Forcepoint

Bilgi Formu

Forcepoint DLP

Tüm kanallarda birleşik yönetim sunan, sektör lideri Veri Kaybı Önleme (DLP) çözümü

Veri güvenliği kritik öneme sahiptir, ancak karmaşık olmak zorunda değildir. Günümüzün hibrit iş gücü, hassas bilgilere herhangi bir cihazdan, herhangi bir konumdan erişmeyi gerektirir. Forcepoint Data Loss Prevention (DLP), modern işletmeler için veri korumayı kolaylaştırır; performanstan veya verimlilikten ödün vermeden kapsamlı şirket içi DLP çözümleri sunar.

Uç noktalar, ağlar ve depolama genelinde veri hareketlerini derinlemesine görünürlükle izleyen Forcepoint DLP, kritik varlıklarınızı korur ve düzenlemelere uyumluluğu garanti eder. Forcepoint DLP, güvenlik politikalarını Forcepoint Security Manager (FSM) üzerinden ek kanallara genişletme yeteneğiyle fark yaratır; bu sayede bulut tabanlı SaaS uygulamaları ve web üzerinde kesintisiz veri koruması sağlarken, tutarlı ve birleşik politika uygulamasını garanti eder. Gelişmiş adli soruşturma, kesintisiz entegrasyon ve ölçeklenebilirlik avantajlarından yararlanın—işletmenizin ihtiyaçlarına uyum sağlayan bir çözümle geleceğe hazır olun.

Veri uyumluluğunu kolaylaştırın

- → 90 ülke ve 160'dan fazla bölgenin mevzuat gerekliliklerine uygun 1.700'den fazla hazır şablon, politika ve sınıflandırıcı ile uyumluluğu kolayca karşılamak ve sürdürmek için **kapsamı düzenleyin.**
- → Ağ, bulut ve uç nokta keşfi ile düzenlenmiş verileri **bulun ve düzeltin.**
- → Bulut, uç nokta, ağ, web ve e-posta dahil olmak üzere tüm kanallarda **merkezi kontrol** ve tutarlı politikalar.

Kapsamlı veri koruması sağlayın

- → Bulutta, ağda, e-postada veya uç noktalarda, her nerede olursa olsun verileri **keşfedin ve kontrol edin.**
- → Çalışanları akıllı kararlar almaya teşvik edin; kullanıcı eylemlerini yönlendiren mesajlarla politika konusunda **eğitim verin** ve kritik verilerle etkileşim sırasında kullanıcı amacını doğrulayın.
- → Kuruluşunuzun dışına çıkan verileri koruyan politika tabanlı otomatik şifreleme yöntemini kullanarak güvenilir iş ortakları ile **güvenli işbirliği yapın.**
- → Forcepoint Data Classification ve Microsoft Purview Information Protection entegrasyonu sayesinde **veri etiketleme ve sınıflandırmayı otomatikleştirin.**

Gelişmiş özelliklerden ve kontrollerden yararlanın

- **Optik Karakter Tanıma (OCR)** durağan veya hareket halindeki görüntülerin içine gömülü verileri belirler.
- Kişisel Bilgiler (PII) için **güçlü tanımlama**; veri doğrulama kontrolleri, gerçek ad tespiti, yakınlık analizi ve bağlam tanıtıcıları hassas verilerinizi güvence altına alır.
- **Özel şifreleme belirleme**, keşif yöntemleri ve geçerli kontrollerden gizlenen verileri ortaya çıkarır.
- **Kümülatif analiz**, drip-DLP (zaman içinde yavaşça sızan veriler) tespitini hedefler.
- **Gelişmiş dosya taraması,** büyük dosyaların rastgele bölümlerini inceleyerek kısmi veri sızıntısını tespit ederek veri sızdıranların hassas bilgileri gizlemelerini önler.
- **Forcepoint Data Classification entegrasyonu**, ileri düzey AI/LLM modellerinden yararlanarak, Forcepoint Data Security Posture Management (DSPM) ile kullanımdaki ve durağan veriler için son derece hassas sınıflandırma sağlar.
- **Gelişmiş üretken yapay zeka**, kullanıcıların sistemi eğiterek kendini geliştiren bir yapay zeka modeli oluşturmasına olanak tanır, tüm verileri otomatik olarak bulup, kategorize edip sınıflandırarak zamandan tasarruf sağlar ve doğruluğu önemli ölçüde artırır.
- Yapılandırılmış (örn. veri tabanları) ve yapılandırılmamış (örn. dokümanlar) verilerin **parmak iziyle tanımlanması**, veri sahiplerinin veri türlerini belirlemesine ve iş dokümanları, tasarım planları ve veri tabanlarında tam veya kısmi eşleşmeleri tespit etmesine olanak tanır, ardından veriye uygun doğru kontrol veya politikayı uygulamalarını sağlar.
- **Risk-Adaptive Protection** ile Forcepoint DLP, davranış analitiğinden yararlanarak kullanıcı riskini anlamada daha da etkili hale gelir ve bu analiz, kullanıcının risk seviyesine göre otomatik politika uygulamasını hayata geçirmek için kullanılır.

Veri koruma risklerini bulun ve azaltın

- **Müdahale ekiplerini**, risk altındaki kritik verileri ve kullanıcılar genelinde görülen yaygın davranış kalıplarını vurgulayan, öncelik verilmiş olaylar ile en riskli yerlere yönlendirin.
- Yönetim konsolundan ayrılmadan belirli destek bilgilerini hızla bulmak için doğrudan çözüme entegre edilmiş, **yapay zeka destekli Akıllı Arama yardım aracını kullanın.**
- Windows ve macOS'ta çalışan eğitimiyle hassas veri ve fikri mülkiyetin yönetimi konusunda **çalışan farkındalığını artırın** ve Forcepoint Data Classification ile Microsoft Purview Bilgi Koruma gibi sınıflandırma çözümleri entegrasyonu ile çalışanları güçlendirin.
- **Gelişmiş DLP veri tanımlama yeteneklerini**, parmak izi tanımlama gibi özellikler de dahil olmak üzere, uzaktan çalışma uç noktalarında ve kurumsal bulut uygulamalarında devreye alın.
- E-posta tabanlı dağıtımlı olay iş akışlarıyla **veri sahiplerinin ve işletme yöneticilerinin** DLP olaylarını inceleyebilmesini ve bu olaylara müdahale edebilmesini sağlayın.
- Anonimleştirme seçenekleri ve erişim kontrolleri ile **kullanıcı gizliliğini koruyun.**
- Forcepoint Risk-Adaptive Protection. ile sağlanan derin entegrasyonlar **yoluyla veri bağlamını** daha kapsamlı kullanıcı analizlerine ekleyin.

Verileriniz üzerinde her yerde görünürlük elde edin

- → **Yöneticilere**, bulut uygulamaları, ağ veri depoları, veri tabanları ve yönetilen veya yönetilmeyen uç noktalar genelinde verileri tanımlama ve koruma yetkisi kazandırın.
- → Hassas verilerin harici kullanıcılarla veya kurum içerisindeki yetkilendirilmemiş kişilerle paylaşıldığı durumları **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 v**erileri gerçek zamanlı olarak koruyun.**
- → Tek bir konsol üzerinden tüm kanallarda—bulut, ağ, uç noktalar, web ve e-posta—hareketii verileri ve veri keşif politikalarını tanımlayıp uygulayarak **politika yönetimini birleştirin.**
- → Şirket içi DLP çözümü ve hibrit seçeneklerle **veri sahipliğini koruyun**; parmak izi oluşturma, makine öğrenimi ve politika uygulama gibi gelişmiş özellikleri bulut uygulamalarına ve web kanallarına genişletin. Sıkı düzenlemelere tabi sektörler için ideal olan bu çözüm, olay kayıtlarını ve adli inceleme verilerini güvenli bir şekilde veri merkezinizde tutarak veri egemenliğini garanti eder ve uyumluluk gereksinimlerini destekler.
- → Açık REST API'ler sayesinde **üçüncü taraf araçlar ile olayları görüntüleyin ve yönetin**. Olay yönetimi iş akışlarını otomatikleştirin ve ServiceNow, Nagios, Tableau gibi otomasyon ve hizmet araçlarının yanı sıra Splunk ve XSOAR gibi SIEM/SOAR çözümleriyle DLP olaylarına dayalı iş süreçlerini destekleyin.

Enterprise DLP çözümlerimiz hakkında daha fazla bilgi için bir demo talep edin.

Ek A: DLP Çözüm Bileşenine Genel Bakış

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. Çalışanların, DLP koçluk diyaloğuyla sağlanan rehberlik sayesinde veri risklerini kendi kendine gidermesini sağlar. Çözüm, HTTPS dahil web yüklemelerini ve Office 365 ile Box Enterprise gibi bulut hizmetlerine yapılan yüklemeleri izler. Outlook, Notes ve e-posta istemcileri ile tam entegrasyon.
Forcepoint ONE CASB	Forcepoint ONE CASB tarafından desteklenen Forcepoint DLP'nin gelişmiş analitiğini ve tek kontrolünü Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack ve çok daha fazlası dahil olmak üzere onaylanmış bulut uygulamalarına genişletin. Kullanıcılar nerede olursa olsun veya hangi cihazı kullanırsa kullansın, iş açısından kritik veriler için sürekli kontrol kazanın.
Forcepoint ONE SWG	Forcepoint ONE SWG, ekibinizin güvendiği yüksek hızlı web performansını elde ederken herhangi bir web sitesine güvenli bir şekilde erişmenizi veya herhangi bir belgeyi indirmenizi sağlar. Riskli sitelerin güvenli bir şekilde işlenmesi için RBI ve indirilebilir tüm belgelerin güvenliğinin tamamen sağlaması için Zero Trust CDR ile entegre edin.
Forcepoint DLP Discover	Forcepoint DLP Discovery 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 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 saldırılar veya içeriden gelen tehditler yoluyla gerçekleşebilecek veri sızdırma ve kazara veri kaybını tespit edip önlemeye yardımcı olur. OCR, bir görüntü içindeki verileri tespit eder. Analitik, verilerin tek tek çalınmasını önlemek için Drip DLP'yi ve diğer yüksek riskli kullanıcı davranışlarını tespit edip durdurmayı 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. Forcepoint DLP'yi Uç Nokta, Ağ, Bulut ve Web gibi diğer DLP kanal çözümleriyle entegre ederek DLP yönetiminizi kolaylaştırabilir, tek bir politika oluşturarak bunu birden fazla kanalda uygulayabilirsiniz. Bulut tabanlı olmayan çözümlerden farklı olarak, Forcepoint DLP for Cloud Email, öngörülemeyen e-posta trafiği artışlarına karşı üstün ölçeklenebilirlik sağlar. Ayrıca, ek donanım kaynakları yapılandırıp yönetmeye gerek kalmadan, giden e-posta trafiğinizin işletmenizin büyümesiyle birlikte ölçeklenmesine olanak tanır.
Forcepoint DLP App Data Security API	Forcepoint DLP App Data Security API, kuruluşların dahili özel uygulamalarında ve hizmetlerinde verileri kolayca güvence altına almasını sağlar. Dosya ve veri trafiğini analiz etmeyi sağlar ve izin verme, engelleme, kişiselleştirilmiş bir açılır pencere ile onay isteme, şifreleme, paylaşımı kaldırma ve karantinaya alma gibi DLP eylemlerini uygular. Geniş çaplı eğitim veya karmaşık protokollere dair derin bilgi gerektirmeden kolayca anlaşılabilen ve basitçe kullanılabilen bir REST API'dir. Ayrıca, dilden bağımsızdır ve herhangi bir programlama dili veya platformunda geliştirmeyi ve kullanımı mümkün kılar.

Ek B: DLP Çözümü Bileşenlerine Genel Bakış

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT ONE SWG	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
Ana işlevi nedir?	Veri keşfi ve veri koruma politikalarının uygulaması; uygulamalar, web, yazdırma ve taşınabilir medya gibi kullanıcı uç noktalarındaki çeşitli kanallar üzerinden gerçekleştirilir.	Bulutta veya bulut tabanlı uygulamalarla veri keşfi ve politika uygulanması	Giden e-posta üzerinden hareket halindeki veriler için görünürlük ve kontrol	Veri merkezleri ve diğer şirket içi ortamlardaki durağan verilerin keşfi, taranması ve iyileştirilmesi	Ağ içinde web ve e-posta yoluyla hareket halindeki veriler için görünürlük ve kontrol	Ağ içinde web ve e-posta yoluyla hareket halindeki veriler için görünürlük ve kontrol	Dahili özel uygulamalar ve hizmetlerdeki verilerin görünürlüğü ve kontrolü
Keşfedilen ve korunan durağan veriler nerede bulunur?	Windows uç noktaları, MacOS uç noktaları	OneDrive, Sharepoint Online, Exchange Online, Google Drive, Box, DropBox, Salesforce, ServiceNow	Şirket içi dosya sunucuları ve ağ depolama, SharePoint Server, Exchange Server, Microsoft SQL Server, Oracle ve IBM Db2 gibi veri tabanları				
Hareketli veriler nerede korunur?	E-posta, Web: HTTP(S), Yazıcılar, Çıkarılabilir medya, Dosya sunucuları / NAS	API üzerinden Office 365, Google Apps, Salesforce.com, Box, Dropbox ve ServiceNow ve proxy sunucu yoluyla diğer TÜM yaygın uygulamalar	HTTP(S)		E-posta, Yazıcılar, FTP, Web: Http(S), ICAP	E-posta	Dahili özel uygulamalar ve özel hizmetler
Kullanımdaki veriler nerede korunur?	Zoom, Webex, Google Hangouts, IM, VOIP dosya paylaşımı, M365 Teams paylaşımı, uygulamalar (bulut depolama istemcileri), OS panosu	Bulut uygulamaları kullanılarak yapılan oluşturma, değiştirme ve iş birliği faaliyetleri sırasında					Dahili özel uygulamalar ve özel hizmetler

Ek B: DLP Çözüm Bileşeni Özellikleri Karşılaştırması

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT ONE SWG	FORCEPOINT DLP DISCOVER	FORCEPOINT DLP NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT DLP APP DATA SECURITY API
Risk-Adaptive Protection	Eklenti		Eklenti, şu anda Forcepoint ONE SWG ile GRE/ IPSec tünelleri ile desteklenmektedir	Eklenti	Eklenti	Eklenti	
Optik Karakter Tanıma (OCR)				Dahil	Dahil	Dahil	
Veri sınıflandırma ve etiketleme entegrasyonları	Forcepoint Data Classification ve Microsoft Purview Information Protection.						
Hangi veriler parmak iziyle tanımlanabilir?	Yapılandırılmış (veri tabanları), Yapılandırılmamış (belgeler), İkili (metin harici dosyalar)						
Birleşik politika yönetimi	Tek bir konsolla uç noktalardan bulut uygulamalarına kadar politika yapılandırması ve uygulaması						
Kapsamlı politika kitaplığı	Sektördeki en büyük uyum politikası kitaplığıyla sağlanan keşif ve uygulama özellikleri						

© 2025 Forcepoint. Forcepoint ve FORCEPOINT logosu, Forcepoint'in ticari markalarıdır.
Bu belgede kullanılan tüm diğer ticari markalar ilgili sahiplerine aittir.
[FP-DLP-Datasheet-TR] 06Jan2025