NX Series

Threat Prevention Platforms that Combat Web-based Cyber Attacks

Highlights

- Deploys in-line (block/monitor mode) or out-of-band (TCP reset mode/monitor mode)

- 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

- Streamlines incident response prioritization with AV-Suite integration

- Integrates with FireEye EX series 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

The FireEye® NX series identifies and blocks zero-day Web exploits, droppers [binaries], and multi-protocol callbacks that traditional and next-generation firewalls, IPS, AV, and Web gateways miss.

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

Real-time threat prevention blocks Web-based attacks

The FireEye NX platforms 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, the FireEye NX series 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, the FireEye NX series 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 the FireEye NX, EX, and CM series, 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

The FireEye NX series 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 the FireEye NX platform.

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

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 the FireEye NX platform. This enables customers to more efficiently prioritize incident response.

Dynamic threat intelligence sharing

The resulting dynamically generated, real-time threat intelligence produced by the FireEye NX 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

The NX series is a group of easy-to-manage, clientless platforms that deploy 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.

Technical Specifications

	NX 1400	NX 2400	NX 4400	NX 4420	NX 7400	NX 7420	NX 10000
Form Factor	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount	1U Rack-Mount	2U Rack-Mount	2U Rack-Mount	2U Rack-Mount
Weight	12 lbs (5.4Kg)	12 lbs (5.4Kg)	30 lbs (13.6 Kg)	30 lbs (13.6 Kg)	50 lbs (22.7 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)	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 25.6" x 3.5" (43.7 x 65.0 x 8.9 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	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	(2) 10/100/1000 BASE-T Ports
Monitoring Ports	(2) 10/100/1000 BASE-T Ports	(4) 10/100/1000 BASE-T Ports	(4) 10/100/1000 BASE-T Ports	(4) 1000 BASE-SX Fiber Optic Ports (LC Multimode)	(4) 10/100/1000 BASE-T Ports	(4) 1000 BASE-SX Fiber Optic Ports (LC Multimode)	(2) 10G BASE - SR/SW 850nm (LC Multimode)
Performance	Up to 20 Mbps	Up to 50 Mbps	Up to 250 Mbps	Up to 250 Mbps	Up to 1 Gbps	Up to 1 Gbps	Up to 4 Gbps
User Count	100	500	2,500	2,500	10,000	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	Auto-switching 100 ~ 240 VAC Full Range
AC Input Current	4.8–2.0 A	4.8–2.0 A	8.5–6.0 A	8.5–6.0 A	8.5–6.0 A	8.5–6.0 A	9.0–7.0 A
Power Supply/ RAID	Single 260W / No	Single 260W / No	Dual 700W / 2 SAS HDD in HW RAID1	Dual 700W / 2 SAS HDD in HW RAID1	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)	648 BTU/hr	682 BTU/hr	921 BTU/hr	921 BTU/hr	1552 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	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	10° C to 35° C

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