Forcepoint Data Loss Prevention

Sınırları olmayan bir dünyada veri koruması

Forcepoint

Broşür

forcepoint.com/tr

Forcepoint Data Loss Protection (DLP)

Yapay Zeka Dönüşümünüzü Forcepoint ile Güvence Altına Alın

Dünya genelinde kuruluşlar, yapay zekanın ve özellikle Üretken Yapay Zeka teknolojisinin iş süreçlerine entegrasyonu ile desteklenen dönüştürücü bir yolculuğa çıkıyor. Bu dönüşüm bir yandan çalışma verimliliğinde önemli artışlar vaat ederken, diğer yandan yeni veri güvenliği zorluklarını da beraberinde getiriyor. Örneğin, kullanıcılar Üretken Yapay Zeka uygulamalarına hassas verileri girebilir veya gizli dosyaları yükleyebilir; bu da veri ihlallerinin gerçekleşmesini kolaylaştırabilir. Forcepoint, en değerli varlığınız olan verilerinizden ödün vermeden yapay zekanın potansiyelini kullanmanıza olanak tanıyan bir çözüm sunuyor.

Üstün AI Mesh teknolojimiz sayesinde Forcepoint, benzersiz veri sınıflandırma doğruluğu ve verimlilik sağlar. Bu, yapay zeka dönüşümündeki zorluklarla baş etmede size güven ve güç kazandırır. ChatGPT, Copilot, Gemini veya benzeri Üretken Yapay Zeka uygulamalarını kullanırken, Forcepoint merkezi görünürlük ve kontrol sağlayarak hassas verilerinizi tüm ortamlarda korur.

Çalışanlarınızın ve Verilerinizin Bulunduğu Her Yerde Veri Güvenliği

Forcepoint DLP, her ölçekteki kuruluşun karşılaştığı kritik veri güvenliği sorunlarını ele alır. Mevzuat koşulları sıkılaştıkça, Kişisel Tanımlayıcı Bilgiler (PII) ve Korunan Sağlık Bilgileri (PHI) gibi hassas bilgilerin korunması son derece önemli hale geliyor. Bulut yazılımları, hibrit kurulumlar ve BYOD trendleri de dahil, modern çalışma ortamları verilerin korunmasını daha da zorlaştırıyor.

Genişleyen saldırıya açık alan, kapsamlı görünürlük ve kontrol gerektiriyor. Forcepoint DLP, uç noktalar, ağlar, bulut, web, özel uygulamalar ve e-posta gibi başlıca kanallardaki küresel politikaları yöneterek veri güvenliği ekiplerine güç katar. Önceden tanımlanmış şablonlarımız ve sınıflandırıcılarımız olay yönetimini kolaylaştırarak riskleri en aza indirirken verimliliğe odaklanmanızı sağlar. Çalışanlarınızın ve verilerinizin bulunduğu her yerde, Forcepoint DLP görünürlük ve kontrol sağlar.

Veri koruması:

- **Çalışanlarınızın verileri oluşturmak,** depolamak ve taşımak için kullandığı tüm uygulamalara yönelik tek bir kontrol noktası ile düzenlenmiş verileri güvenceye almalıdır.
- **Insanların verileri nasıl kullandığını analiz eden**, çalışanlarınıza verilerle doğru kararlar almaları konusunda rehberlik eden ve olayları riske göre önceliklendiren gelişmiş DLP ile hassas verileri koruyun.
- Uç noktadan web'e ve buluta kadar tüm konumlarda ve uygulamalarda kullanımını korumak için güçlü DLP kontrolleri ve politikaları uygulayarak **üretken yapay zekanın güvenli bir şekilde kullanılmasını sağlayın.**

Uyumluluğu Kolaylaştırın

Verileri korumak için çalışanlara yetki vermek

Gelişmiş Tespit ve Kontrol

Riske Müdahale Etmek ve Riski Gidermek

Üretken Yapay Zeka uygulamalarını güvenle kullanın

Uyumluluğu kolaylaştırın

Modern bilişim ortamı, onlarca küresel veri güvenliği düzenlemesine uymayı amaçlayan işletmeler için, özellikle de bulut uygulamalarına ve mobil iş gücüne geçiş aşamasında ürkütücü bir zorluk olarak ortaya çıkmaktadır. Pek çok güvenlik çözümü, CASB ve SWG uygulamalarında olduğu gibi bir tür tümleşik DLP içerir.

Ancak güvenlik ekipleri, ayrı ve tutarsız DLP politikalarını uç noktalar, bulut uygulamaları ve web trafiği genelinde uygularken ve yönetirken istenmeyen karmaşıklık ve ek maliyetlerle karşı karşıya kalmaktadır. Forcepoint DLP, diğer tüm büyük tedarikçilerden daha fazla sayıda kullanıma hazır sınıflandırıcı, politika ve şablon sunarak uyumluluk çabalarınızı hızlandırır. Bu, ilk DLP kurulumunu hızlandırır ve devam eden DLP yönetimini basitleştirir..

- → 90 ülke ve 160'tan fazla bölgenin mevzuat taleplerine uygun 1700'den fazla önceden tanımlanmış şablon, politika ve sınıflandırıcıyla uyumluluğu kolayca karşılamak ve sürdürmek için **kapsamı düzenleyin.**
- → Bulut uygulamaları, web, e-posta ve uç noktalar dahil olmak üzere tüm kanallarda **merkezi kontrol** ve tutarlı politikalar.

Verileri korumak için çalışanlara yetki vermek

Sadece önleyici kontrollere sahip DLP, bunları sadece bir görevi tamamlamak amacıyla aşmaya çalışacak kişileri caydırır. Güvenliği pas geçmek, gereksiz risklere ve kasıtsız veri maruziyetine neden olur.

Forcepoint DLP, çalışanlarınızı günümüz siber tehditlerinin ön safları gibi görmektedir.s.

- → Bulut uygulamaları, web trafiği, e-posta veya uç noktalar olsun, bulunduğu her yerde **verileri keşfedin ve kontrol edin.**
- → Kullanıcı eylemlerini yönlendiren, çalışanları politika konusunda eğiten ve kritik verilerle etkileşime giren kullanıcının niyetini doğrulayan özel mesajları kullanarak **çalışanları akıllı kararlar almaya hazırlayın.**
- → **Kuruluşunuzun dışına çıkan verileri** koruyan politika tabanlı otomatik şifreleme yöntemini kullanarak güvenilir iş ortakları ile güvenli işbirliği yapın.
- → **Veri etiketlemeyi ve sınıflandırmayı otomatikleştirmek için:** Forcepoint Data Classification ve Microsoft Purview Information Protection uygulamalarıyla entegre edin.

Gelişmiş tespit ve verileri takip eden kontroller

Kötü niyetli ve kasıtlı olmayan veri ihlalleri münferit olaylar değil karmaşık olaylardır. Forcepoint DLP; Forrester, Radicati Group ve Frost & Sullivan tarafından DLP çözümleri için endüstri lideri olarak tanınmaktadır. Forcepoint DLP'nin en önemli özelliklerinden biri de durağan, hareket halindeki ve kullanımdaki verileri tanımlayabilmesidir. Temel veri tanımlama özelliklerinden bazıları::

- → **Optik Karakter Tanıma (OCR)** durağan veya hareket halindeki görüntülerin içine gömülü verileri belirler.
- → **Kişisel Bilgilerin (PII) doğru belirlenmes**i veri doğrulama kontrolleri, gerçek ad tespiti, yakınlık analizi ve bağlam tanıtıcıları içerir.
- → **Özel şifrelemenin belirlenmesi** keşif yöntemleri ve geçerli kontrollerden gizlenen verileri ortaya çıkarır.
- → **Kümülatif analiz,** drip-DLP (zaman içinde yavaşça sızan veriler) tespitine yöneliktir.
- → **Daha akıllı uygulama,** kişisel e-postaların kullanımının artması gibi veri etkileşimi ile ilgili olduğu için kullanıcı davranışındaki değişiklikleri tanımlar. Riske Uyarlanabilir Koruma ile Forcepoint DLP, kullanıcı riskinin anlaşılması için davranış analizinden yararlandığı için daha da etkili hale gelir ve bu da kullanıcının risk seviyesine göre otomatik politika uygulamasını gerçekleştirmek için kullanılır. Bu özellik, güvenlik ekiplerinin statik küresel politikalar yerine kişiselleştirilebilir dinamik politikalar uygulamasını sağlar.

AI Mesh

İşletmenizin en değerli varlığı olan verilerinizden ödün vermeden yapay zekanın potansiyelini açığa çıkarın. Forcepoint ile, üstün AI Mesh teknolojimiz benzersiz veri sınıflandırma doğruluğu ve verimliliği sağlayarak içinizin rahat olmasını sağlar. Merkezileştirilmiş görünürlük ve kontrol özelliklerimiz, ChatGPT, Copilot, Gemini ve diğer birçok Üretken Yapay Zeka uygulaması dahil olmak üzere verilerinizi her yerde korur. Ekibinizin Üretken Yapay Zeka ve diğer yazılımları güvenli bir şekilde kullanmasını sağlayarak verimliliği artırın. Basitleştirilmiş operasyonlar ve bütünleşik politikalarla maliyetleri azaltın.

- **Forcepoint Veri Güvenliği Duruş Yönetimi (DSPM)** ile kullanımdaki veriler ve bekleyen veriler için son derece hassas sınıflandırma sağlamak amacıyla ileri düzeyde eğitilmiş AI Mesh ve LLM modellerinden yararlanarak Forcepoint Veri Sınıflandırması ile senkronize çalışın.

Veri koruma riskini belirleyin, yönetin ve ortadan kaldırın

Çoğu DLP çözümünde güçlü bir ön tanımlı sınıflandırma kitaplığı ve tüm veriler için hassas görünürlük özelliği mevcut değildir, bu da hem risk altındaki verilerin gözden kaçmasına hem de kullanıcıların olağanüstü sayıda hatalı pozitif sonuçla karşılaşmasına neden olmaktadır. Bu yaklaşım, güvenlik ekiplerinin etkinliğini azaltmanın yanı sıra, çalışanların veya son kullanıcıların güvenlik çözümlerini verimlerini düşüren bir engel olarak görmesine ve hayal kırıklığı yaşamasına neden olur. Forcepoint DLP, analizden ve sektördeki en büyük ön tanımlı şablon ve politika kitaplığından faydalanarak, hatalı pozitif sonuçları büyük ölçüde azaltır ve güvenlik operasyonlarının daha verimli olmasını sağlar. DLP, ayrıca çalışanların güvenlik konusundaki farkındalığını artırmak için çalışanlara koçluk yapılmasını ve veri sınıflandırma çözümleriyle entegrasyonu da destekler.

- **Müdahale ekiplerini,** risk altındaki kritik verileri ve kullanıcılar genelinde görülen yaygın davranış kalıplarını vurgulayan, öncelik verilmiş olaylar ile en riskli yerlere yönlendirin.
- **Çalışan koçluğu;** kuruluşun adıyla kişiselleştirilebilen açılır pencereler, açılır pencerenin nedenine ilişkin kısa bir eğitim bildirimi ve kullanıcıların kuruluşun ilgili güvenlik politikası hakkında daha fazla bilgi edinmek için tıklayabileceği bir url şeklinde gelir.
- **E-posta tabanlı dağıtımlı olay iş akışlarıyla veri sahiplerinin ve işletme yöneticilerinin** DLP olaylarını inceleyebilmesini ve bu olaylara müdahale edebilmesini sağlayın.
- **Anonim hale getirme seçenekleri** ve erişim kontrolleri ile kullanıcı gizliliğini koruyun.
- Forcepoint Riske Uyarlanabilir Koruma ile sağlanan derin entegrasyonlar yoluyla **veri bağlamını daha kapsamlı kullanıcı analizlerine ekleyin.**

Veri ihlallerini gerçek zamanlı olarak önleyin

Veri ihlalleri anında gerçekleşebilir ve sonuçları hem finansal açıdan hem de itibar açısından maliyetli olabilir. Forcepoint DLP, kuruluşunuzu, ihlalleri oluştuğu anda tespit etmek ve önlemek için gerekli araçlarla donatarak hassas verilerinizi güvende tutar. Gelişmiş gerçek zamanlı koruma ve düzenli yönetim sunarak, ekibinizin gelişen tehditlerden bir adım önde kalmasını sağlarız.

- **Gerçek zamanlı izleme ve engelleme:** Hassas bilgiler açığa çıkmadan önce veri ihlallerini gerçekleştikleri gibi tespit edin ve durdurun.
- **Birleşik politika yönetimi:** Her Yerde Veri Güvenliği için çevrenizdeki politikaları yönetmek için güvenliği tek bir konsolla basitleştirin.
- **Kanallar arası olay görünürlüğü:** Tehditlere hızlı yanıt vermek için web, bulut, e-posta ve uç noktalar genelinde veri hareketlerine ilişkin tam görünürlük elde edin.
- **Adli Bilim:** Olayları araştırmak, ihlalleri önlemek, politikaları güçlendirmek ve uyumluluğu garantilemek için veri hareketinin tüm hikayesini ortaya çıkarın.
- **Risk-Adaptive Protection:** Hassas verilerin verimliliği bozmadan korunmasını sağlamak için güvenlik kontrollerini kullanıcı davranışlarına ve risk seviyelerine göre dinamik olarak ayarlayın.

Hem bulutta hem de kurum içi her yerde veri görünürlüğü

Günümüzün kurumları, verilerin her yerde olduğu ve kuruma ait olmayan veya kurum tarafından yönetilen yerlerde bulunmayan verilerin de korunmasını gerektiren karmaşık çalışma ortamlarının zorluğunu yaşamakta. Forcepoint ONE Data Security for CASB and SWG, analitik ve DLP politikalarını kritik bulut uygulamalarına ve web trafiğine kadar genişleterek verilerinizin bulunduğu her yerde korunmasını sağlar.

- Forcepoint ONE for Email ve Forcepoint ONE for Endpoints ile müdahale ekiplerini bulut uygulamaları ve web'in yanı sıra e-posta ve uç noktalar **genelinde verileri tanımlamaya ve korumaya odaklayın.**
- **Hassas verilerin harici kullanıcılarla** veya kurum içerisindeki yetkisiz kişilerle paylaşılması olaylarını belirleyin ve otomatik olarak engelleyin.
- **Office 365**, Teams, SharePoint, OneDrive, Salesforce, Box, Dropbox, Google Apps, AWS, ServiceNow, Zoom, Slack ve diğer pek çok uygulama dahil olmak üzere kritik bulut uygulamalarına yüklenen veya bu uygulamalardan indirilen verileri gerçek zamanlı olarak koruyun.
- Bulut, ağ, uç nokta, web ve e-posta dahil olmak üzere tüm kanallarda hareketli veri ve veri keşfi politikalarını tanımlamak ve uygulamak için tek bir konsol kullanarak **politika uygulamalarını birleştirin.**
- DLP politikası özelliklerini bulut uygulamalarına taşırken, aynı zamanda da olayları ve adli verileri kendi veri merkezinizde tutma seçeneği de sunan **bir Forcepoint çözümünü kurun.**

DLP hakkında daha fazla bilgi için

Demo Talep Edin

Forcepoint Veri Güvenliği Çözümleri

Forcepoint ONE Data Security (DLP SaaS)	Bulut tabanlı bir çözüm olan Forcepoint ONE Data Security, hassas verileri korur, ihlalleri önler ve küresel uyumluluğu sağlar. Hızlı kurulum ve politika yönetimi ile veri korumasını kolaylaştırır. Bulut uygulamaları, web, e-posta ve uç noktalar genelinde birleşik yönetim sunar. Forcepoint Risk-Adaptive Protection ile gerçek zamanlı kullanıcı riski öngörüleri sunar. Forcepoint ONE Data Security ile düşük maliyet, risk ve yüksek verimlilikten yararlanın.
Forcepoint DSPM	Forcepoint DSPM, benzersiz görünürlük ve kontrol sağlayarak bulut platformları ve sunucular arasında veri yayılımı sorununu çözer. Veri keşfini ve sınıflandırma doğruluğunu sürekli olarak iyileştirmek için AI Mesh teknolojisini kullanır. Ayrıca, süreçleri kolaylaştırmak ve maliyetleri azaltmak için iyileştirme ve raporlama gibi rutin görevleri otomatikleştirir.
Risk-Adaptive Protection	Geleneksel politika merkezli DLP çözümlerinin aksine Risk-Adaptive Protection (RAP), riski proaktif olarak azaltmak amacıyla insanları ön plana çıkararak davranışları anlar. RAP, gerçek zamanlı risk hesapları, 130'dan fazla davranış göstergesi ve sorunsuz kurulum sunarak yüksek riskli kullanıcılara öncelik verir. Okunması kolay panolarla öngörü kazanın, ayrıntılı politika uygulamalarıyla verimliliği artırın ve dinamik otomasyonla iç tehditleri etkin bir şekilde azaltın.
Forcepoint ONE Data Security for Email (DLP SaaS)	Forcepoint ONE Data Security for Email kritik e-posta kanalındaki hassas veri sızıntılarına karşı koruma sağlar. Bu tümüyle buluta özgü çözüm, hem uç noktalar hem de mobil cihazlarda e-posta ihlallerini ve e-posta yoluyla veri kaybını önler. Popüler e-posta sağlayıcılarıyla sorunsuz bir şekilde entegre edilen bu çözüm, önceden oluşturulmuş güvenlik politikaları, sınıflandırıcılar ve şablonlarla basitleştirilmiş yönetim sunar.
Forcepoint ONE Data Security for Cloud Apps and Web (DLP SaaS)	Forcepoint ONE Data Security for Cloud Apps and Web, Forcepoint ONE Data Security for Endpoint ve Forcepoint Data Security for E-mail ile aynı bulut tabanlı DLP çözümünü sunarak 4 kanalın herhangi birini veya tümünü tek bir kullanıcı arayüzünden yönetmenize ve tüm politikaları aynı politika yönetimi konsolundan senkronize etmenize olanak tanır. Politikaları bir kez yazın ve tüm Forcepoint ONE Data Security kanallarında uygulayın. Politikaları birden fazla hizmette senkronize ederek zamandan ve kaynaklardan tasarruf edin.
Forcepoint Data Classification	Forcepoint Data Classification, AI Mesh destekli hassasiyet ve otomasyon kullanarak veri sınıflandırmayı yeniden şekillendirerek manuel hataları ortadan kaldırıyor ve DLP etkinliğini artırıyor. Üstün sınıflandırma doğruluğu sağlamak için AI Mesh teknolojisinden ve Büyük Dil Modellerinden yararlanıyoruz. Bu sayede, sürekli öğrenme ve iyileştirme aracılığıyla, politika uygulamasını ve uyumluluğu geliştirerek güvenilir önerilerde bulunuyoruz. İş akışınızla sorunsuz bir şekilde entegre edin, verimliliği artırın ve yanlış pozitifleri azaltın.
Forcepoint DLP Endpoint	Forcepoint DLP Endpoint, kurumsal ağ üzerindeki ve dışındaki Windows ve Mac uç noktalarında kritik verilerinizi korur. Durağan (keşif), hareketli ve kullanımdaki veriler için gelişmiş koruma ve kontrol içerir. Microsoft Azure Information Protection ile entegrasyon sayesinde şifreli verileri analiz eder ve uygun DLP denetimlerini uygular. DLP koçluk diyaloğundan elde edilen rehberliğe dayalı olarak çalışanların veri riskini kendi kendine düzeltmesini sağlar. Çözüm, HTTPS gibi web yüklemelerinin yanı sıra Office 365 ve Box Enterprise gibi bulut hizmetlerine yapılan yüklemeleri de izler. Outlook, Notes ve e-posta istemcileri ile tam entegrasyon.
Forcepoint DLP Discover	Forcepoint DLP Keşif; dosya sunucularındaki, SharePoint (tesis içi ve bulut), Exchange (tesis içi ve bulut) uygulamalarındaki hassas verileri belirleyip korumanın yanı sıra, SQL server ve Oracle gibi veri tabanları için de tespit özelliği sağlar. Gelişmiş parmak izi kontrolü teknolojisi, düzenlemeye tabi verileri ve fikri mülkiyeti durağan haldeyken belirler ve uygun şifreleme ve kontroller uygulayarak bu verileri korur. Keşif çözümü, ayrıca resimlerdeki veriler için de görünürlük sağlayan OCR özelliğini içerir.
Forcepoint DLP Network	Forcepoint DLP Network; e-posta, web kanalları ve FTP aracılığıyla hareket halindeki verilerin çalınmasını durdurmak için kritik bir uygulama noktası sunar. Çözüm, dış saldırılardan veya iç tehditlerden kaynaklanan veri sızdırma olaylarını ve kazara veri kaybını belirlemeye ve önlemeye yardımcı olur. OCR, bir görüntü içindeki verileri tespit eder. Analizler, verilerin teker teker olaylar halinde çalınmasını ve diğer yüksek riskli kullanıcı davranışlarını durdurmak üzere Drip DLP özelliğini sağlar.
Forcepoint DLP for Cloud Email	Forcepoint DLP for Cloud Email, verilerinizin ve fikri mülkiyet unsurlarınızın giden e-postalar yoluyla istenmeyen şekilde dışarı sızdırılmasını engeller. DLP yönetiminizi basitleştirmek için bu çözümü Uç Nokta, Ağ, Bulut ve Web gibi diğer Forcepoint DLP kanal çözümleriyle birleştirebilir ve tek bir politika oluşturarak bu politikayı birden fazla kanalda uygulayabilirsiniz. Forcepoint DLP for Cloud Email, öngörülemeyen e-posta trafiği artışlarından büyük ölçeklenebilirlik potansiyeli sunar. Ayrıca, giden e-posta trafiğinizin işletmenizin ek donanım kaynaklarını yapılandırmasını ve yönetmesini gerektirmeden artmasına da imkan tanır.
Forcepoint DLP App Data Security API	Forcepoint DLP App Data Security API, kuruluşların dahili özel uygulama ve hizmetlerindeki verileri güvence altına almasını kolaylaştırır. Dosya ve veri trafiğinin analizine olanak tanır ve kişiselleştirilmiş bir açılır pencere ile izin verme, engelleme, onay isteme, şifreleme, paylaşımı geri alma ve karantinaya alma gibi DLP işlemlerini uygular. Kapsamlı bir eğitim veya karmaşık protokoller hakkında bilgi gerektirmeyen, kolay anlaşılır ve kullanımı basit bir REST API'sidir. Ayrıca dilden bağımsızdır ve herhangi bir programlama dili veya platformunda geliştirmeyi ve kullanımı mümkün kılar.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint, küresel şirketler ve hükûmetler için güvenliği basitleştiriyor. Forcepoint'in gerçek bulut tabanlı, hepsi bir arada platformu, Sıfır Güven yaklaşımının benimsenmesini kolaylaştırır ve insanlar nerede çalışırsa çalışsın, hassas verilerin ve fikri mülkiyetin çalınmasını veya kaybolmasını önler. Merkezi Austin, Texas'ta bulunan Forcepoint; 150'den fazla ülkedeki müşteriler ve çalışanları için güvenli ortamlar oluşturmaktadır. Forcepoint ile etkileşime geçin: www.forcepoint.com, Twitter ve LinkedIn.

[DLP-BROCHURE-TR] 17Jan2025