FireEye

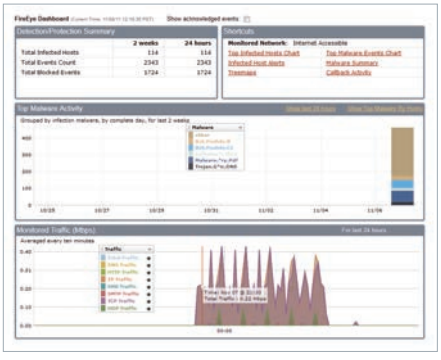
Datasheet

Web Malware Protection System

Next Generation Web Security to Combat Advanced Targeted Attacks

Highlights

- Deploys inline (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
- Custom YARA rule support (compatible with version 1.3)
- AV-Suite integration streamlines incident response prioritization
- Intelligence sharing with FireEye MPS appliances through Central Management System (CMS) and Malware Protection Cloud (MPC)
- Supports remote third-party AAA (Authentication, Authorization, and Accounting) network service access in addition to local authentication



Dashboards let you understand Web malware traffic and navigate threat events

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

Advanced targeted attacks use the Web as a primary threat vector since nearly all organizations allow some Web access. Criminals deliver zero-day exploits during Web browsing or via a malicious URL in an email. The Web is also a transport mechanism for data exfiltration.

Real-time protection to stop Web-based attacks

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

Fights blended attacks across Web and email threat vectors

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

Protects against unknown, zero-day attacks

The signature-less VX engine detects advanced attacks exploiting unknown vulnerabilities as well as malicious code embedded in common Web and multimedia content. The VX engine reports out forensic details of the exploit, such as the vulnerability exploited to create a buffer overflow

"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

condition, attempts at privilege escalation within Windows, and the callbacks used to exfiltrate data.

The VX engine executes suspicious binaries and Web objects against a range of browsers, plug-ins, applications, and operating environments that are instrumented to track vulnerability exploitation, memory corruption, and other definitive malicious actions. As the attack plays out, it captures callback channels and dynamically creates blocking rules.

YARA-based rules enables customization

The Web MPS supports custom YARA rule importation to enable security analysts to quickly analyze Web objects for threats specific to the organization.

Streamlined incident prioritization

With 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 Web MPS. This enables customers to more 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. Intelligence includes callback coordinates, as well as communication characteristics. This intelligence can be shared globally through the FireEye Malware Protection Cloud (MPC) to notify all subscribers of new threats.

No rules tuning and no false positives

This easy-to-manage, clientless appliance deploys in under 30 minutes and requires absolutely no tuning. It offers flexible deployment modes, including out-of-band via a TAP/SPAN, inline monitoring, or inline active blocking. The FireEye VX engine nearly eliminates false alerts and provides administrators with the true incidents that merit attention.

Technical Specifications

	Web MPS 1310	Web MPS 2310	Web MPS 4310	Web MPS 7300	Web MPS 7320
Form Factor	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount
Weight	12 lbs (5.4Kg)	12 lbs (5.4Kg)	25 lbs (11.4 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 27.5" x 1.7" (43.7 x 69.9 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
Management Interfaces	(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 Interfaces	(2) 10/100/1000 BASE-T Ports	(4) 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
Performance Rating	Up to 20 Mbps	Up to 50 Mbps	Up to 250 Mbps	Up to 1 Gbps	Up to 1 Gbps
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
AC Input Current	4.8-2.0 A	4.8-2.0 A	8.5-6 A	8.5-6 A	8.5-6 A
Power Supply/RAID	Single / No	Single / No	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	50-60 Hz	50-60 Hz
AC Power	260 W Max	260 W Max	700 W Max	700 W Max	700 W Max
Ambient Temp	40° C	40° C	40° C	40° C	40° C