AX Series

Forensic analysis platforms that provide a full 360-degree view of a cyber attack

Figure 1. AX 5550 and AX 8400

OVERVIEW

The FireEye® AX series is a group of forensic analysis platforms that give 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 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 AX series utilizes 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 Mac OS X virtual analysis environment, the FireEye MVX engine fully executes suspicious code to allow deep inspection of common Web objects, email attachments and files. The FireEye AX platform 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 AX series 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 AX series enables forensic analysts to arrive at a comprehensive understanding of the attack that is suited to the needs of the enterprise.

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 the FireEye CM platform
- 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 Mac OS X environments

FireEye

Choose live analysis or sandbox modes

The FireEye AX series 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 AX series 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 are able to generate a dynamic and anonymized profile of the attack that can be shared through the FireEye CM platform to other FireEye products. The malware attack profiles generated by the FireEye AX platforms 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 organization's entire FireEye deployment via the FireEye Dynamic Threat Intelligence™ (DTI) enterprise.

YARA-based rules enables customization

The FireEye AX series 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 AX series is designed for easy integration with the entire FireEye threat prevention portfolio. The FireEye AX series can automatically share malware forensics data with other FireEye platforms via the FireEye CM, block outbound data exfiltration attempts and stop inbound known attacks. The FireEye AX series 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 AX series saves administrators setup time and configuration issues. In addition, the FireEye AX series helps threat researchers analyze advanced targeted attacks without adding network and security management overhead.

Table 1. Technical Specifications

	AX 5550	AX 8400
Performance *	Up to 8,200 Analyses Per Day	Up to 16,000 Analyses Per Day
OS Support	Microsoft Windows / Apple Mac OSX	Microsoft Windows
Network Interface Ports	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports
IPMI Port (rear panel)	Included	Included
Front Panel LCD and Keypad	Included	Included
PS/2 Keyboard and Mouse, DB15 VGA ports (rear panel)	Included	Included
USB Ports (rear panel)	4x Type A USB Ports	2x Type A USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Drive Capacity	4x 900 GB HDD, RAID 10, 2.5 inch, FRU	2x 600 GB HDD, RAID 1, 2.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2" x 27.8" x 1.7" (437 x 706 x 43.2 mm)	17.2" x 28.0" x 3.41" (437 x 711 x 86.6 mm)

Table 1. Technical Specifications

	AX 5550	AX 8400
DC Power Supply	Not Available	Not Available
AC Power Supply	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 – 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 – 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU
Power Consumption Maximum (watts)	292 watts	506 watts
Thermal Dissipation Maximum (BTU/h)	996 BTU/h	1726 BTU/h
MTBF (h)	40,700 h	68,900 h
Appliance Alone / As Shipped Weight lb. (kg)	33 lb. (15 kg) / 48 lb. (22 kg)	42 lb. (19 kg) / 57 lb. (26 kg)
Safety Certifications	IEC 60950, EN 60950, CSA 60950-00, CE Marking	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)	FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A)
Regulatory Compliance	RoHS, REACH, WEEE	RoHS, REACH, WEEE
Operating Temperature	10° C to 35° C	10° C to 35° C
Operating Relative Humidity	10% to 85% (non-condensing)	10% to 85% (non-condensing)
Operating Altitude	5,000 ft.	5,000 ft.

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

For more information on FireEye, visit:

www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 tel: 408.321.6300 / 877 FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye® is the leader in intelligence-led security-as-a-service. 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 has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye