Uç nokta güvenliğiniz için entegre çözümler

Sınırlı kaynaklarla güçlü savunmalar oluşturmak

kaspersky

Daha fazla bilgi için kaspersky.com.tr
#geleceğiyakalayın

Giriş

Boyutlarına, konumlarına veya faaliyet gösterdikleri alanlara bakılmaksızın birçok kuruluş, konu siber saldırı olduğunda, saldırıya maruz kalıp kalmayacaklarına değil, ne zaman saldırıya uğrayacaklarına odaklanmaları gerektiğinin farkında. Hiçbir şirket saldırıya karşı dayanıklı olduğunu düşünmemelidir.

Ancak mevcut tehdide ve güvenlik ortamına yön verecek süreye, kaynaklara veya (dürüst olmak gerekirse) motivasyona sahip olmak; bu da tümüyle ayrı bir konu.

Birçok güvenlik analisti (sayıları çok değil), mevcut haliyle dahi bu konu üzerinde çok çalışıyor. Yeni çalışanlar ve onların cihazlarını kontrol etmek, yeni yasaları ve uyumluluk sorunlarını anlamak, en yeni tehditler hakkında bilgi edinmek; tüm bu görevlerin asıl kurumsal koruma işinden önce yapılması gerekir.

Temel olarak, sayıları oldukça az güvenlik uzmanı, yeni ve egzotik tehditleri arayıp bulmak ve onları yanıtlayacak vakti buluyor.

Siber güvenlik tedarikçileri ve onların sunduğu ürünler ve çözümler de tam bu noktada devreye giriyor. Görevimiz zaman ve para ile yüksek maliyetli ve bulması zor olan uzmanlık da dahil olmak üzere en düşük ölçüde kaynak harcaması yaparak altyapınızı tümüyle korumak ve kullanıcılarınızı güvende tutmaktır.

Zorluklar

Öncelikle, günümüzde BT ve BT güvenlik yöneticilerinin karşılaştığı sorunlara göz atalım.

Artan gelişmiş ve hedefli saldırı tehdidi

Hedefli saldırılar ve karmaşık tehditler, sürekli olarak artan büyük bir sorundur. Siber suçlu araçları o kadar ucuz ve erişilebilir bir hal aldı ki bilgisayara sahip herkes gelişmiş düzeyde bir saldırı düzenleyebiliyor. Bu nedenle de, gelişmiş tehditler açısından bir zamanlar "göz önünde" olmadığını düşünen şirketler işlerin değiştiğini zor yoldan öğreniyor.

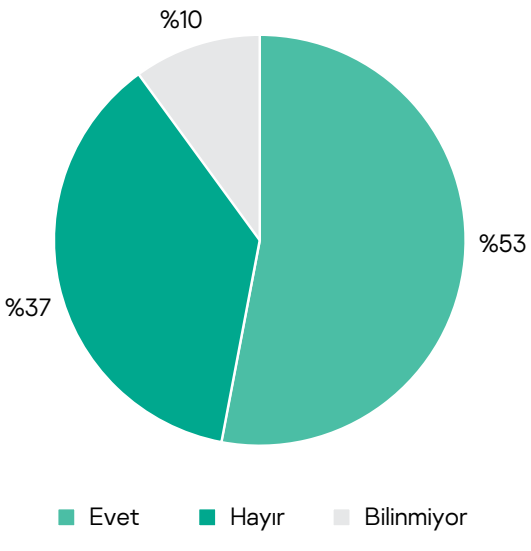
Buna ek olarak, emtia tehditleri de halen varlığını gösteriyor; bu saldırıların sahip olduğu büyük hacim günümüz dünyasında bir sorun olmaya devam ediyor.

Siber tehditlerin büyük bölümü ya uç noktadan içeriye giriyor, ya da bu noktayı tetiklemek üzere tasarlanıyor (bazen her ikisi de).

Dolayısıyla, varlıklarınızı korumak için yapabileceğiniz en yöntemlerden biri de uç noktalarınızı korumaktır.

SANS Institute tarafından yapılan bir çalışmaya[2] göre, kuruluşların uç noktalarının %53'ü ve %10'u güvenliklerinin ihlal edildiğini bilmiyor.

Uç nokta gizliliğinin bozulma oranları



Kuruluşların **%91**[1]'i 1 bir yıllık süre içerisinde en bir saldırıya maruz kaldı.

Her **10**[1] şirketten **1**'i kuruluştan biri aynı süre içerisinde bir fark edebildiği hedefli saldırıyla karşılaştı.

- Kuruluşların **%53**[2]'ü uç noktalarının güvenliğinin tehlikede olduğunu biliyor
- Kuruluşların **%30**[1]'u halen tam anlamıyla bir kötü amaçlı yazılım karşıtı program kullanmıyor
- İhlallerin **%56**[3]'sının ortaya çıkarılması bir ay ve daha uzun zaman aldı

Her **3 kuruluştan 2'si**[4] bilgi güvenliği personeli eksikliği yaşıyor.

2021 yılına gelindiğinde **3.5 milyon**[5] siber güvenlik pozisyonunun boş olacağı öngörülüyor.

1 Kaspersky Lab Global BT Riski Raporu, Kaspersky, 2019

2 Yeni Nesil Uç Noktası Riskleri ve Koruma, The SANS Institute, 2017

3 2019 Veri İhlali Araştırmaları Raporu, Verizon, 2019

4 Siber güvenlik işgücü çalışması, (ISC)² 2019,

5 Resmi Yıllık Siber Güvenlik İşleri Raporu, Siber Güvenlik Girişimleri, 2019

İnsan hatası

Ne yazık ki, uç noktalarınızın birçoğunda her kuruluşun altyapısındaki en savunmasız bileşen yer alır; kullanıcı. Kullanıcılarınız kurumsal verilerinize düzenli olarak uzaktan ve cihazlarından erişiyor olabilir. Bunun yanında birçoğu da çevrimiçi dünya içerisinde yetişirken zararlı alışkanlıklar ve gereğinden fazla öz güven kazanmıştır. Birçok şeyin yanında, kullanıcılarınızın korunması gerekir.

Bu nedenle, günümüzün karmaşık BT ortamlarında güvensiz davranışları tespit etmek ve önlemek de baskı altındaki güvenlik uzmanları için bir iş daha oluyor.

BT uzmanları da hata yapabilir, hepimiz insanız. Örneğin bu hatalar yanlış yama yapılan kurumsal ve kişisel cihazlarda oluşan güvenlik açıkları üzerinden saldırıya maruz kalınmasına sebep olabilir.

Kaynaklar ve eksiklik

BT uzmanlarının yapması gereken çok görevi olduğu ortadadır.

Küçük ölçekli şirketlerde dahi, doğru zamanda incelenmesi, analiz edilmesi ve yanıtlanması gereken güvenlik olaylarının hacmi artmakta. Siber suçlular işletmelerin bu noktada sorun yaşadığının farkında ve bu durumdan faydalanıyorlar.

Maddi açıdan iyi bir konumda olan şirketler için dahi, eğitimli siber güvenlik uzmanı bulmak konusunda küresel ölçekte bir sorun yaşanıyor. Bu yeni bir sorun değil ancak her yıl eğitime tabi tutulan uzman sayısı ele alındığında, bu problem yakın zamanda sona erecekmiş gibi görünmüyor.

Mevcut koşullarda güvenlik uzmanlarınızın mutluluğunu ve odaklanmasını sağlamak, hatta bu çalışanlarınızı bünyenizde tutmak bir zorluk haline gelmiştir. Oldukça yetenekli olan ve yüksek maliyetli eğitimlere tabi tutulan ekibinizin tüm günü sıradan görevleri yapmakla geçtiğinde, tükenme ve yıpranma önemli bir konu oluyor.

Ek olarak, finansal kaynaklar sorunu da bulunuyor. Ve işlemci gücü. Ve işleme hızı, çalışan verimliliği, kullanıcı memnuniyeti ve bütçeler üzerinde herhangi bir etki yaratmadan güvenliğinizi optimize etmek için gerekli olan her şey.

Çözüm

Peki çözümler neler?

Etkili koruma

Öncelikle, her şey **etkili uç nokta korumasına** bağlıdır; aslında yanıt bu kadar basit. Tehditleri uç nokta düzeyinde, henüz uyarı tetiklemeden önce önlemek kaynaklar üzerindeki stresi azaltır, yapılan bir saldırının başarılı olması riskini düşürür ve işin sorunsuz ve güvenli şekilde ilerlemesine yardımcı olur.

Bu durum hem genellikle gerçekleşen emtia saldırıları, hem de başarılı olma ve en fazla hasarı verme olasılığına sahip hedefli saldırılar için geçerlidir. Bizim önerdiğimiz yaklaşım ise, emtia saldırılarına karşı sağlam bir zemin koruması olan çok **katmanlı uç nokta savunmaları** ile daha karmaşık tehditlere karşı katmanlı, çok yüzlü savunmaların bir kombinasyonudur.

EDR (Uç Nokta Tespit ve Yanıt) bir sonraki kritik güvenlik katmanını sunar. EPP (Uç Nokta Koruma Platformu) ilk tanımlama ve korumayı sunarken, EDR de saldırının nasıl başladığını ve şu anda hangi aşamada olduğunu anlamanızı sağlamak üzere görünürlük ve daha kapsamlı analiz seçenekleri sunar. Tespit özelliğinin yanı sıra EDR, tehdidin hızlı şekilde ortaya çıkarılması ve etkili şekilde sınırlanabilmesi için proaktif yanıt seçenekleri de sunar.

EDR yalnızca sağlam bir koruma zeminiyle birlikte kullanıldığında etkili olacaktır. EPP çözümünüz ilk aşamada ne kadar vakayı çözüme ulaştırırsa, EDR çözümünüzün üzerinde çalışması ve kaynaklarınızın odaklanması gereken daha az sorun olacaktır.

İnsan davranışlarını ele almak

Kullanıcı gözünden bakıldığında, insan hatasını önlemenin en iyi yollarından biri tabii ki fırsatı ve isteği **uygulama, web ve cihaz kontrolleri** aracılığıyla ortadan kaldırmaktır. Etkili kontroller, işletme üzerinde hiçbir kısıtlılık oluşturmadan, örneğin vakit alan ve potansiyel olarak tehlikeli eğlence web sitelerini ve sosyal medyayı engelleyerek verimliliğin artmasını sağlayabilir.

Ancak bu noktada, kullanıcı eğitimi temel konudur. Doğru **siber güvenlik farkındalık eğitimi,** kurumsal kültürü değiştirerek, kurumsal riski önemli ölçüde düşürerek ve BT Departmanının iş yükünü büyük oranda azaltarak çalışan davranışı üzerinde büyük bir etki yaratabilir.

Yatırımınızın geri dönüşü

Son olarak, her tür yaklaşım şu anda, gelecekte, sınırlı kaynakların olduğu ve sınırlı güvenlik uzmanı bilgisinin bulunduğu ortamlarda ROI oranı ve maddi açıdan kendini kanıtlamalıdır.

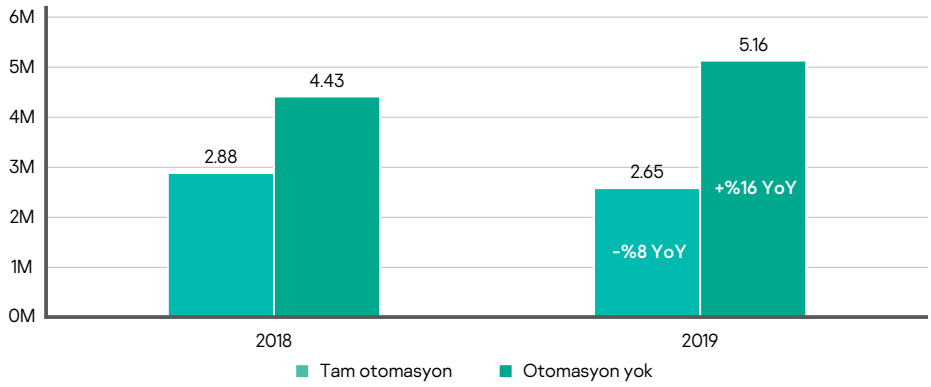
Otomasyon ve hızlandırma

Tehdit hacimlerindeki artış ve sektördeki güvenlik uzmanı sayısındaki azalış göz önüne alındığında, uygun olan her noktada **güvenlik görevlerinin otomatikleştirilmesi** kritik önem taşımaktadır. Bu sayede güvenlik uzmanlarınız, değerli vakitlerini ve yeteneklerini gerçek insan girdisi ve uzmanlığı gerektiren vakalar üzerinde çalışmaya ayırabilir ve sonuç olarak daha mutlu ve motive kalırlar.

Görevlerin otomatikleştirilmesi insan hatası faktörünü de ortadan kaldırır. Örneğin sistem güvenlik açıklarının otomatik olarak önceliklendirilmesi ve yama uygulanması, insanların bu kritik önem taşıyan ancak hiç de heyecan verici olmayan bu eylemi gerçekleştirmesinden çok daha etkili olacaktır.

Doğrudan dağıtım ve merkezileştirilmiş, modern hale getirilmiş **yönetim konsoluda** zamandan ve kaynaklardan tasarruf edilmesini sağlar. Operasyonlar esnasında konsollar arası geçiş yapmak ve komutları aramak yalnızca vakit alan ve can sıkıcı birer iş değil, aynı zamanda da yönetici hatası ve ihmaline zemin hazırlayan işlemlerdir.

Maliyetler
güvenlik otomasyon düzenine göre



Güvenlik otomasyonuna sahip olmayan kuruluşların önleme maliyetleri %16[6] oranında artarken, otomasyona geçen kuruluşların maliyetleri ise %8[6] oranında düşmüştür.

6 Bir Veri İhlalinin Maliyeti Raporu 2019, Ponemon Institute, 2019

Çok katmanlı korumaya ilişkin bir not

Gelişmiş ve hedefli saldırılar da dahil olmak üzere her tür siber tehdide karşı koruma sağlamayı hedefleyen çözümlerin çok katmanlı olması gerektiğini daha önce belirtmiştik.

Çözüm, ilk olarak web, uygulama ve cihaz engelleme ve sınırlama özellikleri bulunan uç nokta kontrollerine ve sağlamlaştırılmış kötü amaçlı yazılım karşıtı bir motora sahip **sağlam bir zemin uç nokta koruması** sunmalıdır. BT personelinin rutin görevleri gerçekleştirirken zamandan ve efordan tasarruf edebilmesi için, bu çözümün otomatikleştirilmiş yama yönetimi ve güvenlik açığı değerlendirme özelliklerine de sahip olması tercih edilir.

Ancak gelişmiş kötü amaçlı yazılımlar, daha ileri düzey güvenlik katmanları gerektiren ilave zorluklar ortaya çıkarmaktadır. Kötü amaçlı yazılım, doğru fırsat ortaya çıkana kadar gizli ve beklemede kalarak en gelişmiş uç nokta tespit mekanizmalarını dahi atlatmak üzere özel olarak tasarlanmış olabilir. Bu noktada yanıt, kötü amaçlı yazılımın güvenli ve kontrol edilen bir ortamda kendini ortaya çıkarması için yönlendirmekten geçer. Bu aşamada ise **sandbox** devreye girmektedir. Günümüzdeki bulunan bazı sandbox'lar tespit edilen tehditleri hızlı ve otomatikleştirilmiş şekilde yanıtlayabilir.

Uç noktalardaki karmaşık davranışları tespit etmek aynı zamanda **EDR** sisteminin odağındadır. EPP'de olduğu gibi EDR de ideal olarak, gerekli olan durumlarda insan girdisini desteklemek üzere otomasyon araçlarıyla görünürlüğü bir araya getirmelidir. Güvenlik analistleri, tehditleri manuel ya da otomatikleştirilmiş yanıt seçeneklerini kullanarak yanıtlayabilmek için vakalar üzerinde temel neden analizi gerçekleştirebilmelidir.

EPP, Sandbox ve EDR teknolojilerinin bir araya getirilmesi sayesinde, emtia kötü amaçlı yazılımları hızlı ve etkili şekilde ele alınır, insan hatası faktörü sınırlanır ve yeni, bilinmeyen ve sıfır gün tehditlerinin dahi tespit edilmesine ve yanıtlanmasına imkan vererek gelişmiş ve hedefli saldırıların başarılı olması riski azaltılır.

Tüm bu işlemler için entegre bir çözüme sahip olmanız, araçları arasında bilgisayar korsanları ve saldırganların faydalanabileceği hiçbir boşluk kalmayacağı anlamını taşır.

Kaspersky çözümü

Kaspersky Uç Nokta Güvenliği olarak, uç nokta koruması ve kontrollerinden, otomatikleştirilmiş bir sandbox'dan, bir EDR'den ve opsiyonel siber güvenlik farkındalık eğitim platformundan oluşan yüksek düzeyde otomatikleştirilmiş entegre bir çözüm oluşturduk.

Güçlü zemin uç nokta koruması

Kaspersky Endpoint Security for Business, piyasada en çok teste tabi tutulmuş ve en çok ödül alan kötü amaçlı yazılım karşıtı motorunu kullanan, yüksek düzeyde sağlam bir EPP (fidye yazılım ve dosyasız saldırılara karşı koruma da dahil olmak üzere) sunan ve oldukça köklü bir çözümdür.

Kaspersky Endpoint Security for Business tarafından sunulan uç nokta koruma katmanları arasında şunlar yer alır:

- Ödüllü kötü amaçlı yazılım karşıtı motorumuz
- Fidye yazılım tespiti ve koruması
- Otomatik Geri Alma özellikli Davranış Tespiti: Dosyasız kötü amaçlı yazılım ve yönetici hesabı ele geçirme ve yapılan değişiklikleri geri alma da dahil olmak üzere gelişmiş tehditleri tanımlar ve engeller.
- Mobil tehdit savunmaları ve EMM entegrasyonu
- IPS/HIPS
- Koruma duvarı ve işletim sistemi koruma duvarı yönetimi
- Kaspersky Security Network tehdit istihbaratı
- Şifreleme - işletim sistemine yerleşik şifreleme yönetimi dahil
- Güvenlik Danışmanı - optimize edilmiş güvenlik ayarları üzerinde yapılan değişiklikleri izler
- Otomatikleştirilmiş güvenlik açığı ve yama yönetimi
- İşletim sistemi ve 3. taraf yazılım yüklemesi
- SIEM sistemleri entegrasyonu

Ayrıntılı kontroller

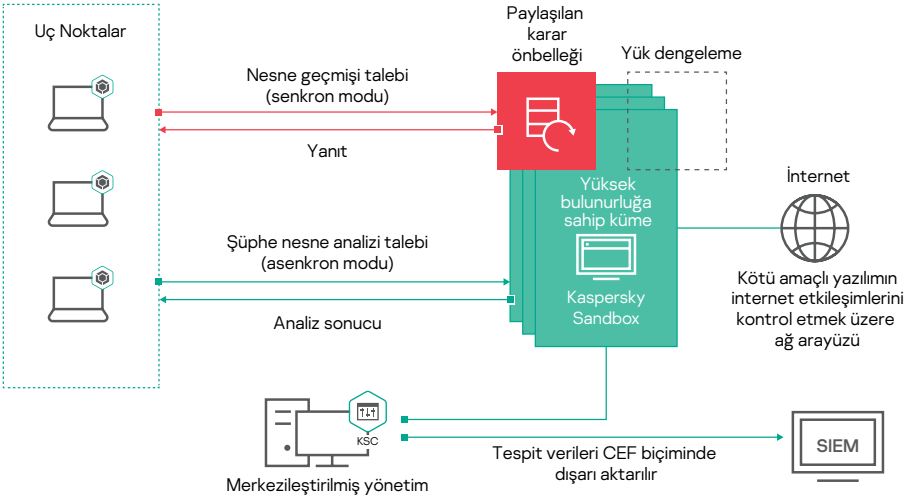
Sistem Sağlamlaştırma ve insan hatası faktörünün azaltılmasını sağlayan kontroller:

- Kategori bazlı beyaz listeye ekleme özellik Uygulama Kontrolü
- Adaptif Anomali Kontrolü: Güvenliği otomatik olarak kuruluş içerisindeki herkese uygun en yüksek düzeye çıkarır
- Cihaz Kontrolü: Harici cihazların eklentisini kontrol eder ve engeller
- Web Kontrolü: Potansiyel olarak tehlikeli, zaman alan ve uygunsuz sitelere erişimi engeller ve kısıtlar

Kaspersky Endpoint Security for Business hakkında daha fazla bilgi almak için lütfen şu adresi ziyaret edin: https://www.kaspersky.com/small-to-medium-business-security/endpoint-advanced

Otomatik sandbox

Kaspersky Sandbox, uç nokta korumasını atlatmak üzere tasarlanmış tehditleri insan müdahalesi olmaksızın otomatik olarak tespit eder ve yanıtlar.



* Bilgi Güvenliği Tehdit ve Olay Yönetimi

Kaspersky Sandbox iş akışı

Taranan nesneler, bir iş istasyonunu simüle eden izole sanal makineler içerisinde kümelenmiş sandbox sunucuları tarafından çalıştırılır.

Sandbox, verileri kötü amaçlı ve şüpheli olmaları yönünden analiz eder ve kararını tarama talebinde bulunan uç nokta yetkilisine iletir. Bunun yanında diğer ana bilgisayarların da taranan nesne için tekrar analiz yapmalarına gerek kalmaması ve hızlı şekilde bilgileri alabilmesi için operasyonel önbelleği sunar.

Dosyanın kötü amaçlı olduğu tespit edildiğinde, Gizlilik Kaybı Göstergesi (IoC) ağda yer alan diğer tüm bilgisayarlarda dosyanın silinmesi için otomatik bir düzeltme işlemi uygulamak için kullanılabilir.

Kaspersky Sandbox tarafından kullanılan teknikler şunlardır:

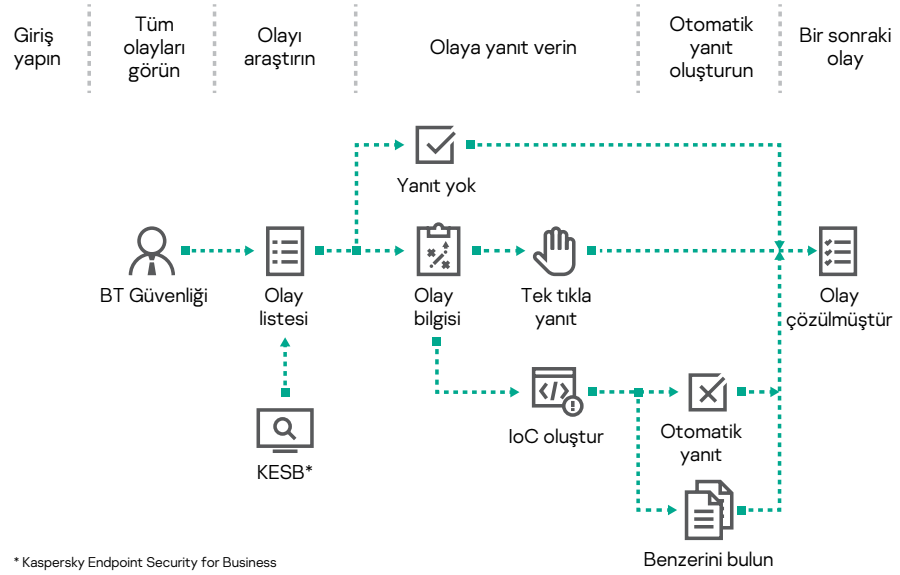
- İnternet kaynaklarıyla etkileşimin izlenmesi
- Modül yükleme
- Senkron ve asenkron tarama modları
- Ters kaçış teknikleri
- Farklı benzetim modlarının uygulanması
- Kullanıcı eylemi modellemesi
- Otomatik IoC oluşturma ve altyapı taraması
- Otomatik önleme

Kaspersky Sandbox hakkında daha fazla bilgi almak için lütfen şu adresi ziyaret edin: https://www.kaspersky.com/enterprise-security/malware-sandbox

Optimum EDR

Kaspersky EDR Optimum, hem otomatikleştirilmiş ve manuel analizler sunar hem de uç nokta düzeyinde oluşan gelişmiş tehditleri yanıtlar.

Normal dışı davranışlar tanımlanabilir, gizlenen ve özellikle de yaygın davranışları taklit etmeye çalışan dosyasız tehditler otomatik olarak tespit edilir ve düzeltilir. Görsel bilgiler ve temel neden analizi yapılabilmesi sayesinde hızlı tepki ve kısa sürede etkisiz kılma sağlanır.



Kaspersky EDR Optimum iş akışı

Kaspersky Uç Nokta Güvenlik çözümünün bir parçası olarak çalışan Kaspersky EDR Optimum, aşağıdaki izler de dahil olmak üzere saldırı öldürme zinciri içerisinde saldırıları tespit etmek ve görselleştirmek için çeşitli teknikler kullanır:

- İşlem ekleme
- Dosya bırakma
- Kayıt defteri anahtarı değişiklikleri
- Bağlantılar
- Kullanıcı davranışındaki anomaliler

Bir tehdit tespit edildikten sonra, verilebilecek yanıt seçenekleri şunlardır:

- Sunucuyu izole edin
- Ana sunucunun taramasını başlatın
- (Karantinaya alınmış) dosyayı kaldırın
- İşlemi kesin
- İşlemin yürütülmesini önleyin

Kaspersky EDR Optimum, IoC'lerin içeri aktarımı ve oluşturulması ile kapsamlı taramalar ve vakaları yanıtlama gibi işlemler de dahil olmak üzere, yüksek düzeyde otomasyonu tek tıklamayla çalışan manuel seçeneklerle bir araya getirmektedir.

Kaspersky EDR Optimum hakkında daha fazla bilgi almak için lütfen şu adresi ziyaret edin: http://www.kaspersky.com/enterprise-security/edr-security-software-solution

Yönetim ve idare

Çözümümüzün tüm bileşenleri kurum içerisinde tek kod tabanlı olarak üretilmiş, aynı tekil konsol aracılığıyla yönetilmekte ve aynı çok amaçlı uç nokta aracısını kullanmaktadır. Bu sayede günlük yönetim merkezileştirilmiş, direkt ve verimli hale gelmiştir.

Forrester'a[7] göre, birçok kuruluş için en temel gerekliliklerden biri güvenlik çözümlerinin kullanıcılar için neredeyse hiç veya çok az oranda aksamaya sebep olmadan dağıtılmasıdır. Bu prensip, Kaspersky Uç Nokta Güvenliği'nin merkezinde yer almaktadır.

7 The Total Economic Impact™ of Kaspersky Security Solutions, Forrester, 2020

- Kuruluşların **%52**'si , kurumsal siber güvenlik açısından en büyük tehdidin çalışanları olduğunu belirtti[7]
- Çalışanların **%60**'ı , kurumsal cihazlarında gizli veriler tutuyor (finansal veriler, e-posta veri tabanı vb.)
- Çalışanların **%30**'u, kişisel bilgisayarlarının giriş bilgilerini iş arkadaşlarıyla paylaştıklarını söylüyor[8]

Güvenlik farkındalığı

Aynı zamanda, siber güvenlik alanızdaki uzmanlık ile oldukça tanınmış eğitim teknolojileri ve uygulamalarını bir araya getiren bilgisayar tabanlı eğitim ürünleri de sunmaktayız. Bu yaklaşım kullanıcıların davranışını değiştirir ve kuruluş genelinde siber açıdan güvenli bir ortam oluşturulmasını sağlar.

Otomatikleştirilmiş öğrenim yönetimi platformunun başlatılması yalnızca 10 dakika sürer, daha sonra aşağıda yer alan eğitim formatları içerisinde otomatik olarak sunulan sürekli güçlendirmeye sahip aralıklı öğrenme ile her çalışan grubu için bir eğitim programı oluşturulur:

- öğrenim modülleri
- e-posta güçlendirme
- testler
- kimlik avı saldırıları simülasyonu

Eğitime katılan çalışanlarınızın ilerlemesini, canlı veri izleme, trendler ve tahminlerle birlikte sonuçlarınızı nasıl daha iyi bir noktaya çıkarabileceğinize ilişkin önerilere sahip kullanıcı dostu panelden takip edebilirsiniz.

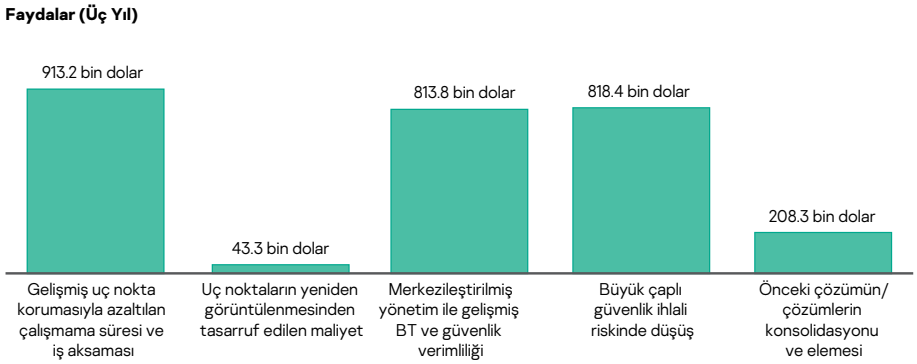
Kaspersky Güvenlik Farkındalığı hakkında daha fazla bilgi almak için lütfen şu adresi ziyaret edin: https://www.kaspersky.co.uk/enterprise-security/security-awareness

ROI değeriniz

Her çözümde olduğu gibi, maliyetler de en az sunduğumuz çözümler kadar önemlidir. Aşağıda, merkezine Kaspersky Endpoint Security for Business ile Kaspersky Security Solution'ı esas alan bir Forrester çalışmasına[7] göre tipik bir Kaspersky çözümü için Yatırımın Geri Dönüşü (ROI) grafiği sunulmaktadır:

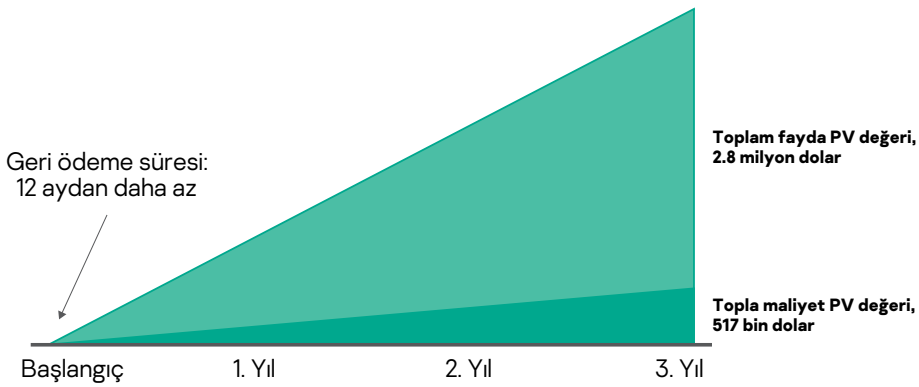
Forrester'ın yürüttüğü çalışmada görüşülmüş şirketlerin deneyimlediği risk ayarlı mevcut değer (PV) nicel faydaları:

- **Yaklaşık 1 milyon dolar:** daha az aksama yaşanmasıyla geliştirilen uç nokta çalışma süresinin ciroya olan etkisi
- **40 bin doları aşkın:** uç noktaların yeniden görüntülenmesi gerekliliğini azaltarak BT üretkenliğinden kazanılmasını sağlayan güvenlikle ilgili daha az vaka
- **800 bin doları aşkın:** merkezileştirilmiş yönetim konsolu aracılığıyla birden fazla güvenlik çözümünün yönetiminin kolaylaştırılması üretkenlikten tasarruf edilmesini sağladı
- **800 bin doları aşkın:** genel güvenlik duruşunda yapılan büyük ölçekli geliştirme, büyük çaptaki güvenlik ihlali risklerini azalttı
- **200 bin doları aşkın:** Kaspersky'e taşıma yapılmasına ilişkin maliyet tasarrufları.



Forrester'ın mevcut müşteriler ile yapmış olduğu görüşmeler ve sonrasında gelen finansal analizler, bu değerler üzerine kurulu bir kuruluşun 500 bin doları aşkın maliyete karşı 2.8 milyon dolarlık kâr sağladığını ve toplamda net mevcut değer (NPV) olarak 2.3 milyon dolar ve %441'lik ROI oranını yakaladığını gösterdi.

Finansal Özet



7 The Total Economic Impact™ of Kaspersky Security Solutions, Forrester, 2020

8 Bir Dijital Kümeyi Çözmek, Kaspersky Lab, 2019

Özetle

Modern tehditlerin bulunduğu mevcut ortamda kuruluşunuzu güvende tutmak için uç nokta koruması hayati öneme sahiptir. Uç noktalarınızı korumanın en iyi yolu da, fazlasıyla otomatikleştirilmiş bir yöntem ile tehditlerin tespiti ve yanıtlanması için farklı teknikler kullanan, aynı zamanda da daha karmaşık görevler ve önemli kararlar için insan girdisine olanak tanıyan çok katmanlı bir çözümden yararlanmaktan geçer.

Kaspersky Uç Nokta Güvenliği entegre çözümü, kuruluşların özellikle emtia tehditlerine, gelişmiş ve hedefli saldırılara ve insan hatasına karşı koruma ihtiyacını aşağıdaki yöntemlerle ele almak üzere tasarlanmıştır:

- **çok katmanlı , entegre koruma, tespit ve yanıt** stratejisini kullanmak
- savunmalarınızı **otomatikleştirerek**, hedefli ve gelişmiş saldırılar için dahi süreyi ve eforu düşürmek
- **en yüksek tespit değerlerini** yakalamak
- **kontroller ve güvenlik farkındalığı ile siber açıdan güvenli bir ortamı** desteklemek
- **yatırımınız için dönüş elde etmenizi** sağlamak

Sunulan tüm bu hizmetler, değerli kaynaklarınızı ayırmadan en karmaşık siber tehditlere karşı dahi en yüksek düzeyde güvenliğin keyfini sürebileceğiniz anlamını taşır.

Kaspersky Uç Nokta Güvenliğinin, kuruluşunuzun kaynakları üzerinde ilave yük oluşturmadan karmaşık saldırılara sizi nasıl koruyacağı hakkında daha fazla bilgi almak için lütfen şu adresi ziyaret edin:
https://www.kaspersky.com/small-to-medium-business-security/endpoint-security-solution

www.kaspersky.com.tr