DATENBLATT

FireEye SmartVision Edition

Zur Erkennung verdächtiger lateraler Bewegungen in Unternehmensnetzwerken

Abbildung 1: NX 2500 SmartVision

FireEye SmartVision Edition ist eine Lösung für die Analyse des Netzwerkverkehrs, mit der verdächtiger lateraler Datenverkehr in einem Unternehmensnetzwerk erkannt werden kann. Im Gegensatz zu Netzwerksicherheitslösungen, die für die Bedrohungserkennung an der Netzwerkgrenze konzipiert wurden, kann FireEye SmartVision Edition überall im Netzwerk eingesetzt werden – zentral, in den Netzwerksegmenten oder vor wichtigen Servern und IT-Ressourcen –, um schädlichen Datenverkehr im Innern des Unternehmensnetzwerks zu erkennen.

Mit FireEye SmartVision Edition können Sicherheitsanalysten und Administratoren verdächtige laterale Datentransfers aufdecken und inspizieren, die weder Firewalls noch Sicherheitsgateways passieren müssen, da sie im Netzwerkinneren bleiben. Dank der Kombination aus der branchenführenden Technologie Cloud MVX™ von FireEye mit leicht zu implementierenden Sensoren mit geringem Ressourcenbedarf können Kunden die SmartVision Edition bis zur Gesamtgröße ihres Netzwerks skalieren, vom zentralen Rechenzentrum bis zur entlegendsten Zweigstelle.

Die SmartVision Edition enthält modernste Software für die Bedrohungserkennung, unter anderem eine Korrelations- und Analyse-Engine und ein Modul für maschinelles Lernen, mit dem versuchter Datendiebstahl erfasst werden kann. Diese werden durch über 120 Intrusion-Detection-Regeln zur Aufdeckung schwacher Gefahrenindikatoren ergänzt.

VORTEILE

- Identifizierung bislang nicht erkennbarer verdächtiger lateraler Datenübertragungen
- Schnellere Erkennung von Hackeraktivitäten in Ihrem Netzwerk
- Flexibilität für die Skalierung bis zur Gesamtgröße Ihres Netzwerks
- Besserer Überblick über Initiativen zur Netzwerksegmentierung
- Bessere Netzwerkforensik und Incident-Response-Maßnahmen
- Kürzere Verweildauer der Angreifer

KOMPONENTEN DER SMARTVISION EDITION

Die folgenden Komponenten sind erforderlich:

- Ein oder mehrere (virtuelle oder hardwarebasierte) SmartVision-Sensoren
- Verbindung zu einer FireEye MVX-Engine (On-Premises, via Smart Grid oder Cloud MVX*)
- Version 8.1.2 oder höher des FireEye OS mit aktivierter SmartVision

Tabelle 1: Merkmale der SmartVision Edition

Merkmal	Beschreibung
Erkennt verdächtigen lateralen Netzwerkverkehr	Kombiniert eine leistungsstarke Korrelations- und Analyse-Engine mit einem Modul für maschinelles Lernen und über 120 verschiedenen Regeln zur Erkennung versteckter lateraler Datenübertragungen.
Führt Objekte über SMB/SMB2-Protokolle aus	Nutzt FireEye MVX zum Entpacken verdächtiger Daten und Objekte, die über das SMB-Protokoll im Netzwerk übertragen werden. So können Ransomware wie WannaCry, andere Malware und sonstige Bedrohungen aufgedeckt werden.
Visualisiert Warnmeldungen für eine schnelle Ersteinschätzung der Ereignisse	Stellt L4-und L7-Daten für ein 10 Minuten langes Zeitfenster bereit (je fünf Minuten vor und nach der Warnmeldung), um die rasche Untersuchung von Angreiferaktivitäten und die forensische Analyse zu unterstützen.
Unterstützt umfassende Metadatenprotokoll-Analyse	Generiert Metadaten für eine umfassende Analyse, unter anderem für folgende Protokolle: FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS
Ergänzt vorhandene FireEye Network Security-Umgebungen	FireEye-Kunden mit Netzwerksicherheits-Appliances der 4. und 5. Generation können die SmartVision Edition problemlos in ihre vorhandenen Infrastrukturen integrieren und ihre Rendite damit steigern.
Mit FireEye Helix kompatibel	Stellt zusätzliche Bedrohungsdaten als Kontextinformationen bereit und unterstützt die teamübergreifende Zusammenarbeit bei der Bewertung von Warnmeldungen.

FireEye SmartVision erkennt neue Bedrohungen in allen Phasen des lateralen Angriffszyklus und reduziert dadurch sowohl die Verweildauer der Angreifer als auch das Risiko eines Datendiebstahls.

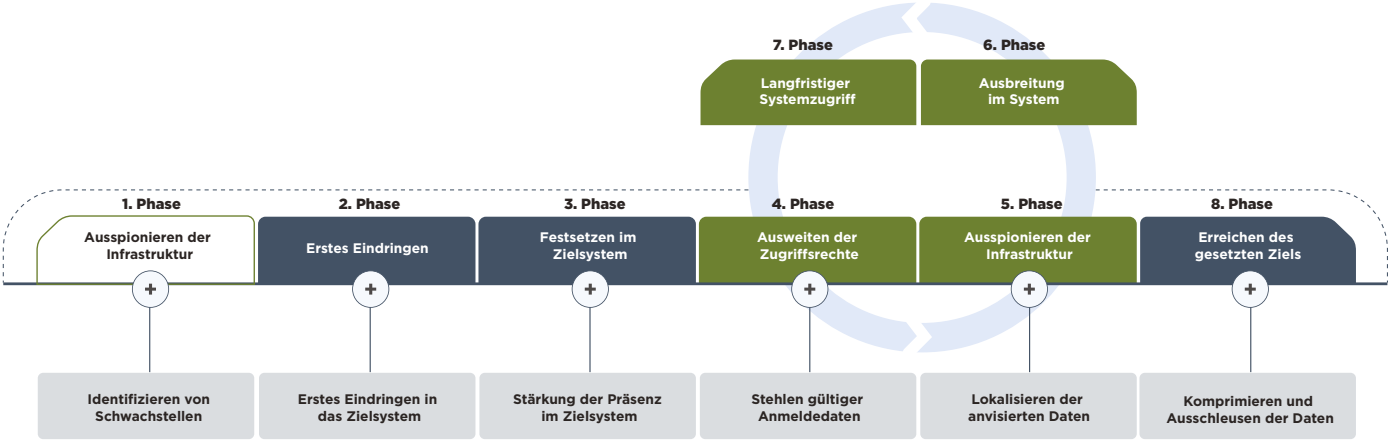

Tabelle 2: Technische Daten der SmartVision Edition, nach Hardwaremodell

Modell	SV-2500-HW	SV-5500-HW	SV-6500-HW
Leistung im Sensor-Modus**	Bis zu 250 Mbit/s	Bis zu 5 Gbit/s	Bis zu 15 Gbit/s
Leistung im integrierten oder Hybrid-Modus**	Bis zu 100 Mbit/s	Bis zu 2,5 Gbit/s	Bis zu 5 Gbit/s
Ports für Netzwerküberwachung	4 Ports für 10/100/1000-BASE-T	8 x 10 GigE SFP+ und 4 × 1 GigE Bypass	8 × 1 GigE/10 GigE SFP+ und 2 x 40 GigE QSFP+
Managementports	2 Ports für 10/100/1000-BASE-T (Vorderseite)	2 Ports für 10/100/1000-BASE-T	4 Ports für 1000-BASE-T
Speicherkapazität	1 interne 3,5-Zoll-SATA-Festplatte mit 1 TB Speicherplatz, nicht auswechselbar	2 3,5-Zoll-SAS3-Festplatten mit je 4 TB; 7.200 U/min; FRU RAID1	2 3,5-Zoll-SAS3-Festplatten mit je 10 TB; 7.200 U/min; FRU RAID1
Gehäuse	1 HE; passend für 19-Zoll-Rack	2 HE; passend für 19-Zoll-Rack	2 HE; passend für 19-Zoll-Rack
Abmessungen (B × T × H)	437 × 500 × 43,2 mm	438 × 620× 88,4 mm	438 × 620× 88,4 mm
Wechselstromanschluss	250 Watt; 90–264 V AC; 3,5–1,5 A; 50–60 Hz; Eingang nach IEC 60320-C14; intern; nicht auswechselbar	Redundant (1+1) 800 W; 100–240 V AC; 10,5–4,0 A; 50–60 Hz; Eingang nach IEC 60320-C14; FRU	Redundant (1+1) 800 W; 100–240 V AC; 10,5–4,0 A; 50–60 Hz; Eingang nach IEC 60320-C14; FRU
Maximaler Stromverbrauch	85 W	658 W	660 W
Nettogewicht der Appliance/ Versandgewicht	7,3 kg 12,8 kg	19,2 kg 29,0 kg	20,0 kg 32,2 kg
Betriebstemperatur	0–40 °C	0–35 °C	10–35 °C, getestet für erweiterten Bereich von 0 °C–40 °C
Lagertemperatur	-20–80 °C	-20–80 °C	-30–70 °C
Unterstützte Metadatenprotokolle	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	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS

Tabelle 3: Sensorspezifikationen der SmartVision Edition, nach virtuellem Modell

Modell	2550v	6500v
Leistung**	Bis zu 250 Mbit/s	Bis zu 1 Gbit/s
Ports für Netzwerküberwachung	1–8	1–8
Managementports	1 oder 2	1 oder 2
CPU-Kerne	6	16
Speicher	16 GB	64 GB
Laufwerkskapazität	384 GB	512 GB
Hypervisor-Unterstützung	VMWare ESXi 6.0 oder höher	VMWare ESXi 6.0 oder höher
Unterstützte Metadatenprotokolle	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 wurde für die einfache Erkennung und Entpackung bekannter und unbekannter Bedrohungen in Echtzeit entwickelt. Im Gegensatz zu generischen, cloudbasierten Sandboxes analysiert Cloud MVX nicht nur den Dateityp und die Objekte, sondern spielt auch Netzwerkverkehr ab. So lassen sich Angriffe erkennen, die über mehrere Netzwerkflüsse verteilt sind.

** Die tatsächliche Leistung schwankt, da sie von den spezifischen Netzwerkbedingungen abhängt.

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)
info-dach@FireEye.com

Über FireEye, Inc.
FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.

FIREEYE™