Forcepoint | SECLORE

Çözüm Özeti

Forcepoint DLP için Seclore

Sorun

- DLP, hassas verilerin işletmeden çıkmasını engelleyebilir veya çıktıktan sonra takip edebilir. Çıkış sırasında veri engelleme, verimlilik iş akışlarında kesintiye neden olurken, verilerin takip edilmesi korunmasız bir şekilde gönderilmesine neden olur.

Çözüm

- Keşfedilen verilere otomatik olarak kalıcı, parçalı kullanım kontrolleri eklemek
- Dosya izinlerini anında ve dinamik olarak atamak ve geri almak
- Güvenlik izinleriyle DLP iş kuralları arasındaki bağlantıyı haritalamak
- Verileri uç noktalarda, ağda veya e-postaların içinde güvenlik altına almak
- Veri kullanımına ilişkin adli ayrıntıları toplamak

Sonuç

- Maliyetleri azaltmak ve "zamanın değere" dönüştürülmesini artırmak için DLP dağıtımını hızlandırmak
- İdari genel masrafları azaltmak için hatalı pozitif sonuçları çok büyük oranda azaltmak
- Kesintisiz dahili ve harici iş birliği sağlamak
- Kontrol sağlamak ve kurumdan ayrıldıklarında hassas verileri takip etmek
- Denetim ve mevzuat uyumu sağlamak

Veri Kaybı Önleme (DLP) çözümü, hassas verileri keşfeder ve ağınızın dışına sızmasını önler. Ancak, veriler keşfedildikten sonra ne olur? Tüm bu olaylarla ne yaparsınız? E-postalar uç noktada engellendiğinde veya korunmasız olarak gönderildiğinde, harici üçüncü taraf iş ortaklarınızla iş birliğini nasıl güvende tutabilirsiniz? Bulut yoluyla paylaşılan veya harici yüklenicilerin mobil cihazlarında görüntülediği dosyaları nasıl koruyabilirsiniz? Yanlış ellere geçtiğinde, hassas verileri nasıl geri alabilirsiniz?

Seclore Hak Yönetimi ve Forcepoint DLP

DLP, belgelerin içeriğini inceleyip hassas verileri keşfedebilir. Hassas veriler tespit edildiğinde, belgeler ve verilerle etkileşim için uygun kullanım kontrollerini (hakları) otomatik olarak ekleyebilirsiniz. Seclore Hak Yönetimi entegrasyonu sayesinde, kurum sınırlarının dışına çıktığında dahi bilgileriniz üzerinde tam kontrole (erişimi tamamen engellemek dahil olmak üzere) sahip olursunuz. Forcepoint DLP hassas verileri keşfeder keşfetmez, Seclore bu verileri uygun kullanım politikalarıyla anında korumaya başlayabilir. Seclore'un kalıcı ve parçalı veri kullanımı kontrolleri kurum içinde veya dışında gittiği her yerde dosyayla birlikte kalır ve kullanımda (üzerinde çalışılan dosyalar), hareket halinde (e-posta ile gönderilen) ve durağan verileri (her türlü veri biçimi, cihaz ve işletim sistemi) korur.

İkinin Gücü

Seclore Hak Yönetimi çözümü, Forcepoint DLP kullanırken güvenlik yaklaşımınızı reaktiften proaktife dönüştürmenizi sağlar. Geleneksel olarak DLP, izleme modunda çalışmak için yapılandırılmıştır ve kurumdan çıktıklarında bilgileri takip eden panolar, raporlar ve uyarılar sağlar. İzleme modu, DLP'nin standart uygulamalarından biridir, ancak güvenlik açısından asıl endişe, hassas verilerin kurumdan çıkmasıdır. Hassas verileriniz kötü niyetli kişilerin eline geçerse veya bu verileri bir üçüncü taraftan geri almanız gerekirse, bunu yapabilmek için hassas verileri kovalamanız gerekir. Seclore sayesinde, kontrol her zaman sizdedir.

Seclore Hak Yönetimi çözümü, aynı zamanda Forcepoint DLP'nin dağıtımını da büyük ölçüde hızlandırır. Keşfedilen bilgilere uygulanacak iş kurallarından (engelleme, karantinaya alma, izin verme, vb.) emin değilseniz, bilgileri Seclore ile otomatik olarak korumak varsayılan eyleminiz haline gelebilir. Ayrıca, sürekli yapılandırma ihtiyacını da ortadan kaldırır.

DLP Keşfeder

- → İçeriği tarar
  - Anahtar kelimeler
  - Kalıplar
  - Dijital Parmak İzleri
  - Optik Karakter Tanıma (OCR)
- → Hassas bilgilerin kurumsal çevre dışına çıkmasını önler
- → Kurum içerisindeki olayları kaydeder

Hak Yönetimi Korur

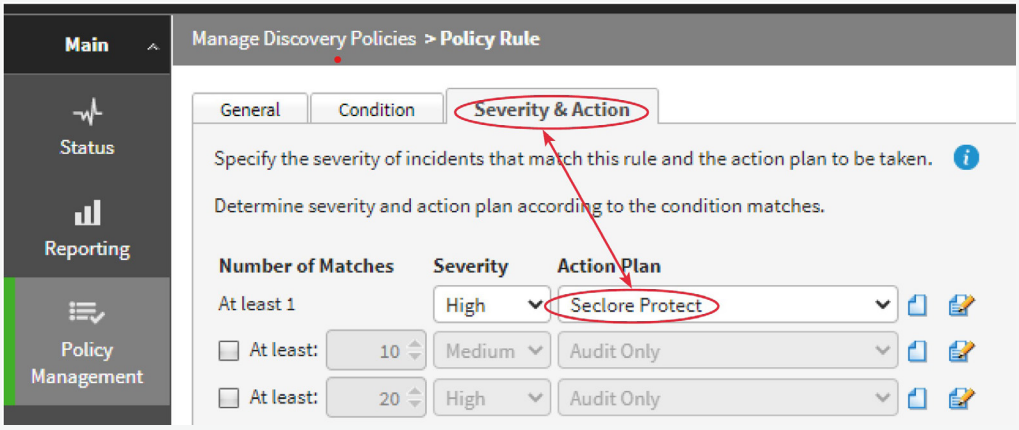
- → İçeriği güvenlik altına alır
  - Parçalı kullanım kontrolleri
  - Kimin, neye, nerede, ne zaman ve nasıl erişebileceğini belirleyin
  - Erişimi kısıtlayın ve reddedin
  - Kullanımdaki, hareketli ve durağan veriler
- → Yetkilendirilmiş harici kullanıcıların hassas bilgilere erişmesine izin verir
- → Verileri kurum sınırları içinde ve dışında takip eder ve denetler

Seclore RM ve Forcepoint DLP çözümlerini bir arada kullandığınızda, belgelere kimlerin erişebileceğini ve o belgeyle neyi, ne zaman ve hangi cihaz veya bilgisayardan yapabileceğini kontrol edebilirsiniz. Kalıcı, veri merkezli kullanım kontrolleri eklendiğinde, Forcepoint DLP'nin kapsamı genel ağlarda veya iş ortaklarının ağlarında hareket halinde olan, bulutta veya dosya paylaşımı hizmetlerinde depolanan veya mobil cihazlardan erişilen belgeleri kapsayacak şekilde genişletilebilir.

Anında Koruma: Uç Noktalarda, Ağda veya Bulutta

Uç noktalarda, ağda veya bulutta Forcepoint DLP keşif taramaları sırasında keşfedilen hassas veriler, Seclore Hak Yönetimi (RM) çözümüyle anında korumaya alınabilir. Örneğin, Seclore koruma politikaları, hassas anahtar kelimelerin veya sık kullanılan ifadelerin (ör. kredi kartı numaraları) keşfine haritalanabilir. Kullanım kontrolleri, dosya kendilerine gönderilse bile bırakın şirket dışındaki kişileri, sorumlu departman dışında kimsenin o dosyayı kullanamamasını sağlar. Forcepoint DLP sayesinde, dosya sunucuları dahil her yerde bulunan veya kullanıcılar tarafından dağıtılmakta olan hassas verilerin tanınması için hassas ID parmak izlerinden faydalanarak koruma kapsamı genişletilir ve yöneticilerin dikkatlerini en riskli kullanıcı ve davranışlara odaklamasına imkan tanınır.

Ayrıca, bu koruma neredeyse anında ve tamamen otomatiktir. DLP keşif politikalarına dayalı otomatik kullanım kontrolü uygulanması, çalışanların ek adımlar atmasına gerek bırakmaz, eğitim maliyetlerini ve değişim yönetimi çabalarını azaltır.



Şekil 1: Keşif sonuçları otomatik olarak koruma politikasına bağlanır.

Seclore Hak Yönetimi ve Forcepoint DLP Uç Nokta

Forcepoint DLP, belgeleri tarayıp ağ uç noktalarında bulunan gizli verileri keşfedebilir. Forcepoint DLP, anahtar kelimeleri (ör. gelir tahminleri), kalıpları ve sık kullanılan ifadeleri (ör. kredi kartı numaraları) eşleştirebilir ve ayrıca belli biçimlerdeki dosyaları aramak için belirli klasörleri inceleyebilir. Keşiften sonra; Seclore, kurum yöneticisinin belirlediği politika tanımlarına bağlı olarak sızmasını veya suistimal edilmesini önlemek için ilgili Seclore politikasını uygulayarak bu hassas bilgileri korur. Forcepoint DLP sayesinde, ağ içi politikaları ağ dışındaki cihazları kapsayacak şekilde genişletebilir ve kullanıcılar uzakta olduğunda dahi verileri korumak için politikaları her bir uç nokta seviyesinde uygulayabilirsiniz.

Avantajları

- → Ağ içindeki veya dışındaki hassas bilgiler için otomatik koruma
- → Hassas verileri korumanın kullanıcılara bağlı olmasının azaltılması
- → Her yerde dosyanın yanında kalan koruma—depolama, hareket halinde ve kullanımdayken

Şekil 2: Uç Nokta Keşfi

Seclore Hak Yönetimi ve Forcepoint DLP Ağ

Forcepoint DLP, dosya sunucularında bulunan hassas belgeleri tarar. Kurum içerisinde ve kurum sınırlarının ötesinde hareket halinde olan verilerin korunması çok önemlidir. DLP Ağ çözümü sayesinde, e-posta ve web gibi iletişim kanallarından akan verileri takip ederek kullanımdaki verileri koruyabilirsiniz. Seclore, hassas bilgileri sızmalarını veya suistimal edilmelerini önleyecek şekilde güvenlik altına alarak koruma kapsamını genişletir.

Şekil 3: Ağ Keşfi

Seclore Veri Sınıflandırma ve Forcepoint DLP

Boldon James tarafından desteklenen Seclore Veri Sınıflandırma çözümü, Forcepoint DLP ile birlikte çalışarak veri keşfi sırasında hatalı pozitif sonuçları azaltır.

- → **Örneğin, bir kullanıcı**, sadece Office kurdele menüsündeki bir sınıflandırma etiketine tıklayarak bir Office dosyasını sınıflandırır.
- → **Forcepoint DLP**, seçilen sınıflandırmaya göre belgeyi etiketler.
- → **Seclore Hak Yönetimi çözümü**, uygun kullanım politikasıyla belgeyi korur. Belge dünyanın neresinde açılırsa açılsın, Seclore koruması çalışmaya devam eder.
- → **Forcepoint parmak izi alma özelliği**, veri sızıntılarının tespit edilip önlenmesi için belgenin kısmi bölümleri kopyalandığında, yapıştırıldığında veya düzenlendiğinde bu durumun keşfedilmesini sağlar.
- → Belge üzerinde gerçekleştirilen her türlü faaliyet gerçek zamanlı ve merkezi olarak kaydedilir. Belge sınıflandırması kullanıcı tarafından seçildiğinden, **hatalı pozitif sonuç ihtimali neredeyse tamamen ortadan kalkar.**

Seclore Otomatik E-Posta Koruması ve Forcepoint E-Posta Güvenliği

DLP E-Posta Güvenliği, hatalı pozitif sonuç riskinden dolayı sıklıkla keşif modunda çalıştırılır. Anormal kullanıcı davranışları, ancak olay gerçekleştikten sonra keşfedilir. İş amacıyla ağın dışına çıkması gereken veriler söz konusu olduğunda, e-postaların tamamen korunmasız şekilde gitmesine izin vermekten başka seçenek yoktur.

Seclore, bu sorunlara kolay ve modernleştirilmiş bir çözüm sunuyor. E-postalar DLP E-Posta Ağ Geçidi tarafından işlendikten sonra, Seclore Hak Yönetimi çözümünün otomatik koruma özelliği, e-postayı ve eklerini uygun kullanım politikasıyla güvenlik altına alır. Bu da alıcıların e-postayı alıp okuduktan sonra kötüye kullanmalarını veya sızdırmalarını engeller. Dolayısıyla, DLP ile uygulanan "izin verme" politikası, Seclore ile "önümüzdeki 10 gün için" politikasına dönüşür.

Seclore Hak Yönetimi çözümünün otomatik e-posta koruması sayesinde, e-posta güvenliği uygulamalarının e-posta ile gerçekleşen kritik iş birliğini durdurması gerekmez. Veri paylaşımı devam ederken, güvenlik ve uyum da korunmuş olur. Üstelik tüm bunlar e-postayı gönderen ve alan kişiler için tamamen şeffaf şekilde gerçekleşir.

Şekil 4: Seclore ve Forcepoint DLP

Forcepoint DLP İçerik Keşfi için Güvenli E-Posta Şifre Çözme

DLP sistemlerinin karşılaştığı zorluklardan biri, bir e-postanın paylaşılması mı yoksa engellenmesi mi gerektiğine karar vermek için şifreli e-posta ve eklerdeki hassas içerikleri keşfetmektir. Seclore E-Posta Şifre Çözücü uygulaması, Seclore şifreli e-posta ve eklerine güvenli erişim sağlayarak bu sorunu çözer. Korunmakta olan e-postanın şifresi çözüldüğünde, Forcepoint DLP hassas içerikleri ve kalıpları arayarak uygun kararı (izin ver/engelle/koru) verebilir.

Seclore E-Posta Şifre Çözücü uygulaması, e-postaların kurum dışına gönderilmeden önce korunmaya alınmasını otomatik hale getirmek için Seclore Otomatik E-Posta Koruyucu ile birlikte çalışır.

Forcepoint DLP korunan ve korunmayan tüm dosyaları keşfedebileceği, takip edebileceği ve denetleyebileceği için, Seclore Hak Yönetimi ve Forcepoint DLP çözümlerini kullanan kurumlar mevzuata uyduklarını söyleyebilir.

Başlıca Ticari Faydaları

Otomatik Veri Koruması
DLP ile Dijital Hak Yönetimi (DRM) çözümlerinin entegrasyonu, tüm sınıflandırma, koruma, erişim kontrolü ve denetim sürecini otomatik hale getirir. Tespitten korumaya devir, sorunsuz şekilde gerçekleşir. DRM koruma süreci, son kullanıcı için tamamen şeffaftır.

Daha Hızlı DLP Dağıtımları
DRM, DLP dağıtıldığı anda fayda sağlamaya başlamak için DLP'nin "varsayılan" iş kuralı olarak ayarlanabilir.

Güvenlik Duvarının Ötesinde Güvenlik ve Uyum
DLP-DRM entegrasyonu, verileri gittikleri her yerde korur ve denetler: tedarikçi ve iş ortağı ağlarında, genel ağlarda, bulutta ve mobil cihazlarda.

Daha Kısa Olay Listesi
DLP; DRM tarafından korunan dosyaları güvenli kabul edecek ve bu dosyalar için uyarı oluşturmayacak şekilde yapılandırılabilir. Bu da çok daha az olay kaydı anlamına gelmektedir.

Minimum Eğitim Giderleri
Koruma otomatik olduğu ve korunan belge diğer tüm belgeler gibi ilgili uygulamada açıldığı için son kullanıcılar için neredeyse hiç eğitim gerekmez.

İş Çevikliğinde Artış
Kurumsal sınırların dışına çıkan bilgileri koruma becerisi, çok ciddi bir uyum sorununu çözer, güvenlik risklerini önemli ölçüde azaltır ve dosya paylaşımı hizmetlerinin, BYOD ve bulut bilişim uygulamalarının güvenle benimsenmesini sağlar.

Uçtan Uca Denetim ve Mevzuata Uyum
DLP-DRM entegrasyonu, kurumsal ağın içindeki ve dışındaki yapılandırılmamış verilerin ömürleri boyunca mevzuat gereksinimlerine uyum sağlanmasına imkan tanır.

BT Politikalarını Üçüncü Taraflara Uygulamak
DLP-DRM entegrasyonu; veri yönetimi ve kurumsal BT politikalarınızın yüklenicilere, tedarikçilere, iş ortaklarına ve diğer üçüncü taraflara uygulanmasına imkan sağlar.

Forcepoint hakkında

Forcepoint, dijital dönüşüm ve büyüme sağlarken kurumları koruması için güvenilen, kullanıcı ve veri koruma alanında lider siber güvenlik şirketidir. Forcepoint'in uyumlu çözümleri, insanların verilerle etkileşime girme şekillerine gerçek zamanlı olarak uyum sağlar ve erişim güvenliği sağlarken, çalışanların değer üretmesine de imkan tanır. Genel merkezi Teksas, Austin'de bulunan Forcepoint, dünya çapında binlerce müşteri için güvenli ve güvenilir ortamlar yaratmaktadır.

forcepoint.com/contact

Seclore hakkında

Seclore, şirketlere kurum sınırları içinde ve dışında her yerdeki verilerinin kullanımını keşfetme, belirleme, koruma ve denetleme odaklı sınıfının en iyisi çözümlerden faydalanma imkanı sağlayan, piyasadaki ilk tarayıcı tabanlı Veri Merkezli Güvenlik Platformunu sunmaktadır. Veri merkezli güvenlik sürecinin otomatik hale getirilmesi, kurumların bilgilerini minimum zorluk ve maliyetle tamamen korumasını sağlamaktadır. 29 ülkede 2000'den fazla şirket; veri güvenliği, yönetim ve uyum hedeflerine ulaşmak için Seclore'dan faydalanmaktadır.

seclore.com/contact