FIREEYE NETWORK SECURITY ESSENTIALS

COST-EFFECTIVE SOLUTION TO DEFEND AGAINST ADVANCED CYBER THREATS

NX 4400 (not pictured: NX 900, NX 1400, NX 2400, NX 4420)

OVERVIEW

FireEye Network Security Essentials is a cost-effective solution that minimizes the risk of costly breaches by accurately detecting and stopping advanced cyber attacks. At the core of Network Security Essentials is the FireEye Multi-Vector Virtual Execution™ (MVX) engine that analyzes web traffic in an isolated, virtual environment to detect known and zero-day exploits, malware executables and multi-protocol callbacks. It also includes FireEye Intrusion Prevention System (IPS) technology to detect common attacks with conventional signature matching.

Unlike firewall, IPS or AV solutions, Network Security Essentials detects both known and unknown attacks with high accuracy while generating low rates of false positives.

Network Security Essentials gives organizations of various sizes the ability to deploy advanced threat defenses and stop attacks with real-time protection. A high degree of automation enables organizations to simplify deployment and day-to-day management.

HIGHLIGHTS

- Detects advanced and zero-day attacks with the patented, signature-less MVX engine
- Prevents future attacks by applying machine learning, and retrospective and weak-signal analysis
- Identifies common and known attacks with traditional, signature-based IPS technology
- Improves operational effectiveness with a low, false-positive rate and alert categorization
- Disrupts attacks in real time with in-line blocking at up to 250 Mbps throughput for up to 2,500 users
- Simplifies management with low-touch deployment and a high degree of automation
- Reduces total cost of ownership (TCO) with affordable pricing and operational cost savings

FireEye
SECURITY REIMAGINED

Accurate Detection of Advanced Threats

Network Security Essentials uses the signature-less MVX engine to execute 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. The MVX engine automatically detects known and never-before-seen exploits and malware introduced into heterogeneous networks with many types of endpoints. As an attack plays out, the MVX engine captures callback channels, dynamically creates blocking rules and shares information about the attack with other Network Security sensors connected through the FireEye Dynamic Threat Intelligence (DTI) cloud. This shared information allows all FireEye Network Security sensors to immediately deploy blocking rules against unknown attacks. Furthermore, new threats are stopped when Network Security sensors automatically receive the latest front-line intelligence directly from Mandiant incident response teams. This occurs via the DTI cloud within minutes of the initial discovery.

Ease of Deployment and Management

Network Security Essentials is an easy-to-manage, clientless platform that deploys in under 60 minutes. It doesn't require rules, policies or tuning. Network Security Essentials offers affordable enterprise-grade advanced threat protection and a range of operational cost savings. Automated alert noise reduction, low false-positive rate and failover systems reduces staffing needs, downtime and overall cost of ownership.

Defense Against Known and Unknown Attacks

By consolidating advanced threat prevention for targeted, persistent and zero-day attacks with conventional IPS technology for known attacks, Network Security Essentials provides comprehensive protection against all types of attacks. The combination of signature-less protection provided by the MVX engine with the signature-based protection of traditional IPS technology simplifies management, improves operational efficency and enables regulatory or policy compliance for advanced threat defense.

Automated Alert Noise Reduction

Network Security Essentials automates validation of IPS alerts, eliminating the need to manually evaluate them. Indicators that trigger IPS alerts are automatically passed to the MVX engine for replay and analysis. Alerts that prove to be malicious are highlighted. This validation process reduces false alerts and drives down operating costs by prioritizing true alerts hidden among the high volume of false and duplicate IPS alerts.

Network Security Essentials also categorizes riskware, a family of undesirable objects such as adware and rasomware, that doesn't necessarily lead to a breach. Together, FireEye IPS alert validation and riskware categorization allow security teams to focus on genuine threats and remediation minimizing business risk and operational overhead.

Real-time Protection

Network Security Essentials offers flexible deployment modes including: out-of-band via a TAP/SPAN, in-line monitoring or in-line active blocking. It can be deployed in-line at Internet egress points to automatically block inbound exploits and malware, and outbound multi-protocol callbacks. In in-line monitoring mode, alerts are generated and organizations decide how to respond to them. In out-of-band prevention mode, Network Security Essentials issues TCP resets for out-of-band blocking of TCP, UDP or HTTP connections.

To maintain strong security, while keeping organizations running smoothly and without interruption or lag, Network Security Essentials supports integration with the FireEye Active Fail Open (AFO) switch to ensure no link downtime. It also drives continued availability for in-line hardware deployments in the face of power or link failures.

Awards and Certifications

The FireEye Network Security product portfolio has been awarded a number of industry and government awards and certifications including the US Department of Homeland Security Safety Act and is listed as a "must- have" in the Frost & Sullivan Network Security Sandbox Market Analysis.

TECHNICAL SPECIFICATIONS

	NX 900	NX 1400	NX 2400	NX 4400/4420
User Count	50	100	500	1,000 or 2,500
OS Support	Microsoft Windows	Microsoft Windows	Microsoft Windows	Microsoft Windows
Performance *	Up to 10 Mbps	Up to 20 Mbps	Up to 50 Mbps	Up to 100 Mbps or 250 Mbps
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 4420: 4x 1000 BASE-SX Fiber Optic Ports (LC Multimode)
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
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
IPMI Port (rear panel)	Included	Included	Included	Included
Front LCD & Keypad	Not Available	Included	Included	Included
PS/2 Keyboard and Mouse, DB15 VGA Ports (rear panel)	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
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
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
Enclosure	1RU, Fits 19 inch Rack	1RU, Fits 19 inch Rack	1RU, Fits 19 inch Rack	1RU, 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)
DC Power Supply	Not Available	Not Available	Not Available	Not Available
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
Power Consumption Maximum (watts)	136 watts	208 watts	210 watts	305 watts
Thermal Dissipation Maximum (BTU/h)	464 BTU/h	710 BTU/h	717 BTU/h	1041 BTU/h
MTBF (h)	94,700 h	67,500 h	55,200 h	37,000 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)
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
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)
Regulatory Compliance	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
Non-Operating Temperature	-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)
Non-Operating Relative Humidity	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

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
IPS Performance	10 Mbps	20 Mbps	50 Mbps	100 Mbps or 250 Mbps
Concurrent Connections	4K	7.5K	15K	80K
New Connections Per Second	200/Sec	375/Sec	750/Sec	4K/Sec
Packets Per Second	600/Sec	1200/Sec	4K/Sec	20K/Sec

ACTIVE FAIL OPEN SWITCH TECHNICAL SPECIFICATIONS	
	AFO 1G SWITCH
Dimensions (WxDxH)	8.75" x 11.0" x 1.35" (22.2 x 27.9 x 3.4 cm)
Management Ports	(1) DB9 Serial Console, (1) RJ45 Cat5e Port (10/100)
Network Ports	(2) RJ45 Cat5e Ports (10/100/1000)
Monitoring Ports	(2) RJ45 Cat5e Ports (10/100/1000)
AC Power Input	100 - 240 VAC, 0.5 A, 47-63 Hz
Operating Temp	0° C to 40° C

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

For more information on FireEye, visit:
www.FireEye.com

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

www.FireEye.com

FireEye