DATA SHEET

FireEye

Malware Analysis

Analyze attacks with 360-degree visibility

Figure 1. FireEye Malware Analysis AX 5550 appliance.

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
- Dynamically generates threat intelligence for immediate local protection via integration with FireEye Central Management
- Captures packets to allow analysis of malicious URL session and code execution
- Includes the FireEye AV-Suite to streamline incident response prioritization
- Includes support for Windows and MacOS X environments

Overview

FireEye Malware Analysis is a forensic analysis solution that gives security 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 cyber criminals 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

Malware Analysis uses the FireEye Multi-Vector Virtual Execution™ (MVX) engine to provide 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 Microsoft Windows and Apple MacOS X virtual analysis environment, the MVX engine fully executes suspicious code to allow deep inspection of common web objects, email attachments and files. Malware Analysis uses the 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

Malware Analysis 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, Malware Analysis uses enables forensic analysts to arrive at a comprehensive understanding of the attack that is suited to the needs of the enterprise.

Choose live analysis or sandbox modes

Malware Analysis provides users with 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 Malware Analysis the ability to track advanced attacks across multiple stages and different vectors. In sandbox mode, the execution path of particular malware samples is fully contained and visible in the virtual environment.

In both modes, users can generate a dynamic and anonymized profile of the attack that can be shared through FireEye Central Management to other FireEye solutions. The malware attack profiles generated by Malware Analysis includes 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 organization's entire FireEye deployment via FireEye Dynamic Threat Intelligence™ (DTI).

YARA-based rules enables customization

Malware Analysis 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

Malware Analysis can automatically share malware forensics data with other FireEye solutions via Central Management, block outbound data exfiltration attempts and stop inbound known attacks. Threat data from Malware Analysis can 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, Malware Analysis saves administrators setup time and configuration issues. This solution also helps threat researchers analyze advanced targeted attacks without adding network and security management overhead.

Table 1. Technical specifications.

	AX 5550
Performance *	Up to 8,200 Analyses Per Day
OS Support	Microsoft Windows / Apple Mac OSX
Network Interface Ports	2x 10/100/1000BASE-T Ports
IPMI Port (rear panel)	Included
Front Panel LCD and Keypad	Included
PS/2 Keyboard and Mouse, DB15 VGA ports (rear panel)	Included
USB Ports (rear panel)	4x Type A USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Drive Capacity	4x 1 TB HDD, RAID 10, 3.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2" x 27.8" x 1.7" (437 x 706 x 43.2 mm)
DC Power Supply	Not Available
AC Power Supply	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 – 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU
Power Consumption Maximum	292 watts
Thermal Dissipation Maximum	996 BTU/h

Table 1. Technical specifications.

	AX 5550
MTBF	54,200 h
Appliance Alone / As Shipped Weight lb. (kg)	33 lb. (15 kg) / 48 lb. (22 kg)
Safety Certifications	IEC 60950, EN 60950, CSA 60950-00, CE Marking
EMC/EMI Certifications	FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A)
Regulatory Compliance	RoHS, REACH, WEEE
Operating Temperature	10° C to 35° C
Operating Relative Humidity	10% to 85% (non-condensing)
Operating Altitude	5,000 ft.

Note: Performance numbers are based on default analysis times when using the Malware Analysis, but will vary depending on the system configuration and traffic profiles being processed.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FireEye