Forcepoint

Çözüm Özeti

Forcepoint ONE: Bulut platformu hibrit iş gücü için güvenliği basitleştiriyor

Kullanım Durumları

- Karma çalışanların web, bulut ve özel uygulamalardaki verilerle etkileşimlerini görün ve kontrol edin.
- Yönetilen veya yönetilmeyen cihazlardan erişilen hassas verilerin suistimal edilmesini önleyin.
- Yüksek riskli web içeriklerine erişimi kontrol altına alın.
- VPN'lerin getirdiği karmaşıklık olmadan iş kaynaklarına ve özel uygulamalara uzaktan, hızlı ve güvenli erişim sağlayın.

Çözüm

- Tek ve birleşik bir platform, bir politika dizisinin tüm uygulamalarda tek bir konsoldan ve tek bir uç nokta aracısı üzerinden yönetilmesini sağlıyor.
- Güvenli Web Ağ Geçidi (SWG), Bulut Erişimi Güvenlik Aracısı (CASB) ve Sıfır Güven Ağ Erişimi (ZTNA) çözümlerini bir araya getirerek erişimi ve verileri güvenli hale getiren hepsi bir arada bulut tabanlı bir hizmet.
- Saldırganları dışarıda, hassas verileriyse içeride tutan entegre gelişmiş tehdit koruması ve veri güvenliği.
- RBI, halka açık bulut kiralayanların riskli yapılandırmalara karşı taranmasını sağlayan CSPM, içerik tehditlerinin ortadan kaldırılmasını sağlayan CDR ve diğer pek çok ek özellik (ayrıntılar için bkz. sayfa 2).

Outcome

- Basitleştirilmiş - web, bulut ve özel uygulama güvenliğini tek bir politika dizisi, tek bir konsol ve aracıda (aracısız destek özelliğiyle) bir araya getirir.
- Modern - Sıfır Güven ilkelerini bir SASE mimarisi ve Uzaktan Tarayıcı İzolasyonu ve indirilen dosyaların sterilize edilmesi gibi gelişmiş güvenlik çözümleriyle birleştirir.
- Her yerde - 300'den fazla varlık noktasıyla (PoP) küresel olarak kullanılabilmektedir.
- Güvenilir - 2015'ten bu yana doğrulanmış şekilde %99,99 çalışma süresi sağlar.
- Hızlı - darboğazları ortadan kaldırmak için dağıtılmış uygulama ve otomatik ölçeklemeden faydalanır.

Veri Öncelikli Güvenlik

Daha etkili bir çözüm var. Kullanıcılar artık web siteleri, bulut uygulamaları ve özel uygulamalar gibi pek çok yere yayılmış verilerle her yerden çalışabiliyor.

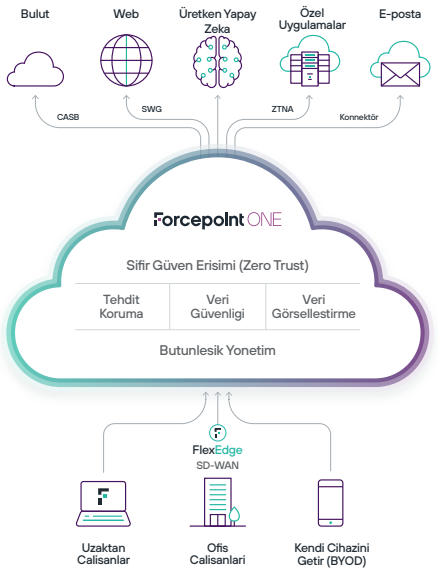
Ofise dönüş (RTO) girişimlerini ve hibrit iş güçlerini desteklemek için güvenlik ekiplerinin, verileri resmin merkezine koyan birleşik bir güvenlik platformuna ihtiyacı var. Güvenlik kontrollerinin web, bulut ve özel uygulama erişimine tutarlı görünürlük ve kontrolle yayılabilmesi gerekiyor, böylece kuruluşlar veri kaybını daha gerçekleşmeden durdurarak kayıpların önüne geçebiliyor.

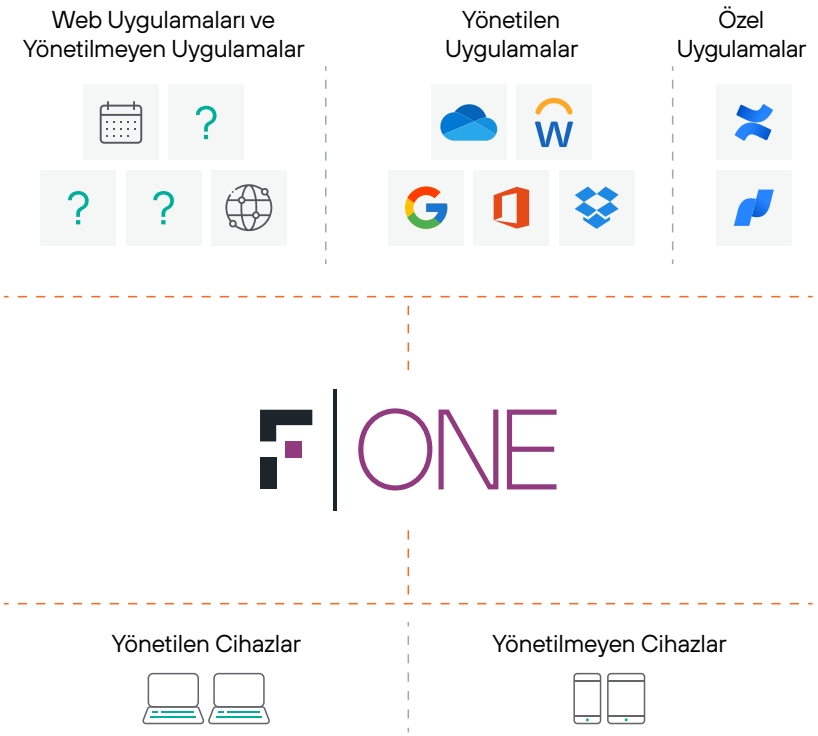
Veri öncelikli bir çözüm sayesinde işletme verilerinin güvenliği artık istedikleri yerde çalışanlar için sağlanabiliyor.

Forcepoint ONE Güvenliği Basitleştiriyor

Forcepoint ONE, güvenliği basitleştiren hepsi bir arada bir bulut platformudur. Güvenli Web Ağ Geçidi (SWG), Bulut Erişimi Güvenlik Aracısı (CASB) ve Sıfır Güven Ağ Erişimi (ZTNA) dahil kritik güvenlik hizmetlerini birleştirmemiz sayesinde, Sıfır Güven ve Güvenlik Hizmetini (SASE'nin güvenlik bileşeni olan SSE) hızla uygulayabilirsiniz.

Artık bölünmüş ürünlerle uğraşmak yok. Size pek çok çözüm sunan tek bir platform, konsol ve aracı sağlıyoruz. Tek bir güvenlik politikası dizisiyle görünürlük sağlayın, erişimi yönetin, yönetilen ve yönetilmeyen uygulamalarda ve tüm cihazlarda bulunan verileri koruyun.





Herhangi bir yerde çalışanlar için her yerde veri güvenliği

Forcepoint ONE'ın bulut tabanlı Sıfır Güven özelliklerinden bazıları:

- **Bulut uygulamaları ve özel uygulamalar için aracısız BYOD güvenliği** – Kişisel cihazlardan özel iş web uygulamalarını güvenle kullanın ve hassas verileri güvende tutun.
- **Entegre gelişmiş tehdit koruması ve veri güvenliği** tüm ağ geçitlerinde veri kaybını veya sızıntısını engeller ve bilgisayar korsanlarını dışarıda tutar.
- **Bulut, web ve özel uygulama erişimi için birleşik ağ geçitleri.** SWG, CASB ve ZTNA için tek bir yerden yönetilen iş uygulamalarına kimlik tabanlı erişim kontrolü.
- **Küresel erişim ve dinamik ölçekleme** – AWS üzerine kurulu 300 PoP, çalışanlarınız nerede olursa olsun hızlı ve düşük gecikmeli bağlantı ve %99,99 çalışma süresi sağlar.

Web, bulut ve özel uygulamalar için birleşik güvenlik

- **Bulut:** CASB, tüm cihazlardan kurumsal SaaS uygulamalarına ve verilerine erişim konusunda parçalı erişim sağlar. CASB, hassas verilerin indirilmesini ve kötü amaçlı yazılımların yüklenmesini gerçek zamanlı olarak engeller. Popüler SaaS ve IaaS uygulamalarındaki durağan verilerde kötü amaçlı yazılım ve hassas veri taraması yaparak gerekli önlemleri alır. CASB, gölge BT uygulamalarını tespit eder ve tüm yönetimli cihazlardan erişimi kontrol altına alır.
- **Web:** SWG, tüm web siteleriyle gerçekleştirilen etkileşimleri riske ve kategoriye bağlı olarak takip ve kontrol eder, kötü amaçlı yazılımların indirilmesini veya hassas verilerin kişisel dosya paylaşımına ve e-posta hesaplarına yüklenmesini engeller. Cihazlara kurulan SWG çözümümüz, kabul edilebilir kullanım politikalarının her yerdeki yönetimli cihazlarda uygulanmasını sağlar.
- **Özel uygulamalar:** ZTNA, VPN'lerin getirdiği karmaşıklık veya riskler olmadan özel uygulamalara güvenli ve basit erişim sağlar.

Entegre gelişmiş tehdit koruması ve veri güvenliği

- **Veri Kaybını Önleme (DLP):** Yüklenen ve indirilen dosya ve metinlerde hassas veri taraması yapılır ve gerektiğinde engelleme, takip, şifreleme veya redaksiyon işlemleri uygulanır.
- **Kötü amaçlı yazılım tarama:** Yüklenen ve indirilen dosyalarda kötü amaçlı yazılım taraması yapılır ve bu yazılımlar tespit edildiğinde engellenir.

Tek bir politika dizisiyle basitleştirilmiş uygulama

- Yapılandırma, takip ve raporlama için **tek bir yönetim konsolu.**
- Kullanıcı konumu, cihaz türü, cihaz durumu, kullanıcı davranışı ve kullanıcı grubuna bağlı olarak web, bulut veya özel uygulamalara erişimin kontrol edilmesini sağlayan **tek bir oturum açma politikası dizisi.** Bu parametreler, hesapların ele geçirilmesini önlemeye yardımcı olur.
- Yönetimli SaaS uygulamaları, özel uygulamalar ve web siteleri için hassas veri ve kötü amaçlı yazılım indirme ve yükleme işlemlerinin yanı sıra yönetimli SaaS ve IaaS uygulamalarında depolanan verileri kontrol etmeyi amaçlayan **tek bir DLP politikaları seti.**
- Windows ve MacOS'te tarayıcı dışı istemci uygulamaları ve gölge BT kontrolü için SWG, CASBm ve ZTNA desteği sağlayan **birleşik cihaz aracıları.**
- Güvenlik riskleri, genel kullanım ve hepsi bir arada bulut güvenliği platformunun etkisi hakkında hızlı içgörüler sunan **birleştirilmiş analiz ve değer görselleştirme** özelliği.

Gerektiğinde ek özellikler sunulmaktadır

- **Bulut Güvenlik Yapısı Yönetimi (CSPM):** AWS, Azure ve GCP kullanıcı ayarlarında riskli yapılandırma taraması yaparak manuel ve otomatik çözümler sağlar.
- **SaaS Güvenlik Yapısı Yönetimi (SSPM):** Salesforce, ServiceNow ve Office 365 kullanıcı ayarlarında riskli yapılandırma taraması yaparak manuel ve otomatik çözümler sağlar.
- **Uzaktan tarayıcı izolasyonu (RBI):** Tarayıcıyı bulutta barındırılan bir sanal makinede çalıştırarak kullanıcıların yerel cihazlarını web tabanlı kötü amaçlı yazılımlardan korur.
- **Forcepoint Classification:** Data Classification etiketleme doğruluğunu artırmak için yapay zeka destekli önerilerle etiketleme.
- **Bulut Güvenlik Duvarı:** Tüm internet trafiğini güvence altına almak ve savunmasız şubeleri suistimal etmek için tasarlanmış saldırılara karşı koruma sağlamak için SWG eklentisi.

İşleri basitleştiren abonelikler

Kullanıcı başına yıllık abonelik imkanı sunulmaktadır:

- Web, bulut ve özel uygulama güvenliği için Hepsi Bir Arada sürümü.
- Müşterilerin daha sonra bulut ve özel uygulama güvenliği ekleyebilmesini sağlayan Web Güvenliği sürümü.
- Tüm abonelikler; merkezi bulut yönetimi, veri koruması sağlayan birleşik politikalar, birleşik bir uç nokta aracısı üzerinden otomatik erişim ve kapsamlı raporlama özelliklerini içerir.

forcepoint.com/contact