FORCEPOINT Data Loss Prevention (DLP)

SINIRLARI OLMAYAN DÜNYADA VERİ KORUMASI

FORCEPOINT

Forcepoint DLP

İNSAN MERKEZLİ SİBER GÜVENLİK YAKLAŞIMI

Veri güvenliği hiç bitmeyen bir sorundur. BT teşkilatları bir yandan mevzuat düzenlemelerine uymak ve fikri mülkiyeti hedeflenmiş saldırılar ve yanlışlıkla ortaya çıkan risklerden korunmak zorundadır. Diğer yandan ise, verilerin kurumunuzun dışına çıkma riskini artıran bulut uygulamalarının, hibrit bulut ortamlarının ve BYOD eğilimlerinin benimsenmesi gibi makro BT hareketlerine ayak uydurmak durumundadır.

Bu genişleyen saldırı ortamı, kritik verilerin korunması açısından en ciddi zorluğu doğurmaktadır. Veri güvenliği ekipleri, veri takibi için en mantıklı görünen yaklaşımı benimsemiştir: Bul, listele ve kontrol et. Ancak, veri kaybını önlemeye yönelik bu geleneksel yaklaşım artık geçerli değildir. Çünkü bu yaklaşım, veri güvenliği açısından en büyük değişken olan çalışanlarınızı göz ardı etmektedir.

Güvenlik sadece verilere odaklanmak yerine, insanlarla başlamalı ve insanlarla bitmelidir. Esas olan, kullanıcının veriler ve uygulamalarla olan etkileşimlerinin görünürlüğünü sağlamaktır. Bu başarıldıktan sonra, kullanıcıya özgü risk ve verilerin hassasiyeti veya değerine bağlı olarak gerekli kontrol seviyesini uygulayabilirsiniz.

Bir kurumun veri koruma programı insan noktasını, yani kullanıcılar, veriler ve ağların etkileşimini dikkate almalıdır. Buna ek olarak, veriler kurum genelinde hareket ederken kurum tetikte olmalı ve bu verileri oluşturan, bunlara temas eden ve bunları taşıyan insanları bilmelidir.

Veri koruması:

- Çalışanlarınızın verileri oluşturmak, depolamak ve taşımak için kullandığı tüm uygulamalar için tek bir kontrol noktası ile **düzenlenmiş verileri güvenceye almalıdır**.
- İnsanların verileri nasıl kullandığını analiz eden, çalışanlarınızı verilerle ilgili doğru kararlar vermeye yönlendiren ve olayları riske göre önceliklendiren gelişmiş DLP ile **fikri mülkiyeti korumalıdır**.

İnsanların çalıştığı ve verilerin bulunduğu her yerde görünürlük ve kontrol sağlama

- Bulut Uygulamaları (Forcepoint CASB ile desteklenen)
- Uç nokta
- Ağ
- Tespit

Forcepoint DLP, kullanıcıların çalıştığı ve verilerin bulunduğu her yerde, insan kaynaklı riskleri görünürlük ve kontrol sağlayarak ele alır. Güvenlik ekipleri, en önemli olaylara odaklanmak ve küresel veri düzenlemeleri ile uyumu hızlandırmak için kullanıcı riski puanlamasını kullanır.

UYUMU HIZLANDIRIN

Modern bilişim ortamı, onlarca küresel veri güvenliği düzenlemesine uymayı amaçlayan kurumlar için, özellikle de bulut uygulamalarına ve mobil iş gücüne geçiş aşamasında zorluk olarak ortaya çıkmaktadır. Pek çok güvenlik çözümü, bulut uygulamalarda olduğu gibi bir tür entegre DLP içerir. Ancak güvenlik ekipleri, ayrı ve tutarsız politikaları uç noktalar, bulut uygulamaları ve ağlar genelinde uygularken ve yönetirken istenmeyen karmaşıklık ve ek maliyetlerle karşı karşıya kalmaktadır.

Forcepoint DLP, küresel düzenlemelerin hazır kapsamı ile BT ortamınız genelindeki merkezi kontrolü birleştirerek uyumluluk çabalarınızı hızlandırır. Forcepoint DLP hassas müşteri bilgileri ve düzenlenmiş verilerin güvenliğini etkin biçimde sağlar, böylece uyumluluğu güvenceye almış olur.

- 83 ülkenin mevzuat şartları için geçerli olan 370'ten fazla politikaya uyumu sağlamak ve bunu sürdürmek için **mevzuat kapsamı**.
- Ağ, bulut ve uç noktası keşfi ile **düzenlenmiş verileri bulun ve onarın**.
- BT ortamı genelinde **merkezi kontrol ve tutarlı politikalar**.

VERİLERİ KORUMAK İÇİN ÇALIŞANLARA YETKİ VERİN

Sadece önleyici kontrollere sahip DLP, bunları sadece bir görevi tamamlamak amacıyla aşmaya çalışacak kişileri caydırır. Güvenliği pas geçmek, gereksiz risklere ve veri maruziyetine neden olur.

Forcepoint DLP, çalışanlarınızı günümüz siber tehditlerini önlemede ön saflardadır..

- Bulutta, ağda, e-postada veya uç noktada, **her nerede olursa olsun verileri keşfedin ve kontrol edin**.
- Kullanıcı eylemlerini yönlendiren, çalışanları politika konusunda eğiten ve kritik verilerle etkileşime giren kullanıcının niyetini doğrulayan mesajları kullanarak, **çalışanları akıllı kararlar almaya hazırlayın**.
- Kurumunuzun dışına çıkan verileri koruyan, politika tabanlı otomatik şifreleme yöntemini kullanarak **güvenilir iş ortakları ile güvenli işbirliği yapın**.
- Önde gelen üçüncü taraf veri sınıflandırma çözümleri (örn. Microsoft Azure Information Protection, Bolden James, Titus) ile entegrasyon yoluyla **veri sınıflandırma ve etiketleme gerçekleştirin**.

GELİŞMİŞ TESPİT VE VERİLERİ TAKİP EDEN KONTROLLER

Kasıtlı veya kasıtlı olmayan veri ihlalleri münferit olaylar değil karmaşık olaylardır. Forcepoint DLP; Gartner, Forrester, vb. analist firmaların sektörde lider olarak kabul ettiği kanıtlanmış bir çözümdür. Forcepoint DLP çözümleri 2 farklı sürüme sahiptir: Uyumluluk için DLP ve IP Koruması için DLP.

Uyumluluk için Forcepoint DLP, uyumluluğa yönelik aşağıdaki özellikler sayesinde kritik bir işleve sahiptir:

- **Optik Karakter Tanıma (OCR)** durağan veya hareket halindeki görüntülerin içine gömülü verileri belirler (Forcepoint DLP – Ağ ile birlikte kullanılabilir).
- **Kişisel Bilgilerin (PII) doğru belirlenmesi** veri doğrulama kontrolleri, gerçek ad tespiti, yakınlık analizi ve içerik tanıtıcıları içerir.
- **Özel şifrelemenin belirlenmesi** keşif yöntemleri ve geçerli kontrollerden gizlenen verileri ortaya çıkarır.
- **Kümülatif analiz** drip-DLP (zaman içinde yavaşça sızan veriler) tespitine yöneliktir.
- **Microsoft Azure Information Protection ile entegrasyon** şifreli dosyaları analiz eder ve veriler için uygun DLP kontrollerini uygular.

IP Koruması için Forcepoint DLP, aşağıdaki özellikler sayesinde potansiyel veri kaybının tespiti ve kontrolüne yönelik en gelişmiş teknikleri uygular:

- **Makine öğrenmesi** kullanıcıların daha önce hiç görülmemiş ilgili verilerin belirlenmesi konusunda sistemi eğitmesini sağlar. Kullanıcılar benzer iş belgeleri, kaynak kodu ve daha fazlasının işaretlenmesi için analitik motorunapozitif ve negatif örnekler gönderir.
- **Yapısal ve yapısal olmayan verilerin parmak izi kontrolü** veri sahiplerinin veri türlerini tanımlamasını ve iş belgeleri, tasarım planları ve veri tabanları genelinde tam ve kısmi eşleşmeleri belirlemesini, ardından verilere uygun doğru kontrolü veya politikayı uygulamasını sağlar.
- **Analizler kullanıcı davranışındaki değişiklikleri belirler** ve kişisel e-postanın artan kullanımı gibi veri etkileşimlerini ortaya çıkarır.

RİSKE MÜDAHALE EDİN VE RİSKİ GİDERİN

Geleneksel DLP yaklaşımları kullanıcıları hatalı onaylanmış sonuçlarla oyalarken riskli verilerin kaybedilmesine neden olur. Forcepoint DLP, görünüşte alakalı olmayan DLP olayları ile öncelik verilmiş olaylar arasında korelasyon kurmak için gelişmiş analizleri kullanır. Forcepoint DLP bünyesinde sunulan Olay Risk Tasnifi (IRR), veri hırsızlığı ve kesilen iş süreçleri gibi veri riski senaryolarının olasılığını değerlendirmek için farklı DLP göstergelerini bir Bayes inanç ağı çerçevesi içinde bir araya toplar.

- Riskten sorumlu insanları, risk altındaki kritik verileri ve kullanıcılar genelinde görülen yaygın davranış kalıplarını vurgulayan önceliklendirilmiş olaylar ile **müdahale ekiplerini en riskli yerlere yönlendirin**.
- Farklı olayları birbirine bağlayan, risk altındaki verilerin bağlamını gösteren ve analistlerin harekete geçmesi için ihtiyaçları olan bilgileri sağlayan iş akışları ile **soruşturun ve müdahale edin**.
- Anonim hale getirme seçenekleri ve erişim kontrolleri ile **kullanıcı gizliliğini koruyun**.
- Forcepoint İç Tehdit ve Forcepoint UEBA ile derin entegrasyonlar yoluyla **veri bağlamını** daha kapsamlı kullanıcı analizlerine ekleyin.

ÇALIŞANLARINIZIN İŞ YAPTIĞI HER YERDE GÖRÜNÜRLÜK, VERİLERİNİZİN BULUNDUĞU HER YERDE KONTROL SAĞLAMA

Forcepoint DLP, ürünün her kurulumunda tek bir kontrol noktasından gelişmiş analizler ve düzenleyici politika şablonları içerir. İşletmeler BT ortamları için kurulum seçeneklerini kendileri seçer.

EK A: DLP ÇÖZÜMÜ BİLEŞENLERİNE GENEL BAKIŞ

Forcepoint DLP – Uç nokta	Forcepoint DLP – Uç Nokta, kurumsal ağ içinde ve dışında, Windows ve Mac uç noktalarındaki kritik verilerinizi korur. Durağan (keşif), hareket halindeki ve kullanımdaki veriler için gelişmiş koruma ve kontrol içerir. Microsoft Azure Information Protection ile entegrasyon sayesinde şifreli verileri analiz eder ve uygun DLP kontrollerini uygular. Çözüm, HTTPS gibi web yüklemelerini ve ayrıca Office 365 ve Box Enterprise gibi bulut hizmetlerine yapılan yüklemeleri izler. Outlook, Notes ve e-posta istemcileri ile tam entegrasyon.
Forcepoint DLP – Bulut Uygulamaları	Forcepoint CASB ile desteklenen DLP – Bulut Uygulamaları, Forcepoint DLP'nin gelişmiş analizleri ve tek noktadan kontrolünü Office 365, Salesforce, Google Apps, Box gibi kritik bulut uygulamalarına aktarır.
Forcepoint DLP – Keşif	Forcepoint DLP – Keşif, ağınız genelinde bulunan hassas verilerin yanı sıra Office 365 ve Box Enterprise gibi bulut hizmetlerinde depolanan verileri belirler ve güvenceye alır. Gelişmiş parmak izi kontrolü teknolojisi, düzenlenmiş verileri ve durağan haldeki fikri mülkiyeti belirler ve uygun şifreleme ve kontrolleri uygulayarak bu verileri korur.
Forcepoint DLP – Ağ	Forcepoint DLP – Ağ, hareket halindeki verilerin e-posta ve web kanalları yoluyla hırsızlığını durdurmak için kritik uygulama noktasını sağlar. Çözüm, dış saldırılardan veya artan iç tehditlerden kaynaklanan, kasıtlı veya kazara gerçekleşen veri kaybını belirlemeye ve önlemeye yardımcı olur. OCR (Optik Karakter Tanıma) bir görüntü içindeki verileri tespit eder. Analizler, tek seferde bir kayıt olmak üzere veri hırsızlığını ve diğer yüksek riskli kullanıcı davranışlarını durdurmak üzere DLP kullanır.

EK B: DLP ÇÖZÜMÜ BİLEŞENLERİNİN AYRINTILARI

	FORCEPOİNT DLP – UÇ NOKTA	FORCEPOİNT DLP – BULUT UYGULAMALAR	FORCEPOİNT DLP – KEŞİF	FORCEPOİNT DLP – AĞ
Nasıl Kurulur?	Uç Noktası Aracısı	Forcepoint Bulut	BT Yönetimli Keşif Sunucusu	Ağ Aracı veya Herkese Açık Bulut
Ana işlevi nedir?	Kullanıcı uç noktası hakkında bilgi toplama	Bulutta veya bulut tabanlı uygulamalar ile veri keşfi ve politika uygulaması	Veri merkezleri bünyesindeki durağan verilerin keşfi, taranması ve onarımı	Web ve e-posta yoluyla hareket halindeki veriler için görünürlük ve kontrol
Tüm durağan veriler nerede keşfedilir/korunur?	Windows uç noktaları MacOS uç noktaları Linux uç noktaları	Exchange Online Sharepoint Online Box	Şirket içi dosya sunucuları ve ağ depolaması Sharepoint Server Exchange Server	
Hareket Halindeki Veriler nerede korunur?	E-posta Web: HTTP(S) Yazıcılar Çıkarılabilir araçlar Mobil cihazlar Dosya sunucuları/NAS	Google Apps yüklemeleri ve paylaşımları Office 365/OneDrive yüklemeleri ve paylaşımları Salesforce.com ve Box		E-posta/Mobil e-posta/ ActiveSync vekil sunucu Web: HTTP(S) ICAP
Kullanımdaki Veriler nerede korunur?	IM, VOIP dosya paylaşımı, uygulamalar (bulut depolama istemcileri), işletim sistemi panosu	Bulut uygulamaları kullanarak işbirliği faaliyetleri sırasında		
Olay Risk Tasnifi*	Dahil	Dahil		Dahil
Optik Karakter Tanıma (OCR)			Dahil	Dahil
Veri Sınıflandırma Entegrasyonları	Microsoft Azure Information Protection, Bolden James, Titus			
Hangi Verilere Parmak İzi Kontrolü yapabilirim?*	Yapısal (veri tabanları), yapısal olmayan (belgeler), İkili (metin harici dosyalar)			

*Bu özellikler IP Koruma sürümünde mevcuttur. Ayrıntılar için bkz. Ek C.

FORCEPOINT HAKKINDA

Forcepoint, nerede bulunursa bulunsun kritik veriler ve fikri mülkiyet ile etkileşim halindeki insanların niyetini anlamaya odaklanarak siber güvenliğe yeni bir bakış açısı kazandırıyor. Ödün vermeyen sistemlerimiz, şirketlerin çalışanlarına gizli veriler için özel erişim vermesini sağlarken fikri mülkiyeti korur ve uyum sürecini kolaylaştırır. Genel merkezi Teksas, Austin'de bulunan Forcepoint, dünya genelinde 20.000'den fazla kuruluşu desteklemektedir. Forcepoint hakkında daha fazla bilgi için, www.forcepoint.com adresini ziyaret edin ve Twitter'da bizi takip edin: @ForcepointSec.

İLETİŞİM

www.forcepoint.com/contact

[BROCHURE_FORCEPOINT_DATA_LOSS_PREVENTION_TUR 400026.06JUL18]