Forcepoint

Çözüm Özeti

Cloud Access Security Broker

Tüm bulut uygulamalarında bulunan ve tüm cihazlardan erişilen verileri 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 yeni iş gücü modelleri, kullanıcıların konumlarından bağımsız olarak iş verilerine her yerden hızlı ancak kontrollü erişim sağlamasını gerektiriyor. Bu da insanların Microsoft 365, Google Workspace, Slack, Jira ve Salesforce gibi bulut uygulamalarındaki verilere her tür cihazdan veya konumdan erişebilmesi gerektiği anlamına gelir. Ortalama bir kuruma yönelik 250'den fazla SaaS uygulaması ile görünürlük ve kontrol kolaylıkla yönetilemez hale gelebilir.

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 performans sunan bir çözüm sunuyoruz. Bu uygulamalara mobil cihazlardan erişimi yönetmek, benimsenme ve üretkenliği kolaylaştırırken, kimlik ve konum bazında farklı politikalara sahip olmak da ayrıntılı Zero Trust kontrolleri sağlayabiliyor. Hassas veriler ve kötü amaçlı yazılımlar için satır içi tarama, tüm SaaS uygulamalarında verileri güvende tutar. Şirket uygulamalarında gizli verilerin paylaşılma şekli üzerinde daha fazla emniyet elde edersiniz ve yerleşik veri kaybı önleme (DLP) sayesinde veri ihlallerini durdurmak için tekil ürünlere ihtiyacınız kalmaz.

İş veri dosyalarında gizlenen kötü amaçlı yazılımları engellemek

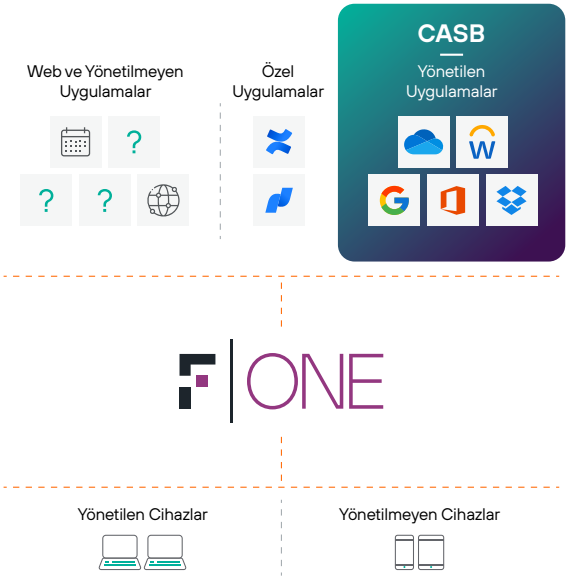
Forcepoint ONE CASB, Bitdefender ve CrowdStrike kötü amaçlı yazılım motorlarını kullanarak, kullanıcılarla SaaS uygulaması arasında aktarılmakta olan verilerdeki kötü amaçlı yazılımları tespit edip engelleyebilir. Ayrıca, popüler SaaS ve IaaS depolama çözümlerindeki dosyalarda bulunan kötü amaçlı yazılımları 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, ağ günlüklerini kullanarak veya Forcepoint ONE Secure Web Gateway telemetrisiyle kullanımdaki yönetilmeyen SaaS uygulamalarını tespit ederek, onaylı ve onaylanmamış SaaS uygulamalarına tutarlı güvenlik politilarının uygulanmasını sağlayarak iş verilerini kullanıldığı her yerde güvende tutar.

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

CASB uygulamamız, 300'den fazla varlık noktasına (PoP'ler), 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 uygulamalarına gelen ve bulut uygulamalarından çıkan ağ trafiğini, kullanıcılara ve onların eriştiği uygulamalara daha yakın konumlara değil, özel veri merkezlerine yönlendirir. Bu da performansın düşmesine, Slack gibi gecikmeye duyarlı uygulamaların başarısız olmasına ve çalışanların yüksek riskli geçici çözümler aramasına neden olur.



Herhangi bir yerde çalışanlar için her yerde veri güvenliği

Gerçek Dünyada Bulut Güvenliğini Basitleştirmek

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

Yöneticiler, tek konsoldan hem yönetilen hem de yönetilmeyen cihazların (BYOD ve yüklenicilerin veya iş ortaklarının bilgisayarları gibi) kullanıcıları için erişimi yönetebilir ve verileri kontrol edebilir.

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 veya ileri 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 yönetilmeyen cihazlara indirilmesini kısıtlıyorsa Kris bir şirket bilgisayarı kullandığından bu indirme işlemine de izin verilir.
Kris, hassas verileri veya kötü amaçlı yazılım içeren bir dosyayı Slack aracılığıyla aktarmaya 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.
- **Ek özellikler:** Gerektiğinde bulut sağlayıcılarını riskli yapılandırmalar için tarama, Cloud Security Posture Management (CSPM) ve SaaS Security Posture Management (SSPM) vb.

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