

Forcepoint DSPM

GetVisibility tarafından
desteklenmektedir



Forcepoint

Broşür

Yapay Zeka Dönüşümü, Dijital Dönüşümün Bir Sonraki Aşamasıdır

Yeni dönemde verileriniz güvende mi?

Dijital dönüşüm geçiren çoğu kuruluş, bir sonraki aşama olan yapay zeka dönüşümü için hazırlanmaktadır. Yapay zekada bu yeni dönem; ChatGPT, Copilot ve Gemini gibi üretken yapay zeka uygulamalarının sunduğu birçok avantajla şekillenir. Kuruluşlar, dijital dönüşüm deneyimlerinden yola çıkarak, veri güvenliğinin en önemli önceliklerinden biri olması gerektiğini öğrenmektedir. Bununla birlikte, günümüzde birçok kuruluş için veriler, büyük bir kısmı suyun altında kalan dev bir buz dağı gibi görünür. Genellikle "karanlık veriler" veya "gölge veriler" olarak adlandırılan bu veriler görünmez ve gizemini korur ancak kuruluşların doğrudan sorumluluk sahibi olduğu, önemli miktarda hassas bilgi içerir. Artık kuruluşlar, bir yandan hassas verilerini korurken diğer yandan kullanıcılarının verimliliği ve üretkenliği artırmak amacıyla üretken yapay zeka uygulamalarından güvenle yararlanmasını sağlama üzerine çalışmaktadır.



DSPM (Data Security Posture Management), bilgilerinizi yetkisiz erişime, ifşaya, değiştirilmeye veya veri imhasına karşı güvence altına almak için kapsamlı bir yaklaşım sunar. Sistemlere ve cihazlara odaklanan diğer veri güvenliği yöntemlerinin aksine DSPM, bir kuruluşun verilerinin tamamına odaklanarak uyumluluğu sağlar ve veri ihlali riskini azaltır.



IDC'ye göre, küresel ölçekte verilerin %80'i yapılandırılmamış halde ve bu verilerin %90'ı da analiz edilmemiş durumda; bu nedenle "karanlık veri" olarak adlandırılıyor.¹



Şirketlerin %94'ü verilerini çoklu bulut ortamlarında saklıyor.²



Equifax, bilgisayar korsanlarının çalışanlara ait kullanıcı adları ve şifrelerin birden fazla kopyasını depolayan ortak bir sürücüyü erişmesiyle daha da kötüleşen veri ihlali³ için açılan dava sonucunda 1,4 milyar dolarlık bir tazminata razı oldu. Şirket, gereksiz ve eski dosyaları tespit etmeyi ve tespit etmeyi sağlayacak araçlardan yoksundu.

¹ The Unseen Data Conundrum, Forbes, Şubat 2022

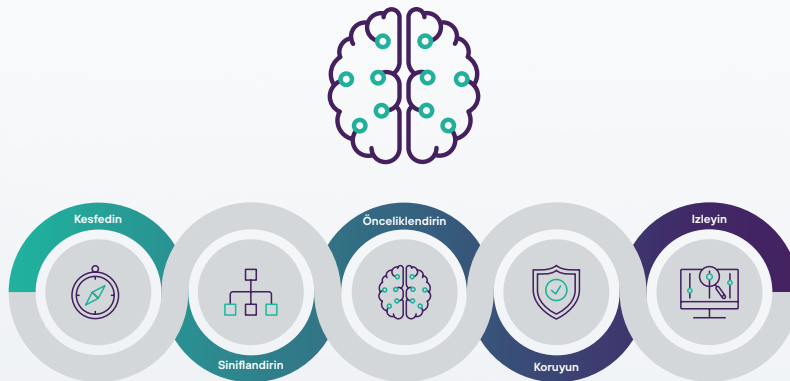
² Dark Data: The Cloud's Unknown Security and Privacy Risk, Forbes, Haziran 2023

³ Equifax agrees \$1.38bn data breach lawsuit settlement, Finextra, Ocak 2020

DSPM neyi ele alır?

- **Yapay zekanın dönüşüm yolculuğu:** Forcepoint DSPM ile yapay zekanın potansiyelini açığa çıkarın ve gelişmiş AI Mesh teknolojimizle verilerinizi her yerde koruyun. Forcepoint DSPM'nin sunduğu merkezi görünürlük ve denetim imkanı sayesinde hassas bilgilerinizi birçok temel kanalda koruyarak üretkenliği artırıyor, riski azaltıyor ve önemli yeniliklere imza atıyoruz. Bu kanallar arasında ChatGPT, Copilot ve Gemini gibi üretken yapay zeka uygulamaları yer alıyor.
- **Hassas verileri belirleme:** DSPM, kuruluşların çeşitli bulut ortamları ve hizmetlerinin yanı sıra şirket içindeki hassas verileri de belirlemelerine yardımcı olur. Hassas verilerin bulunduğu yerleri, bu verilere nasıl erişildiğini ve kimlerin bu verilerle etkileşim kurma iznine sahip olduğunu anlamak da buna dahildir.
- **Güvenlik açığı ve risk değerlendirme:** 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.

Forcepoint DSPM, iş verilerinin görünürlüğünü ve kontrolünü güçlendirmeye ihtiyaç duyan modern organizasyonlar 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, **veri riskinin proaktif keşfini** (DSPM) **verilerin nasıl kullanıldığına** dair aktif **kontrollerle** (DLP ve SSE) birleştirir ve **her kullanıcının eylemlerine göre sürekli olarak uyarlanır** (Risk-Adaptive Protection).



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 verilerinizin üzerinde geniş bir görünürlük ve kontrol elde etmek için güçlü bir çözüm sunar. Endüstri lideri keşif hızları ve gelişmiş AI Mesh destekli veri sınıflandırma özellikleriyle Forcepoint DSPM, veri güvenliğiyle ilgili duruşunuz hakkında bilinçli kararlar almanıza ve olası riskleri proaktif olarak ortadan kaldırmanıza yardımcı olur.

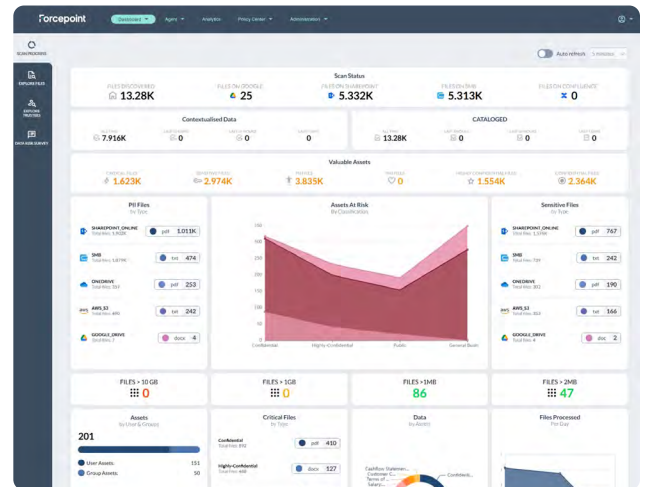
Forcepoint DSPM'nin sunduğu en önemli avantajlar şunlardır:

Hızlı, kapsamlı keşif: Birden fazla bulut ortamında ve on-prem Forcepoint DSPM, saatte yaklaşık 1 milyon dosyaya karşılık gelecek kadar dosyayı hızlı bir şekilde tarayabilir. Kuruluşların terabaytlarca ve hatta bazılarının petabaytlarca veriden sorumlu olması hiç de nadir değildir. Bu yüksek performanslı keşif sayesinde Forcepoint, kuruluşların ChatGPT Enterprise da dahil olmak üzere devasa bir veri ortamındaki verilere ilişkin hızlı bir görünüm elde etmelerini sağlar. Diğer DSPM sağlayıcılarından farklı olarak, Forcepoint keşif çalışmaları için ücret talep etmez. Müşteriler ek ücret olmadan istedikleri sıklıkta keşif gerçekleştirebilir.

AI Mesh destekli doğruluk: Forcepoint DSPM, bulut ve ağ kaynakları genelinde verileri keşfeder ve gelişmiş bir yapay zeka sınıflandırma motorundan yararlanarak otomatik olarak sınıflandırır. 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 bağlamsal 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. Sonuç olarak, bu derece hassas bir doğruluk, diğer popüler sınıflandırma yöntemlerinde sorun yaşayan kuruluşların yanlış pozitifleri/negatifleri önemli ölçüde azaltmasını, fikri mülkiyetlerini başarılı bir şekilde korumasını ve zaman ve kaynak açısından önemli tasarruflar etmesini sağlamaktadır.

Veri ortamınız genelinde veri görünürlüğü:

Forcepoint DSPM, tüm dosyalar ve kullanıcılar için erişim izinlerini denetlemenizi sağlar. Veri yöneticileri, kuruluş genelinde hangi kişilerin bir dosyaya veya dosya paylaşımlarına erişimi olduğunu görebilir. Tek bir tıkla, taranan tüm dosyalar için verilmiş erişim izinlerini anında görüntüleyebilirsiniz. Forcepoint DSPM, karanlık verilere kuş bakışı bir görünüm sağlayan geniş kapsamlı ayrıntılar içeren bir gösterge panosunun yanı sıra gerçek zamanlı raporlar sunar ve en yüksek riskli veri alanlarını belirlemenize 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/DataOps 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 görür.



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

Günümüzün dijital dünyasında bir kurumun en değerli varlığı olan veri, doğru yönetilmediği takdirde önemli bir sorumluluğu da beraberinde getirebilir. Forcepoint DSPM, hassas verilerinizi güvence altına almak, veri ihlali risklerini azaltmak ve mevzuata uyumluluğu sağlamak için proaktif bir yaklaşım sunar. Forcepoint DSPM'yi uyguladığınızda; veri tabanınız üzerinde kapsamlı bir görünürlük elde edebilir, güvenlik açıklarını tespit edip ele alabilir ve veri ihlalleri ile mevzuata uyumsuzluktan kaynaklanan finansal ve itibara yönelik zararları proaktif olarak önleyebilirsiniz. Üstelik bunu, üretken yapay zeka uygulamalarında verilerinizi korurken yapabilirsiniz. Veri güvenliği duruşunuzun kontrolünü bugün elinize alın. DSPM'nin değerli bilgilerinizi nasıl koruyabileceğini keşfetmeye başlayın. Demo talebinde bulunmak veya bir güvenlik mühendisinden şu anda ne tür veri riskleriyle karşı karşıya olduğunuzu görmek üzere kendi verilerinizden örnek bir çalışma alabileceğiniz ücretsiz bir veri riski değerlendirmesine kaydolmak için www.forcepoint.com/tr/dspm adresine gidin.

Forcepoint

forcepoint.com/contact

Forcepoint Hakkında

Forcepoint, küresel işletmeler ve hükümetler için güvenliği kolaylaştırır. Forcepoint'in her şey dahil, gerçek anlamda bulut tabanlı platformu, Zero Trust'i benimsemenizi ve kullanıcılar nerede çalışıyor olursa olsun hassas verilerin ve fikri mülkiyetin çalınmasını veya kaybolmasını önlemenizi kolaylaştırır. Merkezi Austin, Teksas'ta bulunan Forcepoint, 150'den fazla ülkede müşterileri ve çalışanları için emniyetli ve güvenilir ortamlar yaratmaktadır. Forcepoint ile www.forcepoint.com, Twitter ve LinkedIn üzerinden etkileşime geçin.