FireEye

Datasheet

FireEye Network Threat Prevention Platform

Threat Prevention Platform that Combats Web-based Cyber Attacks

Highlights

- Deploys in-line (block/monitor mode) or out-of-band (TCP reset mode/monitor mode) and enables security analysis for IPv6 traffic
- Analyzes all suspicious Web objects including PDFs, Flash, multimedia formats, and ZIP/RAR/TNEF archives as well as blocks outbound malware to thwart data exfiltration
- Integrates with the FireEye Threat Prevention Platform to stop blended spear-phishing attacks
- Distributes threat intelligence locally to the entire FireEye deployment and globally to the FireEye customer base through the FireEye Dynamic Threat Intelligence (DTI) cloud
- Supports remote third-party AAA network service access in addition to local authentication
- Provides role-based access control (RBAC) and audit logging
- Consolidates signature-based and signature-less technologies, with the IPS add-on license to FireEye Network, to automatically reduce false alerts and drive down operational spend

NX 2400, NX 4420, NX 7420, NX 10000
(not pictured NX 1400, NX 4400, NX 7400)

The FireEye® Network Threat Prevention Platform identifies and blocks zero-day Web exploits, droppers (binaries), and multi-protocol callbacks to help organizations scale their advanced threat defenses across a range of deployments, from the multi-gigabit headquarters down to remote, branch, and mobile offices. FireEye Network with Intrusion Prevention System (IPS) technology further optimizes spend, substantially reduces false positives, and enables compliance while driving security across known and unknown threats.

Cybercriminals use the Web as a primary threat vector to deliver zero-day exploits and malicious URLs in email and exfiltrate data. FireEye Network is designed to stop drive-by downloads and blended Web and email attacks. In addition, FireEye Network offers a defense against infections that take place outside the network.

Real-time threat prevention blocks Web-based attacks

FireEye Network can be deployed in-line at Internet egress points to block Web exploits and outbound multi-protocol callbacks. Utilizing the FireEye Multi-vector Virtual Execution™ (MVX) engine, FireEye Network confirms zero-day attacks, creates real-time threat intelligence, and captures dynamic callback destinations. In monitor mode, it signals incident response mechanisms. In out-of-band prevention mode, FireEye Network issues TCP resets for out-of-band blocking of TCP, UDP, or HTTP connections.

Fights blended attacks across Web and email threat vectors

The FireEye Platform protects against blended, advanced attacks that use Web, spear-phishing emails, and zero-day exploits. With FireEye Network, FireEye Email, and FireEye Central Management, customers get real-time protection against malicious URLs and the ability to connect the dots of a blended attack.

Protects against unknown, zero-day attacks

FireEye Network uses the signature-less FireEye MVX engine which executes suspicious binaries and Web objects against a range of browsers, plug-ins, applications, and operating environments that track vulnerability exploitation, memory corruption, and other malicious

actions. As the attack plays out, the FireEye MVX engine captures callback channels, dynamically creates blocking rules, and transmits this information back to FireEye Network.

YARA-based rules enable customization

With support for custom YARA rules, security analysts can specify which Web objects should be analyzed for threats.

Streamlined incident prioritization

With the FireEye AV-Suite, each malicious object can be further analyzed to determine if anti-virus vendors were able to detect the malware stopped by FireEye Network. This enables customers to more efficiently prioritize incident response.

Dynamic threat intelligence sharing

The resulting dynamically generated, real-time threat intelligence produced by FireEye Network helps all FireEye products protect the local network. This intelligence includes callback coordinates and communication characteristics which can be shared globally through the FireEye Dynamic Threat Intelligence™ (DTI) cloud to notify all subscribers of new threats.

No rules tuning and near-zero false positives

FireEye Network is an easy-to-manage, clientless platform that deploys in under 60 minutes and requires absolutely no tuning. It offers flexible deployment modes, including out-of- band via a TAP/SPAN, in-line monitoring, or in-line active blocking.

Active fail open support

FireEye Network supports integration with the active fail open switch to ensure no link downtime and drives continued availability for in-line hardware deployments in the face of power or link failures. The active fail open switch leverages heartbeat technology to monitor availability of the FireEye Network device and automatically switches to bypass in case of failure.

IPS support

FireEye Network with IPS consolidates advanced threat prevention with traditional security to optimize spend. It automates alert validation, leveraging the power of MVX to reduce false alerts and illuminates attacks hidden within the noise to drive down OPEX and reduce the business exposure of missed incidents. FireEye Network complements the signature-less security provided by MVX with the signature-based security of the traditional IPS technology to augment security and enable compliance.

FireEye™

Datasheet

Technical Specifications

	NX 900	NX 1400	NX 2400	NX 4400/4420	NX 7400/7420	NX 10000
Form Factor	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount	2U Rack-Mount	2U Rack-Mount
Weight	17 lbs (7.7Kg)	22 lbs (9.9Kg)	22 lbs (9.9Kg)	30 lbs (13.6 Kg)	50 lbs (22.7 Kg)	60 lbs (27.2 Kg)
Dimensions (WxDxH)	16.8" x 14.0" x 1.7" (42.6 x 35.6 x 4.3 cm)	16.8" x 14.0" x 1.7" (42.6 x 35.6 x 4.3 cm)	16.8" x 14.0" x 1.7" (42.6 x 35.6 x 4.3 cm)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3 cm)	17.2" x 25.6" x 3.5" (43.7 x 65.0 x 8.9 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	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	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Monitoring Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(4) 10/100/1000 BASE-T Ports	4400: (4) 10/100/1000 BASE-T Ports 4420: (4) 1000 BASE-SX Fiber Optic Ports (LC Multimode)	7400: (4) 10/100/1000 BASE-T Ports 7420: (4) 1000 BASE-SX Fiber Optic Ports (LC Multimode)	(2) 10G BASE-SR/SW 850nm (LC Multimode)
Performance	Up to 10 Mbps	Up to 20 Mbps	Up to 50 Mbps	Up to 250 Mbps	Up to 1 Gbps	Up to 4 Gbps
User Count	50	100	500	2,500	10,000	40,000
AC Input Voltage	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range
AC Input Current	4.8–2.0 A	4.8–2.0 A	4.8–2.0 A	8.5–6.0 A	8.5–6.0 A	9.0–7.0 A
Power Supply/RAID	Single 200W / No	Single 260W / No	Single 260W / No	Dual 700W / 2 SAS HDD in HW RAID1	Dual 700W / 2 SAS HDD in HW RAID1	Dual 1200W / 2 SAS SSD in HW RAID1
Power Consumption (Max)	528 BTU/hr	648 BTU/hr	682 BTU/hr	921 BTU/hr	1552 BTU/hr	4095 BTU/hr
Frequency	50–60 Hz	50–60 Hz	50–60 Hz	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	10° C to 35° C	10° C to 35° C	10° C to 35° C

IPS Technical Specifications

	NX 900	NX 1400	NX 2400	NX 4400/4420	NX 7400/7420	NX 10000
IPS Performance	10 Mbps	20 Mbps	50 Mbps	250 Mbps	1 Gbps	4 Gbps
Concurrent Connections	4K	7.5K	15K	80K	500K	2M
New Connections Per Second	200/Sec	375/Sec	750/Sec	4K/Sec	10K/Sec	40K/Sec
Packets Per Second	600/Sec	1200/Sec	4k/Sec	20K/Sec	90K/Sec	120K/Sec

Active Fail Open Switch Technical Specifications

	AFO 1G Switch	AFO 10G Switch
Dimensions (WxDxH)	8.75" x 11.0" x 1.35" (22.2 x 27.9 x 3.4 cm)	6.5" x 14.0" x 1.125" (16.5 x 35.6 x 2.8 cm)
Management Ports	(1) DB9 Serial Console, (1) RJ45 Cat5e Port (10/100)	(1) DB9 Serial Console, (1) RJ45 Cat5e Port (10/100)
Network Ports	(2) RJ45 Cat5e Ports (10/100/1000)	(1) Quad LC Connector
Monitoring Ports	(2) RJ45 Cat5e Ports (10/100/1000)	(2) XFP Ports
AC Power Input	100 ~ 240 VAC, 0.5 A, 47-63 Hz	100 ~ 240 VAC, 1.0 A, 47-63 Hz
Operating Temp	0° C to 40° C	0° C to 40° C

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