Forcepoint

Çözüm Özeti

Forcepoint Web Ağ Geçitleri için Zero Trust Content Disarm and Reconstruction

İnternette iç huzuruyla gezinme

Zorluklar

- İşletmelerin güvenliği, tespit tabanlı savunma yöntemleri tehdidi algılamadan önce kuruma sızan sıfır gün tehditleri veya daha önce görülmemiş ve dolayısıyla tespit dahi edilemeyen tehditleriyle ihlal edilmekte.
- İnternetten indirilen dosyalar, uygulamaların arızalanmasına ve saldırganların iş sistemlerinin kontrolünü ele geçirmesine neden olan tehditler içerebiliyor.
- İnternete yüklenen dosyalar, kurumların paylaşmak istemeyeceği kadar çok bilgi içerebiliyor ve fikri mülkiyet unsurlarını ifşa ederek işletmelere zarar verebiliyor.

Çözüm

- Forcepoint'in benzersiz Zero Trust CDR teknolojisi, tüm verileri güvensiz veya zararlı olarak kabul eder; iyiyi kötüden ayırmaya çalışmaz. Bu yaklaşım, gerçek bir Zero Trust çözümü sağlar.
- Zero Trust CDR, mevcut web savunmalarınıza anında entegre olabilir.

Faydaları

- Web sınırlarında her zaman güvenli ve tehditlerden arındırılmış içerik sağlar
- Bilinmeyen tehditleri ortadan kaldırın
- Web güvenliğinizi dönüştürün
- Tarama deneyiminizi zenginleştirin
- Kusursuz entegrasyon
- Kötü amaçlı yazılımları engelleyin
- Steganografi ile mücadele edin
- Benzersiz korumadan faydalanın

Kurumlar, bilgi paylaşmak, temel iş süreçleri için bilgi sağlamak ve işlemlerini gerçekleştirmek için internete bağımlıdır. Mevcut çevre web savunmaları (web ağ geçitleri ve güvenlik duvarları), iş belge ve resimlerine gizlenen bilinen ve bilinmeyen tehditlerle ve sıfır gün tehditleriyle baş edememektedir. Bu saldırı vektörü, kontrol altına alınmadığında işletmeler için yaşamsal bir tehdittir. Kullanıcıların indirdiği belge ve resimler, uygulamaların arızalanmasına ve saldırganların iş sistemlerinin kontrolünü ele geçirmesine neden olan tehditler içerebilmektedir. İnternete yükledikleri belge ve resimler de kurumların paylaşmak istemeyeceği kadar çok bilgi içerebilmekte ve fikri mülkiyet unsurlarını ifşa ederek işletmelere zarar verebilmektedir. Şu ana kadar bu tehdit akışını durdurmanın bir yolu bulunamamıştır.

Bilinmeyen Tehditleri Ortadan Kaldırın

Mevcut çevre web savunmaları, ağ geçitleri ve güvenlik duvarları, 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.

Web Ağ Geçitleri için Zero Trust Content Disarm and Reconstruction (CDR) çözümü, tespit veya korumalı alan yöntemlerine dayanmadığı için web 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.

Web Güvenliğinizi Dönüştürün

Web Ağ Geçitleri için Zero Trust CDR, web tarama akışındaki belge ve resimlerde bulunan iş bilgilerini çıkararak çalışır. Bu bilgileri taşıyan veriler tüm tehditlerle birlikte imha edilir. Ardından yepyeni belge ve resimler 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.

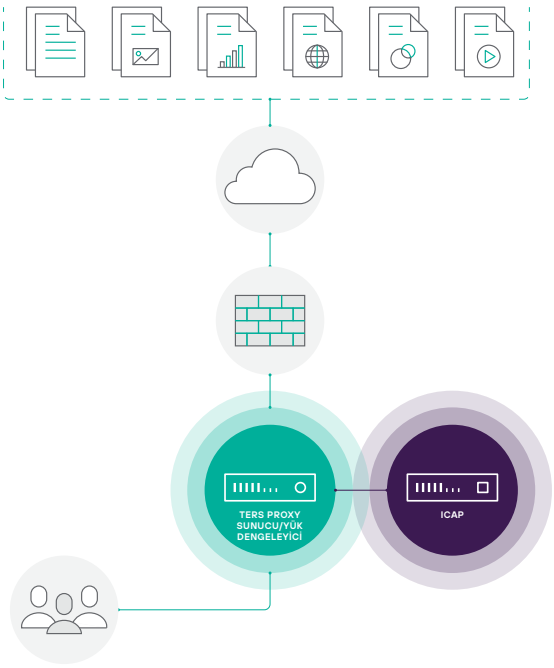
Tarama Deneyiminizi Zenginleştirin

Güvenlik ekipleri her zaman bir adım önde kalmayı başaran siber saldırganlarla mücadele ederken, bu mücadelenin zararını şirket kullanıcıları görmektedir. Hatalı pozitif sonuçlarla uğraşmak veya belgelerin kontrol edilip serbest bırakılmasını beklemek için harcanan zaman, iş süreçlerini sekteye uğratmakta ve verimi düşürmektedir. İşler kötü gittiğinde de düzeltme çalışmaları maliyetli ve zaman alıcı olmaktadır.

Web Ağ Geçitleri için Zero Trust CDR, kullanıcıların okumaları, paylaşmaları ve işlemeleri gereken iş bilgilerine hiçbir tehdit riski yaşamadan zamanında erişmelerini sağlayarak web ve sosyal medya deneyimini zenginleştirir.

Saf Dijital İçerik Sağlayın

Web ve sosyal medya kullanımı işletmelerin tüm bölümlerine bilgi sağlamaya devam ettiği için iletilen içeriklerin güvenli, saf ve tehditlerden arındırılmış olması her zamankinden daha önemlidir. Kullanıcılarının, iş ortaklarının ve müşterilerinin temiz ve saf iş içeriğine ulaşmasını sağlamak konusunda bir performans geçmişine sahip olan işletmeler, hızla hukuksuz bir siber ortam haline gelen bu dünyada farklılaşmayı başaracaktır.



Web Ağ Geçitleri için Zero Trust CDR çözümü de tam olarak bunu yapıyor: işletmelerin kullandıkları iş içeriklerinin tehditlerden arındırılmış olduğunu bilerek Web ve sosyal medya kullanımından fayda sağlamasına imkan tanıyor.

Mevcut Savunmalarla Kusursuz Entegrasyon

Web Ağ Geçitleri için Zero Trust CDR çözümü, endüstri standardı olan ICAP protokolünü kullanarak mevcut çevre web savunmaları, web ağ geçitleri ve uygulama güvenlik duvarlarıyla kusursuz bir şekilde entegre olur. Bir "yan uygulama" olarak kurulan çözüm, web ağ geçidi veya güvenlik duvarının belge ve resimleri ICAP üzerinden bir Forcepoint Gateway eXtension (GX) sunucusuna aktarılmasını, burada gizli tehditlerden arındırılacak şekilde dönüştürülmesini ve ardından kullanıcıya teslim edilmek üzere tekrar ağ geçidine iade edilmesini sağlayacak şekilde yapılandırılmıştır.

Mevcut web savunmalarıyla entegrasyon saniyeler içinde gerçekleşir ve süreci daha da kolaylaştırmak için pek çok popüler web ağ geçidi ve güvenlik duvarı için dahili entegrasyon dosyaları mevcuttur.

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 internet işletmelere sızmak için mükemmel bir vektördür.

Web Ağ Geçitleri için Zero Trust CDR çözümü, sağladığı benzersiz dönüşüm yöntemiyle şirket kullanıcılarının iş dosyalarını ve resimleri tam bir iç huzuruyla indirmesini ve yüklemesini sağlar. Her bir dosya ve resim, dönüşüm işleminden geçer ve tehditlerden arındırılır.

Resim Steganografisinde Gizli Veri Kayıplarını Engelleyin

Steganografi, verilerin görünüşte zararsız olan dosyalara saklanmasıdır. Taşıyıcı adı verilen bir mesajın içerisine yalnızca istenen alıcının okuyabileceği gizli bir mesajın kodlanmasını içeren bir yöntemdir. Siber saldırganların steganografiyi bir silah haline getirmek için kullandıkları ve günümüzde Stegware adı verilen bu yöntem gitgide daha sık kullanılmaktadır. Karanlık Ağda (Dark Web) sunulan hizmet olarak kötü amaçlı yazılımlarda varsayılan çözüm olarak sunulmaktadır. Binlerce kullanıcıdan para sızdırmak ve saygın haber sitelerine diz çöktürmek için kötü amaçlı yazılım saldırılarında kullanılmıştır. Ayrıca, görünüşte zararsız olan resimlere gizlenmiş yüksek değerde finansal varlıkların çalınması için sosyal medya web siteleriyle birlikte de kullanılmıştır. Steganografinin tespit edilmesi imkansız olduğundan, tüm bunlar güvenli olmayan verileri tespit eden araçları kullanan BT profesyonelleri için kötü haberlerdir.

Web Ağ Geçitleri için Zero Trust CDR çözümü, internette gezinen veya sosyal medya üzerinden iletişim kuran kullanıcıların gördüğü her görüntünün Stegware kullanılarak gizlenmiş her türlü içerikten arındırılmasını sağlar. Dönüşüm işlemi, tüm gizli içeriği yok ederek resmi saldırgan için faydasız hale getirir. Web Ağ Geçitleri için Zero Trust CDR çözümü, resim steganografisi yoluyla gizli veri kayıplarını tamamen engellediğinden, Genel Veri Koruma Yönetmeliği (GDPR) gibi mevcut veri kaybı önleme ve yönetim girişimlerini güçlendirir.

Komuta ve Kontrol Kanallarını (CnC) Bozun

En sofistike ve tehlikeli siber saldırılar, genellikle uzaktaki saldırganla şirket ağının içerisindeki iş istasyonları arasında bir Komuta ve Kontrol Kanalı (CnC) oluşturmayı içerir. Bu kanallar genellikle güvenliği önceden ihlal edilmiş bir iş istasyonu, uzaktaki bir sunucuyla temas kurduğunda (ör. bir sosyal medya sitesindeki bir resim aracılığıyla) veya daha önceden bilinmeyen bir kötü amaçlı yazılım meşru bir iş dosyası kisvesiyle sisteme sızdığında oluşur.

Web Ağ Geçitleri için Zero Trust CDR çözümü, bir CnC oluşturma çabalarını boşa çıkartır. Dönüşüm işlemi, belgelerde, internette ve sosyal medyadaki resimlerde gizli olabilecek her türlü tehdidi ortadan kaldırır. Bir adli kontrol panosu, belge ve resimlerin "önceki ve sonraki" hallerinin görülmesini sağlayarak, şüpheli davranışların belirlenmesine ve ilgili kullanıcıların sorumlu tutulmasına yardımcı olur.

Kazanan bir Çözüm Oluşturmak

Forcepoint çözüm ekibi, Forcepoint bayi ortaklarıyla birlikte Zero Trust CDR teknolojisine yaptığınız yatırımdan maksimum fayda sağlamanıza yardımcı olan pek çok profesyonel hizmet sunmaktadır. Web Ağ Geçitleri için Zero Trust CDR çözümünüzün kapsamını belirlemenize, çözümü planlamanıza, kurmanıza, yapılandırmanıza ve yönetmenize yardımcı olabiliriz.

Forcepoint Teknik Destekle kurulum sırasında ve sonrasında her şeyin sorunsuz çalıştığından emin olun. Yetenekli çözüm ekibimiz, büyük bir uzmanlığa ve geniş bir bilgi ağına sahiptir ve kurum içi ekibinizin doğal bir uzantısı olarak hareket edebilir.

Özet: Benzersiz Korumadan Faydalanın

Teknolojik bir devrimin eşiğindeyiz. Acımasız ve konsantre siber saldırılarla karşı karşıya olan kurumlar, dijital ortamda veri toplama, paylaşma ve işlem yapma yöntemlerini her açıdan yeniden değerlendirmeye zorlanmakta.

Daha fazla bilgi için, bkz.
Forcepoint Zero Trust CDR

forcepoint.com/contact