Forcepoint

Bilgi formu

Forcepoint Veri Tespiti ve Müdahalesi

En hassas bilgilerinizi korumak için sürekli tespit ve müdahale

Temel özellikler ve avantajlar:

- **Sürekli Tehdit Tespiti ve Müdahale:** Forcepoint DDR, güvenlik tehditlerini dinamik olarak tespit etmek ve bunlara müdahale etmek için veri hareketlerini sürekli olarak izler ve tehditleri önemli zararlar vermeden önce kısıtlamaya ve azaltmaya yardımcı olur.
- **Gelişmiş Veri Analizi ve Yapay Zeka Sınıflandırması:** Gelişmiş veri analizinden ve Forcepoint DSPM AI Mesh'ten yararlanan Forcepoint DDR, veri güvenlik açıklarını ve şüpheli faaliyetleri tespit ederek proaktif tehdit yönetimini mümkün kılar.
- **Kapsamlı Veri Görünürlüğü:** Forcepoint DDR, bulut ve uç nokta ortamlarında geniş kapsamlı görünürlük sunar ve potansiyel güvenlik açıklarının giderilmesini sağlayarak veri ihlallerini önler.
- **Gelişmiş Olay Soruşturması:** Bir dosyanın yaşam döngülerini izleyerek adli düzeyde ayrıntılar sağlayan Forcepoint DDR, güvenlik olaylarının soruşturulma sürecini geliştirerek daha doğru iyileştirme kararlarının alınmasına ve hatalı pozitiflerin azaltılmasına yardımcı olur.

Kuruluşlar, veri ihlallerindeki bulut bilişim ve yapay zeka teknolojilerinin hızla benimsenmesinden kaynaklanan endişe verici artışla mücadele etmektedir. Bu veri ihlalleri işletmeleri küresel ölçekte etkilemekte ve önemli finansal kayıplara ve itibar zararına yol açmaktadır. Buradaki zorluk, bu ihlalleri gerçekleşmeden önce tespit edip bunlara müdahale etme ve hassas verilerin korunmasını sağlama becerisi ile ilgilidir.

Forcepoint Veri Tespiti ve Müdahale (DDR)

GetVisibility destekli Forcepoint DDR, bu zorlukları gidermede kilit bir çözümdür. Sürekli tehdit tespiti ve gelişmiş veri riski görünürlüğü sağlayarak kuruluşların veri ihlallerine yol açabilecek veri değişikliklerini etkin bir şekilde görmelerini sağlar. Forcepoint DDR, yapay zeka destekli müdahalelerden yararlanarak tehditleri etkisiz hale getirme imkanı sunarak kuruluşların güçlü güvenlik önlemlerini sürdürmelerine yardımcı olur. Bulut ve uç noktalardaki geniş kapsamlı görünürlüğü, Veri geçmişi ile birlikte onu hassas bilgileri korumak, finansal kayıpları azaltmak ve müşteri güvenini sürdürmek için gerekli bir araç haline getirir.

Sürekli Tehdit Tespiti ve Yapay Zeka Destekli Müdahaleler

Forcepoint DDR, sürekli tehdit tespiti ve gelişmiş veri riski görünürlüğü sağlayarak kuruluşların tehditleri tanımlayabilmesini, izleyebilmesini ve bunlara müdahale edebilmesini sağlar. Forcepoint AI Mesh tarafından desteklenen müdahalelerden yararlanan Forcepoint DDR, tehditleri etkisiz hale getirmek için çalışır ve veri ihlallerine karşı güçlü bir savunma sağlar.

Bulutta ve Uç Noktalarda Kapsamlı Görünürlük

Forcepoint DDR, hem bulut hem de uç nokta ortamlarında geniş kapsamlı görünürlük sağlar. Bu kapsamlı görünürlük, kuruluşların veri sızıntısını önlemesine yardımcı olur ve potansiyel güvenlik açıklarının izlenmesini ve giderilmesini sağlar. Veri geçmişi takibinin dahil edilmesi, potansiyel ihlallerle doğru bir şekilde mücadele etme kabiliyetini daha da artırır.

Gelişmiş Verimlilik ve Maliyeti Düşürme

Forcepoint DDR, sürekli tehdit tespiti ve dinamik müdahaleler ile güvenlik ekiplerinin odaklanmasına olanak tanıyarak gerçekleşmekte olan potansiyel veri ihlallerini işaret eden veri ve izin değişikliklerine öncelik verilmesine yardımcı olur. Bu, verimliliği artırır ve maliyetleri düşürme, riskleri azaltma ve müşteri güvenini koruma gibi kurumsal hedefleri destekler.

Forcepoint DSPM'ye Önemli Ek Özellik

Şirketler veri yaklaşımlarını güvence altına almaya çalışırken, bulut ve şirket içi konumlardaki riskli verileri azaltan Forcepoint DDR, Forcepoint DSPM'ye sürekli risk görünürlüğü sağlar. Forcepoint DDR, önce veri konumları için eksiksiz bir keşif taraması yapmaya ihtiyaç duymak yerine, dağıtımdan hemen sonra veri güvenliği yaklaşımının sürekli olarak izlenmesini sağlar. Önceden keşif taramaları yapılmasa bile, Forcepoint DDR yeni veri risklerini ortaya çıktıkları anda tespit eder ve bunların giderilmesini sağlar. Bu, genel veri güvenliği duruşu için yeni riskleri sürekli olarak önler.

Forcepoint DDR, bu gelişmiş özellikleri entegre ederek yalnızca verileri korumakla kalmaz, aynı zamanda Üretken Yapay Zeka ve bulut bilişim çağında kuruluşların geleceğini de güvence altına alır.

ÖZELLİK	AVANTAJ
Sürekli Takip	Kuruluşların potansiyel tehditleri tespit etmesini ve bunlara müdahale etmesini sağlayan riskli veri hareketleri ile ilgili sürekli görünürlük elde edilmesini sağlar.
Otomatik Uyarılar	Tespit edilen veri riski tehditlerine göre uyarıları önceliklendirerek ve göndererek potansiyel veri ihlallerine müdahale süresini azaltır.
Veri Hareketi Tespiti	Verilerin izinli sınırlar içinde kalmasını sağlayarak fikri mülkiyeti ve hassas bilgileri korur.
Politika İhlali Uygulaması	Politika ihlallerini tespit ederek ve bildirerek veri koruma düzenlemelerine uyumluluğu sağlar.
Uyumluluk Araçları	Denetimleri ve uyumluluk raporlamasını kolaylaştırmak için sürekli izleme ve ayrıntılı veri geçmişleri sunarak yasal gerekliliklere uyumluluğu kolaylaştırır.
Proaktif Risk Yönetimi	Özelleştirilebilir yönetişim politikaları kullanarak kuruluş içinde risk oluşturan unsurlara yönelik uygulamaları tanımlar ve sağlar.
Aşırı Paylaşılan Dosya İzleme	Veri sızıntısı görünürlüğünü artırarak kötü niyetli bir olaylar zincirini veya kazara gerçekleşen ihlalleri ortaya çıkarır.
3. Taraf Güvenlik Aracı Entegrasyonu	SIEM ve SOAR çözümleri ile entegrasyon yoluyla olaylara müdahale ve tehdit yönetimi süreçlerini iyileştirir.
Bulut ve Uç Nokta Kapsamı	Veri ekosisteminde geniş bir görünürlük sağlayarak kuruluşların verilerini tamamen anlamalarına ve güvence altına almalarına olanak verir.
Ayrıntılı veri türü ve hassasiyet sınıflandırması	Veri bağlamının görünürlüğü sağlayarak güvenlik ekiplerinin riskleri değerlendirmesini ve bunlara etkili bir şekilde müdahale etmesini sağlar.
Yapay Zeka Sınıflandırması (AI Mesh)	Verimli ve yüksek düzeyde eğitilebilir olan üstün veri sınıflandırma doğruluğu sağlar.
Adli Tıp Özellikleri	Kapsamlı güvenlik olayları araştırması sayesinde iyileştirme doğruluğunu artırır ve hatalı pozitifleri azaltır.
Dinamik Olay Soruşturması	Olaylara müdahaleyi hızlandırarak güvenlik olaylarının etkisini azaltır ve kuruluşun genel güvenlik yaklaşımını sürekli olarak iyileştirir.
Veri Geçmişi Görünürlüğü	Yapılandırılmamış dosyaların geçmişinin ayrıntılı takibi yoluyla, kuruluşların verilerinin yaşam döngülerini tam olarak anlamalarını sağlar.

Forcepoint

forcepoint.com/contact