



## DATA SHEET

# FireEye Network Security

## Effective protection against cyber breaches for midsize to large organizations

### Overview

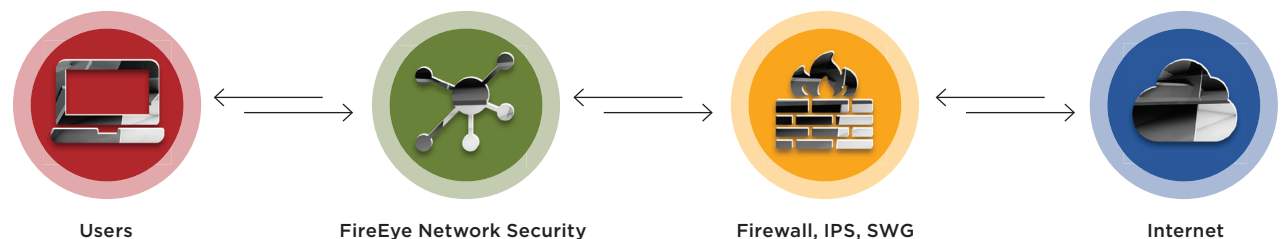
FireEye Network Security is an effective cyber threat protection solution that helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic. It facilitates efficient resolution of detected security incidents in minutes with concrete evidence, actionable intelligence and response workflow integration. With FireEye Network Security, organizations are effectively protected against today's threats whether they exploit Microsoft Windows, Apple OS X operating systems, or application vulnerabilities; are directed at the headquarters or branch offices; or are hidden in a large volume of inbound Internet traffic that has to be inspected in real time.

At the core of FireEye Network Security are the Multi-Vector Virtual Execution™ (MVX) and Intelligence-Driven Analysis (IDA) technologies. MVX is a signature-less, dynamic analysis engine that inspects suspicious network traffic to identify

attacks that evade traditional signature- and policy-based defenses. IDA is a collection of contextual, dynamic rules engines that detects and blocks malicious activity in real-time and retroactively, based on the latest machine-, attacker- and victim-intelligence. FireEye Network Security also includes intrusion prevention system (IPS) technology to detect common attacks using conventional signature matching.

FireEye Network Security is available in a variety of form factors, deployment and performance options. It is typically placed in the path of Internet traffic behind traditional network security appliances such as next-generation firewalls, IPS and secure web gateways (SWG). FireEye Network Security supplements these solutions by rapidly detecting both known and unknown attacks with high accuracy and a low rate of false positives, while facilitating an efficient response to each alert.

Figure 1. Typical configuration — Network Security solutions.



Capabilities	Benefits
<b>Detection</b>	
Accurate detection of advanced, targeted and other evasive cyber attacks	Minimizes risk of costly cyber breaches
Extensible, modular security architecture	Provides investment protection
Consistent level of protection for multi-OS environments and all Internet access points	Creates a strong defense across the entire organization for all types of devices
Integrated, distributed, physical, virtual, on-premise and cloud deployment options	Offers flexibility to align with organizational preferences and resources
Multi-vector correlation with Email and Content Security	Provides visibility across wider attack surface
<b>Prevention</b>	
Immediate blocking of attacks at line rates from 10 Mbps to 8 Gbps	Gives real-time protection against evasive attacks
<b>Response</b>	
Low rate of false alerts, riskware categorization and automated IPS alert validation	Reduces operational cost of triaging unreliable alerts
Pivot to investigation and alert validation, endpoint containment and incident response	Automates and simplifies security workflows
Execution evidence and actionable threat intelligence with contextual insight	Accelerates prioritization and resolution of detected security incidents
Scalability from one site to thousands of sites	Supports business growth

**Technical Advantages**

**Accurate Threat Detection**

FireEye Network Security uses multiple analysis techniques to detect attacks with high accuracy and a low rate of false alerts:

- **Multi-Vector Virtual Execution™ (MVX)** engine detects zero-day, multi-flow and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops infection and compromise phases of the cyber-attack kill chain by identifying never-before-seen exploits and malware.
- **Intelligence-Driven Analysis (IDA)** engines detect and block obfuscated, targeted and other customized attacks with contextual, rule-based analysis from real-time insights gathered on the front lines from millions of MVX verdicts, thousands of hours of incident response experience gathered by Mandiant, a FireEye company and hundreds of iSight threat researchers. It stops infection, compromise and intrusion phases of the cyber-attack kill chain by identifying malicious exploits, malware and command and control (CnC) callbacks. It also extracts and submits suspicious network traffic to the MVX engine for a definitive verdict analysis.
- **Structured Threat Intelligence eXpression (STIX)** allows the ingestion of third-party threat intelligence using an industry-standard format to add custom threat indicators into the IDA engines.

**Immediate and Resilient Protection**

FireEye Network Security offers flexible configuration modes including:

- Out-of-band monitoring via a TAP/SPAN, inline monitoring or inline active blocking. Inline blocking mode automatically blocks

inbound exploits and malware and outbound multi-protocol callbacks. In inline monitoring mode, alerts are generated and organizations decide how to respond to them. In out-of-band prevention mode, FireEye Network Security issues TCP resets for out-of-band blocking of TCP, UDP or HTTP connections.

- Selected models offer an active high availability (HA) option to provide resilience in case of network or device failures.

**Wide Attack Surface Coverage**

FireEye Network Security delivers a consistent level of protection for today’s diverse network environments:

- Support for most common Microsoft Windows and Apple Mac OS X operating systems
- Analysis of over 140 different file types, including portable executables (PEs), web content, archives, images, Java, Microsoft and Adobe applications and multimedia
- Execution of suspicious network traffic against thousands of operating system, service pack, application type and application version combinations

**Validated and Prioritized Alerts**

In addition to detecting genuine attacks, FireEye MVX technology is also used to determine the reliability of alerts detected by conventional signature-matching methods and to identify and prioritize critical threats:

- Intrusion prevention system (IPS) with MVX engine validation reduces the time required to triage signature-based detection that is traditionally prone to false alerts
- Riskware categorization separates genuine breach attempts from undesirable, but less malicious activity (such as adware and spyware) to prioritize alert response

**Actionable Threat Insights**

Alerts generated by FireEye Network Security include concrete evidence and contextual intelligence to quickly respond to, prioritize and contain a threat:

- **Dynamic Threat Intelligence (DTI):** concrete, real-time, globally-shared data to quickly and proactively stop targeted and newly discovered attacks
- **Advanced Threat Intelligence (ATI):** contextual insights about the attack to accelerate response and prescriptive guidance to contain the threat

**Response Workflow Integration**

FireEye Network Security can be augmented in several ways to automate alert response workflows:

- FireEye Central Management correlates alerts from both FireEye Network Security and FireEye Email Security for a broader view of an attack and to set blocking rules that prevent the attack from spreading further
- FireEye Network Forensics integrates with FireEye Network Security to provide detailed packet captures associated with an alert and enable in-depth investigations
- FireEye Endpoint Security identifies, validates and contains compromises detected by FireEye Network Security to simplify containment and remediation of affected endpoints

**Flexible Deployment Options**

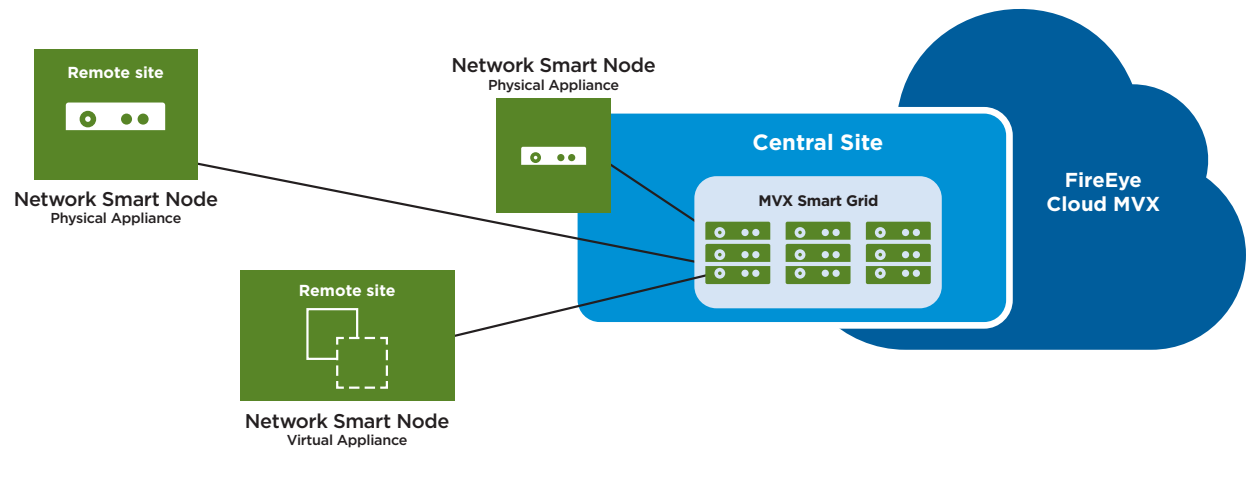
FireEye Network Security offers various deployment options to match an organization’s needs and budget:

- **Integrated Network Security:** standalone, all-in-one hardware appliance with integrated MVX service to secure an Internet access point at a single site. FireEye Network Security is an easy-to-manage, clientless platform that deploys in under 60 minutes. It doesn’t require rules, policies or tuning.

- **Distributed Network Security:** extensible appliances with centrally shared MVX service to secure Internet access points within organizations
  - **Network Smart Node:** physical or virtual appliances that analyze Internet traffic to detect and block malicious traffic and submit suspicious activity over an encrypted connection to the MVX service for definitive verdict analysis
  - **MVX Smart Grid:** on-premise, centrally located, elastic MVX service that offers transparent scalability, built-in N+1 fault tolerance and automated load balancing
  - **FireEye Cloud MVX:** FireEye-hosted MVX service subscription that ensures privacy by analyzing traffic on the Network Smart Node. Only suspicious objects are sent over an encrypted connection to the MVX service, where objects revealed as benign are discarded.



**Figure 2.** Examples of Integrated Network Security include NX 2550, NX 3500, NX 5500, NX 6500.



**Figure 3.** Distributed deployment models for Network Security.

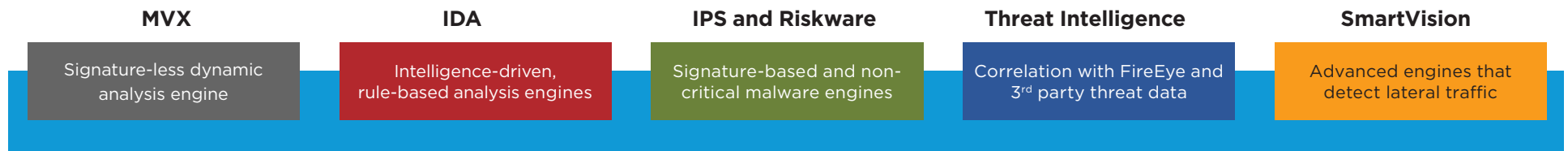


Figure 4. Modular components of FireEye Network Security.

**Extensible Architecture**

FireEye Network Smart Nodes feature a modular and extensible software architecture and system design to deliver multiple threat protection capabilities as software modules.

**High Performance and Scalability**

FireEye Network Security protects Internet access points at line rate with performance options for a wide variety of branch and central office sizes:

The MVX Smart Grid and FireEye Cloud MVX scalable architecture allows the MVX service to support one Network Smart Node to thousands and scale seamlessly as needed.

Form Factor	Performance
Integrated Network Security	50 Mbps to 5 Gbps
Physical Network Smart Node	50 Mbps to 10 Gbps
Virtual Network Smart Node	50 Mbps to 1 Gbps

**Business Benefits**

Designed to meet the needs of single-site and distributed multi-site organizations, FireEye Network Security delivers several benefits:

**Minimizes Risk of Cyber Breaches**

FireEye Network Security is a highly-effective cyber defense solution that:

- Prevents intruders from breaking into an organization to steal valuable assets or disrupt business by stopping advanced, targeted and other evasive attacks
- Stops attacks and contains intrusions faster with concrete evidence, actionable intelligence, inline blocking and response workflow automation
- Eliminates weak points from an organization’s cyber defenses with consistent protection for various operating systems, application types, branches and central sites

**Short Payback Period**

According to a recent Forrester Consulting study<sup>1</sup>, FireEye Network Security customers can expect a 152% ROI savings over three years and payback on their initial investment in just 9.7 months. FireEye Network Security:

- Focuses security team resources on real attacks to reduce operational expenses
- Optimizes capital spend with a shared MVX service and a large variety of performance points to rightsize deployment to meet requirements

- Future-proofs security investment by scaling smoothly when the number of branches or the amount of Internet traffic grows
- Protects existing investments by allowing cost-free migration from an integrated to a distributed deployment
- Reduces future capital outlay with modular and extensible architecture

**Awards and Certifications**

The FireEye Network Security product portfolio has been awarded a number of industry and government awards and certifications:

- In 2016, Frost & Sullivan recognized FireEye as the undisputed market leader with 56% market share, more than the next ten competitors combined<sup>2</sup>
- FireEye Network Security has been a recipient of numerous awards from SANS Institute, SC Magazine, CRN and others
- FireEye Network Security was the first security solution on the market to receive the US Department of Homeland Security SAFETY Act Certification



<sup>1</sup> Forrester (May 2016). The Total Economic Impact of FireEye.  
<sup>2</sup> Frost & Sullivan (October 2016). Network Security Sandbox Market Analysis

**Table 1.** FireEye Network Security specifications, integrated appliance.

	<b>NX 2500</b>	<b>NX 2550</b>	<b>NX 3500</b>	<b>NX 4500</b>	<b>NX 5500</b>	<b>NX 6500</b>
<b>OS Support</b>	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X
<b>Performance *</b>	Up to 50 Mbps or 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2.5 Gbps	Up to 5 Gbps
<b>Network Monitoring Ports</b>	4x 10/100/1000 BASE-T Ports (in front panel)	4x 10GigE SFP+ 4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 1GigE/10GigE SFP+ 2x 40GigE QSFP+
<b>Network Ports Mode of Operation</b>	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line, Monitor,TAP/SPAN
<b>High Availability (HA)</b>	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
<b>High Availability (HA) Ports (rear panel)</b>	Not Available	Not Available	Not Available	Not Available	2x 100/1000/10G Base-T Ports	Not Available
<b>Management Ports (rear panel)</b>	2x 10/100/1000 BASE- T Ports (in front 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	4x 1000BaseT Ports
<b>IPMI Port (rear panel)</b>	Included	Included	Included	Included	Included	Included
<b>Front LCD &amp; Keypad</b>	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
<b>VGA Port</b>	No	Yes	Yes	Yes	Yes	Yes
<b>USB Ports</b>	2x Type A USB Ports (front panel)	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	2x Type 3 USB Ports
<b>Serial Port (rear panel)</b>	115,200 bps, No Parity, 8 bits, 1 Stop Bit (RJ45 connector RJ45-to-Dsub adapter cable is included)	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	115200 bps, No Parity, 8 bits, 1 Stop Bit
<b>Drive Capacity</b>	Single 1TB 3.5 inch, SATA HDD, internal, fixed	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2x 10TB HDD 3.5", SAS3, 7.2krpm FRU RAID1
<b>Enclosure</b>	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
<b>Chassis Dimension WxDxH</b>	17.2in(437mm) x 19.7in(500mm) x 1.7in(43.2 mm)	17.2in(437mm) x 25.6in(650mm) x 1.7in(43.2mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in (88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.2"(437mm) x 31.0"(787mm) x 3.5"(89mm)
<b>AC Power Supply</b>	Single 250 watt, 90-264 VAC, 3.5 - 1.5 A, 50-60 Hz, IEC60320-C14, inlet, Internal, Fixed	Redundant (1+1) 750 watt, 100 - 240 VAC 9.0 - 4.5A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 - 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 - 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 - 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 1000 watt, 100 - 240 VAC 10.5 - 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU



**Table 2.** FireEye Network Security IPS performance, integrated appliance.

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
<b>Max IPS Performance</b>	Up to 50 Mbps or 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2.5 Gbps	Up to 5 Gbps
<b>Max Concurrent Connections</b>	15K or 80K	80K	160K	500K	1M	2M
<b>New Connections Per Second</b>	750/Sec or 4K/Sec	4K/Sec	8K/Sec	10K/Sec	20K/Sec	40K/Sec

**Table 3.** FireEye Network Security smart node, physical specifications.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
<b>OS Support</b>	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X
<b>Performance</b>	Up to 50 Mbps	Up to 100 Mbps or 250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2 Gbps	Up to 5 Gbps	Up to 10Gbps
<b>Network Monitoring Ports</b>	4x 10/100/1000 BASE-T Ports	4x 10/100/1000 BASE-T Ports (in front panel)	4x 10GigE SFP+ 4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 1GigE/10GigE SFP+ 2x 40GigE QSFP+
<b>Network Ports Mode of Operation</b>	In-line Monitor, Fail-Close or Tap	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line, Monitor,TAP/SPAN
<b>High Availability (HA)</b>	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
<b>High Availability (HA) Ports (rear panel)</b>	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
<b>Management Ports (rear panel)</b>	2x 10/100/1000 BASE- T Ports	4x 10/100/1000 BASE- T Ports (in front 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	4x 1000 BaseT Ports
<b>IPMI Port (rear panel)</b>	Not Available	Rear Panel	Included	Included	Included	Included	Included
<b>Front LCD &amp; Keypad</b>	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
<b>VGA Port</b>	Not Available	Not Available	Yes	Yes	Yes	Yes	Yes
<b>USB Ports</b>	2x Type A USB Ports	2x Type A USB Ports (front panel)	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	2x Type 3 USB Ports







**Table 3.** FireEye Network Security smart node, physical specifications. (continued)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500	
<b>Regulatory Compliance EMC</b>	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	Safety: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J60950, SI60950 EMC: FCC Part 15 SubPart B Class A; ICES-003; EN55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR32; KN 32; KN 35
<b>Environmental Compliance</b>	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS; REACH; WEEE Conflict Minerals	
<b>Operating Temperature</b>	0 - 40°C 32 - 104°F	0 - 40°C 32 - 104°F	0 - 35°C 32 - 95°F	0 - 35°C 32 - 95°F	0 - 35°C 32 - 95°F	0 - 35°C 32 - 95°F	10° C to 35° C Tested from 0°C to 40°C for additional margin	
<b>Non-Operating Temperature</b>	-20 - 80°C -4 - 176°F	-20 - 80°C -4 - 176°F	-40 - 70°C -40 - 158°F	-40 - 70°C -40 - 158°F	-40 - 70°C -40 - 158°F	-40 - 70°C -40 - 158°F	-30 - 70°C -22 - 158°F	
<b>Operating Relative Humidity</b>	5% - 85% non-condensing	5% - 85% non-condensing	10 - 95% @ 40° C, non-condensing	10 - 95% @ 40° C, non-condensing	10 - 95% @ 40° C, non-condensing	10 - 95% @ 40° C, non-condensing	10% - 90%@40°C non-condensing	
<b>Non-Operating Relative Humidity</b>	5% - 95% non-condensing	5% - 95% non-condensing	10 - 95% @ 60° C, non-condensing	10 - 95% @ 60° C, non-condensing	10 - 95% @ 60° C non- condensing	10 - 95% @ 60° C non- condensing	10% - 95%@55°C non-condensing	
<b>Operating Altitude</b>	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	

**Table 4.** FireEye Network Security smart node IPS, physical specifications.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
<b>Max IPS Performance</b>	Up to 50 Mbps	Up to 100 /250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2 Gbps	Up to 5 Gbps	Up to 10 Gbps
<b>Max Concurrent Connections</b>	15K	80K	160K	500K	1M	2M	4M
<b>New Connections Per Second</b>	750/sec	4K/Sec	8K/Sec	10K/Sec	20K/sec	40K/Sec	80K/Sec

**Table 5.** FireEye Network smart node, virtual specifications.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
<b>OS Support</b>	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X
<b>Performance *</b>	Up to 50 Mbps	Up to 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps
<b>Network Monitoring Ports</b>	1-8	1-8	1-8	1-8	1-8
<b>Network Management Ports</b>	1 or 2	1 or 2	1 or 2	1 or 2	1 or 2
<b>Network Ports Mode of Operation</b>	Inline, SPAN	Inline, SPAN	Inline, SPAN	Inline, SPAN	Inline, SPAN
<b>CPU Cores</b>	3	6	8	8	16
<b>Memory</b>	10GB	16GB	16GB	32 GB	32 GB
<b>Drive Capacity</b>	384 GB	384 GB	384 GB	512 GB	512 GB
<b>Network Adapters</b>	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC
<b>Hypervisor Support</b>	VMWare ESXi 6.0 or later	VMWare ESXi 6.0 or later	VMWare ESXi 6.0 or later	VMWare ESXi 6.0 or later	VMWare ESXi 6.0 or later
<b>Security Certifications</b>	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)

**Table 6.** FireEye Network smart node IPS, virtual specifications.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
<b>Max IPS Performance</b>	Up to 50 Mbps	Up to 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps
<b>Max Concurrent Connections</b>	15K	80K	80K	160K	500K
<b>New Connections Per Second</b>	750/Sec	4K/Sec	4K/Sec	8K/Sec	10K/Sec

**Table 7.** FireEye MVX smart grid specifications.

	<b>VX 5500</b>	<b>VX 12550</b>
<b>OS Support</b>	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X
<b>Performance *</b>	Up to 2 Gbps	Up to 14 Gbps
<b>High Availability **</b>	N+1	N+1
<b>Management Ports (rear panel)</b>	1x 10/100/1000 Mbps BASE- T Ports	1x 10/100/1000 Mbps BASE- T Ports
<b>Cluster Ports (rear panel)</b>	3x 10/100/1000 Mbps BASE-T Ports	1x 10/100/1000 Mbps BASE-T Ports, 2x 10 Gbps BASE-T Ports
<b>IPMI Port (rear panel)</b>	Included	Included
<b>Front LCD &amp; Keypad</b>	Not Available	Included
<b>VGA Ports</b>	Included	Included
<b>USB Ports (rear panel)</b>	4x Type A USB Ports	2x Type A USB Ports
<b>Serial Port (rear panel)</b>	115,200 bps, No Parity, 8 bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
<b>Drive Capacity</b>	2x 2TB 3.5 SAS HDD, RAID 1, hot-swappable, FRU	2x 2TB 3.5" SAS3 HDD, RAID 1, FRU
<b>Enclosure</b>	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
<b>Chassis Dimension WxDxH</b>	17. 2x25.6x1.7 Inches (437 x 650 x 43.2 mm)	17.2x33.5x3.5 Inches (437 x 851 x 89 mm)
<b>DC Power Supply</b>	Not Available	Not Available
<b>AC Power Supply</b>	Redundant (1+1) 750 watt, 100-240 VAC, 8 - 3.8 A, 50-60 Hz, IEC60320-C14, inlet, hot-swappable, FRU	Redundant (1+1) 800W: 100-127V, 9.8A-7A 1000W: 220-240V, 7-5A, 50-60Hz, FRU IEC60320-C14 inlet, FRU
<b>Power Consumption Maximum (watts)</b>	285 watts	760 watts
<b>Thermal Dissipation Maximum (BTU/h)</b>	972 BTU/h	2594 BTU/h
<b>MTBF (h)</b>	54,200 h	38,836 h
<b>Appliance Alone / As Shipped Weight lb. (kg)</b>	33 lb (15 kg) / 48 lb (21.8 kg)	46 lb (21 kg) / 90 lb (40.2 kg)
<b>Security Certification</b>	FIPS 140-2 Level 1, CC NDPP v1.1 (Pending)	FIPS 140-2 Level 1, CC NDPP v1.1 (Pending)
<b>Regulatory Compliance Safety</b>	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

**Table 7.** FireEye MVX smart grid specifications.

	VX 5500	VX 12500
<b>Regulatory Compliance EMC</b>	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 &V-3/2015
<b>Environmental Compliance</b>	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU
<b>Operating Temperature</b>	10 - 35°C (50 - 95°F)	0 - 40°C (32 - 104°F)
<b>Non-Operating Temperature</b>	-40 - 70°C (-40 - 158°F)	-30 - 70°C (-22 - 158°F)
<b>Operating Relative Humidity</b>	10% - 85% non-condensing	10% - 90% @ 40°C non-condensing
<b>Non-Operating Relative Humidity</b>	5% - 95% non-condensing	10% - 95% @ 55°C non-condensing
<b>Operating Altitude</b>	3000 m 9842 ft	3000 m 9842 ft

### Support Services

FireEye offers simple and flexible support programs to maximize the value of your FireEye products and services. Four different levels of support services are available: Platinum, Platinum Priority Plus, Government and Government Priority Plus. For more information about FireEye support, refer to FireEye Support services.

To learn more about FireEye, visit: [www.FireEye.com](http://www.FireEye.com)

#### FireEye, Inc.

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

© 2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners.  
NS-EXT-DS-US-EN-000048-07

#### 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.

