FireEye

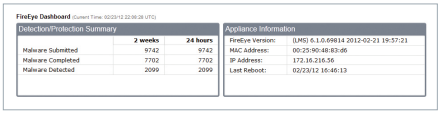
Datasheet

Malware Analysis System

Real-Time Global Exchange of Threat Data Stops Emerging Zero-Day Attacks

Highlights

- Performs deep forensic analysis through the full attack life cycle, using the FireEye MVX engine
- Streamlines and batches analysis of suspicious Web code, executables, and files
- Reports in-depth on system-level OS and application changes to file systems, memory, and registries
- Offers live-mode or sandbox analysis to confirm zero-day exploits
- Eliminates deployment issues and tuning with a pre-configured environment, plus automated setup and teardown of virtual test images
- Dynamically generates threat intelligence for immediate local protection via integration with the FireEye CMS
- Captures packets to allow analysis of malicious URL session and code execution
- Supports custom YARA rules
- Includes the FireEye AV-Suite to streamline incident response prioritization
- Supports remote third-party AAA network service access in addition to local authentication



FireEye MAS dashboard shows status of completed and pending FireEye MVX engine analysis

The FireEye® Malware Analysis System™ (MAS) gives threat analysts hands-on control over powerful auto-configured test environments to safely execute and inspect advanced malware, zero-day, and advanced persistent threat (APT) attacks embedded in Web pages, email attachments, and files.

As cybercriminals tailor attacks to penetrate a specific business, user account, or system, analysts need easy-to-use forensic tools that help them rapidly address targeted malicious activities.

Assess OS, browser, and application attacks

The FireEye Multi-Vector Virtual Execution™ (MVX) engine empowers in-house analysts with a full 360-degree view of an attack, from the initial exploit to callback destinations, and follow-on binary download attempts. Through a pre-configured, instrumented Windows virtual analysis environment, the FireEye MVX engine fully executes suspicious code to allow deep inspection of common Web objects, email attachments, and file formats. The FireEye MAS uses the FireEye MVX engine to inspect single files or batches of files for malware and tracks outbound connection attempts across multiple protocols.

Spend time analyzing, not administering

The FireEye MAS appliance frees administrators from time-consuming setup, baselining, and restoration of the virtual machine environments used in manual malware analysis. With built-in customization and granular control over payload detonations, the FireEye MAS enables forensic analysts to arrive at a comprehensive understanding of the attack that is suited to the needs of the enterprise.

"One of the big attractions of the FireEye solution is that analysis is performed in a virtual execution environment to determine if a flagged piece of code actually is a threat. The detailed information that is generated allows us to pinpoint the ideal option for resolving an issue. It puts us in the position of knowing exactly how to react."

— Director of Cyber Security, Energy Sector

FireEye™

Datasheet

Choose live analysis or sandbox modes

The FireEye MAS has the ability to provide users two analysis modes—live and sandbox. Malware analysts use the live, on-network mode for full malware life cycle analysis, allowing external connectivity. This gives the FireEye MAS the ability to track advanced attacks as across multiple stages and different vectors. In sandbox mode, the execution path of particular malware samples are fully contained and visible in the virtual environment.

In both modes, users are able to generate a dynamic and anonymized profile of the attack that can be shared through the FireEye Content Management System™ (CMS) to other FireEye appliances. The malware attack profiles generated by the FireEye MAS include identifiers of malware code, exploit URLs, and other sources of infections and attacks. Also, malware communication protocol characteristics are shared to provide dynamic blocking of data exfiltration attempts across the entire enterprise FireEye deployment forming the FireEye Dynamic Threat Intelligence™ (DTI) enterprise.

YARA-based rules enables customization

The FireEye MAS supports custom YARA rules importation to specify byte-level rules and quickly analyze suspicious objects for threats specific to the organization.

Global malware protection network

The FireEye MAS is designed for easy integration with the entire FireEye platform. The FireEye MAS can automatically share malware forensics data with other FireEye MPS appliances via the FireEye CMS, block outbound data exfiltration attempts, and also stop inbound known attacks. The FireEye MAS threat data can also be shared via the FireEye DTI cloud to protect against new emerging attacks.

With pre-configured FireEye MVX engines eliminating the need for tuning heuristics, the FireEye MAS saves administrators setup time and configuration issues. The FireEye MAS appliance helps threat researchers analyze advanced targeted attacks without adding network and security management overhead.

Technical Specifications

	MAS 4310	MAS 7300	MAS 8300
Form Factor	1U Rack-Mount	1U Rack-Mount	2U Rack-Mount
Weight	30 lbs (13.6 Kg)	30 lbs (13.6 Kg)	50 lbs (22.7 Kg)
Dimensions (WxDxH)	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 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 Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Monitoring Ports	N/A	N/A	(2) 10/100/1000 BASE-T Ports
Performance	Up to 25,000 Objects Per Day	Up to 50,000 Objects Per Day	Up to 100,000 Objects 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	8.5–6.0 A	8.5–6.0 A	9.5–7.2 A
Power Supply/RAID	Dual 700W / 2 SAS HDD in HW RAID1	Dual 700W / 2 SAS HDD in HW RAID1	Dual 1400W / 2 SAS HDD in HW RAID1
Frequency	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

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