

Forcepoint ONE Web Security

Verimliliği değil, veri kaybını ve kötü amaçlı yazılım saldırılarını engelleyin

Kullanım Durumları

- › Çalışanların internete hızlı ve güvenli erişmesini sağlayın
- › Kabul edilebilir kullanım politikalarını uygulayın
- › Hassas verilerin onaylı olmayan web sitelerine yüklenmesini engelleyin
- › Kullanılabilirlikten taviz vermeden kötü amaçlı yazılımların kullanıcı cihazlarına girmesini engelleyin
- › Gölge BT'yi tespit ve kontrol edin
- › Kullanıcıların özel verilerinin kurumsal olarak ifşa edilmesini önleyin

Çözüm

- › Entegre DLP ve gelişmiş tehdit koruması ile sağlanan hızlı web güvenliği
- › Kullanıcı grubu, cihaz türü, kullanıcı konumu, web sitesi kategorisi, web sitesi risk puanı ve daha pek çok unsura dayalı detaylı Sıfır Güven erişim ve veri kontrolleri
- › Dağıtık mimari sürekli çalışan platformlardaki tıkanma noktalarını ortadan kaldırıyor
- › Kategorize edilmemiş ve yeni kaydedilmiş sitelerde güvenle gezinmeyi ve dosya indirmeyi sağlamak için Uzak Tarayıcı İzolasyonu (RBI) içerir

Sonuçlar

- › Verimlilik artışı, çalışanların internete her yerden sorunsuz ve güvenli bir şekilde girmesinin sağlanması
- › Bulut ortamındaki hassas verilerin kontrol edilmesi ve kötü amaçlı yazılımların engellenmesi yoluyla riskin azaltılması
- › Güvenlik operasyonlarını basitleştirerek maliyetleri azaltın

İnternet hem bir nimet hem de bir lanettir. Pek çok insan işlerini yapmak için bilgiye ihtiyaç duyuyor, ancak internet aynı zamanda veri sızıntıları, İK politikası ihlalleri, üretkenlik kaybı ve kötü amaçlı yazılım bulaşma riskleri de yaratıyor. Üretken Yapay Zeka riskleri daha da artırdı - büyük verimlilik artışları vaat ederken bir yandan da işletmenizi daha fazla riske maruz bırakıyor. Bununla birlikte, doğru koruma önlemleri ile hassas verileri güvende tutabilir ve kabul edilebilir kullanım olanakları sağlarken yapay zekanın sunabileceği verimlilik artışlarından yararlanabilirsiniz. Verileri ve insanları güvende tutmamanın yarattığı etkiler her geçen gün artarken, internet üzerindeki etkileşimleri güvence altına almak modern kuruluşlar için stratejik bir gerekliliktir.

Çalışanların internete hızlı ve güvenli erişmesini sağlayın

Modern web güvenliği çözümlerinin birçoğu, şirket içinde veya bulutta olması fark etmeksizin, tüm web trafiğini merkezileştirilmiş bir veri merkezinden geçmeye zorlar ve bu da modern web uygulamalarına önemli ölçüde etki edebilecek bir gecikme süresi ekler. Ayrıca, bulut mimarileri talep üzerine ölçeklenebilecek şekilde tasarlanırken birçok SWG tedarikçisi bu kadar yüksek bir oranda dağıtık olan bulut varlığı sunamıyor. Buna karşılık Forcepoint ONE, dünya çapındaki 300'den fazla Varlık Noktası ile son derece esnek bir bulut mimarisi sağlamakla kalmaz, aynı zamanda müşterilere daha fazla esneklik sunan alternatif bir seçenekle daha da fazlasını gerçekleştirir: Tıkanıklık noktalarını ortadan kaldıran ve performansa duyarlı web içeriği ve uygulamaları açısından rakip Güvenli Web Ağ Geçitlerine göre iki kata kadar daha fazla verim sağlayabilen bir cihaz içi araç sunar. Bu seçenek, güvenlik politikalarını kullanıcının cihazında yerel olarak uygular ve böylece, trafik doğrudan kullanıcı ve web sitesi arasında gerçekleşebilir.

Riskli web sitelerinde kabul edilebilir kullanım politikası (AUP) denetimlerini uygulamak

Web, şirket işleri dışında başka amaçlar için de kullanılan dikkat dağıtıcı bir yer olabilir. Forcepoint ONE'daki web kontrolleri trafiği izole etmek için engelleme, onay sayfası kullanma, kota süresi kullanma, çok faktörlü kimlik doğrulama isteme, erişim izni verme gibi işlemlere ve hatta RBI kullanmanıza olanak tanır. Kullanıcı grubuna, cihaz durumlarına, konuma göre erişimi yönetebilirsiniz. Bu sayede bir kuruluş, Üretken Yapay Zeka sitelerinin gölge BT kullanmalarını engelleyecek kontrolleri kolaylıkla uygulayabilir; örneğin, kod yazarları kurumsal onaylı kaynaklara yönlendirecek bir engelleme sayfası oluşturabilir, farklı Üretken Yapay Zeka sitelerini birbirinden ayırarak ayrıntı düzeyi sağlayabilir, sohbet bazlı veya multimedya üreten Üretken Yapay Zeka sitelerine erişime izin verirken aynı zamanda bu sitelere hangi verilerin gönderilebileceğine dair koruma önlemleri uygulayabilir.

Hassas verilerin onaylı olmayan web sitelerine yüklenmesini engelleyin

Güvenlik altyapımız sayesinde, yasal düzenlemelere tabi verilerin veya fikri mülkiyetin kişisel depolama alanlarına, sosyal medyaya, kişisel e-posta hesaplarına veya üretken Yapay Zeka sitelerine gönderilmesini önleyebilirsiniz. Kolayca kullanılabilen kontroller ile hassas veriler için dosya yüklemelerini ve metin gönderilerini tarayabilir ve engelleyebilirsiniz. İsteğe bağlı olarak müşteriler, sektörün önde gelen bu gelişmiş veri güvenliği çözümünü daha da güçlendirmek için Forcepoint ONE Data Security'nin gelişmiş DLP politikalarını da alabilir.

Kullanılabilirlikten taviz vermeden kötü amaçlı yazılımların kullanıcı cihazlarına girmesini engelleyin

Forcepoint ONE Web Security hizmeti, kategorilere göre web sitelerinin engellenmesi, indirilen dosyaların dahili olarak taranması ve Uzak Tarayıcı İzolasyonu gibi Zero Trust tabanlı gelişmiş tehdit koruması dahil olmak üzere web kaynaklı kötü amaçlı yazılımlara karşı çoklu koruma biçimleri sağlar. Forcepoint RBI sayesinde, virüs bulaşmış siteler veya indirilmiş dosyalar bile güvenli ve verimli bir şekilde kullanılabilir.

Gölge BT'yi tespit ve kontrol edin

Web güvenliği hizmeti, tercih edilen şirket uygulamaları yerine kullanılan web sitelerini belirlemeye yarar. Bu "gölge BT" siteleri otomatik olarak derlenir ve Cloud Apps gösterge panosunda görüntülenir.

Kullanıcıların özel verilerinin kurumsal olarak ifşa edilmesini önleyin

Kurumlar, çalışanların gizliliğini korumak için bankacılık, sağlık ve sigorta verileri gibi kişisel bilgilerle (PII) kullanılan belirli web sitesi kategorilerine giden ve bu sitelerden gelen trafiğin şifrelerinin çözülmesini ve incelenmesini önleyebilir.

Forcepoint ONE Web Security çalışma süresini, üretkenliği ve performansı en üst düzeye çıkarır

Web Güvenliği hizmeti, web erişimini güvence altına almak ve kullanıcı verimliliğini korumayı sağlayan 300 varlık noktası (PoP), küresel erişilebilirlik ve kanıtlanmış %99,999 çalışma süresine sahip gelişmiş bulut platformumuz Forcepoint ONE'in bir parçasıdır. Forcepoint ONE, kurumsal SaaS, web ve özel uygulamalara erişimi güvence altına almak için CASB, SWG ve ZTNA'yı entegre ederek güvenliği kolaylaştırır.

Gerçek dünyada bulut güvenliğini basitleştirmek

Forcepoint ONE bulut platformu, bulut güvenliğinin uygulanması için "kolay bir düğme" sağlar.

Yöneticiler tek bir konsoldan, Forcepoint RBI kullanarak Zero Trust Web Access'i zorunlu kılmak da dahil olmak üzere gerçek zamanlı olarak herhangi bir siteye erişimi yönetebilir ve dosya indirme ve yüklemelerini kontrol edebilir.





Evden çalışan bir iş analisti olan Kris iş gününe başladığında web güvenlik hizmetinin işlerini nasıl basitleştirdiğini görelim.

<p>Kris, şirketle ilgili bir araştırma için reddit.com sitesini tarıyor.</p>	<p>Kris, kötü amaçlı yazılımlar konusundaki en son paylaşımları araştırmak için reddit.com/r/technology adresini ziyaret ediyor. SWG içerik politikaları, izin seviyesinde detaylı kontrol sunar; Reddit'in bu alt bölümü işle ilgili olarak kabul edildiğinden Kris bu bölüme erişebilir.</p>
<p>r/technology alt bölümünde, Kris yanlışlıkla uygunsuz bir sayfanın bağlantısına tıklıyor.</p>	<p>Kris'in Forcepoint ONE yöneticisi, r/technology gibi dizinlere erişime izin veren ancak uygunsuz alt bölümlere ve sayfalara erişimi engelleyen SWG içerik politikaları oluşturmuş. SWG, Kris'in hatasını önler ve yeni sayfayı engeller.</p>
<p>Kris, şirket bilgisayarında müşterilerin kişisel bilgilerini içeren gizli bir çalışma belgesi oluşturuyor ve ardından çalışmaya kişisel bilgisayarında devam etmek istiyor. Dosyayı kişisel bulut depolama uygulamasına yükleyip, ardından kişisel bilgisayarına yüklemeye çalışıyor.</p>	<p>Şirketin Forcepoint ONE yöneticisi, iş verilerinin kaybolmasını önlemek için hassas müşteri bilgilerinin (PII) herhangi bir kişisel dosya paylaşımı web sitesine yüklenmesini önleyen bir SWG içerik politikası yaratmış durumda. Kris yükleme işlemini yapmak istediğinde, işlem engelleniyor ve neden engellendiğini açıklayan bir mesaj görüntüleniyor.</p>

Web, bulut ve özel uygulamalar için entegre güvenlik çözümünün bir parçası entegre güvenlik çözümünün bir parçası

Web güvenliğine ek olarak Forcepoint ONE bulut güvenlik platformu, herhangi bir kurumsal SaaS kullanıcısının ve özel uygulamaların iş bilgilerine erişimini güvence altına alır:

- **Cloud (SaaS and IaaS):** CASB internete bağlı herhangi bir cihazda bulunan modern bir tarayıcıdan, üçüncü taraf kimlik sağlayıcıları (IdP'ler) ile SAML 2 entegrasyonunu destekleyen herkese açık web uygulamalarına bağlamsal erişim kontrolü, veri kaybı önleme (DLP) ve kötü amaçlı yazılım koruması uygular. Popüler IaaS ve SaaS'lardaki bekleyen veriler de hassas veriler ve kötü amaçlı yazılımlar için taranıp düzeltme yapılabilir. SSE kanalları üzerinden gelişmiş DLP politikalarını uygulamak üzere Forcepoint ONE Data Security ile entegre olur.
- **Özel uygulamalar:** ZTNA, VPN'lerin getirdiği karmaşıklık veya riskler olmadan özel uygulamalara güvenli ve basit erişim sağlar. Diğer Forcepoint ONE çözümleri gibi, ZTNA da tüm özel web uygulamaları için bağlamsal erişim kontrolü, DLP ve kötü amaçlı yazılım korumasına sahiptir.
- **Diğer özellikler:** Web'deki tehditlere karşı en üst düzeyde koruma sağlamak için tanınmayan veya henüz kayıt altına alınmış olan siteler haricinde de kullanılmak için CDR ile temel RPI düzeyini artırın veya kurumsal düzeyde kötü amaçlı yazılım korumalı alanı ve analizi için Gelişmiş Kötü Amaçlı Yazılım Tespiti ve Koruması ekleyin.

Daha fazla ayrıntı için Forcepoint ONE Çözüm Özetini okuyun.



Bulut uygulamalarında bulunan ve tüm cihazlardan erişilen verileri güvenlik altına almaya hazır mısınız?

Bir demo ile başlayalım.

forcepoint.com/contact