Kaspersky Web Traffic Security

Network sisteminiz için stratejik savunma

Proxy sunucusu şirket altyapısı ile dış dünya arasında geçen web trafiği için bir darboğaz görevi görür. Bu stratejik pozisyon, tehditleri erkenden ve nispeten daha az çaba ile yakalama fırsatları sunar.

Kaspersky Web Traffic Security, proxy sunucuları ile bütünleşerek kurumsal BT ağını global ağların tehlikelerine karşı koruyan ve internet kullanımını kontrol ederek verimliliği artıran bir uygulamadır. Web trafiğini kontrolden geçirir ve kurumsal güvenlik politikası ile çelişen her türlü tehdidi engeller. Çevre güvenliğine olan yaklaşım standart olmakla birlikte, özelliklerinin genişliği ve tehdit korumasının eşsiz kalitesi Kaspersky Web Traffic Security'nin benzerleri arasından sıyrılmasını sağlar.

Öne Çıkan Özellikler

- Gerçek zamanlı yeni nesil kötü amaçlı yazılım koruması ve kimlik avından korunma
- Riskli dosyaları ve veri kaçaklarını engelleyen içerik filtreleme
- Aşırı yüklü ağlara ölçeklenebilirlik
- Son kullanıcılar ve MSP'ler için aylık abonelik lisansıyla sunulabilir
- Sıfır gün tehditlerine karşı koruma
- Kaspersky Security Network'ün global tehdit istihbaratı desteği
- Microsoft Active Directory desteği
- Yönetim ve web kullanımına rol tabanlı erişim
- Web kaynağı kullanımını yönetmek için Web Control
- Fidye yazılımlarını ağa girmeden önce engelleme
- MSP'ler ve çeşitli işletmeler için çoklu müşteri mimarisi

Avantajlar

Bulaşma riskini büyük ölçüde azaltarak işletme faaliyetlerinin aksamasını önler.

Kaspersky Web Traffic Security gelen tehditlerin çoğunluğunu giriş aşamasında durdurarak ve uç noktalara erişimlerini engelleyerek, son kullanıcılar ve iş istasyonları üzerindeki etkisini önemli ölçüde azaltır.

Kurumsal ağ geçidi korumasının etkinliğini artırır

Üstün algılama oranı ve sıfıra yakın hata payı ile sektördeki en güçlü koruyucu teknolojilerden birine sahip Kaspersky Web Traffic Security uygulaması, mevcut web ağ geçidi tedbirlerine mükemmel bir şekilde uyum sağlar ve sistemin korunmasında hissedilir bir destek sunar. Bu özellik, yüksek hassasiyetli verilerle çalışan ve/veya güvenlik olaylarına karşı düşük toleransa sahip şirketler ve kurumlar için özellikle önemlidir.

BT ve BT güvenlik personeli için ek yükleri azaltır

Uç nokta koruması yeterli olsa bile, uç nokta düzeyinde daha az alarm, daha az panik anlamına geleceği için olay incelenme sürecinde daha az zaman kaybı yaşanır.

Verimliliği artırır

Kaspersky Web Traffic Security, internet kaynaklarının kullanımını yöneterek siber saldırı riskini azaltmakla kalmayıp, gölge BT'lere yer bırakmayarak, özellikle BT dışındaki uç noktaların söz konusu olduğu durumlarda dikkat dağılmasını önler.

İşletmenizin boyutuna uyum sağlar

Sistemin yüküne bağlı olarak çözüm, çoklu düğüm yönetimi ve hiyerarşik dağıtıma izin verecek şekilde ölçeklendirilebilir.

Kaspersky Web Traffic Security kurulumu için kullanılacak sunuculara yönelik donanım gereklilikleri

Sunucular:

- CPU: Intel Xeon E5606 (4 çekirdek) 1,86 GHz ya da fazlası;
- 8 GB RAM;
- En az 4 GB takas bölümü;
- Aşağıdakiler dahil 100 GB sabit disk alanı:
- Geçici dosyalar için depolama: 25 GB;
- Günlük dosyaları için depolama: 25 GB.

Ana sunucu:

- CPU: Intel Xeon E5606 (4 çekirdek) 1,86 GHz ya da fazlası;
- 8 GB RAM;
- En az 4 GB takas bölümü;
- 100 GB sabit disk alanı.

Ana sunucuyu ve bir çalışan sunucusunu aynı fiziksel sunucuya kurarsanız:

- CPU: 2 x Intel Xeon E5606 (8 çekirdek) 1,86 GHz ya da daha fazlası;
- 16 GB RAM;
- En az 4 GB takas bölümü;
- Aşağıdakiler dahil 200 GB sabit disk alanı:
- Geçici dosyalar için depolama: 25 GB;
- Günlük dosyaları için depolama: 25 GB.

Kaspersky Web Traffic Security kurulumu için kullanılacak sunuculara yönelik yazılım gereklilikleri

- Red Hat Enterprise Linux sürüm 7.5 x64.
- Ubuntu 18.04.1 LTS.
- Debian 9.5.
- SUSE Linux Enterprise Server 12 SP3.
- CentOS sürüm 7.5 x64.

Ek gereklilikler

- Ngnix sürüm 1.10.3, 1.12.2 ve 1.14.0.
- Yük Dengeleme için HAProxy sürüm 1.5.
- Squid hizmetini Çalışan sunucusuna yüklerseniz Squid 3.5.20.

Kaspersky Web Traffic Security'nin ağınızın trafiğini işlemesi için ICAP ve Talep Değiştirme (REQMOD) ve Yanıt Değiştirme (RESPMOD) hizmetlerini destekleyen bir HTTP(S) proxy sunucusu kurmanız ve yapılandırmanız gerekir. Ayrı bir proxy sunucu kullanabilir veya örneğin, Squid hizmetini Kaspersky Web Traffic Security'nin bir Çalışan sunucusuna kurabilirsiniz.

Kaspersky Web Traffic Security'i web arabirimi üzerinden yönetmek için yazılım gereklilikleri

Web arabirimini çalıştırmak için aşağıdaki tarayıcılardan birinin bilgisayarda yüklü olması gerekir:

- Mozilla Firefox sürüm 39.
- Internet Explorer sürüm 11.
- Google Chrome sürüm 43.
- Microsoft Edge sürüm 40.

Belirli dosyalardan kaynaklanan iki yönlü bulaşma riskini azaltır

Kaspersky Web Traffic Security, belirli dosya türlerinin bulaşma kapasitesini kısıtlayarak güvenliğin artırılmasına yardımcı olur. Bu şekilde belgelerin içine gömülmüş kötü amaçlı içerik kullanan yazılımların sisteme bulaşmasını önler ve ayrıca veri sızıntısı riskini azaltır. Medya dosyalarına erişme ihtiyacı olmayan kullanıcıları engelleyerek verimliliği artırır.

Yönetilen Servis Sağlayıcılara (MSP'ler) kolaylık sağlar

Gittikçe artan sayıda MSP, değer önerilerine siber güvenliği ekledikleri için Kaspersky Web Traffic Security çoklu kiracı yönetimi yeteneklerini ve esnek lisanslamayı destekler ve kiracı yöneticilerine uygun seviyede kontrol izni sağlar.

Özellikler

HuMachine™destekli, tehditlere karşı çok katmanlı koruma

Kaspersky'nin yeni nesil kötü amaçlı yazılım korumasının, makine öğrenimi algoritmalarına dayanan ve güçlü bulut tabanlı mekanizmalarla desteklenen birden fazla proaktif güvenlik katmanı. Giden ve gelen internet trafiğindeki kötü amaçlı yazılımları, fidye yazılımlarını ve potansiyel olarak istenmeyen programları filtreleme.

Global tehdit istihbaratı: Kaspersky Web Traffic Security sürekli gelişen tehdit ortamının son halini görmek için dünyanın dört bir tarafından toplanan verileri kullanır.

Makine öğrenimi: Global tehdit istihbaratından büyük verisi, makine öğrenimi algoritmalarının ve insan uzmanlığının birleşimi ile işlenerek minimum sayıda false-pozitive sonuç veren, başarısını kanıtlamış yüksek tespit düzeyi sunar.

Korumalı alan emülasyonu

E-posta ekleri en karmaşık ve en gizli kötü amaçlı yazılımlara karşı koruma sağlamak için güvenli bir emülasyon ortamında yürütülür. Tehlikeli örneklerin kurumsal sisteme giriş yapmadığından emin olmak için ekler bu ortamda analiz edilir.

Komut dosyası algılama

Siber güvenlik analistlerine göre, komut dosyaları giderek artan bir şekilde, hem web tabanlı saldırılar için hem de görünüşte zararsız olan Office dosyalarına kötü amaçlı yazılımların gömülmesi için kullanılır. Kaspersky Web Traffic Security bunların her ikisiyle de savaşarak, deneme amaçlı yapılan saldırılar ve sistem için ölümcül olabilecek kötü amaçlı yazılımları daha istenilen hedefe ulaşmadan durdurur.

Siber saldırı ile ilgili ana bilgisayar veritabanı

Tehlikeli kaynaklarla en küçük etkileşim riskini engellemek için bulut tabanlı çalışan bu hizmet; istenilen kaynağı, aktif siber saldırganların komuta ve kontrol sunucularına karşı tarar. Sıfır gün açıklarını, zaralı web sitelerini ve güvenliği kırmak isteyen kötü amaçlı yazılımların dağıtım noktalarını engeller. Veritabanları sürekli ve gerçek zamanlı olarak, kendini kanıtlamış Kaspersky Lab GREat ekibinden gelen istihbarat bilgileri ile güncellenir. Komut çalıştırılmadan önce, en yeni tehditleri oluşum aşamasında yok eder.

İtibar tabanlı filtreleme

Kaspersky Web Traffic Security, sürekli yenilenen Kaspersky Security Network bulut tabanlı veritabanından dosya ve adres itibarı isteyebilir. Bu sayede şüpheli veya istenmeyen dosyalar ve internet kaynakları daha derin analize gerek kalmadan derhal engellenir.

Kaspersky HuMachine™ Yaklaşımı

Büyük Veri tehdit istihbaratından, otomatik makine öğrenimi becerilerinden ve uzmanların deneyiminden güç alan Kaspersky HuMachine™, çok sayıda avantaj sunar ve daha etkili bir koruma sağlar. Birbirinden ayrı bileşenler, her bir unsurun birleştirilmesiyle daha etkili ve verimli bir bütün haline gelir.

Kimlik avı saldırılarına karşı gelişmiş koruma

Kaspersky'nin kimlik avı saldırılarına karşı gelişmiş koruma sistemi, etkili tespit modelleri için Nöral Ağlar analizini temel alır. Resimler, dil denetimleri, özel komut dizileri dahil olmak üzere 1000'den fazla kriter kullanan bu bulut destekli yaklaşım, kötü amaçlı yazılımları ve kimlik avı yapan URL'leri içeren global verilerle desteklenir. Bilinen ve bilinmeyen bütün URL'lerden indirilmiş sıfır saat kimlik avı kapasiteli dosyalara karşı koruma sağlanır.

İçerik filtreleme

Bazı dosya tiplerinin aktarılması engellenebilir. Filtreleme; ad, uzantı/tip (format tanıyıcı sahte uzantılı dosyalar için kullanılır), boyut, MIME Type ve doğrulama algoritmaları gibi birtakım parametreler üzerine kurulmuştur. Bu, siber saldırı riskinin azaltılması, veri sızıntısının önlenmesi, trafiğin azaltılması ve verimliliğin artırılması gibi birçok amaca hizmet eder.

Kaspersky Lab kategorileri ile Web denetimi

Her web kaynağı her kullanıcı için gerekli değildir. Bu kaynaklar kötü amaçlı yazılım içermeleri ya da korsan ürün satmaları halide işletmenin güvenliği ve itibarı açısından önemli bir tehdit oluşturur. Web Control, belirli web kaynakları kategorilerini riski azaltmak ve kesintisiz çalışma imkanı sağlamak için sınırlandırır. Gerekli olursa, kullanıcının ihtiyaç duyacağı siteler hariç, tüm web kaynaklarının kullanımını sınırlandırmak için Varsayılan Olarak Reddedilen senaryosu uygulanabilir.

Güvenli SSL şifreli internet gözetimi

Çözüm, kurumsal internet trafik gözetiminin ('kurumsal bağlantıyı izinsiz izleme' olarak da bilinir) uygulanmasını kolaylaştırır. İnternet iletişiminde SSL şifreli internet trafiğinin standart haline gelmesi nedeniyle olmazsa olmaz bir özellik olma niteliği kazanmıştır.

ICAP özellikli güvenlik sistemleri

Kaspersky Lab çözümü, proxy sunucularına ek olarak, ICAP protokolünü destekleyen diğer bütün cihazlardaki internet trafiğini güvence altına alır. Örneğin, Ağa Bağlı Depolama (NAS) veya şirket içi güvenlik çözümleri ile korunamayacak diğer sistemler gibi.

SIEM entegrasyonu

Şirketiniz kurumsal ağdaki etkinlikleri takip etmek için bir Bilgi Güvenliği Tehdit ve Olay Yönetimi (SIEM) Sistemi kullanıyorsa, Kaspersky Web Traffic Security, yaygın olarak kullanılan syslog ile beraber, Ortak Olay Biçimi (CEF) ile bilgi göndererek güvenlik içeriğinizi zenginleştirir.

Basit yönetim

Kaspersky Web Traffic Security esnek ancak kullanımı kolay bir yönetim sistemi sunar.

Merkezi konsol: Güvenlik yöneticileriniz için mükemmel görünürlük ve yönetilebilirlik sağlayan tek noktadan web arabirimi ile proxy'ler ve depolama alanları da dahil olmak üzere bütün ICAP özellikli sistemlerinizi kontrol edin.

Basit kontrol paneli: Ağ geçidi düzeyinde mevcut kurumsal güvenlik durumunu ölçmek için gereken her şey tek bir kontrol panelinde toplanır. Bu ise, acil durumlar da dahil olmak üzere, sorunlara anlık ve eksiksiz bir bakış açısı sağlar.

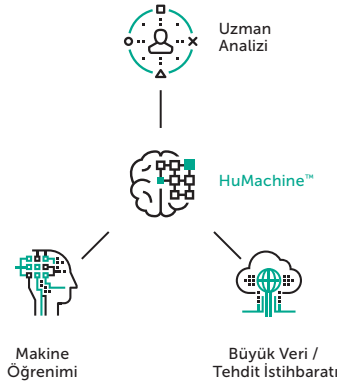
Olay yönetimi: Tehdit analizi sonuçları, olay merkezli bir yaklaşım kullanılarak sunulur ve gerçek zamanlı aktiviteleri gösterir. Kullanıcının internet davranışı da analiz edilebilir.

Esnek kural yapılandırma sistemi: Çözümün güvenlik katmanları gücünün yanı sıra, çözümün verimliliğin temelinde, mevcut iş süreçleriyle tutarlı olacak şekilde özel yapılandırılmış güvenlik politikaları yer alır. Kaspersky Web Traffic Security, yöneticilerin programı öğrenme sürecinde fazla vakit kaybetmeden, ağ geçidi güvenliğinin ayrıntılı yönetilmesine imkan vererek esnek fakat kullanımı kolay bir kural yapılandırma sistemi sunar.

Rol tabanlı erişim sistemi: Yöneticiler, farklı yönetici kategorilerinin kullanım haklarını kısıtlamak için belirli roller tanımlayabilir. Bu, şirket içi görev dağılımı veya MSP durumunda hizmet verilen müşterilere gerekli kontrol derecesinin sağlanması açısından kullanışlıdır.

Active Directory entegrasyonu: Kaspersky Web Traffic Security, bir şirketin BT ağında çalışan bilinen nesneler hakkında rol tabanlı erişim kurallarını ve güvenlik politikalarını yapılandırmak için kurumsal domain varlıkları (kullanıcılar, kullanıcı grupları, bilgisayarlar vb.) ile ilgili bilgiler edinir. Nesneleri tanımlayan veriler, kurumsal altyapıdaki en son değişikliklerle tutarlılığı sağlamak için Active Directory ve uygulama arasında sürekli olarak senkronize edilir.

Çoklu kullanıcı yapısı: MSP'ler ve çeşitli şirketler için geliştirilen özel bir mod farklı birimler veya yönetilen şirketler için özel alanlar ("çalışma alanları") atamanıza ve gerektiği şekilde "global" ve "yerel" politikaları birleştirerek bunları ayrı ayrı yönetmenize olanak tanır.



Nasıl satın alınır?
Kaspersky Web Security, satın aldığınız lisansa bağlı olarak çeşitli Kaspersky Lab ürünlerinde aktifleştirilmiş bir uygulamadır.

- Kaspersky Security for Internet Gateways
- Kaspersky Security for Storages
- Kaspersky Security for xSP
- Kaspersky Total Security for Business

www.kaspersky.com.tr