Forcepoint

Çözüm Özeti

Forcepoint Bulut E-Postaları için Data Loss Prevention Çözümü

Sektördeki en güvenilir DLP teknolojisinden faydalanarak e-postalarınızı koruyun ve kontrol edin

Zorluk

- Gitgide daha fazla hassas veri, birden fazla kanal yoluyla kurumların dışına çıkmakta.
- E-posta, en popüler saldırı vektörlerinden biri olarak görülmekte.
- Verimliliği düşürmeden verilerin güvenlik altına alınması hiç bu kadar karmaşık veya önemli hale gelmemişti.

Çözüm

- Forcepoint, sektörün en güvenilir Data Loss Prevention (DLP) çözümünü e-posta kanalına taşıyor.
- E-posta yoluyla gerçekleşen hassas veri kayıpları'nı hassas bir şekilde takip edin ve önleyin.
- Giden e-posta korumasını şirketinizin ihtiyaçlarını karşılayacak şekilde ölçeklendirmek için, tam yönetimli bir bulut çözümünden faydalanın.

Sonuç

- E-posta yoluyla gerçekleşen hatalı pozitif olay sayısını büyük ölçüde azaltarak verimi artırın
- Diğer tüm DLP sağlayıcılarına göre 3 kat daha fazla ön tanımlı politikayla mevzuata uyumu artırın.
- Forcepoint'in uzmanlığından, kullanıma hazır politikalarından ve birinci sınıf bilgi aktarımı süreçlerinden faydalanarak DLP çözümünüzü 6 hafta gibi kısa bir sürede Forcepoint'e taşıyın.

Veri güvenliği, küresel anlamda kurumlar için ana odak noktalarından biri haline gelmeye devam ediyor. Çalışanlarınız ister bir ofisin geleneksel sınırları içerisinde isterse de yeni karma veya uzaktan çalışma yöntemiyle çalışıyor olsun, birden fazla kanaldaki verilerin güvenliğini sağlamak gittikçe karmaşıklaşıyor. E-posta; kurumların değerli dosyalarının, fikri mülkiyet unsurlarının ve verilerinin dışarı sızdırılmasını önlemek amacıyla görünürlük ve kontrol elde etmesini sağlayan kritik bir kanaldır. E-posta yoluyla en sık gerçekleşen veri kaybı örneklerinden bazıları şunlardır:

→ **Bir kurumun dosya veya verilerinin şirket** e-postası üzerinden özel bir e-posta adresine gönderilmesi.

→ **Hassas verilerin,** kullanıcı ihmali veya güvenliği ihlal edilen hesaplar yoluyla kurum dışına çıkması.

→ **Şirket içerisindeki kötü niyetli bir kişinin hassas veri ve dosyaları harici rakiplere,** haber kaynaklarına ve web sitelerine göndermesi. Bu işlemlerdeki niyet genellikle sahtekarlık yapmak, kurumu sabote etmek veya özel verileri çalmaktır.

→ **Kimlik hırsızlığı ve kötü amaçlı yazılım saldırıları veya reklam yazılımları veya istenmeyen e-postalar,** iyi niyetli dahili kullanıcıların kötü niyetli kişilerin kritik verileri ve fikri mülkiyet unsurlarını sızdırma çabalarına istemeden ortak olmasına neden olur.

"E-posta, saldırganların kurumlara kötü amaçlı yazılımlarla sızmak için kullandığı en popüler saldırı vektörü. E-posta aynı zamanda kullanıcılarla siber suçlular arasında doğrudan bir iletişim hattı sağlayarak, her yıl dolandırıcılık ve iş e-postalarının güvenliğinin ihlal edilmesinden kaynaklanan milyarlarca dolar zarara yol açmakta."

IDC, WORLDWIDE MESSAGING SECURITY MARKET SHARES, 2021: HYBRID WORK DRIVES NEED FOR THREAT INVESTIGATION INTEGRATION, DOC # US49144522, JUNE 2022

Kurumlar, fikri mülkiyet unsurlarını hedefli saldırılardan ve kazayla ifşa edilme durumlarından korumak için giden e-postaları konusunda güçlü bir görünürlük ve kontrol sağlamak zorunda. Bunu sağlayan teknoloji de DLP çözümüdür. IDC'ye göre, "Son 24 ayda veri kaybı teknolojileri pazarında bir Rönesans yaşandı. Manuel ve eski sınıflandırma tekniklerinin yerini, makine öğrenimi ve otomasyon almış durumda. Bağlam, bu teknolojinin çalışmasını sağlayan esas unsur haline geldi. Çözümlerin etkinliği ve verimi de arttı." [1] Hassas bilgileri keşfeden, koruyan ve kontrol eden DLP teknolojisindeki ilerlemelerle birlikte kullanılan email security (e-posta güvenliği) çözümleri, güvenlik için büyük önem taşıyan e-posta vektörünün kontrol edilmesi açısından esastır. Güçlü bir DLP koruması olmadığında, e-posta güvenliği'nin ihlal edilmesi işlerinize ve itibarınıza büyük zararlar verebilir.

Forcepoint DLP for Cloud Email çözümünün avantajları

Forcepoint DLP for Cloud Email çözümü, veri güvenliği çözümleri alanında bir lider olarak, giden e-postalara yönelik benzersiz bir görünürlük ve kontrol sağlar. DLP for Cloud Email çözümü; uç nokta, bulut, web ve ağa yönelik DLP çözümleriyle birlikte kurumların verilerini korumak için güçlü ve çok yönlü bir çözüm sağlar. Forcepoint DLP, çalışanlarınızın çalıştığı ve verilerinizin bulunduğu her yerde veri kaybı'nı önlemek için tasarlanmıştır.

Maksimum veri tanımlama

Forcepoint DLP, hızlı uygulama ve hassas verilerin tanımlanmasını sağlayan 1.600'den fazla sınıflandırıcı ve ön tanımlı şablon sağlar. Ayrıca durağan, hareket halindeki ve kullanımdaki verileri hassas bir şekilde tanımlamak için doğal dil analizi, makine öğrenimi ve sektördeki en güçlü parmak izi tanıma teknolojilerinden birini kullanma gibi gelişmiş teknolojilerden de faydalanır. Görünürlük, veri güvenliği için esastır ve Forcepoint DLP Discover çözümü, tüm veri türlerinin uygun şekilde kontrol edilebilmesi için güçlü bir görünürlüğün yanı sıra resmi veri tanımlama özelliği de sağlamaktadır. Bu, birçok açıdan önemlidir:

- → **Uyum.** GDPR, HIPA ve 83'ten fazla ülkede geçerli olan diğer yasa ve kurallar dahil kritik mevzuatı kapsayan Forcepoint DLP kurumların her zaman uyum standartlarını karşılamasını sağlar.
- → **Basitlik.** Bir DLP uygulaması için kurumun ihtiyaçlarını ve iş gereksinimlerini karşılayan sınıflandırıcıların oluşturulması ve uygulanması, çok büyük miktarda zaman ve kaynak gerektiren bir işlemdir. Forcepoint'in ön tanımlı şablon ve sınıflandırıcıları, kurumların belli sektörlere ve veri türlerine özel sınıflandırıcıları hızla uygulamaya başlayarak DLP sürecini büyük ölçüde basitleştirmesini sağlar.
- → **Verimlilik.** Forcepoint'in kapsamlı veri tanımlama teknolojisi, Forcepoint DLP çözümünün hatalı pozitif sonuç sayısını dramatik ölçüde azaltmasını ve incelenmesi gereken kritik olayları sıralayıp, öncelik sırasına almasını sağlar.

Birleşik politika kontrolü

Güçlü bir DLP stratejisi; uç nokta, bulut, web ve e-posta gibi temel kanalların hepsini kapsamalıdır. Kurumlar bu kanalları sıklıkla bulut veya e-posta gibi tek bir kanala odaklanan, birbirinden farklı DLP ürünleriyle kontrol edilen silolar şeklinde ele alır. Forcepoint, tüm bu kanalları tek bir çözümle güvenlik altına almanızı ve tek bir politikayla yönetmenizi sağlar. Politikaların bir kez yazılıp, birden çok kez uygulanabilmesi, kurumunuz dahilindeki veriler üzerinde benzersiz bir kontrol imkanı sunar ve veri kaybı'nın yaşandığı tüm kritik kanalları tek bir yerden görüntülemenizi sağlar. DLP for Cloud Email çözümüyle sağlanan politikaların kullanılması, ayrıca normal uç nokta çözümlerinin kapsamına girmeyen tablet ve telefon gibi ek cihazlar konusunda da görünürlük sağlar.

Benzersiz ölçeklenebilirlik

Forcepoint DLP for Cloud Email çözümü, bulut tabanlı ve tam yönetimli bir çözüm olmanın avantajıyla bulut uygulamalarında bulunan kaynakların tüm esnekliğinden faydalanmanızı sağlar. Örneğin, herhangi bir zamanda giden e-postalarda büyük bir artış yaşanması durumunda, DLP for Cloud Email çözümü o anki iş yükü ihtiyaçlarının karşılanması için ayrılan kaynakların hızla artırılmasını ve ardından azaltılmasını sağlar. Ayrıca, ek donanım kaynaklarının uygulanmasını ve yapılandırılmasını gerektirmeden kurumunuzun artan ihtiyaçlarını karşılayacak sürekli bir DLP hizmeti sağlar.

Riske uyarlanabilir koruma

Forcepoint, sektörde riske ayarlanabilir DLP çözümü sunan ilk şirkettir. Çözüm, kullanıcı faaliyetlerini sürekli takip ederek çalışanlarınızı daha fazla iş yapmaları için özgür bırakır ve yalnızca yüksek riskli bir faaliyet veya riskli davranış modelleri tespit ettiğinde devreye girer. Otomasyon, kuralların neredeyse gerçek zamanlı olarak uygulanmasını sağlar; başka bir deyişle, ihlalleri öngörüp, gerçekleşmeden durdurabilir.

1 IDC, Worldwide Digital Loss Technologies Market Shares, 2020: DLP IS Dead, Long Live DLP, Doc # US48261521, Ekim 2021

Forcepoint DLP for Cloud Email Çözümleri

DLP for Cloud Email; dışarı aktarılan verilerin korunması

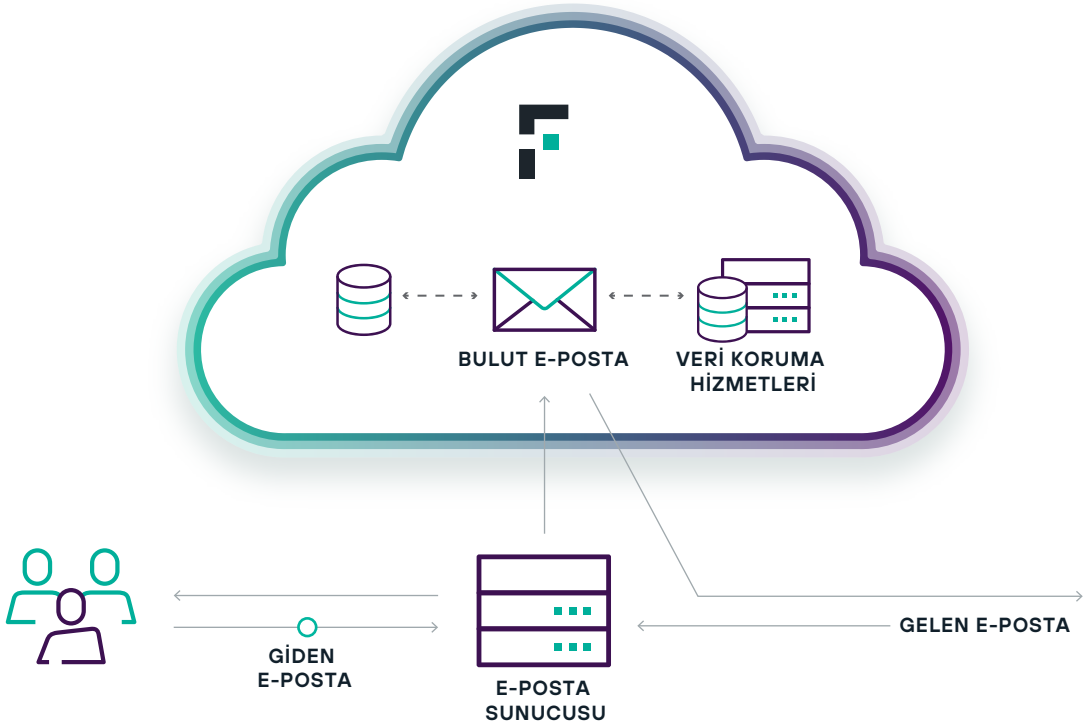
Forcepoint, giden e-postaların taranması için mevcut e-posta güvenliği tedarikçinizle uyumlu bir şekilde çalışarak DLP for Cloud Email çözümünün uygulanmasını basitleştirir. Forcepoint, DLP for Cloud Email Evrensel bağlantılarını kullanarak, Google ve Microsoft gibi popüler üçüncü taraf üreticilerin ürünlerini entegre eder ve giden e-postaların tamamını veya istenen kısmını Forcepoint Cloud'a yönlendirir. Bu noktada, Forcepoint DLP; e-postaları ön tanımlı DLP planınızda bulunan DLP politikaları ve eylemlerine uygun şekilde tarar. E-postalar gönderilmeden önce izin verme, karantinaya alma veya şifreleme (ayrı bir şifreleme modülüyle) işlemleri yapılabilir. Karantinaya alınan e-postalar için bildirimler gönderilebilir; bu e-postalar, yetkili bir yönetici tarafından serbest bırakılmadıkları sürece 30 güne kadar saklanacak şekilde yapılandırılabilir. Kurumların itibarının korunması için giden tüm e-postalarda istenmeyen e-posta, virüs ve kötü amaçlı yazılım taraması yapılır.

Standart özellikler:

- → **Virüs, kötü amaçlı yazılım** ve istenmeyen e-posta koruması sağlayan basit politika arayüzü
- → **Kontrol panoları, günlükler ve sunum raporları**
- → **Kişisel e-posta abonelikleri**

Eklentiler:

- → **Forcepoint Cloud Email Genişletilmiş Raporlama Geçmişi** (6, 12 ve 18 ay seçenekleri)
- → **Forcepoint Email Security Şifreleme Modülü**
- → **Forcepoint Email Security Görüntü Analizi Modülü**



forcepoint.com/contact