FORCEPOINT
POWERED BY Raytheon

Bilgi Formu

Forcepoint CASB

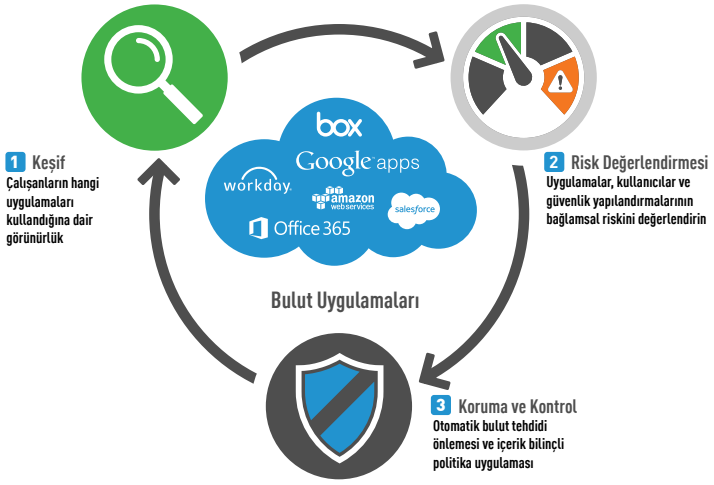
Forcepoint Bulut Erişimi Güvenlik Aracısı (CASB), bulut uygulama kullanımını otomatik olarak keşfeder, riskleri analiz eder, SaaS ve üretim uygulamaları için gerekli kontrolleri uygular. Forcepoint CASB ile kullanıcılar istedikleri uygulamaları alır ve BT personeli ihtiyaçları olan kontrole sahip olur.

BULUT UYGULAMALARIN KULLANIMI ÜZERİNDE GÖRÜNÜRLÜK VE KONTROL SAĞLAMA

Bulut uygulamaları kurumların maliyetleri azaltmasına ve kaynakları esnek biçimde tahsis etmesine imkan verir, fakat aynı zamanda güvenlik ve uyum açısından riskler oluşturur. İş yerinde bulut uygulamaların giderek daha çok benimsenmesi ve BYOD uygulamasının yaygınlaşması, Office 365, Dropbox ve Salesforce gibi bulut tabanlı, onaylanmış uygulamaların güvenliğini sağlama ihtiyacını doğurmuştur. BT için veri kaybını önlemek ve granüler erişim kontrolleri uygulamak en başta gelen sorumluluktur.

Şirket içindeki kötü niyetli kişiler veri sızdırmak amacıyla kurumun bulut uygulamalarına serbest erişim imkanından yararlandığı için çalışanlar büyük bir güvenlik riski kaynağı olabilir.

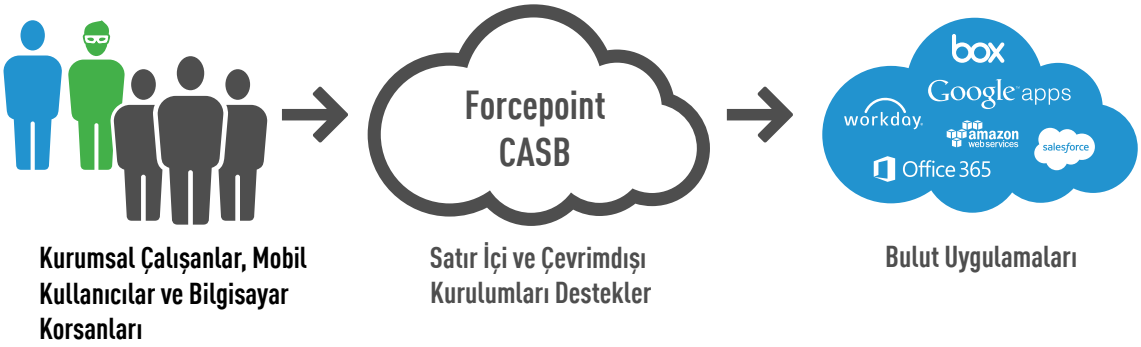
Forcepoint, tüm kullanıcılar ve uç noktalar genelinde bulut uygulamalarının güvenli ve verimli kullanımını sağlar.



Görünürlüğü ve kontrolü sağlamak amacıyla, hem onaylanmış hem de onaylanmamış uygulamalar için uygulama keşfi, risk yönetişimi, erişim kontrolü ve veri korumayı destekleyen bir bulut erişimi güvenlik aracısı gereklidir.

BULUT UYGULAMA RİSKİNİ HAFİFLETME

Kurumlar riski ortadan kaldıran veya sınırlandıran politikaları uygulamadan önce genellikle bulut erişimi görünürlüğüne ihtiyaç duymaktadır. Bu nedenle, risk durumunuzu belirlemede ve değerlendirmede yardımcı olacak çevrimdışı özelliklere sahip olmak önemlidir. Tehdit ortamını inceledikten ve güvenlik risklerini ele alacak gerekli politikaları oluşturduktan sonra, bu çevrimdışı özellikleri, oluşturulan politikaların fiili olarak uygulanmasını sağlayacak satır içi çözümlere dönüştürebilirsiniz. Gartner, günümüz kuruluşlarında tüm bulut güvenliği kullanım durumlarını kapsamak için "bir taşla iki kuş vuran" çözümleri (vekil sunucular ve API'lerin kombinasyonu) tavsiye etmektedir.



Forcepoint Bulut Erişimi Güvenlik Aracısı hem onaylanmış hem de onaylanmamış bulut uygulamaları için görünürlük ve kontrol sağlar.

ÖZELLİKLER VE AVANTAJLAR

- Forcepoint Bulut Güvenliği ürün ailesinin şirket içi ve bulut ortamlarını kapsayan bölümü
- Kapsamlı Uygulama Keşfi, Yönetişim, Analizler ve Koruma tek bir entegre çözümde
- Çevrimdışı (API modu) ve/veya satır içi (vekil sunucu modu) kullanım seçenekleri
- Mobil ve uç noktası cihazlarına yönelik granüler politikalar, yönetilen ve yönetilmeyen cep telefonları, tabletler ve dizüstü bilgisayarlar için erişim kontrolü ve veri koruması sağlar
- İşletme dizinleri, SIEM ve MDM ile dahili entegrasyon
- Office 365, AWS, Salesforce, Box, Dropbox, NetSuite, Workday, vb. için detaylı destek
- Hizmet Olarak Kimlik iş ortakları ile onaylanmış birlikte çalışabilirlik: Centrify, Ping, Okta, OneLogin, SecureAuth ve Microsoft
- Bir kurumun anormal davranış ve tehdit tespiti kabiliyetlerini bulut uygulamalarına genişletir
- Fikri Mülkiyet itibar verileri, daha doğru risk hafifletme politikalarının oluşturulması ve uygulanmasını sağlar

BULUT KEŞFİ VE YÖNETİŞİMİ

Forcepoint CASB, kurumunuza özgü ve benzersiz olan risk faktörleri ile ilgili detayları vererek geleneksel bulut uygulama keşfi bilgilerini genişletmektedir. Örneğin, Forcepoint CASB çeşitli güvenlik riskleri oluşturan eylemsiz (pasif) hesaplar, sahipsiz hesaplar (örn. eski çalışanların) ve harici hesaplar (örn. yükleniciler) ile ilgili görünürlük sağlar.

Buna ek olarak, Forcepoint kurumunuzun bulut uygulama güvenliği yapılandırmaları ile sektörün en iyi uygulamaları ve mevzuat şartlarını karşılaştırır. Böylece güvenlik ve uyumla ilgili açıklarınızı daha kolay belirleyebilir ve bunu düzeltmek için önlem alabilirsiniz.

Bulut Keşfi ve Yönetişimi özelliklerinin tümü, bir bulut uygulaması tedarikçi API'si üzerinden aktif hale getirilir. Bu çevrimdışı süreç kesintisizdir ve hiçbir aracı ve uygulama değişikliği gerektirmez ya da logların kurumunuz dışına Forcepoint'e gönderilmesi gerekmez.

BULUT DENETİMİ VE KORUMASI

Forcepoint CASB Bulut Denetimi ve Koruması, Bulut ortamındaki verileri korumak için ihtiyacınız olan operasyonel istihbarat ve araçları sağlar, kullanıcı erişimi ile ilgili kapsamlı kontroller uygular. Forcepoint şu konularda kritik içgörü ve istihbarat sağlar:

- **Durağan Veriler ve Hareket Halindeki Veriler için Veri Kaybı Koruması:** Bulut ortamındaki hassas ve düzenlenmiş veriler için kontroller
- **Kullanıcı İzlemesi :** Son kullanıcılar ve yöneticilerin gerçek zamanlı faaliyet takibi ve raporlaması
- **Siber Tehdit Koruması:** Şüpheli faaliyetler için uyarı, engelleme veya kimlik doğrulamasına ilişkin politika uygulamaları

Forcepoint CASB varış noktası, kullanıcı veya bulut uygulaması gibi çeşitli kriterlere göre hassas verilerin yüklenmesi, indirilmesi ve paylaşılmasını takip ve kontrol eder. Ayrıca, OneDrive ve Box gibi dosya eşitleme hizmetlerinde depolanan kurumsal verileri tarayarak hassas veya düzenlenmiş dosyaları belirler, böylece riski hafifletmek için ilgili politikayı (örn. uyarı gönderme) uygulayabilirsiniz.

Forcepoint CASB, dosyaları ve içerikleri gerçek zamanlı olarak denetleyerek PII, PCI, HIPAA ve diğer hassas bilgilerin korunmasını sağlar. Yöneticiler dosyaları karantinaya alma, hassas dosyaları bulut veri havuzundan çıkarma ve son kullanıcıları bilgilendirme arasında seçim yapabilir. Dosyanın bir kopyası daha sonra incelenmek üzere güvenilen bir klasöre eklenebilir. Forcepoint CASB, dahili veri kaybı koruması (DLP) veya önde gelen DLP çözümleri ile standart ICAP tabanlı entegrasyon sunar, böylece mevcut veri koruma politikalarını kullanabilirsiniz.

Forcepoint CASB, bulut uygulamalarına yönelik tehditleri otomatik olarak tespit ederek engeller ve risk hafifletme politikaları uygular. Forcepoint CASB, benzersiz parmak izi teknikleri yoluyla her kullanıcı, bölüm ve cihaz için normal kullanım kalıplarına dayanarak detaylı davranış profillerini hızlı bir şekilde hazırlar. Parmak izi testinden geçemeyen erişimler derhal uyarı verecek, engellenecek veya gerçek zamanlı olarak iki faktörlü kimlik doğrulaması gerektirecek şekilde yapılandırılabilir. Ayrıca hızlı bir şekilde özel politikalar oluşturabilir ve bunları seçilen bulut uygulamalarına yansıtabilirsiniz.

Forcepoint CASB, yönetilmeyen uç noktalardan (örn. BYOD veya kişisel cihazlar) bulut uygulaması erişimlerini engellemeniz veya kısıtlamanıza imkan verir, böylece tüm uzaktan erişimleri VPN üzerinden yönlendirebileceğiniz uygun maliyetli bir alternatif sunar. Buna ek olarak, Forcepoint CASB işletme dizinleri ve pazar lideri SIEM çözümleri ile entegrasyonu kolaylaştıran dahili bağdaştırıcılara sahiptir.

FORCEPOINT CASB—ÜRÜN ÖZELLİĞİ KARŞILAŞTIRMASI

		FORCEPOINT ÜRÜNLERİ		
ÖZELLİK GRUP	**ÖZELLİK AÇIKLAMASI**	**BULUT YÖNETİŞİMİ**	**BULUT DENETİM VE KORUMA**	**BULUT GÜVENLİK PAKETİ**
Uygulama Görünürlüğü ve Risk Değerlendirmesi (çevrimdışı/API kullanımlarında)	BULUT UYGULAMA KEŞFİ—Kullanılan bulut uygulamalarının otomatik keşfi ve kategorizasyonu için mevcut günlük dosyalarını kullanın	●		●
	BULUT UYGULAMA RİSK PUANLAMASI—Her bulut uygulamasının toplam riskini mevzuat ve sektör sertifikasyonları ve en iyi uygulamalarına göre puanlayın	●		●
	BULUT UYGULAMA KULLANIM ÖZETİ—Her bulut uygulaması için kullanıcı sayısı, faaliyetler, trafik hacmi ve yoğun kullanım saatlerini içerir	●		●
	GELİŞMİŞ RİSK METRİKLERİ—Her uygulama için detaylı bulut uygulaması risk durumu metrikleri ve bilgileri	●		●
	ÖZELLEŞTİRİLEBİLİR RİSK METRİKLERİ—Özelleştirilebilir ağırlıkları bulunan detaylı bulut uygulaması risk durumu metrikleri	●		●
	SÜREKLİ KEŞİF—Günlük dosyalarının otomatik taranması ve keşif raporlarının oluşturulması için periyodik zaman dilimini programlayın	●		●
	MERKEZİ KEŞİF PANOSU—Toplu keşif sonuçları, önceki faaliyete kıyasla mevcut kullanım ve kullanım eğilimleri	●		●
	SIEM ENTEGRASYONU—Mevcut SIEM ortamları ile entegrasyon için keşif verilerini Yaygın Olay Formatında oluşturun	●		●
	UYGULAMA KATALOĞU VE RİSK GÜNCELLEMELERİ—Bulut uygulama kataloğunda otomatik güncellemeler ve risk özelliklerinde değişiklikler	●		●
	LOG TOPLAMA —Bulut uygulama API'leri vasıtasıyla kullanıcılar ve ayrıcalıklı kullanıcılar için temel faaliyet günlüklerini toplayın	●		●
Hesap ve Veriler Yönetişim (çevrimdışı/API kullanımlarında)	VERİ SINIFLANDIRMASI—PCI, SOX ve HIPAA gibi düzenlemelerle uyumu sağlamak için dosya eşitleme hizmetlerinde depolanan hassas veya düzenlenmiş verileri (her bir dosya için paylaşım izinleri dahil) kataloglayın ve belirleyin.	●		●
	KULLANICI YÖNETİŞİMİ—İşletme maliyetlerini azaltmak ve ilişkili güvenlik tehditlerini en aza indirmek için eylemsiz (pasif) hesaplar, sahipsiz hesaplar (örn. eski çalışanlar) ve harici kullanıcıları (örn. Yükleniciler) belirleyin	●		●
	UYGULAMA YÖNETİŞİMİ—Güvenlik ve uyum açıklarını belirlemek için bulut uygulaması güvenlik yapılandırmalarınızı sektördeki en iyi uygulamalar ve mevzuat şartları (örn. PCI DSS, NIST, HIPAA, CJIS, MAS, ISO) ile kıyaslayarak değerlendirin	●		●
	ENTEGRE ONARIM İŞ AKIŞI—Forcepoint CASB yoluyla veya 3. taraf biletleme sistemleri ile entegrasyon vasıtasıyla risk hafifletme görevlerini atamak ve tamamlamak için bir dahili kurumsal iş akışı kullanın	●		●
Gerçek Zamanlı Faaliyet Takibi ve Analizleri (satır içi/ vekil sunucu kullanımlarında)	FAALİYET TAKİBİ VE ANALİZLERİ —Kullanıcı, grup, konum, cihaz, uygulama işlemi, vb. unsurlara göre gerçek zamanlı faaliyet takibi ve analizleri		●	●
	AYRICALIKLI KULLANICI TAKİBİ—Ayrıcalıklı kullanıcılar ve yöneticilerin gerçek zamanlı faaliyet takibi ve raporlaması		●	●
	İŞLETME SIEM ENTEGRASYONU—Faaliyet günlüklerini doğrudan ArcSight, Splunk ve Q1 Labs gibi önde gelen SIEM çözümlerine besleyen bağdaştırıcılar		●	●
	İŞLETME DİZİNİ ENTEGRASYONU—Mevcut AD veya LDAP dizini altyapısını kullanıcı, grup ve kurum raporlaması ve politikası amacıyla kullanın		●	●
	GÖREVE DAYALI YÖNETİM—Varlıklar, politikalar ve sistem ayarlarının düzenlenmesi için yönetici izinlerini tanımlayın		●	●
	İŞLETME RAPORLAMASI—Özelleştirilmiş raporları düzenleme ve kaydetme özelliği bulunan, önceden tanımlanmış raporları da içeren esnek raporlama seçenekleri		●	●

		FORCEPOINT ÜRÜNLERİ		
ÖZELLİK GRUP	**ÖZELLİK AÇIKLAMASI**	**BULUT YÖNETİŞİMİ**	**BULUT DENETİM VE KORUMA**	**BULUT GÜVENLİK PAKETİ**
Hesap ve Veriler Yönetişim (çevrimdışı/API kullanımlarında)	OTOMATİK ANORMAL FAALİYET TESPİTİ—Davranışları sürekli takip edin ve yüksek riskli iç ve dış saldırılar dahil anormal faaliyetleri tespit edin		●	●
	GERÇEK ZAMANLI TEHDİT KORUMASI—Anormal faaliyetler ile IP adresleri arasında korelasyon kurun.[1] Herhangi bir uygulama veya uygulama içindeki özel bir eylemi uyarmak, engellemek, karantinaya almak veya bunun için kimlik doğrulaması istemek üzere politika uygulayın		●	●
	VERİ SIZDIRMAYI ÖNLEME—100'den fazla dosya türü ve yüzlerce önceden tanımlanmış veri türü için çeşitli düzenlemelerin (örn. PCI, PII, PHI, HIPAA, SOX) şartlarını yerine getiren durağan veri sınıflandırması ve gerçek zamanlı içerik denetimi		●	●
	ÇOK FAKTÖRLÜ KİMLİK DOĞRULAMASI—Anormal veya yüksek riskli faaliyetler tespit edildiğinde riske dayalı kimlik doğrulaması (örn. Kullanıcının mobil cihazına tek seferlik şifre gönderilir)		●	●
	ÇOKLU OTURUM AÇMA—SAML tabanlı uygulamalara erişim için dahili SSO veya 3. taraf çözümü kullanın		●	●
	DİNAMİK UYARILAR—Politika ihlalleri veya faaliyet eşikleri için SMS/e-posta yoluyla gerçek zamanlı bildirimler alın		●	●
	MOBİL VE UÇ NOKTA ERİŞİM KONTROLÜ—Yönetilen ve yönetilmeyen cihazlar için tarayıcılardan veya zengin mobil uygulamalardan kaynaklanan benzersiz politikaları etkinleştirin		●	●
	KONUM TABANLI ERİŞİM KONTROLLERİ—Kullanıcının konumu veya bulut hizmetinin konumuna bağlı olarak erişimi kısıtlayın		●	●
	MDM ENTEGRASYONU—Uç noktakaydı ve bulut erişimini yönetmek için mevcut MDM kurulumundan yararlanın		●	●
	ÖZEL POLİTİKALAR—Görsel politika düzenleyici, özel politikaların çeşitli niteliklere bağlı olarak kolay yapılandırmasını mümkün kılar		●	●
Gelişmiş Bulut Mimarisi	PERFORMANS OPTİMİZASYONU—Dünya genelinde 30'dan fazla veri merkezi bulunan birinci sınıf bir içerik dağıtım ağının, ön belleğe alma ve içerik optimizasyonu özellikleri yoluyla bulut uygulamalarına erişimi hızlandırın		●	●
	MERKEZİ TEHDİT İSTİHBARATI—İşletme veri tabanı tabloları, dosya paylaşımlarında depolanan dosyalar ve bulut uygulamalarında depolanan verilerle ilgili anormal durumlar ve tehditlerin birleşik görünümü		●	●

[1] Temel Forcepoint CASB lisansına ek olarak ayrıca satın alınan opsiyonel ürün.

İLETİŞİM

www.forcepoint.com/contact

FORCEPOINT HAKKINDA

[DATASHEET_FORCEPOINT_CASB_TUR 100055 06JUL18]