FireEye

Datasheet

Email Malware Protection System

Next Generation Email Security to Stop Advanced Targeted Attacks

Highlights

- Analyzes all email attachments including all common file formats and ZIP/RAR/TNEF archives
- Complements existing email control infrastructure, such as anti-spam gateways
- Deploys in active protection-mode as an MTA, or monitor-mode (SPAN / BCC)
- Quarantines malicious emails with optional user notifications
- Supports blended attack protection across Web and email threat vectors
- Supports custom YARA rules (compatible with version 1.3)
- Integrates with third-party anti-virus to streamline email threat management
- Shares threat data with FireEye MPS appliances through Central Management System (CMS) and Malware Protection Cloud (MPC)

Dashboards let you understand email threat events within your network

The FireEye Email Malware Protection System (MPS) secures against spear phishing emails that bypass anti-spam and reputation-based technologies. FireEye MPS is the only solution to address blended, advanced targeted attacks using zero-day exploits, email, and malicious URLs.

With all the personal information available online, a criminal can socially engineer almost any user into clicking a URL or opening an attachment. The Email MPS provides real-time security against spear phishing attacks that easily evade traditional defenses. Used with the Web MPS, organizations gain a new level of security against blended attacks that leverage the Web and email threat vectors.

Real-time quarantine of malicious emails

To block spear phishing emails, the Email MPS analyzes every attachment using a signature-less Virtual Execution (VX) engine that can safely and accurately identify zero-day attacks. The VX engine detonates files against a cross-matrix of operating systems and applications, including multiple Web browsers and plug-ins like Adobe Reader and Flash. Malicious emails can be quarantined for further analysis or deletion.

Fights blended attacks across Web and email threat vectors

Advanced attacks use spear phishing as the opening salvo of a multi-vector attack strategy. When the Email MPS is deployed along with the Web MPS and Central Management System (CMS), customers get real-time protection against malicious URLs and the ability to identify other individuals who were also targeted. This is the actionable intelligence necessary to protect organizations against advanced targeted attacks.

"In addition to the rapid deployment capabilities, the FireEye appliances are an all-in-one solution that effectively halts zero-day attacks across the enterprise. The protection provided is independent of signatures and we enjoy an extremely low false positive rate; from day one the total count remains in the low single digits."

— Information Security Specialist, Global Manufacturer

FireEye™

Datasheet

Dynamic analysis of zero-day email attacks

The signature-less VX engine detects and stops advanced attacks exploiting truly unknown OS, browser, and application vulnerabilities as well as malicious code embedded in common file and multimedia content. The VX engine reports out forensic-quality details of the exploit, such as the vulnerability exploited in a buffer overflow and callback coordinates used to exfiltrate data.

Malware intelligence sharing

With CMS integration, the resulting dynamically generated, real-time malware intelligence can be distributed to all FireEye appliances in real-time. The FireEye MPS will then immediately protect across the entire deployment, from quarantining zero-day malicious emails to blocking multi-protocol callback channels. This malware intelligence is also shared globally through the MPC to stop emerging threats.

YARA-based rules enables customization

The Email MPS supports custom YARA rule importation to enable security analysts to specify rules to analyze email attachments for threats specific to the organization. The custom rules are added to the VX engine analysis to determine likely malicious attachments as well as attachments previously classified as malicious.

Streamlined email threat management

With FireEye third-party anti-virus integration, each malicious object is analyzed to determine if anti-virus was able to detect the malware stopped by the Email MPS. This enables customers to gain deeper forensic information about the attack as well as standardize naming terminology for more efficient incident response prioritization.

Spear phishing security

The appliance requires no tuning and can be setup as an MTA, SPAN device, or transparent BCC destination. FireEye supports remote third-party AAA (Authentication, Authorization, and Accounting) network service access in addition to local authentication.

Technical Specifications

	Email MPS 5300	Email MPS 8300	Email MPS 8320
Form Factor	1U Rack-Mount	2U Rack-Mount	2U Rack-Mount
Weight	30 lbs (13.6 Kg)	55 lbs (24.94 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)	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	Fits 19-Inch Rack
Management Interfaces	(2) 10/100/1000 BASE-T Ports	(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	(2) 1000 BASE-SX Ports
Performance Rating	300,000 emails per day	750,000 emails per day	750,000 emails per day
AC Input Voltage	Auto-switching 100 ~ 240 VAC Full Range	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	9.5-7.2 A
Power Supply/RAID	Dual / 2 SAS HDD in HW RAID1	Dual / 2 SAS HDD in HW RAID1	Dual / 2 SAS HDD in HW RAID1
Frequency	50-60 Hz	50-60 Hz	50-60 Hz
AC Power	700 W Max	1400 W Max	1400 W Max
Ambient Temp	40° C	40° C	40° C