

Forcepoint Data Loss Prevention

Sınırları olmayan bir
dünyada veri koruması

Forcepoint

Broşür

Forcepoint Data Loss Protection (DLP)

Çalışanlarınızın faaliyet gösterdiği ve verilerinizin bulunduğu her yerde veri güvenliği

Büyükölçüden bağımsız her kuruluş, günümüzde kritik veri güvenliği zorluklarıyla karşı karşıya. Kişisel Tanımlanabilir Bilgiler (PII), Koruma Altındaki Sağlık Bilgileri (PHI), ve diğer düzenlemeye tabi veriler gibi hassas bilgileri korumak için yasal düzenlemelerle uyumlu olmaları gerekir. Aynı zamanda bulut uygulamaları, hibrit çalışma ortamları ve BYOD trendleri gibi modern çalışma ortamlarını benimsemeleri gerekir ve bunların hepsi verilerin kuruluştan ayrılma şeklini çeşitlendirir.

Bu genişleyen saldırı yüzeyi günümüzde kritik verilerin korunmasında en büyük zorluğu temsil etmektedir. Veri güvenliği ekiplerinin, hem kuruluş içinde hem de ötesinde veri hareketindeki artışla ilgilenmeleri gerekir. Bulut, web ve şirket içi veriler genelinde geniş çaplı görünürlüğe ihtiyaç duyarlar. Ek olarak, kontrol ve gözetim, merkezi olarak yönetilen tüm kanallar (uç noktalar, web trafiği, ağ, e-posta, bulut uygulamaları ve özel uygulamalar) genelinde hayati öneme sahiptir.



Forcepoint DLP; küresel politikalarınızı uç nokta, ağ, bulut, web, özel uygulamalar veya e-posta dahil olmak üzere tüm büyük kanallarda kolayca yönetmeniz için gereken tüm araçları sağlayan, sektörün en güvenilir çözümdür. Sektördeki diğer tüm DLP sağlayıcılarından daha fazla ön tanımlı şablon, politika ve sınıflandırıcı sunarak işinizi basitleştirebiliriz. Bu da olay yönetiminizi önemli ölçüde düzene sokarak en önemli unsurlara odaklanabilir ve riskleri ortadan kaldırarak çalışanlarınızın üretkenliğine katkıda bulunabilirsiniz. Forcepoint DLP, çalışanlarınızın faaliyet gösterdiği ve verilerinizin bulunduğu her yerde size görünürlük ve kontrol sağlayarak riskle mücadele edilmesini sağlar.

Veri koruması:

- › **Çalışanlarınızın verileri oluşturmak,** depolamak ve taşımak için kullandığı tüm uygulamalara yönelik tek bir kontrol noktası ile düzenlenmiş verileri güvenceye almalıdır.
- › **İnsanların 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.**



Uyumu
hızlandırmak



Verileri korumak
için çalışanlara
yetki vermek



Gelişmiş
Tespit ve
Kontrol



Riske
Müdahale
Etmek ve Riski
Gidermek



Uyumu hızlandırmak

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 150'den fazla bölgenin mevzuat gerekliliklerine uygun 1.700'den fazla hazır şablon, politika ve sınıflandırıcı ile 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 belirlenmesi** 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.
- **Forcepoint Data Security Posture Management (DSPM)** ile kullanımda olan veriler ve durağan veriler için son derece hassas sınıflandırmalar sunmak üzere **Forcepoint Data Classification ile entegrasyon**, yüksek düzeyde eğitilmiş AI/LLM modellerinden yararlanır.



→ **Analizler**, kullanıcı davranışındaki değişiklikleri belirler ve kişisel e-postanın artan kullanımını gibi veri etkileşimlerini ortaya çıkarır. Forcepoint DLP, Riske Uyarlanabilir Koruma özelliğiyle kullanıcı riskini anlamak için davranış analizini kullanarak ve ardından bu analizden her kullanıcının risk seviyesine göre otomatik politika uygulaması sağlamak için faydalanarak daha da etkili hale gelmektedir. Bu özellik, güvenlik ekiplerinin statik küresel politikalar yerine kişiselleştirilebilir dinamik politikalar uygulamasını sağlar.

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 bildirim ve kullanıcıların kuruluşun ilgili güvenlik politikası hakkında daha fazla bilgi edinmek için tıklayabileceği bir url şeklinde gelir.
- **E-posta tabanlı dağıtımli 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.**

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 taşıırken, 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	<p>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 öngörülerini sunar. Forcepoint ONE Data Security ile düşük maliyet, risk ve yüksek verimlilikten yararlanın.</p>
Forcepoint DSPM	<p>Forcepoint DSPM, bulut platformları ve sunucuları genelinde veri yayılımının zorluğunun üstesinden gelerek benzersiz görünürlük ve kontrol sağlar. Veri keşfini ve sınıflandırma doğruluğunu sürekli olarak iyileştirmek için yapay zeka destekli makine öğrenimini kullanır. Ayrıca, süreçleri kolaylaştırmak ve maliyetleri azaltmak için düzeltme ve raporlama gibi görevleri otomatikleştirir.</p>
Risk-Adaptive Protection	<p>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.</p>
Forcepoint Data Classification	<p>Forcepoint Data Classification veri sınıflandırmasını yapay zeka destekli hassasiyet ve otomasyon ile yeniden tanımlar; manuel hataları ortadan kaldırır ve DLP etkinliğini artırır. Üstün sınıflandırma doğruluğu sunmak için Üretken Yapay Zeka ve Büyük Dil Modellerinden yararlanırsınız. Sürekli öğrenme ve iyileştirme sayesinde güvenilir öneriler sunar, politika uygulamalarını ve uyumluluğu artırır. İş akışınızla sorunsuz bir şekilde entegre edin, verimliliği artırın ve yanlış pozitifleri azaltın.</p>
Forcepoint ONE Data Security for Email	<p>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.</p>
Forcepoint DLP for Cloud Email (kurum içi Enterprise DLP)	<p>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, öngörülemez 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.</p>
Forcepoint ONE CASB ve SWG	<p>Forcepoint ONE Data Security for CASB and SWG, Forcepoint ONE Data Security for Endpoint ve Forcepoint Data Security for Email ile aynı tümüyle buluta özgü DLP çözümünü sunar. 4 kanaldan herhangi birini veya tümünün 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 etme süresinden ve kaynaklardan tasarruf edin.</p>

Forcepoint

[forcepoint.com/contact](https://www.forcepoint.com/contact)

About Forcepoint

Forcepoint, küresel şirketler ve hükümetler 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.