The FireEye Malware Protection System blocks Modern Malware in real-time without signatures to prevent broad and targeted data breaches.

FireEye Malware Protection System

Breaking the Modern Malware Infection Lifecycle

The modernization of malware has enabled criminals to easily bypass conventional security mechanisms, such as firewalls, URL filters, and intrusion prevention systems. While these components play a policy enforcement role, organizations are left with a gap in network security against today's Modern Malware. True zero-day, targeted threats continue to penetrate and infect systems using tactics, such as obfuscating malicious code on Web pages, embedding attacks in PDF documents, and exploiting other unknown application and OS vulnerabilities to gain a foothold on the system.

Compromising endpoint systems is still the path of least resistance for criminals to penetrate the network and steal valuable resources stored in the data center and within the cloud. Modern Malware attacks are no longer single incidents in which a PC is infected and can be scanned and cleaned. Today's attacks are coordinated efforts to establish long-term control over endpoint systems for the purposes of data theft, hijacking network resources, cyber reconnaissance, or establishing ongoing access into the network/cloud infrastructure.

Attempts to strengthen endpoint and perimeter security have typically relied upon stringing together conventional technologies like port-based filters, signature-based scanners, and heuristics-based detectors. However, these attempts, whether on the endpoint or within the network, have not been able to accurately and reliably stop attacks targeting truly unknown vulnerabilities. Technologies that use techniques like signature pattern matching, rules-based filtering, or heuristic analysis of network anomalies or DNS patterns ultimately collapse due to inaccurate attack identification (false positives) and missed attacks (false negatives). A fundamentally new technique is required to stop today's advanced, persistent threats and break the Modern Malware infection lifecycle.

KEY FEATURES & BENEFITS

- Blocks Modern Malware, Trojans, bots, and advanced persistent threats
- Captures zero-day malware and targeted attacks in real-time
- Cuts off outbound malware transmissions to stop data exfiltration
- Eliminates overhead of false positive analysis and tuning
- Deploys inline (block/monitor-mode) or out-of-band (monitor-only)

FireEye®

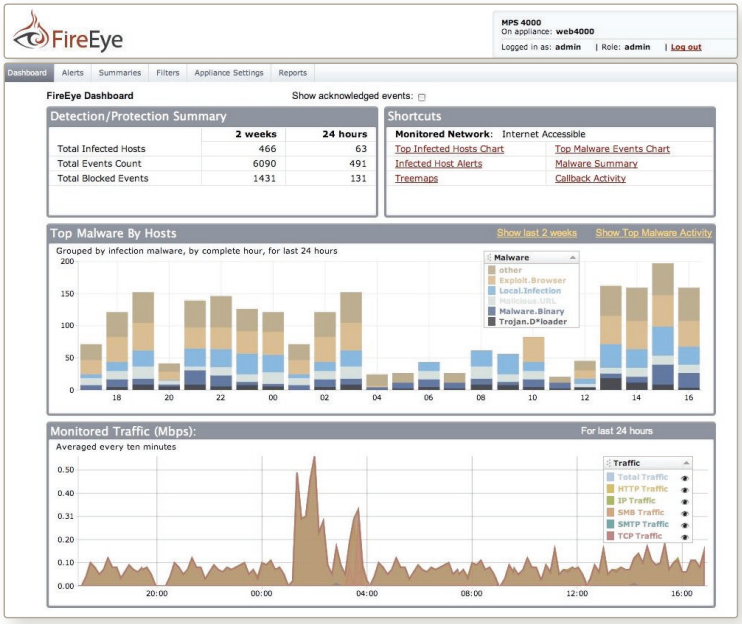
FireEye Malware Protection System

PRODUCT DATASHEET

The FireEye Malware Protection System (MPS) accurately blocks Modern Malware, such as Trojans, bots, crimeware, and advanced persistent threats, in real-time using an advanced multi-phase analysis engine to capture and confirm zero-day malware and targeted attacks. It is an enterprise-class security gateway deployed at the Internet egress point to prevent broad and targeted theft of information and resources due to Modern Malware. The FireEye MPS family of appliances dynamically learns new vulnerabilities, exploits, and techniques in real time to prevent data loss, intellectual property theft, and resource hijacking.

Key Principles For Modern Malware Protection

- **Dynamic defenses to stop inbound targeted attacks:** Automate malware analysis and accurately identify malware targeting completely unknown vulnerabilities across protocols and applications
- **Real-time protection to block data exfiltration attempts:** Stop outbound malware transmissions to criminals servers used to transfer stolen data and download more malware to solidfy long-term control over the system
- **Integrated inbound and outbound filtering across multiple protocols:** Correlate the real-time, zero-hour malware analysis with the outbound blocking filter to stop data exfiltration attempts
- **Accurate, low false positive rates:** Accurate blocking and alerts form the foundation for any effective IT security system to ensure ongoing usability and IT productivity
- **Global intelligence on advanced threats to protect the local network:** Benefit from a global analysis network in which subscribers receive and optionally share malware intelligence such as zero-day attacks and callback destinations



IT administrators get an instant view into modern malware infection types and frequency

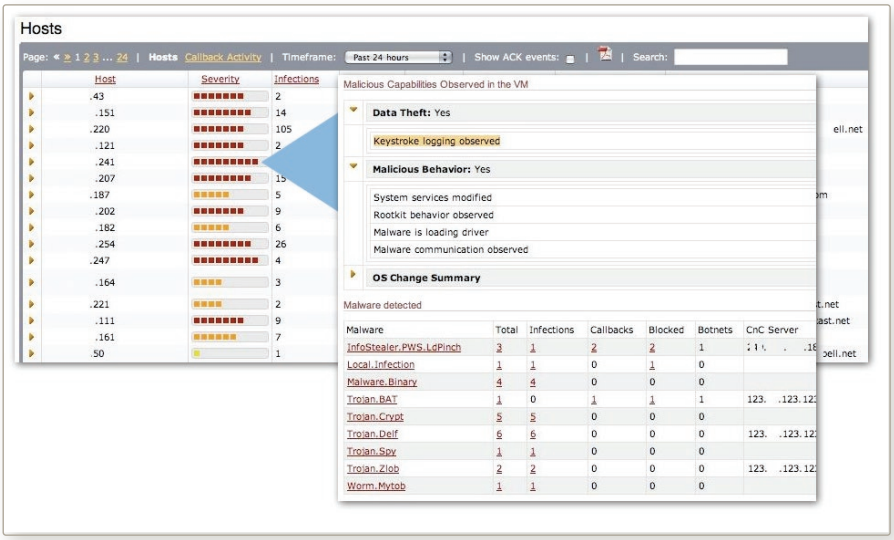
Real-time, Dynamic Modern Malware Protection

At the core of each security appliance are the FireEye Malware-VM™ and Malware-Callback™ technologies, which combines inbound and outbound filtering to break the malware infection lifecycle.

The Malware-VM filter features aggressive capture heuristics coupled with deep packet inspection within instrumented virtual machines. The first stage of aggressive capture heuristics maximizes attack detection and feeds the second virtual machine analysis stage, which confirms attacks and eliminates any false positives. As a result, the Malware-VM engine in uniquely designed to detect zero-day attacks while eliminating the false alerts that plague conventional security technologies. The Malware-VM analysis stage performs both static analyses to catalog information about suspicious binaries/URLs as well as dynamic analyses when it executes the potentially malicious binaries or Web pages. It identifies arbitrary code execution and when an exploit is confirmed by the virtual machine, malware and its outbound transmissions are blocked. The resulting

zero-day malware intelligence is dynamically-generated, real-time malware forensics used to protect the local network as well as shared globally through the MAX Cloud Intelligence network for use by all subscribers to stop data and resource thefts. With deep instrumentation, the FireEye Malware-VM filter is uniquely able to trace the full execution path of zero-day and known attacks as well as provide details on custom malware communication protocols.

Using the output of the Malware-VM analyses as well as MAX Cloud Intelligence data, the Malware-Callback filter blocks outbound malware transmissions to criminal servers stopping data exfiltration attempts. The malware content includes destination characteristics, such as IP and port, as well as communication characteristics, such as the malware protocol being used, to accurately stop data theft and identify previously compromised systems on the network. Organizations can now dynamically capture, fingerprint, and block zero-day malware and its unauthorized outbound callbacks to criminal command and control servers.



Administrators can prioritize their work based on threat severity and drill-down into attack characteristics.

Inbound and Outbound Threat Protection

FireEye inspects both inbound traffic for malware attacks as well as outbound traffic across multiple protocols to identify compromised systems transmitting your data to criminal servers. This integrated approach enables the most comprehensive threat protection against modern threats that attack across multiple vectors to penetrate the network. The initial compromise of a system could be a social engineering attack like a spear-phish email with a URL or malicious PDF. Once the dropper malware is installed, it calls back out to a server to upload stolen data and download further malware payloads. With both inbound and outbound threat protection, FireEye offers the most complete Modern Malware protection system that goes beyond simple signature matching or rudimentary packet/DNS analysis. FireEye is able to pinpoint today's stealth malware that have circumvented conventional security technologies and makes it is possible to stop the proliferation of Modern Malware targeted at organizations for the purpose of cybercrime, cyber espionage, and cyber reconnaissance.

Global Network to Share Local Malware Intelligence

In order to share the benefits of the real-time malware intelligence gathered by the local analysis engines, FireEye has built a worldwide Malware Analysis and Exchange (MAX) Cloud Intelligence network to distribute the auto-generated security intelligence about Modern Malware and its covert callback channels. The MAX Cloud is essentially an Internet cyber crime watch system to provide subscribers the latest intelligence on inbound attacks and unauthorized outbound callback destinations in real-time to prevent data exfiltration, alteration, and destruction.

Eliminates Overhead of False Positive Analysis and Tuning

With FireEye, IT administrators have a clientless solution that deploys in 30 minutes and requires absolutely no tuning. It deploys in several modes, including out-of-band monitoring via a SPAN port, inline monitoring, or inline active blocking to stop attacks and outbound transmissions. By providing accurate malware detection and blocking, FireEye secures the network while eliminating the headaches associated with false positive analysis. There are several FireEye MPS models supporting organizations with egress bandwidths of up to 1 Gbps. The appliance is transparent to both end users and criminals alike. This is an easy-to-manage, cost effective solution that maximizes Modern Malware protection without adding network and security management overhead.

Advancing the State-of-the-Art For Malware Protection

FireEye has significantly advanced the state-of-the-art for malware protection, and has now made it possible to accurately stop Modern Malware in real time. With integrated inbound attack detection and outbound malware transmission filtering tied into a global security exchange network, administrators have a clientless solution that is easy to deploy and maintain to provide modern protection against today's modern threats.

SPECIFICATIONS

Appliance Series	7000	4000	2000	1000
Form Factor	2U Rack-Mount	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount
Weight	36 lbs (16.3 kg)	23 lbs (10.4 kg)	16 lbs (7.3 kg)	16 lbs (7.3 kg)
Dimensions	17.25"W x 21.75"D x 3.5"H (43.8 cm x 55.3 cm x 8.9 cm)	17.25"W x 21.75"D x 3.5"H (43.8 cm x 55.3 cm x 4.5 cm)	17.25"W x 10.87"D x 1.75"H (43.8 cm x 27.6 cm x 4.5 cm)	17.25"W x 10.87"D x 1.75"H (43.8 cm x 27.6 cm x 4.5 cm)
Enclosure	Fits 19-Inch Rack	Fits 19-Inch Rack	Fits 19-Inch Rack	Fits 19-Inch Rack
Interfaces	(6)10/100/1000 BASE-T Ports	(6)10/100/1000 BASE-T Ports	(3)10/100/1000 BASE-T Ports	(3)10/100/1000 BASE-T Ports
Throughput	2.4 Gbps	1.2 Gbps	500 Mbps	200 Mbps
Malware-VM Threat Prevention	1 Gbps	250 Mbps	50 Mbps	20 Mbps
Concurrent Sessions	120,000	50,000	10,000	10,000
AC Input Voltage	100 ~ 240 VAC Full Range	100 ~ 240 VAC Full Range	100 ~ 240 VAC Full Range	100 ~ 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	Dual / 2 SAS HDD in RAID1	Single / No	Single / No	Single / No
Frequency	50-60Hz	50-60Hz	50-60Hz	50-60Hz
AC Power	400 W Max	400 W Max	180 W Max	180 W Max
Ambient Temp	40 °C	40 °C	40 °C	40 °C

About FireEye, Inc.

FireEye, Inc. is the leader in malware protection systems and next generation network threat prevention solutions that safeguard valuable data and networks against Modern Malware infiltration and theft in commercial enterprises, higher education, and government institutions. The FireEye Malware Protection System is the industry's first solution that completely breaks the Modern Malware infection lifecycle by stopping inbound, zero hour, targeted attacks, outbound data exfiltration callbacks, and dynamically inoculating networks from future attacks through both local and global intelligence. FireEye finds and blocks the 90% of Modern Malware attacks that conventional defenses miss, at network speeds and near-zero false positive rates, delivering an extremely low security TCO. FireEye is based in Milpitas, Calif. and backed by Sequoia Capital, Norwest Venture Partners, JAFCO Ventures, DAG Ventures, Juniper Networks, and In-Q-Tel.

FireEye

FireEye, Inc.
1390 McCarthy Blvd
Milpitas, CA 95035
+1 (877) FIREEYE (347.3393) info@fireeye.com

www.FireEye.com