FireEye
SECURITY REIMAGINED

FireEye Network Threat Prevention Platform

Threat-Prevention-Plattform zur Bekämpfung von Cyberangriffen

DATENBLATT

HIGHLIGHTS

- Implementierung wahlweise im Inline- (Blockierung/Überwachung) oder im Out-of-Band-Modus (TCP-Reset/Überwachung) und Möglichkeit zur Analyse des IPv6-Datenverkehrs
- Analyse aller verdächtigen Webobjekte, darunter PDF-Dateien, Flash, Multimediaformate sowie ZIP-, RAR- und TNEF-Archive, und Blockierung ausgehender Malware-Verbindungen zur Verhinderung von Datendiebstahl
- Anbindung an die FireEye Threat-Prevention-Plattform zur Abwehr kombinierter Spear-Phishing-Angriffe
- Verteilung der Bedrohungsdaten lokal an die gesamte FireEye-Installation und global an andere FireEye-Kunden über die FireEye DTI-Cloud (Dynamic Threat Intelligence)
- Unterstützung lokaler Authentifizierung und des Fernzugriffs auf AAA-Netzwerkdienste anderer Anbieter
- rollenabhängige Zugriffsrechte (RBACs) und Audit-Protokollierung
- Support für Windows- und Mac-OS-X-Umgebungen
- Konsolidierung signaturabhängiger und -unabhängiger Technologien mit der IPS-Add-on-Lizenz für FireEye Network, um Fehlalarme automatisch zu reduzieren und die Betriebskosten zu senken
- Senkung der IPS-Betriebskosten durch automatisierte Rauschunterdrückung

NX 2400, NX 4420, NX 7420, NX 10000
(nicht abgebildet: NX 1400, NX 4400, NX 7400)

Überblick

Die FireEye® Network Threat Prevention Platform erkennt und blockiert Zero-Day-Exploits, Dropper-Malware (Binärdateien) und protokollübergreifende Callbacks. Auf diese Weise können Unternehmen mit ihren Abwehrmaßnahmen eine Vielzahl von Installationen unterschiedlicher Größe abdecken – von der Zentrale mit einem Datendurchsatz im Gigabitbereich bis hin zu kleinen Außenstellen, Zweigstellen und mobilen Büros. FireEye Network und die integrierte IPS-Technologie (Intrusion-Prevention-System) bieten erhöhten Schutz vor bekannten und unbekannten Bedrohungen und sorgen gleichzeitig für optimierte Betriebskosten, weniger falsch positive Ergebnisse und eine verbesserte Compliance.

Cyberkriminelle nutzen das Internet als primären Angriffsvektor, um Zero-Day-Exploits und schädliche Links per E-Mail zu versenden und so Daten zu entwenden. FireEye Network kann Drive-by-Downloads und kombinierte Web- und E-Mail-Angriffe stoppen. Außerdem wehrt es Infektionen ab, die außerhalb des Netzwerks stattfinden.

Threat Prevention in Echtzeit zum Schutz vor Webangriffen

FireEye Network kann im Inline-Modus an den Ausgangspunkten zum Internet platziert werden, um Web-Exploits abzuwehren und ausgehende Callbacks protokollübergreifend zu unterbinden. Mithilfe der MVX-Engine (Multi-Vector Virtual Execution™) kann FireEye Network Zero-Day-Angriffe zuverlässig erkennen und in Echtzeit Informationen über die Bedrohung und dynamische Callback-Ziele erfassen. Im Überwachungsmodus zeigt sie Incident-Response-Mechanismen an. Im Out-of-Band-Schutzmodus löst FireEye Network TCP-Resets aus, um TCP-, UDP- und HTTP-Verbindungen zu blockieren.

Abwehr kombinierter Angriffe über das Internet und per E-Mail

Die FireEye-Plattform bietet Schutz vor kombinierten, komplexen Angriffen, bei denen das Internet, Spear-Phishing-E-Mails und Zero-Day-Exploits eingesetzt werden. Mit FireEye Network, FireEye Email und FireEye Central Management erhalten Kunden Echtzeitschutz vor schädlichen Links und sind in der Lage, die einzelnen Puzzleteile eines kombinierten Angriffs zusammenzufügen.

Schutz vor neuen Zero-Day-Angriffen

FireEye Network führt verdächtige Binärdateien und Webobjekte mithilfe der signaturunabhängigen FireEye MVX-Engine aus, um ihre Wirkung auf verschiedene Browser, Plug-ins, Anwendungen und Betriebssysteme zu ermitteln. Auf diese Weise können Exploits von Schwachstellen und Speicherfehlern sowie andere schädliche Vorgänge verfolgt werden. Während des simulierten Angriffs erfasst die FireEye MVX-Engine die Callback-Kanäle, erstellt dynamisch Blockierregeln und übermittelt diese Informationen an das FireEye Network.

Konfigurationsmöglichkeiten durch YARA-Regeln

Die Plattform unterstützt benutzerdefinierte YARA-Regeln, mit deren Hilfe festgelegt werden kann, welche Webobjekte auf Bedrohungen untersucht werden sollten.

Einfachere Priorisierung von Sicherheitsvorfällen

Mit der AV-Suite von FireEye kann bei jedem schädlichen Objekt geprüft werden, ob Antiviruslösungen die von FireEye Network gestoppte Malware erkennen würden. Damit können Kunden bei der Reaktion auf Sicherheitsvorfälle effizienter Prioritäten setzen.

Austausch von Dynamic Threat Intelligence

Dank der von FireEye Network dynamisch in Echtzeit erzeugten Bedrohungsdaten können alle FireEye-Produkte das lokale Netzwerk besser schützen. Die Daten enthalten Callback-Koordinaten und Kommunikationsmerkmale, die weltweit über die FireEye DTI-Cloud (Dynamic Threat Intelligence™) verbreitet werden können, um alle Abonnenten über die neuen Bedrohungen in Kenntnis zu setzen.

Keine Konfiguration von Regeln und nahezu keine False Positives

Bei FireEye Network handelt es sich um eine verwaltungsfreundliche Plattform ohne Client, die in weniger als einer Stunde einsatzbereit ist und keine Anpassung benötigt. Sie bietet flexible Implementierungsmodi, unter anderem Out-of-Band über TAP/SPAN, Inline-Überwachung oder Inline mit aktiver Abwehr.

Unterstützung für Active Fail Open

FireEye Network kann mit dem Active Fail Open Switch verbunden werden, um einen Ausfall der Verbindung zu verhindern und für eine höhere Verfügbarkeit von Inline-Installationen bei Stromausfällen oder Verbindungsunterbrechungen zu sorgen. Der Active Fail Open Switch nutzt die sogenannte Heartbeat-Technologie, um die Verfügbarkeit von FireEye Network-Geräten zu überwachen, und wechselt im Störungsfall automatisch in den Bypass-Modus.

Unterstützung für IPS

FireEye Network mit IPS (Intrusion-Prevention-System) verbindet Advanced Threat Prevention mit herkömmlichen Sicherheitsmechanismen und ermöglicht so umfangreiche Kostenoptimierungen. Die Plattform automatisiert mithilfe der MVX-Engine die Bedrohungsvalidierung, um Fehlalarme zu vermeiden, und erkennt Angriffe im Hintergrundrauschen. Dadurch senkt sie die Betriebskosten und minimiert zugleich das Risiko nicht erkannter Vorfälle. FireEye Network ergänzt die signaturunabhängigen Sicherheitsverfahren der MVX-Engine um die signaturabhängigen Abwehrmaßnahmen der herkömmlichen IPS-Technologie. Das Ergebnis: größere Sicherheit und verbesserte Compliance.

Technische Daten

	NX 900	NX 1400	NX 2400	NX 4400/4420	NX 7400/7420	NX 7500	NX 9450	NX 10000	NX 10450
Anzahl der Benutzer	50	100	500	2.500	10.000	10.000	20.000	40.000	40.000
Unterstützte Betriebssysteme	Microsoft Windows	Microsoft Windows	Microsoft Windows	Microsoft Windows	Microsoft Windows	Microsoft Windows Mac OS X	Microsoft Windows	Microsoft Windows	Microsoft Windows
Leistung*	Bis zu 10 Mbit/s	Bis zu 20 Mbit/s	Bis zu 50 Mbit/s	Bis zu 250 Mbit/s	Bis zu 1 Gbit/s	Bis zu 1 Gbit/s	Bis zu 2 Gbit/s	Bis zu 4 Gbit/s	Bis zu 4 Gbit/s
Überwachungs-ports	2 10/100/1000-BASE-T-Ports	2 10/100/1000-BASE-T-Ports	4 10/100/1000-BASE-T-Ports	4400: 4 10/100/1000-BASE-T-Ports 4420: 4 1000-BASE-SX-Glasfaser-Ports (LC-Multimode)	7400: 4 10/100/1000-BASE-T-Ports 7420: 4 1000-BASE-SX-Glasfaser-Ports (LC-Multimode)	4 10/100/1000-BASE-T-Ports	4 SFP+-Ports, 4 SFP-Ports, 1000 BASE-SX (LC-MMF), 1000 BASE-LX (LC-SMF), 1000 BASE-T (RJ45, UTP5)	2 feste Schnittstellen für 10GBASE-SR/SW 850 nm: 10GBASE-SX (LC-MMF)	8 SFP+ (4 1000 BASE und 4 10GBASE), 1000 BASE-SX/10GBASE-SR (LC-MMF), 1000BASE-LX/10GBASE-LR (LC SMF), 1000 BASE-T (RJ45, UTP5), 10GBASE-Cu (5-m-Direkt-anschlusskabel)
Betriebsmodi Netzwerkports	Inline-Monitor, Fail-Open, Fail-Close oder TAP/SPAN, HW-Bypass	Inline-Monitor, Fail-Open, Fail-Close oder TAP/SPAN, HW-Bypass	Inline-Monitor, Fail-Open, Fail-Close oder TAP/SPAN, HW-Bypass	Inline-Monitor, Fail-Open, Fail-Close oder TAP/SPAN, HW-Bypass	Inline-Monitor, Fail-Open, Fail-Close oder TAP/SPAN, HW-Bypass	Inline-Monitor, Fail-Open, Fail-Close oder TAP/SPAN, HW-Bypass	Inline-Monitor oder TAP/SPAN	Inline-Monitor, Fail-Open, Fail-Close oder TAP/SPAN, HW-Bypass	Inline-Monitor oder TAP/SPAN
Management-ports (Rückseite)	2 10/100/1000-BASE-T-Ports	2 10/100/1000-BASE-T-Ports	2 10/100/1000-BASE-T-Ports	2 10/100/1000-BASE-T-Ports	2 10/100/1000-BASE-T-Ports	2 10/100/1000-BASE-T-Ports	2 10/100/1000-BASE-T-Ports	2 10/100/1000-BASE-T-Ports	2 10/100/1000-BASE-T-Ports
IPMI-Port (Rückseite)	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden
LCD-Anzeige und Tastenfeld auf Vorderseite	Nicht verfügbar	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden
PS/2-Tastatur und -Maus, DB15-VGA-Ports (Rückseite)	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden
USB-Ports (Rückseite)	2 USB-Ports Typ A	2 USB-Ports Typ A	2 USB-Ports Typ A	2 USB-Ports Typ A	2 USB-Ports Typ A	4 USB-Ports Typ A	2 USB-Ports Typ A	2 USB-Ports Typ A	2 USB-Ports Typ A
Serieller Port (Rückseite)	115.200 bit/s, keine Parität, 8 Bit, 1 Stoppbit	115.200 bit/s, keine Parität, 8 Bit, 1 Stoppbit	115.200 bit/s, keine Parität, 8 Bit, 1 Stoppbit	115.200 bit/s, keine Parität, 8 Bit, 1 Stoppbit	115.200 bit/s, keine Parität, 8 Bit, 1 Stoppbit	115.200 bit/s, keine Parität, 8 Bit, 1 Stoppbit	115.200 bit/s, keine Parität, 8 Bit, 1 Stoppbit	115.200 bit/s, keine Parität, 8 Bit, 1 Stoppbit	115.200 bit/s, keine Parität, 8 Bit, 1 Stoppbit
Laufwerks-kapazität	Interne Festplatte mit 500 GB Speicherplatz	Interne Festplatte mit 500 GB Speicherplatz	Interne Festplatte mit 500 GB Speicherplatz	2 Festplatten mit 600 GB Speicherplatz, RAID 1, 2,5 Zoll, FRU	2 Festplatten mit 600 GB Speicherplatz, RAID 1, 2,5 Zoll, FRU	4 Festplatten mit 900 GB Speicherplatz, RAID 10, 2,5 Zoll, FRU	4 Festplatten mit 900 GB Speicherplatz, RAID 10, 2,5 Zoll, FRU	2 SSDs mit 800 GB Speicherplatz, RAID 1, 2,5 Zoll, FRU	4 SSDs mit 800 GB Speicherplatz, RAID 10, 2,5 Zoll, FRU
Gehäuse	1 HE, passend für 19-Zoll-Rack	1 HE, passend für 19-Zoll-Rack	1 HE, passend für 19-Zoll-Rack	1 HE, passend für 19-Zoll-Rack	2 HE, passend für 19-Zoll-Rack	2 HE, passend für 19-Zoll-Rack	2 HE, passend für 19-Zoll-Rack	2 HE, passend für 19-Zoll-Rack	2 HE, passend für 19-Zoll-Rack
Abmessungen (B × T × H)	427 × 356 × 43 mm	437 × 612 × 43,2 mm	437 × 612 × 43,2 mm	437 × 706 × 43,2 mm	437 × 711 × 86,5 mm	437 × 711 × 86,6 mm	437 × 709 × 89 mm	437 × 709 × 89 mm	437 × 709 × 89 mm
Gleichstrom-anschluss	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar

Technische Daten

	NX 900	NX 1400	NX 2400	NX 4400/4420	NX 7400/7420	NX 7500	NX 9450	NX 10000	NX 10450
Wechselstromanschluss	Nicht redundant, keine FRU-Einheit, intern 200 W bei 100–240 V AC, 3–1,5 A, 50–60 Hz, Eingang nach IEC 60320-C14	Nicht redundant, keine FRU-Einheit, intern 500 W bei 100~240 V AC, 5–2,5 A, 50–60 Hz, Eingang nach IEC 60320-C14	Nicht redundant, keine FRU-Einheit, intern 500 W bei 100~240 V AC, 5–2,5 A, 50–60 Hz, Eingang nach IEC 60320-C14	Redundant (1+1), 750 W bei 100–240 V AC, 9–4,5 A, 50–60 Hz, Eingang nach IEC 60320-C14, FRU	Redundant (1+1), 750 W bei 100–240 V AC, 9–4,5 A, 50–60 Hz, Eingang nach IEC 60320-C14, FRU	Redundant (1+1), 750 W bei 100–240 V AC, 9–4,5 A, 50–60 Hz, Eingang nach IEC 60320-C14, FRU	Redundant (1+1) 1200 W bei 100–140 V AC, 14,7–10,5 A 1400 W bei 180–240 V AC, 9,5–7,2 A, 50–60 Hz, FRU-Eingang nach ICE 60320-C14, FRU	Redundant (1+1) 1200 W bei 100–140 V AC, 14,7–10,5 A 1400 W bei 180–240 V AC, 9,5–7,2 A, 50–60 Hz, FRU-Eingang nach ICE 60320-C14, FRU	Redundant (1+1) 1200 W bei 100–140 V AC, 14,7–10,5 A 1400 W bei 180–240 V AC, 9,5–7,2 A, 50–60 Hz, FRU-Eingang nach ICE 60320-C14, FRU
Maximaler Stromverbrauch	136 W	208 W	210 W	305 W	501 W	479 W	550 W	962 W	850 W
Maximale thermische Verlustleistung	464 BTU/h (~136 W)	710 BTU/h (~208 W)	717 BTU/h (~210 W)	1041 BTU/h (~305 W)	1709 BTU/h (~501 W)	1634 BTU/h (~479 W)	1881 BTU/h (~551 W)	3282 BTU/h (~962 W)	2908 BTU/h (~852 W)
Mittlere Betriebsdauer zwischen Ausfällen (MTBF)	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
Nettogewicht Appliance/ Versandgewicht	5 kg 9 kg	11 kg 18 kg	11 kg 18 kg	14 kg 21 kg	19 kg 26 kg	19,5 kg 27 kg	23 kg 30 kg	23 kg 30 kg	23 kg 30 kg
Sicherheitszertifizierungen	IEC 60950 EN 60950 CSA 60950-00 CE-Kennzeichnung	IEC 60950 EN 60950 CSA 60950-00 CE-Kennzeichnung	IEC 60950 EN 60950 CSA 60950-00 CE-Kennzeichnung	IEC 60950 EN 60950 CSA 60950-00 CE-Kennzeichnung	IEC 60950 EN 60950 CSA 60950-00 CE-Kennzeichnung	IEC 60950 EN 60950 CSA 60950-00 CE-Kennzeichnung	IEC 60950-1 EN 60950-1 CSA 60950-1 CE-Kennzeichnung	IEC 60950-1 EN 60950-1 CSA 60950-1 CE-Kennzeichnung	IEC 60950-1 EN 60950-1 CSA 60950-1 CE-Kennzeichnung
EMC-/ EMI-Zertifizierungen	FCC (Teil 15 Klasse A), CE (Klasse A), CNS, AS/NZS, VCCI (Klasse A)	FCC (Teil 15 Klasse A), CE (Klasse A), CNS, AS/NZS, VCCI (Klasse A)	FCC (Teil 15 Klasse A), CE (Klasse A), CNS, AS/NZS, VCCI (Klasse A)	FCC (Teil 15 Klasse A), CE (Klasse A), CNS, AS/NZS, VCCI (Klasse A)	FCC (Teil 15 Klasse A), CE (Klasse A), CNS, AS/NZS, VCCI (Klasse A)	FCC (Teil 15 Klasse A), CE (Klasse A), CNS, AS/NZS, VCCI (Klasse A)	FCC (Teil 15 Klasse A), CE (Klasse A), CNS, AS/NZS, VCCI (Klasse A)	FCC (Teil 15 Klasse A), CE (Klasse A), CNS, AS/NZS, VCCI (Klasse A)	FCC (Teil 15 Klasse A), CE (Klasse A), CNS, AS/NZS, VCCI (Klasse A)
Richtlinien und Normen	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
Betriebstemperatur	10 °C bis 35 °C Getestet für erweiterten Bereich von 0 °C bis 40 °C	10 °C bis 35 °C Getestet für erweiterten Bereich von 0 °C bis 40 °C	10 °C bis 35 °C Getestet für erweiterten Bereich von 0 °C bis 40 °C	10 °C bis 35 °C Getestet für erweiterten Bereich von 0 °C bis 40 °C	10 °C bis 35 °C Getestet für erweiterten Bereich von 0 °C bis 40 °C	10 °C bis 35 °C Getestet für erweiterten Bereich von 0 °C bis 40 °C	10 °C bis 35 °C	10 °C bis 35 °C	10 °C bis 35 °C
Lagertemperatur	-40 °C bis 70 °C	-40 °C bis 70 °C	-40 °C bis 70 °C	-40 °C bis 70 °C	-40 °C bis 70 °C	-40 °C bis 70 °C	-40 °C bis 70 °C	-40 °C bis 70 °C	-40 °C bis 70 °C
Relative Luftfeuchtigkeit bei Betrieb	8–90 % (nicht kondensierend)	8–90 % (nicht kondensierend)	8–90 % (nicht kondensierend)	8–90 % (nicht kondensierend)	8–90 % (nicht kondensierend)	8–90 % (nicht kondensierend)	10–85 % (nicht kondensierend)	10–85 % (nicht kondensierend)	10–85 % (nicht kondensierend)
Relative Luftfeuchtigkeit bei Lagerung	5–95 % (nicht kondensierend)	5–95 % (nicht kondensierend)	5–95 % (nicht kondensierend)	5–95 % (nicht kondensierend)	5–95 % (nicht kondensierend)	5–95 % (nicht kondensierend)	5–95 % (nicht kondensierend)	5–95 % (nicht kondensierend)	5–95 % (nicht kondensierend)
Betriebshöhe	0–3.000 m, Temperaturabnahme von 1 °C pro 1000 m	0–3.000 m, Temperaturabnahme von 1 °C pro 1000 m	0–3.000 m, Temperaturabnahme von 1 °C pro 1000 m	0–3.000 m, Temperaturabnahme von 1 °C pro 1000 m	0–3.000 m, Temperaturabnahme von 1 °C pro 1000 m	0–3.000 m, Temperaturabnahme von 1 °C pro 1000 m	1.500 m	1.500 m	1.500 m

Hinweis: Die tatsächlichen Leistungswerte sind abhängig von der Systemkonfiguration und dem verarbeiteten Datenverkehr.

Technische Daten der Intrusion-Prevention-Systeme

	NX 900	NX 1400	NX 2400	NX 4400/4420	NX 7400/7420	NX 7500	NX 9450	NX 10000	NX 10450
IPS-Leistung	10 Mbit/s	20 Mbit/s	50 Mbit/s	250 Mbit/s	1 Gbit/s	1 Gbit/s	2 Gbit/s	4 Gbit/s	4 Gbit/s
Gleichzeitige Verbindungen	4.000	7.500	15.000	80.000	500.000	500.000	1.000.000	2.000.000	2.000.000
Neue Verbindungen pro Sekunde	200	375	750	4.000	10.000	10.000	20.000	40.000	40.000
Pakete pro Sekunde	600	1.200	4.000	20.000	90.000	90.000	105.000	120.000	120.000

Technische Daten des Active Fail Open Switch

	1G Active Fail Open Switch	10G Active Fail Open Switch
Abmessungen (B × T × H)	22,2 × 27,9 × 3,4 cm	16,5 × 35,6 × 2,8 cm
Managementports	1 serieller DB9-Konsolenanschluss, 1 Port für 10/100 Cat5e-RJ45	1 serieller DB9-Konsolenanschluss, 1 Port für 10/100 Cat5e-RJ45
Netzwerkports	2 Ports für 10/100/1000 Cat5e-RJ45	1 LC-Quad-Steckverbinder
Überwachungsports	2 Ports für 10/100/1000 Cat5e-RJ45	2 XFP-Ports
Wechselstromanschluss	100–240 V AC, 0,5 A, 47–63 Hz	100–240 V AC, 1,0 A, 47–63 Hz
Betriebstemperatur	0 °C bis 40 °C	0 °C bis 40 °C

Hinweis: Die tatsächlichen Leistungswerte sind abhängig von der Systemkonfiguration und dem verarbeiteten Datenverkehr.

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