Forcepoint

Çözüm Özeti

Forcepoint E-Posta için Zero Trust Content Disarm and Reconstruction

Tehditlerden arındırılmış e-posta, basit ve saf

Zorluklar

- Kimlik avı saldırılarıyla mücadele - CISCO, 2021'de veri ihlallerinin %90'ının kimlik avından kaynaklandığını bildirdi.
- Sıfır gün saldırıları

Çözüm

- Zero Trust Content Disarm and Reconstruction (CDR) çözümüyle e-posta güvenliğinizi artırın: E-posta sınırlarını geçen içeriklerde bulunan bilinen ve bilinmeyen tehditleri ve sıfır gün saldırılarını durdurmanın tek yolu.

Faydaları

- Tehdidin tespit edilmesine veya kullanıcıların ihtiyaç duydukları iş içeriklerinden izole edilmesine gerek kalmadan tüm ağ sınırında tehditten arındırılmış, güvenli e-posta mesajları ve ekleri sağlar. Sıfır gün saldırıları, fidye yazılımları, steganografi saldırıları, dosyasız kötü amaçlı yazılımlar ve çok biçimli dosyalarda bulunan tehditlerin tamamı ortadan kaldırılır.
- Mevcut E-Posta Güvenliği Ağ Geçitlerinizle, istenmeyen e-posta filtreleriyle ve sınır antivirüs teknolojilerinizle birlikte çalışır ve sınır siber savunmalarınıza kusursuz bir şekilde entegre olarak içerik kaynaklı tehditlere karşı tam koruma için düşük riskli ve düşük maliyetli bir yol sağlar.

Normalde, kurumsal kullanıcılar iş yerlerinde hem kurum içerisindeki hem de internetteki kullanıcılarla e-posta mesajları paylaşabilir. E-postalar zengin içeriklere sahip olabilir ve kullanıcılar sıklıkla hem ekli dosyalar göndermekte hem de biçimlendirme, köprü bağlantıları, renkler, resimler ve ekler içeren mesajlar oluşturmak için HTML veya Zengin Metin biçimlerini kullanmaktadır. Bu da kurumları e-postaların zengin içeriklerine gizlenmiş kötü amaçlı yazılımlara maruz kalma riskiyle karşı karşıya bırakmaktadır.

Geleneksel e-posta güvenliği ağ geçitleri, potansiyel tehditlerin tespitine dayanmakta ve günümüzde görülen sofistike saldırılara karşı yetersiz kalmaktadır.

Bilinmeyen Tehditleri Ortadan Kaldırın

Mevcut çevre e-posta savunmaları ve ağ geçitleri (antivirüs, tehdit istihbaratı, korumalı alan ve istenmeyen e-posta filtrelerinin bir birleşimi), daha önce karşılaşılan tehditlerin imzalarını veya güvenli olmayan davranışları aramak suretiyle bilinen tehditleri tespit ederek ilk savunma hattını sağlamaktadır. Ancak, işletmelerin güvenliği, tespit tabanlı savunma yöntemleri tehdidi algılamadan önce kuruma sızan sıfır gün tehditleri veya daha önce görülmemiş ve dolayısıyla tespit dahi edilemeyen tehditleriyle sürekli olarak ihlal edilmekte.

E-Posta için Zero Trust CDR, tespit veya korumalı alan yöntemlerine dayanmadığı için e-posta sınırlarını geçen tüm bilinen ve bilinmeyen tehditleri ve sıfır gün saldırılarını ortadan kaldırmanın tek yoludur. Bunun yerine, tam koruma sağlamak için tespit yöntemi yerine benzersiz bir dönüşüm işleminden faydalanır.

E-Posta Güvenliğinizi Dönüştürün

E-Posta için Zero Trust CDR, sınır noktasında e-posta mesaj ve eklerinde bulunan iş bilgilerini çıkararak çalışır. Bu bilgileri taşıyan veriler tüm tehditlerle birlikte imha edilir. Ardından yepyeni mesaj ve ekler oluşturulup kullanıcıya teslim edilir. Bir uçtan diğerine, yalnızca güvenli içerikler ulaşabilir. Saldırganlar kuruma sızamaz ve işletme ihtiyaç duyduğu bilgilere erişir.

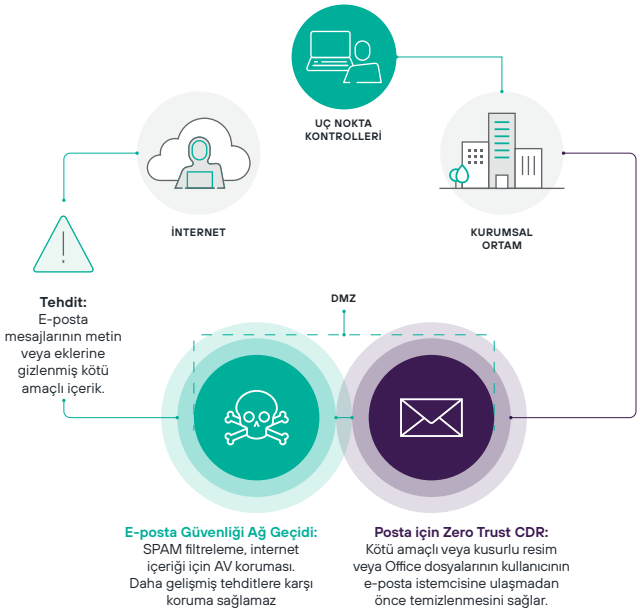
Bu işleme, dönüşüm adı verilmektedir. Üstesinden gelinemez; güvenlik ekibi, tehdit ortadan kaldırıldığı için mutludur. Şirket kullanıcıları da ihtiyaç duydukları bilgiye eriştikleri için memnundur.

Zero Trust CDR, içeriklerin tehditlerden arındırılmasını sağlamanın tek yoludur. Başarısız olmuş tehdit tespiti ve izolasyon paradigmalarından uzaklaşan Forcepoint'in benzersiz Zero Trust CDR teknolojisi, tüm verileri güvensiz veya zararlı olarak kabul eder; iyiyi kötüden ayırmaya çalışmaz.

Mevcut Savunmanızı Genişletin

E-Posta için Zero Trust CDR, mevcut E-Posta Güvenlik Ağ Geçidini ve E-Posta Sunucusunu e-posta metinlerinde ve en sık kullanılan ek dosya türlerinde (resimler, Microsoft Office belgeleri ve PDF dosyaları) bulunan tehditleri ortadan kaldıracak şekilde güçlendirir. E-Posta için Zero Trust CDR, tesis içine veya buluta kurulabilir.

E-Posta için Zero Trust CDR, gelen ve giden e-posta trafiği akışına ek bir bileşen yerleştirerek mevcut e-posta güvenlik kontrollerini tamamlar.



Kusursuz Entegrasyon

E-Posta için Zero Trust CDR, mevcut bir E-Posta Güvenlik Ağ Geçidinin kurumsal tarafındaki bir sunucuda çalışır. Gelen e-postalar, E-Posta Güvenlik Ağ Geçidinden E-Posta için Zero Trust CDR çözümüne yönlendirilir ve kurumsal posta sunucusuna teslim edilmeden önce tehditlerden arındırılmak için dönüştürülür.

İçerikle Gelen Kötü Amaçlı Yazılımların Kurumunuza Sızmasını Engelleyin

Office belgeleri, Adobe PDF dosyaları ve resimler, şu anda kötü amaçlı yazılım iletmek için en sık kullanılan yöntemlerdir. Bu dosya biçimlerinin ve bu dosyaları kullanan uygulamaların karmaşıklığı, saldırganlar için doğal bir hedef teşkil etmektedir. Siber suçlular, fidye yazılımlarından bankacılık Truva atlarına, uzaktan erişim kitlerine ve tuş kaydedicilere kadar hangi kötü amaçlı yazılımı kullanıyor olurlarsa olsunlar, sıfır gün tehditlerini gizleyebilecekleri en uygun yerin günlük iş belgeleri olduğunu bilir. Dosyasız kötü amaçlı yazılımlar ve çok biçimli dosyalar gibi teknikler, bu tehditlerin geleneksel tespit tabanlı siber güvenlik yöntemleriyle engellenmesini daha da zorlaştırmaktadır ve e-posta işletmelere sızmak için mükemmel bir vektördür. E-Posta için Zero Trust CDR, sağladığı benzersiz mesaj dönüşüm yöntemiyle şirket kullanıcılarının e-postalarını tam bir iç huzuruyla kullanabilmelerini sağlar. Her bir dosya ve resim, dönüşüm işleminden geçer ve tehditlerden arındırılır.

Uygulama Katmanı Proxy Sunucusu

E-Posta için Zero Trust CDR, SMTP için çift taraflı bir uygulama katmanı proxy sunucusu görevi görür. Kurumsal ağ ile harici sistemler arasında güvenli bir sınır oluşturur ve gelen e-postalara yönelik Posta Güvenliği Ağ Geçidi ve giden mesajlara yönelik e-posta sunucusu için akıllı bir ana bilgisayar görevi görür. MIME ve mesaj ekleri de dahil olmak üzere tüm içerik kurumsal ağa güvenli bir şekilde teslim edilmesini temin etmek üzere Zero Trust CDR tarafından dönüştürülür. Zero Trust CDR ayrıca tutulan şifre korumalı belgelere erişim için kullanıcı portal taleplerinin ve yanıtların dönüştürülmesi ve alınan şifre korumalı eklerin dönüştürülmesini gerçekleştirir.

E-Posta için Zero Trust CDR aldığı içeriği, bilgilerin dahili bir temsiline dönüştürür. Orijinal veriler imha edilir ve elde edilen bilgilerden yeni "güvenli" veriler oluşturulur. Bu şekilde, içerik yoluyla yapılan saldırılar (bilinmiyor olsalar dahi) ortadan kaldırılır ve bilgiler istenen alıcıya ulaştırılır. Bu işlem, dönüştürülen tüm içerikler için gerçekleştirilir.

Parola Korumalı Ekler

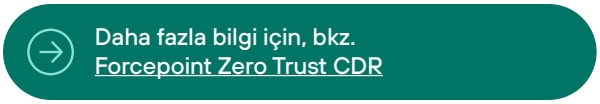
Bazı kurumlarda kullanıcılar daha sonra internet üzerinden birer ek olarak gönderilen dosyaları parola ile korumaktadır. Bu belgeler, dönüştürülüp tehditlerden arındırılamadıkları için potansiyel bir tehdit oluşturur.

E-Posta için Zero Trust CDR, iş ihtiyaçlarıyla güvenlik riskini dengelemek amacıyla parola korumalı ek içeren mesajları göndermeyecek veya mesajlardaki parola korumalı ekleri sansürleyecek şekilde yapılandırılabilir. Alternatif olarak, parola korumalı ekler göndermenin çok gerekli olduğu belirli kullanıcılar veya gruplar için dönüştürme işlemini atlayacak şekilde de yapılandırılabilir.

İmzalı ve Şifreli Mesajlar
İmzalı ve/veya S/MIME veya PGP ile şifrelenmiş mesajlar için gereken destek, ağ geçidi seviyesinde sağlanabilmektedir. Mesajlar ilk olarak Zero Trust CDR ile tehditlerden arındırılır, ardından ayrı bir Forcepoint koruma sunucusuna gönderilir ve burada imzalanır veya şifrelenir.

Makrolar ve Yürütülebilir İçerik
Bazı kurumlarda, kullanıcılar e-posta yoluyla makro özelliği açık Office belgeleri paylaşabilir. Makrolar yürütülebilir içerikler olduğu ve dönüşüm işlemiyle güvenli hale getirilemeyeceğinden bu belgeler potansiyel bir tehdit oluşturur.

E-Posta için Zero Trust CDR, iş ihtiyaçlarıyla güvenlik riskini dengelemek amacıyla Office makroları içeren mesajları göndermeyecek veya mesajlardaki Office makroları içeren ekleri sansürleyecek şekilde yapılandırılabilir. Alternatif olarak, makro özelliği açık Office belgeleri göndermenin çok gerekli olduğu belirli kullanıcılar veya gruplar için dönüştürme işlemini atlayacak şekilde de yapılandırılabilir.



forcepoint.com/contact