SCHEDA TECNICA

FireEye Network Security

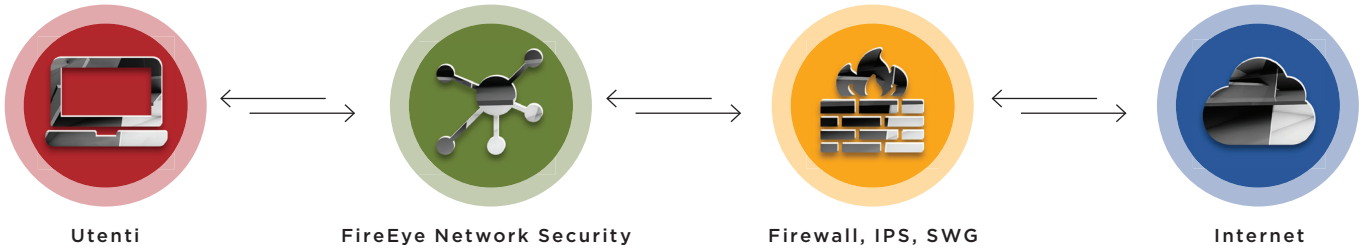
Protezione efficace contro le intrusioni informatiche per imprese di medie e grandi dimensioni

Panoramica
FireEye Network Security è un'efficace soluzione di protezione dalle minacce informatiche che aiuta le imprese a ridurre al minimo il rischio di costose violazioni, rilevando con precisione e bloccando immediatamente attacchi avanzati, mirati e altri tipi di attacchi evasivi nascosti nel traffico Internet. Consente di risolvere i ciberincidenti rilevati in modo efficiente, in pochi minuti, con prove concrete, informazioni fruibili e integrazione delle attività di risposta. Con FireEye Network Security, le imprese sono protette in modo efficace contro le attuali minacce, da quelle che sfruttano i sistemi operativi Microsoft Windows e Apple OS X o le vulnerabilità delle applicazioni a quelle dirette alle sedi centrali o filiali, passando per quelle nascoste in un grande volume di traffico Internet in ingresso che deve essere ispezionato in tempo reale.

Alla base di FireEye Network Security vi sono le tecnologie Multi-Vector Virtual Execution™ (MVX) e Intelligence-Driven Analysis (IDA). MVX è un motore di analisi dinamico senza firma che controlla il traffico di rete sospetto per identificare attacchi che eludono i sistemi di difesa tradizionali basati su criteri e firme. IDA è una raccolta di motori contestuali con regole dinamiche, che rilevano e bloccano le attività dannose in tempo reale e retroattivamente grazie alle ultime informazioni basate su macchina, aggressore e vittima. Inoltre, FireEye Network Security include la tecnologia (*intrusion prevention system,* IPS) per rilevare gli attacchi comuni con la convenzionale corrispondenza delle firme.

FireEye Network Security è disponibile in diverse opzioni suddivise per fattore di forma, implementazione e prestazioni. Normalmente si inserisce nel percorso del traffico Internet dietro alle apparecchiature di sicurezza di rete tradizionali come firewall di nuova generazione, IPS e gateway web sicuri (*secure web gateways,* SWG). FireEye Network Security integra queste soluzioni mediante una rapida rilevazione di attacchi noti e sconosciuti con elevata precisione e un basso indice di falsi positivi, facilitando al contempo una risposta efficiente a ogni avviso.

Figura 1. Configurazione tipica - Soluzioni di sicurezza di rete.



Funzionalità	Vantaggi
Rilevamento	
Rilevamento accurato di attacchi informatici avanzati, mirati e altri tipi di attacchi evasivi	Riduce al minimo il rischio di costosi ciberincidenti
Architettura di protezione modulare ed estensibile	Fornisce una protezione degli investimenti
Livello coerente di protezione per ambienti multi-OS e tutti i punti di accesso a Internet	Crea una difesa solida in tutta l'azienda per tutti i tipi di dispositivi
Opzioni di distribuzione integrata, distribuita, fisica, virtuale, in loco e su cloud	Offre la flessibilità necessaria per allinearsi alle preferenze e alle risorse aziendali
Correlazione multi-vettoriale con Email e Content Security	Fornisce visibilità su una più ampia superficie di attacco
Prevenzione	
Blocco immediato degli attacchi a velocità di linea da 10 Mbit/s a 8 Gbit/s	Fornisce protezione in tempo reale contro gli attacchi evasivi
Risposta	
Basso tasso di falsi allarmi, categorizzazione riskware e convalida avvisi IPS automatizzata	Riduce i costi operativi per filtrare gli avvisi inaffidabili
Agevola convalida di avvisi e indagini, contenimento degli endpoint e risposta agli incidenti	**Automatizza e semplifica i flussi di lavoro di sicurezza**
Prove di esecuzione e informazioni fruibili sulle minacce con una visione contestuale	**Accelera la definizione delle priorità e la risoluzione dei ciberincidenti rilevati**
Scalabilità da un sito a migliaia di siti	**Sostiene la crescita aziendale**

Vantaggi tecnici

Rilevamento accurato delle minacce

FireEye Network Security utilizza più tecniche di analisi per rilevare attacchi con elevata precisione e un basso tasso di falsi allarmi:

- Il motore **Multi-Vector Virtual Execution™ (MVX)** rileva attacchi zero-day, multi-flusso e altri attacchi evasivi con analisi dinamica, senza firma in un ambiente sicuro e virtuale. Ferma le fasi di infezione e compromissione della catena di attacchi informatici identificando exploit e malware mai visti prima.
- I motori **Intelligence-Driven Analysis (IDA)** rilevano e bloccano attacchi camuffati, mirati e altri attacchi personalizzati attraverso l'analisi contestuale basata su regole grazie a informazioni di prima mano raccolte in tempo reale da milioni di verdetti MVX, migliaia di ore di attività di risposta agli incidenti svolta da Mandiant, un'azienda FireEye, e centinaia di esperti di cibersicurezza iSight. Ferma le fasi di infezione, compromissione e intrusione della catena di cyber-attacco identificando exploit dannosi, malware e callback di comando e controllo (CnC). Inoltre, estrae e sottopone il traffico di rete sospetto al motore MVX per un'analisi di verdetto definitiva.
- **Structured Threat Intelligence eXpression (STIX)** permette di inglobare le informazioni sulle minacce di terze parti utilizzando un formato standard di settore per aggiungere indicatori di minaccia personalizzati nei motori IDA.

Protezione immediata e resiliente

FireEye Network Security offre modalità di configurazione flessibili, tra cui:

- Monitoraggio fuori banda tramite un TAP/SPAN, monitoraggio in linea o blocco attivo in linea. La modalità di blocco in linea blocca automaticamente gli exploit web in ingresso e i callback multiprotocollo in uscita. In modalità monitoraggio in linea genera gli avvisi e permette alle aziende di decidere come reagire. In modalità di prevenzione fuori banda, FireEye Network Security rilascia reset TCP per il blocco fuori banda di connessioni TCP, UDP o HTTP.
- Alcuni modelli offrono un'opzione di elevata disponibilità attiva (*high availability*, HA) per fornire capacità di recupero in caso di guasti di rete o del dispositivo.

Ampia copertura della superficie di attacco

FireEye Network Security offre un livello coerente di protezione per gli eterogenei ambienti di rete di oggi:

- Supporto per i sistemi operativi più diffusi di Microsoft Windows e Apple Mac OS X.
- Analisi di oltre 140 tipi di file diversi, tra cui eseguibili portatili (*portable executables,* PEs), contenuti web, archivi, immagini, Java, applicazioni e file multimediali Microsoft e Adobe.
- Esecuzione del traffico di rete sospetto su migliaia di combinazioni di sistemi operativi, service pack, tipi di applicazione e versioni dell'applicazione.
- Protezione contro attacchi avanzati e tipi di malware difficili da rilevare tramite firma: caricamento ed esecuzione delle webshell, ransomware, cryptominer.

Avvisi convalidati e prioritari

Oltre a rilevare gli attacchi veri e propri, la tecnologia FireEye MVX è utilizzata anche per determinare l'affidabilità degli avvisi rilevati con metodi convenzionali di corrispondenza della firma, e per individuare le minacce critiche e stabilirne l'ordine di priorità:

- Il sistema di prevenzione delle intrusioni (IPS) con convalida del motore MVX riduce il tempo necessario per valutare il rilevamento basato su firme che è tradizionalmente soggetto a falsi allarmi.
- La categorizzazione del riskware separa reali tentativi di violazione da attività indesiderabili, ma meno dannose (come adware e spyware) per stabilire l'ordine di priorità per le risposte agli avvisi.

Informazioni fruibili sulle minacce

Gli avvisi generati da FireEye Network Security si basano su prove concrete e informazioni contestuali che permettono di rispondere rapidamente, ordinare per priorità e contenere una minaccia:

- **Dynamic Threat Intelligence (DTI):** dati concreti, in tempo reale e globalmente condivisi per fermare rapidamente e in modo proattivo gli attacchi mirati e di recente scoperta.
- **Advanced Threat Intelligence (ATI):** informazioni contestuali sull'attacco per accelerare la risposta e indicazioni prescrittive per contenere la minaccia.

Integrazione delle attività di risposta

FireEye Network Security può essere potenziato in vari modi per automatizzare le attività di risposta agli avvisi:

- FireEye Central Management correla gli avvisi inviati da FireEye Email Security e da FireEye Network Security per una visibilità più ampia dell'attacco e per impostare regole di blocco che ne impediscano un'ulteriore diffusione.
- FireEye Network Forensics si integra con FireEye Network Security per fornire una dettagliata acquisizione di pacchetti associata a un avviso e consentire indagini approfondite.
- FireEye Endpoint Security identifica, convalida e contiene compromissioni rilevate da FireEye Security Network per semplificare il contenimento e la correzione degli endpoint colpiti.

Opzioni di distribuzione flessibili

FireEye Network Security offre varie opzioni di distribuzione per soddisfare le esigenze e il budget di un'azienda:

- **Integrated Network Security:** appliance hardware autonoma all-in-one con servizio MVX integrato per proteggere i punti di accesso a Internet in un unico sito. FireEye Network Security è una piattaforma senza client, di facile gestione, che può essere distribuita in meno di 60 minuti. Non necessita di regole, criteri o messa a punto.
- **Distributed Network Security:** appliance estensibili con servizio MVX condiviso centralmente per garantire punti di accesso a Internet all'interno delle aziende.
  - **Network Smart Node:** appliance fisiche o virtuali che analizzano il traffico Internet per rilevare e bloccare il traffico dannoso e segnalare le attività sospette tramite una connessione crittografata al servizio MVX per l'analisi definitiva del verdetto.
  - **MVX Smart Grid:** servizio MVX elastico, locale, gestito centralmente, che offre scalabilità trasparente, tolleranza ai guasti integrata N+1 e bilanciamento automatizzato del carico.
  - **FireEye Cloud MVX:** servizio in abbonamento MVX ospitato da FireEye che garantisce la privacy, analizzando il traffico sul Network Smart Node. Solo gli oggetti sospetti sono inviati tramite una connessione crittografata al servizio MVX, dove gli oggetti che si rivelano non dannosi vengono scartati.
  - **Protezione in loco o su cloud:** Oltre ad appliance autonome e virtuali, FireEye offre Network Security su cloud pubblico con la disponibilità delle Amazon Machine Image (AMI).

Figura 2. Esempi di integrazione di Network Security comprendono NX 2550, NX 3500, NX 5500, NX 10550.

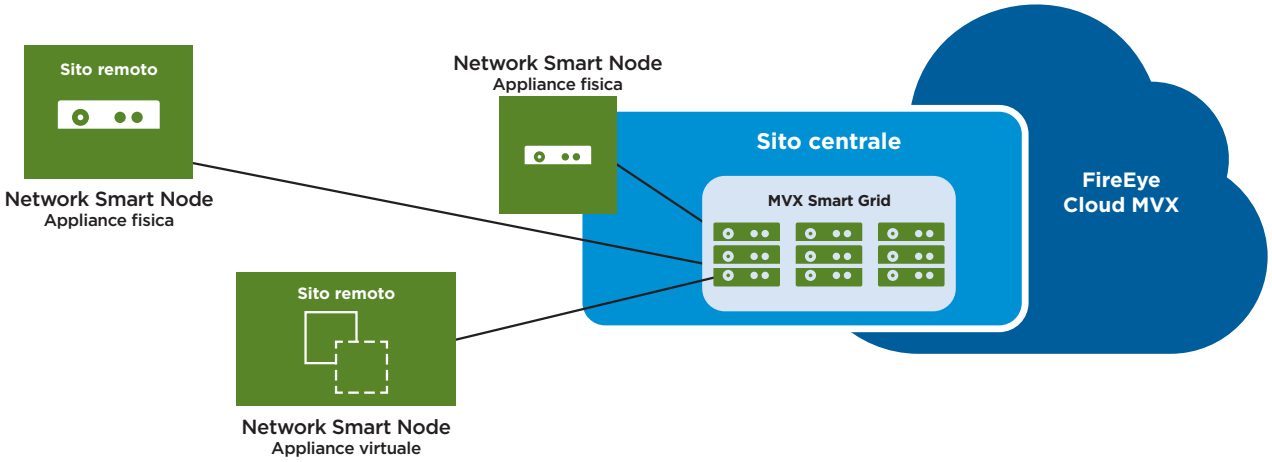


Figura 3. Modelli di implementazione distribuita per la sicurezza di rete.

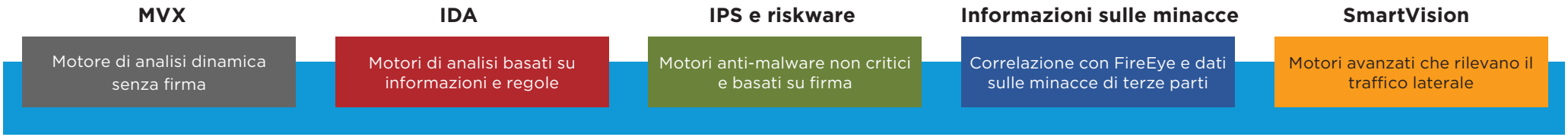


Figura 4. Componenti modulari di FireEye Network Security.

Elevate prestazioni e scalabilità

FireEye Network Security protegge i punti di accesso a Internet a velocità di linea con un'ampia gamma di scelte prestazionali per filiali e uffici centrali di svariate dimensioni:

L'architettura scalabile di MVX Smart Grid e FireEye Cloud MVX consente al servizio MVX di supportare fino a mille Network Smart Node e scalare senza problemi in base alle esigenze.

Formato	Prestazioni
Integrated Network Security	Da 50 Mbit/s a 5 Gbit/s
Network Smart Node fisico	Da 50 Mbit/s a 10 Gbit/s
Network Smart Node virtuale e su cloud pubblico	Da 50 Mbit/s a 1 Gbit/s

Vantaggi per le aziende

Progettato per soddisfare le esigenze di aziende con un'unica sede o varie sedi distribuite, FireEye Network Security offre diversi vantaggi:

Riduce al minimo il rischio di ciberincidenti

FireEye Network Security è una soluzione altamente efficace per la protezione dai ciberattacchi:

- Impedisce agli intrusi di entrare in un'azienda per rubare beni di valore o interrompere l'attività fermando attacchi avanzati, mirati e altri tipi di attacchi evasivi.
- Blocca gli attacchi e contiene le intrusioni più velocemente con prove concrete, informazioni fruibili, blocco in linea e automazione delle attività di risposta.
- Tappa le falle dei sistemi di difesa informatici di un'azienda con una protezione coerente per i vari sistemi operativi, tipi di applicazione, filiali e sedi centrali.

Breve periodo di recupero dell'investimento

Secondo un recente studio di Forrester Consulting[1], i clienti con FireEye Network Security possono aspettarsi un ROI del 152% in tre anni e ammortizzare l'investimento iniziale in soli 9,7 mesi. FireEye Network Security:

- Concentra le risorse del team di sicurezza sugli attacchi reali per ridurre le spese operative.
- Ottimizza la spesa di capitale con un servizio MVX condiviso e una grande varietà di punti di performance per una distribuzione che soddisfi i requisiti.
- Investimenti adeguati alle future esigenze di sicurezza con possibilità di scalare senza problemi quando il numero di filiali o la quantità di traffico Internet aumenta.
- Protegge gli investimenti esistenti, consentendo la migrazione a costo zero da un sistema integrato a un'implementazione distribuita.
- Riduce le spese in conto capitale grazie a un'architettura modulare ed estensibile.

Premi e certificazioni

Il portafoglio di prodotti FireEye Network Security ha ricevuto numerosi premi e certificazioni da organismi statali e associazioni di settore:

- Nel 2018, Frost & Sullivan ha riconosciuto FireEye come il leader indiscusso del mercato con una quota di mercato del 46%, più dei dieci principali concorrenti messi insieme[2].
- FireEye Network Security ha ricevuto numerosi premi da SANS Institute, SC Magazine, CRN e altri.
- FireEye Network Security è stata la prima soluzione di sicurezza sul mercato a ricevere la certificazione del SAFETY Act del Dipartimento della sicurezza interna degli Stati Uniti.

1 Forrester (maggio 2016). The Total Economic Impact Of FireEye.
2 Frost & Sullivan (2018) Advanced Malware Sandbox (AMS) Solutions Market, Global, Forecast to 2022.

Tabella 1. Specifiche FireEye Network Security, appliance integrata.

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Sistema operativo supportato	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Prestazioni*	Fino a 50 Mbit/s o 100 Mbit/s	Fino a 250 Mbit/s	Fino a 500 Mbit/s	Fino a 1 Gbit/s	Fino a 2,5 Gbit/s	Fino a 5 Gbit/s
Porte per il monitoraggio della rete	4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 2x 40GigE QSFP+
Modalità di funzionamento delle porte di rete	Monitoraggio in linea, fail-open, fail-close (bypass HW) o TAP/SPAN	Monitoraggio in linea, fail-open, fail-close (bypass HW) o TAP/SPAN	Monitoraggio in linea, fail-open, fail-close (bypass HW) o TAP/SPAN	Monitoraggio in linea, fail-open, fail-close (bypass HW) o TAP/SPAN	Monitoraggio in linea, fail-open, fail-close (bypass HW) o TAP/SPAN	In linea, Monitoraggio, TAP/SPAN
Disponibilità elevata (HA)	Non disponibile	Non disponibile	Non disponibile	Disponibile	Disponibile	Disponibile
Porte di gestione (pannello posteriore)	2 porte 10/100/1000 BASE-T	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE
Porta IPMI	Pannello anteriore	Pannello posteriore	Pannello posteriore	Pannello posteriore	Pannello posteriore	Pannello posteriore
LCD frontale e tastierino numerico	Non disponibile	Non disponibile	Non disponibile	Non disponibile	Non disponibile	Non disponibile
Porta VGA	No	Sì	Sì	Sì	Sì	Sì
Porte USB	2 porte USB Tipo A (pannello anteriore)	4 porte USB Tipo A (tutte posteriori)	4 porte USB Tipo A 2 anteriori, 2 posteriori	4 porte USB Tipo A 2 anteriori, 2 posteriori	4 porte USB Tipo A 2 anteriori, 2 posteriori	2 porte USB Tipo A
Porta seriale (pannello posteriore)	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop (connettore RJ45, il cavo adattatore RJ45-to-Dsub è incluso)	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop
Capacità unità	HDD singolo 1 TB 3,5 pollici SATA, interno, fisso	2 x 4 TB HDD, 3,5 po, SAS3, 7,2 krpm, FRU RAID1	2 x 4TB HDD, 3,5 po, SAS3, 7,2 krpm, FRU RAID1	2 x 4TB HDD, 3,5 po, SAS3, 7,2 krpm, FRU RAID1	2 x 4TB HDD, 3,5 po, SAS3, 7,2 krpm, FRU RAID1	2x 10TB HDD,3,5 po, SAS3, 7,2 krpm FRU RAID1
Involucro	1RU, Rack 19 pollici	1RU, Rack 19 pollici	2RU, Rack 19 pollici	2RU, Rack 19 pollici	2RU, Rack 19 pollici	2RU, Rack 19 pollici
Dimensioni chassis (LxPxA)	17,2 po (437 mm) x 19,7 po (500 mm) x 1,7 po (43,2 mm)	17,2 po (437 mm) x 25,6 po (650 mm) x 1,7 po (43,2 mm)	17,24 po (438 mm) x 24,41 po (620 mm) x 3,48 po (88,4mm)	17,24 po (438 mm) x 24,41 po (620 mm) x 3,48 po (88,4mm)	17,24 po (438 mm) x 24,41 po (620 mm) x 3,48 po (88,4mm)	17,2 po (437 mm) x 31,0 po (787 mm) x 3,5 po (89 mm)
Alimentatore CA	Singolo 250 watt, 90–264 VAC, 3,5–1,5 A, 50–60 Hz, ingresso IEC 60320-C14, interno, fisso	Ridondante (1+1) 750 watt, 100–240 VAC 8,0–4,5 A, 50–60 Hz, ingresso IEC 60320-C14, FRU	Ridondante (1+1) 800 watt, 100–240 VAC 10,5–4,0 A, 50–60 Hz, ingresso IEC 60320-C14, FRU	Ridondante (1+1) 800 watt, 100–240 VAC 10,5–4,0 A, 50–60 Hz, ingresso IEC 60320-C14, FRU	Ridondante (1+1) 800 watt, 100–240 VAC 10,5–4,0 A, 50–60 Hz, ingresso IEC 60320-C14, FRU	Ridondante (1+1) 1000 watt, 100-240 VAC 10,5 – 4,0 A, 50-60 Hz ingresso IEC 60320-C14, FRU

Tabella 1. Specifiche FireEye Network Security, appliance integrata. (continua)

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Consumo massimo (watt)	85 watt	265 watt	426 watt	519 watt	658 watt	660 watt
Dissipazione termica massima (BTU/h)	290 BTU/h	904 BTU/h	1.454 BTU/h	1.771 BTU/h	2.245 BTU/h	2.252 BTU/h
MTBF (h)	108.944 h	54.200 h	65.466 h	57.766 h	52.802 h	54.041 h
Peso sola appliance/con confezione, lb (kg)	16,2 lb (7,3 kg)/ 28,2 lb (12,79 kg)	29,8 lb (13,5 kg) / 40,8 lb (18,5 kg)	37,4 lb (17,0 kg) / 58,6 lb (26,6 kg)	42,4 lb (19,2 kg) / 63,5 lb (28,8 kg)	42,7 lb (19,2 kg) / 63,8 lb (29,0 kg)	44 lb (20 kg) 71 lb (32,2 kg)
Conformità alle normative sulla sicurezza	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
Certificazioni di sicurezza	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP vw1.1
Conformità normativa EMC	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	Sicurezza: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J60950, SI60950 EMC: FCC Part 15 SubPart B Class A; ICES-003; EN55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR32; KN 32; KN 35
Conformità ambientale	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	RoHS; REACH; minerali provenienti da aree di conflitto WEEE
Temperatura operativa	0–40 °C 32–104 °F	0–40 °C 32–104 °F	0–40 °C 32–104 °F	0–40 °C 32–104 °F	0–40 °C 32–104 °F	0–40 °C 32–104 °F
Temperatura non operativa	-20–80 °C -4–176 °F	-30–70 °C -22–158 °F	-40–70 °C -40–158 °F	-40–70 °C -40–158 °F	-40–70 °C -40–158 °F	-30–70 ºC -22–158 ºF
Umidità operativa relativa	5–85% a 40 °C senza condensa	10–95% a 40 °C, senza condensa	10–95% a 40 °C, senza condensa	10–95% a 40 °C, senza condensa	10–95% a 40 °C, senza condensa	10%–90% a 40 °C senza condensa
Umidità non operativa relativa	5–85% a 40 °C senza condensa	10–95% a 60 °C, senza condensa	10–95% a 60 °C, senza condensa	10–95% a 60 °C, senza condensa	10–95% a 60 °C, senza condensa	10%–95% a 55 ºC senza condensa
Altitudine operativa	3.000 m 9.842 piedi	3.000 m 9.842 piedi	3.000 m 9.842 piedi	3.000 m 9.842 piedi	3.000 m 9.842 piedi	3.000 m 9.842 piedi

Tabella 2. Prestazioni FireEye Network Security IPS, appliance integrata.

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Prestazioni IPS massime	Fino a 50 Mbit/s o 100 Mbit/s	Fino a 250 Mbit/s	Fino a 500 Mbit/s	Fino a 1 Gbit/s	Fino a 2,5 Gbit/s	Fino a 5 Gbit/s
Connessioni simultanee massime	15.000 o 80.000	80.000	160.000	500.000	1 milione	2 milioni
Nuove connessioni al secondo	750/sec o 4.000/sec	4.000/sec	8.000/sec	10.000/sec	20.000/sec	40.000/sec

Tabella 3. FireEye Network Security Smart Node, specifiche fisiche.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Sistema operativo supportato	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Prestazioni	Fino a 50 Mbit/s	Fino a 100 Mbit/s o 250 Mbit/s	Fino a 500 Mbit/s	Fino a 1 Gbit/s	Fino a 2 Gbit/s	Fino a 5 Gbit/s	Fino a 10Gbit/s
Porte per il monitoraggio della rete	4 porte 10/100/1000 BASE-T	4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	4x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 4x 1GigE Bypass	8x 10GigE SFP+ 2x 40GigE QSFP+
Modalità di funzionamento delle porte di rete	Monitoraggio in linea, fail-open, fail-close o Tap	Monitoraggio in linea, fail-open, fail-close (bypass HW) o TAP/SPAN	Monitoraggio in linea, fail-open, fail-close (bypass HW) o TAP/SPAN	Monitoraggio in linea, fail-open, fail-close (bypass HW) o TAP/SPAN	Monitoraggio in linea, fail-open, fail-close (bypass HW) o TAP/SPAN	Monitoraggio in linea, fail-open, fail-close (bypass HW) o TAP/SPAN	In linea, Monitoraggio, TAP/SPAN
Disponibilità elevata (HA)	Non disponibile	Non disponibile	Non disponibile	Non disponibile	Non disponibile	Non disponibile	Non disponibile
Porte di gestione (pannello posteriore)	2 porte 10/100/1000 BASE-T	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE	2x 1GigE
Porta IPMI	Non disponibile	Pannello anteriore	Pannello posteriore	Pannello posteriore	Pannello posteriore	Pannello posteriore	Pannello posteriore
LCD frontale e tastierino numerico	Non disponibile	Non disponibile	Non disponibile	Non disponibile	Non disponibile	Non disponibile	Non disponibile
Porta VGA	Non disponibile	Non disponibile	Sì	Sì	Sì	Sì	Sì
Porte USB	2 porte USB Tipo A	2 porte USB Tipo A (pannello anteriore)	4 porte USB Tipo A (tutte posteriori)	4 porte USB Tipo A 2 anteriori, 2 posteriori	4 porte USB Tipo A 2 anteriori, 2 posteriori	4 porte USB Tipo A 2 anteriori, 2 posteriori	2 porte USB Tipo A

Tabella 3. FireEye Network Security Smart Node, specifiche fisiche. (continua)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Porta seriale (pannello posteriore)	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop (connettore RJ45; il cavo adattatore RJ45-to-Dsub è incluso)	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop (connettore RJ45; il cavo adattatore RJ45-to-Dsub è incluso)	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop
Capacità unità	HDD singolo 500 GB 2,5 pollici SATA, interno, fisso	HDD singolo 1 TB 3,5 pollici SATA, interno, fisso	2 x 4 TB HDD, 3,5 po, SAS3, 7,2 krpm, FRU RAID1	2 x 4 TB HDD, 3,5 po, SAS3, 7,2 krpm, FRU RAID1	2 x 4 TB HDD, 3,5 po, SAS3, 7,2 krpm, FRU RAID1	2 x 4 TB HDD, 3,5 po, SAS3, 7,2 krpm, FRU RAID1	2x 10TB HDD 3,5 po, SAS3, 7,2 krpm FRU RAID1
Involucro	Fattore di forma desktop	1RU, Rack 19 pollici	1RU, Rack 19 pollici	2RU, Rack 19 pollici	2RU, Rack 19 pollici	2RU, Rack 19 pollici	2RU, Rack 19 pollici
Dimensioni chassis (LxPxA)	11 po (280 mm) x 6,9 po (175 mm) x 1,7 po (44 mm)	17,2 po (437 mm) x 19,7 po (500 mm) x 1,7 po (43,2 mm)	17,2 po (437 mm) x 25,6 po (650 mm) x 1,7 po (43,2 mm)	17,24 po (438 mm) x 24,41 po (620 mm) x 3,48 po (88,4 mm)	17,24 po (438 mm) x 24,41 po (620 mm) x 3,48” (88,4 mm)	17,24 po (438 mm) x 24,41 po (620 mm) x 3,48” (88,4 mm)	17,2 po (437 mm) x 31,0 po (787 mm) x 3,5 po (89 mm)
Alimentatore CA	Adattatore esterno AC 60 watt 12V@5A in uscita, 90–264 VAC, 50–60 Hz, ingresso IEC 60320-C14, FRU	Singolo 250 watt, 90–264 VAC, 3,5–1,5 A, 50–60 Hz, ingresso IEC 60320-C14, Interno, Fisso	Ridondante (1+1) 750 watt, 100–240 VAC, 9–4,5 A, 50–60 Hz, ingresso IEC 60320-C14 , FRU	Ridondante (1+1) 800 watt, 100–240 VAC, 9–4,5 A, 50–60 Hz, ingresso IEC 60320-C14 , FRU	Ridondante (1+1) 800 watt, 100–240 VAC, 9–4,5 A, 50–60 Hz, ingresso IEC 60320-C14 , FRU	Ridondante (1+1) 800 watt, 100–240 VAC, 10.5–4,0 A, 50–60 Hz, ingresso IEC 60320-C14, FRU	Ridondante (1+1) 1000 watt, 100–240 VAC, 10,5–4,0 A, 50–60 Hz ingresso IEC 60320-C14, FRU
Consumo massimo (watt)	24 watt	85 watt	265 watt	426 watt	519 watt	658 watt	660 watt
Dissipazione termica massima (BTU/h)	82 BTU/h	290 BTU/h	904 BTU/h	1.454 BTU/h	1.771 BTU/h	2.245 BTU/h	2.252 BTU/h
MTBF (h)	193.772 h	108.944 h	54.200 h	65.466 h	57.766 h	52.802 h	54.041 h
Peso sola appliance/con confezione, lb (kg)	3,75 lb (1,7 kg)/ 6,5 lb (2,95 kg)	16,2 lb (7,3 kg) / 28,2 lb (12,79 kg)	29,8 lb (13,5 kg)/ 40,8 lb (18,5 kg)	37,4 lb (17,0 kg)/ 58,6 lb (26,6 kg	42,4 lb (19,2 kg)/ 63,5 lb (28,8 kg)	42,7 lb (19,2 kg)/ 63,8 lb (29,0 kg)	44 lb (20 kg) 71 lb (32,2 kg)
Conformità alle normative sulla sicurezza	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
Certificazioni di sicurezza	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP v1.1	FIPS 140-2 Livello 1 CC NDPP v1.1

Tabella 3. FireEye Network Security Smart Node, specifiche fisiche. (continua)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Conformità normativa EMC	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	Sicurezza: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J60950, SI60950 EMC: FCC Part 15 SubPart B Class A; ICES-003; EN55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR32; KN 32; KN 35
Conformità ambientale	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	RoHS; REACH; minerali provenienti da aree di conflitto WEEE
Temperatura operativa	0–40 °C 32–104 °F	0–40 °C 32–104 °F	0–40 °C 32–104 °F	0–40 °C 32–104 °F	0–40 °C 32–104 °F	0–40 °C 32–104 °F	0–40 °C 32–104 °F
Temperatura non operativa	-20–80 °C -4–176 °F	-20–80 °C -4–176 °F	-30–70 °C (-22–158 °F)	-40–70 °C -40–158 °F	-40–70 °C -40–158 °F	-40–70 °C -40–158 °F	-30–70 °C -22–158 °F
Umidità operativa relativa	10–95% a 40 °C senza condensa	5–85% a 40 °C senza condensa	10–95% a 40 °C, senza condensa	10–95% a 40 °C, senza condensa	10–95% a 40 °C, senza condensa	10–95% a 40 °C, senza condensa	10%–90% a 40 °C senza condensa
Umidità non operativa relativa	10–95% a 60 °C senza condensa	5–95% a 40 °C senza condensa	10–95% a 60 °C, senza condensa	10–95% a 60 °C, senza condensa	10–95% a 60 °C senza condensa	10–95% a 60 °C senza condensa	10%–95% a 55 °C senza condensa
Altitudine operativa	3.000 m 9.842 piedi	3.000 m 9.842 piedi	3.000 m 9.842 piedi	3.000 m 9.842 piedi	3.000 m 9.842 piedi	3.000 m 9.842 piedi	3.000 m 9.842 piedi

Tabella 4. FireEye Network Security smart node IPS, specifiche fisiche.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Prestazioni IPS massime	Fino a 50 Mbit/s	Fino a 100/250 Mbit/s	Fino a 500 Mbit/s	Fino a 1 Gbit/s	Fino a 2 Gbit/s	Fino a 5 Gbit/s	Fino a 10 Gbit/s
Connessioni simultanee massime	15.000	80.000	160.000	500.000	1 milione	2 milioni	4 milioni
Nuove connessioni al secondo	750/sec	4.000/sec	8.000/sec	10.000/sec	20.000/sec	40.000/sec	80.000/sec

Tabella 5. FireEye Network Security smart node, specifiche virtuali.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Sistema operativo supportato	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Prestazioni*	Fino a 50 Mbit/s	Fino a 100 Mbit/s	Fino a 250 Mbit/s	Fino a 500 Mbit/s	Fino a 1 Gbit/s
Porte per il monitoraggio della rete	1–8	1–8	1–8	1–8	1–8
Porte per la gestione della rete	1 o 2	1 o 2	1 o 2	1 o 2	1 o 2
Modalità di funzionamento delle porte di rete	In linea, SPAN	In linea, SPAN	In linea, SPAN	In linea, SPAN	In linea, SPAN
CPU Cores	3	6	8	8	16
Memoria	10 GB	16 GB	16 GB	32 GB	32 GB
Capacità unità	384 GB	384 GB	384 GB	512 GB	512 GB
Adattatori di rete	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC
Supporto Hypervisor	VMWare ESXi6.0 o versione successiva e KVM 1.5.3 o versione successiva	VMWare ESXi6.0 o versione successiva e KVM 1.5.3 o versione successiva	VMWare ESXi6.0 o versione successiva e KVM 1.5.3 o versione successiva	VMWare ESXi6.0 o versione successiva e KVM 1.5.3 o versione successiva	VMWare ESXi6.0 o versione successiva e KVM 1.5.3 o versione successiva
Certificazioni di sicurezza	FIPS 140-2 Livello 1 CC NDPP v1.1 (In corso)	FIPS 140-2 Livello 1 CC NDPP v1.1 (In corso)	FIPS 140-2 Livello 1 CC NDPP v1.1 (In corso)	FIPS 140-2 Livello 1 CC NDPP v1.1 (In corso)	FIPS 140-2 Livello 1 CC NDPP v1.1 (In corso)

Tabella 6. FireEye Network Security smart node IPS, specifiche virtuali.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Prestazioni IPS massime	Fino a 50 Mbit/s	Fino a 100 Mbit/s	Fino a 250 Mbit/s	Fino a 500 Mbit/s	Fino a 1 Gbit/s
Connessioni simultanee massime	15.000	80.000	80.000	160.000	500.000
Nuove connessioni al secondo	750/sec	4.000/sec	4.000/sec	8.000/sec	10.000/sec

Tabella 7. Dimensioni delle AMI supportate da FireEye Network Security su AWS.

Modello	Throughput	vCPU	Memoria	Disco	Interfacce di rete	Tipo di istanza AWS
NX4500v	500 Mbit/s	8	32 GB	512 GB (EBS)	Una porta di gestione, una porta di invio e due porte di monitoraggio (per un totale di 4 porte)	M5.2xlarge
NX6500v	1 Gbit/s	16	64 GB	512 GB (EBS)	Una porta di gestione, una porta di invio e sei porte di monitoraggio (per un totale di 8 porte)	M5.4xlarge

Tabella 8. Specifiche FireEye MVX Smart Grid.

	VX 5500	VX 12550
Sistema operativo supportato	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
Prestazioni*	Fino a 2 Gbit/s	Fino a 14 Gbit/s
Disponibilità elevata**	N+1	N+1
Porte di gestione (pannello posteriore)	1 porta 10/100/1000 Mbit/s BASE-T	1 porta 10/100/1000 Mbit/s BASE-T
Porte cluster (pannello posteriore)	3 porte 10/100/1000 Mbit/s BASE-T	1 porta 10/100/1000 Mbit/s BASE-T, 2 porte 10 Gbit/s BASE-T, 4 porte 10 GigE SFP
Porta IPMI (pannello posteriore)	Incluso	Incluso
LCD frontale e tastierino numerico	Non disponibile	LCD non incluso
Porte VGA	Incluso	Incluso
Porte USB (pannello posteriore)	4 porte USB Tipo A	2 porte USB Tipo A
Porta seriale (pannello posteriore)	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop
Capacità unità	2 unità HDD 2TB 3,5 pollici SAS3, RAID 1, collegabile a caldo, FRU	2 unità HDD 4TB 3,5 pollici SAS3, RAID 1, collegabile a caldo, FRU
Involucro	1RU, Rack 19 pollici	2RU, Rack 19 pollici
Dimensioni chassis (LxPxA)	17,2 x 25,6 x 1,7 po (437 x 650 x 43,2 mm)	17.2 x 31 x 3.5 po (437 x 787 x 89 mm)
Alimentatore CC	Non disponibile	Non disponibile
Alimentatore CA	Ridondante (1+1) 750 watt, 100–240 VAC, 8 - 3,8 A, 50–60 Hz, ingresso IEC 60320-C14, collegabile a caldo, FRU	Ridondante (1+1) 1000 watt, 100–240 VAC 10,5–4,0 A 50-60 Hz ingresso IEC 60320-C14, FRU
Consumo massimo (watt)	285 watt	660 watt
Dissipazione termica massima (BTU/h)	972 BTU/h	2594 BTU/h
MTBF (h)	54.200 h	54.041 h
Peso sola appliance/con confezione, lb (kg)	27,0 lb (12,2 kg)/38,0 lb (17,2 kg)	44 lb (20 kg)/71 lb (32,2 kg)
Certificazione di sicurezza	FIPS 140-2 Livello 1, CC NDPP v1.1 (in attesa)	FIPS 140-2 Livello 1, CC NDPP v1.1 (in attesa)
Conformità alle normative sulla sicurezza	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

Tabella 9. Specifiche FireEye MVX Smart Grid.

	VX 5500	VX 12500
Conformità normativa EMC	FCC Parte 15 ICES-003 Classe 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 e V-3/2015	FCC Parte 15 ICES-003 Classe 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 e V-3/2015
Conformità ambientale	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE REACH Direttiva RAEE 2012/19/UE
Temperatura operativa	0–40 °C (32–104 °F)	0–40 °C (32–104 °F)
Temperatura non operativa	-30–70 °C (-22–158 °F)	-30–70 °C (-22–158 °F)
Umidità operativa relativa	10–95% a 40 °C senza condensa	10–90% a 40 °C senza condensa
Umidità non operativa relativa	10–95% a 60 °C senza condensa	10–95% a 55 °C senza condensa
Altitudine operativa	3.000 m 9.842 piedi	3.000 m 9.842 piedi

Servizi di supporto

FireEye offre programmi di supporto semplici e flessibili per massimizzare il valore dei vostri prodotti e servizi FireEye. Sono disponibili quattro diversi livelli di servizi di supporto: Platinum, Platinum Priority Plus, Government e Government Priority Plus. Per ulteriori informazioni sui programmi di supporto FireEye, fate riferimento ai servizi FireEye Support.

Per ulteriori informazioni su FireEye, visita il sito Web **www.FireEye.com**

FireEye Italia Srl
Piazza IV Novembre, 7 20124 Milano
+39 0294750535
italy@FireEye.com

Informazioni su FireEye, Inc

FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Operando come estensione intuitiva e scalabile dei processi operativi di sicurezza dei clienti, FireEye offre un'unica piattaforma in grado di coniugare tecnologie di sicurezza innovative, intelligence sulle minacce a livello nazionale e servizi di consulenza Mandiant® di fama mondiale. Grazie a questo approccio, FireEye elimina la complessità e l'onere della sicurezza informatica per le aziende che hanno difficoltà a prepararsi per futuri attacchi, prevenirli e rispondere ad essi.