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 edin ve kontrol altında tutun

Çözüm

- Entegre DLP ve gelişmiş tehdit koruması ile sağlanan Saas 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 kullanıcıların Microsoft 365, Google Workspace, Slack, Jira ve Salesforce gibi SaaS uygulamalarındaki verilere her türlü cihaz veya konumdan erişmesi gerektiği anlamına geliyor. Ortalama bir kurumda 250'den fazla SaaS uygulamasının olduğu düşünüldüğünde, görünürlük ve kontrol yönetimi son derece zorlaşabilir.

BYOD ve yönetimsiz cihazlardan iş uygulamalarına erişimi güvenlik altına alın

Forcepoint, bulut güvenliğini basitleştiriyor. Forcepoint ONE'ın CASB güvenlik hizmeti, iş açısından kritik SaaS uygulamalarının çalışanların kişisel cihazlarından (BYOD) ve iş ortakları ve yüklenicilerin yönetimsiz cihazlarından güvenle kullanılmasını sağlayan Zero Trust 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

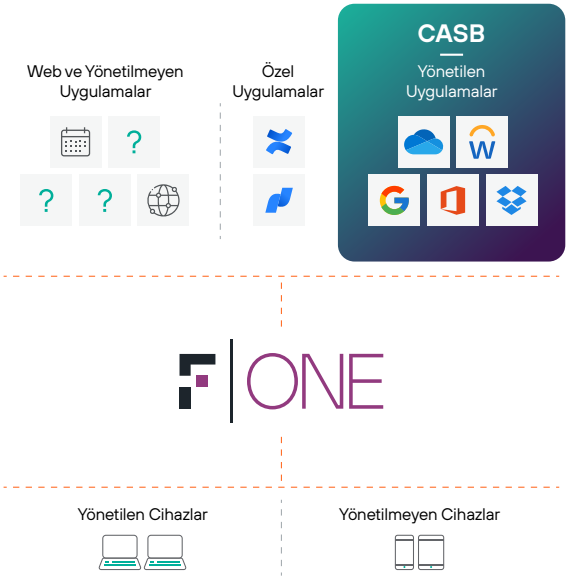
Forcepoint ONE CASB, birden fazla kötü amaçlı yazılım önleme motorunu kullanarak, kullanıcılarla SaaS uygulaması arasında aktarılmakta olan verilerdeki kötü amaçlı yazılımları tespit edip engelleyebilir. Ayrıca, popüler SaaS ve IaaS depolama çözümlerindeki dosyalarda bulunan kötü amaçlı yazılımları da tespit edip bu dosyaları karantinaya alabilir.

Gölge BT'yi tespit edin ve kontrol altında tutun

Forcepoint ONE CASB, gölge BT'yi açığa çıkarır ve birden fazla özniteliği analiz ederek onaylanmamış uygulamalar için bir risk skoru oluşturur. Bu sayede BT ekipleri, kuruluşlarındaki SaaS kullanımı hakkında daha derin bir anlayışa sahip olabilir ve gerekli güvenlik kontrollerini uygulamaya koyabilir. CASB, kurumsal güvenlik duvarlarından ve proxylerden gelen ağ günlüklerini kullanarak kullanımdaki yönetilmeyen SaaS uygulamalarını tespit eder ve böylece iş verilerinin kullanıldıkları her yerde güvende kalması için onaylı olan ve olmayan SaaS uygulamalarına tutarlı güvenlik politikalarının uygulanmasını sağlar.

Çalışma süresi, kullanılabilirlik ve verimliliği en üst düzeye çıkaran SaaS güvenliği çözümü

CASB'miz, SaaS uygulamalarını sorunsuz bir şekilde güvence altına almak ve kullanıcı üretkenliğini korumak üzere, 300'den fazla varlık noktası (PoP), küresel erişilebilirlik ve kanıtlanmış %99,99 kesintisiz çalışma süresi ile bulut tabanlı, hiper ölçeklendirici tabanlı bir mimari üzerine inşa edilmiştir. Diğer çözümler, bulut uygulamalarına gelen ve SaaS 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

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 ayrıca SaaS uygulamalarına yüklenmekte olan dosyaları da kontrol edebilir. CASB yüklemeyi otomatik olarak engelleyebilir. Ayrıca, cihaz üzerindeki birleşik aracıyı kullanarak dosyaların onaylı olmayan uygulamalara yüklenmesini dahi engelleyebilir.

Forcepoint'in Her Yerde Veri Güvenliği yaklaşımının bir parçası

Forcepoint'in Her Yerde Veri Güvenliği misyonu, kuruluşların SaaS, web, e-posta, ağ ve uç noktalar genelinde verileri korumasını sağlar; böylece kullanıcılar her yerde verilerle güvenle çalışabilir.

Endüstri lideri DLP özelliklerini SaaS uygulamalarına taşıma

Forcepoint ile kuruluşlar, SaaS uygulamalarındaki verileri güvence altına almak için mevcut Forcepoint DLP politikalarını kullanabilir ve aynı sektör lideri veri güvenliğini sadece birkaç tıklamayla buluta da yayabilir. Tek bir konsoldan uygulanan birleşik DLP politikaları, SaaS uygulamalarına tutarlı, kurumsal sınıfta veri güvenliği sunmaya yardımcı olur, veri güvenliği yönetimini basitleştirir, ihlalleri en aza indirir ve uyumluluğu kolaylaştırır. Müşteriler bu entegrasyon yoluyla aşağıdaki avantajları elde edebilir:

- → Birleştirilmiş politikalar ve konsolla basitleştirilmiş bulut veri güvenliği.
- → 150'den fazla bölge için kapsamlı ve uyumluluk desteği için kullanıma hazır 1.700 sınıflandırıcı ve politika şablonu.
- → BT/güvenlik ekiplerinin verimliliğini artıran yapılandırma kurulumu ve dakikalar içinde değer kazanma.
- → Önemli ölçüde maliyet tasarrufu elde etmek için gereksiz ve parçalı güvenlik ürünlerini ortadan kaldırmak.

Daha fazla ayrıntı için Forcepoint DLP broşürünü okuyun.

Bulut uygulamalarında bulunan ve tüm cihazlardan erişilen verileri güvenlik altına almaya hazır mısınız?

Bir demo ile başlayalım.

forcepoint.com/contact