Forcepoint

Çözüm Özeti

Secure Web Gateway

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
- Dağıtılmış mimari, yüksek çalışma süresine ve hiper ölçeğe sahip AWS platformundaki darboğazları ortadan kaldırır
- Güvenli tarama ve indirmeler için isteğe bağlı RBI çözümü

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
- Politikaların tek bir yerden belirlenmesiyle güvenlik operasyonlarının basitleştirilmesi ve maliyetlerin azaltılması

İnternet, hem iyi hem de kötü özelliklere sahiptir. Çoğumuz işimizi yapmak için gereken bilgileri almak adına internete güveniyoruz. Ancak internet; veri sızdırma, İK politikası ihlalleri, verim kaybı ve kötü amaçlı yazılım bulaşması gibi riskler de teşkil etmekte. Verileri ve insanları güvende tutamamanın maliyeti her geçen gün ağırlaşırken, internetteki etkileşimleri güvenli hale getirmek, modern kurumlar için stratejik bir gereksinime dönüşmüş durumda.

Çalışanların internete hızlı ve güvenli erişmesini sağlayın

Pek çok SWG uygulaması, tüm web trafiğini merkezi bir veri merkezi (tesis içi veya bulutta) üzerinden yönlendirerek, modern web uygulamalarına ciddi şekilde engel olabilecek bir gecikmeye neden olmaktadır. Forcepoint ONE'da bulunan SWG çözümü ise tam tersine bu tür darboğazları ortadan kaldıran dağıtılmış bir mimariye sahiptir ve performans açısından hassas web içeriği ve uygulamaları için iki kat fazla performans sağlayabilir. Bunu, güvenlik politikalarını yerel olarak kullanıcının cihazında uygulamak suretiyle trafiğin doğrudan kullanıcı ile web sitesi arasında akmasını sağlayarak yapıyoruz.

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

İnternet, her zaman şirket işleri için kullanılmayan, dikkat dağıtıcı bir yer olabilir. Forcepoint ONE ile sunulan SWG çözümü, tam yol kontrolüyle insanların verimli olmayan veya uygunsuz web sitelerini ziyaret etmelerini engellemenizi veya buna izin vermenizi sağlar; örneğin, bazı Reddit sayfalarını engellerken, diğerlerine izin verebilirsiniz. Erişimi; kullanıcı grubu, cihaz durumu, konum, URL kategorisi (önceden belirlenmiş veya özel), saygınlık puanı ve kurumsal uygulama risk puanı gibi unsurları baz alarak yönetebilirsiniz. Özel URL kategorileri, tam URL dizin yolu girdilerini içerebilir ve yöneticilerin farklı dizinlere farklı politikalar uygulamasına imkan tanır.

Hassas verilerin onaylı olmayan web sitelerine yüklenmesini engelleyin

SWG çözümümüzle, düzenlenen verilerin veya fikri mülkiyet unsurlarının kişisel dosya depolama alanlarına, sosyal medyaya veya kişisel e-posta hesaplarına gönderilmesini engelleyebilirsiniz. Forcepoint ONE'da bulunan CASB ve ZTNA hizmetleri tarafından kullanılan aynı ön tanımlı ve özel DLP modellerini kullanarak hassas verilere ilişkin dosya yükleme ve HTTPS gönderim yöntemlerini tarayabilir ve engelleyebilirsiniz.

Kullanılabilirlikten taviz vermeden kötü amaçlı yazılımların kullanıcı cihazlarına girmesini engelleyin

SWG çözümümüz, web kaynaklı kötü amaçlı yazılımlara karşı, belli web sitesi kategorilerinin engellenmesi, indirilen dosyaların taranması ve Remote Browser Isolation gibi Sıfır Güven tabanlı gelişmiş tehdit koruması yöntemleri dahil pek çok koruma yöntemi sağlar. RBI çözümümüz sayesinde kötü amaçlı yazılımlar içeren siteler veya indirilmiş dosyalar dahi güvenli ve etkin bir şekilde kullanılabilir.

Gölge BT'yi tespit ve kontrol edin

SWG hizmeti, tercih edilen şirket uygulamalarının yerine kullanılan web sitelerini tespit etmek için CASB çözümümüzle birlikte kullanılabilir. Bu "gölge BT" siteleri otomatik olarak toplanır ve konsolda 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.

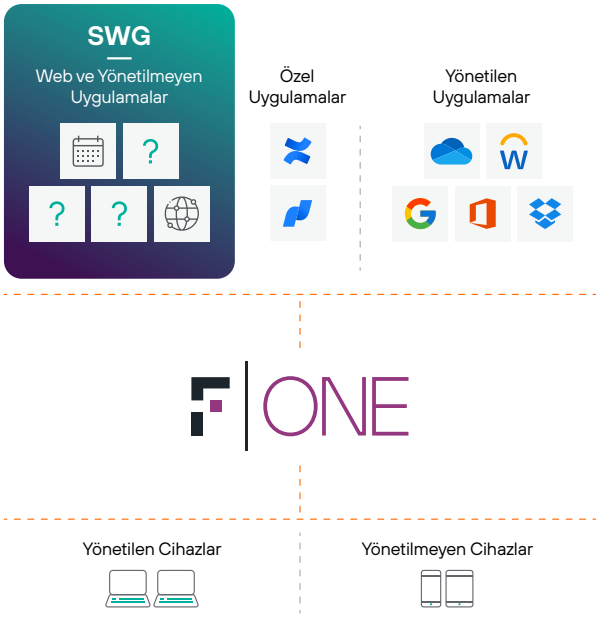
Forcepoint ONE ile sunulan SWG çözümü; çalışma süresini, verimi ve performansı maksimuma çıkarır

SWG çözümü, 300 varlık noktasına (PoP), küresel erişilebilirliğe ve web erişimini ve kullanıcıların verimliliğini korumak için kanıtlanmış %99,99 çalışma süresine sahip olan hiper ölçek tabanlı bulut platformumuz olan Forcepoint ONE'ın bir parçasıdır. Forcepoint ONE, kurumsal SaaS uygulamalarına, web uygulamalarına ve özel uygulamalara erişimi güvenlik altına almak için CASB, SWG ve ZTNA çözümlerini birleştirerek güvenliği basitleştirir.

Gerçek Dünyada Web Güvenliğini Basitleştirmek

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

Yöneticiler, tek bir konsoldan erişimi yönetebilir ve yönetimli cihazlarla herhangi bir web sitesi arasında gerçekleşen dosya indirme ve yükleme işlemlerini kontrol edebilir.



Her etkileşim için **toplam bulut güvenliği** sağlayın

Evden çalışan bir iş analisti olan Kris iş gününe başlarken, SWG'nin web güvenliğini nasıl basitleştirdiğini görelim.

Kris, şirketle ilgili bir araştırma için reddit.com sitesini tarıyor.	Kris, kötü amaçlı yazılımlar konusundaki en son paylaşımları araştırmak için reddit.com/r/technology adresini ziyaret ediyor. SWG içerik politikaları, dizin seviyesinde detaylı kontrol sunar; Reddit'in bu alt bölümü işle ilgili olarak kabul edildiğinden Kris bu bölüme erişebilir.
r/technology alt bölümünde, Kris yanlışlıkla uygunsuz bir sayfanın bağlantısına tıklıyor.	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.
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.	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.

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

Forcepoint ONE hepsi bir arada platform, SWG çözümüne ek olarak, her türlü kurumsal SaaS uygulaması ve özel uygulamadaki iş bilgilerine erişimi de güvenlik altına alır:

- → **Bulut (SaaS ve IaaS):** CASB, tüm internete bağlı cihazlarda ve tüm modern tarayıcılarda üçüncü taraf kimlik sağlayıcılar (IdP'ler) ile SAML 2 entegrasyonunu destekleyen halka açık tüm web uygulamaları için bağlamsal erişim kontrolü, data loss prevention (DLP) ve kötü amaçlı yazılım koruması sağlamaktadır. Popüler SaaS ve IaaS uygulamalarındaki durağan verilerde de kötü amaçlı yazılım ve hassas veri taraması yapılabilir ve gerekli önlemler alınır. Özel web uygulamaları için SWG ve ZTNA'da kullanılan aynı DLP eşleştirme modellerini kullanır.
- → **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.
- → RBI veya gerektiğinde bulut sağlayıcılarda riskli yapılandırmalar (CSPM) olup olmadığının taranması gibi **ek özellikler**.

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/tr/contact