Forcepoint

Çözüm Özeti

Sıfır Güven Ağ Erişimi

VPN kullanmadan özel uygulamalar için güvenliği basitleştirin

Kullanım Durumları

- Veri merkezlerinizdeki ve özel bulutlardaki özel uygulamalara erişim için VPN'lerden kurtulmak.
- BYOD ve yönetimsiz cihazlardan özel web uygulamalarına güvenli ve aracısız erişim sağlamak.
- Tüm özel web uygulamalarına yüklenen ve uygulamalardan indirilen hassas verileri kontrol altına almak.
- Özel web uygulamalarına gönderilen ve bu uygulamalardan alınan iş veri dosyalarında gizlenen kötü amaçlı yazılımları engellemek.
- Yönetimli Windows ve macOS cihazlardan özel web dışı sunuculara güvenli erişim sağlamak.

Çözüm

- Gelişmiş tehdit koruması ve DLP ile entegre özel uygulama güvenliği.
- BYOD ve yönetimli cihazlardan özel web uygulamalarına aracısız ve Sıfır Güven erişim kontrolleri.
- Yönetimli Windows ve macOS cihazlardan özel web dışı uygulamalara uzaktan erişim.
- SWG, CASB ve diğer modern güvenlik çözümleriyle birlikte bulutta sunulan hepsi bir arada hizmetin bir parçasıdır.

Sonuç

- Verimlilik artışı, çalışanların özel uygulamalara her yerden sorunsuz ve güvenli bir şekilde erişmesinin sağlanması.
- Politikaların tek bir yerden belirlenmesiyle güvenlik operasyonlarının basitleştirilmesi ve maliyetlerin azaltılması.
- Özel web uygulamalarına gönderilen ve bu uygulamalardan alınan hassas verilerin ve kötü amaçlı yazılımların kontrol edilmesi yoluyla riskin azaltılması.
- Kanıtlanabilir bilgi kontrolü süreçleriyle yasal uyumun kolaylaştırılması.

Uzaktan çalışma, özel sanal ağların (VPN) sınırlarını, maliyetlerini ve risklerini ortaya çıkardı. VPN'ler, bir kez bağlantı kurduktan sonra aşırı bir güven vererek kullanıcıların o özel veri merkezi veya sanal özel buluttaki diğer IP adreslerini taramalarına izin veriyor ve bu da ihlallere yol açabiliyor. Ancak, VPN'lerden Sıfır Güven Ağ Erişimi (ZTNA) çözümlerine geçiş yapmak isteyen kurumlar, daha fazla karmaşıklık ve uç nokta ürünüyle uğraşmak zorunda kalmamalı; Sıfır Güven erişiminin benimsenmesi, basit ve sorunsuz olmalı.

Forcepoint ZTNA, her çalışan, tedarikçi ve ortağın kullanmak için açık izne sahip olduğu özel web ve web dışı uygulamalara erişimi kontrol altına alır. Forcepoint ZTNA, çalışanların yönetimsiz cihazlar ve BYOD cihazları dahil olmak üzere en çok işlerine yarayan cihazları kullanma güveniyle çok daha geniş bir kontrol imkanı sağlamaktadır.

Diğer çözümlerin aksine, Forcepoint ZTNA, modern ağların karmaşık yapısına rağmen mükemmel bir kullanıcı deneyimi sunmak için sürekli ve ince ayarlanmış kontroller, sektördeki en yüksek performans ve dahili kötü amaçlı yazılım ve veri koruması özelliklerini de sunmaktadır. Ayrıca, gerektiğinde tamamen Forcepoint ONE bulut platformunun entegre parçaları olarak Cloud Access Security Broker (CASB) ve Secure Web Gateway (SWG) gibi diğer güvenlik çözümlerini de ekleyebilirsiniz.

Veri merkezlerinizdeki ve özel bulutlardaki özel uygulamalara erişim için VPN'lerden kurtulmak

Özel uygulamalara güvenli erişim, hızlı ve hassas bir kontrol gerektirir. ERP veya tedarik zinciri sunucuları gibi özel uygulamalara erişimi kimlik, grup üyeliği, cihaz türü ve konuma göre sınırlayabilirsiniz. Web dışı uygulamalarda her bir bağlantı noktası için kontroller uygulayabilir ve bilinmeyen konum veya cihazlardan erişimi engelleyebilirsiniz. Oturum açma denemesi şüpheli görünüyorsa kullanıcıların çok faktörlü kimlik doğrulama (MFA) yoluyla kimliklerini kanıtlamaları gerekir. Tüm bunlar, Forcepoint'in hiper ölçekli platformuyla milisaniyeler içinde gerçekleşir.

BYOD cihazlardan özel web uygulamalarına güvenli ve aracısız erişim sağlamak

Kullanıcılar, güvenlik duvarlarıyla korunan web uygulamalarına internet üzerinden ve aracıya ihtiyaç duymadan BYOD ve yönetimsiz cihazları kullanarak güvenli ve kolay bir şekilde bağlanabilir.

Tüm özel web uygulamalarına yüklenen ve uygulamalardan indirilen hassas verileri kontrol altına almak

Bilgisayar korsanlarını ve veri ihlallerini engelleyen dahili kötü amaçlı yazılım tarama ve DLP özellikleriyle birlikte hassas verileri kontrol etmek için tek bir güvenlik politikası setini yönetin. Veri güvenliğinin cihaz durumu ve konumuna ilişkin politikalarla birleştirilmesi, insanların herhangi bir cihazdan özel web uygulamalarına nasıl veri gönderip aldıklarını kontrol etmeyi kolaylaştırmaktadır.

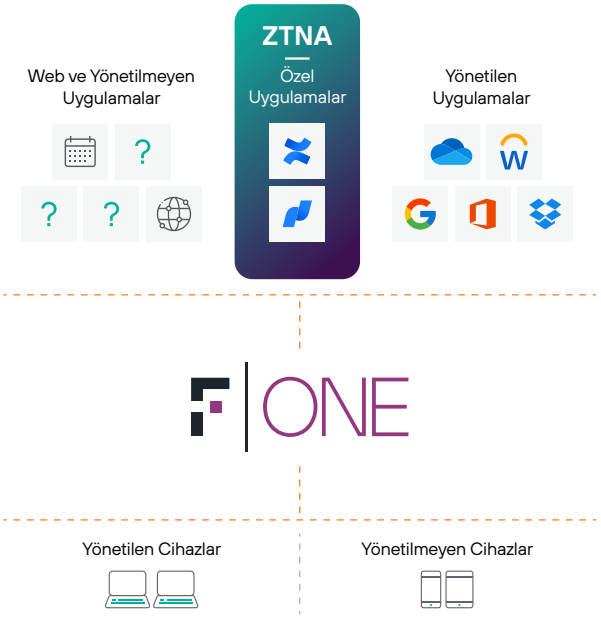
Özel web uygulamalarına gönderilen ve bu uygulamalardan alınan iş veri dosyalarında gizlenen kötü amaçlı yazılımları engellemek

Forcepoint, fidye yazılımlarını engeller. Bitdefender ve CrowdStrike tarama motorlarını kullanarak, kullanıcılarla tüm özel web uygulamaları arasında aktarılmakta olan verilerdeki kötü amaçlı yazılımları tespit edip engelleyin.

Yönetimli cihazlardan özel web dışı sunuculara güvenli erişim sağlamak
ZTNA çözümümüz, Forcepoint ONE birleşik aracısıyla güvenli kabuk (SSH) gibi özel web dışı uygulamalara erişim ve yönetimli PC veya Mac bilgisayarlardan uzak masa üstü erişimi sağlar.

Forcepoint ONE ile sunulan ZTNA çözümü çalışma süresini, kullanılabilirliği ve verimi maksimuma çıkarır
ZTNA çözümü, 300 varlık noktasına (PoP), küresel erişilebilirliğe ve özel uygulamaları ve kullanıcıların verimliliğini korumak için kanıtlanmış %99,99 çalışma süresine sahip hiper ölçek tabanlı bulut platformumuz olan Forcepoint ONE'ın bir parçasıdır. Diğer çözümler, ağ trafiğini kullanıcılara yakın konumlar yerine özel veri merkezlerine yönlendirir ki bu da düşük performansa neden olabilir. 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 Özel Uygulama Güvenliğini Basitleştirmek
Forcepoint ONE bulut platformu, özel uygulama güvenliğinin uygulanması için "kolay bir düğme" sağlar. Yöneticiler, tek bir konsoldan hem yönetimli hem de yönetimsiz cihazları (BYOD cihazlar ve yüklenicilerin veya ortakların bilgisayarları gibi) kullanan kullanıcıların yüklediği ve indirdiği dosyaları kontrol edebilir ve bu belgelere erişimi yönetebilir.



Her etkileşim için **eksiksiz bulut güvenliği** sağlayın

Evden çalışan bir satın alma yöneticisi olan Kris iş gününe başlarken, ZTNA'nın özel uygulama güvenliğini nasıl basitleştirdiğini görelim.

Kris, şirket dizüstü bilgisayarından Forcepoint ONE hesabında oturum açıyor.	Kris yönetimli bir cihazdan ve izin verilen bir konumdan oturum açmaya çalıştığı için erişime izin veriliyor. Bilinmeyen bir konumdan oturum açılmaya çalışılması durumda, MFA uygulamaları üzerinden doğru bir yanıt verilmesi gerekecektir.
Kris, Forcepoint ONE kullanıcı portalından şirketin özel tedarik zinciri uygulamasına tek tıklamayla erişim sağlıyor.	Kris'in tarayıcısı, Kris'in ve tedarik zinciri ortaklarının erişebileceği her bir web uygulamasının simgelerini gösteren Forcepoint ONE portalını görüntülüyor. (Kris'in şirketi Forcepoint ONE CASB çözümünü kullanıyorsa tutarlı bir deneyim sağlamak için Kris'in yönetimli SaaS uygulamalarına da aynı kullanıcı portalından erişilebilir.)
Kris'e yönetimli uygulamalara erişim izni veriliyor.	Kris'in bilgisayarıyla tedarik zinciri uygulaması arasındaki trafik, otomatik olarak Forcepoint ONE ters proxy sunucusundan geçiyor. Forcepoint, indirilen ve yüklenen tüm dosyalarda kötü amaçlı yazılım ve hassas veri taraması yapıyor.
Kris, bir tedarikçi sözleşmesini ek olarak yüklüyor.	Kris'in bağlantısı için geçerli olan politika, dosyaların taranması gerektiğini belirttiğinden, kötü amaçlı yazılım içermiyorsa dosyanın yüklenmesine izin veriliyor. Kötü amaçlı yazılım bulaşmış olması durumunda, ZTNA ağ geçidi yüklemeyi engelleyecek, Kris'i uyaracak ve engellenen olayı kaydedip bildirecektir.
Kris, bir tedarikçi sözleşmesini ek olarak yüklüyor.	Kris'in bağlantısı için geçerli olan politika, dosyaların taranması gerektiğini belirttiğinden, kötü amaçlı yazılım içermiyorsa dosyanın yüklenmesine izin veriliyor. Kötü amaçlı yazılım bulaşmış olması durumunda, ZTNA ağ geçidi yüklemeyi engelleyecek, Kris'i uyaracak ve engellenen olayı kaydedip bildirecektir.

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

Forcepoint ONE hepsi bir arada platform, ZTNA çözümüne ek olarak, her türlü web sitesi ve özel uygulamadaki iş bilgilerine erişimi de güvenlik 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 veya e-posta hesaplarına yüklenmesini engeller. Cihazlara kurulan SWG çözümümüz, kabul edilebilir kullanım politikalarının her yerdeki yönetimli cihazlarda uygulanmasını sağlar.
- **Bulut:** CASB, kurumsal SaaS ve IaaS uygulamalarına erişimi güvence altına almanın ve basitleştirmenin yanı sıra, cihaza kurulu herhangi bir aracıya ihtiyaç duymadan hassas verilerin ve kötü amaçlı yazılımların iletimini kontrol altına alır.
- 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/contact