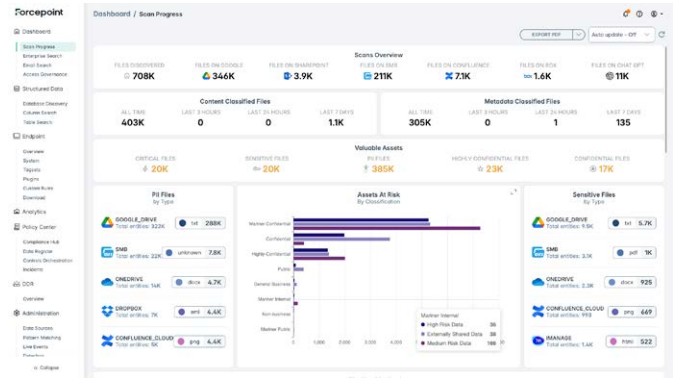


Görün. Koruyun. Basitleştirin.

Forcepoint Data Security Posture Management

Verilerinizle ilgili risklerin farkında mısınız?

Yapay zeka çağı, verilerin kullanılma, taşınma ve oluşturulma hızını hız artırıyor. Kuruluşlar, birden fazla bulut platformunda, şirket içi (on-premises) ortamlarda, jeneratif yapay zeka uygulamalarında ve ajan yapay zekada yaşanan veri dağınıklığına ayak uydurmakta zorlanıyor. Bu karmaşık ortam önemli zorluklar yaratıyor: Göremediğiniz şeyi koruyamazsınız. Birçok kuruluş, hassas verilerin nerede bulunduğu, kimlerin bu verilere erişebildiği ve verilerin nasıl kullanıldığı konusunda görünürlük ve kontrolden yoksun. Veri ihlalleri, özellikle sistemlerde kalan büyük miktarlardaki bilinmeyen “karanlık veri” (bir kuruluşun verilerinin %80’ine kadar) nedeniyle önemli bir tehdit oluşturuyor. Ayrıca, veri gizliliği düzenlemeleri giderek daha katı hale geliyor. Kuruluşların para cezalarından ve itibar kaybından kaçınmak için uyumluluğu gösterebilmesi gerekiyor.



Forcepoint Data Security Posture Management (DSPM): Veri Riskine Karşı Çözümünüz

Forcepoint DSPM bu zorlukların üstesinden gelir ve veri güvenliği duruşunuzu kontrol etmenizi sağlar. Yapay zeka sistemleri sorunları büyütmeden ve saldırganlar bunları istismar etmeden önce, karanlık veriyle ilişkili güvenlik risklerini belirlemenize ve gidermenize olanak tanıyan proaktif veri riski keşfi ve giderimi sunar. Yapay Zeka Ağı ve Jeneratif Yapay Zeka Küçük Dil Modeli (SLM) gibi en son yeniliklerden yararlanan Forcepoint DSPM, kuruluşlara üstün kapsama alanı ve veri sınıflandırma doğruluğu sağlar. Forcepoint DSPM şunları yapmanızı sağlar:

- Güvenlik politikalarını daha doğru ve verimli bir şekilde tanımlamak ve otomatikleştirmek için verileri anlayın ve kategorize edin.
- Basitleştirilmiş veri erişim yönetimiyle veri sahipliği ve konumu hakkında net bir görünürlük kazanın, böylece uygun erişim izinlerinin verilme sürecini hızlandırın.
- DSPM’yi belirli sektörlere, düzenleyici gereksinimlere ve kullanıcı tercihlerine uyarlayarak uyumluluğu kolaylaştırın; böylece kuruluşlar gizlilik düzenlemelerine daha iyi uyum sağlayabilir. Ayarlanabilir hassasiyet ayarları ve kullanıcıya özel dedektörler, hassas veri işlemeyi mümkün kılarak uyumluluk risklerini azaltır.
- Veri güvenliği risklerini proaktif olarak belirleyerek maliyetli veri ihlali riskini azaltın.

Forcepoint DSPM, yapay zeka sistemleri riskleri büyütmeden ve saldırganlar bunları istismar etmeden önce veri güvenliği risklerini belirleyip gidererek veri güvenliğinizi güçlendirir. Uyumluluk raporlamasını basitleştirerek uyumluluk maliyetlerini azaltır ve veri gizliliği ihlalleriyle ilişkili para cezalarından kaçınmanıza yardımcı olur. Diğer DSPM çözümlerinin aksine, jeneratif yapay zeka, makine öğrenimi ve Forcepoint’in sektörün en iyi veri sınıflandırıcılarını kullanarak son derece doğru ve verimli veri sınıflandırması sağlamak için tam içerik incelemesi sunar.

Forcepoint DSPM’in eksiksiz veri güvenliği elde etmenize nasıl yardımcı olabileceği hakkında daha fazla bilgi edinmek için bugün bizimle iletişime geçin.