FireEye
SECURITY REIMAGINED

# FireEye Network Threat Prevention Platform

## Threat Prevention Platform that Combats Web-based Cyber Attacks

DATA SHEET

### 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
- Includes support for Windows and Mac OS X environments
- 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
- Drives down IPS operational spend with automated noise reduction capability

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

### Overview

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.

## Technical Specifications

| | NX 900 | NX 1400 | NX 2400 | NX 4400/4420 | NX 7400/7420 | NX 7500 | NX 9450 | NX 10000 | NX 10450 |
|---|---|---|---|---|---|---|---|---|---|
| User Count | 50 | 100 | 500 | 2,500 | 10,000 | 10,000 | 20,000 | 40,000 | 40,000 |
| OS Support | Microsoft Windows | Microsoft Windows | Microsoft Windows | Microsoft Windows | Microsoft Windows | Microsoft Windows Mac OS X | Microsoft Windows | Microsoft Windows | Microsoft Windows |
| Performance * | Up to 10 Mbps | Up to 20 Mbps | Up to 50 Mbps | Up to 250 Mbps | Up to 1 Gbps | Up to 1 Gbps | Up to 2 Gbps | Up to 4 Gbps | Up to 4 Gbps |
| Network Monitoring Ports | 2x 10/100/1000 BASE- T Ports | 2x 10/100/1000 BASE- T Ports | 4x 10/100/1000 BASE- T Ports | 4400: 4x 10/100/ 1000 BASE- T Ports<br><br>4420: 4x 1000 BASE-SX Fiber Optic Ports (LC Multimode) | 7400: 4x 10/100/ 1000 BASE- T Ports<br><br>7420: 4x 1000 BASE-SX Fiber Optic Ports (LC Multimode) | 4x 10/100/1000 BASE- T Ports | 4x SFP+, 4xSFP ports, 1000baseSX (LC MMF), 1000baseLX (LC, SMF), 1000baseT (RJ45, UTP5) | 2x 10GBASE - SR/ SW 850nm Fixed interfaces: 10GbaseSX (LC MMF) | 8 x SFP+ (4 x 1000base and 4 x 10Gbase), 1000baseSX/ 10GbaseSR (LC, MMF), 1000baseLX/ 10GbaseLR (LC SMF), 1000baseT (RJ45, UTP5), 10GbaseCu (5m direct-attached-cable) |
| Network Ports Mode of Operation | Inline Monitor, Fail-Open, Fail-Close, or Tap/Span, HW Bypass | Inline Monitor, Fail-Open, Fail-Close, or Tap/Span, HW Bypass | Inline Monitor, Fail-Open, Fail-Close, or Tap/Span, HW Bypass | Inline Monitor, Fail-Open, Fail-Close, or Tap/Span, HW Bypass | Inline Monitor, Fail-Open, Fail-Close, or Tap/Span, HW Bypass | Inline Monitor, Fail-Open, Fail-Close, or Tap/Span, HW | Inline Monitor, or Tap/Span | Inline Monitor, Fail-Open, Fail-Close, or Tap/Span, HW Bypass | Inline Monitor, or Tap/Span |
| Management Ports (rear panel) | 2x 10/100/1000 BASE-T Ports | 2x 10/100/1000 BASE- T Ports | 2x 10/100/1000 BASE- T Ports | 2x 10/100/1000 BASE- T Ports | 2x 10/100/1000 BASE- T Ports | 2x 10/100/1000 BASE- T Ports | 2x 10/100/1000 BASE- T Ports | 2x 10/100/1000 BASE- T Ports | 2x 10/100/1000 BASE- T Ports |
| IPMI Port (rear panel) | Included | Included | Included | Included | Included | Included | Included | Included | Included |
| Front LCD & Keypad | Not Available | Included | Included | Included | Included | Included | Included | Included | Included |
| PS/2 Keyboard and Mouse, DB15 VGA Ports (rear panel) | Included | Included | Included | Included | Included | Included | Included | Included | Included |
| USB Ports (rear panel) | 2x Type A USB Ports | 2x Type A USB Ports | 2x Type A USB Ports | 2x Type A USB Ports | 2x Type A USB Ports | 4x Type A USB Ports | 2x Type A USB Ports | 2x 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 | 115,200 bps, No Parity, 8 Bits, 1 Stop Bit | 115,200 bps, No Parity, 8 Bits, 1 Stop Bit | 115,200 bps, No Parity, 8 Bits, 1 Stop Bit | 115,200 bps, No Parity, 8 Bits, 1 Stop | 115,200 bps, No Parity, 8 Bits, 1 Stop Bit | 115,200 bps, No Parity, 8 Bits, 1 Stop Bit | 115,200 bps, No Parity, 8 Bits, 1 Stop Bit |
| Drive Capacity | Single 500 GB HDD, Internal, fixed | Single 500 GB HDD, Internal, fixed | Single 500 GB HDD, Internal, fixed | 2x 600 GB HDD, RAID 1, 2.5 inch, FRU | 2x 600 GB HDD, RAID 1, 2.5 inch, FRU | 4x 900 GB HDD, RAID 10, 2.5 inch, FRU | 4x 900 GB HDD, RAID 10, 2.5 inch, FRU | 2x 800 GB SSD, RAID 1, 2.5 inch, FRU | 4x 800 GB SSD, RAID 10, 2.5 inch, FRU |
| Enclosure | 1RU, Fits 19 inch Rack | 1RU, Fits 19 inch Rack | 1RU, Fits 19 inch Rack | 1RU, Fits 19 inch Rack | 2RU, Fits 19 inch Rack | 2RU, Fits 19 inch Rack | 2RU, Fits 19 inch Rack | 2RU, Fits 19 inch Rack | 2RU, Fits 19 inch Rack |
| Chassis Dimension WxDxH | 16.8" x 14" x 1.7" (427 x 356 x 43 mm) | 17.2" x 24.1" x 1.70" (437 x 612 x 43.2mm) | 17.2" x 24.1" x 1.70" (437 x 612 x 43.2 mm) | 17.2" x 27.8" x 1.70" (437 x 706 x 43.2 mm) | 17.2" x 28.0" x 3.41" (437 x 711 x 86.5 mm) | 17.2" x 28" x 3.41" (437 x 711 x 86.6mm) | 17.2" x 27.9" x 3.5" (437 x 709 x 89 mm) | 17.2" x 27.9" x 3.5" (437 x 709 x 89 mm) | 17.2" x 27.9" x 3.5" (437 x 709 x 89 mm) |
| DC Power Supply | Not Available | Not Available | Not Available | Not Available | Not Available | Not Available | Not Available | Not Available | Not Available |

## Technical Specifications

| | NX 900 | NX 1400 | NX 2400 | NX 4400/4420 | NX 7400/7420 | NX 7500 | NX 9450 | NX 10000 | NX 10450 |
|---|---|---|---|---|---|---|---|---|---|
| AC Power Supply | Non-redundant, non-FRU, internal 200 watt, 100 - 240 VAC 3 – 1.5A, 50-60 Hz IEC60320-C14 Inlet | Non-redundant, non-FRU, internal 500 watt, 100 ~ 240 VAC 5 – 2.5A, 50-60 Hz IEC60320-C14 inlet | Non-redundant, non-FRU, internal 500 watt, 100 ~ 240 VAC 5 – 2.5A, 50-60 Hz IEC60320-C14 inlet | 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 | Redundant (1+1) 750 watt, 100 - 240 VAC 9 – 4.5A, 50-60 Hz IEC60320-C14 inlet, FRU | Redundant (1+1) 1200 watt, 100-140 VAC, 14.7 - 10.5 A 1400 watt, 180-240 VAC, 9.5 - 7.2 A, 50-60 Hz, FRU IEC60320-C14 inlet, FRU | Redundant (1+1) 1200 watt, 100-140 VAC, 14.7 - 10.5 A 1400 watt, 180-240 VAC, 9.5 - 7.2 A, 50-60 Hz, FRU IEC60320-C14 inlet, FRU | Redundant (1+1) 1200 watt, 100-140 VAC, 14.7 - 10.5 A 1400 watt, 180-240 VAC, 9.5 - 7.2 A, 50-60 Hz, FRU IEC60320-C14 inlet, FRU |
| Power Consumption Maximum (watts) | 136 watts | 208 watts | 210 watts | 305 watts | 501 watts | 479 watts | 550W | 962 watts | 850W |
| Thermal Dissipation Maximum (BTU/h) | 464 BTU/h | 710 BTU/h | 717 BTU/h | 1041 BTU/h | 1709 BTU/h | 1634 BTU/h | 1881 BTU/h | 3282 BTU/h | 2908 BTU/h |
| MTBF (h) | 94,700 h | 67,500 h | 55,200 h | 37,000 h | 58,900 h | 58,900 h | 52,469 h | 50,200 h | 40,275 h |
| Appliance Alone / As Shipped Weight lb. (kg) | 11 lb. (5 kg) / 20 lb. (9 kg) | 24 lb. (11 kg) / 39 lb. (18 kg) | 24 lb. (11 kg) / 39 lb. (18 kg) | 31 lb. (14 kg) / 46 lb. (21 kg) | 42 lb. (19 kg) / 58 lb. (26 kg) | 43 lb. (19.5 kg) / 59 lb. (27kg) | 51 lb. (23 kg) / 66 lb. (30 kg) | 51 lb. (23 kg) / 66 lb. (30 kg) | 51 lb. (23 kg) / 66 lb. (30 kg) |
| Safety Certifications | IEC 60950 EN 60950 CSA 60950-00 CE Marking | IEC 60950 EN 60950 CSA 60950-00 CE Marking | IEC 60950 EN 60950 CSA 60950-00 CE Marking | IEC 60950 EN 60950 CSA 60950-00 CE Marking | IEC 60950 EN 60950 CSA 60950-00 CE Marking | IEC 60950 EN 60950 CSA 60950-00 CE Marking | IEC 60950-1 EN 60950-1 CSA 60950-1 CE Marking | IEC 60950-1 EN 60950-1 CSA 60950-1 CE Marking | IEC 60950-1 EN 60950-1 CSA 60950-1 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) | 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) | 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) | 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) | FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A) |
| Regulatory Compliance | RoHS, REACH, WEEE | RoHS, REACH, WEEE | RoHS, REACH, WEEE | RoHS, REACH, WEEE | RoHS, REACH, WEEE | RoHS, REACH, WEEE | RoHS, REACH, WEEE | RoHS, REACH, WEEE | RoHS, REACH, WEEE |
| Operating Temperature | 10°C to 35°C Tested from 0°C to 40°C for additional margin | 10° C to 35° C Tested from 0°C to 40°C for additional margin | 10° C to 35° C Tested from 0°C to 40°C for additional margin | 10° C to 35° C Tested from 0°C to 40°C for additional margin | 10° C to 35° C Tested from 0°C to 40°C for additional margin | 10° C to 35° C Tested from 0°C to 40°C for additional margin | 10° C to 35° C | 10° C to 35° C | 10° C to 35° C |
| Non-Operating Temperature | -40°C to 70°C | -40°C to 70°C | -40°C to 70°C | -40°C to 70°C | -40°C to 70°C | -40°C to 70°C | -40°C to 70°C | -40°C to 70°C | -40°C to 70°C |
| Operating Relative Humidity | 8% - 90% (non-condensing) | 8% - 90% (non-condensing) | 8% - 90% (non-condensing) | 8% - 90% (non-condensing) | 8% - 90% (non-condensing) | 8% - 90% (non-condensing) | 10% - 85% (non-condensing) | 10% - 85% (non-condensing) | 10% - 85% (non-condensing) |
| Non-Operating Relative Humidity | 5% - 95% (non-condensing) | 5% - 95% (non-condensing) | 5% - 95% (non-condensing) | 5% - 95% (non-condensing) | 5% - 95% (non-condensing) | 5% - 95% (non-condensing) | 5% - 95% (non-condensing) | 5% - 95% (non-condensing) | 5% - 95% (non-condensing) |
| Operating Altitude | 0m – 3000m with temperature de-rating of 1°C per 1000 m | 0m – 3000m with temperature de-rating of 1°C per 1000 m. | 0m – 3000m with temperature de-rating of 1°C per 1000 m | 0m – 3000m with temperature de-rating of 1°C per 1000 m | 0m – 3000m with temperature de-rating of 1°C per 1000 m | 0m – 3000m with temperature de-rating of 1°C per 1000 m | 5.000 ft | 5.000 ft | 5.000 ft |

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

## IPS Technical Specifications

| | NX 900 | NX 1400 | NX 2400 | NX 4400/4420 | NX 7400/7420 | NX 7500 | NX 9450 | NX 10000 | NX 10450 |
|---|---|---|---|---|---|---|---|---|---|
| IPS Performance | 10 Mbps | 20 Mbps | 50 Mbps | 250 Mbps | 1 Gbps | 1 Gbps | 2 Gbps | 4 Gbps | 4 Gbps |
| Concurrent Connections | 4K | 7.5K | 15K | 80K | 500K | 500K | 1M | 2M | 2M |
| New Connections Per Second | 200/Sec | 375/Sec | 750/Sec | 4K/Sec | 10K/Sec | 10K/Sec | 20K/Sec | 40K/Sec | 40K/Sec |
| Packets Per Second | 600/Sec | 1200/Sec | 4K/Sec | 20K/Sec | 90K/Sec | 90K/Sec | 105K/Sec | 120K/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.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@FireEye.com | **www.FireEye.com**