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 ve çeşitli GenAI sitelerine erişimi kontrol altında tutun.
- VPN'lerin getirdiği karmaşıklık olmadan iş kaynaklarına ve özel uygulamalara uzaktan, hızlı ve güvenli erişim sağlayın.

Çözüm

- Tek ve birleşik bir platform, tüm iş uygulamaları genelinde tutarlı güvenlik politikalarının yönetilmesini sağlar.
- 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.
- Veri etiketleme için Forcepoint Classification.

Outcome

- Sadeleştirilmiş - web, bulut ve özel yazılımlar için güvenliği bütünleşik bir platformda bir araya getirir (aracısız destekle).
- 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.

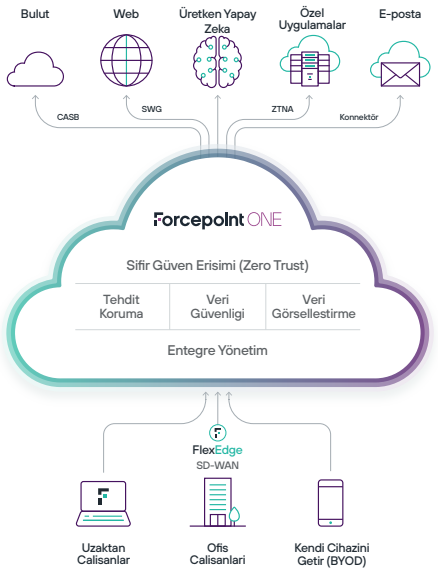
Ofise dönüş (RTO) girişimlerini ve hibrit iş güçlerini desteklemek için güvenlik ekiplerinin, verileri resmin merkezine koyan birleşik bir güvenlik platformuna ihtiyacı var. Güvenlik kontrollerinin web, bulut ve özel uygulama erişimine tutarlı görünürlük ve kontrolle yayılabilmesi gerekiyor, böylece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

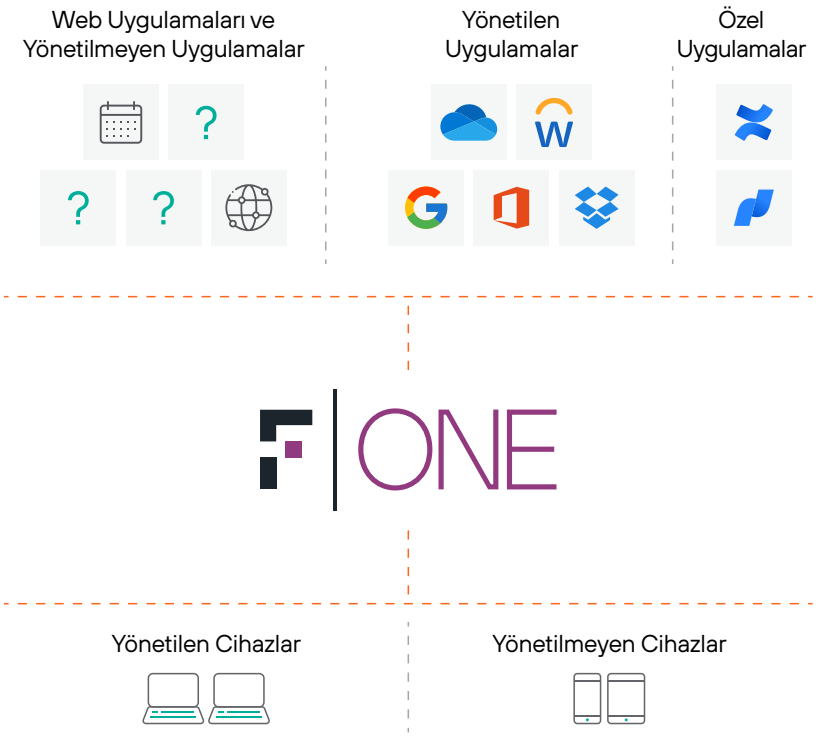
Veri öncelikli bir çözüm ile iş verileri herhangi bir yerde çalışan kullanıcılar için her yerde güvence altına alınabilir.

Forcepoint ONE Güvenliği Basitleştiriyor

Forcepoint ONE, güvenliği kolaylaştıran entegre bir bulut plantformudur. SWG, CASB ve ZTNA gibi önemli güvenlik hizmetlerini bir araya getirdiğimiz için Zero Trust ve Security Service Edge'i (SSE, SASE'nin güvenlik bileşeni) hızla kullanıma alabilirsiniz.

Çeşitli GenAI sitelerine erişimi kontrol altında tutarak ve hassas verileri korumak ve kötü amaçlı yazılımlara karşı koruma sağlamak için koruma mekanizmalarını tutarlı bir biçimde yürürlüğe koyup GenAI gibi yeni teknolojileri güvenli bir şekilde kullanarak üretkenliği serbest bırakın.





Herhangi bir yerde çalışanlar için her yerde veri güvenliği

Forcepoint ONE'ın bulut tabanlı Sıfır Güven özelliklerinden bazıları:

- **Bulut ve özel uygulamalar için aracısız DLP güvenliği.** Hassas verileri güvende tutarken özel iş web uygulamalarını kişisel cihazlardan güvenle kullanın.
- **Entegre gelişmiş tehdit koruması ve veri güvenliği.** Veri kaybını veya verilerin dışarı sızmasını önleyin ve her yerde tutarlı kontrollerle bilgisayar korsanlarının sisteminize girmelerini engelleyin.
- **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, risk ve kategorilerine göre tüm web siteleriyle olan etkileşimleri izler ve kontrol altında tutar, kötü amaçlı yazılımların indirilmesini veya hassas verilerin kişisel dosya paylaşma ve e-posta hesaplarına yüklenmesini engeller. Cihaz içi web güvenliğimiz, nerede olursa olsun yönetilen cihazlarda kabul edilebilir kullanım politikalarının 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.

Entegre görünürlük ve kontrol

- Tüm SSE kanalları genelinde **yapılandırma, izleme ve raporlama** için **entegre yönetim paketi.**
- Kullanıcının konumuna, cihaz türüne, cihaz durumuna, kullanıcı davranışına ve kullanıcı grubuna göre web, bulut veya özel uygulamalara erişimi kontrol etmek üzere **oturum açma politikaları.** Bu özellikler hesapların ele geçirilmesini önlemeye yardımcı olur.
- **Yönetilen SaaS uygulamaları,** özel uygulamalar ve web sitelerinin yanı sıra yönetilen SaaS ve IaaS'de tutulan verilere yönelik hassas verilerin ve kötü amaçlı yazılımların indirilmesini ve yüklenmesini kontrol etmek için kolayca kullanılabilen DLP politikaları.
- **Tarayıcı harici istemci uygulamaları i**çin SWG, CASB veya ZTNA'yı destekleyen, Windows ve MacOS için cihaz içi araç.
- 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.
- **AMDP:** Gizli ve kötü amaçlı içerikleri tanımlamak amacıyla dosya hareketlerini denetimli bir kötü amaçlı yazılım kontrol alanında analiz eder.

İşleri basitleştiren abonelikler

Kullanıcı başına yıllık abonelik imkanı sunulmaktadır:

- Web, bulut ve özel uygulama güvenliği için Hepsi Bir Arada sürümü.
- **Web güvenliği sürümü,** web ağ geçidi, sınırsız bulut uygulamaları için dahili CASB ve bulut uygulamalarına yönelik API desteği ile daha sonra özel uygulamalara destek sağlamak üzere kategorize edilmemiş ve yeni kaydedilmiş siteler için RBI temellerini içerir.
- **ZTNA sürümü** sınırsız sayıda özel uygulamayı korur.
- **CASB sürümü,** sınırsız sayıda bulut uygulamasını çevrimiçi olarak korur ve ek uygulama paketleri veya özel API yoklama düğümleri ekleme olanağıyla birlikte 3 uygulama için API'ler içerir.
- **Tüm üyeliklerde** merkezi bulut yönetimi, veri kaybı önleme politikaları, uç nokta aracısı üzerinden otomatik erişim ve kapsamlı raporlama özelliği bulunmaktadır.

forcepoint.com/contact