DATENBLATT

FireEye

FireEye Network Security

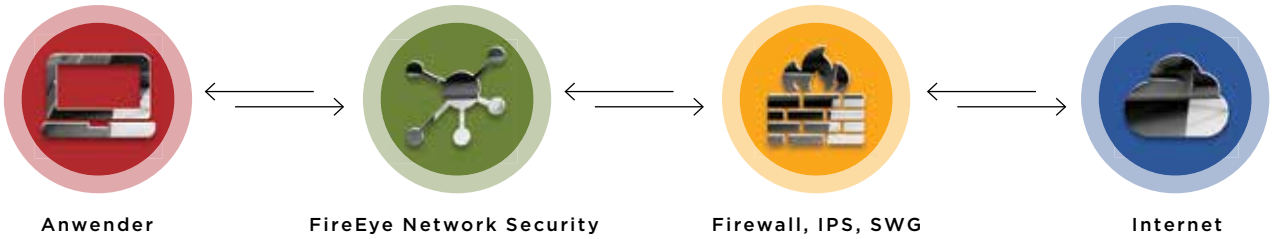
Wirksamer Schutz vor Cyberangriffen für mittelgroße und große Unternehmen

Überblick
FireEye Network Security ist eine effektive Cybersicherheitslösung, die komplexe, gezielte und im Internetverkehr versteckte Angriffe in Echtzeit aufdeckt und abwehrt und damit das Risiko kostspieliger Sicherheitsverletzungen senkt. Zudem liefert FireEye Network Security binnen weniger Minuten konkrete Beweise, verwertbare Daten und Handlungsempfehlungen für die effektive Behebung der aufgedeckten Sicherheitsvorfälle. Mit FireEye Network Security können sich Unternehmen effektiv vor Bedrohungen schützen – unabhängig davon, ob diese eine Schwachstelle in Windows, Apple OS X oder einer bestimmten Anwendung ausnutzen, ob der Hauptsitz oder eine Niederlassung angegriffen wird und wie gut die Bedrohung in dem umfangreichen eingehenden Internetdatenverkehr versteckt ist, der in Echtzeit überwacht werden muss.

Die beiden Kernkomponenten der Lösung sind die MVX-Engine (Multi-Vector Virtual Execution™) und IDA-Technologien (Intelligence-Driven Analysis). Bei MVX handelt es sich um eine signaturunabhängige, dynamische Analyse-Engine, die das Netzwerk auf verdächtigen Verkehr prüft und so Angriffe erkennt, die konventionelle signatur- und regelbasierte Sicherheitssysteme umgehen. IDA umfasst mehrere kontextbezogene, auf dynamischen Regeln basierende Engines, die mithilfe von Informationen zu Technologien, Angreifern und Opfern Angriffe sowohl in Echtzeit als auch rückwirkend erkennen und abwehren. Gleichzeitig greift FireEye Network Security auf ein herkömmliches IPS (Intrusion Prevention System) zurück, das bereits bekannte Angriffsmuster mithilfe eines konventionellen Signaturabgleichs erkennt.

FireEye Network Security ist in verschiedenen Formfaktoren bzw. als Service mit unterschiedlichen Bereitstellungs- und Leistungsoptionen erhältlich. Die Lösung wird normalerweise an der Schnittstelle zum Internet hinter den gängigen Netzwerksicherheitslösungen wie Firewalls der nächsten Generation, IPS und Secure Web Gateways (SWG) installiert. FireEye Network Security ergänzt diese Lösungen durch die rasche und zuverlässige Erkennung bekannter und unbekannter Bedrohungen. Es zeichnet sich insbesondere durch einen niedrigen Anteil an Fehlalarmen aus und versetzt Sicherheitsteams so in die Lage, effizient und effektiv auf jede Warnung zu reagieren.

Abbildung 1: Typische Konfiguration – Netzwerksicherheitslösungen



Leistungsmerkmale	Vorteile
Aufdeckung	
Zuverlässige Erkennung komplexer, gezielter und gut getarnter Cyberangriffe	Minimierung des Risikos kostspieliger Sicherheitsverletzungen
Erweiterbare, modulare Sicherheitsarchitektur	Investitionsschutz
Konsistenter Schutz für alle Internet-Zugangspunkte, auch in Umgebungen mit verschiedenen Betriebssystemen	Zuverlässiger Schutz für alle Gerätetypen im gesamten Unternehmen
Optionen für die integrierte oder verteilte, physische oder virtuelle sowie die unternehmensinterne oder cloudbasierte Bereitstellung	Flexibilität zur Anpassung an die individuellen Anforderungen und Ressourcen verschiedenster Unternehmen
Abgleich mehrerer Angriffsvektoren mit Daten aus E-Mail- und Content-Sicherheitslösungen	Überwachung großer Angriffsflächen
Abwehr	
Unmittelbare Blockierung von Angriffen für Netzwerkverbindungen mit Bandbreiten von 10 Mbit/s bis 8 Gbit/s	Echtzeit-Schutz gegen gut getarnte Angriffe
Reaktion	
Niedriger Anteil von Fehlalarmen, Riskware-Kategorisierung und automatisierte Prüfung von IPS-Warnmeldungen	Geringere Kosten für das Herausfiltern von unzuverlässigen Warnmeldungen
Unmittelbarer Übergang zur Untersuchung und Validierung von Warnmeldungen, ihrer Isolation auf dem betroffenen Endpunkt und der Einleitung geeigneter Gegenmaßnahmen	**Automatisierung und Vereinfachung von Sicherheitsworkflows**
Ausführungsnachweise und verwertbare Bedrohungsdaten mit kontextbezogenen Informationen	**Schnellere Priorisierung und Behebung der aufgedeckten Sicherheitsvorfälle**
Skalierbarkeit von einem Standort auf Tausende von Standorten	**Unterstützung von Wachstumsphasen**

Technische Vorteile

Präzise Bedrohungserkennung

FireEye Network Security nutzt verschiedene Analysemethoden, um Angriffe zuverlässig zu erkennen und den Anteil der Fehlalarme gering zu halten:

- Die **MVX-Engine (Multi-Vector Virtual Execution™)** erfasst Zero-Day-Exploits, Multi-Flow-Angriffe und andere gut getarnte Angriffe mithilfe einer dynamischen, signaturunabhängigen Analyse in einer sicheren, virtuellen Umgebung. Durch die Identifizierung bisher vollkommen unbekannter Exploits und Malware können Angriffe bereits in den ersten Phasen des Angriffszyklus gestoppt werden.
- **IDA-Engines (Intelligence-Driven Analysis)** erkennen gut getarnte, gezielte und andere speziell auf das jeweilige Opfer zugeschnittene Angriffe und wehren diese erfolgreich ab. Dabei stützen sie sich auf die kontextbezogene, regelbasierte Analyse von Echtzeitinformationen, die aus Millionen von MVX-Berichten, den zahlreichen Incident-Response-Einsätzen von Mandiant (einem FireEye-Unternehmen) und den Erkenntnissen Hunderter von iSight-Analysten stammen. Durch die Identifizierung schädlicher Exploits, Malware und CnC-Callbacks (Command and Control) können Bedrohungen bereits in den frühen Phasen des Angriffszyklus abgewehrt werden, wenn einzelne Systeme infiziert und infiltriert werden. Verdächtiger Netzwerkverkehr wird extrahiert und an die MVX-Engine zur Analyse weitergeleitet.
- **STIX (Structured Threat Intelligence eXpression)** ermöglicht das Einlesen der Bedrohungsdaten anderer Anbieter in einem branchenüblichen Format. So können die IDA-Engines durch spezifische Bedrohungsindikatoren aktualisiert werden.

Unmittelbarer, zuverlässiger Schutz

FireEye Network Security bietet unter anderem folgende flexible Konfigurationsmodi:

- Out-of-Band-Überwachung über TAP/SPAN, Inline-Überwachung sowie Inline mit aktiver Abwehr: Bei der Bereitstellung im Inline-Abwehrmodus werden eingehende Exploits und Malware automatisch abgewehrt sowie ausgehende Verbindungen über verschiedene Protokolle unterbunden. Dagegen werden im Inline-Überwachungsmodus lediglich Warnmeldungen generiert, wenn eine Bedrohung erkannt wird. Die Verantwortlichen des Unternehmens entscheiden dann, welche Gegenmaßnahmen angemessen sind. Im Out-of-Band-Schutzmodus löst FireEye Network Security TCP-Resets aus, um TCP-, UDP- und HTTP-Verbindungen zu blockieren.
- Durch die Anbindung an den FireEye AFO-Switch (Active Fail Open) kann eine potenzielle Unterbrechung der Netzwerkverbindung verhindert werden.
- Ausgewählte Modelle bieten aktive Hochverfügbarkeit, damit auch bei Netzwerk- oder Geräteausfällen ein zuverlässiger Schutz gegeben ist.

Vielseitiger und umfassender Schutz

FireEye Network Security bietet zuverlässigen Schutz für moderne heterogene Netzwerkumgebungen:

- Unterstützung der gängigsten Versionen von Microsoft Windows und Apple Mac OS X
- Analyse von mehr als 140 verschiedenen Dateitypen, darunter PEs (Portable Executables), Webinhalte, Archive, Bilddateien sowie Java-, Microsoft- und Adobe-Anwendungen und Multimedia-Dateien
- Ausführung verdächtiger Netzwerkpakete in Testumgebungen, die auf unterschiedlichsten Kombinationen von Betriebssystem, Service Pack, Anwendungstyp und Anwendungsversion basieren.

Überprüfte und priorisierte Warnmeldungen

Zusätzlich zur Erkennung von Angriffen wird die FireEye MVX-Technologie auch zur Überprüfung der Warnmeldungen konventioneller signaturabhängiger Sicherheitssysteme und zur Identifizierung und Priorisierung kritischer Bedrohungen eingesetzt:

- Wenn die von einem IPS (Intrusion Prevention System) generierten Warnmeldungen von der MVX-Engine überprüft werden, lässt sich die üblicherweise recht hohe Zahl der IPS-Fehlalarme reduzieren, sodass der Arbeitsaufwand für die Einstufung der verbleibenden Warnmeldungen sinkt.
- Mit der Kategorisierung von Riskware kann zwischen kritischen Sicherheitsverletzungen und unerwünschten, aber weniger gefährlichen Aktivitäten (z. B. durch Adware und Spyware) unterschieden werden. Dies ermöglicht eine Priorisierung der erforderlichen Gegenmaßnahmen anhand der Dringlichkeit.

Praxistaugliche Informationen über Bedrohungen

Die von FireEye Network Security generierten Warnmeldungen beinhalten konkrete verwertbare und kontextbezogene Daten, damit Bedrohungen rasch priorisiert, eingedämmt und abgewehrt werden können.

- **Dynamic Threat Intelligence (DTI):** konkrete, global genutzte Echtzeitdaten zur umgehenden und proaktiven Abwehr gezielter und neu erkannter Angriffe
- **Advanced Threat Intelligence (ATI):** kontextbezogene Informationen über den Angriff, damit umgehend die entsprechenden Maßnahmen zur Eindämmung der Bedrohung eingeleitet werden können

Integration in die Prozesse zur Bedrohungsabwehr

FireEye Network Security kann für die Automatisierung der Reaktion auf Warnmeldungen ergänzt werden:

- FireEye Central Management gleicht die Warnmeldungen von FireEye Network Security und FireEye Email Security ab, um einen umfassenderen Überblick über den Angriff bereitzustellen und Abwehrregeln zu definieren, die eine Ausbreitung verhindern.
- FireEye Network Forensics lässt sich mit FireEye Network Security integrieren. Dies ermöglicht die lückenlose Erfassung und gründliche Untersuchung der mit einer Warnmeldung zusammenhängenden Datenpakete.
- FireEye Endpoint Security identifiziert, prüft und isoliert von FireEye Network Security erkannte Sicherheitsverletzungen, um die Eindämmung und Schadensbehebung an den betroffenen Endpunkten zu erleichtern.

Flexible Bereitstellungsoptionen

FireEye Network Security bietet verschiedene Bereitstellungsoptionen für unterschiedliche Unternehmensanforderungen und -budgets:

- **Integrated Network Security:** eine All-in-one-Hardware-Appliance mit integriertem MVX-Dienst zur Sicherung des Internet-Zugangspunkts an einem spezifischen Standort. Bei FireEye Network Security handelt es sich um eine einfach zu administrierende Plattform ohne Client, die in weniger als 60 Minuten einsatzbereit ist. Ihr Einsatz erfordert weder die Konfiguration von Regeln und Richtlinien noch Anpassungen der Konfigurationseinstellungen.
- **Distributed Network Security:** erweiterbare Appliances mit zentral genutztem MVX-Dienst zur Sicherung von Internet-Zugangspunkten im Unternehmen.
  - **Network Smart Nodes: physische oder virtuelle Appliances, die den Internet-Datenverkehr überwachen, um schädlichen Traffic zu identifizieren und zu blockieren und verdächtige Aktivitäten über eine verschlüsselte Verbindung an den MVX-Dienst zur detaillierten Analyse weiterzuleiten.**
  - **MVX Smart Grid: unternehmensintern installierter, zentraler und flexibler MVX-Dienst, der transparente Skalierbarkeit, integrierte N+1-Fehlertoleranz und automatisiertes Load Balancing bietet.**
  - **FireEye Cloud MVX: abonnementbasierter, von FireEye gehosteter MVX-Dienst, der eine datenschutzgerechte Überwachung des Datenverkehrs auf dem Network Smart Node ermöglicht. Nur verdächtige Objekte werden über eine verschlüsselte Verbindung an den MVX-Dienst weitergeleitet, wo sie später umgehend gelöscht werden, falls sie sich bei der Analyse als harmlos erweisen.**

Abbildung 2: Ausgewählte Appliances für Integrated Network Security: NX 2550, NX 3500, NX 5500, NX 6500

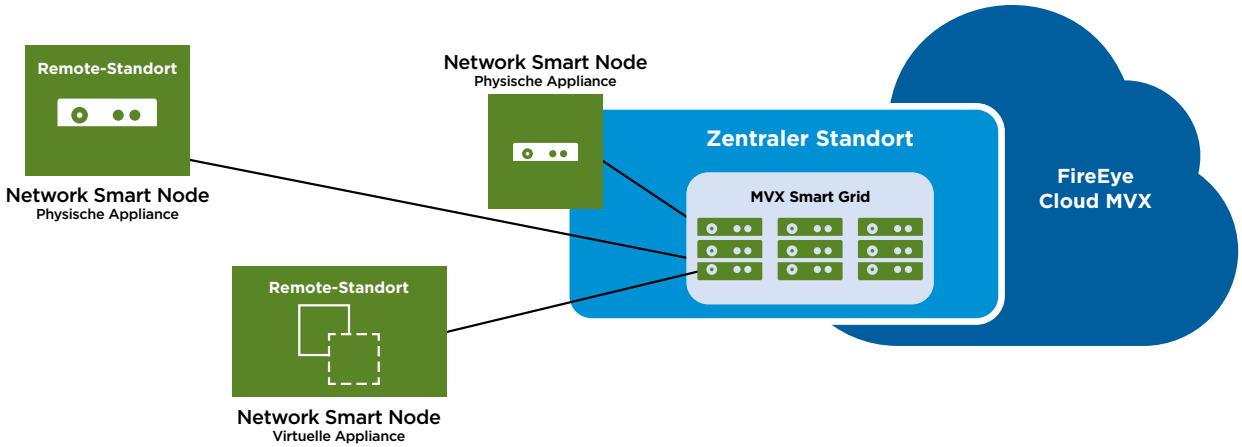


Abbildung 3: Bereitstellungsoptionen für Distributed Network Security

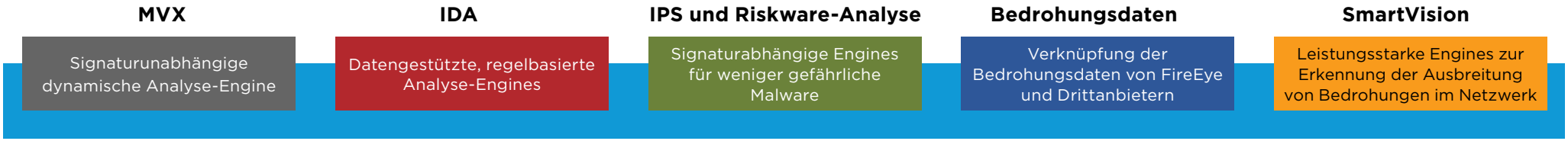


Abbildung 4: Modulare Komponenten von FireEye Network Security

Erweiterbare Architektur

FireEye Network Smart Nodes zeichnen sich durch eine modulare und erweiterbare Softwarearchitektur und ein dazu passendes Systemdesign aus. Infolgedessen können verschiedene Funktionen für den Schutz vor Bedrohungen als Softwaremodule bereitgestellt werden.

Herausragende Leistung und Skalierbarkeit

FireEye Network Security bietet verschiedene Leistungsoptionen für den Schutz von Internet-Zugangspunkten in den Zweigstellen und am Hauptsitz des Kundenunternehmens:

Dank der skalierbaren Architektur von MVX Smart Grid und FireEye Cloud MVX kann der MVX-Service Umgebungen jeder Größe unterstützen – von einem einzigen bis zu Tausenden von Network Smart Nodes.

Formfaktor	Leistung
Integrated Network Security	50 Mbit/s bis 1 Gbit/s
Physischer Network Smart Node	50 Mbit/s bis 10 Gbit/s
Virtueller Network Smart Node	50 Mbit/s bis 1 Gbit/s

Mehrwert und Vorteile

FireEye Network Security bietet sowohl Unternehmen mit einem Standort als auch Unternehmen mit mehreren Standorten zahlreiche Vorteile:

Minimierung des Risikos von Sicherheitsverletzungen

FireEye Network Security ist eine äußerst effektive Cybersicherheitslösung zur …

- Unterbindung gezielter und gut getarnter Angriffe: Cyberkriminelle werden daran gehindert, das Unternehmensnetzwerk zu infiltrieren und dort wertvolle Daten zu stehlen oder den Geschäftsbetrieb zu stören.
- Eindämmung und Abwehr von Angriffen: Die Lösung liefert forensische Beweise und praxistaugliche Bedrohungsdaten, ermöglicht Inline-Abwehrmaßnahmen und unterstützt automatisierte Notfallprozesse.
- Behebung von Schwachstellen und Sicherheitslücken in der Infrastruktur des Unternehmens: An den Hauptstandorten und in den Zweigstellen werden Komponenten mit diversen Betriebssystemen und Anwendungen kontinuierlich geschützt.

Rasche Amortisierung

Laut einem kürzlich von Forrester Consulting veröffentlichten Bericht[1] können Kunden von FireEye Network Security mit beträchtlichen Einsparungen rechnen und dadurch eine Rendite von 152% in drei Jahren realisieren sowie die Amortisierung ihrer ursprünglichen Investition in nur 9,7 Monaten erwarten. Im Einzelnen bietet FireEye Network Security folgende finanziellen Vorteile:

- Sicherheitsteams können sich auf tatsächliche Angriffe konzentrieren und so die Betriebskosten senken.
- Die Lösung fördert die optimale Nutzung getätigter Investitionen durch den gemeinsam genutzten MVX-Dienst und eine Vielzahl an Leistungsoptionen für die genaue Anpassung der Sicherheitsinfrastruktur an spezifische Anforderungen.
- Dank der nahtlosen Skalierbarkeit kann der Schutz auf neue Standorte ausgedehnt und an steigende Traffic-Volumen angepasst werden. Das ermöglicht zukunftsorientierte Investitionsstrategien.
- Die Möglichkeit zur kostenlosen Migration von einem integrierten zu einem verteilten Bereitstellungsmodell bietet Investitionssicherheit.
- Die modulare und erweiterbare Architektur minimiert künftige Investitionskosten.

Auszeichnungen und Zertifizierungen

Das Produktportfolio von FireEye Network Security hat bereits zahlreiche staatliche Auszeichnungen und Branchenpreise erhalten:

- Im Jahr 2016 führte Frost & Sullivan FireEye als unumstrittenen Marktführer auf und bezifferte den Marktanteil des Unternehmens auf 56% – mehr als die nachfolgenden zehn Anbieter zusammen.[2]
- FireEye Network Security hat zahlreiche Auszeichnungen gewonnen, unter anderem von SANS Institute, SC Magazine und CRN.
- FireEye Network Security war die erste nach dem US Department of Homeland Security Safety Act zertifizierte Sicherheitslösung auf dem Markt.

[1] Forrester (Mai 2016): The Total Economic Impact Of FireEye
[2] Frost & Sullivan (Oktober 2016): Network Security Sandbox Market Analysis

Tabelle 1: FireEye Network Security, integrierte Appliances – technische Daten

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Unterstützte Betriebssysteme	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
Leistung*	Bis zu 50 Mbit/s oder 100 Mbit/s	Bis zu 250 Mbit/s	Bis zu 500 Mbit/s	Bis zu 1 Gbit/s	Bis zu 2,5 Gbit/s	Bis zu 5 Gbit/s
Ports für Netzwerküberwachung	4 Ports für 10/100/1000-BASE-T (Vorderseite)	4 x 10 GigE SFP+ 4 × 1 GigE Bypass	4 x 10 GigE SFP+ 4 × 1 GigE Bypass	8 x 10 GigE SFP+ 4 × 1 GigE Bypass	8 x 10 GigE SFP+ 4 × 1 GigE Bypass	8 × 1 GigE/10GigE SFP+ 2 × 40GigE QSFP+
Betriebsmodi Netzwerkports	Inline-Überwachung, Fail-Open, Fail-Close (HW-Bypass) oder TAP/SPAN	Inline-Überwachung, Fail-Open, Fail-Close (HW-Bypass) oder TAP/SPAN	Inline-Überwachung, Fail-Open, Fail-Close (HW-Bypass) oder TAP/SPAN	Inline-Überwachung, Fail-Open, Fail-Close (HW-Bypass) oder TAP/SPAN	Inline-Überwachung, Fail-Open, Fail-Close (HW-Bypass) oder TAP/SPAN	Inline-Überwachung oder TAP/SPAN
Hochverfügbarkeit	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Hochverfügbarkeits-Ports (Rückseite)	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	2 Ports für 100/1000/10G-BASE-T	Nicht vorhanden
Managementports (Rückseite)	2 Ports für 10/100/1000-BASE-T (Vorderseite)	2 Ports für 10/100/1000-BASE-T	2 Ports für 10/100/1000-BASE-T	2 Ports für 10/100/1000-BASE-T	2 Ports für 10/100/1000-BASE-T	4 Ports für 1000BASE-T
IPMI-Port (Rückseite)	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden
LCD-Anzeige und Tastenfeld auf Vorderseite	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden
VGA-Port	Nein	Ja	Ja	Ja	Ja	Ja
USB-Ports	2 USB-Ports Typ A (Vorderseite)	4 USB-Ports Typ A je 2 auf Vorder- und Rückseite	4 USB-Ports Typ A je 2 auf Vorder- und Rückseite	4 USB-Ports Typ A je 2 auf Vorder- und Rückseite	4 USB-Ports Typ A je 2 auf Vorder- und Rückseite	2 USB-Ports Typ A
Serieller Port (Rückseite)	115.200 bit/s; keine Parität; 8 Bits; 1 Stoppbit (RJ45-Anschluss, RJ45-zu-DSUB-Adapterkabel im Lieferumfang enthalten)	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
Laufwerkskapazität	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 4 TB, 7.200 U/min, FRU RAID1	2 3,5-Zoll-SAS3-Festplatten mit je 4 TB, 7.200 U/min, FRU RAID1	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, 7200 U/min FRU RAID1
Gehäuse	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
Abmessungen (B × T × H)	437 × 500 ×43,2 mm	437 × 650 × 43,2 mm	438 × 620× 88,4 mm	438 × 620× 88,4 mm	438 × 620× 88,4 mm	437 x 787 x 89 mm
Wechselstromanschluss	Ein 250 Watt-Anschluss; 90–264 V; 3,5–1,5 A; 50–60 Hz; Eingang nach IEC60320-C14; intern; nicht auswechselbar	Redundant (1+1) 750 W bei 100–240 V, 9,0–4.5 A, 50-60 Hz; Eingang nach IEC 60320-C14; FRU	Redundant (1+1) 800 W bei 100–240 V, 10,5–4,0 A, 50-60 Hz; Eingang nach IEC 60320-C14; FRU	Redundant (1+1) 800 W bei 100–240 V, 10,5–4,0 A, 50-60 Hz; Eingang nach IEC 60320-C14; FRU	Redundant (1+1) 800 W bei 100–240 V, 10,5–4,0 A, 50-60 Hz; Eingang nach IEC 60320-C14; FRU	Redundant (1+1) 1000 Watt bei 100–240 V, 10,5–4,0 A, 50–60 Hz; Eingang nach IEC 60320-C14; FRU

Tabelle 1: FireEye Network Security, integrierte Appliances – technische Daten (Forts.)

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Maximaler Stromverbrauch	85 W	265 W	426 W	519 W	658 W	660 W
Maximale thermische Verlustleistung	85 W	265 W	426 W	519 W	658 W	660 W
Mittlere Betriebsdauer zwischen Ausfällen (MTBF)	56.400 h	54.200 h	65.466 h	57.766 h	52.802 h	54.041 h
Nettogewicht der Appliance /Versandgewicht	7,3 kg / 12,79 kg	13,5 kg/ 18,5 kg	17,0 kg/ 26,6 kg	19,2 kg/ 28,8 kg	19,2 kg/ 29,0 kg	20 kg 32,2 kg
Erfüllte Sicherheitsstandards	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Sicherheitszertifizierungen	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1
Erfüllte EMV-Standards	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	Sicherheit: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J 60950, SI 60950 EMV:FCC Teil 15 Abschnitt B Klasse A; ICES-003; EN 55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR 32; KN 32; KN 35
Erfüllte Umweltrichtlinien	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS; REACH; WEEE Konfliktrohstoffe
Betriebstemperatur	0 °C bis ca. 40 °C	0 °C bis ca. 35 °C	0 °C bis ca. 35 °C	0 °C bis ca. 35 °C	0 °C bis ca. 35 °C	10 °C bis 35 °C, getestet für erweiterten Bereich von 0 °C bis 40 °C
Lagertemperatur	-20 °C bis ca. 80 °C	-40 °C bis ca. 70 °C	-40 °C bis ca. 70 °C	-40 °C bis ca. 70 °C	-40 °C bis ca. 70 °C	-30 °C bis ca. 70 °C
Relative Luftfeuchtigkeit bei Betrieb	5–85% (nicht kondensierend)	10 bis ca. 95% bei 40 °C, nicht kondensierend	10 bis ca. 95% bei 40 °C, nicht kondensierend	10 bis ca. 95% bei 40 °C, nicht kondensierend	10 bis ca. 95% bei 40 °C, nicht kondensierend	10 bis ca. 95% bei 60 °C, nicht kondensierend
Relative Luftfeuchtigkeit bei Lagerung	5–95% (nicht kondensierend)	10 bis ca. 95% bei 60 °C, nicht kondensierend	10 bis ca. 95% bei 60 °C, nicht kondensierend	10 bis ca. 95% bei 60 °C, nicht kondensierend	10 bis ca. 95% bei 60 °C, nicht kondensierend	10 bis ca. 95% bei 55 °C, nicht kondensierend
Maximale Betriebshöhe	3.000 m	3.000 m	3.000 m	3.000 m	3.000 m	3.000 m

Tabelle 2: Technische Daten zum IPS der integrierten Appliances von FireEye Network Security

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Max. IPS-Leistung	Bis zu 50 Mbit/s oder 100 Mbit/s	Bis zu 250 Mbit/s	Bis zu 500 Mbit/s	Bis zu 1 Gbit/s	Bis zu 2,5 Gbit/s	Bis zu 5 Gbit/s
Max. gleichzeitige Verbindungen	15.000 oder 80.000	80.000	160.000	500.000	1.000.000	2.000.000
Neue Verbindungen pro Sekunde	750 oder 4.000	4.000	8.000	10.000	20.000	40.000

Tabelle 3: Physische FireEye Network Security Smart Nodes – technische Daten

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Unterstützte Betriebssysteme	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
Leistung	Bis zu 50 Mbit/s	Bis zu 100 oder 250 Mbit/s	Bis zu 500 Mbit/s	Bis zu 1 Gbit/s	Bis zu 2 Gbit/s	Bis zu 5 Gbit/s	Bis zu 10 Gbit/s
Ports für Netzwerk-überwachung	4 Ports für 10/100/1000-BASE-T	4 Ports für 10/100/1000-BASE-T (Vorderseite)	4 x 10 GigE SFP+ 4 × 1 GigE Bypass	4 x 10 GigE SFP+ 4 × 1 GigE Bypass	8 x 10 GigE SFP+ 4 × 1 GigE Bypass	8 x 10 GigE SFP+ 4 × 1 GigE Bypass	8 × 1 GigE/10GigE SFP+ 2 × 40GigE QSFP+
Betriebsmodi Netzwerkports	Inline-Überwachung, Fail Close oder TAP	Inline-Überwachung, Fail-Open, Fail-Close (HW-Bypass) oder TAP/SPAN	Inline-Überwachung, Fail-Open, Fail-Close (HW-Bypass) oder TAP/SPAN	Inline-Überwachung, Fail-Open, Fail-Close (HW-Bypass) oder TAP/SPAN	Inline-Überwachung, Fail-Open, Fail-Close (HW-Bypass) oder TAP/SPAN	Inline-Überwachung, Fail-Open, Fail-Close (HW-Bypass) oder TAP/SPAN	Inline-Überwachung oder TAP/SPAN
Hochverfügbarkeit	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar	Nicht verfügbar
Hochverfügbarkeits-Ports (Rückseite)	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden
Managementports (Rückseite)	2 Ports für 10/100/1000 -BASE-T	4 Ports für 10/100/1000 -BASE-T (Vorderseite)	2 Ports für 10/100/1000 -BASE-T	2 Ports für 10/100/1000 -BASE-T	2 Ports für 10/100/1000 -BASE-T	2 Ports für 10/100/1000 -BASE-T	4 Ports für 1000BASE-T
IPMI-Port (Rückseite)	Nicht vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden	Vorhanden
LCD-Anzeige und Tastenfeld auf Vorderseite	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden	Nicht vorhanden
VGA-Port	Nicht vorhanden	Nicht vorhanden	Ja	Ja	Ja	Ja	Ja
USB-Ports	2 USB-Ports Typ A	2 USB-Ports Typ A (Vorderseite)	4 USB-Ports Typ A je 2 auf Vorder- und Rückseite	4 USB-Ports Typ A je 2 auf Vorder- und Rückseite	4 USB-Ports Typ A je 2 auf Vorder- und Rückseite	4 USB-Ports Typ A je 2 auf Vorder- und Rückseite	2 USB-Ports Typ A

Tabelle 3: Physische FireEye Network Security Smart Nodes – technische Daten (Forts.)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Serieller Port (Rückseite)	115.200 bit/s; keine Parität; 8 Bits; 1 Stoppbit (RJ45-Anschluss; RJ45-zu-DSUB-Adapterkabel im Lieferumfang enthalten)	115.200 bit/s; keine Parität; 8 Bits; 1 Stoppbit (RJ45-Anschluss; RJ45-zu-DSUB-Adapterkabel im Lieferumfang enthalten)	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
Laufwerkskapazität	1 interne 2,5-Zoll-SATA-Festplatte mit 500 GB Speicherplatz; nicht auswechselbar	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 4 TB, 7.200 U/min, FRU RAID1	2 3,5-Zoll-SAS3-Festplatten mit je 4 TB, 7.200 U/min, FRU RAID1	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, 7200 U/min, FRU RAID1
Gehäuse	Desktop-Baugröße	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
Abmessungen (B × T × H)	280 mm × 175 mm × 45,7 mm	437 mm × 500 mm × 43,2 mm	437 mm × 650 mm × 43,2 mm	438 mm × 620 mm × 88,4 mm	438 mm × 620 mm × 88,4 mm	438 mm × 620 mm × 88,4 mm	437 mm × 709 mm × 89 mm
Wechsel-stromanschluss	Externes 12V/5A-Ausgangswechsel-stromadapter mit 60 Watt; 90–264 V; 50–60 Hz; Eingang nach IEC60320-C14; FRU	Ein 250 Watt-Anschluss; 90–264 V; 3,5–1,5 A; 50–60 Hz; Eingang nach IEC60320-C14; intern; nicht auswechselbar	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) 800 W bei 100–240 V AC; 9–4,5 A; 50–60 Hz; Eingang nach IEC 60320-C14, FRU	Redundant (1+1) 800 W bei 100–240 V AC; 9–4,5 A; 50–60 Hz; Eingang nach IEC 60320-C14, FRU	Redundant (1+1) 800 W bei 100–240 V, 10,5–4,0 A, 50-60 Hz; Eingang nach IEC 60320-C14; FRU	Redundant (1+1) 1000 Watt bei 100–240 V, 10,5–4,0 A, 50–60 Hz; Eingang nach IEC 60320-C14; FRU
Maximaler Stromverbrauch	27 W	85 W	265 W	426 W	519 W	658 W	660 W
Maximale thermische Verlustleistung	27 W	85 W	265 W	426 W	519 W	658 W	660 W
Mittlere Betriebsdauer zwischen Ausfällen (MTBF)	95.400 h	56.400 h	54.200 h	65.466 h	57.766 h	52.802 h	54.041 h
Nettogewicht der Appliance / Versandgewicht	1,7 kg / 2,95 kg	7,3 kg / 12,79 kg	13,5 kg / 18,5 kg	17,0 kg / 26,6 kg	19,2 kg / 28,8 kg	19,2 kg / 29,0 kg	20 kg 32,2 kg
Erfüllte Sicherheitsstandards	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Sicherheits-zertifizierungen	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1	FIPS 140-2 Level 1 CC NDPP v1.1

Tabelle 3: Physische FireEye Network Security Smart Nodes – technische Daten (Forts.)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Erfüllte EMV-Standards	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	Sicherheit: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J 60950, SI 60950 EMV: FCC Teil 15 Abschnitt B Klasse A; ICES-003; EN 55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR 32; KN 32; KN 35
Erfüllte Umweltrichtlinien	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS; REACH; WEEE Konfliktrohstoffe
Betriebstemperatur	0 °C bis ca. 40 °C	0 °C bis ca. 40 °C	0 °C bis ca. 35 °C	0 °C bis ca. 35 °C	0 °C bis ca. 35 °C	0 °C bis ca. 35 °C	10 °C bis 35 °C, getestet für erweiterten Bereich von 0 °C bis 40 °C
Lagertemperatur	-20 °C bis ca. 80 °C	-20 °C bis ca. 80 °C	-40 °C bis ca. 70 °C	-40 °C bis ca. 70 °C	-40 °C bis ca. 70 °C	-40 °C bis ca. 70 °C	-30 °C bis ca. 70 °C
Relative Luftfeuchtigkeit bei Betrieb	5–85% (nicht kondensierend)	5–85% (nicht kondensierend)	10 bis ca. 95% bei 40 °C, nicht kondensierend	10 bis ca. 95% bei 40 °C, nicht kondensierend	10 bis ca. 95% bei 40 °C, nicht kondensierend	10 bis ca. 95% bei 40 °C, nicht kondensierend	10 bis ca. 95% bei 60 °C, nicht kondensierend
Relative Luftfeuchtigkeit bei Lagerung	5–95% (nicht kondensierend)	5–95% (nicht kondensierend)	10 bis ca. 95% bei 60 °C, nicht kondensierend	10 bis ca. 95% bei 60 °C, nicht kondensierend	10 bis ca. 95% bei 60 °C, nicht kondensierend	10 bis ca. 95% bei 60 °C, nicht kondensierend	10 bis ca. 95% bei 55 °C, nicht kondensierend
Maximale Betriebshöhe	3.000 m	3.000 m	3.000 m	3.000 m	3.000 m	3.000 m	3.000 m

Tabelle 4: Technische Daten zum IPS der physischen FireEye Network Smart Nodes

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Max. IPS-Leistung	Bis zu 50 Mbit/s	Bis zu 100/250 Mbit/s	Bis zu 500 Mbit/s	Bis zu 1 Gbit/s	Bis zu 2 Gbit/s	Bis zu 5 Gbit/s	Bis zu 10 Gbit/s
Max. gleichzeitige Verbindungen	15.000	80.000	160.000	500.000	1.000.000	2.000.000	4.000.000
Neue Verbindungen pro Sekunde	750	4.000	8.000	10.000	20.000	40.000	80.000

Tabelle 5: Virtuelle FireEye Network Smart Nodes – technische Daten

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Unterstützte Betriebssysteme	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
Leistung*	Bis zu 50 Mbit/s	Bis zu 100 Mbit/s	Bis zu 250 Mbit/s	Bis zu 500 Mbit/s	Bis zu 1 Gbit/s
Ports für Netzwerküberwachung	1–8	1–8	1–8	1–8	1–8
Netzwerk-Managementports	1 oder 2	1 oder 2	1 oder 2	1 oder 2	1 oder 2
Betriebsmodi Netzwerkports	Inline, SPAN	Inline, SPAN	Inline, SPAN	Inline, SPAN	Inline, SPAN
CPU-Kerne	3	6	8	8	16
Speicher	10 GB	16 GB	16 GB	32 GB	32 GB
Laufwerkskapazität	384 GB	384 GB	384 GB	512 GB	512 GB
Netzwerkadapter	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC
Hypervisor-Unterstützung	VMWare ESXi 6.0 oder höher	VMWare ESXi 6.0 oder höher	VMWare ESXi 6.0 oder höher	VMWare ESXi 6.0 oder höher	VMWare ESXi 6.0 oder höher
Sicherheitszertifizierungen	FIPS 140-2 Level 1 CC NDPP v1.1 (in Bearbeitung)	FIPS 140-2 Level 1 CC NDPP v1.1 (in Bearbeitung)	FIPS 140-2 Level 1 CC NDPP v1.1 (in Bearbeitung)	FIPS 140-2 Level 1 CC NDPP v1.1 (in Bearbeitung)	FIPS 140-2 Level 1 CC NDPP v1.1 (in Bearbeitung)

Tabelle 6: Technische Daten zum IPS der virtuellen FireEye Network Smart Nodes

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Max. IPS-Leistung	Bis zu 50 Mbit/s	Bis zu 100 Mbit/s	Bis zu 250 Mbit/s	Bis zu 500 Mbit/s	Bis zu 1 Gbit/s
Max. gleichzeitige Verbindungen	15.000	80.000	80.000	160.000	500.000
Neue Verbindungen pro Sekunde	750	4.000	4.000	8.000	10.000

Tabelle 7: Daten zu FireEye MVX Smart Grid

	VX 5500	VX 12500
Unterstützte Betriebssysteme	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X
Leistung*	Bis zu 2 Gbit/s	Bis zu 10 Gbit/s
Hochverfügbarkeit**	N+1	N+1
Managementports (Rückseite)	1 Port für 10/100/1000 Mbit/s BASE-T	1 Port für 10/100/1000 Mbit/s BASE-T
Cluster-Ports (Rückseite)	3 Ports für 10/100/1000 Mbit/s BASE-T	1 Port für 10/100/1000 Mbit/s BASE-T, 2 Ports für 10 Gbit/s BASE-T
IPMI-Port (Rückseite)	Vorhanden	Vorhanden
LCD-Anzeige und Tastenfeld auf Vorderseite	Nicht vorhanden	Vorhanden
VGA-Ports	Vorhanden	Vorhanden
USB-Ports (Rückseite)	4 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
Laufwerkskapazität	2 3,5-Zoll-SAS-Festplatten mit je 2 TB; RAID 1; im Betrieb austauschbar; FRU	4 2,5-Zoll-Festplatten mit je 900 GB; RAID 10; FRU
Gehäuse	1 HE; passend für 19-Zoll-Rack	2 HE; passend für 19-Zoll-Rack
Abmessungen (B × T × H)	437 × 650 × 43,2 mm	437 × 851 × 89 mm
Gleichstromanschluss	Nicht vorhanden	Nicht vorhanden
Wechselstromanschluss	Redundant (1+1) 750 W; 100–240 V; 8–3,8 A; 50–60 Hz; Eingang nach IEC 60320-C14; im Betrieb austauschbar; FRU	Redundant (1+1) 800 W: 100–127 V, 9,8–7 A; 1000 W: 220–240 V, 7–5 A; 50–60 Hz; FRU-Eingang nach IEC 60320-C14; FRU
Maximaler Stromverbrauch	285 W	760 W
Maximale thermische Verlustleistung	285 W	760 W
Mittlere Betriebsdauer zwischen Ausfällen (MTBF)	54.200 h	38.836 h
Nettogewicht der Appliance / Versandgewicht	15 kg / 21,8 kg	21 kg / 40,2 kg
Sicherheitszertifizierungen	FIPS 140-2 Level 1, CC NDPP v1.1 (Ausstehend)	FIPS 140-2 Level 1, CC NDPP v1.1 (Ausstehend)
Erfüllte Sicherheitsstandards	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

Tabelle 7: Daten zu FireEye MVX Smart Grid

	VX 5500	VX 12500
Erfüllte EMV-Standards	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015	FCC Teil 15 ICES-003 Klasse 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 und V-3/2015
Erfüllte Umweltrichtlinien	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU	RoHS-Richtlinie 2011/65/EU REACH WEEE-Richtlinie 2012/19/EU
Betriebstemperatur	10 °C bis ca. 35 °C	10 °C bis ca. 35 °C
Lagertemperatur	-40 °C bis ca. 70 °C	-40 °C bis ca. 70 °C
Relative Luftfeuchtigkeit bei Betrieb	10–85% (nicht kondensierend)	10–85% (nicht kondensierend)
Relative Luftfeuchtigkeit bei Lagerung	5–95% (nicht kondensierend)	5–95% (nicht kondensierend)
Maximale Betriebshöhe	3.000 m	3.000 m

Tabelle 8: Active Fail Open Switch, technische Daten

	AFO 10G SWITCH
Abmessungen (B × T × H)	165 × 356 × 28 mm
Managementports	1 serieller DB9-Konsolenanschluss, 1 Port für 10/100 Cat5e-RJ45
Netzwerkports	1 LC-Quad-Steckverbinder
Überwachungsports	2 XFP-Ports
Stromversorgung	100–240 V Wechselstrom; 1,0 A; 47–63 Hz
Betriebstemperatur	0 °C bis ca. 40 °C

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

** Mit der erforderlichen redundanten Hardwarekonfiguration

Supportleistungen

FireEye bietet einfache und flexible Support-programme an, damit Sie den größtmöglichen Nutzen aus Ihren Produkten und Lösungen von FireEye ziehen können. Vier verschiedene Supportleistungsstufen sind verfügbar: Platinum, Platinum Priority Plus, Government und Government Priority Plus. Weitere Informationen zum FireEye-Support erhalten Sie von den Experten von FireEye Support Services.

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 unterstützt FireEye Kundenunternehmen bei der Vorbereitung auf die Erkennung und Abwehr von Cyberangriffen. FireEye hat über 5.300 Kunden in 67 Ländern, darunter mehr als 845 der Forbes-Global-2000-Unternehmen.