



McAfee IntruShield Network Security Platform

Najbardziej zaawansowane i sprawdzone rozwiązanie w dziedzinie zapobiegania włamaniom w sieci

Szybszy czas zapewnienia ochrony. Szybszy czas rozwiązania problemu. Szybszy czas uzyskania pewności. Platforma ochrony sieci McAfee® IntruShield® zapewnia ochronę na podstawie doskonałej wiedzy, która jest w pełni zintegrowana, zautomatyzowana i pewna. Tylko IntruShield łączy sieciową i systemową infrastrukturę bezpieczeństwa w celu zapewnienia proaktywnej ochrony całej firmy. Jest ona nieporównywalnie dokładniejsza i bardziej wydajna niż tradycyjne pojedyncze produkty. Zarządzaj ryzykiem i zapewniaj zgodność z regulacjami, wkładając w to o wiele mniej wysiłku. Inteligentne i niezawodne platformy sieciowe IntruShield gwarantują pewność zabezpieczeń zasobów firmy.

KLUCZOWE ZALETY

Działanie we wszystkich obszarach sieci

- Pojedyncze, sprawdzone w branży urządzenie zapewnia kompleksową i proaktywną ochronę sieci oraz systemów

Integracja z systemem zarządzania ryzykiem (SRM) firmy McAfee

- Integracja z produktami McAfee Foundstone i ePO zapewnia natychmiastowy wgląd w krytyczne informacje na temat hosta oraz określa krytyczność zagrożenia i możliwość jego wykorzystania.

Szybkie i trafne decyzje

- Skracaj czas reakcji na zagrożenie (time-to-protection) oraz czas uzyskania pewności (time-to-confidence) dzięki ochronie działającej w czasie rzeczywistym, która jest nie tylko zautomatyzowana, ale której informacje są pewne.

Niezawodne platformy sieciowe - kolejna generacja ochrony sieci

- Praca z szybkością od 100 Mb/s do 10 Gb/s
- Najwyższa gęstość portów
- Ochrona IPv6

Wydajność pracy

- Współpraca pomiędzy siecią McAfee, systemem oraz produktami ochrony i zarządzania powoduje duże oszczędności czasu i zasobów informatycznych

Efektywność operacyjna

- Współpraca pomiędzy ochroną sieciową McAfee, ochroną systemową oraz produktami do zarządzania ryzykiem powoduje duże oszczędności czasu i zasobów informatycznych

Niezawodna ochrona każdego urządzenia podłączonego do sieci

Jak inteligentna jest ochrona sieci w Twojej firmie? Tradycyjne systemy zapobiegania włamaniom (IPS) to rozwiązania punktowe pełne fałszywych alarmów oraz przepelnionych dzienników zdarzeń. Brak możliwości ich koordynacji oznacza stratę wielu cennych godzin na zbędne procesy analizy zdarzeń. Wiele rozwiązań opartych na komputerach PC nie skaluje się podczas ataków, a tylko niektóre z nich zapewniają odpowiednie narzędzia zmniejszające potrzebę szybkiego wdrażania aktualizacji.

Dlatego też ponad 4500 najbardziej wymagających firm oraz usługodawców wybrało McAfee IntruShield do ochrony swych sieci i podłączonych do nich urządzeń.

Zintegrowana ochrona sieci i systemów

Platforma ochrony sieci McAfee IntruShield to idealne rozwiązanie dla firm wymagających niezawodnego zabezpieczenia w czasie rzeczywistym o wydajności wielu gigabitów oraz zintegrowanej ochronie sieci i systemów w całej firmie. Ochrona IntruShield oparta na najlepszej wiedzy umożliwia automatyczne zarządzanie ochroną oraz spełnianie wymagań prawnych przy jednoczesnym zwiększeniu sprawności operacyjnej i ograniczeniu działań wykonywanych przez dział informatyczny.

Wykorzystując mechanizmy zarządzania ryzykiem (SRM) McAfee, IntruShield współpracuje z McAfee Foundstone®, McAfee ePolicy Orchestrator® (ePO™) oraz McAfee Network Access Control (NAC), zapewniając to, co bardzo ważne w biznesie – ochronę, widzialność, skuteczność i oszczędność.

Absolutna pewność bezpieczeństwa

IntruShield chroni wszystkie urządzenia podłączone do sieci za pomocą połączenia rozwiązań IPS i wewnętrznej zapory sieciowej, integrując i łącząc ich funkcjonalność, a także rozciągając działanie zapory na sieć wewnętrzną. Korelujemy sygnatury, anomalie oraz informacje na temat ataków typu DoS (Denial of Service) i DDoS (Distributed Denial of Service), aby dokładnie blokować te ataki zanim dotrą one do swych celów. Dynamiczne aktualizacje chroniące przed zagrożeniami i wykorzystaniem słabych punktów zapewniają ciągłą ochronę.

Platforma klasy sieciowej o wydajności wielu gigabitów

Zestaw specjalnie zaprojektowanych urządzeń IntruShield zapewnia ekonomiczną i wysokowydajną ochronę różnych lokalizacji – od zdalnych filii, aż po rdzeń sieci. IntruShield zapewnia łatwą konfigurację i eksploatację. Konfiguracja systemów zajmuje kilka minut, a ich skuteczne zarządzanie i wprowadzanie aktualizacji jest wykonywane za pomocą centralnej konsoli opartej na przeglądarce internetowej.

Nieźródlna jakość i wydajność IntruShield przewyższa wymogi i standardy operatorów telekomunikacyjnych (carrier-class). IntruShield jako jedyny system IPS posiada certyfikat Multi-Gigabit IPS NSS Group. Seria M zapewnia naszym klientom niezawodność zgodną z wymogami i standardami operatorów telekomunikacyjnych, oferując im wydajność równą 10 Gb/s z największą gęstością portów dostępną na rynku.





PLATFORMA OCHRONY SIECI INTRUSHIELD

Ochrona firmy w czasie rzeczywistym

- Zapobiegaj atakom przy obniżeniu kosztów i czasu przestoju
- Chroni dane i infrastrukturę swojej firmy
- Spełnia wymagania przepisów

Chron swoje systemy

- Proaktywna ochrona systemów bez uaktualnień
- Proaktywna ochrona przed nieznanymi atakami (Zero Day Attacks)
- Świadomość stanu systemów po integracji z McAfee ePO
- Wgląd w zdarzenia z hostowego zabezpieczenia IPS

Chron swoją sieć

- 10-gigabitowy Ethernet nowej generacji
- Ochrona IPv6
- Adaptacyjne ograniczanie ruchu sieciowego
- Kompleksowa ochrona infrastruktury

Zgodność z przepisami i polityką bezpieczeństwa

- Świadomość występowania słabych punktów w czasie rzeczywistym i raportowanie zgodności z przepisami
- IPS świadomy występowania ryzyka po integracji z McAfee Vulnerability Manager
- Kwarantanna hosta na podstawie zachowania
- Wdrażanie polityki wewnętrznej i reguł zgodnych z przepisami prawnymi

Rozwiąż problemy z uaktualnieniami i wdrażaj swoje reguły

Masz całkowitą kontrolę. Za pomocą IntruShield izolujesz swe systemy od ryzyka, jednocześnie testując i wprowadzając uaktualnienia. Możesz kontrolować ruch sieciowy i wdrażać unikalne reguły i zabezpieczenia w danym segmencie sieci, grupie hostów lub nawet w pojedynczym systemie. Elastyczność IntruShield powoduje, że uaktualnienia można wprowadzać w odpowiednim czasie, a reguły wymuszać zgodnie z potrzebami danej organizacji.

Jedynе sprawdzone w branży urządzenie zabezpieczające

Zapewnij swojej firmie sprawdzoną ochronę McAfee tworzoną na podstawie badań prowadzonych non-stop w McAfee Avert® Labs. Dostosuj swe zabezpieczenia do wymogów i standardów operatorów telekomunikacyjnych (carrier-class) za pomocą jednego zintegrowanego rozwiązania ochrony sieci.

Skuteczne zapobieganie zagrożeniom w całej firmie

- Chroni swą firmę przed atakami znanymi i nieznanymi jeszcze producentom, atakami DoS, DDoS, SYN flood, zaszyfowanymi atakami i zagrożeniami takimi jak oprogramowanie szpiegujące, ataki wykorzystujące słabe punkty VoIP, sieci komputerów-zombie (botnet), malware, robaki, konie trojańskie, phishing oraz tunelowanie w sieciach peer-to-peer.
- Zwiększaj dokładność działania systemu, korzystając z wielu zaawansowanych metod wykrywania zagrożeń obejmujących anomalie sygnatur, aplikacji i protokołów, algorytmy wykrywania kodu shellcode oraz mechanizmy nowej generacji zapobiegające atakom typu DoS i DDoS.
- Analizuj ponad 100 protokołów i przeglądaj ponad 3000 wysokiej jakości sygnatur wielokrotnych sprawdzonych obejmujących wiele tokenów wraz z kontrolą połączeń w ruchu sieciowym.
- Proaktywnie i automatycznie blokuj setki ataków za pomocą wstępnie skonfigurowanych reguł *Zalecone do zablokowania*.
- Non-stop otrzymuj aktualizacje zagrożeń od globalnego zespołu badawczego w McAfee Avert Labs.

Integracja z McAfee ePolicy Orchestrator® (ePO™)

- Uzyskaj wgląd w czasie rzeczywistym w gotowe do wykorzystania informacje z zasobów systemowych obejmujące nazwę hosta, nazwę użytkownika, system operacyjny, poziom uaktualnienia, adres MAC, datę ostatniego skanowania, informacje na temat zainstalowanych zabezpieczeń oraz ostatnie informacje pochodzące z systemu na temat zdarzeń związanych z IPS, ochroną antywirusową i ochroną przed oprogramowaniem szpiegującym.
- Syntetyzuj i filtruj dane w celu stworzenia raportu dostosowanego do indywidualnych potrzeb.

Platforma ochrony sieci zapewnia wgląd w zagrożenia w czasie rzeczywistym

- Integracja z McAfee Foundstone zapewnia automatyczne importowanie danych na temat systemów narażonych na ataki oraz skanowanie regularne, jak i na żądanie w celu dokładnego określenia skali zagrożenia.

Adaptacyjne ograniczenie ruchu sieciowego

- IntruShield w czasie rzeczywistym stosuje ograniczanie ruchu sieciowego dla odpowiednich protokołów występujących na dowolnych portach lub tych, które zostaną wybrane przez administratorów do ograniczenia ruchu aplikacji i protokołów w celu poprawienia jakości usług.
- Określaj ruch sieciowy pod względem ważności dla firmy oraz blokuj niepożądane i groźne aplikacje.

Certyfikacja NSS Group

- IntruShield jako jedyne sieciowe rozwiązanie IPS posiada certyfikat Multi-Gigabit IPS NSS Group.

Sprawdzona zarządzalność i dostępność

Proste, centralne zarządzanie systemem IntruShield w oparciu o przeglądarkę internetową obejmuje:

- Czternaście gotowych do użytku i wstępnie zdefiniowanych reguł polityki IPS
- Zintegrowane wsparcie uwierzytelniania użytkowników za pomocą zewnętrznych baz danych obejmujących Radius, LDAP i TACACS
- IntruShield Security Manager (ISM) oferuje nieprzerwaną pracę w trybie wysokiej niezawodności (HA), automatyczne podtrzymanie pracy i powrót do pracy po awarii (failover i failback) oraz przywracanie krytycznych danych konfiguracyjnych po awarii (disaster recovery)
- IntruShield Command Center (ICC) zapewnia hierarchiczne zarządzanie w celu centralnej kontroli przeglądania, modyfikacji i dystrybucji reguł polityki IPS w celu zapewnienia wsparcia dla urządzeń rozproszonych na dużym obszarze geograficznym
- Konfiguracja wysokiej dostępności umożliwia przezroczyste podtrzymanie funkcjonalności i przełączenie stanowe w warstwie 7 modelu ISO/OSI, z uniknięciem pojedynczego punktu awarii.

Specyfikacje urządzenia IntruShield



Urządzenia Intrushield	M-8000	M-6050	I-4010	I-4000	I-3000	I-2700	I-1400	I-1200	
Lokalizacja w sieci	Rdzeń	Rdzeń	Rdzeń	Rdzeń	Rdzeń	Na styku z Internetem	Filia/na styku z Internetem	Filia	
Przepustowość	Maks. 10 Gb/s	Maks. 5 Gb/s	Maks. 2 Gb/s	Maks. 2 Gb/s	Maks. 1 Gb/s	Maks. 600 Mb/s	Maks. 200 Mb/s	Maks. 100 Mb/s	
Maksymalna liczba równoczesnych połączeń	4 000 000	2 000 000	1 000 000	1 000 000	500 000	250 000	80 000	40 000	
Porty									
Porty monitorujące Gigabit Ethernet	16	8	12	4	12	2	–	–	
Porty monitorujące 1 Gigabit Ethernet	12	8	–	–	–	–	–	–	
Porty monitorujące Fast Ethernet (FE)	–	–	–	–	–	6	4	2	
Dedykowane porty odpowiedzi	1	1	2	2	2	3	1	1	
Dedykowane porty zarządzania	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Porty sterujące zestawem podtrzymującym połączenie w razie awarii	14	8	6	2	6	1	–	–	
Porty konsoli i porty dodatkowe	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Wbudowane sieciowe urządzenia TAP	Nie	Nie	Nie	Nie	Nie	Tak (dla portów FE)	Tak	Tak	
Zestawienie połączenia w razie awarii	Opcja	Opcja	Opcja	Opcja	Opcja	Tak (dla portów FE)	Tak	Tak	
Blokowanie połączenia w razie awarii	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Tryby pracy									
Monitorowanie poprzez SPAN	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Tryb przyłączeniowy (TAP)	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Tryb przezroczysty (In-Line)	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Grupowanie portów	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Liczba wirtualnych systemów IPS	1000	1000	1000	1000	1000	100	32	16	
Monitorowanie ruchu na łączach w układzie aktywne-aktywne	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Monitorowanie ruchu na łączach w układzie aktywne-pasywne	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Monitorowanie ruchu asymetrycznego ruchu w sieci	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Funkcje zapewnienia wysokiej dostępności									
Nadmiarowe zasilanie	Tak (opcja)	Tak (opcja)	Tak (opcja)	Tak (opcja)	Tak (opcja)	Tak (opcja)	Nie	Nie	
Wykrywanie awarii urządzenia	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Wykrywanie awarii łącza	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Dane fizyczne									
Wymiary	2 x 2RU do montażu w szelaku 16,75 (szer.) x 3,05 (wys.) x 30,00 (gł.) każdy	2RU do montażu szelaku 16,75 (szer.) x 3,05 (wys.) x 30,00 (gł.)	2RU do montażu w szelaku 17,44 (szer.) x 3,44 (wys.) x 23,00 (gł.)	2RU do montażu w szelaku 17,44 (szer.) x 3,44 (wys.) x 23,00 (gł.)	2RU do montażu w szelaku 17,44 (szer.) x 3,44 (wys.) x 23,00 (gł.)	2RU do montażu w szelaku 17,44 (szer.) x 3,44 (wys.) x 23,00 (gł.)	2RU do montażu w szelaku 17,44 (szer.) x 3,44 (wys.) x 23,00 (gł.)	1RU do montażu w szelaku 17,32 (szer.) x 1,65 (wys.) x 10,5 (gł.)	1RU do montażu w szelaku 17,32 (szer.) x 1,65 (wys.) x 10,5 (gł.)
Waga	42,6 kg (2x21,3)	21,4 kg	21,4 kg	21,4 kg	21,4 kg	21,4 kg	7,8 kg	6,8 kg	
Zasilanie	100-240 V prąd zmienny (50/60 Hz)								
Pobór mocy	2 x 450 W	450 W	350 W	350 W	350 W	250 W	100 W	100 W	
Temperatura	od 0° do 35°C (praca); od -40° do 70°C (przechowywanie)			od 0° do 40°C (praca); od -40° do 70°C (przechowywanie)					
Wilgotność względna (bez kondensacji)	Praca: od 10% do 90% Przechowywanie: od 5% do 95%								
Wysokość n.p.m.	od 0 do 3000 m								
Certyfikat bezpieczeństwa	UL 1950, CSA-C22.2 nr 950, EN-60950, IEC 950, EN 60825, IEC 60825, 21CFR1040 – homologacja CB i raport dotyczący odstępstw obowiązujących w poszczególnych krajach.								
Certyfikat EMI	FCC część 15, Klasa A (CFR 47) (USA) ICES-003 Klasa A (Kanada), EN55022 Klasa A (Europa), CISPR22 Klasa A (międzynarodowa)								

Charakterystyka techniczna

Funkcjonalność urządzeń		M-8000	M-6050	I-4010	I-4000	I-3000	I-2700	I-1400	I-1200
Kontrola połączeń w ruchu sieciowym	Defragmentacja ruchu IP i reasemblacja strumienia TCP	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Szczegółowa analiza protokołów	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Monitorowanie ruchu asymetrycznego	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Normalizacja protokołów	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Zaawansowana ochrona przed pomijaniem zabezpieczeń	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Gromadzenie danych do celów sądowych	Nie	Nie	Tak	Tak	Tak	Tak	Tak	Tak
	Obsługa tunelowania protokołów	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Wykrywanie protokołów	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Obsługa VLAN	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak	
Wykrywanie sygnatur	Sygnatury definiowane przez użytkownika	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Aktualizacja sygnatur w czasie rzeczywistym	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Wykrywanie anomalii	Anomalie statystyczne	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Anomalie protokołów	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Anomalie aplikacji	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Wykrywanie ataków typu DoS	Wykrywanie wg wartości progowych	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Wykrywanie z wykorzystaniem inteligentnych samoczynnych się profili	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Maksymalna liczba profili ataków typu DoS	5000	5000	3000	3000	3000	300	120	100
Zapobieganie włamaniom	Zatrzymywanie trwających ataków w czasie rzeczywistym	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Eliminacja pakietów/sesji związanych z atakiem	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Kwarantanna hosta	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Inicjalizacja resetu sesji TCP, wiadomość ICMP host nieosiągalny	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Rejestrowanie pakietów	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Ochrona automatyczna i inicjowana przez użytkownika	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Ochrona przed atakami szfrowanymi	Blokowanie ataków szfrowanych w czasie rzeczywistym	Nie	Nie	Tak	Tak	Tak	Tak	Nie	Nie
Wewnętrzna zapora sieciowa	Blokowanie niepożądanego i uciążliwego ruchu sieciowego	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Wdrażanie szczegółowych reguł bezpieczeństwa	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Wysoka dostępność	Obsługa tunelowania protokołów	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
Zarządzanie	Interfejs z wierszem poleceń (konsola)	Tak	Tak	Tak	Tak	Tak	Tak	Tak	Tak
	Komunikacja z IntruShield Manager	Bezpieczny kanał	Bezpieczny kanał	Bezpieczny kanał	Tak	Tak	Tak	Tak	Tak



McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee i/lub inne powiązane produkty McAfee opisane w niniejszym dokumencie są zastrzeżonymi znakami towarowymi lub znakami towarowymi McAfee Inc. i/lub jej podmiotów zależnych w Stanach Zjednoczonych i/lub w innych krajach. Kolor czerwony w połączeniu z zabezpieczeniami jest wyróżniającą cechą produktów marki McAfee. Pozostałe produkty niezwiązane z McAfee i/lub zastrzeżone i niezastrzeżone znaki towarowe zostały wymienione w niniejszej publikacji tylko w celach referencyjnych i są wyłączną własnością odpowiednich podmiotów.
© 2008 McAfee, Inc. Wszelkie prawa zastrzeżone.

McAfee®

1-is-ips-003-0208