DATASHEET

FireEye

FX Series

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

SECURITY REIMAGINED

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 CIFSand 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

FX 5400 and FX 8400

Overview

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 to file shares and content repositories. The FireEye FX platform analyzes network file shares and enterprise content management stores to detectand 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 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. 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 and enterprise content repositories using the patented FireEye Multi-Vector Virtual Execution™ (MVX) engine that detects zeroday 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

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.

Proactive SharePoint Content Scanning and Quarantine

The FireEye FX series 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 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
Performance *	Up to 80,000 Files Per Day	Up to 160,000 Files Per Day
Network Interface Ports	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports
IPMI Port (rear panel)	Included	Included
Front Panel LCD & Keypad	Included	Included
PS/2 Keyboard and Mouse, DB15 VGA Ports (rear panel)	Included	Included
USB Ports (rear panel)	2x Type A USB Ports	2x Type A USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Storage Capacity	2x 600 GB HDD, RAID 1, 2.5 inch, FRU	2x 600 GB HDD, RAID 1, 2.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2" x 27.8" x 1.70" (437 x 706 x 43.2 mm)	17.2" x 28.0" x 3.41" (437 x 711 x 86.6 mm)
AC Power Supply	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 – 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 – 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU
DC Power Supply	Not Available	Not Available
Power Consumption Maximum (watts)	463 watts	506 watts
Thermal Dissipation Maximum (BTU/h)	1580 BTU/h	1726 BTU/h
MTBF (h)	40,700 h	68,900 h
Appliance Alone / As Shipped Weight lb. (kg)	32 lb. (15 kg) / 47 lb. (21 kg)	42 lb. (19 kg) / 58 lb. (26 kg)
Safety Certifications	IEC 60950, EN 60950, CSA 60950-00, CE Marking	IEC 60950, EN 60950, CSA 60950-00, CE Marking
EMC/EMI Certifications	FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A)	FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A)
Regulatory Compliance	RoHS, REACH, WEEE	RoHS, REACH, WEEE
Operating Temperature	10° C to 35° C	10° C to 35° C
Operating Relative Humidity	10% to 85% (non-condensing)	10% to 85% (non-condensing)
Operating Altitude	5,000 ft.	5,000 ft.

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.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@FireEye.com | **www.FireEye.com**