DATA SHEET

FireEye Network Security

Effective protection against cyber breaches for midsize to large organizations

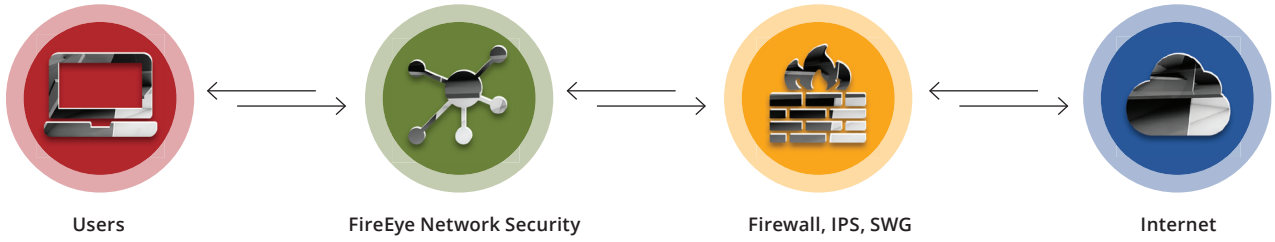
Przegląd

FireEye Network Security to kompleksowe rozwiązanie, które minimalizuje ryzyko włamań do wnętrza sieci organizacji, dzięki precyzyjnemu wykrywaniu i zatrzymywaniu zaawansowanych cyberataków. Podstawą rozwiązania Network Security jest dedykowany hypervisor FireEye MVX (Multi-Vector Virtual ExecutionTM) wraz z technologią inteligentnej analizy (IDA Intelligence – Driven Analysis). MVX analizuje ruch sieciowy w izolowanych środowiskach wirtualnych, w celu wykrycia podatności (exploits) zarówno znanych jak i „zero-day", plików wykonywalnych złośliwego oprogramowania oraz prób nawiązania połączeń zwrotnych (callbacks). IDA jest natomiast silnikiem dynamicznych zasad, które w oparciu o kontekst zdarzenia wykrywają i blokują złośliwe zachowania w czasie rzeczywistym i wstecz.

FireEye Network Security zawiera również tradycyjny silnik IPS (Intrusion Prevention System), który wykrywa typowe ataki korzystając z sygnatur. Wygenerowane alerty zawierają szczegóły analizy dynamicznej, oraz informacje o kontekście ataku (threat intelligence), co pozwala na ustalanie priorytetów reakcji na zagrożenie oraz szybką izolację intruza.

FireEye Network Security można wdrażać na wiele sposobów (hardware/ VMs / Cloud), jest dostępny w wielu wersjach wydajności i jest najczęściej umieszczany w ścieżce ruchu, zaraz za tradycyjnymi rozwiązaniami do zabezpieczania styku z siecią takimi, jak Firewall, IPS, Web Gateway. W uzupełnieniu do używanych systemów, rozwiązanie FireEye Network Security wykrywa zarówno znane, jak i nieznane ataki z dużą dokładnością i jednocześnie generuje niewielkie ilości fałszywych zdarzeń.

Rys 1. Typowa konfiguracja



Przewagi Technologiczne:

Precyzyjne wykrywanie zaawansowanych zagrożeń

Fireeye Network Security wykorzystuje różne metody analizy, aby wykrywać zarówno znane, jak i nieznane ataki z dużą dokładnością i jednocześnie generuje niewielkie ilości fałszywych zdarzeń.

- **Multi-Vector Virtual Execution™ (MVX)** w czasie rzeczywistym analizuje podejrzane pliki binarne i obiekty WWW z użyciem różnych wersji przeglądarek, wtyczek, aplikacji i środowisk operacyjnych pod kątem identyfikacji prób wykorzystania ich podatności, ataków na pamięć operacyjną, czy prób nawiązania połączeń zwrotnych.

  Dzięki takiemu podejściu hypervisor MVX może automatycznie wykrywać zarówno istniejące, jak również nieznane wcześniej podatności (exploits) i szkodliwe oprogramowanie w środowiskach heterogenicznych z wieloma typami urządzeń końcowych. Po wykryciu ataku silnik MVX na podstawie zidentyfikowanych połączeń callback, dynamicznie tworzy reguły ich blokowania i współdzieli informacje o szczegółach ataku z innymi urządzeniami FireEye, połączonymi do chmury FireEye DTI (Dynamic Threat Intelligence). Te informacje pozwalają wszystkim innym sensorom FireEye natychmiast wdrożyć reguły blokowania dla nieznanych ataków.

  Analiza FireEye MVX jest uzupełniana algorytmami analizy wielkich zbiorów danych (Big Data) i uczenia maszynowego, które przetwarzają dane z FireEye DTI, korelujące z podobnymi, starszymi i najnowszymi próbkami szkodliwego oprogramowania z laboratoriów FireEye tak, aby również przewidywać i zapobiegać przyszłym atakom. Podobnie informacje o nowych technikach ataków, zidentyfikowanych przez zespół Mandiant Incident Response, są automatycznie dostarczane do urządzeń FireEye na całym świecie za pośrednictwem chmury DTI już w ciągu kilku minut po początkowym wykryciu.

- **Intelligence-Driven Analysis (IDA)**
  Silnik IDA w czasie rzeczywistym wykrywają i blokują ataki celowane, ukrywane i szyte na miarę ofiary, korzystając z kontekstowej analizy zachowań i zasad w oparciu o wiedzę z milionów werdyktów MVX, tysięcy godzin doświadczenia zbieranego w trakcie świadczenia usług Incident Response przez Mandiant i setek analityków iSight zajmujących się zbieraniem informacji i analizą zagrożeń. IDA przerywa cykl życia ataku w momencie infekcji (poprzez wykrycie złośliwego exploitu), kompromitacji (poprzez wykrycie malware'u) i włamania (poprzez wykrycie połączeń callback do serwerów hakera – C&C Command and Control Center). Dodatkowo IDA wysyła podejrzany ruch sieciowy do silnika MVX w celu uzyskania ostatecznego werdyktu po analizie dynamicznej.

- **Structured Threat Intelligence eXpression** pozwala na wykorzystanie zewnętrznych źródeł wiedzy, dostarczanych przez innych producentów i jednostki badawcze korzystające z formatów będących standardem rynkowym, w celu dodania własnych reguł i wskaźników zagrożeń do silnika IDA.

Wszechstronna ochrona w czasie rzeczywistym

FireEye Network Security obsługuje najczęściej spotykane oraz najnowsze wersje systemów Microsoft Windows i Apple Mac OS X i umożliwia elastyczne tryby wdrożenia:

- analiza kopii ruchu sieciowego tzw. TAP/SPAN, monitorowanie lub aktywne blokowanie połączeń w trybie inline. Urządzenie można wdrożyć bezpośrednio w punktach styku z Internetem, aby automatycznie blokować wykryte ataki w ruchu webowym, szkodliwe oprogramowanie i próby zestawiania połączeń callback.

  W trybie monitorowania FireEye NX generuje alerty i pozostawia administratorowi decyzję o sposobie odpowiedzi na atak. W trybie analizy kopii ruchu TAP/SPAN urządzenie FireEye NX Power może wysyłać polecenia resetowania połączeń TCP/UDP.

- Aby zapewnić organizacji zarówno odpowiednie bezpieczeństwo jak również ciągłość działania, FireEye Network Security obsługuje integrację z modułami FireEye Active Fail Open (AFO) zapewniając ciągłą dostępność sieci w trybie pracy Inline w przypadku awarii zasilania lub łącza między AFO a urządzeniem FireEye NX.

Pełny przegląd ataków w organizacji

FireEye Network Security dostarcza stały poziom ochrony niezależnie od skomplikowania i zróżnicowania dzisiejszych środowisk sieciowych:

- Wspiera najpopularniejsze wersje systemów operacyjnych Microsoft Windows i Apple MAC OS.

- Analizuje ponad 140 różnych typów plików włączając w to portable executables (PEs), treści w ruchu webowym, archiwa, obrazy, JAVA, oraz aplikacje i multimedia Microsoft i Adobe.

- Detonuje podejrzany ruch sieciowy poprzez przekrój tysięcy kombinacji wersji systemów operacyjnych, service pack'ów, typów aplikacji i wersji aplikacji.

Zautomatyzowana redukcja nieistotnych alertów

FireEye Network Security automatycznie kwalifikuje i potwierdza podejrzane alerty IPS, co zmniejsza nakład pracy związany z ich analizą. Alerty IPS o potwierdzonej szkodliwości są wyraźnie oznaczone w konsoli zarządzającej. Ten proces weryfikacji dla modułu IPS znacząco zmniejsza liczbę fałszywych alertów i pozwala nadać właściwy priorytet tylko rzeczywistym zagrożeniom, ukrytym wśród tysięcy innych incydentów pochodzących z tradycyjnego IPS – bardzo często fałszywych lub zduplikowanych.

FireEye Network Security kategoryzuje także potencjalnie ryzykowne oprogramowanie — niepożądane obiekty, które nie muszą w każdym wypadku prowadzić do naruszenia zabezpieczeń - na przykład adware lub PUP (Potentially Unwanted Program). Mechanizm potwierdzania alertów IPS oraz klasyfikowanie oprogramowania typu „riskware" efektywnie wspiera zespoły ds. zabezpieczeń i pozwala skupić się na walce z prawdziwymi zagrożeniami, minimalizując ryzyko biznesowe i nakłady operacyjne.

Praktyczna analiza kontekstowa

Alerty wygenerowane przez FireEye Network Security dostarczają również danych do analizy kontekstowej ataku, pozwalając szybko reagować na alerty, ustalać priorytety obsługi i izolować zagrożenia. Analiza kontekstowa łączy ponad 10-letnie doświadczenie FireEye w wykrywaniu i analizie najpoważniejszych cyberataków, globalną sieć składającą się z ponad 10 milionów urządzeń FireEye na świecie oraz wiedzę zespołu doświadczonych analityków, badaczy i ekspertów. Informacje o kontekście wykrytych zagrożeń pomagają w szybkiej i efektywnej odpowiedzi na incydent.

Zintegrowanie reakcji na incydenty

Fireeye Network Security może być rozbudowany na kilka sposobów w celu automatyzacji i zintegrowania reakcji na incydenty:

- Fireeye Central Management koreluje alerty zarówno z Fireeye Network Security i Fireeye Email Security dla szerszego spojrzenia na zakres ataku i w celu uruchomienia zasad zapobiegających dalszemu rozprzestrzenianiu się infekcji.
- Fireeye Network Forensics integruje się z Fireye Network Security, dodając szczegółową analizę pakietów powiązanych z alertem i umożliwia pogłębioną analizę zdarzeń.
- Fireeye Endpoint Security identyfikuje i weryfikuje na poziomie stacji końcowej włamania wykryte przez Fireeye Network Security i zabezpiecza skompromitowane hosty, upraszczając procedurę wykrycia i reakcji na Endpointach skompromitowanych przez atak.

Łatwość wdrażania i zarządzania

FireEye Network Security to łatwa w zarządzaniu platforma sieciowa, którą można wdrożyćw czasie krótszym niż 60 minut. Nie wymaga konfigurowania dodatkowych reguł, polityk i strojenia oraz integruje się z innymi produktami bezpieczeństwa za pośrednictwem interfejsu REST/JSON API. Ponadto FireEye Network Security jest ściśle zintegrowany z innymi urządzeniami FireEye za pośrednictwem systemu centralnego zarządzania CM. Zautomatyzowane działanie, niski współczynnik fałszywych alertów i funkcja podtrzymania połączeń sieciowych w przypadku awarii urządzenia zmniejsza zaangażowanie personelu administracyjnego, czasy przestoju i całkowity koszt użytkowania produktu.

Opcje wdrożenia:

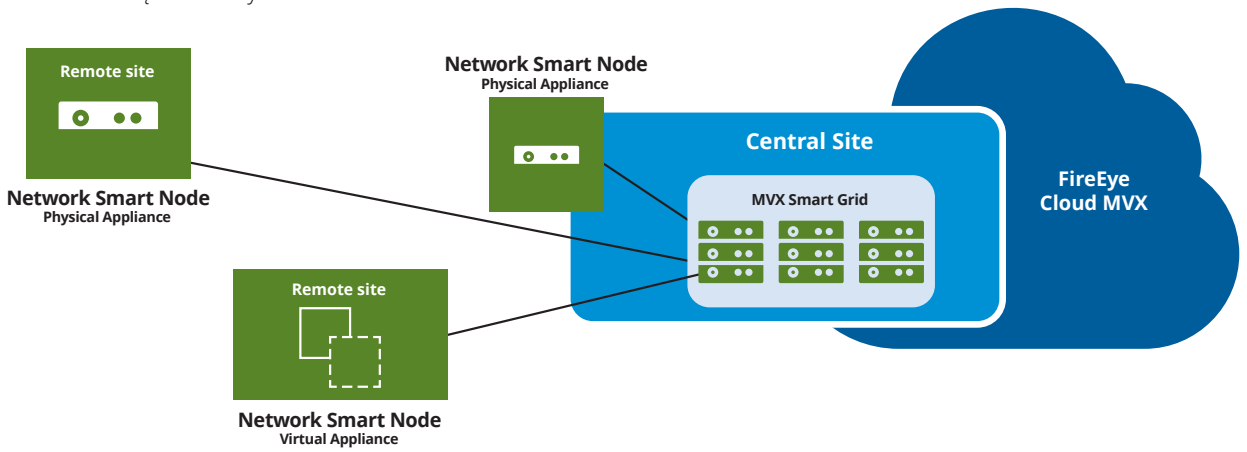
- **Integrated Network Security:** Urządzenie All-in-one (hardware) zawierające lokalny silnik MVX, aby zapewnić bezpieczeństwo styku z siecią w pojedynczej lokalizacji.
- **Distributed Network Security:** Urządzenia fizyczne i wirtualne, z centralnie współdzielonym silnikiem MVX, zabezpieczające wszystkie punkty styku z internetem w lokalizacji. Możliwe elementy wdrożenia:

  - **Network Smart Node:** Urządzenie fizyczne lub wirtualny appliance, który analizuje ruch sieciowy, w celu wykrycia i zablokowania złośliwego ruchu oraz przekazania podejrzanej kopii aktywności poprzez zaszyfrowany kanał do zewnętrznego silnika MVX, w celu ostatecznego werdyktu.

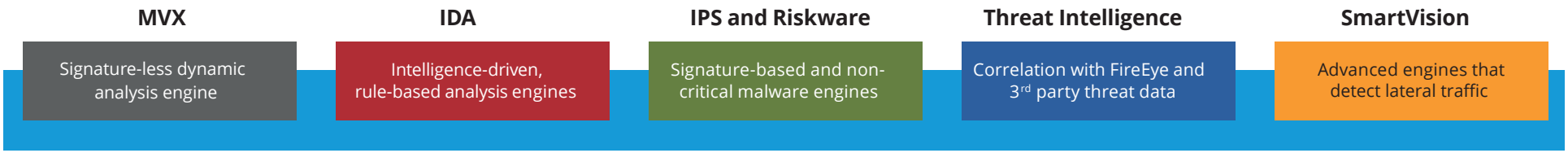
  - **MVX Smart Grid:** Urządzenie fizyczne z lokalnym silnikiem MVX, oferujące skalowalność infrastruktury Network Security z wbudowanym mechanizmem tolerancji uszkodzeń N+1 i automatycznym load balancingiem.

  - **FireEye Cloud MVX:** Zewnętrzny silnik MVX, umiejscowiony w data center Fireeye, dostępny jako subskrypcja. Analiza ruchu w celu zachowania prywatności odbywa się na Fireeye Smart Node, jedynie podejrzane obiekty są wysyłane zaszyfrowanym kanałem do Cloud MVX. Obiekty zakwalifikowane jako nieszkodliwe są automatycznie usuwane.

Rys. 2 Komponenty Fireeye Network Security: NX 2550, NX 3500, NX 5500, NX 6500.



Rys. 3 Model wdrożenia Distributed Network Security



Rys. 4 Modular components of FireEye Network Security.

Korzyści:
Niezależnie od modelu wdrożenia, FireEye Network Security daje poniższe korzyści:

Zminimalizowanie ryzyka włamania do infrastruktury IT.

FireEye Network Security to wysokowydajne rozwiązanie zapewniające cyberbezpieczeństwo:

- Zapobiega kradzieży istotnych danych i zakłóceniom działania organizacji, chroniąc przed zaawansowanymi i celowanymi atakami, mającymi na celu niewykryte obejście istniejących zabezpieczeń.
- Zatrzymuje ataki i ogranicza zasięg infekcji/włamania szybciej, zapewniając konkretne dowody, blokując ruch, usprawniając metody reakcji na incydent i dostarczając informacje, w oparciu o które można podjąć szybkie działania zapobiegawcze.
- Eliminuje słabe punkty w obecnej strukturze cyber-bezpieczeństwa organizacji, zapewniając stały poziom ochrony dla różnorakich systemów operacyjnych, typów aplikacji w sieci centralnej oraz w zewnętrznych lokalizacjach

Szybki zwrot z inwestycji.

Według opracowania Forrester Consulting[1], Klienci FireEye Network Security mogą spodziewać się oszczędności na poziomie 152% ROI w przeciągu trzech lat i zwrotu z wstępnej inwestycji już po 9,7 miesiąca.

FireEye Network Security:

- Skupia zasoby zespołu ds. cyberbezpieczeństwa na faktycznych atakach, zmniejszając koszty operacyjne.
- Optymalizuje koszt inwestycji za pomocą współdzielonego silnika MVX i różnych modeli wdrożenia oraz elastycznemu wymiarowaniu rozwiązania.
- Zabezpiecza optymalizacje przyszłych inwestycji, łatwo skalując się w przypadku rozwoju infrastruktury o kolejne zewnętrzne lokalizacje, punkty styku z Internetem i wzrost przepustowości sieci.
- Chroni pierwotne inwestycje, zapewniając bezpłatną migrację z trybu Integrated do Distributed.

Nagrody i certyfikacje

Produkty FireEye Network Security były wielokrotnie wyróżniane nagrodami branżowymi i rządowymi, oraz certyfikowane m.in.:

- w ramach US Department of Homeland Security Safety Act.
- W 2016 Frost & Sullivan określił FireEye jako niekwestionowanego lidera z 56% udziałem w rynku Network Security Sandbox[2]
- różne nagrody z: SANS institute, SC Magazine, CRN i inni

1 Forrester (May 2016). The Total Economic Impact of FireEye.
2 Frost & Sullivan (October 2016). Network Security Sandbox Market Analysis

Tabela 1. Specyfikacja techniczna:

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
OS Support	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
Performance *	Up to 50 Mbps or 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2.5 Gbps	Up to 5 Gbps
Network Monitoring Ports	4x 10/100/1000 BASE-T Ports (in front panel)	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 1GigE/10GigE SFP+ 2x 40GigE QSFP+
Network Ports Mode of Operation	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line, Monitor,TAP/SPAN
High Availability (HA)	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
High Availability (HA) Ports (rear panel)	Not Available	Not Available	Not Available	Not Available	2x 100/1000/10G Base-T Ports	Not Available
Management Ports (rear panel)	2x 10/100/1000 BASE- T Ports (in front panel)	2x 10/100/1000 BASE- T Ports	2x 10/100/1000 BASE- T Ports	2x 10/100/1000 BASE- T Ports	2x 10/100/1000 BASE- T Ports	4x 1000BaseT Ports
IPMI Port (rear panel)	Included	Included	Included	Included	Included	Included
Front LCD & Keypad	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
VGA Port	No	Yes	Yes	Yes	Yes	Yes
USB Ports	2x Type A USB Ports (front panel)	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	2x Type 3 USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 bits, 1 Stop Bit (RJ45 connector RJ45-to-Dsub adapter cable is included)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115200 bps, No Parity, 8 bits, 1 Stop Bit
Drive Capacity	Single 1TB 3.5 inch, SATA HDD, internal, fixed	2 x 4TB HDD, 3.5”, SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5”, SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5”, SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5”, SAS3, 7.2krpm, FRU RAID1	2x 10TB HDD 3.5”, SAS3, 7.2krpm FRU RAID1
Enclosure	1RU, Fits 19 inch Rack	1RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19 inch Rack
Chassis Dimension WxDxH	17.2in(437mm) x 19.7in(500mm) x 1.7in(43.2 mm)	17.2in(437mm) x 25.6in(650mm) x 1.7in(43.2mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in (88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.2”(437mm) x 31.0”(787mm) x 3.5”(89mm)
AC Power Supply	Single 250 watt, 90-264 VAC, 3.5 - 1.5 A, 50-60 Hz, IEC60320-C14, inlet, Internal, Fixed	Redundant (1+1) 750 watt, 100 - 240 VAC 9.0 - 4.5A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 – 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 – 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 – 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 1000 watt, 100 - 240 VAC 10.5 – 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU

Tabela 1. Specyfikacja techniczna:

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Power Consumption Maximum (watts)	85 watts	265 watts	426 watts	519 watts	658 watts	660 watts
Thermal Dissipation Maximum (BTU/h)	290 BTU/h	904 BTU/h	1,454 BTU/hr	1,771 BTU/h	2,245 BTU/h	2,252 BTU/h
MTBF (h)	56,400 h	54,200 h	65,466 h	57,766 h	52,802 h	54,041 h
Appliance Alone / As Shipped Weight lb. (kg)	16.2 lb (7.3 kg) / 28.2 lb (12.79 kg)	29.8 lbs (13.5 Kg) / 40.8 lbs (18.5 Kg)	37.4 lbs (17.0 Kg) / 58.6 lbs (26.6 kg)	42.4 lbs (19.2 Kg) / 63.5 lbs (28.8 kg)	42.7 lbs (19.2 Kg) / 63.8 lbs (29.0 kg)	44 lbs (20 kgs) 71 lbs (32.2Kg)
Regulatory Compliance Safety	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
Security Certifications	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 vw1.1
Regulatory Compliance EMC	FCC Part 15 ICES-003 Class 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 &V-3/2015	FCC Part 15 ICES-003 Class 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 &V-3/2015	FCC Part 15 ICES-003 Class 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 &V-3/2015	FCC Part 15 ICES-003 Class 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 &V-3/2015	FCC Part 15 ICES-003 Class 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 &V-3/2015	Safety: 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
Environmental Compliance	RoHS Directive 2011/65/ EU REACH WEEE Directive 2012/19/ EU	RoHS Directive 2011/65/ EU REACH WEEE Directive 2012/19/ EU	RoHS Directive 2011/65/ EU REACH WEEE Directive 2012/19/ EU	RoHS Directive 2011/65/ EU REACH WEEE Directive 2012/19/ EU	RoHS Directive 2011/65/ EU REACH WEEE Directive 2012/19/ EU	RoHS; REACH; WEEE Conflict Minerals
Operating Temperature	0 ~ 40°C 32 ~ 104°F	0 ~ 35°C 32 ~ 95°F	0 ~ 35°C 32 ~ 95°F	0 ~ 35°C 32 ~ 95°F	0 ~ 35°C 32 ~ 95°F	10° C to 35° C Tested from 0°C to 40°C for additional margin
Non-Operating Temperature	-20 ~ 80°C -4 ~ 176°F	-40 ~ 70°C -40 ~ 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
Operating Relative Humidity	5% - 85% non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10% - 90%@40°C non-condensing
Non-Operating Relative Humidity	5% - 95% non-condensing	10 ~ 95% @ 60° C, non-condensing	10 ~ 95% @ 60° C, non-condensing	10 ~ 95% @ 60° C, non-condensing	10 ~ 95% @ 60° C, non-condensing	10% - 95%@55°C non-condensating
Operating Altitude	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft

Tabela 2. FireEye Network Security IPS performance, integrated appliance.

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Max IPS Performance	Up to 50 Mbps or 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2.5 Gbps	Up to 5 Gbps
Max Concurrent Connections	15K or 80K	80K	160K	500K	1M	2M
New Connections Per Second	750/Sec or 4K/Sec	4K/Sec	8K/Sec	10K/Sec	20K/Sec	40K/Sec

Tabela 3. FireEye Network Security smart node, physical specifications.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
OS Support	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
Performance	Up to 50 Mbps	Up to 100 Mbps or 250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2 Gbps	Up to 5 Gbps	Up to 10Gbps
Network Monitoring Ports	4x 10/100/1000 BASE-T Ports	4x 10/100/1000 BASE-T Ports (in front panel)	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 1GigE/10GigE SFP+ 2x 40GigE QSFP+
Network Ports Mode of Operation	In-line Monitor, Fail-Close or Tap	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line Monitor, Fail-Open, Fail- Close (HW Bypass) or TAP/SPAN	In-line, Monitor,TAP/ SPAN
High Availability (HA)	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
High Availability (HA) Ports (rear panel)	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
Management Ports (rear panel)	2x 10/100/1000 BASE- T Ports	4x 10/100/1000 BASE- T Ports (in front panel)	2x 10/100/1000 BASE- T Ports	2x 10/100/1000 BASE- T Ports	2x 10/100/1000 BASE- T Ports	2x 10/100/1000 BASE- T Ports	4x 1000 BaseT Ports
IPMI Port (rear panel)	Not Available	Rear Panel	Included	Included	Included	Included	Included
Front LCD & Keypad	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available	Not Available
VGA Port	Not Available	Not Available	Yes	Yes	Yes	Yes	Yes
USB Ports	2x Type A USB Ports	2x Type A USB Ports (front panel)	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	4x Type A USB Ports 2 front, 2 rear	2x Type 3 USB Ports

Tabela 3. FireEye Network Security smart node, physical specifications. (continued)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Serial Port (rear panel)	115,200 bps, No Parity, 8 bits, 1 Stop Bit (RJ45 connector; RJ45-to-Dsub adapter cable is included)	115,200 bps, No Parity, 8 bits, 1 Stop Bit (RJ45 connector RJ45-to-Dsub adapter cable is included)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115200 bps, No Parity, 8 bits, 1 Stop Bit
Drive Capacity	Single 500GB 2.5 inch SATA HDD, internal, fixed	Single 1TB 3.5 inch SATA HDD, internal, fixed	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2 x 4TB HDD, 3.5", SAS3, 7.2krpm, FRU RAID1	2x 10TB HDD 3.5", SAS3, 7.2krpm FRU RAID1
Enclosure	Desktop formfactor	1RU, Fits 19 inch Rack	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis Dimension WxDxH	11in(280mm) x 6.9in(175mm) x 1.8in(45.7mm)	17.2in(437mm) x 19.7in(500mm) x 1.7in(43.2mm)	17.2in(437mm) x 25.6in(650mm) x 1.7in(43.2mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in (88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.24in(438mm) x 24.41in(620mm) x 3.48in(88.4mm)	17.2in(437mm) x 27.9in(709mm) x 3.5in(89 mm)
AC Power Supply	External 60 Watt 12V@5A Ouput AC Adapter, 90-264 VAC, 50-60 Hz, IEC60320-C14, inlet, FRU	Single 250 watt, 90-264 VAC, 3.5 - 1.5 A, 50-60 Hz, IEC60320-C14, inlet, Internal, Fixed	Redundant (1+1) 750 watt, 100 - 240 VAC 9 – 4.5A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC 9 – 4.5A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC 9 – 4.5A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 – 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU	Redundant (1+1) 1000 watt, 100 - 240 VAC 10.5 – 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU
Power Consumption Maximum (watts)	27 watts	85 watts	265 watts	426 watts	519 watts	658 watts	660 watts
Thermal Dissipation Maximum (BTU/h)	92 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)	95,400 h	56,400 h	54,200 h	65,466 h	57,766 h	52,802 h	54,041 h
Appliance Alone / As Shipped Weight 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 lbs (13.5 kg) / 40.8 lbs (18.5 Kg)	37.4 lbs (17.0 kg) / 58.6 lbs (26.6 kg	42.4 lbs (19.2 kg) / 63.5 lbs (28.8 kg)	42.7 lbs (19.2 kg) / 63.8 lbs (29.0 kg)	44 lbs (20 kgs) 71 lbs (32.2 Kg)
Regulatory Compliance Safety	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
Security Certifications	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

Tabela 3. FireEye Network Security smart node, physical specifications. (continued)

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Regulatory Compliance EMC	FCC Part 15 ICES-003 Class 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 &V-3/2015	FCC Part 15 ICES-003 Class 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 &V-3/2015	FCC Part 15 ICES-003 Class 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 &V-3/2015	FCC Part 15 ICES-003 Class 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 &V-3/2015	FCC Part 15 ICES-003 Class 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 &V-3/2015	FCC Part 15 ICES-003 Class 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 &V-3/2015	Safety: 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
Environmental Compliance	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS; REACH; WEEE Conflict Minerals
Operating Temperature	0 ~ 40°C 32 ~ 104°F	0 ~ 40°C 32 ~ 104°F	0 ~ 35°C 32 ~ 95°F	0 ~ 35°C 32 ~ 95°F	0 ~ 35°C 32 ~ 95°F	0 ~ 35°C 32 ~ 95°F	10° C to 35° C Tested from 0°C to 40°C for additional margin
Non-Operating Temperature	-20 ~ 80°C -4 ~ 176°F	-20 ~ 80°C -4 ~ 176°F	-40 ~ 70°C -40 ~ 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
Operating Relative Humidity	5% - 85% non-condensing	5% - 85% non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10% - 90%@40°C non-condensing
Non-Operating Relative Humidity	5% - 95% non-condensing	5% - 95% non-condensing	10 ~ 95% @ 60° C, non-condensing	10 ~ 95% @ 60° C, non-condensing	10 ~ 95% @ 60° C non-condensing	10 ~ 95% @ 60° C non-condensing	10% - 95%@55°C non-condensating
Operating Altitude	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft	3,000 m 9,842 ft

Tabela 4. FireEye Network smart node IPS, physical specifications.

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
Max IPS Performance	Up to 50 Mbps	Up to 100 /250 Mbps	Up to 500 Mbps	Up to 1 Gbps	Up to 2 Gbps	Up to 5 Gbps	Up to 10 Gbps
Max Concurrent Connections	15K	80K	160K	500K	1M	2M	4M
New Connections Per Second	750/sec	4K/Sec	8K/Sec	10K/Sec	20K/sec	40K/Sec	80K/Sec

Tabela 5. FireEye Network smart node, virtual specifications.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
OS Support	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
Performance *	Up to 50 Mbps	Up to 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps
Network Monitoring Ports	1-8	1-8	1-8	1-8	1-8
Network Management Ports	1 or 2	1 or 2	1 or 2	1 or 2	1 or 2
Network Ports Mode of Operation	Inline, SPAN	Inline, SPAN	Inline, SPAN	Inline, SPAN	Inline, SPAN
CPU Cores	3	6	8	8	16
Memory	10GB	16GB	16GB	32 GB	32 GB
Drive Capacity	384 GB	384 GB	384 GB	512 GB	512 GB
Network Adapters	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC	VMXNet 3, vNIC
Hypervisor Support	VMWare ESXi 6.0 or later	VMWare ESXi 6.0 or later	VMWare ESXi 6.0 or later	VMWare ESXi 6.0 or later	VMWare ESXi 6.0 or later
Security Certifications	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)	FIPS 140-2 Level 1 CC NDPP v1.1 (In Process)

Tabela 6. FireEye Network smart node IPS, virtual specifications.

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
Max IPS Performance	Up to 50 Mbps	Up to 100 Mbps	Up to 250 Mbps	Up to 500 Mbps	Up to 1 Gbps
Max Concurrent Connections	15K	80K	80K	160K	500K
New Connections Per Second	750/Sec	4K/Sec	4K/Sec	8K/Sec	10K/Sec

Tabela 7. FireEye MVX smart grid specifications.

	VX 5500	VX 12550
OS Support	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X
Performance *	Up to 2 Gbps	Up to 14 Gbps
High Availability **	N+1	N+1
Management Ports (rear panel)	1x 10/100/1000 Mbps BASE- T Ports	1x 10/100/1000 Mbps BASE- T Ports
Cluster Ports (rear panel)	3x 10/100/1000 Mbps BASE-T Ports	1x 10/100/1000 Mbps BASE-T Ports, 2x 10 Gbps BASE-T Ports
IPMI Port (rear panel)	Included	Included
Front LCD & Keypad	Not Available	Included
VGA Ports	Included	Included
USB Ports (rear panel)	4x Type A USB Ports	2x Type A USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Drive Capacity	2x 2TB 3.5 SAS HDD, RAID 1, hot-swappable, FRU	2x 2TB 3.5” SAS3 HDD, RAID 1, FRU
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis Dimension WxDxH	17. 2x25.6x1.7 Inches (437 x 650 x 43.2 mm)	17.2x33.5x3.5 Inches (437 x 851 x 89 mm)
DC Power Supply	Not Available	Not Available
AC Power Supply	Redundant (1+1) 750 watt, 100-240 VAC, 8 - 3.8 A, 50-60 Hz, IEC60320-C14, inlet, hot-swappable, FRU	Redundant (1+1) 800W: 100-127V, 9.8A-7A 1000W: 220-240V, 7-5A, 50-60Hz, FRU IEC60320-C14 inlet, FRU
Power Consumption Maximum (watts)	285 watts	760 watts
Thermal Dissipation Maximum (BTU/h)	972 BTU/h	2594 BTU/h
MTBF (h)	54,200 h	38,836 h
Appliance Alone / As Shipped Weight lb. (kg)	33 lb (15 kg) / 48 lb (21.8 kg)	46 lb (21 kg) / 90 lb (40.2 kg)
Security Certification	FIPS 140-2 Level 1, CC NDPP v1.1 (Pending)	FIPS 140-2 Level 1, CC NDPP v1.1 (Pending)
Regulatory Compliance Safety	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

Tabela 7. FireEye MVX smart grid specifications.

	VX 5500	VX 12500
Regulatory Compliance EMC	FCC Part 15 ICES-003 Class 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 &V-3/2015	FCC Part 15 ICES-003 Class 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 &V-3/2015
Environmental Compliance	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU REACH WEEE Directive 2012/19/EU
Operating Temperature	10 ~ 35°C (50 ~ 95°F)	0 - 40°C (32 - 104°F)
Non-Operating Temperature	-40 ~ 70°C (-40 ~ 158°F)	-30 - 70°C (-22 - 158°F)
Operating Relative Humidity	10% - 85% non-condensing	10% - 90% @ 40°C non-condensing
Non-Operating Relative Humidity	5% - 95% non-condensing	10% - 95% @ 55°C non-condensing
Operating Altitude	3000 m 9842 ft	3000 m 9842 ft

Support Services

FireEye offers simple and flexible support programs to maximize the value of your FireEye products and services. Four different levels of support services are available: Platinum, Platinum Priority Plus, Government and Government Priority Plus. For more information about FireEye support, refer to FireEye Support services.

Aby dowiedzieć się więcej, odwiedź stronę: **www.FireEye.com**

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

DLACZEGO FIREEYE?

SPECJALISTYCZNA WIEDZA. TECHNOLOGIA. INTELIGENCJA.

FireEye dysponuje unikalną w branży zabezpieczeń IT kombinacją specjalistycznej wiedzy, technologii oraz praktycznego doświadczenia z realizacji usług Incident Response.Specjaliści ds. zabezpieczeń FireEye współpracują ze wszystkimi klientami, aby zrozumieć i rozwiązać określone problemy z zabezpieczeniami, zapewniając szybkie odpowiedzi najwyższej klasy ekspertów. Platforma ochrony przed zagrożeniami zapewnia firmie FireEye wgląd w unikalne informacje o świecie zaawansowanych zagrożeń, atakach kierowanych, ciągłych zagrożeniach i cyberprzestępczości, umożliwiając firmie FireEye udostępnianie klientom branżowej i dynamicznej analizy zagrożeń. FireEye dostarcza specjalistyczną wiedzę i analitykę niezbędne organizacjom do ochrony przed współczesnymi zagrożeniami.

FIREEYE™