

Pakiet IBM Proventia Network Multi-Function Security — zunifikowane zarządzanie zagrożeniami i ochrona prewencyjna

Kompleksowa ochrona prewencyjna — teraz prosta w obsłudze i w atrakcyjnej cenie

Opracowany przez IBM Internet Security Systems (ISS) system IBM Proventia® Network Multi-Function Security (Proventia Network MFS) zawiera szereg zaawansowanych, a przy tym ekonomicznych narzędzi, które blokują zagrożenia internetowe jeszcze zanim dotrą one do sieci i zakłócą funkcjonowanie przedsiębiorstwa.

Rodzina produktów IBM Proventia realizuje prewencyjną ochronę środowiska informatycznego za pomocą aplikacji zatrzymujących ataki oraz oprogramowania zabezpieczającego pomagającego chronić serwery i stacje robocze przed zagrożeniami zewnętrznymi i wewnętrznymi. Dopelnieniem oferty produktowej IBM ISS są usługi

konsultingowe i outsourcingowe dotyczące problematyki bezpieczeństwa.

Proventia Network MFS w jednym urządzeniu łączy najlepsze na rynku mechanizmy wykrywania włamań z narzędziami zapory sieciowej, ochrony antywirusowej, filtrowania treści WWW i zwalczania spamu. Zapewnia ochronę na poziomie bram sieciowych i wewnętrznych struktur sieci bez uszczerbku dla przepustowości ani dostępności. Ponadto jest w stanie zwalczać jednocześnie bardzo wiele różnych zagrożeń — dostęp ze strony nieuprawnionych osób, ataki sieciowe, szkodliwe oprogramowanie, zagrożenia mieszane, ataki bazujące na treści, oprogramowanie szpiegujące czy oprogramowanie mające na celu wyludzenie informacji.

Dlaczego warto stosować zabezpieczenia wielofunkcyjne?

Zapory sieciowe i narzędzia antywirusowe to już za mało.

Zagrożenia o charakterze mieszanym oraz wyrafinowani hakerzy mogą obejść i pokonać te konwencjonalne metody obrony, poważnie zakłócając działanie firmy.

Zarządzanie zbiorem autonomicznych rozwiązań jest trudne i kosztowne.

Stosowanie szeregu niezależnych rozwiązań mających zwalczać poszczególne rodzaje zagrożeń jest bardzo kosztowne i nieefektywne, jeśli różne aplikacje nie współpracują ze sobą.

Dlaczego Proventia MFS?

Najlepsze dostępne na rynku moduły zabezpieczające są naprawdę zintegrowane, a nie tylko tworzą luźno powiązany zbiór narzędzi.

Każda warstwa zabezpieczeń zawarta w Proventia Network MFS — zapora sieciowa/obsługa sieci VPN (IPSec/SSL), ochrona antywirusowa, filtrowanie treści WWW, zwalczanie spamu i ochrona aplikacji — może z powodzeniem pełnić rolę autonomicznego produktu. Jednocześnie ich staranne połączenie w jeden pakiet pozwoliło utworzyć bardzo zaawansowany, a przy tym prosty w obsłudze i konfiguracji zunifikowany system do zarządzania zagrożeniami.

Oferuje ochronę prewencyjną powstrzymującą zagrożenia, zanim wyrządzą jakąkolwiek szkodę.

Wykorzystując technologie wykrywania włamań VirtualPatch opracowaną przez IBM ISS, Proventia MFS wychodzi poza ochronę reakcyjną i wprowadza mechanizm ochrony prewencyjnej.

Bazuje na najnowocześniejszych rozwiązaniach technicznych.

Proventia korzysta ze wsparcia zespołu badawczo rozwojowego X-Force® działającego w ramach IBM Internet Security Systems — jednego z nielicznych na świecie, który łączy badania nad lukami w zabezpieczeniach z tradycyjnym analizowaniem ataków. Dzięki specjalistycznej wiedzy zespołu X-Force system Proventia Network MFS jest w stanie błyskawicznie zapobiegać ponad 1000 typów różnych ataków.

Pozwala zaoferować najlepsze w branży warunki gwarancji ochrony.

Jeśli klient dodatkowo korzysta z usług ochrony zdalnej

oferowanych przez IBM, system jest oferowany z „gwarancją” ochrony — najlepszą na rynku umową świadczenia usług przewidującą zwrot 50 tys. USD w gotówce za każde naruszenie zabezpieczeń spowodowane skutecznym atakiem wymienionym na liście rozpoznanych ataków prowadzonej przez zespół X-Force.

Jedna z najlepszych relacji ceny do funkcjonalności dostępnych na rynku. Proventia Network MFS oferuje wysoką skuteczność ochrony przed zagrożeniami przy jednym z najbardziej atrakcyjnych współczynników cena/możliwości wśród rozwiązań dostępnych na rynku.

Znakomite rozwiązanie dla przedsiębiorstw o rozproszonej strukturze. Aplikacja umożliwia poszerzenie zasięgu ochrony prewencyjnej na małe firmy i zdalne oddziały dysponujące małymi działami informatycznymi.

Wspomaga ciągłość działania firmy, oferując niższy całkowity koszt użytkowania.

Pakiet oferuje szereg korzyści w postaci najwyższej klasy ochrony przy utrzymaniu integralności systemów i sieci, niższych kosztów operacyjnych dzięki zoptymalizowaniu systemów informatycznych oraz prostoty obsługi eliminującej konieczność utrzymywania własnych specjalistów od problematyki zabezpieczeń.

Zapewnia zgodność z zewnętrznymi regulacjami PCI, SOX i HIPAA. Proventia MFS jest jedynym rozwiązaniem na rynku certyfikowanym przez NSS Labs pod kątem zgodności ze standardem PCI DSS. Szczegółowe testy pokazały, że Proventia MFS pokrywa 10 z 12 wymagań stawianych przez PCI Council.

Połączenie najlepszych na świecie technologii zabezpieczeń w jeden produkt

Bazując na platformie zapory sieciowej/obsługi sieci VPN uzupełnionej o funkcje ochrony antywirusowej, filtrowania zawartości WWW, blokowania spamu i ochrony aplikacji, Proventia Network MFS łączy zaawansowane systemy zabezpieczeń stosowane w skomplikowanych sieciach w jeden kompaktowy, kompleksowy system:

Zapobieganie włamaniom — IBM ISS to jeden z liderów w dziedzinie rozwiązań zapobiegających włamaniom. Pakiet Proventia Network MFS oferuje poziom ochrony zastrzeżony jeszcze niedawno dla agend rządowych i przedsiębiorstw z listy Fortune 500.

Technologia IBM Virtual Patch® — Technologia Virtual Patch eliminuje potrzebę natychmiastowego/awaryjnego stosowania poprawek dzięki uszczelnieniu luk w zabezpieczeniach na poziomie sieci.

Zapora sieciowa — Moduł zapory sieciowej uzyskał certyfikat laboratorium ICASA. Zawiera funkcje wymagane w typowym środowisku korporacyjnym, obejmujące m.in. reguły zezwalania/blokowania według adresów/portów, nazwane listy obiektów oraz zarządzanie pasmem QoS.

Ochrona antywirusowa w oparciu o sygnatury — Moduł ochrony antywirusowej na poziomie bramy sieciowej analizuje w czasie rzeczywistym pliki pochodzące z witryn internetowych, poczty internetowej, witryn pobierania i systemów poczty e mail. Obejmuje swoim zasięgiem m.in. wszystkie ataki wymienione na listach organizacji Wildlist1. Wirusy są blokowane nawet wtedy, gdy ochrona antywirusowa na stacji roboczej jest wyłączona/nieaktualna.

Ochrona antywirusowa w oparciu o wzorce zachowań — Oferowany przez IBM ISS system zapobiegania infekcjom wirusowym wykrywa i blokuje szkodliwe pliki, w tym oprogramowanie szpiegujące, nieznane wirusy i nieznane robaki, bez dostępu do najnowszych sygnatur. Wykorzystując system rozpoznawania bazujący na wzorcach zachowań system antywirusowy jest w stanie blokować ponad 93% szkodliwych plików mimo braku najnowszych sygnatur wirusów.

Filtrowanie treści WWW — Z ponad 90 miliardami skatalogowanych witryn internetowych baza danych filtra internetowego Proventia WebFilter jest kilkukrotnie większa niż większość innych baz tego typu. Baza jest stale aktualizowana — codziennie trafia do niej ponad 120 tys. adresów nowych stron WWW.

Filtr antyspamowy — To zaawansowane narzędzie wykorzystuje 10 różnych metod wykrywania spamu, wykrywa spam ze skutecznością 95% przy błędnej identyfikacji poprawnych wiadomości jako spam na poziomie 1/10 000 i zapewnia aktualizacje bazy danych spamu co cztery godziny. Aplikacja sprawdza wiadomości względem zawartości bazy danych i zbioru różnych kategorii tekstu oraz porównuje adresy URL zawarte w wiadomościach e-mail z zawartością rozbudowanej bazy danych filtra WWW.

Moduł	Najważniejsze cechy
Zapobieganie włamaniom	Ponad 1000 blokad luk w zabezpieczeniach chroni przed 2500 różnymi atakami
Ochrona antywirusowa w oparciu o sygnatury	120 tys. znanych wirusów blokowanych przez mechanizm sygnaturowy
Ochrona antywirusowa w oparciu o wzorce zachowań	Blokada ponad 93% nieznanych wirusów oraz ataków typu „zero day”
Filtr antyspamowy	Blokowanie 95% całego spamu
Filtrowanie zawartości stron internetowych	Ponad 9 miliardów skatalogowanych adresów URL

Ochrona prewencyjna — dopasowana do unikatowych wymagań klienta

Konfiguracje pakietu Proventia Network MFS są przeznaczone dla grup użytkowników o różnej wielkości. Obejmują one propozycje zarówno dla dużych przedsiębiorstw, jak i firm małych/użytkowników pracujących w domu (SOHO) oraz środowisk z pracą zdalną/ze strukturą lokalnych oddziałów (ROBO). Oprogramowanie IBM Proventia Management SiteProtector™ umożliwia zarządzanie różnymi aplikacjami z jednej centralnej lokalizacji.

- IBM Proventia Network MFS MX0804: maksymalnie 50 użytkowników
- IBM Proventia Network MFS MX3006: maksymalnie 500 użytkowników
- IBM Proventia Network MFS MX5110: maksymalnie 3000 użytkowników

Więcej informacji

Zobacz, jak oprogramowanie Proventia Network MFS może chronić infrastrukturę firmy przed zagrożeniami internetowymi oraz uprościć zarządzanie bezpieczeństwem. Aby zamówić prezentację na miejscu, skontaktuj się z najbliższym biurem IBM ISS (iss@pl.ibm.com). Więcej informacji o produktach ISS można uzyskać pod adresem:

ibm.com/smb/pl/issproventia



© IBM Polska Sp. z o.o.
Wiśniowy Business Park

ul. 1 Sierpnia 8
02-134 Warszawa
tel. +48 22 878 6777
fax: +48 22 878 6888
Strona główna IBM znajduje się pod
adresem:
ibm.com/pl

Wyprodukowano w Polsce
Wszelkie prawa zastrzeżone
IBM i logo IBM są znakami towarowymi lub
zastrzeżonymi znakami towarowymi firmy
International Business Machines Corporation
w Stanach Zjednoczonych i/lub innych
krajach.

Proventia, Virtual Patch i X-Force są znakami
towarowymi lub zastrzeżonymi znakami
towarowymi firmy Internet Security Systems,
Inc. w Stanach Zjednoczonych i/lub innych
krajach. Internet Security Systems, Inc. jest
w pełni zależną filią International Business
Machines Corporation.

Nazwy innych firm, produktów lub usług
mogą być ich znakami towarowymi lub
znakami usługowymi.

Zawarte w tym dokumencie odniesienia do
produktów lub usług IBM nie oznaczają, że
są one dostępne we wszystkich krajach, w
których działa IBM.

Wszystkie dane pomiarowe zawarte w
niniejszej publikacji uzyskano w określonym
środowisku roboczym i warunkach
opisanych powyżej. Pełnią one wyłącznie
rolę ilustracyjną. Wyniki uzyskane w innych
środowiskach mogą się różnić. Klienci
powinni przeprowadzić własne testy.

* Zwrot pieniędzy (dla usług zdalnej ochrony
— wyłącznie poziom Premium): Jeśli IBM
Internet Security Systems nie wypełni swoich
zobowiązań z tytułu gwarancji zapobiegania
naruszeniom zabezpieczeń, klient otrzyma 50
tys. USD za każdy przypadek niewypełnienia
tych zobowiązań. Szczegółowe informacje
znajdują się w umowie świadczenia usług
przez IBM Internet Security Systems.

** www.wildlist.org