber güvenlik ve iş ihtiyaçlarınız ile ekibiniz ve kaynaklarınız için mükemmel bir uyum sağlamalıdır. Bu nedenle, kuruluşunuzun profiline bağlı olarak üç farklı seçenekle şu anda ana odak noktanız olan siber güvenlik düzeyini seçmenizi kolaylaştırdık.

Kaspersky Security Foundations

Tehditlerin büyük çoğunluğunu otomatik olarak engelleme.

- Emtia tehditlerinin neden olduğu olayların – tüm siber saldırıların büyük çoğunluğu – çok vektörlü otomatik olarak önlenmesi.
- Entegre bir savunma stratejisi oluş-turmada her boyut ve karmaşıklıktaki kuruluşlar için temel aşama.
- Küçük BT ekiplerine ve yeni ortaya çıkan güvenlik uzmanlığına sahip olanlar için güvenilir uç nokta koruması.

» Daha fazla bilgi edinin

Kaspersky Optimum Security

Aşağıdakilere sahipseniz, kaçınma tehditlerine karşı savunmalarınızı geliştirin:

- Temel siber güvenlik uzmanlığına sahip küçük bir Bilgi Teknolojileri güvenlik ekibi.
- Boyutu ve karmaşıklığı artan, saldırı yüzeyini artıran bir BT ortamı.
- Gelişmiş koruma ihtiyacının aksine, siber güvenlik kaynaklarının eksikliği.
- Bir olay müdahale yeteneği geliştirmek için artan bir ihtiyaç.

» Daha fazla bilgi edinin

Kaspersky Expert Security

Organizasyonlar için karmaşık ve APT benzeri saldırılara hazır olma:

- Karmaşık ve dağıtılmış BT ortamları.
- Eski bir Bilgi Teknolojileri güvenlik ekibine veya yerleşik bir Güvenlik Operasyonları Merkezine (SOC) sahip olanlar.
- Güvenlik olaylarının ve veri ihlallerinin yüksek maliyetleri nedeniyle risk iştahının düşük olması.
- Düzenleyici uyumluluğun önemli olduğu bir alanda faaliyet gösterenler.

» Daha fazla bilgi edinin

Hakkımızda

Dünya çapında yüz binlerce müşterisi ve iş ortağı olan, **şeffaflık ve bağımsızlık taahhüdünde bulunan küresel bir özel siber güvenlik şirketiyiz.** 25 yıldır **En Çok Test Edilen, En Çok Ödüllendirilen teknolojilerimizle** sizi güvende tutmak için araçlar geliştiriyor ve hizmetler sunuyoruz.

IDC

IDC MarketScape Worldwide İşletmeler için Modern Endpoint Security 2021 Satıcı Değerlendirmesi

Büyük Oyuncu

AV Testi

Gelişmiş Uç Nokta Koruması: Fidye Yazılımı Koruma Testi

%100 koruma

Radicati Group

Gelişmiş Kalıcı Tehdit (APT) Pazar Çeyreği

En iyi oyuncu

Daha fazlasına ihtiyacınız varsa

Uzmanlarınızı derinlemesine tehdit avlama yetenekleri, geniş kapsamlı özelleştirme ve üstün tespit mekanizmaları ile donatmak için güçlü bir EDR aracı olan **Kaspersky EDR Expert'e** göz atın.

Daha yakından bakın.

Kaspersky EDR Optimum'un güvenlik ekibinizin ve kaynaklarınızın işini kolaylaştırırken siber tehditleri nasıl ele aldığı hakkında daha fazla bilgi edinmek için www.kaspersky.com/enterprise-security/edr-security-software-solution adresini ziyaret **edin**

Siber Tehdit Haberleri: securelist.com
BT Güvenlik Haberleri: business.kaspersky.com
KOBİ'ler için BT Güvenliği: kaspersky.com.tr/business
Kurumlar için BT Güvenliği: kaspersky.com.tr/enterprise

kaspersky.com.tr