FireEye

Datasheet

File Malware Protection System

Next Generation File Security to Detect and Eliminate Malware Resident on File Shares

Highlights

- Finds latent malware no AV engine can
- Deploys in active quarantine (protection-mode) or analysis only (monitor-mode)
- Provides recursive, scheduled, and on-demand scans of CIFS-compatible file shares
- Includes analysis of a wide range of file types. These are the defaults—Adobe® PDFs, Microsoft Office® documents, and multimedia files
- Supports custom YARA rule support (compatible with version 1.3)
- Integrates AV-Suite to streamline incident response prioritization
- Shares threat data with FireEye MPS appliances through Central Management System (CMS) and Malware Protection Cloud (MPC)

Dashboard provides a progress snapshot of file share analysis and threat status

The FireEye File Malware Protection System (MPS) analyzes network file shares to detect and quarantine malware brought in by employees, partners, and others using collaboration tools that bypass next-generation firewalls, IPS, AV, and gateways. Tools like Web mail, online file transfer tools, and portable file storage can introduce malware that can spread to file shares.

The problem of malware resident on file shares

Advanced targeted attacks use sophisticated malware and APT tactics, not only to penetrate defenses, but also to spread laterally through file shares to establish a long-term foothold in the network and to infect systems, even those without access to the external Internet. Many corporate data centers remain vulnerable to advanced malware because of the ineffectiveness of traditional defenses like anti-virus. Criminals leverage this vulnerability in the current security architecture to spread malware into network file shares, embed malicious code in the vast data stores, and become a persistent threat vector to infect and re-infect key systems even after IT remediates them.

File share protection critical to halt advanced attack lifecycle

FireEye File MPS security appliances analyze file shares using the patented FireEye Virtual Execution (VX) engine that detects zero-day malicious code embedded in common file types, including PDF, Microsoft Office documents, vCards, ZIP/RAR/TNEF, and multimedia content such as QuickTime, MP3 and JPEG files. The File MPS performs recursive, scheduled, and on-demand scanning of accessible network file shares to identify and quarantine resident malware without impact to corporate productivity. This halts a key stage of the advanced attack lifecycle.

"We brought in the FireEye File MPS because we had recurring malware infections, even on systems we had just re-imaged and disconnected from the Web. The File MPS technology was able to detect malware hidden in the file shares that anti-virus and other signature-based technologies failed to do. Using the File MPS we were also able to confirm that hosts were infected."

— VP, Global Financial Services Company

FireEye™

Datasheet

VX engine reveals unknown, zero–day threats

The multi-phase VX engine inspects each file to confirm if zero-day exploits or malicious code exists. The VX engine detonates against a range of browsers, plug-ins, applications, and operating environments looking for malicious activities. With the sophisticated instrumentation of virtual analysis environments, the VX engine can monitor the code throughout the entire execution path.

YARA-based rules enables customization

The File MPS supports custom YARA rule importation to enable security analysts to specify rules to analyze large quantities of file threats specific to the organization. The custom rules are added to the VX engine analysis to determine malicious activity.

Streamlined incident prioritization

With FireEye's AV-Suite and third-party anti-virus integration, each malicious object can be further analyzed to determine whether anti-virus vendors were able to detect the malware identified and quarantined by the File MPS. This enables customers to efficiently prioritize incident response follow-ups.

Malware intelligence sharing

The resulting dynamically generated, real-time malware intelligence can help all FireEye appliances protect the local network through integration with the FireEye CMS. Dynamically generated malware intelligence includes callback coordinates as well as communication characteristics, such as the malware protocol being used. This intelligence can be shared globally through the FireEye Malware Protection Cloud to notify all subscribers of emerging threats.

No rules tuning and no false positives

This easy-to-manage, clientless appliance deploys in under 30 minutes and requires absolutely no tuning. Flexible deployment modes include analysis only monitoring and active quarantining. This enables companies to first learn how much malware is resident on file shares and then to actively stop those files from claiming additional victims. By providing highly accurate malware detection and quarantining, FireEye gives administrators the ability to secure their file sharing networks and stop a key stage of the attack lifecycle.

Technical Specifications

	File MPS 5300	File MPS 8300
Form Factor	1U Rack-Mount	2U Rack-Mount
Weight	30 lbs (13.6 Kg)	55 lbs (24.94 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 Interfaces	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Monitoring Interfaces	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Performance Rating	35,000 file objects per day	70,000 file objects 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 A	9.5-7.2 A
Power Supply/RAID	Dual / 2 SAS HDD in HW RAID1	Dual / 2 SAS HDD in HW RAID1
Frequency	50-60 Hz	50-60 Hz
AC Power	700 W Max	1400 W Max
Ambient Temp	40° C	40° C