



FORCEPOINT Web Güvenliđi

FORCEPOINT BULUT VE KURUM İÇİ WEB GÜVENLİĞİ





Forcepoint Web Güvenliđi

FORCEPOINT BULUT VE KURUM İÇİ WEB GÜVENLİĐİ

İşletmeniz ve verileri sürekli saldırı altındadır. Geleneksel güvenlik çözümleri artık yeterli koruma sağlayamamaktadır. Hatta sizi veri kaybı ve uyumluluk riskleri ile karşı karşıya bırakabilir. Giderek riskli hale gelen mobil ve bulut bağlantılı dijital dünyada işletmenizin hayatta kalabilmesi için ağınızın ve verilerinizin gelişmiş tehditler, şifreli fidye yazılımları ve yetkisiz erişim kitlerine karşı korunması çok önemlidir.

İhtiyaca uygun ölçeklendirme yapılabilir.

Bu tür tehditlere karşı korunmak için şirketlerin birbirleri ile etkileşim halinde olan ve kurumun BT gereksinimlerine uygun çözümlere ihtiyacı vardır. Forcepoint Web Güvenliđi, web koruma paketinizi kuruluşunuzun ihtiyaçlarına göre uyarlamana yardımcı olan çeşitli kurulum seçenekleri ve modülleri sayesinde gelişmiş tehditler ve veri hırsızlığına karşı gerçek zamanlı koruma sağlar.

Forcepoint Web Güvenliđi, içeriđi anlayan, ve de bulut uygulaması keşif ve takibi yoluyla güçlü koruma sağlayarak, hem şirket içindeki kullanıcılar hem de mobil kullanıcılar için hassas verilerle ilgili riskleri azaltır.

Dahası, Forcepoint Web Güvenliđi diğer Forcepoint çözümleri ile kolayca entegre edilerek, en küçük güvenlik ekipleriyle bile gelen ve giden tehditlere karşı koruyabilen bütüncül ve tutarlı güvenlik kontrolleri oluşturabilir.

Web Güvenliđi Hedefleri

Günümüzde güvenlik çözümlerinin çođu Gelişmiş Tehditleri anında ele alamamaktadır. Forcepoint Web Güvenliđi gerçek zamanlı, gelişmiş bir tehdit savunmasıdır.

► Her Kullanıcıyı, Her Yerde Gelişmiş Tehditlerden Koruma

- » Hem şirket içi hem de uzaktan çalışanlar için ađa bağlandıkları her yerde koruma sağlayın.

► Bütüncül Görünürlük ve Kontrol

- » Kurumunuz bünyesinde kullanılan bulut uygulamalarını keşfedin. Bu uygulamaların kullanımını takip ederek en yüksek risk teşkil edenleri belirleyin ve engelleyin.

► Güvenlik Harcamanızı Azaltın ve İşletme Verimliliđini Artırın

- » Kuruluşunuz bünyesindeki bulut uygulamaları için görünürlük ve kontrol. Risk maruziyetinin yönetilmesini sağlamak için Shadow IT'yi keşfedin. Satır içi (vekil sunucu) yoluyla desteklenen bulut uygulamalara yönelik Web Güvenliđi Ağ Geçidinin bir parçası olarak entegre Bulut Erişimi Güvenlik Aracısı (CASB) özelliklerini kullanarak kontroller uygulayın.



"Forcepoint farklı ve mimari bir açıdan düşünmemizi ve daha fazla bulut uygulamayı kullanarak daha iyi ticari sonuçlara ulaşmamızı sağladı."

**— Chris Anderson, Altyapı Hizmetleri Başkanı,
Bendigo and Adelaide Bank**





Forcepoint Web Güvenliđi sekiz savunma deęerlendirme alanı sayesinde anti-virüs savunmasından çok daha fazlasını sunar

Forcepoint Web Güvenliđi

Gelişmiş Tehdit Koruması için Gerçek Zamanlı Analiz

Forcepoint Web Güvenliđi, Forcepoint ACE öngörü ve analiz yeteneđi ile birlikte karma bir puanlama sürecini kullanan sekiz savunma deęerlendirme alanı sayesinde anti-virüs savunmasından çok daha fazlasını sunar. Birden fazla gerçek zamanlı içerik motoru tüm web sayfası içeriđi, aktif komut dosyaları, web bağlantıları, bağlamsal profiller, dosyalar ve yürütülebilir öğeleri analiz eder.

Adli Verilere Gösterge Panelinden Kolay Erişim

Forcepoint Web Güvenliđi gelişmiş tehdit panosu, saldırının kime yapıldığı, hangi verilerin hedef alındığı, verilerin hedeflenen uç noktası ve saldırının nasıl gerçekleştirildiđi konularında adli raporlama sağlar. Güvenlik olayları, uygun durumlarda, veri hırsızlığı görüntü kaydını da içerir. Sistem, tüm haberleşmeleri analiz edecek yeteneđe sahiptir.

Entegre Veri Hırsızlığı Savunmaları

Sektör lideri entegre veri hırsızlığı savunmaları (opsiyonel) veri hırsızlığı girişimlerini tespit ederek engeller ve veri kaybı koruması (DLP) konusunda mevzuata uyum imkanı sağlar. Bu özelliklere örnek olarak: özel şifrelenmiş yüklemeler, parola dosyası veri hırsızlığı, yavaş veri sızıntıları (Drip-DLP), görsellerin içinde metnin optik karakter tanınması (OCR) ve konum belirleme farkındalığı gösterilebilir.

Entegre Sandboxing Sistemi

Entegre Sandboxing sistemi ile kötü niyetli davranışların otomatik analizini yaparak şirketinizin varlıklarını nasıl daha iyi koruyabileceğinizi öğrenin.

Bulut Uygulaması Keşfi, Takibi ve Kontrolü

Kurumunuz bünyesinde kullanılan bulut uygulamaları keşfedin ve kullanıcıların verilerinizi onaylanmamış bulut uygulamalar ve hizmetlere göndererek tehlikeye atmasını engelleyin. Bulut Erişimi Güvenlik Aracısı(CASB) ile kolay entegrasyon sağlayın.



Geliştirilmiş Koruma Modülleri

Hibrit Bulut Kullanımı

Web koruması ve politika uygulamalarını uzaktan çalışan kullanıcılara aktarın
Forcepoint Web Güvenliği'ni fiziksel veya sanal araç olarak özel bulutunuza uygulayın. Bu iki seçim de uzaktan çalışan kullanıcı korumasına yönelik olarak Forcepoint'in küresel bulut altyapısı ile daha da genişletilebilir.

WEB DLP

Veri hırsızlığına karşı dışa dönük ek koruma için içerik bilinçli, güçlü bir DLP motoru ekleyin
Forcepoint Web DLP, önceden tanımlanmış 1.700'den fazla politika ve şablonu kullanarak veri hırsızlığına karşı kısıtlama savunması yapar ve mevzuata uyum imkanı verir. Ayrıca, yavaş veri sızıntılarına karşı Drip-DLP, resim dosyalarındaki veri dosyalarının hırsızlığına karşı Optik Karakter Tanıma (OCR) ve suç amacıyla şifrelenmiş dosyaların tespitine yönelik Özel Şifreleme Tespiti gibi sektör lideri korumaları da içerir.

Sandboxing Sistemi

Kötü amaçlı yazılım dosyalarının otomatik ve manuel analizi için davranışa dayalı sandboxing sistemini entegre edin. Şüpheli dosyaları sanal ortamda analiz edin ve gelişmiş kötü amaçlı yazılımlardan en yüksek seviyede koruma sağlamak için basit dosya yürütmesi yerine çok daha derinlere bakın. Kötü niyetli dosyalar tespit edildiğinde otomatik olarak detaylı adli raporlama gerçekleştirilir.

Mobil Güvenlik

Politika ve korumalara iOS ve Android kullanıcılarını da dahil edin
Mevcut güvenlik politikalarınızı mobil cihazlara aktarın ve bu cihazları Gelişmiş Tehditler, kötü amaçlı mobil yazılımlar, kimlik avı saldırıları, sahtekarlık ve daha fazlasına karşı koruyun. Forcepoint Mobil Güvenlik, mobil cihazlara tam koruma sağlamak için mobil cihaz yöneticiniz (MDM) ile birlikte çalışır.

Bulut Erişimi Güvenlik Aracısı (CASB)

Hangi bulut uygulamalarının kullanıldığına dair görünürlük sağlamaya yönelik mevcut kabiliyeti tamamlamak için CASB işlevlerini kullanın
Bu CASB işlevleri satır içi (vekil sunucu) kurulumlara yönelik bulut uygulamalarını kontrol etmek için kullanılabilir ve web güvenliği ağ geçidinden kolayca aktarılabilir.



Forcepoint çözümlerinin arkasındaki güç

Forcepoint ACE

Forcepoint ACE, en etkili güvenlik çözümünü sunmak için karma risk puanlaması ve tahmine dayalı analizleri kullanarak web, e-posta, veri ve mobil güvenlik için gerçek zamanlı, satır içi ve bağlamsal savunmalar sağlar. Ayrıca, sektör lideri veri hırsızlığı koruması için veri bilinçli savunmalar yoluyla, gelen ve giden trafiği analiz ederek ihlallerin yayılmasını kısıtlar. Yıllar süren araştırma ve geliştirmenin ürünü olan gerçek zamanlı güvenlik, veri ve içerik analizine yönelik sınıflandırıcılar, ACE'nin geleneksel anti-virüs motorlarına göre her gün daha fazla tehdidi tespit etmesini sağlar (her gün güncellenen kanıtlar için bkz. <http://securitylabs.forcepoint.com>). ACE tüm Forcepoint çözümlerinin arkasındaki temel savunmadır ve Forcepoint ThreatSeeker Intelligence ile desteklenir.

Forcepoint ThreatSeeker Intelligence

Forcepoint Security Labs tarafından yönetilen Forcepoint ThreatSeeker Intelligence, tüm Forcepoint güvenlik ürünleri için temel kolektif güvenlik istihbaratını sağlar. Facebook'tan gelenler dahil 900 milyondan fazla uç noktayı birleştirir ve Forcepoint ACE güvenlik savunmaları ile birlikte günde 5 milyara yakın talebi analiz eder. Güvenlik tehditlerine yönelik bu geniş kapsamlı farkındalık sayesinde, Forcepoint ThreatSeeker Intelligence bir yandan gelişmiş tehditler, kötü amaçlı yazılımlar, kimlik avı saldırıları, tuzaklar ve sahtekarlıkları engelleyen gerçek zamanlı güvenlik güncellemeleri yaparken diğer yandan en son web derecelendirmelerini verir. Forcepoint ThreatSeeker Intelligence, tüm girdileri analiz etmek için ACE gerçek zamanlı savunmalarını kullanması açısından rakipsizdir. (Web Güvenliği'ne yükseltme yaptığınız zaman, Forcepoint ThreatSeeker Intelligence web tehditleri ve veri hırsızlığına maruz kalma olasılığınızı azaltmaya yardımcı olur.)

Birleşik Mimari

Forcepoint, sınıfının en iyisi güvenlik ve birleşik mimarisi sayesinde, Forcepoint ACE'nin gerçek zamanlı ve satır içi savunmaları ile anında koruma sağlar. ACE'nin rakipsiz gerçek zamanlı savunmaları, Forcepoint ThreatSeeker Intelligence ve Forcepoint Security Labs araştırmacılarının uzmanlığı ile desteklenir. Tek bir birleşik kullanıcı arayüzü ve bütünlük güvenlik istihbaratına sahip mimari sayesinde güçlü bir sonuç elde edilir.



8 temel alanda bütüncü siber değerlendirme özellikleri.

- Derinlemesine yapılan denetimleri desteklemek için 10.000'i aşkın analitik kuralı.
- Öngörebilen güvenlik motoru birçok hamleyi önceden görür.
- Satır içi çalışma, tehditleri sadece izlemez aynı zamanda **engeller**.

Diğer Kabiliyetler

- ▶ **Ofis Dışı Çalışanın Korunması.** Hibrit Bulut Kullanımı sayesinde kurumsal, şube ve ofis dışı çalışan kullanıcıları tek bir konsol ve politika vasıtasıyla yönetin.
- ▶ **Esnek SSL Denetimi.** Granüler SSL denetimi kabiliyetleri, HTTPS trafiğini takip ederken gizlilik ve mevzuat şartlarına da uymanızı sağlar.
- ▶ **Tehdit İstihbaratı için API.** Özel API'lar ile, sektöre ve bölgeye özgü istihbaratı toplayarak web güvenliğinizi daha akıllı hale getirir ve güvenlik yönetimi otomasyonunu mümkün kılar.
- ▶ **Uygulama ve Protokol Kontrolü.** Ağ Aracısı, daha güçlü bir güvenlik pozisyonu için yüzlerce protokol ve uygulama arasında granüler kontrol sağlar.
- ▶ **Esnek Raporlama.** Dört özelleştirilebilir pano ile birlikte 60'tan fazla önceden tanımlanmış, özelleştirilebilir rapor, okunması kolay ticari ve teknik bilgilerin yanı sıra tehdit seviyeleri gibi konularda değerli bilgiler içerir.
- ▶ **Çoklu Kullanım Seçenekleri.** Bulut, hibrit veya şirket içi (sanal veya fiziksel) olarak kullanım tercihinizi yapın.
- ▶ **Vekil Sunucu Olmadan Uç Noktası Koruması.** Çözümümüz her yerde, her ağda çalışarak kullanıcıları korur. Uygulamalar, genellikle vekil sunucu tabanlı bulut çözümlerde sorun yaratan ortamlarda çalışmaya devam etmektedir.
- ▶ **Entegre DLP Incident Risk Ranking .** Sektörde bir ilk olan güvenlik analizi kabiliyeti DLP soruşturmalarının maliyetini düşürürken verimliliğini artırır.
- ▶ **Uzaktan Çalışan Kullanıcılar için Genişletilmiş İnternet Erişimi.** Bir çalışan kurumsal ve kurumsal olmayan yerlerden bağlantı kurduğunda farklı politikalar uygulayın (evde video yayınlarına izin verilir, kayıtlı bir kurumsal yerde ise engellenir).
- ▶ **Bulut Uygulama Kontrolü.** Onaylanmamış bulut uygulamaların kullanımını engellerken, kurum tarafından onaylandığı kabul edilen uygulamaların kullanımına izin verin. Satır içi (vekil sunucu) kurulum modunda bulut uygulamalar için kontrol sağlamak üzere web güvenliği çözümlerini içeren tüm CASB özelliklerini kolayca ekleyin.
- ▶ **Web Güvenliği Buluta Aktarma araçları.** Forcepoint'in lider şirket içi araçlarından sektörün en güvenli bulut uygulaması olan Forcepoint Web Security Cloud'a geçiş yapın.



FORCEPOINT HAKKINDA

Forcepoint, nerede bulunursa bulunsun kritik veriler ve fikri mülkiyet ile etkileşim halindeki insanların niyetini anlamaya odaklanarak siber güvenliğe yeni bir bakış açısı kazandırıyor, dönüştürüyor. Ödün vermeyen sistemlerimiz, şirketlerin çalışanlarına gizli veriler için sınırsız erişim vermesini sağlarken fikri mülkiyeti korur ve uyumluluğu kolaylaştırır. Genel merkezi Teksas, Austin'de bulunan Forcepoint, dünya genelinde 20.000'den fazla kuruluşu desteklemektedir. Forcepoint hakkında daha fazla bilgi için, www.forcepoint.com adresini ziyaret edin ve Twitter'da bizi takip edin: @ForcepointSec.

İLETİŞİM

www.forcepoint.com/contact

©2018 Forcepoint.

[BROCHURE_FORCEPOINT_EMAIL_SECURITY_TUR] 400002.022718