FireEye

FireEye | Siber Saldırılarla Savaşan Tehdit Önleme Platformları

## Ağ Güvenliği

### NX Serisi

**Öne Çıkanlar**

•in-line (engelleme/izleme konu-munda) veya out-of-band (TCP rest konumu/izleme konumu) olarak görevlendirilebilir
•PDF'ler, Flash, multimedya formatları ve ZIP/RAR/TNEF arşivleri de dahil olmak üzere şüpheli tüm WEB objelerini analiz etmenin yanı sıra verilerin dışarı sızmasına engel teşkil etmek amacıyla outbound kötü niyetli yazılımı bloke eder.
•Hadise tepkisi önceliklendirmesinin daha etkin şekilde yapılabilmesi için FireEye AV Suite'i ile entegre olur.
•Harmanlanmış "spear-phishing" saldırılarının durdurulmasını teminen FireEye EX Serisi ile entegre olur.
•FireEye Dynamic Threat Intelligence (DTI) bulutu üzerinden, yerel olarak FireEye dağıtımının tamamına ve küresel olarak tüm FireEye müşteri tabanına tehdit istihbaratını dağıtır.
•Yerel otantikasyonun yanısıra uzak üçüncü taraf AAA şebeke hizmet erişimini de desteklemektedir.

## Eposta Güvenliği

### EX Serisi

**Öne Çıkanlar**

•Spear-phishing niteliğindeki e-posta saldırılarına karşı koruma sağlar
•Çoklu tehdit vektörleri üzerinden harmanlanmış saldırıları durdurmak amacıyla FireEye NX ile entegre edilebilir
•zero-day exploit'leri , ZIP,RAR,TNEF arşivlerinin içerisine gizlenmiş saldırılar ve kötü niyetli URL'ler gibi tehditler açısından e-postaları analiz eder
•Anti-spam ve e-posta ağ geçidi gibi unsurları içeren mevcut e-posta kontrol altyapısını tamamlar
•MTA olarak aktif koruma konumunda, veya (SPAN/ BCC) olarak monitor konumunda çalışır
•Opsiyonel kullanıcı bildirimleri yoluyla kötü niyetli e-postaları karantinaya alır.

### Bulut Tabanlı E-posta Tehdit Önleme Platformu

E-posta Saldırılarını Tespit Eden, Analizini Yapan ve Engelleyen Bulut-Tabanlı Platform

**Genel Bakış**

FireEye® E-posta Tehdit Önleme Bulut Tabanlı Platformu günümüzün gelişmiş e-posta saldırılarıyla mücadele eden, spam ve virüs karşıtı koruma sağlayan bir SaaS çözümüdür.

E-posta Tehdit Önleme Bulut Tabanlı Platformu, e-posta ihtiyaçlarında bulut platformunu benimseyen kurumların bulut posta kutularına yönelik, eksiksiz bir e-posta güvenliği sunmaktadır. Kurumların karşılaştıkları e-posta tabanlı istenmeyen e-posta, virüs ve gelişmiş tehditlerin sayısı gitgide artmaktadır.
E-posta tabanlı saldırılar, özellikle de kimlik hırsızlığı tespit edilmelerinde yaşanan güçlükler nedeniyle, gelişmiş ısrarcı tehditlerin (advanced persistent threat-APT) başlatılmasında kullanılan temel yöntemlerden biri olarak kalmıştır.

Kurumların kötü niyetli e-postalara karşı koruma sağlamak amacıyla tek yapması gereken, mesajları E-posta Tehdit Önleme Bulut Tabanlı Platformu'na yönlendirmektir. Bulut, e-postaları ilk olarak istenmeyen e-posta (spam) ve bilindik virüsler açısından analiz etmektedir. Sonrasında ise imzasız (signature-less) FireEye Multi-vector Virtual Execution™ (MVX) motorunu kullanarak, e-postanın tüm eklerinin ve URL'nin analizini yapmakta, gerçek zamanlı olarak tehditleri tespit edip, APT saldırılarını durdurmaktadır.

## Dosya Sistemi ve Yedekleme

### FX Serisi

**Öne Çıkanlar**

•-Geleneksel AV motorları vasıtasıyla saptanamayan gizli/örtük kötü niyetli yazılımı bulur.
-Aktif karantina konumunda (koruma modu) ya da sadece analiz konumunda (izleme modu) konuşlandırılabilir.
-CIFS ve NFS uyumlu dosya paylaşımlarının yinelemeli olarak, planlı olarak ve istendiği anda denetlenebilmesine olanak sağlar.
-PDFler, Microsoft Office dokümanları ve multimedya dosyaları gibi geniş bir yelpazeye yayılan dosya türlerinde analiz yapılmasına olanak sağlar.
-Hadise tepkisi önceliklendirmesi ve isimlendirme geleneklerinin daha etkin şekilde yapılabilmesi için FireEye AV Suite'i ile entegre olur.
-Tehdit verilerini, FireEye CM ve FireEye
DTI bulutu üzerinden FireEye platformlarıyla paylaşır.

## Merkezi Yönetim

### CM Serisi

Dinamik Tehdit İstihbaratının Gerçek Zamanlı Değiş Tokuşu ve Kurum Uygulamalarının Konsolide Yönetimi

**Öne Çıkanlar**

•Çoklu platform uygulamalarına yönelik entegre kontrol imkanı sağlar.
•Çoklu vektör korelasyonu sayesinde harmanlanmış bir tehdit önleme olanağı tanır.
•60 dakikadan daha kısa bir sürede konuşlandırılabilen, amaca uygun bir platform sağlar.
•Hedeflenen saldırıdan korunmaya yönelik gelişmiş bir konum sağlayan ve tek bakışta anlaşılabilen bir güvenlik panosu sunar.
•Konsolide güvenlik vakası deposu üzerinden yapılan raporlama ve denetimleri hızlandırır.
Çoklu FireEye platformlarının yönetimini daha etkin hale getirerek konfigürasyonların yönetimine, tehdit güncellemelerine ve yazılım iyileştirmelerine harcanan zamanı azaltır.

FireEye

**FireEye** **Siber Saldırılarla Savaşan Tehdit Önleme Platformları** FireEye

# Uç Nokta

## Uç Nokta Güvenliği; HX Serisi

Uç Nokta'da Yaşanan Güvenlik Vakalarını Tespit Eden, Analizini Yapan ve Çözüme Ulaştıran Uç Nokta Tehdit Önleme Platformudur.

Güvenli Şebekeler oluşturarak saldırganları IT ortamlarından uzak tutmak ve tehditleri önlemek isteyen kurumlar, birinci sınıf güvenlik ekiplerini bünyelerinde çalıştırabilmek için milyonlarca dolar harcamaktadır. Ancak tüm bu yatırımlara rağmen, azimli ve kararlı birtakım saldırganlar kurumların içine sızmayı başararak fikri haklarını ve finansal varlıklarını çalabilmektedir.

Uç Nokta Tehdit Önleme Platformu; güvenlik ekiplerine, vakaları, geleneksel yaklaşımlarla kıyasla oldukça kısa sürede ve güvenli bir şekilde, tespit etme, analizini yapma ve çözüme ulaştırma olanağı sunmaktadır.

Gelişmiş saldırganları ve APT'leri Arama
Gizlilik İhlal Göstergeleri'nin anasistem tabanlı şekilde tespiti sayesinde, gelişmiş saldırganlar ve gelişmiş ısrarcı tehditler (advanced persistent threat-APT'ler) de dahil olmak üzere AV'nin kaçırdığı tehditler tespit edilebilmektedir. Gizliliği ihlal edilmiş bir aygıt Gizlilik İhlal Göstergesi (IOC) tarafından tespit edildiğinde kullanıcılar durumdan derhal bilgilendirilmektedir.

### Uç Nokta Delil Karartma (Forensics)

Mandiant Akıllı Yanıt (Mandiant Intelligent Response (MIR)

Gizliliğiniz ihlal mi edildi? Saldırgan içeriye nasıl sızdı? Hangi sistemler işin içinde? Mandiant Akıllı Yanıt bu sorulara cevap vermenize olanak tanıdığından, anında müdahale etmeniz ve gelişmiş saldırganları sisteminizdeki hedeflerine ulaşmaktan alıkoymanız mümkün olmaktadır.

Uç Noktaların Gizliliği İhlal Kanıtlarına Yönelik Olarak Taranması
Kötü niyetli yazılımlar, kötücül yazılımlara dair genel davranışlar ve kötücül olmayan saldırgan taktikleri de dâhil olmak üzere, uç noktalarınızın tamamını gizlilik ihlal kanıtları açısından tarar.

# Mobil Güvenlik

## Mobil Tehdit Önleme

Mobil cihazları güçlü birer suç aleti haline getiren casusluk, profil çıkarma ve siber saldırıların tespiti ve önlenmesi
Kötü niyetli mobil uygulamalar kullanılarak; kişi listeleri ve takvime bağlı program detayları gibi birtakım kişisel bilgilere ve kamera ve mikrofon gibi birtakım mobil cihaz özelliklerini yöneterek, casusluk yapmak, profil çıkarmak veya siber saldırıları yapabilmek mümkün olabilmektedir.

FireEye Mobil Güvenlik (Mobil Tehdit Önleme), yukarıda bahsedilen türden mobil tehditleri tespit edip, önleyebilme olanağı sunmanın yanı sıra, kurum çapındaki tüm mobil güvenlik eğilimlerine de bir görünebilirlik kazandırmaktadır. FireEye Mobil Tehdit Önleme aynı zamanda sektörün önde gelen mobil cihaz yönetim (MDM) sağlayıcılarıyla da entegre olabilmektedir.

# Kurumsal Adli Bilişim

## PX ve IA Serileri

Siber güvenlik ihlallerine ilişkin en son haberlerin de ortaya çıkardığı üzere, herhangi bir güvenlik vakasının etkisini en aza indirgemenin en önemli unsurları erken tespit ve hızlı araştırmadır. Her iki unsur için de, güçlü adli bilişim kabiliyetlerine gereksinim duyulmaktadır. Bir kurum, saldırıya uğradığında, saldırı vakasını hızlı bir şekilde araştırabilme, vakanın kapsam ve etkisini yine aynı hızla tespit edebilme yeteneklerine sahip olmalıdır. Tehdidi ancak böylelikle etkin bir şekilde kontrol altına alabilir ve şebekelerini tekrar güvenli hale getirebilirler

FireEye Network Forensics Platform (Ağ Adli Bilişim Platformu-PX serisi) ve Investigation Analysis system (Araştırma Analiz-IA serisi) sistemi, güçlü bir kombinasyon oluşturarak, merkezileştirilmiş analiz ve görselleştirme yoluyla sektörün en hızlı ve kayıpsız ağ verisi yakalama ve geri kazanma çözümünü bir arada sunmaktadır. Araştırma çalışmalarına yardımcı olan analiz araçları sayesinde yüksek performanslı paket yakalama özelliği ise diğer FireEye tehdit önleme ve tespit yeteneklerini tamamlar niteliktedir.

## AX Serisi

Siber Ataklara yönelik olarak eksiksiz bir 360-derece görüş sağlayan Adli Analiz Platformları

**Öne Çıkanlar**

- FireEye MVX Motoru kullanılarak atak yaşam döngüsünün tamamı üzerinde derin bir adli analiz gerçekleştirilebilir.
- Şüpheli WEB kodlarının, executables'ların ve dosyaların analizini daha etkin hale getirir ve toplu işleme tabi tutar.
- Dosya sistemlerine, hafıza ve tescillere yönelik sistem seviyesinde OS ve uygulama değişikliklerine ilişkin detaylı raporlama gerçekleştirir.
- Zero-day exploit'lerin teyidi amacıyla canlı mod ya da sandbox analizi imkanı tanır.
- FireEye CM platformu ile entegrasyon yoluyla acil yerel koruma sağlanabilmesi için tehdit istihbaratını dinamik olarak oluşturur.
- Kötü niyetli URL oturumu ve kod çalıştırmalarında paketleri tutarak analize olanak sağlar.

Daha etkin bir hadise tepkisi (incident repsonse) önceliklendirmesi için FireEye AV Suit'ini de içerir.