FireEye

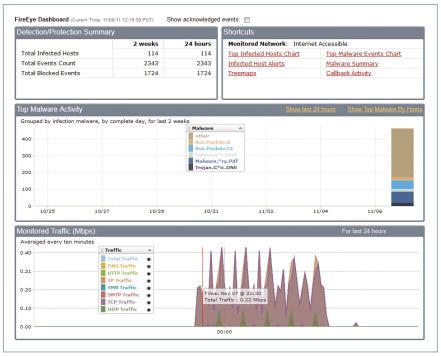
Datasheet

Web Malware Protection System

Next-Generation Web Security to Combat Advanced Cyber Attacks

Highlights

- Deploys in-line (block/monitor mode) or out-of-band (TCP reset mode/monitor mode)
- Supports X-Forwarded-For to identify the IP address of a host within a proxied environment
- Blocks outbound malware transmissions across multiple protocols to thwart data exfiltration
- Analyzes all suspicious Web objects including PDFs, Flash, multimedia formats, and ZIP/RAR/TNEF archives
- Supports custom YARA rules
- Streamlines incident response prioritization with AV-Suite integration
- Integrates with FireEye Email MPS to stop blended spear phishing attacks
- Shares intelligence with FireEye MPS appliances through the FireEye CMS forming the FireEye Dynamic Threat Intelligence™ (DTI) enterprise
- Distributes threat intelligence globally through the FireEye Dynamic Threat Intelligence (DTI) cloud
- Supports remote third-party AAA network service access in addition to local authentication



Dashboards display Web malware traffic and enable threat event navigation

The FireEye® Web Malware Protection System™ (MPS) stops Web-based attacks that traditional and next-generation firewalls, IPS, AV, and Web gateways miss and protects against zero-day Web exploits and multi-protocol callbacks to keep sensitive data and systems safe.

Cybercriminals use the Web as a primary threat vector to deliver zero-day exploits and malicious URLs in email and exfiltrate data. The FireEye Web MPS is designed to protect against drive by downloads and blended Web and email attacks, and in addition, offers a defense against infections that take place outside the network.

Real-time protection to stop Web-based attacks

FireEye Web MPS appliances can be deployed in-line at Internet egress points to block Web exploits and outbound multi-protocol callbacks. Utilizing the FireEye Multi-Vector Virtual Execution™ (MVX) engine, the FireEye Web MPS confirms zero-day attacks, creates real-time protections, and captures dynamic callback destinations. In monitor mode, it signals incident response mechanisms. In out-of-band, protection mode, the FireEye Web MPS issues TCP resets for out-of-band blocking of TCP, UDP, or HTTP connections.

Fights blended attacks across Web and email threat vectors

The FireEye platform protects against blended, advanced attacks that use Web, spear phishing emails, and zero-day exploits. With the FireEye Web MPS, FireEye Email Malware Protection System™ (MPS), and the FireEye Central Management System™ (CMS), customers get real-time protection against malicious URLs and the ability to connect the dots of a blended attack.

"The FireEye Malware Protection System was the only product that focused on real-time interpretation of the specific intent of potentially malicious code, versus the rigid signature-based and difficult to administer heuristics approaches that everyone else offered."

— Director of IT, Legal Services Firm

FireEye™

Datasheet

Protects against unknown, zero-day attacks

The signature-less FireEye MVX engine executes suspicious binaries and Web objects against a range of browsers, plug-ins, applications, and operating environments that track vulnerability exploitation, memory corruption, and other malicious actions. As the attack plays out, the FireEye MVX engine captures callback channels, dynamically creates blocking rules, and transmits this information back to the FireEye Web MPS.

YARA-based rules enable customization

With support for custom YARA rules, security analysts can specify which Web objects should be analyzed for threats.

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 Web MPS. This enables customers to more efficiently prioritize incident response.

Dynamic threat intelligence sharing

The resulting dynamically generated, real-time threat intelligence produced by the FireEye Web MPS, helps all FireEye appliances protect the local network. This intelligence includes callback coordinates and communication characteristics which can be shared globally through the FireEye Dynamic Threat Intelligence cloud to notify all subscribers of new threats.

No rules tuning and no false positives

This easy-to-manage, clientless appliance deploys in under 60 minutes and does not require tuning. It offers flexible deployment modes, including out-of-band via a TAP/SPAN, in-line monitoring, or in-line active blocking.

Technical Specifications

	Web MPS 1310	Web MPS 2310	Web MPS 4310	Web MPS 4320	Web MPS 7300	Web MPS 7320
Form Factor	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount
Weight	12 lbs (5.4Kg)	12 lbs (5.4Kg)	30 lbs (13.6 Kg)	30 lbs (13.6 Kg)	30 lbs (13.6 Kg)	30 lbs (13.6 Kg)
Dimensions (WxDxH)	16.8" x 14.0" x 1.7" (42.6 x 35.6 x 4.3 cm)	16.8" x 14.0" x 1.7" (42.6 x 35.6 x 4.3 cm)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3 cm)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3 cm)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3 cm)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3 cm)
Enclosure	Fits 19-Inch Rack	Fits 19-Inch Rack	Fits 19-Inch Rack	Fits 19-Inch Rack	Fits 19-Inch Rack	Fits 19-Inch Rack
Management Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Monitoring Ports	(2) 10/100/1000 BASE-T Ports	(4) 10/100/1000 BASE-T Ports	(4) 10/100/1000 BASE-T Ports	(4) 1000 BASE-SX Fiber Optic Ports (LC Multimode)	(4) 10/100/1000 BASE-T Ports	(4) 1000 BASE-SX Fiber Optic Ports (LC Multimode)
Performance	Up to 20 Mbps	Up to 50 Mbps	Up to 250 Mbps	Up to 250 Mbps	Up to 1 Gbps	Up to 1 Gbps
User Count	100	500	2,500	2,500	10,000	10,000
AC Input Voltage	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range
AC Input Current	4.8–2.0 A	4.8–2.0 A	8.5–6.0 A	8.5–6.0 A	8.5–6.0 A	8.5–6.0 A
Power Supply/RAID	Single 260W / No	Single 260W / No	Dual 700W / 2 SAS HDD in HW RAID1	Dual 700W / 2 SAS HDD in HW RAID1	Dual 700W / 2 SAS HDD in HW RAID1	Dual 700W / 2 SAS HDD in HW RAID1
Frequency	50–60 Hz	50–60 Hz	50–60 Hz	50–60 Hz	50–60 Hz	50–60 Hz
Operating Temp	10° C to 35° C	10° C to 35° C	10° C to 35° C	10° C to 35° C	10° C to 35° C	10° C to 35° C

Note: All performance values vary depending on the system configuration and traffic profile being processed.