FIREEYE FX

Content Threat Prevention

Detect and Eliminate Malware Resident on File Shares and Content Stores

OVERVIEW

FireEye® FX threat prevention platform protects data assets against attacks originating in a wide range of file types. Web mail, online file transfer tools, the cloud, and portable file storage devices can introduce malware that can then spread to file shares and content repositories. FireEye FX analyzes network file shares and enterprise content management stores to detect and quarantine malware that bypass next-generation firewalls, IPS, AV and gateways.

The problem of malware resident on file shares

Today's advanced cyber attacks use sophisticated malware and advanced persistent threat (APT) tactics to penetrate defenses and spread laterally through file shares and content repositories. This enables the malware to establish a long-term foothold in the network and infect multiple systems, even those offline. Many corporate data centers remain especially vulnerable to advanced, content-based malware because traditional defenses are ineffective against these attacks, which often enter the network through legitimate means. Cyber criminals leverage this vulnerability to spread malware into network file shares and embed malicious code in vast data stores, resulting in a persistent threat even after remediation.

Content protection critical to halt advanced attack life cycle

Without a way to detect resting malware in content, APTs can exploit network assets to extract proprietary information and cause significant damage. The FireEye FX series analyzes file shares and enterprise content repositories using the patented FireEye Multi-Vector Virtual Execution™ (MVX) engine that detects zero-day malicious code embedded in common file types (PDF, MS Office, vCards, ZIP/RAR/TNEF, etc.) and multimedia content (QuickTime, MP3, Real Player, JPG, PNG, etc.). The FireEye FX series performs recursive, scheduled and on-demand scanning of accessible network file shares and content stores to identify and quarantine resident malware. This halts a key stage of the advanced attack life cycle.

The FireEye MVX engine reveals unknown, zero-day threats

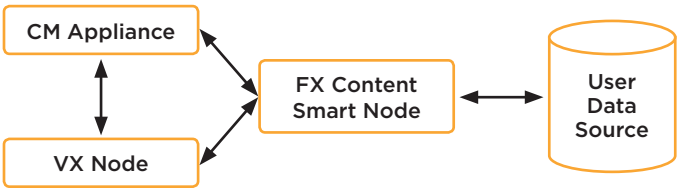
FireEye FX uses the purpose-built FireEye MVX engine, which inspects each file and confirms if zero-day exploits or malicious code exist. The FireEye MVX engine detects zero-day, multi-flow and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops infection and compromise phases of the cyber-attack kill chain by identifying never-before seen exploits and malware.

HIGHLIGHTS

- Finds latent malware undetected by traditional AV engines
- Deploys in active quarantine (protection mode) or analysis only (monitor mode)
- Provides recursive, scheduled and on-demand scans of CIFS and NFS compatible file shares
- Provides proactive Sharepoint protection by leveraging WebDAV protocol
- Includes analysis of a wide range of file types such as PDFs, Microsoft Office documents and multimedia files
- Integrates with the FireEye AV-Suite to streamline incident response prioritization and naming conventions
- Shares threat data with the FireEye platforms through the FireEye CM and the FireEye DTI cloud

Leveraging the Power of FireEye MVX Smart Grid

MVX Smart Grid takes the world's leading network security and makes it even better with a flexible and scalable deployment architecture via hybrid or private cloud. MVX Smart Grid uses an innovative approach to more effectively secure campuses, branch offices, and remote users through the separation of FireEye's pioneering MVX engine and the development of hardware and virtual Smart Nodes™. Smart Nodes analyze Internet traffic to detect and block threats using a variety of techniques such as static analysis, analytics, IPS, applied intelligence, and more, while the MVX engine performs core dynamic analysis.



Proactive SharePoint Content Scanning and Quarantine

FireEye FX continuously scans content to alert and permanently quarantine malware discovered in Sharepoint repositories. The platform leverages WebDAV protocol to securely integrate with Sharepoint services to protect enterprise business workflows utilizing Sharepoint repositories.

YARA-based rules enable customization

FireEye FX supports custom YARA rules to analyze large quantities of file threats specific to the organization.

Streamlined incident prioritization

With the FireEye AV-Suite, each malicious object can be further analyzed to determine if anti-virus vendors were able to detect the malware stopped by FireEye FX. This enables organizations to efficiently prioritize incident response follow-ups and utilize common naming conventions for known malware.

Malware intelligence sharing

The resulting dynamically generated, real-time threat intelligence can help all FireEye products protect the local network through integration with the FireEye CM platform. This intelligence can be shared globally through the FireEye Dynamic Threat Intelligence™ (DTI) cloud to notify all subscribers of emerging threats.

No rules tuning and near-zero false positives

FireEye FX is a group of easy-to-manage, client-less platforms that require absolutely no tuning. Flexible deployment modes include analysis-only monitoring and active quarantining. This enables companies to learn how much malware is resident on file shares and to actively stop the lateral spread of malware.

Content Smart Nodes Provide Protection Where You Need It

With FireEye Content Smart Nodes, content and security managers gain a flexible, virtual solution to protect mission-critical content throughout the enterprise. And, when coupled with a FireEye MVX Smart Grid platform, content protection scales and deploys seamlessly to where you need it.

Table 1. FireEye Content Smart Node

	FX 2500V
OS Support	Microsoft Windows, Mac OS X
Performance	70, 000 files/day
Network Interface Ports	Ether 1, Ether 2
CPU Cores	2
Memory	8 GB
Drive Capacity	512 GB
Hypervisor Support	VMWare ESXi 6.0 or later

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 tel: 408.321.6300 / 877 FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye® is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye