DATA SHEET

FireEye SmartVision Edition

Detect suspicious lateral movements within an enterprise network

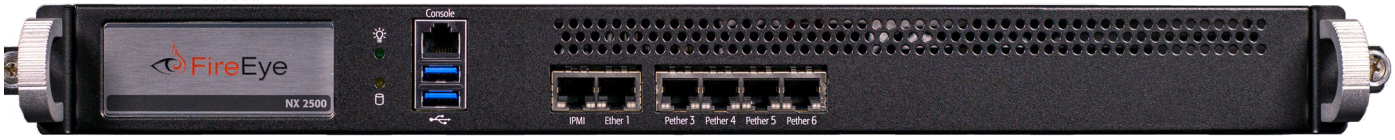

Figure 1. NX 2500 SmartVision hardware.

BENEFITS

- Detects formerly undetectable suspicious lateral traffic
- Decreases time to detect post-breach activities
- Provides flexibility to scale throughout the entire network
- Enables visibility into network segmentation initiatives
- Improves network forensics and incident response
- Reduces attacker dwell time

FireEye SmartVision Edition is a network traffic analysis (NTA) solution that detects suspicious lateral traffic within an enterprise network. Unlike other network security solutions that sit at the perimeter to thwart malicious incoming attacks, FireEye SmartVision Edition can be deployed throughout the network — at the core, across network segments and in front of key server assets — to detect malicious internal traffic.

With FireEye SmartVision Edition, security analysts and administrators gain new insight and visibility of suspicious lateral traffic that firewalls and other security gateways miss. By using easy to deploy, lightweight sensors working in conjunction with FireEye's industry - leading Cloud MVX™ technology, customers can scale SmartVision Edition visibility across the entire network – from the data center to remote branch office locations.

At the heart of SmartVision Edition is advanced threat detection software, which includes an advanced correlation and analytics engine and a machine learning module to detect attempted data exfiltration, bolstered by 120+ intrusion detection rules that identify weak indicators of compromise.

COMPONENTS OF SMARTVISION EDITION

Three components are required to enable SmartVision Edition:

- A minimum of one or more SmartVision Sensors (hardware or virtual)
- Connection to a FireEye MVX engine (either on-premise, Smart Grid or via Cloud MVX*)
- FireEye OS release 8.1.2 or greater with SmartVision activated

Table 1. SmartVision Edition features.

Features	Description
Detects suspicious lateral network traffic	Combines advanced correlation and analytics engine with a machine learning module and 120+ unique rules to detect stealthy lateral (east-west) traffic
Detonates objects over SMB/SMB2 protocols	Uses FireEye MVX technology to detonate malware and ransomware such as WannaCry, as well as other suspicious files and objects moving internally via the SMB protocol
Visualizes alerts to quickly triage events	Provides 10 minutes (+/- 5 minutes) of L4 and L7 alert context to quickly investigate attacker activity and conduct forensics analysis
Supports extensive metadata protocols	Generates metadata for comprehensive analysis, including the following protocols: FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS
Complements existing FireEye Network Security deployments	FireEye customers with 4th and 5th generation Network Security appliances can easily integrate SmartVision Edition into their existing infrastructure, further increasing their return on investment
Integrates with FireEye Helix	Provides additional threat intelligence context and integrated alert triage for collaboration across teams

FireEye SmartVision Edition identifies unique threat actions across the lateral attack cycle, further reducing post-breach dwell time and risk of loss.

The Eight Phases of the Lateral Attack Life Cycle

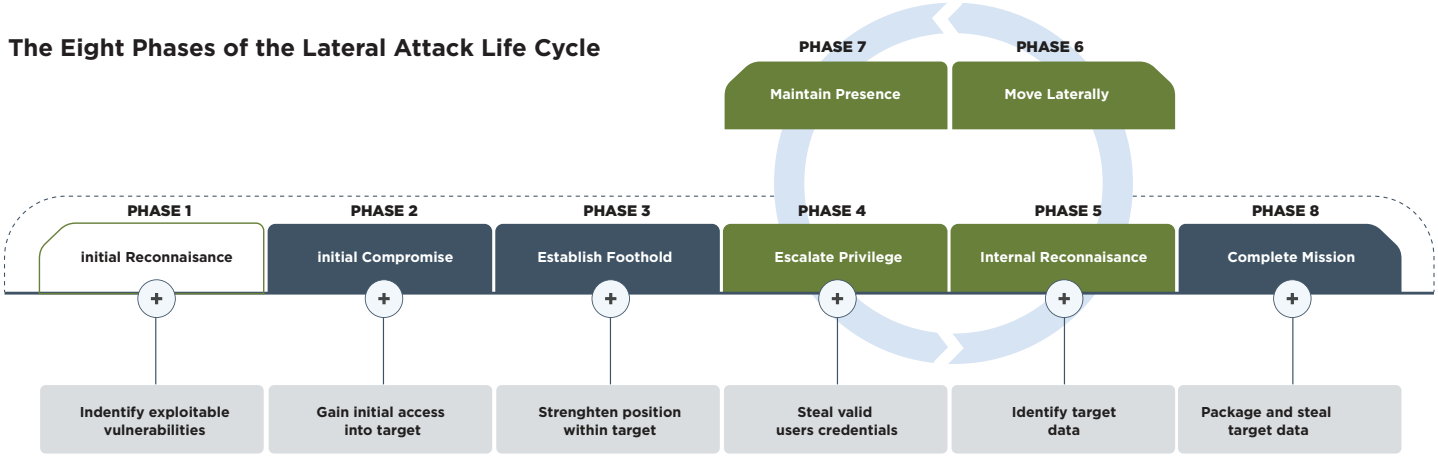

Table 2. SmartVision Edition specifications, by hardware model.		
Model	SV-2500-HW	SV-5500-HW
Sensor Mode Performance**	Up to 250 Mbps	Up to 5 Gbps
Integrated or Hybrid Mode Performance**	Up to 100 Mbps	Up to 2.5 Gbps
Network monitoring ports	4x 10/100/1000 BASE-T Ports	8x 10GigE SFP+ 4x 1Gig E Bypass
Management ports	2x 10/100/1000 Base-T Ports (in front panel)	2x 10/100/1000 Base-T Ports
Storage capacity	Single 1TB 3.5 inch, SATA HDD, internal, fixed	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU, RAID1
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis dimension (WxDxH)	17.2in(437mm) x 19.7in(500mm) x 1.7in(43.2 mm)	17.24in (438mm) x 24.41in (620mm) x 3.48in (88.4mm)
AC power supply	Single 250 watt, 90-264 VAC, 3.5 - 1.5 A, 50-60 Hz, IEC60320-C14, inlet, Internal, Fixed	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 – 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU
Power consumption maximum	85 watts	658 watts
Weight of appliance alone/as shipped in lbs (kg)	16.2 lbs (7.3kg) 28.2 lbs (2.95kg)	42.7 lbs (19.2kg) 63.8 lbs (29.0kg)
Operating temperature	0°-40°C 32°-104°F	0-35°C 32-95°F
Non-operating temperature	-20-80°C -4-176°F	-40-70°C -40-158°F
Supported metadata protocols	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS

Table 3. SmartVision Edition Sensor specifications, by virtual model.		
Model	2550v	6500v
Performance**	Up to 250 Mbps	Up to 1 Gbps
Network monitoring ports	1-8	1-8
Management ports	1 or 2	1 or 2
CPU cores	6	16
Memory	16 GB	64 GB
Drive capacity	384 GB	512 GB
Hypervisor support	VMWare ESXi 6.0 or later	VMWare ESXi 6.0 or later
Supported metadata protocols	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS

* Cloud MVX is designed to ensure simple, real-time detection and detonation of known and unknown threats. Unlike generic cloud-based sandboxes, Cloud MVX does not simply analyze file types and objects, but instead replays network traffic to identify attacks that span multiple network flows.

** Performance numbers will vary based on individual network conditions.

To learn more about FireEye, visit: **www.FireEye.com**

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

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. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

FireEye®