FireEye

Datasheet

Malware Analysis System

Next Generation Forensic Analysis of Advanced Targeted Attacks

Highlights

- Streamlines and batches analysis of suspicious files, Web code, and executables
- Reports in-depth on system-level OS and application changes to file systems, memory, and registries
- Offers sandbox or live–mode analysis to confirm zero-day exploits
- Eliminates deployment headaches and tuning with a pre-configured environment, plus automated setup and teardown of virtual test images
- Dynamically generates malware intelligence for immediate local protection via Central Management System (CMS) integration
- Captures packets to allow analysis of malicious URL session and code execution
- Supports custom YARA rules (compatible with version 1.3)
- Includes AV-Suite checks to streamline incident response prioritization
- Supports remote third-party AAA (Authentication, Authorization, and Accounting) network service access in addition to local authentication

MAS dashboard shows status of completed and pending VX 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 targeted APT attacks embedded in files, email attachments, and Web objects.

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 very targeted malicious activities.

Assess OS, browser and application attacks

The FireEye Virtual Execution (VX) 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 VX engine fully executes suspicious code to allow deep inspection of common file formats, email attachments, and Web objects. FireEye MAS inspects single files or batches of files for malware and tracks outbound connection attempts across multiple protocols.

Spend time analyzing, not administering

The VX engine features virtualized PC hardware running full-fledged versions of Microsoft operating systems as well as browsers, plug-ins, and other third-party applications. The MAS appliance frees administrators from time-consuming setup, baselining, and restoration of the virtual machine environments used in manual malware analysis.

Choose sandbox or honeypot analysis modes

In sandbox mode, researchers can witness the execution path of particular malware samples as well as generate a dynamic and anonymized profile of the attack that can be distributed through the

"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 optimal option for resolving an issue. It puts us in the position of knowing exactly how to react."

— Director of Cyber Security, Energy Sector

CMS to other FireEye Web, Email, and File Malware Protection System (MPS) appliances. Malware attack profiles 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.

In addition to sandbox analysis, FireEye offers a live, on-network "honeypot" mode for full malware lifecycle analysis. Today's advanced malware circumvents traditional security by unfolding in multiple stages. The first vulnerability exploit stage simply establishes a beachhead for criminals.

FireEye integrates inbound and outbound inspections across multiple protocols for comprehensive threat analysis of OS, Web, email, and application threats that attack across multiple vectors.

YARA-based rules enables customization

The MAS supports custom YARA rule importation to specify byte-level rules and quickly analyze suspicious objects for threats specific to the organization. The custom rules are used as part of the VX engine analysis to identify likely malicious objects as well as objects previously classified as malicious.

Global malware protection network

Malware Analysis Systems can automatically share malware forensics data to other MPS appliances via the FireEye CMS to block outbound data exfiltration attempts and stop inbound known attacks. MAS threat data can also be shared via the FireEye Malware Protection Cloud (MPC) to protect against emerging attacks.

With pre-configured virtual execution engines eliminating the need for tuning heuristics, the FireEye MAS saves administrators setup time and configuration headaches. This is an easy-to-manage, cost-effective solution that helps threat researchers analyze advanced targeted attacks without adding network and security management overhead.

Technical Specifications

	MAS 4310	MAS 7300
Form Factor	1U Rack-Mount	1U Rack-Mount
Weight	30 lbs (13.6 Kg)	30 lbs (13.6 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)
Enclosure	Fits 19-Inch Rack	Fits 19-Inch Rack
Management Interfaces	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Monitoring Interfaces	N/A	N/A
Performance Rating	25,000 objects per day	50,000 objects per day
AC Input Voltage	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range
AC Input Current	8.5-6 A	8.5-6 A
Power Supply/RAID	Dual / 2 SAS HDD in HW RAID1	Dual / 2 SAS HDD in HW RAID1
Frequency	50-60 Hz	50-60 Hz
AC Power	700 W Max	700 W Max
Ambient Temp	40° C	40° C