FireEye

Datasheet

FX Series

Content Threat Prevention Platforms to Detect and Eliminate Malware Resident on File Shares

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
- 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

FX 5400 and FX 8400

The FireEye® FX series is a group of threat prevention platforms that protect content 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 spread to file shares. The FireEye FX platform analyzes network file shares to detect and quarantine malware brought in by employees and others 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. 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. Cybercriminals 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 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 to identify and quarantine resident malware. This halts a key stage of the advanced attack life cycle.

FireEye™

Datasheet

The FireEye MVX engine reveals unknown, zero-day threats

The FX series 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 detonates against a range of browsers, plug-ins, applications, and operating environments looking for malicious activities.

YARA-based rules enables customization

The FireEye FX series 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 the FireEye FX platform. 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

The FX series is a group of easy-to-manage, client-less platforms that deploy in under 60 minutes and 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.

Technical Specifications

	FX 5400	FX 8400
Form Factor	1U Rack-Mount	2U Rack-Mount
Weight	30 lbs (13.6 Kg)	50 lbs (22.7 Kg)
Dimensions (WxDxH)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3 cm)	17.2" x 27.9" x 3.5" (43.7 x 70.9 x 8.9 cm)
Enclosure	Fits 19-Inch Rack	Fits 19-Inch Rack
Management Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Performance	Up to 70,000 Files Per Day	Up to 120,000 Files Per Day
AC Input Voltage	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range
AC Input Current	8.5–6.0 A	9.5–7.2 A
Power Supply/RAID	Dual 700W / 2 SAS HDD in HW RAID1	Dual 1400W / 2 SAS HDD in HW RAID1
Power Consumption (Max)	1484 BTU/hr	1586 BTU/hr
Frequency	50–60 Hz	50–60 Hz
Operating Temp	10° C to 35° C	Up to 40° C

Note: All performance values vary depending on the system configuration and traffic profile being processed. Performance numbers listed are based on the files seen in typical enterprise environment.