

# Web Malware Protection System

Next generation Web security to combat advanced malware, zero-day and targeted APT attacks

**The FireEye Web Malware Protection System (MPS) deploys behind other security gateways to catch the zero-day threats that policy- and signature-based firewalls, IPS, AV, and Web gateways miss. It stands in front of outbound traffic to keep your sensitive data and systems safe.**

Today's coordinated attackers often enter the network as Web traffic, then hijack resources, perform reconnaissance, and establish long-term control over endpoints.

## Inbound Inspections Block Known Web Malware

FireEye Web security appliances use several techniques to detect known and suspicious code, eliminating the noisy false positives that plague traditional security technologies. First, deep packet inspection weeds out known threats based on signatures. Next, aggressive heuristics look for suspicious Web objects and executable code.

## Virtual Execution Environment Reveals Unknown, Zero-Day Threats

To decide if suspicious code is true malware, the multi-phase Virtual Execution (VX) engine inspects, captures and confirms zero-day malware and targeted attacks. Instead of simply estimating risk by heuristics, which can generate both false positives and false negatives, FireEye runs suspected malware in a full-featured virtual endpoint environment to uncover the true nature of the attack.

## Outbound Blocking Thwarts Data Theft & Botnets

One by-product of this rich, automated analysis is the detail FireEye captures about each attack's external connections. FireEye uses this information to shut down outbound transmissions that carry credentials, keystrokes and other data and can control a compromised host, or bot. Administrators also learn which systems to remediate.

## Highlights

- Deploys inline (block/monitor-mode) or out-of-band (monitor-only)
- Safely detonates unknown code and suspicious Web objects to block attacks including malicious image, PDF, and Flash files
- Cuts off outbound malware transmissions across multiple protocols to thwart data exfiltration, botnets and APTs
- Traces the full execution path of zero-day and known attacks to empower analysts
- Replaces wasteful false positive analysis with laser focused investigations into real events
- Works with FireEye email protection to identify and block blended spear phishing attacks



Dashboards let you understand Web malware traffic and navigate threat events

**“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

### Real-time, Dynamic Analysis of the Unknown

The VX engine executes potentially malicious binaries and Web objects to confirm an attack and eliminate any false positives. Unlike a simple sandbox, the VX engine detonates code against a range of browsers, plug-ins, applications, and operating environments, looking for any sign of unusual activity or attempt to exploit a vulnerability. For instance, the VX engine can identify buffer overflow conditions, where an attacker might be able to inject malicious software on a host.

With its virtualization and deep instrumentation, it can monitor the code throughout the entire execution path. It can detect an exploit of a zero-day browser plug-in vulnerability, an obfuscated JavaScript attack, an escalation of privileges within Windows, and memory corruption to facilitate arbitrary code execution.

### Sharing Intelligence Through the Cloud

The resulting dynamically generated, real-time malware intelligence can help all FireEye appliances protect the local network. Dynamically generated malware intelligence includes callback coordinates, such as IP address and port, 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 new threats.

### Disconnects Malware that Phones Home

Through the malware insight captured inbound, plus updates from the FireEye Malware Protection Cloud, the appliance recognizes and blocks malware that tries to dial out. It can block based on source and destination IP addresses, ports and protocols including HTTP, FTP or IRC. Unlike other perimeter protections, it guards against both known and unknown threats and botnets that get a foothold in your network and phone home. For example, it can dynamically discover a previously unknown callback channel by observing the inbound attack. The Web MPS will then create detection and blocking rules for that channel.

### 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, including out-of-band monitoring via a SPAN port, inline monitoring or inline active blocking, enable the move from learning what the deployed security gateways are missing to actively stopping attacks and outbound transmissions. By providing highly accurate malware detection and blocking, FireEye cuts out noisy false alerts. It leaves administrators with just the true incidents that merit attention, which can be blocked in both inbound and outbound directions. Just a single click is required to move from monitor to blocking mode.

Technical Specifications				
	1300	2300	4000	7000
Form Factor	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount	2U Rack-Mount
Weight	32 lbs (16.78 kg)	32 lbs (16.78 kg)	32 lbs (16.78 kg)	65 lbs (34.2 kg)
Dimensions (WxDxH)	17.25" x 21.75" x 1.75" (43.8 x 55.3 x 4.5 cm)	17.25" x 21.75" x 1.75" (43.8 x 55.3 x 4.5 cm)	17.25" x 21.75" x 1.75" (43.8 x 55.3 x 4.5 cm)	17.25" x 21.75" x 3.5" (43.8 x 55.3 x 9.0 cm)
Enclosure	Fits 19-Inch Rack	Fits 19-Inch Rack	Fits 19-Inch Rack	Fits 19-Inch Rack
Monitoring Interfaces	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(4) 10/100/1000 BASE-T Ports	(4) 10/100/1000 BASE-T Ports
Management Interfaces			(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Performance Rating	Up to 20 Mbps	Up to 50 Mbps	Up to 250 Mbps	Up to 1 Gbps
AC Input Voltage	99 ~ 240 VAC Full Range	99 ~ 240 VAC Full Range	100 ~ 240 VAC Full Range	101 ~ 240 VAC Full Range
AC Input Current	4.8 - 2.0 A	4.8 - 2.0 A	4.8 - 2.0 A	4.8 - 2.0 A
Power Supply/RAID	Single / No	Single / No	Single / No	Dual / 2 SAS HDD in RAID1
Frequency	50-60Hz	50-60Hz	50-60Hz	50-60Hz
AC Power	400 W Max	400 W Max	400 W Max	180 W Max
Ambient Temp	40 °C	40 °C	40 °C	40 °C