kaspersky GELECEĞİ YAKALAYIN

Kaspersky Endpoint Detection and Response Optimum

Anlık otomatik yanıt ve basit kök neden analizi ile gerçek ve kapsamlı savunma oluşturun

Sorun

2019 yılı boyunca tüm işletmelerin **%91'i** siber saldırılardan etkilendi; bunların **10'da 1'i** ise hedefli bir saldırı[1] ile karşı karşıya kaldı.

Karmaşık tehditler aksama yaratır

Basit kötü amaçlı yazılımların etkili olduğu günler çoktan geride kaldı. İşletmeler için daha fazla aksama ve daha fazla kayba neden olan tehditler çok daha karmaşık hale geldi; üstelik artık uzun süre fark edilmeden kalabiliyorlar.

Saldırı altındasınız

Bu karmaşık tehditler çok daha yaygın ve sık görülür hale geldiği için kendini güvende hisseden işletmelerin artık kendilerini güvenceye alması gerekiyor.

Verimlilik olmazsa olmaz

Başta zaman ve beceri sahibi personel eksikliği olmak üzere değerli kaynakların eksikliği ise bu yangına körükle gidiyor.

Size nasıl yardım ediyoruz?

«Zayıf bir EPP çözümü EDR aracının değerini yok eder»[2]

«Dolayısıyla EDR araçlarının yeni yatırım getirisi artık insanlar ve zaman»[2]

Kaspersky Endpoint Detection and Response (EDR) Optimum; gelişmiş algılama, basitleştirilmiş araştırma ve otomatik yanıt özellikleriyle karmaşık ve gelişmiş tehditler karşısında güvende kalmanıza yardımcı olur.

Temel becerilerin ötesinde

Sadece tehdidi tespit etmekle kalmayıp aynı zamanda tüm kapsamını ve kökenlerini ortaya çıkarıp anında yanıt vererek iş kesintisini önler; derin görünürlük, basit araştırma araçları ve otomatik yanıt seçenekleri sunar.

Gerçek derinlemesine savunma

Kaspersky Endpoint Security for Business'ın eşsiz uç nokta koruma özellikleri ve gelişmiş algılamasıyla birlikte kullanımı kolay, üst düzeyde otomatik algılama ve yanıt araç seti sunarak birleşik tek bir çözüm oluşturur.

Akıllı araç, verimliliği garanti eder

Basit merkezi kontroller ve yüksek düzeyde otomasyon sağlayarak harcanan zamanı azaltmanın yanı sıra, insan gücü kaynaklarını ve genel BT giderlerini optimize eder. Tek bir konsoldan yönetilen, hem şirket içi hem de bulut için erişilebilir iş akışı[3].

Önemli avantajlar

- Kendinizi daha sık görülen, daha yıkıcı gelişmiş ve karmaşık tehditlere karşı koruyun
- Basit ve otomatik bir araçla zamandan ve kaynaklardan tasarruf edin
- Tüm ağ üzerindeki karmaşık tehditlerin tamamını görün
- Tehdidin kök nedenini ve nasıl ortaya çıktığını anlayın
- Hızlı otomatik yanıt sayesinde daha fazla hasardan kaçının

Önemli EDR kullanım örnekleri

Önemli soruları cevaplayın

- Uyarının bağlamı nedir?
- Uyarıyla ilgili halihazırda hangi eylemler gerçekleştirildi?
- Tespit edilen tehdit hala aktif mi?
- Diğer ana bilgisayarlar saldırı altında mı?
- Saldırı hangi yolu izledi?
- Tehdidin kök nedeni nedir?

Tehdidin tüm kapsamını öğrenin

Küresel bir tehdit altında olduğunuzu öğrendiğinizde (örneğin, düzenleyici otorite sizden risk göstergeleri için tarama yapmanızı isterse) şunları yapabilirsiniz:

- Risk göstergelerini güvenilir kaynaklardan içe aktarabilir ve saldırı işaretleri için düzenli taramalar gerçekleştirebilirsiniz.
- Bir uyarıyı iyice araştırabilir, keşfedilen tehditlere dayalı risk göstergeleri oluşturabilir ve diğer ana bilgisayarların etkilenip etkilenmediğini öğrenmek için tüm ağda taramalar yapabilirsiniz.

Çabuk yayılan tehditlere anında yanıt verin

- Karmaşık tehditlerle ilişkili dosyaları tüm uç noktalarda otomatik olarak karantinaya alın.
- Etkilenen ana bilgisayarları, hızla yayılan bir tehdide ilişkin bir risk göstergesi bulmak üzere otomatik olarak izole edin.
- İnceleme sırasında kötü amaçlı dosyanın çalışmasını ve ağa yayılmasını önleyin.

[1] Kaspersky Lab Küresel BT Riski Raporu, Kaspersky, 2019

[2] IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, Doc # US45794219, 2020"

[3] Bulut konsolu üzerinden yönetilebilen özelliklerde ve işlevlerde bazı kısıtlamalar vardır. Ayrıntılı bilgi için lütfen https://kas.pr/epp-management-options adresini ziyaret edin.

Artık:

Tehdidin tüm kapsamını görebilirsiniz

Uç noktalarınızdaki güvenlik uyarılarını görebilir ve tehdidin tam genişliğini ve derinliğini anlamak için bunları daha fazla analiz edebilirsiniz. Bu, olayların tamamen kontrol altına alınmasına yardımcı olur ve uç noktada tehditten hiçbir iz kalmaz.

İş akışınızı basitleştirebilirsiniz

Hem şirket içi hem de bulutta bulunan tek bir konsoldan kolaylaştırılmış iş akışının yanı sıra, ayrıntılı inceleme, risk göstergesi tarama ve çok fazla siber güvenlik uzmanlığı veya süresi gerektirmeyen yanıt seçenekleri de dahil olmak üzere basit EDR senaryoları ve kontrolleri.

Savunmanıza destek verebilirsiniz

Ek olarak Kaspersky Sandbox'ın eklenmesi; ürün tehditlerine, karmaşık tehditlere ve elden kaçabilen tehditlere karşı basit, etkili ve yüksek düzeyde otomatikleştirilmiş çok katmanlı savunma sağlayan eksiksiz bir Entegre Uç Nokta Güvenliği çözümü oluşturur.

Zenginleştirilmiş uyarı verilerini analiz edebilirsiniz

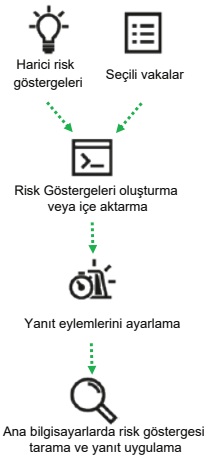
Kaspersky EDR Optimum, olayları gerekli bilgilerle zenginleştirir ve saldırının yayılma yolunu görselleştirerek farklı olaylar arasındaki bağlantıları anlamanıza yardımcı olur.

İçe aktarılan veya oluşturulan Risk Göstergeleri otomatik olarak taranarak ağdaki tüm ana bilgisayarlarda görünürlük sağlanır.

Otomatik olarak yanıt verebilirsiniz

Risk göstergesi taramalarına dayalı olarak tüm uç noktalarda bulunan tehditler için otomatik yanıtlar ayarlayın veya 'tek tıklama' seçeneğiyle keşif üzerine olaylara anında yanıt verin.

Ana bilgisayarı ayırma, karantina dosyası, ana bilgisayarın taramasını başlatma ve dosyanın yürütülmesini engelleme, yanıt seçenekleri arasındadır.



Diğer EDR Seçenekleri

Kaspersky Endpoint Detection and Response Optimum, belirli müşteri ihtiyaçlarına yönelik sunduğumuz çeşitli EDR seçeneklerinden biridir. Ayrıca şunları da inceleyebilirsiniz:

Kaspersky Endpoint Detection and Response

Gelişmiş BT güvenlik ekiplerine sahip BT organizasyonları için mükemmel olan, sektör ve müşteri tarafından en çok beğenilen, en gelişmiş ileri düzey ve hedefli saldırıların üstesinden gelmeye yardımcı olan uzman EDR çözümü. Gelişmiş tehdit keşfi, güçlü inceleme, proaktif tehdit avcılığı ve merkezi olay müdahalesi sağlar.
https://www.kaspersky.com/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

20 yılı aşkın süredir sürekli olarak olağanüstü tehdit araştırmalarıyla desteklenen, tamamen yönetilebilir ve kişiye özel uyarlanmış 24 saat algılama, önceliklendirme, araştırma ve yanıt; bizzat sizin kurmanıza gerek kalmadan kendi güvenlik operasyon merkezinize sahip olmanın tüm önemli faydalarını elde etmenizi sağlar.
https://www.kaspersky.com/enterprise-security/managed-detection-and-response

Kaspersky Endpoint Detection and Response Optimum'un güvenlik ekibinize ve kaynaklarınıza fazla yüklenmeden siber tehditlere nasıl yanıt verdiğiyle ilgili daha fazla bilgi edinmek için şu adresi ziyaret edin:
http://www.kaspersky.com/enterprise-security/edr-security-software-solution

Siber Tehdit Haberleri: www.securelist.com
BT Güvenliği Haberleri: business.kaspersky.com
İşletmeler için BT Güvenliği: kaspersky.com/enterprise
Tehdit İstihbarat Portalı: opentip.kaspersky.com

www.kaspersky.com.tr

Başarımız kanıtlanmıştır. Bağımsızız. Şeffafız. Teknolojinin hayatımızı iyileştirdiği daha güvenli bir dünya inşa etmeye kararlıyız. Bu yüzden teknolojiyi güvenli hale getiriyoruz; böylece, sunduğu sayısız fırsatlardan herkesin her yerde faydalanmasını sağlıyoruz. Daha güvenli yarınlar için siber güvenliği sağlayın.

Proven.
Transparent.
Independent.