Forcepoint

Bilgi Formu

Forcepoint Data Security Posture Management

Temel özellikler ve avantajlar:

- **AI Mesh Sınıflandırması –** GenAI, öngörücü yapay zeka ve veri bilimi özelliklerini kullanan son derece doğru ve verimli ağ bağlantılı sınıflandırma mimarisi.
- **Hızlı keşif –** Forcepoint DSPM'yi bulut ve yerinde depolama konumlarında istediğiniz sıklıkta çalıştırın.
- **Gerçek zamanlı risk değerlendirmesi –** Erişim izinlerini ve diğer veri risklerini kontrol edin.
- **İş akışı yönetimi –** Paydaşlar için iş önceliklerini uygulamaya alın.

Dijital dönüşüm, yapay zeka teknolojilerinin, özellikle de GenAI uygulamalarının iş süreçlerine entegrasyonu sayesinde yapay zeka dönüşümü halini aldı. Uygulamalarını ve verilerini kurum içinden buluta taşıyan ve ChatGPT, Copilot ve Gemini gibi GenAI araçlarından yararlanan veri yayılımıyla birlikte kurumlar, hassas verilerinin nerede olduğunu, bunlara kimlerin erişebileceğini ve nasıl kullanıldığını takip etmenin zorluğuyla karşı karşıya kalıyorlar. Bulut tabanlı depolar içinde gizlenen veya bireysel cihazlara yayılan, şimdi de Gen AI uygulamaları olan "karanlık verilerin" katlanarak büyümesi önemli bir risk oluşturuyor. Kuruluşun verilerinin yüzde 80'lik bölümünü bu belirsiz "karanlık" durumda olan ve geleneksel gözetimin dışında kalan verilerin oluşturduğu tahmin edilmektedir.

Bu belirsiz verilerin neden olduğu görünümün sonucu kritik öneme sahiptir. Kuruluşlar, net görünürlük ve yönetim olmadan yüksek risk ihlallerine maruz kalıyor ve ticari, kar amacı olmayan ve kamu sektörlerinde potansiyel olarak yıkıcı sonuçlara yol açabiliyor. Günümüzün dijital dönüşüm çağında, hassas bilgilerin kontrolünün yeniden ele alınması acil bir zorunluluk halini almıştır.

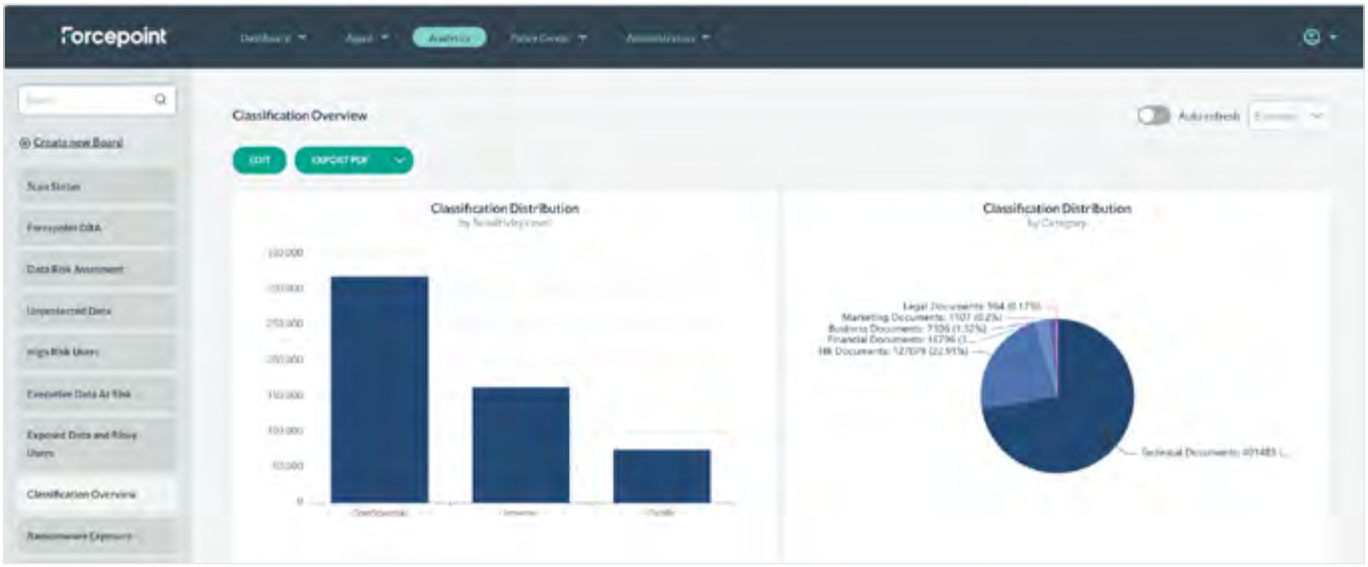
Forcepoint DSPM'nin AI Mesh teknolojisi, kuruluşlara veri sınıflandırmada üstün doğruluk sağlar. Üretken yapay zeka Küçük Dil Modeli (SLM) ile gelişmiş veri ve yapay zeka bileşenlerinden yararlanan ağ bağlantılı yapay zeka mimarisi; yapılandırılmamış metinlerden bağlamı verimli bir şekilde yakalar. Bu özelleştirilebilir ve verimli sistem; kapsamlı bir eğitime gerek kalmadan hızlı ve doğru sınıflandırma imkanı sunar. Bu sayede güveni ve uyumluluğu destekler.

Hızlı, kapsamlı keşif

Çok sayıda bağlayıcıyla Forcepoint DSPM, bulut veya kurum içi seçeneklerde de hassas verileri verimli bir şekilde bulur. Bu sayede Amazon (AWS S3 ve AEM), Microsoft (Azure AD, OneDrive, SharePoint Online) ve Google (Google Drive ve AEM) gibi büyük platformlarda ve yerel LDAP ve SharePoint sistemlerinde saatte yaklaşık bir milyon dosyayı taramaya imkan tanır.

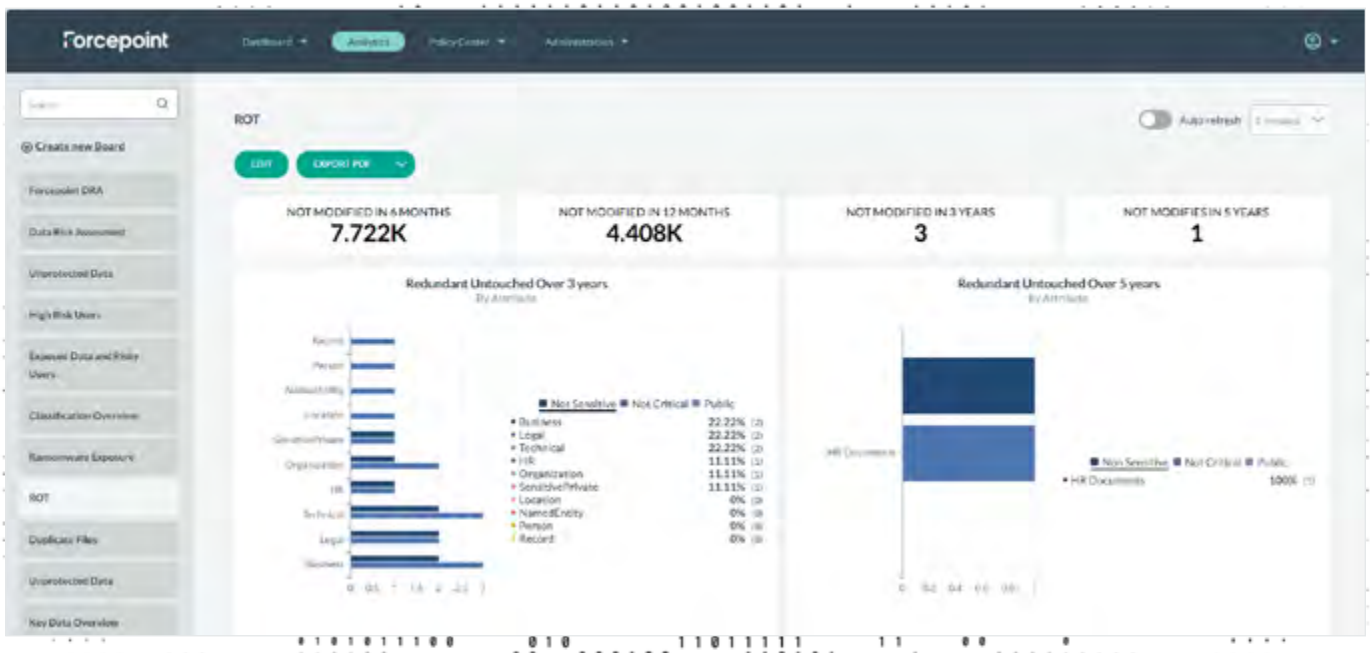
AI Mesh doğruluğu mümkün kıldı

Forcepoint DSPM'nin AI Mesh özelliği, günümüz kuruluşlarını üstün veri sınıflandırma doğruluğu ile güçlendirmede üstünlük kazanır. Diğer DSPM çözümlerinden farklı olarak, bir GenAI SLM'den ve gelişmiş veri ve yapay zeka bileşenlerinden oluşan bir ağdan yararlanan çok düğümlü, bağlı bir yapay zeka mimarisi sunar. Bu yapı, içeriği verimli bir şekilde yakalar ve yapılandırılmayan metinleri kesin belge sınıflandırmalarına dönüştürür. AI Mesh özelleştirilebilir, endüstri ihtiyaçlarına ve düzenleyici çevrelere uyarlanabilir. Yüksek performanslı sınıflandırma sağlarken GPU gerektirmeden standart bilgi işlem kaynaklarında verimli bir şekilde çalışır. Geniş ML eğitimi olmadan yüksek doğruluk elde edilir ve bakım maliyetlerini azaltır. AI Mesh açıklanabilirliği, güven ve uyumluluğu artırarak son derece güvenli bir veri duruşunu ve gizlilik düzenlemelerine uymayı sağlar.



Yüksek performanslı izleme ve veri riski değerlendirmesi

Forcepoint DSPM, verileri tarar ve keşfederken, kritik bilgiler içeren dahili olarak paylaşılan dosyaların sayısı, risk altındaki PII dosyalarının sayısı ve gereksiz, eski ve önemsiz veri (ROT) dosyalarının sayısı gibi ayrıntılı bilgiler sunar.



İş akışı yönetimi

Forcepoint DSPM ile veri güvenliği yönetimini zahmetsizce kolaylaştırın. Sezgisel iş akışı yönetimi, veri sahipliğinin ve hesap verebilirliğinin verimli bir şekilde izlenmesini sağlar. Siloları ortadan kaldırıp paydaşlar arasında işbirliğini kolaylaştırarak sorumlulukları aynı doğrultuya getirir, operasyonel verimliliği artırır ve kuruluş genelinde netliği teşvik eder.

Güçlü bir DSPM çözümünün uygulanması, veri duruşunu güvence altına almayı ve bulut ve tesis içi veri depolama konumlarında hassas bilgileri korumayı hedefleyen kuruluşlar için çok önemlidir. Kuruluşlar, Forcepoint DSPM'yi kullanarak veri erişimi ve paylaşımının güvenilirliğini artırarak, yenilikleri teşvik ederek ve işbirliğini teşvik ederek verimliliği artırabilir. Aynı anda, hassas verilerin yanlış kullanımını proaktif olarak belirleyerek ve ele alarak riski azaltabilir, böylece veri ihlallerini önleyebilir. Sonuç olarak, kuruluşlar tüm çevrelerdeki hassas veriler üzerinde gerçek görünürlük ve kontrol elde ederek uyumluluk çabalarını kolaylaştırabilir.

Güçlü Keşif

ÖZELLİK	AVANTAJ
Hızlı keşif ve kataloglandırma	Saniye/saat başına daha fazla dosya hacmini taramak için birden fazla kaynakta çalışır ve yapılandırılmayan veri kaynaklarıyla ilgili ayrıntıları sentezleyerek bunları işlemesi kolay bir biçimde düzenler.
Önemli veri kaynaklarına bağlanır	Bir dizi veri kaynağı bağlayıcısı sayesinde yapılandırılmamış verilere dair kapsamlı görünürlük.
Risk altındaki verilerin analizi	Herkese açık olarak paylaşılan, üçüncü taraflarla harici olarak paylaşılan ve dahili olarak çok fazla paylaşılan risk altındaki verileri tanımlayın.
İzinleri görüntüleyin ve düzeltin	Her dosya için erişimi görüntüleyin ve en az ayrıcalık (POLP) sıfır güven güvenliği ilkesi oluşturmak için düzeltin.
ROT (gereksiz, eski, önemsiz) verilerinden kaynaklanan riski ortadan kaldırın	Gereksiz, eski veya önemsiz (ROT) dosyaları tanımlayın ve ortadan kaldırın.
Erişim ve izinlere görünürlük	Active Directory ve diğer IRM çözümleriyle yapılan entegrasyonlar, kuruluşlardaki erişim güvenliğini artırır.

AI Mesh Data Classification

ÖZELLİK	AVANTAJ
Yapılandırılmamış veriler için AI Mesh sınıflandırması	Yapılandırılmamış veriler için yapay zeka ile son derece hassas sınıflandırma.
Özel model eğitimi	Kuruluşlar, son derece hassas veri sınıflandırması için AI Mesh modelini benzersiz veri ihtiyaçlarını (ör. IP, ticari sırlar vb.) karşılayacak şekilde uyarlayabilir, DSPM ve DLP yanlış pozitifleri/negatifleri azaltabilir.
Etiketleri Microsoft Purview IP etiketlemesine eşleştirebilir.	MIP etiketlerini birleştirerek ek sınıflandırma ayrıntılandırması katmanı sağlar. MIP etiketlemeyi düzeltebilir.
Veri etiketleme	Taranan ve sınıflandırılan tüm dosyaları, DLP tarafından okunabilen kalıcı etiketlerle standart etiketlemenin (gizli, çok gizli, herkese açık) yanı sıra, iş kataloglama/ etiketleme (İK, pazarlama, finans, devops - özgeçmişler, PO'lar vb. gibi alt etiketlerle) ile etiketler.
Forcepoint DLP ile entegre olur	Güçlü politikalar oluşturmak için dosyaların DSPM AI Mesh etiketlemesini (sınıflandırma) kullanmak üzere Forcepoint DLP ile entegre edilebilir.

Gerçek Zamanlı İzleme ve Veri Riski Değerlendirmesi

ÖZELLİK	AVANTAJ
Veri Riski Değerlendirmeleri (DRA)	Ücretsiz Veri Riski Değerlendirmeleri ile bir kurumun mevcut veri güvenliği duruşu birden fazla kategoride analiz edilebilir.
Ayrıntılı interaktif pano	Kapsamlı dosya ayrıntılarını tek bir ekranda görüntüleyin. Risk düzeyi, izinler ve konumlar (IP adresi, yol) gibi önemli dosya verilerinin detaylarına ulaşın.
Raporlama işlevi	Hem genel uyumluluğa hazırlığa hem de belirli gizlilik düzenlemelerine ilişkin raporlar oluşturun.
Gelişmiş uyarı sistemi	Herhangi bir anomaliye veya olası ihlale karşı taramalar sırasında bulunan sofistike veri kontrolleri ve uyarılar sağlar.
Veri Sahibi Erişim Talebi (DSAR) arama	Gizlilik düzenleme taleplerine hızlı bir şekilde uyun sağlamak için bir DSAR oluşturmayı basitleştirin.
Analiz paketi	Bir bakışta güvenlik ve sınıflandırma içgörülerine kolay erişim için gelişmiş bir analitik paketini kullanın. Çeşitli önceden tanımlanmış panolardan seçim yapın veya kendi panolarınızı oluşturun ve yalnızca bir tıkla PDF anlık görüntülerini zahmetsizce dışa aktarın. Önceden tanımlanmış paneller, riske aşırı maruz kalma ve fidye yazılımı analizi, kritik veri çoğaltma, riskli kullanıcı tespiti, veri tutma, yanlış yerleştirilmiş veriler, veri riski sorumluluğu, bağımsızlık ve veri kontrolü ihlalleri için olay takibini ve çok daha fazlasını içerir.
Fidye yazılımına maruz kalma analizi	Bir fidye yazılımı saldırısına maruz kalabilecek kritik verileri tanımlayın.
Kod içermeyen raporlar ve analiz oluşturucu	Kod yazma becerileri gerektirmeyen özel kullanım senaryolarını ve analiz raporlarını kolayca oluşturun.
Riskli kullanıcı tanımlanması	Önemli miktarlarda kritik bilgilere erişimi olan yüksek risk profillerine sahip kullanıcıları tanımlayın.
Veri kontrolü olayı	Tüm veri kontrolü ihlalleri ve olay çözümleme durumu hakkında net bir görünüm sağlar.