Forcepoint

Çözüm Özeti

Cloud Access Security Broker

Tüm bulut uygulamalarında bulunan ve tüm cihazlardan erişilen verileri kolayca güvenlik altına alın

Zorluk

- BYOD cihazlardan yönetimli uygulamalara erişimi korumak ve kontrol altına almak
- Tüm yönetimli SaaS uygulamalarına yüklenen ve uygulamalardan indirilen hassas verileri korumak
- İş veri dosyalarında gizlenen kötü amaçlı yazılımları engellemek
- Gölge BT'yi tespit ve kontrol etmek

Çözüm

- Entegre DLP ve gelişmiş tehdit koruması ile sağlanan bulut uygulaması güvenliği
- Kullanıcı, cihaz veya konuma bağlı parçalı Sıfır Güven erişim ve veri kontrolleri
- Çok büyük ölçeklere taşınabilen AWS platformu, çalışma süresini maksimuma çıkarır ve gecikmeyi minimuma indirir
- Yönetilen ve yönetilmeyen cihazlarda DLP uygulaması

Sonuç

- Verimlilik artışı, çalışanların bilgiyi her yerde sorunsuz ve güvenli bir şekilde kullanmasının 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
- Kanıtlanabilir bilgi kontrolü süreçleriyle yasal uyumun kolaylaştırılması

Günümüzün karma iş gücü için mobil cihazlardan bulut uygulamalarına ve verilerine erişim çok normal bir durum. Ortalama bir kurum; uzaktan çalışanlar ve yükleniciler için vazgeçilmez olan Microsoft 365, Google Workplace, Slack veya Jira gibi iş birliği araçları dahil olmak üzere 280'den fazla SaaS uygulaması kullanmakta. Bu hizmetlerin, mobil cihazlardan erişimin yönetilmesini veya cihazlara güven duyulmasını sağlayacak bir yöntem olmadan kullanılması, sürece karmaşıklık ve risk eklemektedir.

BYOD ve yönetimsiz cihazlardan iş uygulamalarına erişimi güvenlik altına alın

Forcepoint, bulut güvenliğini basitleştiriyor. Forcepoint ONE'ın CASB güvenlik hizmeti, iş açısından kritik bulut uygulamalarının çalışanların kişisel cihazlarından (BYOD) ve iş ortakları ve yüklenicilerin yönetimsiz cihazlarından güvenle kullanılmasını sağlayan Sıfır Güven erişim yöntemini kullanmaktadır.

Tüm yönetimli SaaS uygulamalarına yüklenen ve uygulamalardan indirilen hassas verileri korumak

Size, hassas verilerinizi kontrol etmeniz için tek bir güvenlik politikaları setinin yanı sıra, çalışanlarınız ve yüklenicileriniz internete nereden ve nasıl bağlanırsa bağlansın endüstri lideri bir performans sunan bir çözüm sunuyoruz. Mobil cihazlardan bu uygulamalara erişimin yönetilmesi, benimseme ve verimliliği artırırken, cihaz durumuna ve konumuna göre farklı politikaların uygulanması da verilerin güvende kalmasını sağlayan parçalı Sıfır Güven kontrol yaklaşımını sağlar. Gizli bilgilerin, kişisel cihazlar dahil olmak üzere tüm cihazlarda bulunan şirket uygulamalarında nasıl paylaşıldığını kesin bir şekilde görürsünüz. Data loss prevention (DLP) çözümü dahili olarak sunulmaktadır, dolayısıyla veri ihlallerini durdurmak için uç nokta ürünlerine ihtiyaç duymazsınız.

İş veri dosyalarında gizlenen kötü amaçlı yazılımları engellemek

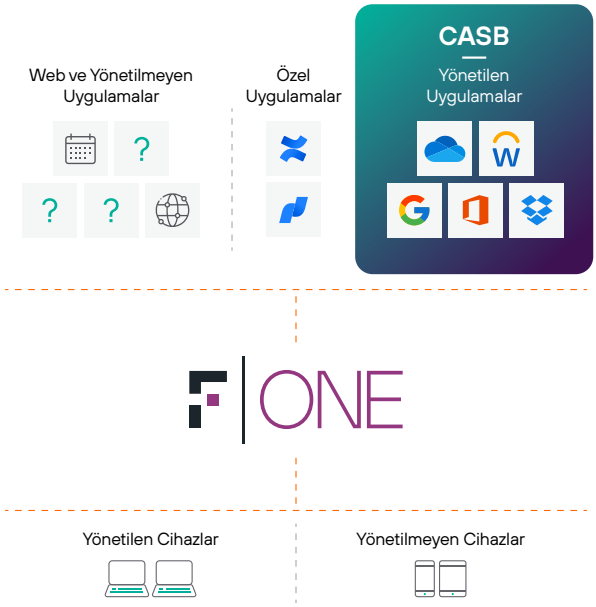
CASB çözümümüz, Bitdefender ve CrowdStrike kötü amaçlı yazılım motorlarını kullanarak, kullanıcılarla SaaS uygulaması arasında aktarılmakta olan verilerdeki kötü amaçlı yazılımları tespit edip engelleyebilir. Ayrıca, popüler SaaS ve IaaS depolama çözümlerindeki dosyalarda bulunan kötü amaçlı yazılımları da tespit edip bu dosyaları karantinaya alabilir.

Gölge BT'yi tespit ve kontrol etmek

CASB, gölge BT'yi açığa çıkarmakla kalmaz, aynı zamanda kontrol ve güvenli kullanım ve daha iyi alternatifler konusunda eğitim imkanı da sağlar. CASB, kullanılmakta olan yönetimsiz SaaS uygulamalarını tespit edip listeleyerek, yöneticilerin şirket cihazları için erişimi engelleyen veya kullanıcıları onaylı SaaS uygulamalarına yönlendiren bir mesaj görüntüleyen politikalar oluşturmasına imkan tanır.

Forcepoint ONE ile sunulan CASB çözümü; çalışma süresini, kullanılabilirliği ve verimi maksimuma çıkarır

CASB uygulamamız, 300 varlık noktasına (PoP), küresel erişilebilirliğe ve bulut uygulamalarını ve kullanıcıların verimliliğini korumak için kanıtlanmış %99,99 çalışma süresine sahip hiper ölçek tabanlı bulut platformumuz olan Forcepoint ONE'ın bir parçasıdır. Diğer çözümler, bulut uygulamalarından gelen ve bu uygulamalara giden trafiği, kullanıcılara yakın konumlar yerine özel veri merkezlerine yönlendirir. Bu da performansın düşmesine, Slack gibi gecikmeye duyarlı uygulamaların başarısız olmasına ve çalışanların yüksek riskli geçici çözümler aramasına neden olur.



Her etkileşim için **eksiksiz bulut güvenliği** sağlayın

Gerçek Dünyada Bulut Güvenliğini Basitleştirmek

Forcepoint ONE bulut platformu, bulut 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.

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

Kris, şirket dizüstü bilgisayarından Salesforce hesabında oturum açıyor.	Forcepoint ONE platformundaki CASB çözümü, iş uygulamalarına olan bağlantıları yöneterek kullanıcıların sorunsuz ve güvenli bir şekilde oturum açmasını sağlıyor.
Kris doğrudan salesforce.com adresine gidiyor veya siteye bir kurumsal uygulama portalı üzerinden ulaşıyor.	Salesforce, oturumu CASB'ye yönlendiriyor (SAML yoluyla) ve CASB de cihazın yönetimli olup olmadığını, konumunu ve güvenlik durumunu analiz ediyor. CASB, önceden tanımlı güvenlik politikalarına dayanarak çok faktörlü kimlik doğrulama uygulamalarıyla Kris'in kimliğini onaylıyor.
Kris'e yönetimli uygulamalara erişim izni veriliyor.	Ayrıca uygulamaya doğrudan veya kontrollü erişim sağlanması veya hiç erişim izni verilmemesi de yönetici politikaları ile belirleniyor. Bu işlemler, çalışanların verimini etkilemeden milisaniyeler içinde gerçekleşiyor. Kris'in cihazından ve uygulamadan gelen tüm trafik, CASB'den geçiyor (ters proxy sunucu kullanılarak).
Kris, Salesforce'tan bir gelir tahminini indirmeye karar veriyor.	CASB, uygulamadan indirilen tüm dosyalarda kötü amaçlı yazılım ve hassas veri taraması yapıyor. Sonuçlara ve geçerli politikaya bağlı olarak, kötü amaçlı dosyaları engelleyebiliyor ve hassas verileri engelleme, takip veya şifreleme işlemine tabi tutabiliyor. Bir politika hassas verilerin yönetimli cihazlara indirilmesine izin veriyorsa, Kris bir şirket bilgisayarı kullandığından bu indirme işlemine de izin verilir.
Kris, Slack yoluyla hassas verileri veya kötü amaçlı yazılım bulaşmış bir dosyayı aktarmaya veya verileri kişisel Dropbox hesabına yüklemeye çalışıyor.	CASB, bulut uygulamalarına yüklenen dosyaları da kontrol edebilir. CASB, yükleme işlemini otomatik olarak engelleyebilir. Ayrıca, cihaz üzerindeki birleşik aracıyı kullanarak dosyaların onaylı olmayan uygulamalara yüklenmesini dahi engelleyebilir.

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

Forcepoint ONE hepsi bir arada platform, CASB 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.
- → **Özel uygulamalar:** ZTNA, VPN'lerin getirdiği karmaşıklık veya riskler olmadan özel uygulamalara güvenli ve basit erişim sağlar.
- → 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.