# Forcepoint Zero Trust Content Disarm and Reconstruction

Bilinen ve bilinmeyen tehditleri, sıfır gün saldırılarını ve kötü amaçlı yazılımları durdurun

Forcepoint

Broşür

# Forcepoint Zero Trust Content Disarm and Reconstruction

## Bilinen ve bilinmeyen tehditleri, sıfır gün saldırılarını ve kötü amaçlı yazılımları durdurun

Teknoloji; e-posta gönderip almaktan web ve sosyal medyadaki etkileşimlere, dosya yüklemeye ve web uygulamalarına kadar her kurum için hayati dijital bilgiler üretmektedir. Bu dijital bilgiler; iş ortakları, müşteriler, tedarik zincirleri, yerel iş gücü ve uzaktan çalışanlarla paylaşılmaktadır. Bilgilerin bu ölçekte paylaşılması, siber suçluların günlük dosya, belge ve resimlere gizlenen kötü amaçlı yazılımlar yoluyla suistimal edebileceği çok büyük bir saldırı yüzeyi oluşturmaktadır.

Bu duruma tepki olarak, sorunu çözmeye çalışan savunma teknolojilerinin sayısında da artış yaşanmaktadır. Ancak tüm bu savunma yöntemleri, belli bir düzeyde tespit kavramına dayanmaktadır. Tespit temelli savunma yöntemlerinin sorunu, yalnızca daha önce "görmüş oldukları" unsurları tespit edebilmeleridir. Bu savunma yöntemlerini güçlendirmek için çalışmalar yapılmıştır. Korumalı alanlar faydalı olabilse de saldırganlar bu ortamları nasıl tespit edebileceklerini öğrenmiştir ve tehditlerin belirlenebilmesi için halen tespit yöntemi kullanılmaktadır. Yapay Zekâ ve Makine Öğrenimi algoritmaları faydalıdır ancak aslında yaptıkları şey, daha önce karşılaşılan tehditleri daha hızlı tespit etmek için bilgi işlem gücünden faydalanmaktadır. Siber suçlular, bu gelişmelere yanıt olarak kurumlara savunma yöntemlerinin daha önce karşılaşmadığı, dolayısıyla da güvenli olarak gördüğü kötü amaçlı yazılımlarla saldırmayı denemektedir.

## Tespit tabanlı savunma yöntemleri, tek başına yeterli değildir.

Forcepoint Zero Trust Content Disarm and Reconstruction (CDR), farklı bir çözümdür. Kötü amaçlı yazılımları tespit etmeye çalışmak yerine, hiçbir şeye güvenilmeyeceği varsayımıyla çalışır. Çalışma prensibi, dosyalardaki geçerli iş bilgilerinin çıkarılması (ve orijinal dosyanın imha edilmesi veya saklanması), çıkarılan bilgilerin doğru yapılandırılmış olduğunun doğrulanması ve ardından bilgileri hedeflenen yere ulaştıracak yeni ve tamamen işlevsel dosyaların oluşturulması şeklindedir. Zero Trust CDR, en gelişmiş sıfır gün saldırılarını da içeren tüm tehditlere karşı mücadele için bir devrim niteliğindedir. Bu şekilde tespitten önlemeye geçilmesi, karma iş gücü ve dijital dönüşüm konusunda son zamanlarda yaşanan evrim ile içerik ve elektronik bilgilerin her yerden kullanılmakta olduğu düşünüldüğünde daha da önem kazanmaktadır.

## Kötü amaçlı yazılım engelleyici savunma yöntemleri:

- Kullanıcıların kurum dışından gelen dosyaları güvenle açabilmesi için **her zaman güvenli ve tamamen işlevsel içerikler sağlamalıdır**.
- Savunma sağlamak için en son yama veya imzalara ihtiyaç duymadan **sıfır gün tehditlerini durdurmalıdır**.

## Korunması gereken saldırı vektörleri:

- **Web taraması**
- **İnternetten dosya indirme**
- **Web posta**
- **Sosyal medya**
- **Dosya yükleme**
- **Posta**
- **Web uygulamaları**
- **Dosya paylaşımı**

Kötü amaçlı yazılım içermeyen veriler

Aslına uygun, tamamen revize edilebilir dosyalar

Sıfır hatalı pozitif sonuç

Gecikme yaşanmaması

## Her tehdidin durdurulması

Dijital içerikler, siber suçluların kötü amaçlı yazılım saldırıları ve açıklardan yararlanma için tercih ettiği vektördür. Daha önceden bilinen tehditler, sıfır gün saldırıları ve tamamen tespit edilemeyecek durumda olan tehditler dahil olmak üzere pek çok tehdit, her gün kullandığımız dosya ve resimlere gizlenerek web taramasından e-postaya, dosya yüklemeye ve sosyal medyaya kadar tüm dijital içeriklere rutin bir şekilde sirayet etmektedir.

25 yıldan uzun bir süredir, bu tehditlerle mücadele için kullanılan standart yaklaşım, tespit tabanlı siber savunmaların kullanılmasıydı. Buradaki sorun, tespitten kaçınmanın kolay olması. Tehdidin imzasını değiştirdiğiniz anda, kötü amaçlı yazılımlar güvenlik sınırlarını rahatça aşmakta. Tespit yöntemi, artık kullanıcıları bilinen ve bilinmeyen tehditlerden, sıfır gün saldırılarından ve kötü amaçlı yazılımlardan korumak için tek başına yeterli olamamakta.

Forcepoint Zero Trust CDR, tespit yöntemini kullanmadan dosya tabanlı kötü amaçlı yazılımların kurumlara sızmasını önlüyor. Sıfır Güven CDR'nin kötü unsurları tespit etmeye çalışmadan yalnızca dosyalardaki iyi unsurları çıkarıp teslim etmeye dayanan benzersiz yaklaşımı, kullanıcıların sıfır gün saldırıları ve bilinmeyen kötü amaçlı yazılımlardan da korunmasını sağlamaktadır. Bu kötü amaçlı yazılım engelleme yaklaşımı, en yeni ve sıfır gün kötü amaçlı yazılım imzalarıyla sürekli güncelleme gerektirmediğinden, savunma her zaman güncel kalmaktadır.

## Kullanıcı deneyimini iyileştirmek

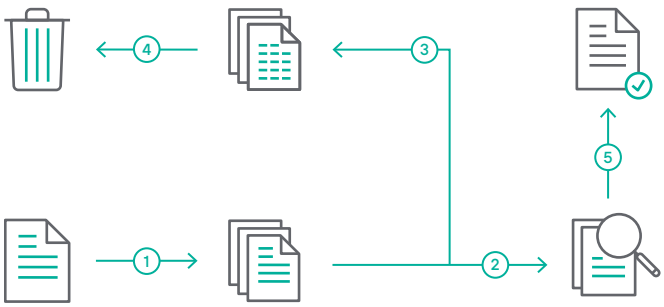
Kurumlar, gizli kötü amaçlı yazılım sorununa sürekli yeni ve daha etkili çözümler ararken, kullanıcı deneyimini olumsuz etkileme riskiyle karşı karşıyadır. Gelen dosyaların birden fazla virüs tarayıcısından geçirilmesi veya daha fazla inceleme yapılana kadar beklemeye ve korumalı alana alınması, iş süreçlerinde gecikmelere neden olabilmektedir. Dosyaların "düzleştirilerek", yani orijinal düzenlenebilir biçimlerinden sabit ve düzenlenemez bir biçime dönüştürülerek güvenli hale getirilmeye çalışılması, iş kullanıcılarını kolayca paylaşılamayan, düzenlenemeyen veya güncellenemeyen dosyalarla çalışmak zorunda bırakmaktadır. Çoğu durumda niyet iyi olsa da nihai sonuç, iş süreçlerinin yavaşlaması ve kullanıcıların gitgide daha fazla hüsrana uğramasıdır.
Forcepoint Zero Trust CDR, güvenlikten taviz vermeden kullanıcı deneyimini iyileştirir. Zero Trust CDR süreci, tespit yöntemini kullanmadığından, sistemin dosyaları taraması ve bilinen tehditleri tespit etmeye çalışması için bir bekleme süresi gerekmez. Korumalı alan kullanmadığından, kritik iş süreçlerinde dosyaların inceleme için izole edilmesinden kaynaklanan büyük gecikmeler yaşanmaz. Zero Trust CDR, saniyenin küçük bir bölümünde çalışır ve işletmelerin hem güvenli olan hem de gecikme olmadan kullanılabilen bilgi ihtiyacını karşılar. Kullanıcıların ihtiyaç duydukları dosyalara erişim hızını etkilemeyen Zero Trust CDR, kullanıcı deneyimini iyileştirir ve her seferinde kötü amaçlı yazılım içermeyen, orijinalinin aynısı ve tamamen düzenlenebilir dosyalar sunar.

## SOC ekibinizi serbest bırakın

En iyi tespit tabanlı savunma yöntemleri kullanılsa dahi, pek çok güvenlik operasyon merkezi (SOC) ekibi, gelen dosyalara gizlenen kötü amaçlı yazılımların neden olduğu siber güvenlik olaylarını tespit etmek, analiz etmek, önlemek ve bu olaylara yanıt vermek için çok fazla zaman ve para harcamaya devam etmektedir.

Forcepoint Zero Trust CDR, SOC ekibinin karantina sıralarını ve hatalı pozitif sonuçları yönetmek, imza güncellemelerini uygulamak ve potansiyel ihlal uyarılarıyla uğraşmak gibi günlük zahmetli işlerden kurtarmaktadır. Kötü amaçlı yazılım içersin veya içermesin, gelen her dosya Zero Trust CDR sürecine tabidir ve her dosya tehditlerden arınmış bir şekilde yeniden oluşturulur.

## Nasıl çalışıyor?




1. Zero Trust CDR, bilinen kötü amaçlı yazılımları tespit etmek yerine, verileri alır ve içerdikleri faydalı bilgileri çıkarır.
2. Çıkarılan bilgiler, geçici bir biçime dönüştürülür ve doğrulanır.
3. Bu gelişmiş tehdit önleme süreci, hiçbir tehdit veya saldırının bir sonraki aşamaya ulaşamamasını sağlar.
4. Orijinal veriler saklanır veya bilinen veya bilinmeyen kötü amaçlı yazılımlarla birlikte imha edilir.
5. Oluşturulan yeni veriler, doğrulanan bilgileri de içerecek normalleştirilmiş bir biçimde yeniden oluşturulur. Yeni veriler, orijinal verilerin aynısıdır ve yerleşik kötü amaçlı yazılım tehdidi içermedikleri için güvenli olmaları garantidir.

## Benzersiz koruma

- Tehditlerden arındırıldığı garantilenen veriler sunar - orijinalinin tamamen aynısıdır ve tamamen düzenlenebilir.
- En karmaşık saldırılar dahi bir risk oluşturmaz.
- "Sıfır gün" tehditlerine maruz kalma riski yoktur.

## Çok yönlüdür

- Mevcut sınır savunma ve teknolojileriyle birlikte çalışır.
- Tüm Office dosyaları, resimler ve PDF (saldırganlar tarafından en sık kullanılan biçimler) dahil olmak üzere en popüler dosya biçimlerini dönüştürür.
- Web, e-posta ve dosya yükleme dahil pek çok saldırı vektöründe koruma sağlar.

## Kurulum seçimi

- Tesis içi, sanal ve bulutta kurulum seçenekleri.
- Dakikalar içerisinde kurulup çalışmaya başlayabilir.

## Ek A. Çözüm bileşenleri hakkında genel bilgi

| | |
|---|---|
| Web Ağ Geçitleri için Forcepoint Zero Trust CDR | Web Ağ Geçitleri için Forcepoint Zero Trust CDR, web kullanıcılarını internetten indirilen dosyalarda, web posta ve sosyal medyada gizli olan kötü amaçlı yazılımlardan korur. Ağ sınırına kurulur ve mevcut Secure Web Gateway (SWG) çözümüne entegre olur. Web Ağ Geçidindeki politika kuralları, hangi dosya türlerinin işlenmek için Forcepoint Zero Trust CDR'ye aktarılacağını belirler. |
| Uzaktan Tarayıcı İzolasyonu için Forcepoint Zero Trust CDR | Uzaktan Tarayıcı İzolasyonu için Forcepoint Zero Trust CDR, interneti Uzaktan Tarayıcı İzolasyonu ile tarayan kullanıcıların hiçbir şekilde kötü amaçlı yazılım içermediklerinden emin olarak dosyaları fiziksel makinelerine güvenle indirebilmesini sağlar. |
| Dosya Yükleme için Forcepoint Zero Trust CDR | Dosya Yükleme için Forcepoint Zero Trust CDR, kurumu internetten yüklenen dosyalarda bulunan kötü amaçlı yazılımlara karşı korur ve ters web proxy sunucuyla birlikte veya bulut tabanlı bir web uygulamasının bir parçası olarak kurulabilir. |
| E-posta için Forcepoint Zero Trust CDR | E-posta için Forcepoint Zero Trust CDR, kullanıcıları e-posta mesajlarında ve eklerinde gizli olan kötü amaçlı yazılımlardan korur. Genelde sınır e-posta savunması ile kurumun e-posta sunucusunun arasına kurulur. |
| Dosya Paylaşımı için Forcepoint Zero Trust CDR | Dosya Paylaşımı için Forcepoint Zero Trust CDR, farklı ağlardaki dosya havuzları arasında aktarılan dosyalarda dosya tabanlı kötü amaçlı yazılım olmamasını sağlar. |
| Web Uygulamaları için Forcepoint Zero Trust CDR | Web Uygulamaları için Forcepoint Zero Trust CDR, ağlar arasında aktarılan yapılandırılmış verilerin önceden tanımlanan taslaklara uygun olmasını ve dolayısıyla saldırı vektörü olarak kullanılamamasını sağlar. |
| Forcepoint Zero Trust CDR - Bulut API'leri | Forcepoint Zero Trust CDR, tesis içerisine kurulmanın yanı sıra, içerik devre dışı bırakma ve yeniden oluşturma çözümünü Web uygulamalarına ve iş akışlarına entegre etmek zorunda olan geliştiriciler için bulut tabanlı API'ler yoluyla da sunulmaktadır. |

## Ek B. Forcepoint Zero Trust CDR ile tehditlerden arındırılan dosya türleri

Aşağıdaki dosya türleri, Forcepoint Zero Trust CDR tarafından dönüştürülür ve tehditlerden arındırılır:

| OFFICE DOSYALARI | |
|---|---|
| **DOSYA TÜRÜ** | **UZANTI** |
| Bitmap resim | BMP |
| Microsoft Office X Belgesi | DOCX |
| Microsoft güçlendirilmiş meta dosyası | EMF |
| E-posta mesajı | EML |
| GIF resim | GIF |
| HTML dosyası | HTML |
| ICAL dosyası | ICAL |
| JPEG 2000 | JP2K |
| JPEG resim | JPEG |
| MIME HTML Arşivi | MHT |
| Çok Amaçlı İnternet Posta Uzantıları | MIME |
| Adobe PDF | PDF |
| PNG resim | PNG |
| Microsoft Office X PowerPoint | PPTX |
| Zengin Metin | RTF |
| Düz Metin | TXT |
| TIFF resim | TIFF |
| Microsoft Windows meta dosyası | WMF |
| Microsoft Office X Excel | XLSX |
| Zip arşivi | ZIP |

| YAPILANDIRILMIŞ VERİ DOSYALARI | |
|---|---|
| **DOSYA TÜRÜ** | **UZANTI** |
| Virgülle ayrılmış değerler | CSV |
| JSON yapılandırılmış veri | JSON |
| Google Protocol Buffers 3 | Proto3 |
| XML yapılandırılmış veri | XML |

Aşağıdaki dosya türleri de öncelikle ara bir biçime dönüştürülerek tehditlerden arındırılır:

| BİÇİM | ORİJİNAL | DÖNÜŞ-TÜRÜLMÜŞ | NİHAİ |
|---|---|---|---|
| Eski Microsoft Word | DOC | DOCX | DOC |
| Eski Microsoft PowerPoint | PPT | PPTX | PPT |
| Eski Microsoft Excel | XLS | XLSX | XLS |
| OpenDocumentText | ODT | DOCX | ODT |
| OpenDocument Spreadsheet | ODS | XLSX | ODS |
| OpenDocument Presentation | ODP | PPTX | ODP |
| Zengin Metin | RTF | DOCX | RTF |
| eXtensbile Paper Specification | XPS | PDF | XPS |
| EPUB kitap okuyucu biçimi | EPUB | PDF | EPUB |
| Mobipocket e-kitap biçimi | MOBI | DOCX | - |
| Bilgisayar Grafik Meta Dosyası | CGM | PDF | - |
| Adobe Photoshop | PSD | PNG | PSD |
| Microsoft One Note | ONE | PDF | - |
| AutoCAD Çizimi | DWG | PDF | - |
| Eski AutoCAD Çizimi | DXF | PDF | - |
| Eski Microsoft Visio | VSD | PDF | - |
| Microsoft Visio | VSDX | PDF | - |
| XLS Biçimlendirme Nesnesi | FO | PDF | - |
| 7Zip arşivi | 7Zip | ZIP | 7Zip |
| BZip2 Arşivi | BZip2 | ZIP | BZip2 |
| GZIP Arşivi | Gzip | ZIP | GZip |
| Z Arşivi | Z | ZIP | Z |
| TAR Arşivi | TAR | ZIP | TAR |
| Microsoft CAB arşivi | CAB | - | ZIP |

Forcepoint

**forcepoint.com/contact**

## Forcepoint hakkında

Forcepoint, dijital dönüşüm ve büyüme sağlarken kurumları koruması için güvenilen, kullanıcı ve veri koruma alanında lider siber güvenlik şirketidir. Forcepoint'in uyumlu çözümleri, insanların verilerle etkileşime girme şekillerine gerçek zamanlı olarak uyum sağlar ve erişim güvenliği sağlarken, çalışanların değer üretmesine de imkan tanır. Genel merkezi Teksas, Austin'de bulunan Forcepoint, dünya çapında binlerce müşteri için güvenli ve güvenilir ortamlar yaratmaktadır.


[FP-Zero Trust CDR-Brochure-TR] 10Mar2022