KASPERSKY ENDPOINT SECURITY FOR BUSINESS: TEKNOLOJİ İŞ BAŞINDA

Görebildiğiniz ve göremediğiniz tehditler için

KASPERSKY lab

THE POWER OF PROTECTION

kaspersky.com/business
#Securebiz

İÇİNDEKİLER

Şirketlerin %94'ü harici güvenlik tehditlerinin birkaç biçimine maruz kalmıştır

Kaynak: Kaspersky Lab Global BT Risk Raporu 2014

İŞLETMENİZİ GÖREBİLDİĞİNİZ VE GÖREMEDİĞİNİZ TEHDİTLERE KARŞI KORUYUN

Doğru BT güvenliğine sahip olmak hiç bu kadar önemli olmamıştı.

BİLMEDİĞİNİZ ŞEYLER SİZE ZARAR *VEREBİLİR*

Güvenlik ihlallerinin yüzde 30'dan fazlası 100 veya daha az çalışana sahip şirketlerde gerçekleşir.[1] Küçük ve orta ölçekli işletmelerin (KOBİ'ler) yüzde 44'ü siber suçluların saldırılarına maruz kalmıştır.[2]

Bununla birlikte söz konusu işletmelerin büyük bölümü siber suç ve gelişmiş kötü amaçlı yazılımların kendileri için oluşturduğu son derece gerçek tehditlerin hala farkında değildir. Küçük işletmelerin yüzde beşten daha az bir bölümü siber suça karşı hiçbir önlem almadıklarını kabul ederken, sadece yüzde 60'ı kötü amaçlı yazılımdan koruma yazılımlarını güncel tutmaktadır.[3]

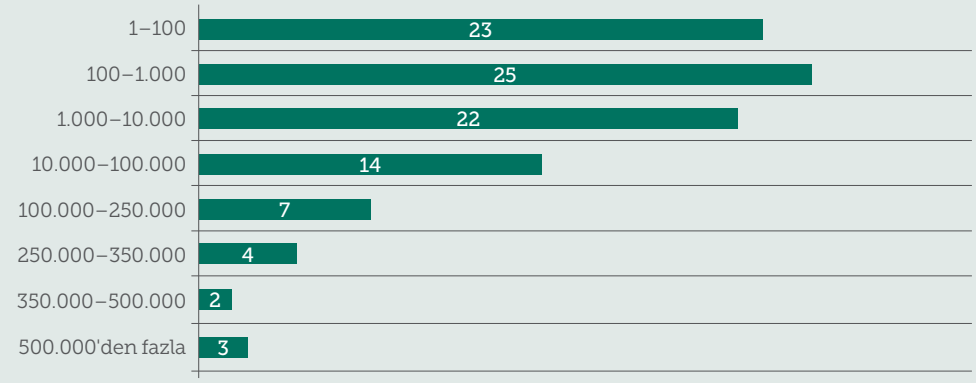
İlgi çekmek için çok küçük bir şirket olduğunuzu düşünmek, siber suçluların her gün daha karmaşık hale gelen kötü amaçlı yazılımları işletmenize karşı kullanmaları için tam olarak ihtiyaç duydukları bakış açısıdır. Siber suçlular birçok KOBİ'nin bilmediği bir şeyi biliyorlar: Siz bir hedefsiniz.

[1] Verizon 2013 Veri İhlali Araştırma Raporu
[2] Ulusal Küçük İşletmeler Birliği tarafından 2013'te gerçekleştirilen anket
[3] Kaspersky Lab, Threatpost, 24 Mayıs 2013

GÖREMEDİKLERİNİZ

Bir tür BT güvenlik çözümü kullanan yüzde 80'lik KOBİ dilimindeki bir işletme olduğunuzu varsayalım. Kendinize bu kadar güvenmeyin: işletme kullanıcılarının büyük bölümü tehdit hacimlerini küçümserler.[4] Anket katılımcılarının sadece yüzde dördü her gün algılanan tehdit sayısı hakkında yakın bir tahminde bulunabilmiştir.[4]

GÜNLÜK OLARAK ALGILANAN YENİ KÖTÜ AMAÇLI YAZILIM ÖRNEĞİ SAYISI (%)



Kaynak: Kaspersky Lab Global BT Risk Raporu 2014

Bu bağlamda, BT güvenliğini bir "ticari mal" olarak algılayan kullanıcıların güvenlik çözümleri arasında çok az fark görmesi şaşırtıcı değildir. Bu tehlikeli bir söylentidir; algılama oranları arasındaki yüzde birlik fark bile bir yıllık bir süre içinde ağlara sızmayı başaran yüz binlerce kötü amaçlı yazılıma karşılık gelir. Bunu nereden biliyoruz?

- Kaspersky Lab, her gün 325.000 yeni kötü amaçlı yazılım örneği algılamaktadır.
- 2014'ün ikinci çeyreğinde, kötü amaçlı yazılımdan koruma çözümümüz son kullanıcı sistemlerine yönelik 528.799.591 virüs saldırısı algılamış, işlemlere sızmayı başarmış toplam 114.984.065 özgün kötü amaçlı nesne belirlemiştir.[5]

En tehlikeli tehditler, Kaspersky Lab uzmanlarının her gün izlediği, analiz ettiği ve önlediği, sizin ise henüz haberdar olmadığınız tehditlerdir. Biz sorun oluşturabilecek öğeleri ararız. Bu öğeyi bulduğumuzda, on yılı aşkın tehdit istihbaratı ve uzmanlığımızı kullanarak özellikle gelişmiş kötü amaçlı yazılımlar ve Gelişmiş Kalıcı Tehditler (APT'ler) gibi işletmenizin en fazla korunması gereken tehditlere karşı daha fazla koruma sağlarız.

İşletmelerin tehdit algısı ve tehdidin gerçek büyüklüğü arasında büyümekte olan bir uçurum mevcuttur. Biz buna "algı boşluğu" adını veriyoruz. Bu terim, büyüklüklerinden bağımsız olarak kuruluşların, karşı karşıya oldukları tehditlerin miktarını ve önem derecesini korkutucu biçimde küçümsediğini gösterir.

Costin Raiu, Global Araştırma ve Analiz Ekibi, Kaspersky Lab

[4] Kaspersky Lab Global BT Risk Raporu 2014
[5] Kaspersky Lab 2. Çeyrek Tehdit Gelişim Raporu 2014

PROAKTİF, DUYARLI, AKILLI

Kaspersky Lab, aralarında Carbanak (dünyanın en büyük siber bankacılık soygunu), Dark Hotel, The Mask, Icefog ve Red October gibi tehditlerin bulunduğu dünyanın en yüksek profilli, en fazla kişiyi etkileyen tehditlerini ortaya çıkarma konusunda başarılı bir geçmişe sahiptir. Çalışanlarımızın üçte birden büyük bölümü Araştırma ve Geliştirme alanında görev yapmaktadır. Bu çalışanlar, özel İstihbarat ve Analiz Araştırmacılarımızın her gün inceledikleri, sürekli olarak gelişen tehditlere karşı koruma geliştirme ve bu tehditleri öngörebilme alanına odaklanırlar.

Kaspersky Lab'in dünyanın en gelişmiş tehditlerini şirket bünyesinde inceleme anlayışı, bilinen, bilinmeyen ve gelişmiş tehditlere karşı kapsamlı koruma sağlayabilen güvenlik teknolojilerinden oluşan, çok katmanlı bir platform geliştirmemize olanak sağlamıştır. Teknolojilerimiz görebildiğiniz ve göremediğiniz tehditleri algılar ve etkisiz hale getirir.

Bunu nasıl yapıyoruz? Şimdi Kaspersky Lab'in yüklendiği andan itibaren birlikte çalışmaya başlayan birçok kötü amaçlı yazılımdan koruma ve tehdit algılama teknolojisine yakından bakalım. Bu platform, uç noktalar ve diğer BT altyapısı bileşenlerine yönelik çok katmanlı, kapsamlı tehdit algılama ve tehditten korunma sağlayan istihbarat tabanlı teknolojilerin benzersiz bir kombinasyonudur.

BİLİNEN TEHDİTLERİ ALGILAMA

Dosya indirme, web sayfası açma veya uygulama başlatma eylemlerinin gerçekleşme anından itibaren, Kaspersky Lab'in gelişmiş kötü amaçlı yazılımdan koruma motorları bilinen, bilinmeyen ve gelişmiş web ve posta tabanlı virüsleri, Truva Atları'nı, rootkit'leri, solucanları, casus yazılımları, komut dosyalarını, reklam yazılımlarını ve diğer bilinen kötü amaçlı nesne tehditleri eşzamanlı olarak kontrol eder, algılar ve koruma sağlar. Temel olarak bilinen tehditlerle başlayan bu motorlar şu bileşenlerden oluşur:

AĞ SALDIRISI ENGELLEYİCİ

Bilinen imzaları kullanarak, bağlantı noktası tarama, hizmet reddetme (DoS) saldırıları, arabellek taşmaları ve diğer kötü amaçlı uzaktan yönetilen eylemler gibi ağ tabanlı saldırıları algılamak ve engellemek için tüm ağ trafiğini tarar.

KARA LİSTE

Kötü amaçlı yazılım analistlerinden oluşan özel ekipler Kaspersky Lab veritabanlarının en yeni kötü amaçlı yazılım imzaları ve verilerini içerecek şekilde güncel olmasını sağlar. Bunlar tüm bilinen kötü amaçlı yazılımları otomatik olarak engellemek için kullanılır.

URL FİLTRELEME

Gelen/giden trafikteki URL adreslerini Kaspersky Lab'in bilinen kötü amaçlı ve kimlik avı sitelerine karşı tarayarak ve kontrol ederek, web tabanlı saldırıları, sunucu tarafındaki polimorfik kötü amaçlı yazılımları ve "komut ve kontrol" (C&C) sunucularını engeller.

GÜVENLİK DUVARI

Ağa giren ve ağı terk eden tüm paketleri analiz ederek, güvenlik riski oluşturup oluşturmamalarına bağlı olarak bu paketleri engeller veya izin verir. İzinsiz bağlantılar engellenerek, saldırı alanını daraltır ve virüs bulaşma olasılığını azaltır. Virüs bulaşan veya başka bir şekilde zarar gören makinelerin ağ etkinlikleri kısıtlanarak, kötü amaçlı yazılım yayma olanakları azaltılır ve güvenlik ihlallerinden kaynaklanan zarar en aza indirilebilir.

Kaspersky Lab'in uzun yıllara dayanan birikimi ve deneyimi ile inşa edilen imza tabanlı teknolojileri. Yukarıda açıklanan teknolojiler ve tehditlerin büyük bölümünü kısa süre içinde ortaya çıkaran, daha sonra değineceğimiz Kaspersky Security Network sayesinde bilinen kötü amaçlı yazılımlar başarıyla engellenir. Peki daha önce belirttiğimiz bilinmesi zor veya gelişmiş tehditler ne olacak? Bunları da savaş alanımıza dahil ediyoruz...

[6] Kaspersky Lab Anti-Spam teknolojisi %99,75 algılama oranı ve sıfır hatalı tespitle Kasım 2014'te düzenlenen VB Spam Testinde ilk sırayı kazanmıştır.

BİLİNMEYEN TEHDİTLERİ ALGILAMA

Şimdi de bir dosya bilinen tehditler için düzenlenen imza tabanlı denetimleri geçerek başlatma denemesi gerçekleştirdiği anda olanlara göz atalım. Kaspersky Lab'in çok katmanlı, proaktif teknolojileri dosyaları çalıştırıldıkları anda analiz edip denetleyerek, bilinmeyen bir tehditle karşı karşıya olunduğunu gösteren şüpheli veya kötü amaçlı etkinlikleri arar.

SEZGİSEL ARAÇLAR

Sezgisel analiz klasik anti-virüs veritabanları kullanılarak algılanamayan tehditlere karşı proaktif koruma sağlar. Kaspersky Lab sezgisel araçları yeni kötü amaçlı yazılımların veya bilinen kötü amaçlı yazılımlardaki değişikliklerin algılanmasına olanak sağlar. Statik analiz kodu kötü amaçlı yazılımla ilişkili şüpheli komutlara karşı tararken, dinamik analiz makine kodunu çalıştırmayı deneyen dosyalara karşı kontrol eder, olası "yanıtlara" sahip öykünen "çağrıları" yanıtlayarak kodun güvenli olup olmadığının anlaşılmasını sağlar.

SEZGİSEL KİMLİK AVI KORUMASI

Az sayıda kullanıcının etkilendiği son derece yeni kimlik avı saldırılarında, Kaspersky Lab teknolojisi sözlük, giriş formları veya okunamayan simgelerden oluşan sıralar gibi daha fazla şüpheli etkinlik kanıtlarını araştırır. Bu araçlar, daha önce açıklanan nispeten geleneksel, veritabanı yönlendirmeli yaklaşımın koruma kapsamını genişletir.

Kimlik avı tabanlı tehditler yeni ve son derece tehlikeli gelişmiş birçok tehdit için bir başlangıç noktası teşkil eder.

ANA BİLGİSAYAR İZİNSİZ GİRİŞ ÖNLEME SİSTEMİ (HIPS)

Kaspersky Lab HIPS teknolojisi, şüpheli uygulama ve etkinlikleri algılayan ve yöneten, tehditleri başlatılmadan önleyen ekstra bir koruma katmanı sunar. HIPS, ilk analizden sonra güvenilirlik düzeyi belirleyerek uygulamanın nasıl davranacağını kontrol eder. Bu düzeyler uygulamaların kullanabilecekleri kaynakları, erişebilecekleri veya değiştirebilecekleri veri türünü vb. belirler. Bu katman tehlike olasılığı taşıyan programları izin verilen, güvenli uygulamaların performansını etkilemeden engeller. Güvenli olmayan bir uygulamanın, başlatma dahil hiçbir eylem gerçekleştirmesine izin verilmez.

UYGULAMA KONTROLÜ VE BEYAZ LİSTEYE ALMA

Uygulama kontrolü, yönetici tarafından belirlenen uygulamaları engeller veya izin verir. Kaspersky Lab'in yaklaşımı sadece belirli kurallar ve ilkeler çerçevesinde çalıştırılmalarına izin verilen güvenilir uygulamalar ve yazılım kategorilerinden oluşan ve sürekli güncellenen listeler olan Dinamik Beyaz Listeye Alma ile hayata taşınmıştır. Kaspersky Lab, beyaz listelerin oluşturulması ve denetlenmesine yönelik özel bir laboratuvara sahiptir. Bu veritabanı bir milyarı aşan sayıda dosyadan oluşmaktadır ve her gün bir milyon yeni dosya eklenmektedir.

Birçok kötü amaçlı yazılımın beyaz listede yer almayan yürütülebilir bir dosya olarak gönderildiği düşünüldüğünde, Uygulama Kontrolü ve Beyaz Listeye Alma henüz ortaya çıkaramadığımız tehditlerin neden olduğu riski azaltır. Bu yaklaşımı ve destekleyen teknolojileri hayata taşıyan kuruluşlar, kötü amaçlı dosyaları belirleme veya algılama gereksinimi olmadan bu dosyaların çalıştırılmasını engelleyebilirler.

KASPERSKY SECURITY NETWORK

Küresel, bulut tabanlı ve son derece etkin bir tehdit laboratuvarı olan Kaspersky Security Network, bilinen, bilinmeyen ve gelişmiş tehditleri ve çevrimiçi saldırıları saniyeler içinde analiz eder, yönetir ve bu istihbaratı doğrudan müşterilerin sistemlerine gönderir.

Dünya çapında 60 milyon uç nokta sensöründen gelen gerçek zamanlı, kaynağı gizlenen verileri kullanan bu platform, Kaspersky Lab korumalı sistemlerden geçen her bir dosyaya ilgili tehdit istihbaratına dayalı analizler uygulanmasını sağlar. Bu veriler en uygun eylemlerin hayata geçirilmesinde kullanılır; Kaspersky Lab motorunun tüm diğer bileşenleriyle bir arada çalışan Kaspersky Security Network, bilinmeyen tehditlere karşı imzalar kullanılabilir hale gelmeden önce koruma sağlar. Geleneksel imza tabanlı yanıtların oluşturulması saatler sürebilirken, Kaspersky Security Network tehditleri yaklaşık 40 saniye içinde yanıtlar.

GELİŞMİŞ TEHDİTLERİ ALGILAMA

Dosyanız indirildiğinde ve başlatıldığında; Kaspersky Lab teknolojileri dosyayı tarar, analiz eder, istihbarat uygular ve bilinen ve bilinmeyen tehdit kapsamında yer alıp almamasına dayalı olarak dosyayı engeller ya da dosyaya izin verir.

Peki ya Gelişmiş Tehditler?

İşlem davranışlarını izleyen, şüpheli şablonları fark eden, kötü amaçlı etkinlikleri engelleyen ve Cryptors gibi zararlı değişikleri geri alan geniş kapsamlı proaktif, gelişmiş davranış mekanizmaları kullanan Kaspersky Lab gelişmiş tehdit algılama teknolojileri, gelişmiş tehditleri algılamak ve engellemek üzere tasarlanmıştır.

Şimdi bu teknolojileri daha yakından inceleyelim...

SİSTEM İZLEYİCİ

Bu teknoloji, izleme etkinlikleri kullanarak ve davranış şablonlarını belirleyerek uygulama ve diğer önemli sistem etkinliklerini izler ve veri toplar. Bu bilgiler daha önce değindiğimiz diğer Kaspersky Lab koruma bileşenlerine iletilir. Tehdit şablonları kapsamında yer alan tüm etkinliklere, yönetici tarafından belirlenen ilkelerle veya kötü amaçlı işlemleri sonlandıran ve daha sonra analiz edilmek üzere karantina altına alan varsayılan ayar kullanılarak müdahale edilir.

Dosya işlemlerini, Kaspersky kötü amaçlı yazılımdan koruma bileşeni için kesintiye uğratan sürücü ayrıca kayıt defterinde gerçekleştirilen değişikliklere yönelik bilgi toplarken, güvenlik duvarı uygulamaların ağ etkinliklerine yönelik bilgileri edinir. Tüm bu bilgiler Sistem İzleyici'ye iletilir ve program sürücülerinin yüklenmesi gibi karmaşık sistem etkinliklerini yönetebilen bir modül oluşturur.

Kötü amaçlı eylemler ve kötü amaçlı yazılım benzeri zarar verici davranış şablonları engellenir.

OTOMATİK GÜVENLİK AÇIKLARINI ÖNLEME (AEP)

Bu teknoloji özellikle yazılım güvenlik açıklarından faydalanan kötü amaçlı yazılımları hedef alır. Sık karşılaşılan kötü amaçlı girişimlerin özellikleri ve davranışları derinlemesine analiz edilerek geliştirilen bu teknoloji, güvenlik açığından faydalanma davranış şablonlarını belirler ve bu şablonlar henüz tamamlanmadan engeller.

AEP, diğer Kaspersky Lab teknolojilerini tamamlayan ekstra bir güvenlik katmanı, güvenlik ağı gibi davranır. Bu teknoloji, Kaspersky Lab Sistem İzleyici ile bir arada çalışır.

GERİ ALMA

Bu kesintisiz, ayrıntılı sistem izleme teknolojisi tüm virüs bulaşmalarının etkisini azaltan ve sistemleri önceki güvenli parametrelere döndüren olağanüstü yüksek doğrulukta sistem Geri Alma işlevi sunar. Geri Alma mekanizmaları güncellenebilir ve oluşturulan ve değiştirilen yürütülebilir dosyalar, MBR değişiklikleri, önemli Windows dosyaları ve kayıt defteri anahtarlarıyla birlikte çalışabilir.

VARSAYILAN OLARAK REDDET

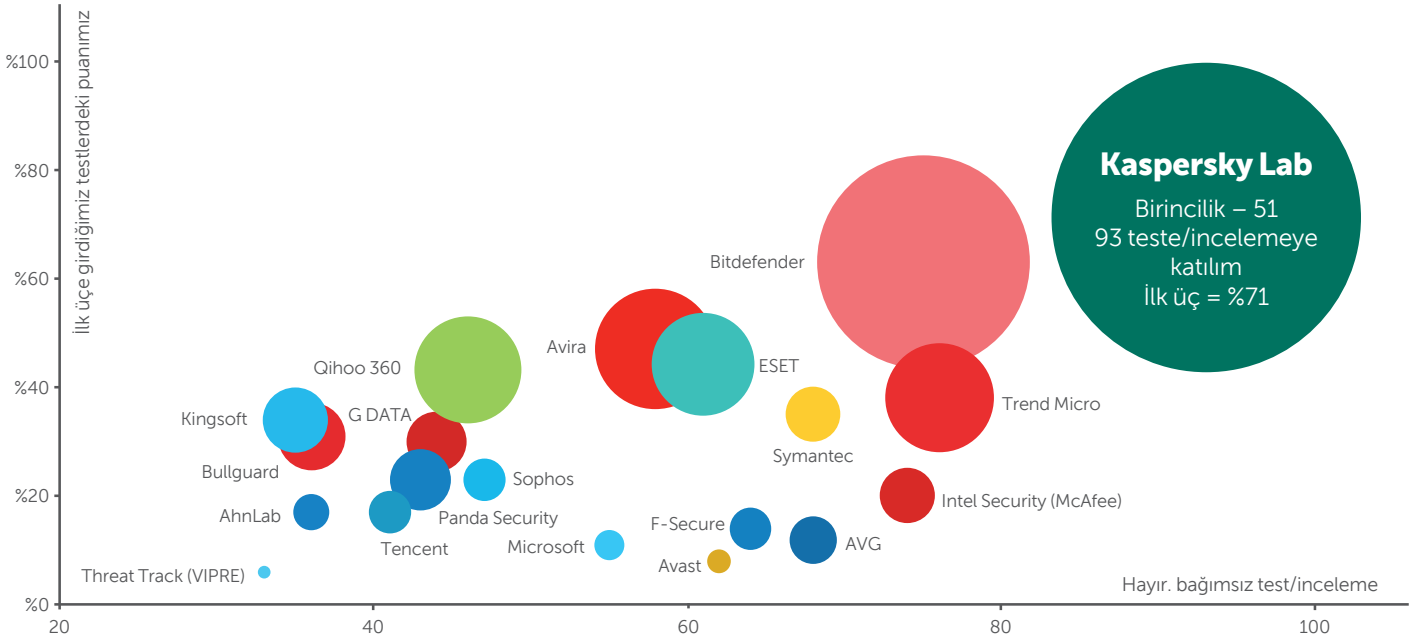
Bu teknolojiyi sürekli yenilenen ve gelişmiş tehditlere karşı uygulanabilecek en etkili güvenlik kurulumu olarak gören profesyonellerin sayısı gün geçtikçe artmaktadır. Teknoloji, tüm istasyonlarında yönetici tarafından açık şekilde izin verilemeyen tüm uygulamaların çalıştırılmasını engeller.

Varsayılan Olarak Reddet, hedefli saldırılar dahil olmak üzere tüm yeni, dosya tabanlı kötü amaçlı yazılımların otomatik olarak engellenmesini sağlar.

KÜÇÜK BİR DEĞİŞİKLİK BÜYÜK BİR FARK YARATABİLİR

Algılama oranındaki yüzde bir birimlik değişikliğin bile ağlara sızmayı başaran yüz binlerce kötü amaçlı yazılıma karşılık gelebileceğini gördük. Ayrıca Kaspersky Lab'in daha fazla azaltma, algılama ve analiz "ağı" yaklaşımının, bilinmeyen ve hatta gelişmiş tehditleri daha işe koyulmadan yakalayabildiğini öğrendik.

KASPERSKY LAB: SEKTÖRDE EN İYİ KORUMAYI SAĞLAR*



Bağımsız test sonuçları sürekli olarak Kaspersky Lab'in sektördeki en iyi korumayı sağladığını ortaya koymaktadır. Sadece 2014'te, 93 bağımsız test ve incelemeye katılarak 51 birincilik kazandık ve katıldığımız inceleme testlerde yüzde 71 oranında ilk üçte yer almayı başardık. Bu başarı Microsoft, Cisco Meraki, Juniper Networks ve Alcatel Lucent gibi OEM'lerin ürünleriyle birlikte sunacakları güvenlik konusunda Kaspersky Lab'e güvenmelerinin nedenlerinden biridir.

Tüm Kaspersky Lab güvenlik teknolojilerinin şirket bünyesinde aynı kod tabanından geliştirilmesi ve sağlanması, birbirleriyle sorunsuz bir şekilde entegre olmalarına olanak sağlar ve parçalarının toplamından daha etkin, çok katmanlı bir platform ortaya çıkarır. Bu entegrasyon seviyesiyle birlikte Kaspersky Lab güvenliğinizi sağlarken, siz de gelişmiş performans, daha hızlı güncellemeler ve tüm ürünlere ortak bir bakış açısı sunarak en iyi yaptığınız işe odaklanabilirsiniz.

* Notlar:
2014'teki kurumsal, tüketici ve mobil ürünler için yapılan bağımsız testlerin sonuç özetlerine göre.

Özet, şu bağımsız test laboratuvarları ve dergiler tarafından gerçekleştirilen testleri içerir:
AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin.
Balonun boyutu, kazanılan birinciliklerle doğru orantılıdır.

ŞİMDİ BAŞLAYIN: 30 GÜNLÜK ÜCRETSİZ DENEME SÜRÜMÜ

Hiçbir zorunluluk içermeyen deneme sürümüyle üstün güvenlik platformumuzun işletmenizi kötü amaçlı yazılım ve siber suça karşı nasıl koruduğunu keşfedin.

Ürünlerin tam sürümlerini indirmek için **kaspersky.com/trials** adresini bugün ziyaret edin ve ürünlerimizin BT altyapınızı, uç noktalarınızı ve gizli işletme verilerinizi ne kadar başarılı koruduğunu değerlendirin.

ÜCRETSİZ DENEME SÜRÜMÜNÜZÜ ŞİMDİ EDİNİN

İLETİŞİME KATILIN

#Securebiz

Bizi YouTube'da izleyin

Bizi Facebook'ta beğenin

Bizi Twitter'da takip edin

LinkedIn'de bize katılın

Bizi SlideShare'de görüntüleyin

Blogumuzu gözden geçirin

Bize Threatpost'ta katılın

Bizi Securelist'te görüntüleyin

KASPERSKY LAB HAKKINDA

Kaspersky Lab, bugün uç nokta koruma çözümleri alanında dünyanın en büyük özel tedarikçisidir. Şirket uç nokta kullanıcılarına yönelik güvenlik çözümleri üreten tedarikçiler arasında dünyada ilk dört arasında yer alır*. 17 yıldan daha uzun bir geçmişiyle BT güvenliği konusunda birçok yeniliğe imza atan Kaspersky Lab, büyük kuruluşlar, KOBİ'ler ve tüketicilere yönelik verimli dijital güvenlik çözümleri sunar. İngiltere'de tescilli bir holding şirketine sahip olan Kaspersky Lab, bugün dünya çapında 200'ün üzerinde ülke ve bölgede faaliyet göstermekte, dünyanın dört bir köşesindeki 400 milyonun üzerinde kullanıcıya koruma sağlamaktadır. www.kaspersky.com adresinden daha fazla bilgi alabilirsiniz.

* Şirket, 2013 IDC Dünya Çapında Uç Nokta Güvenliği Gelirleri değerlendirmesinde Tedarikçi kategorisinde dördüncü sırada yer almıştır. Bu değerlendirme, Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares (Dünya Çapında Uç Nokta Güvenliği 2014–2018 Tahminleri ve 2013 Tedarikçi Pazar Payları) (IDC No. 250210, Ağustos 2014) başlıklı IDC raporunda yayınlanmıştır. Raporda yazılım tedarikçileri, 2013 yılındaki uç nokta güvenliği çözümlerinin satışından elde edilen kazanca göre sıralanmıştır.

kaspersky.com/business
#Securebiz