

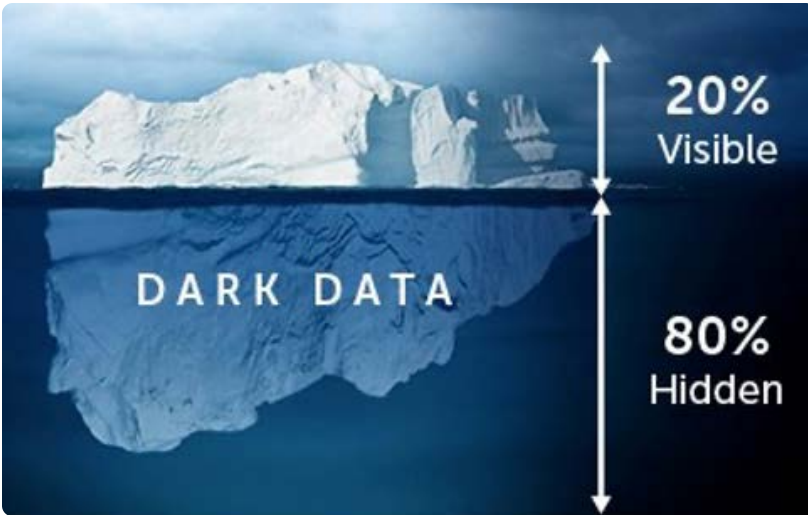
Forcepoint DSPM



Yapay Zeka Dönüşümü, Dijital Dönüşümün Bir Sonraki Aşamasıdır

Yeni dönemde verileriniz güvende mi?

Sektörler genelinde kuruluşlar, üretkenliği büyük ölçüde artıracığı vaadiyle ortaya çıkan yapay zeka dönüşümüyle mücadele ediyor. Yapay zekanın güçlendirdiği bu çağ; kurumsal yapay zeka hizmetlerini devreye almaya yönelik girişimler, izinsiz yapay zeka kullanımının yönetilmesi ve ajan yapay zeka etkinliğiyle ilişkili risklerin azaltılmasıyla öne çıkıyor. Genel olarak bu çabaların temelinde yatan öncelik, hassas verilerin nasıl kullanıldığına dair görünürlük ve kontrol sağlamaktır. Ancak neredeyse her kuruluş, verileri üzerinde ölçekte tutarlı bir görünürlük elde etmekte, kontrolü sağlamak bir yana, zorlanıyor. Bu durum, yüzeyde yalnızca küçük bir kısmını gördüğümüz, büyük çoğunluğu ise yüzeyin altında fark edilmeden kalan bir buzdağına benzetilebilir. Genellikle "karanlık veri" (dark data) olarak adlandırılan bu veriler görünmez ve bilinmez durumda kalır; ancak kuruluşun doğrudan sorumlu olduğu önemli miktarda hassas bilgi içerir. Kuruluşlar artık kullanıcıların yapay zekadan güvenli bir şekilde yararlanmasını sağlarken hassas verilerinin korunmasını nasıl güvence altına alacaklarını çözmeye çalışıyor; ancak yapay zeka kullanımının kendisi, benzeri görülmemiş bir hızla daha fazla veri oluşturulmasına yardımcı olarak sorunu daha da kötüleştiriyor.



Data Security Posture Management (DSPM), bilgilerinizi yetkisiz erişime, ifşaya, değişikliğe veya veri imhasına karşı korumak için kapsamlı bir yaklaşım sunar. Belirli uygulamalara ve cihazlara odaklanan diğer veri güvenliği yöntemlerinin aksine DSPM, ister bulutta ister özel ağlarda olsun, bir kuruluşun verilerinin tamamını görebilir ve kontrol edebilir; böylece uyumluluğu sağlar ve veri ihlali riskini azaltır.



Yapay zekayla ilişkili bir ihlal bildiren ve uygun yapay zeka erişim kontrollerinden yoksun olan kuruluşların oranı¹.



Güvenlik operasyonlarında yapay zekanın yoğun kullanımından kaynaklanan maliyet tasarrufu. Yapay zeka ve otomasyonu yoğun şekilde kullanan güvenlik ekipleri, bu çözümleri kullanmayanlara kıyasla ihlal sürelerini 65 gün kısalttı ve ortalama maliyetlerini 1,93 milyon ABD doları düşürdü².



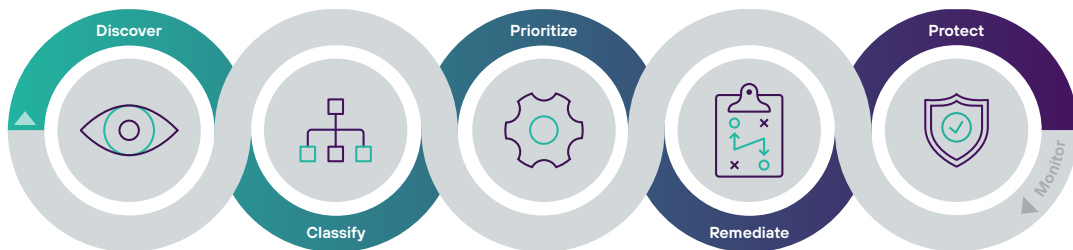
AT&T, 2024 yılında yaşanan iki veri ihlaline bağlı bir toplu davayı 177 milyon dolar karşılığında sonuçlandırmayı kabul etti. İlk ihalde, 73 milyon mevcut ve eski müşteriye ait Sosyal Güvenlik numaraları dahil veriler ifşa oldu; ikinci ihalde ise yeterli izleme olmadan bulut ortamında barındırılan, hassas müşteri bilgileri içeren bir çalışma alanına yetkisiz erişim gerçekleşti².

¹ IBM's Cost of a Data Breach Report 2026
² Top Class Actions AT&T veri ihlali toplu dava anlaşması

DSPM neyi ele alır?

- **Yapay Zeka dönüşüm yolculuğu:** Gelişmiş AI Mesh (Yapay Zeka Ağı) teknolojiğimizle verilerinizi her yerde koruyarak Forcepoint DSPM ile yapay zekanın gücünü serbest bırakın. Forcepoint DSPM'in sunduğu merkezi görünürlük ve düzeltme yetenekleri ile Forcepoint DLP'nin gerçek zamanlı engelleme kontrolleri sayesinde, ChatGPT, Copilot, Gemini ve diğer birçok üretken yapay zeka uygulaması dahil olmak üzere, en önemli kanalların tamamında hassas bilgilerinizi koruyor; yenilikçi çalışmaları desteklerken üretkenliği artırıyor ve riski azaltıyoruz.
- **Hassas verilerin belirlenmesi:** DSPM, yapılandırılmış ve yapılandırılmamış veriler dahil, birden fazla bulut ortamı ve hizmetinin yanı sıra kurum içi konumlarda yer alan hassas verileri belirlemelerine yardımcı olur. Buna hassas verilerin nerede bulunduğunu, bu verilere nasıl erişildiğini ve kimlerin bu verilere erişim iznine sahip olduğunu anlamak da dahildir.
- **Güvenlik açığı ve risk değerlendirmesi:** DSPM, hassas verilerin güvenlik tehditlerine karşı savunmasızlığını ve mevzuata uyumsuzluk konusundaki riski değerlendirir. Kuruluşlar, verilerin güvenlik duruşunu analiz ederek potansiyel riskleri proaktif olarak ele alabilirler.
- **Verilere kaynağında odaklanma:** Öncelikle cihazları, sistemleri ve uygulamaları güvence altına alan diğer veri güvenliği araçlarının aksine, DSPM doğrudan kuruluşun verilerinin tamamını korumaya odaklanır. Veri ihlallerini önlemeyi ve verileri kaynağında güvence altına alarak uyumluluğun sağlanmasını hedefler.
- **Karanlık ve gereksiz, eski ve önemsiz (ROT) verilerin ele alınması:** DSPM doğrudan karanlık verileri ele alır (halihazırda normal iş süreçlerinde görülmeyen veya kullanılmayan veriler). Benzer şekilde DSPM, şirketlerin çeşitli nedenlerle ve uyumluluklarını sürdürmelerine yardımcı olacağını düşünerek büyük miktarda veriyi muhafaza etmeye devam etmeleri nedeniyle kuruluşlar genelinde çoğalma eğiliminde olan ROT (gereksiz, modası geçmiş ve önemsiz) verileri de ele alabilir. Bu durum aslında daha da büyük bir veri riski yaratır ve DSPM bu riski yönetmenize de yardımcı olur.
- **Gereğinden fazla erişim izni verilen/paylaşılmış verilerin belirlenmesi:** Verilerin yeni versiyonlarının kopyalanması ve düzenlenmesi yoluyla çoğalması nedeniyle, verilere yönelik izinler de genellikle kullanıcılara, gruplara ve hatta kuruluşun tamamına yayılabilir. DSPM, veri ihlallerini önlemenin bir yolu olarak gereğinden fazla erişim izni verilen verileri önemli ölçüde azaltan "en az ayrıcalık ilkesi" Zero Trust anlayışının uygulanmasını sağlar.
- **Çoklu-bulut ve hibrit bulut ortamları:** Kuruluşlar çoklu bulut ve hibrit bulut ortamlarını benimsedikçe, veri ihlalleri riskleri önemli ölçüde artmaktadır. DSPM, şirket içi ortamlara ek olarak, farklı bilgi işlem ortamlarında bulunan hassas veriler üzerinde de görünürlük ve kontrol sağlar.
- **Sürekli risk izleme:** Forcepoint Data Detection and Response (DDR) eklentisi, Forcepoint DSPM'nin yeni veri risklerini ortaya çıktıkları anda tespit etmesini ve gidermesini sağlar. Bir sonraki eksiksiz DSPM taramasını beklemeye gerek kalmadan, veri güvenliği duruşunuzla ilgili riskleri dinamik olarak belirleyip ortadan kaldırın.

Forcepoint DSPM, hassas verileri için güçlü görünürlük ve kontrol gerektiren modern kuruluş için tasarlanmıştır. Veri ihlallerinin önlenmesi ve gizlilik mevzuatına uyumsuzluk riskinin azaltılması için çeşitli bulut ortamlarında ve sunucularında görünürlük sağlar. Forcepoint, veri yaşam döngüsü boyunca tam görünürlük ve kontrol sağlayarak Her Yerde Veri Güvenliği sunar. **Proaktif veri riski keşfi** (DSPM) ile verilerin nasıl kullanıldığına yönelik **aktif kontrolleri** (DLP) birleştirir ve **her kullanıcının davranışlarına sürekli uyum sağlayarak** (Risk-Adaptive Protection) güçlü ve dinamik bir veri güvenliği sunar. Veri ihlallerini önlemek ve veri güvenliği duruşunuzu için sürekli izleme (Forcepoint DDR) ile veri risklerinin dinamik olarak keşfedilmesini sağlar.



Yapay zeka destekli keşif, sınıflandırma ve yönetim

Forcepoint DSPM ile veri tabanınız üzerindeki görünürlüğü ve kontrolü birleştirin

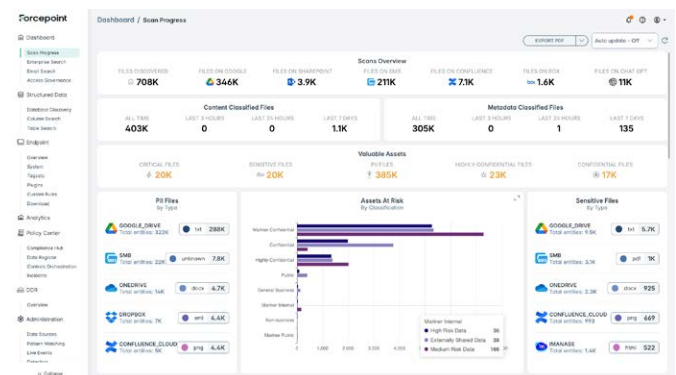
Kuruluşunuzun verilerini yönetmek ve güvence altına almak hiç bu kadar karmaşık olmamıştı. Forcepoint DSPM, konumdan bağımsız olarak verileriniz üzerinde kapsamlı görünürlük ve kontrol elde etmenizi sağlayan güçlü bir çözüm sunar. Forcepoint'in YZ Ağı ve gelişmiş DLP sınıflandırıcıları tarafından desteklenen tam içerik incelemesini kullanan, sektör lideri veri sınıflandırması sayesinde Forcepoint DSPM, veri güvenliği duruşunuz hakkında bilinçli kararlar almanızı ve olası riskleri proaktif şekilde ele almanızı sağlar.

Forcepoint DSPM'nin başlıca avantajları şunlardır:

Hızlı ve kapsamlı keşif: Forcepoint DSPM, basit meta veri etiketleme veya yalnızca örnekleme yaklaşımlarına dayanmak yerine tam içerik incelemesi gerçekleştirerek çoklu bulut ve şirket içi ortamlarda dosyaların ve veritabanlarının hızlı, yüksek performanslı taranmasını sağlar. Bu analiz derinliği, hassas verilerin yalnızca tahmin edilmesini değil, doğru şekilde tespit edilmesini sağlar. Forcepoint'in yüksek performanslı keşif ve sınıflandırma özellikleri; ChatGPT Enterprise, Anthropic Claude ve Microsoft Copilot gibi üretken yapay zeka platformlarında bulunan veriler de dahil olmak üzere yapılandırılmış ve yapılandırılmamış depoları kapsayacak şekilde, kuruluşların veri ortamları üzerinde ölçekte hızlı ve kapsamlı görünürlük kazanmasını sağlayarak güvenlik ekiplerinin yapay zeka kaynaklı ortaya çıkan veri maruziyeti risklerinin önünde kalmasına yardımcı olur.

Yapay Zeka Ağı ile sağlanan doğruluk: Forcepoint Forcepoint DSPM, bulut ve ağ kaynakları genelinde verileri keşfeder ve gelişmiş bir yapay zeka sınıflandırma motoru kullanarak bu verileri otomatik olarak sınıflandırır. Forcepoint DSPM'nin Yapay Zeka Ağı, kuruluşlara üstün veri sınıflandırma doğruluğu sunar. Bir GenAI Küçük Dil Modeli'nden (SLM) ve

Forcepoint'in uzun süredir güvenilen, özenle seçilmiş DLP sınıflandırıcılarından yararlanan ağa bağlı yapay zeka mimarisi, yapılandırılmamış metinden bağlamı verimli bir şekilde yakalar. Özelleştirilebilir ve verimli olan bu yapı, kapsamlı eğitime gerek kalmadan hızlı ve doğru sınıflandırma sağlayarak güveni ve uyumluluğu artırır. Sonuç olarak bu yüksek doğruluk, diğer popüler sınıflandırma yöntemleriyle sorun yaşayan kuruluşların yanlış pozitif/negatif oranlarını büyük ölçüde azaltmasına, fikri mülkiyetlerini başarıyla korumasına ve zaman ile kaynaklardan büyük ölçüde tasarruf etmesine olanak sağladı.



Veri ortamınızda görünürlük: Forcepoint DSPM, tüm dosyalar ve kullanıcılar için izinleri denetlemenizi sağlar. Veri yöneticileri, kuruluş genelindeki dosya ve veritabanlarına hangi kişilerin erişimi olduğunu görebilir. Tek bir tıkla, taranan tüm dosyalar için verilmiş erişim izinlerini anında görüntüleyebilirsiniz. Forcepoint DSPM, gizli verilere dair kuş bakışı bir görünüm sağlayan, kapsamlı ayrıntılara sahip bir panonun yanı sıra en yüksek veri riski taşıyan alanları anlamanıza yardımcı olmak için genel bir veri riski değerlendirmesi sağlar.

İş akışı yönetimi: Paydaşlar arasında uyum sağlama sürecini kolaylaştırmak üzere farklı veri setleri için sahiplik ve sorumluluk tanımlarını kolayca yapın. Böylece her bir veri kaynağı ve varlık üzerinde gerçekleştirilen eylemler etrafında daha verimli iş akışları sağlanır. Başarılı bir iyileştirme, güvenlik organizasyonunun ötesine geçerek CDO/Yönetişim, Risk ve Uyumluluk grubunun yanı sıra pazarlama, finans, DevOps ve diğer birçok birimi de

kapsayan geniş bir katılım ve işbirliği gerektirir. Forcepoint DSPM, veri duruşunu güvenceye almayı sadece bir güvenlik sorunu olarak değil, bir işletme önceliği olarak ele alır.

Forcepoint DDR: Forcepoint DSPM için güçlü bir eklenti ve veri ihlallerini ele almada kilit bir çözümdür. Sürekli tehdit tespiti ve gelişmiş veri riski görünürlüğü sağlayarak kuruluşların veri ihlallerine yol açabilecek veri değişikliklerini henüz gerçekleşme aşamasındayken etkin bir şekilde görmelerini sağlar. Forcepoint DDR, yapay zeka destekli müdahalelerden yararlanarak tehditleri kusursuz bir şekilde etkisiz hale getirme imkanı sunarak kuruluşların güçlü güvenlik önlemlerini sürdürmelerine yardımcı olur. Bulut ve uç noktalarda sağladığı geniş kapsamlı görünürlük, veri geçmişi ile birlikte onu hassas bilgileri korumak, finansal kayıpları azaltmak ve müşteri güvenliğini sürdürmek için gerekli bir araç haline getirir.



Verilerin işinizi felce uğratmasına izin vermeyin. Forcepoint size yardım edebilir!

Günümüzün dijital çağında veri, bir kuruluşun en değerli varlığıdır; ancak doğru yönetilmediği takdirde önemli bir risk unsuru da olabilir. Forcepoint DSPM; hassas verilerinizi korumak, veri ihlali risklerini azaltmak ve mevzuat uyumluluğunu sağlamak için proaktif bir yaklaşım sunar. Forcepoint DSPM'i hayata geçirerek veri ortamınızda kapsamlı bir görünürlük elde edebilir, güvenlik açıklarını tespit edip giderebilir ve GenAI uygulamalarındaki verilerinizi güvence altına alırken; veri ihlalleri ile mevzuata uyumsuzluktan kaynaklanan finansal ve itibar zararlarına karşı kuruluşunuzu proaktif bir şekilde koruyabilirsiniz. Veri güvenliği duruşunuzun kontrolünü bugün elinize alın. DSPM'in değerli bilgilerinizi nasıl koruyabileceğini keşfetmeye başlayın. Demo talebinde bulunmak için www.forcepoint.com/tr/dspm adresini ziyaret edin.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint; kuruluşların ve devlet kurumlarının verilerini her yerde bilmesine, riskler ve düzenlemelere gerçek zamanlı olarak uyum sağlamasına ve birleşik, tek politikalı bir çerçeveye ölçekte koruma sağlamasına yardımcı olan yapay zeka-doğal bir yaklaşım olan Self-Aware Data Security'yi mümkün kılar. Austin, Teksas merkezli Forcepoint; 150'den fazla ülkede müşterileri ve çalışanları için güvenli, güvenilir ortamlar oluşturur. Forcepoint ile www.forcepoint.com, [LinkedIn](#), [Instagram](#) ve [YouTube](#) üzerinden etkileşime geçin.