DATA SHEET

FireEye Email Security Server Edition

Adaptacyjna, inteligentna i dobrze skalowalna ochrona przed zagrożeniami pochodzącymi z poczty elektronicznej

PODSTAWOWE INFORMACJE

- Produkt chroni przed atakami typu spear-phishing i spoofing w wiadomościach e-mail.
- Analizuje wiadomości e-mail pod kątem zagrożeń typu zero-day, ataków ukrytych w archiwach ZIP/RAR/TNEF i złośliwych adresów URL.
- FireEye Email Security obsługuje analizy na najczęściej spotykanych i najnowszych wersjach systemów Microsoft Windows oraz Apple Mac OS X.
- Analiza widomosci e-mail zawierających zagrożenia ukryte w chronionych hasłem plikach, zaszyfrowane i zawierające adresy URL.
- Zapewnia komunikację w czasie rzeczywistym z chmurą FireEye DTI.
- Priorytetyzuje zagrożenia, dostarczając kontekstu do alertów.
- Współpracuje zarówno ze zintegrowanym, jak i zewnętrznym silnikiem MVX.

Rys.1 FireEye Email Security appliances: EX 3500, EX 5500 and EX 8500.

PRZEGLĄD

Widomość e-mail jest najbardziej popularnym wektorem cyberataków, ponieważ jest podstawowym punktem wejścia danych do firmy. Organizacje stają w obliczu stale rosnącej liczby wyzwań, związanych z bezpieczeństwem, wynikających z zaawansowanych zagrożeń przesyłanych przez e-mail. Najbardziej zaawansowane zagrożenia używają widomości e-mail do dostarczania adresów URL powiązanych z witrynami phishingowymi i kierującymi do niebezpiecznych plików. Ponieważ jest to narzędzie, które można precyzyjnie ustawić i dostosować, e-mail to podstawowy nośnik cyberprzestępczości.

FireEye Email Security pomaga organizacjom zminimalizować ryzyko kosztownych włamań, spowodowanych zaawansowanymi atakami drogą e-mail. Wdrożenie w organizacji, FireEye Email Security, czyli rozwiązania będącego liderem w branży w identyfikacji, izolowania i natychmiastowego zatrzymywania ataków opartych na adresach URL i załącznikach, zanim wejdą one do środowiska organizacji, dostarcza również kontekst oparty na danych wywiadowczych i plug-in'ach, pozwala zidentyfikować złośliwe adresy phishingowe w dużych zbiorach danych. Silnik Multi-Vector Virtual Execution ™ (MVX) analizuje załączniki dołączane do wiadomości e-mail i adresy URL powiązane z treściami do pobrania, w oparciu o kompleksową macierz systemów operacyjnych, aplikacji i przeglądarki internetowe wbudowane w rozwiązanie. Zagrożenia są identyfikowane przy minimalnym nakładzie pracy, a fałszywe alarmy prawie się nie zdarzają.

FireEye gromadzi obszerne informacje o zagrożeniach poprzez analizy pochodzące z milionów czujników. Ochrona poczty e-mail opiera się na dwóch filarach – dowodach oraz inteligencji kontekstowej na temat ataków i atakujących, aby nadawać priorytety alertom i blokować zagrożenia w czasie rzeczywistym.

Dzięki integracja z FireEye Network Security oraz FireEye Endpoint, organizacje mogą uzyskać szerszy wgląd w różne wektory ataku i koordynować ochronę w czasie rzeczywistym.

Obrona przed zagrożeniami e-mail

Dzięki naszym danym osobowym, które cały czas są dostępne online, cyberprzestępca może wykorzystać socjotechnikę, aby nakłonić prawie dowolnego użytkownik do podjęcia działania, takich jak choćby kliknięcia adresu URL lub otwarcie załącznika.

Email Security zapewnia wykrywanie w czasie rzeczywistym i zapobieganie przejmowaniu poświadczeń, podszywaniu się oraz atakom typu spear-phishing, które zazwyczaj nie są wykrywane przez tradycyjne zabezpieczenia poczty e-mail. Wiadomości są analizowane i poddawane kwarantannie (blokowane), jeśli są w nich ukryte nieznane i zaawansowane zagrożenia. FireEye Email Security bada:

- Analizowane typy załączników, to tym między innymi: EXE, DLL, PDF, SWF, DOC / DOCX, XLS / XLSX, PPT / PPTX, Archiwa JPG, PNG, MP3, MP4 i ZIP / RAR / TNEF.
- Chronione hasłem i zaszyfrowane załączniki.
- Załączniki chronione hasłem z hasłem ukrytym w obrazie.
- Adresy URL osadzone w wiadomościach e-mail, dokumenty MS Office, PDF i pliki archiwalne (ZIP, ALZIP, JAR) oraz inne typy plików (Uuencoded, HTML).
- Pliki pobierane przez adresy URL - a nawet łącza FTP.
- Niewidoczne, sfałszowane, skrócone i dynamiczne przekierowane adresy URL.
- Adresy URL wyłudzające dane uwierzytelniające oraz typosquatting.
- Nieznane podatności systemów Microsoft Windows i Apple MacOS X, przeglądarek i aplikacji.
- Złośliwy kod osadzony w e-mailach typu phishing.

Ataki ransomware najczęściej zaczynają się od widomości e-mail, ale bardzo często to połączenie zwrotne (callback) do serwera C&C jest wymagane, aby rozpocząć proces szyfrowania danych. Email Security identyfikuje i zatrzymuje te trudne do wykrycia wielostopniowe kampanie szkodliwego oprogramowania.

Doskonałe wykrywanie zagrożeń

Bezpieczeństwo poczty e-mail pomaga zmniejszyć ryzyko kosztownych włamań identyfikując i izolując zaawansowane, ukierunkowane ataki, które potrafią wykorzystać techniki kamuflażu tak, aby być rozpoznawane jako normalny ruch. Raz wykryte ataki są natychmiast zatrzymywane, analizowane i oznaczane dla szybszej identyfikacji przyszłych zagrożeń.

Podstawą rozwiązania FireEye Email Security jest zaawansowana ochrona adresów URL, silnik MVX i MalwareGuard. Te technologie wykorzystują uczenie maszynowe i analitykę, aby zidentyfikować ataki unikające tradycyjnej ochrony opartej na sygnaturach i regułach.

Integralna część Advanced URL Defense jest PhishVision - to silnik klasyfikacji obrazu, który wykorzystuje głęboką analizę, aby skompilować i porównać zrzuty ekranu zaufanych i powszechnie uznanych marek w stosunku do stron internetowych wskazanych przez adresy URL w wiadomości e-mail. Pracujący w tandemie z technologią PhishVision, Kraken jest wtyczką wykrywającą phishing poprzez analizę machine-learning. Skyfeed natomiast to znaczący postęp w wykrywaniu zagrożeń w adresach URL. Jest to specjalnie zaprojektowany, w pełni zautomatyzowany system zbierania inteligencji szkodliwego oprogramowania. Konta mediów społecznościowych, blogi, fora i inne kanały komunikacji są gromadzone w celu wykrycia potencjalnych zagrożeń.

MalwareGuard to narzędzie do uczenia maszynowego, biorące pod uwagę pliki binarne jako dane wejściowe i wyliczające punktację. Każdy plik Portable Executable (PE) widoczny w przesyłanych wiadomościach jest analizowany przez MalwareGuard. Decyzja podejmowana jest na podstawie wyniku punktacji i wykrycia wywołanego przez MalwareGuard.

Silnik MVX wykrywa zagrożenia zero-day, multi-flow i inne ataki wymijające za pomocą dynamicznej analizy bezsygnaturowej w środowisku wirtualnym. Jest w stanie zidentyfikować nigdy przedtem nie wykryt exploity i złośliwe oprogramowanie, aby zatrzymać infekcję i nie dopuścić do kompromitacji.

Skuteczne zapobieganie ukrytym atakom

Zabezpieczenia poczty e-mail obsługują funkcję „controlled live mode" pozwalającą bronić się przed atakami, które wymagają do aktywacji połączenia z siecią Internet. Silnik MVX wykrywa złośliwe oprogramowanie, wymagające pobrania dodatkowych danych i zwraca zdalne obiekty wymagane przez przykładowy plik binarny. Kontrolowany tryb live mode pozwala zredukować ilość ataków typu phishing i zaawansowane kampanie ransomware.

Atakujący cały czas próbują ominąć technologię wykorzystywaną do wykrywania podejrzanych adresów URL. W ramach Advanced URL Defense, FireEye EX pozwala na unikanie oszustw na stronach phishingowych, gdyż mechanizm ten cały czas ewoluuje. Kolejne mechanizmy wykrywania technik unikania są stale ulepszane przez FireEye jako część Advanced URL Defense.

Integracja w celu poprawy wydajności obsługi alertów

FireEye EX analizuje każdy załącznik i adres URL aby dokładnie zidentyfikować zaawansowane ataki. Aktualizacje przekazywane w czasie rzeczywistym, z całego ekosystemu zabezpieczeń FireEye, w połączeniu z atrybutami alertów znanych zagrożeń, zapewniają kontekst dla ustalania priorytetów i podejmowania działań związanych z krytycznymi zdarzeniami, a w konsekwencji blokowanie ataków prowadzone drogą e-mail.

Znane, nieznane i zagrożenia niezwiązane ze złośliwym oprogramowaniem są identyfikowane z minimalnym narzutem i małą liczbą fałszywych alarmów, co pozwala skoncentrować zasoby na prawdziwych atakach w celu zmniejszenia kosztów operacyjnych. Kategoria Riskware oddziela prawdziwe próby naruszenia od niepożądanej, ale mniej szkodliwej aktywności (takiej jak adware i spyware), aby nadać priorytet odpowiednim alarmom.

Szybkie dostosowanie do zmieniającego się krajobrazu zagrożeń

FireEye EX pomaga Twojej organizacji nieustannie dostosowywać Twoją proaktywną obchronę do zagrożeń pochodzących z poczty elektronicznej, za pośrednictwem informacje o zagrożeniach przekazywanych w czasie rzeczywistym z chmury FireEye Dynamic Threat Intelligence (DTI). Dogłębna wiedza dot. zagrożeń i ataków pozwala na:

- Zapewnienie aktualnej i szerokiej widoczność zagrożeń.
- Określa konkretne możliwości i cechy wykrytego złośliwego oprogramowanie i złośliwych załączników.
- Zapewnia kontekstowe informacje, aby ustalić priorytety i przyspieszyć reakcję.
- Określa prawdopodobną tożsamość i motywy atakujących i śledzi ich działania w Twojej organizacji.
- Przepisuje wszystkie adresy URL, osadzone w wiadomości e-mail, aby chronić użytkowników przed użyciem szkodliwych linków.
- Identyfikuje nawet już po ich wystąpieniu ataki typu spear-phishing i zapobiegaj dostępowi do stron phishingowych, oznaczając złośliwe adresy URL.

Współpraca FireEye EX zarówno z FireEye Helix jak i FireEye CM (Central Management)

- Jako składnik platformy bezpieczeństwa - FireEye Helix - zapewnia widoczność całej infrastruktury. FireEye Helix koreluje alerty dot. poczty elektronicznej oraz alerty firm trzecich ze zdarzeniami z punktów końcowych, i wskazówkami dot. potencjalnego śledztwa. Dzięki tym możliwościom, FireEye Helix uwidacznia dotąd niewidzialne zagrożenia i ułatwia analitykom podejmowanie właściwych decyzji.
- FireEye CM koreluje alerty z rozwiązań Email Security (EX) oraz Network Security (NX) dla szerszego widoku ataku i ustanawia zasady blokowania, aby zapobiec rozprzestrzenianiu się ataku.
- CM obsługuje tagowanie oparte na rolach, aby wiedzieć kto jest celem.

Dodatkowe możliwości

Reguły YARA pozwalające na dostosowanie systemu do własnych potrzeb

Seria EX pozwala na importowanie reguł YARA, które pozwalają analitykom zabezpieczeń na określenie własnych zasad analizy załączników wiadomości e-mail w celu dopasowania działania do zagrożeń specyficznych dla danej organizacji.

Ochrona wysoko postawionych pracowników przed podszywaniem się (Impersonation protection)

FireEye Email Security - Server Edition oferuje możliwość zablokowania kompromitacji w e-mailach biznesowych (BEC), w celu ochrony ważnych pracowników przed fałszowaniem adresu nadawcy. Polityka porównuje nazwy wyświetlanych nadawców wiadomości e-maili z zatwierdzoną listą nadawców.

Zarządzanie kolejką wiadomości, zarządzanie alertami i kwarantanną

Fireeye Email Protection zapewnia wysoki stopień kontroli nad analizowanymi wiadomościami e-mail. W przypadku aktywnych wdrożeń w trybie ochrony wiadomości mogą być śledzone i zarządzane, gdy przemieszczają się w kolejce MTA; atrybuty wiadomości mogą być używane do wyszukiwania, a następnie sprawdzenia, czy wiadomości zostały odebrane, przeanalizowane i dostarczane do następnego węzła pocztowego; trendy w czasie mogą być monitorowane za pośrednictwem intuicyjnego panelu kontrolnego. Jawne listy dozwolonych i zablokowanych adresatów pozwalają na dostosowanie kontroli przetwarzania wiadomości e-mail do swoich potrzeb. Wspólne atrybuty alertów można wyszukiwać i wybierać - mogą to być operacje masowe, wykonywane na alertach i wiadomościach poddanych kwarantannie.

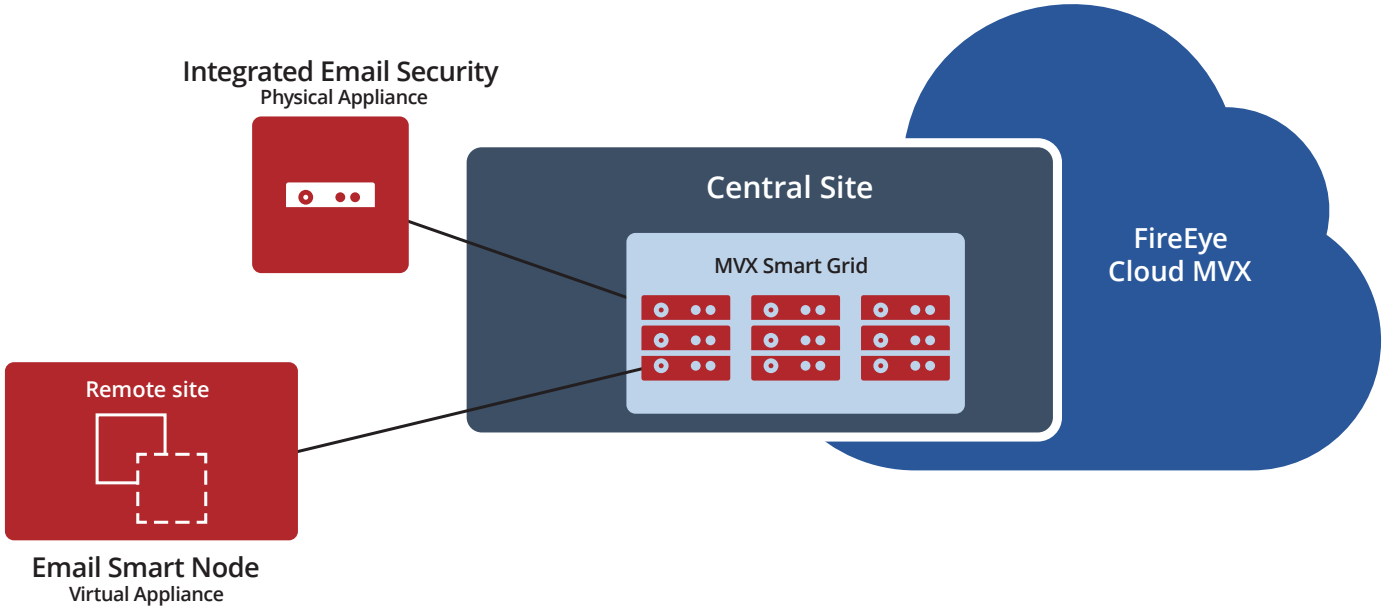
Tryb aktywnej ochrony lub monitorowania

Email Security może analizować wiadomości e-mail i zagrożenia umieszczone w kwarantannie dla uzyskania aktywnej ochrony. W przypadku wdrożeń tylko w trybie monitor należy skonfigurować tryb BCC, w celu wysyłania kopii widomości e-mali do analizy w lokalnym rozwiązaniu FireEye Email Security Server.

Flexible Deployment Options

FireEye Email Security - Server Edition oferuje różne opcje wdrożenia, odpowiadające potrzebom i budżetowi organizacji:

- **Zintegrowane zabezpieczenia poczty e-mail:** samodzielne, urządzenie sprzętowe ze zintegrowaną usługą MVX, pozwalające zabezpieczyć punkt wejścia poczty e-mail. FireEye Email Security to łatwe w zarządzaniu rozwiązanie, wdrażane w mniej niż 60 minut, gdyż nie wymaga tworzenia reguł, polityk lub strojenia.
- **Distributed Email Security:** urządzenia fizyczne lub wirtualne z centralnie udostępnioną usługa MVX, w celu zabezpieczenia poczty e-mail w wielu punktach w organizacjach.
- **Email Smart Node:** wirtualne czujniki, analizują pocztę elektroniczną w celu wykrywania i blokowania złośliwego ruchu i przesyłania podejrzanej aktywność zaszyfrowanym kanałem do usługi MVX do ostatecznej analizy werdyktu.
- **MVX Smart Grid:** urządzenie fizyczne z lokalnym silnikiem MVX, oferujące skalowalność infrastruktury Email 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 widomości e-mail w celu zachowania prywatności odbywa się na Fireeye Smart Node, jedynie podejrzane obiekty są wysyłane zaszyfrowanym kanałem do Cloud MVX. Obiekty zakwalifikowane jako nieszkodliwe nie są przesyłane do dalszej analizy.



Rys.2 Modele wdrażania zabezpieczeń poczty elektronicznej.

Tabela 1. Specyfikacja techniczna

	EX 3500	EX 5500	EX 8500
Performance*	Up to 700 unique attachments per hour	Up to 1,800 unique attachments per hour	Up to 2,650 unique attachments per hour
Network Interface Ports	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+ (supporting 10GigE Fiber, 10GigE Copper, 1GigE Copper), 2x 1GigE BaseT
Management Ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI Monitoring	Included	Included	Included
VGA Port (rear panel)	Included	Included	Included
USB Ports (rear panel)	4x USB Type A Rear	2x USB Type A Front, 2x USB Type A Rear	2x USB Type A Front, 2x USB Type A Rear
Serial Port (rear panel)	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
Storage Capacity	4x 2TB, RAID 10, HDD 3.5 inch, FRU	4x 2TB, RAID 10, HDD 3.5 inch, FRU	4x 2TB, RAID 10, HDD 3.5 inch, FRU
Enclosure	1RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack
Chassis Dimensions (WxDxH)	17.2" x 25.6" x 1.7" (437 x 650 x 43.2 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
AC Power Supply	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
DC Power Supply	Not Available	Not Available	Not Available
Thermal Maximum Power	245 watts (836 BTU per hour)	456 watts (1,556 BTU per hour)	530 watts (1,808 BTU per hour)
MTBF (h)	54,200 hours	57,401 hours	53,742 hours
Appliance Alone / As Shipped Weight, lb (kg)	30.0 lbs (13.6 kg) / 41.0 lbs (18.6 kg)	44.1 lbs (20.0 kg) / 65.3 lbs (29.6 kg)	44.4 lbs (20.2 Kg) / 65.6 lbs (29.8 kg)
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
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
Security Certifications	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
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
Operating Temperature	0 ~ 35° C (32 ~ 95° F)	0 ~ 35° C (32 ~ 95° F)	0 ~ 35° C (32 ~ 95° F)
Operating Relative Humidity	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing
Operating Altitude	3,000 m / 9,842 ft	3,000 m / 9,842 ft	3,000 m / 9,842 ft

* All performance values vary depending on the system configuration and email traffic profile being processed. Size appliance(s) based on unique attachments per hour.

Tabela 2. Specyfikacja FireEye MVX smart grid

	VX 5500	VX 12500
OS Support	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
Performance*	Up to 480 unique attachments per hour	Up to 3,780 unique attachments per hour
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	4 x 4TB 3.5" SAS3 HDD, RAID 1, FRU
Enclosure	1RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack
Chassis Dimensions (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	285 watts	760 watts
Thermal Dissipation Maximum	972 BTU per hour	2594 BTU per hour
MTBF	54,200 hours	38,836 hours
Appliance Alone / As Shipped Weight	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	FIPS 140-2 Level 1, CC NDPP v1.1
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

* All performance values vary depending on the system configuration and traffic profile being processed.

** With appropriate redundant hardware configurations.

Tabela 3. Specyfikacja FireEye Email Security smart node, virtual sensor

	EX 5500V
OS Support	Microsoft Windows, Apple macOS X
Performance*	Up to 1,250 unique attachments per hour
Network Monitoring Ports	2
Network Management Ports	2
CPU cores	8
Memory	16 GB
Drive Capacity	384 GB
Network Adapters	VMXNet 3, vNIC
Hypervisor Support	VMWare ESXi 6.0 or later

* All performance values vary depending on the system configuration and traffic profile being processed.

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