McAfee Complete Endpoint Protection—Business

Mocne, szybkie i proste zabezpieczenia w jednym, łatwym w zarządzaniu pakiecie

Cieszące się największym uznaniem w branży zabezpieczenie urządzeń końcowych, od tradycyjnych komputerów stacjonarnych i laptopów do serwerów pamięci masowej i urządzeń przenośnych. Pakiet McAfee® Complete Endpoint Protection—Business to ekonomiczne i kompleksowe rozwiązanie obejmujące funkcję szyfrowania służące ochronie cennych danych, funkcję behawioralnego zapobiegania atakom w tle wykorzystujące niewykryte dotąd przez producenta luki, a także funkcje zabezpieczeń poczty internetowej, sieci web oraz urządzeń przenośnych przed wyłudzaniem informacji i atakami. Funkcje zarządzania oparte na pojedynczej konsoli oraz interfejsie webowym ułatwiają pracę personelowi informatycznemu oraz umożliwiają błyskawiczną reakcję na zagrożenia.

Kluczowe zalety

- Najwyższej jakości wielowarstwowa ochrona obejmująca zaawansowane zabezpieczenia przed złośliwym oprogramowaniem, narzędzia do wykrywania intruzów na poziomie hosta, narzędzia kontroli urządzeń, hostowy firewall, narzędzia szyfrowania itd.
- Możliwość unifikacji zarządzania we wszystkich punktach końcowych, od maszyn wirtualnych oraz serwerów do komputerów PC i urządzeń przenośnych.
- Działanie w czasie rzeczywistym w celu likwidacji słabych punktów i eliminowania zagrożeń na wczesnych etapach.
- Zabezpieczenie poufnych informacji na wszystkich urządzeniach i nośnikach wymiennych w celu bezpiecznego współdzielenia danych.

Zabezpieczenie punktów końcowych nie jest już problemem dla użytkowników i działów informatycznych. Pakiet McAfee Complete Endpoint Protection — Business zabezpiecza rozwijające się organizacje od chwili wdrożenia do momentu, w którym wymagana jest szybka reakcja. Jedno ujednolicone rozwiązanie obsługuje wszystkie urządzenia w firmie — komputery PC, Mac, systemy Linux, serwery, smartfony oraz tablety. Ograniczenie złożoności, obniżenie kosztów oraz ochrona przed programami typu „rootkit", złośliwym oprogramowaniem atakującym urządzenia przenośne, atakami ukierunkowanymi na witryny WWW i pocztę elektroniczną oraz przed malware. Użytkownik otrzymuje niezawodną i wydajną ochronę, a także proste narzędzia zarządzające, które w tak szerokim zakresie dostarcza tylko firma McAfee, lider na rynku zabezpieczeń urządzeń końcowych.

Kompletna ochrona

Jeden zainfekowany system może zakłócić działanie całej firmy, a same programy antywirusowe nie stawią czoła współczesnym zaawansowanym zagrożeniom. Najlepszą ochroną przed zagrożeniami jest wykorzystanie rozwiązania McAfee Complete Endpoint Protection—Business. W najnowszych **badaniach NSS Labs** firma McAfee otrzymała najwięcej punktów za swe produkty chroniące przed atakami i próbami obejścia zabezpieczeń.

Rozwiązania McAfee szybko znajdują, zamrażają oraz usuwają złośliwe oprogramowanie przy wykorzystaniu wielowarstwowych zabezpieczeń obejmujących zaawansowaną ochronę przed złośliwym oprogramowaniem, narzędzia zapobiegające ingerencji intruzów na poziomie hosta, narzędzia kontroli urządzeń, hostowy firewall oraz narzędzia szyfrowania itd.

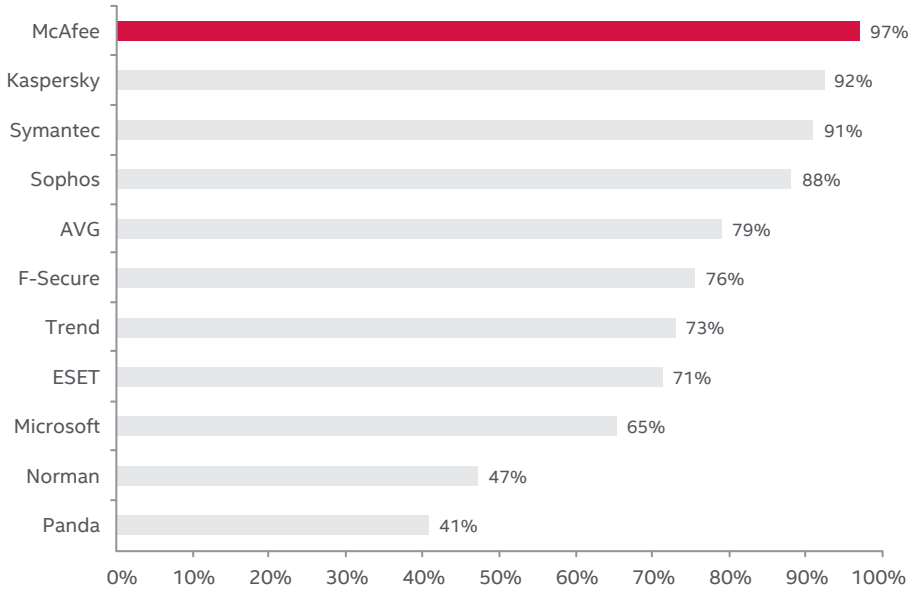
Dzięki proaktywnemu podejściu do ochrony danych Firma McAfee zdobyła najwięcej punktów w badaniach **Gartner Magic Quadrant for Mobile Data Protection** oraz **Magic Quadrant for Endpoint Protection Platforms,** poprzez zapewnienie wielu poziomów zabezpieczeń. Dzięki zaawansowanym funkcjom szyfrowania użytkownik może automatycznie zabezpieczać poufne informacje oraz zapobiegać nieupoważnionemu dostępowi do komputerów PC i Mac, laptopów, maszyn wirtualnych oraz nośników wymiennych. Możliwość ochrony kluczowych zasobów bez negatywnego wpływu na wydajność systemu, a także łatwe zarządzanie i wdrażanie procedur ze scentralizowanej internetowej platformy zarządzania McAfee* ePolicy Orchestrator® (McAfee ePO™).

Działające na poziomie chmury serwis reputacyjny McAfee Global Threat Intelligence zapewnia pełne spektrum informacji i możliwości lepszej ochrony organizacji, a także wgląd w pełen zakres nowych i powstających zagrożeń w czasie rzeczywistym i w pełnym zakresie, tzn. pliki, Internet, poczta i sieć.

intel Security

McAfee: Lider w branży

- Najlepsze wyniki badań Magic Quadrant for Endpoint Protection Platforms nieustannie od 2007 r. (Gartner)
- Najlepsze wyniki badań Magic Quadrant for Mobile Data Protection przez ostatnie cztery lata. (Gartner)
- Najlepsze wyniki w zakresie ochrony przed atakami i próbami obejścia zabezpieczeń. (NSS Labs)
- Najwyższa liczba zablokowanych ataków oraz ogólna skuteczność na poziomie 97% w zakresie ochrony przed próbami obejścia zabezpieczeń. (NSS Labs)



Ilustracja 1 . Wskaźniki zablokowanych ataków (zawierające alternatywne wektory ataku)
Źródło: Raport NSS Labs—*Corporate AV/EPP Comparative Analysis,* 2013

Prostota rozwiązań

Zatrudnienie eksperta ds. bezpieczeństwa w każdym biurze jest niemożliwe, dlatego obsługa naszych rozwiązań jest bardzo prosta. Zarządzanie bezpieczeństwem organizacji z oprogramowaniem McAfee ePO jest bardzo proste —jedno okno daje wgląd w zabezpieczenia oraz możliwość zarządzania politykami określonymi dla wszystkich urządzeń.

Kompletne działanie

Odpowiednio ukierunkowane skanowanie i działania zapewniają bezpieczeństwo, wspierając zamiast hamować firmę. Doskonała wydajność na wszystkich platformach wynika z zastosowania zaawansowanych technik inteligentnego skanowania oraz zarządzania pamięcią, które optymalizują wykorzystanie procesora i pamięci.

Anatomia ataku

Etapy ataku	Jak oprogramowanie McAfee Complete Endpoint Protection—Business chroni firmę
Faza przed atakiem Proaktywne zabezpieczenia ograniczają obszar narażony na atak oraz podatny na zagrożenia.	• Natychmiastowy wgląd w stan zabezpieczeń punktów końcowych z łatwością i skutecznie ogranicza obszar narażony na atak. • Ochrona cennych danych za pomocą funkcji szyfrowania plików, folderów oraz całych dysków.
Pierwszy kontakt Złośliwe oprogramowanie dociera do nieświadomych użytkowników, zwykle poprzez odpowiednio spreparowaną witrynę internetową. Inne punkty dostępu obejmują nośniki wymienne, niechciane wiadomości z portali społecznościowych oraz źle skonfigurowane lub niezabezpieczone sieci bezprzewodowe.	• Funkcje bezpiecznego surfowania, wyszukiwania danych oraz filtrowania zawartości witryn ograniczają możliwość wystawienia na działanie złośliwego oprogramowania lub jego przypadkowego pobrania. • Funkcja kontroli urządzeń blokuje użycie niezatwierdzonych nośników, które mogą być zainfekowane przez złośliwe oprogramowanie. • Funkcja sprawdzania reputacji połączenia sieciowego chroni przed atakami z grup komputerów zainfekowanych złośliwym oprogramowaniem (botnet), atakami typu DoS (denial-of-service) oraz potencjalnie niebezpiecznym transferem danych. • Zabezpieczenia urządzeń przenośnych chronią smartfony i tablety przed złośliwym oprogramowaniem.
Działanie na poziomie lokalnym Złośliwy kod działa na zainfekowanych maszynach w celu wykrycia słabych punktów aplikacji lub systemu operacyjnego. Jeśli złośliwe oprogramowanie obejdzie zabezpieczenia, zapisuje swój kod na dysku.	• Funkcja wykrywania intruzów na poziomie hosta (Hostowy IPS) blokuje ataki i chroni słabe punkty, do których nie zostały wprowadzone poprawki. • Funkcje skanowania dostępu monitorują pamięć i ruch sieciowy. • Bezpieczny kontener przeznaczony do przechowywania wiadomości e-mail otrzymywane na urządzenia przenośne chroni dane firmowe zapisane w urządzeniach.
Konsolidacja obecności Złośliwy kod ukrywa się w systemie. Jest on tak zbudowany, aby przetrwać ponowne uruchomienie systemu oraz ukrywać się przed zabezpieczeniami i użytkownikiem.	• Tradycyjne oprogramowanie zabezpieczające przeciwko wirusom i złośliwym oprogramowaniem. • Hostowy IPS zapewnia ochronę podczas startu systemu oraz poza siecią firmową.
Złośliwe działanie Cel ataku został osiągnięty, tzn. kradzież tożsamości lub własności intelektualnej, a nawet oszustwo bankowe.	• Zapora sieciowa działająca na każdym urządzeniu końcowym uniemożliwiają połączenie ze znanymi złośliwymi sieciami komputerów-„zombie" oraz ograniczają utratę poufnych danych.

Ochrona punktów końcowych przed wszystkimi etapami złośliwego ataku

Oprogramowanie McAfee Complete Endpoint Protection - Business łączy w sobie doskonały zestaw proaktywnych zabezpieczeń chroniących przed dzisiejszymi złożonymi atakami podczas każdej ich fazy. Poniżej opisany jest sposób ograniczenia ryzyka podczas typowego ataku.

Wszechstronna ochrona

Pakiet McAfee Complete Endpoint Protection-Business zapewnia bezpieczeństwo i natychmiastową reakcję na zagrożenia. Obejmuje on wszystkie elementy, upraszcza zarządzanie zabezpieczeniami oraz zapobiega wpływaniu cyber-zagrożeń na działalność firmy, która może skupić się na swym rozwoju. Więcej informacji na ten temat znajduje się na stronie: **www.mcafee.com/complete-endpoint-business.**

Najważniejsze informacje na temat pakietu McAfee Complete Endpoint Protection—Business

Ochrona przed złośliwym oprogramowaniem (PC, Mac, Linux, maszyny wirtualne)	
McAfee VirusScan® Enterprise • Wiodące w branży zabezpieczenie klasy korporacyjnej, chroniące przed złośliwym oprogramowaniem ze zintegrowaną funkcją ochrony przed atakami wykorzystującymi luki nieznane jeszcze producentom.	•
Hostowy IPS oraz Firewall • Ochrona przed atakami wykorzystującymi luki nieznane jeszcze producentom oraz zabezpieczenie nowych podatności. • Ograniczenie konieczności instalowania poprawek.	•
Chmura reputacyjna GTI (Global Threat Intelligence) • Ochrona przed nowymi i powstającymi zagrożeniami na wszystkich poziomach przy użyciu informacji zbieranych w czasie rzeczywistym przez miliony czujników na całym świecie.	•
Bezpieczeństwo w Internecie oraz podczas przesyłania wiadomości	
McAfee SiteAdvisor® z filtrowaniem URL • Ostrzeganie użytkowników przed wejściem na złośliwą witrynę w celu ograniczenia zagrożenia i zachowania zgodności z regulacjami. • Autoryzacja lub blokowanie dostępu do witryny.	•
Zabezpieczenie poczty e-mail przed złośliwym oprogramowaniem i spamem • Ochrona serwerów pocztowych oraz przechwytywanie złośliwego oprogramowania zanim dotrze do skrzynek pocztowych. • Wykrywanie, usuwanie i blokowanie złośliwego oprogramowania na serwerach Microsoft Exchange i Lotus Domino przy użyciu rozwiązania McAfee GroupShield.	•
Ochrona urządzeń przenośnych	
Zabezpieczenie przed złośliwym oprogramowaniem i zarządzanie urządzeniami • Ochrona urządzeń przenośnych, danych oraz sieci. • Uproszczone udostępnienie i blokowanie udostępnienia.	•
Ochrona danych	
Device Control • Zapobieganie utracie poufnych danych poprzez ograniczenie użycia nośników wymiennych.	•
Szyfrowanie całych dysków, plików, folderów i nośników wymiennych • Ochrona poufnych danych zapisanych na komputerach PC, Mac, laptopach, serwerach sieciowych oraz nośnikach wymiennych.	•
Zarządzanie	
McAfee ePO • Zarządzanie procedurami, zgodnością oraz raportowanie z pojedynczej centralnej konsoli.	•

Autoryzowany Dystrybutor rozwiązań
McAfee w Polsce:
Arrow ECS Sp. z o.o.
ul. Stawowa 119, 31-346 Kraków
tel. +48 12 616 43 00
www.arrowecs.pl

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

Intel oraz logo Intel są zastrzeżonymi znakami towarowymi firmy Intel Corporation w Stanach Zjednoczonych i/lub innych krajach. McAfee, logo McAfee, ePolicy Orchestrator, McAfee ePO oraz SiteAdvisor są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy McAfee, Inc. lub jej podmiotów zależnych w Stanach Zjednoczonych i innych krajach. Wszystkie inne znaki i marki wymienione w niniejszej publikacji mogą być własnością innych podmiotów.
Plany produktów, specyfikacje oraz opisy zostały zawarte w niniejszym dokumencie tylko do celów informacyjnych i mogą zostać zmienione bez uprzedzenia. Ich publikacja nie jest objęta jakąkolwiek gwarancją jawną lub domniemaną.
Copyright © 2013 McAfee, Inc. 61569ds_complete-ep-protection-bus_1214_ETMG