

McAfee Endpoint Encryption

Przechowuj swoje dane bezpiecznie

Podstawowe komponenty systemów zabezpieczeń danych dostępne w pakietach ochronnych McAfee®

Rozwiązania do szyfrowania punktów końcowych firmy McAfee chronią cenne dane firmowe na urządzeniach użytkownika końcowego oraz współdzielonych zasobach dzięki zastosowaniu kompleksowych funkcji szyfrowania oraz zintegrowanych i scentralizowanych funkcji zarządzania, konsekwentnych procedur oraz doskonałych narzędzi raportowania

Zapewnienie wydajności przy doskonałej ochronie danych zapisanych na biurowych komputerach stacjonarnych PC i Mac, laptopach oraz współdzielonych serwerach, np. zabezpieczenie zasobów sieciowych, urządzeń USB oraz płyt CD/DVD. Infrastruktura zarządzająca oprogramowania McAfee® ePolicy Orchestrator® (McAfee ePO™) w pełni umożliwia scentralizowane wdrożenia, zarządzanie, administrację politykami, odzyskiwanie haseł, monitorowanie, raportowanie oraz audyty w celu ułatwienia zarządzania, zapewnienia konsekwentnej ochrony oraz obniżenia całkowitego kosztu posiadania (TCO).

Rozwiązania szyfrujące McAfee są kluczowymi komponentami w następujących pakietach McAfee:

- **Pakiet McAfee Complete Data Protection**
- **Pakiet McAfee Complete Data Protection — Advanced**
- **Pakiet McAfee Complete Endpoint Protection — Business**

Kompleksowa ochrona danych

Rozwiązania firmy McAfee służące do ochrony danych oferują wiele poziomów zabezpieczeń przed ich utratą i nieupoważnionym dostępem. Podstawą bezpieczeństwa danych jest szyfrowanie wykorzystywane głównie do uniemożliwienia nieupoważnionego dostępu z zewnątrz, szczególnie w przypadku kradzieży lub zagubienia urządzenia.

Zakres rozwiązań szyfrujących dostępnych w pakietach zabezpieczeń firmy McAfee obejmuje:

- **Szyfrowanie dysku** — Rozwiązanie to szyfruje dane zapisane na komputerach stacjonarnych PC oraz laptopach.
- **Ochrona plików i nośników wymiennych** — Rozwiązanie to szyfruje dane w plikach i folderach sieciowych, nośnikach wymiennych oraz przenośnych urządzeniach pamięci masowych.
- **Zarządzanie natywnym szyfrowaniem** — Rozwiązanie to zarządza funkcją natywnego szyfrowania oferowaną przez Apple FileVault w systemie OS X oraz Microsoft BitLocker w Windows, bezpośrednio z poziomu oprogramowania McAfee ePO.

Kluczowe zalety

- Zabezpieczenie danych na biurowych komputerach stacjonarnych PC oraz Mac, przenośnych laptopach, stacjach roboczych VDI oraz narzędziach do wymiany danych, np. we współdzielonych folderach lub na dyskach flash USB.
- Skuteczne zapewnienie konsekwentnej i stałej ochrony danych na wszystkich urządzeniach.
- Ochrona własności intelektualnej firmy oraz spełnienie wymagań związanych ze zgodnością z regulacjami.
- Uproszczenie procesu zarządzania zabezpieczeniami oraz zapewnienie szerokiego, a zarazem szczegółowego wglądu przy użyciu oprogramowania McAfee ePO do celów scentralizowanego wdrażania, zarządzania, administrowania procedurami, prowadzenia audytów i raportowania.
- Łatwe i konsekwentne wdrażanie firmowych procedur bezpieczeństwa.
- Obniżenie całkowitego kosztu posiadania oraz złożoności poprzez wykorzystywanie kompleksowych rozwiązań do ochrony danych zintegrowanych ze scentralizowanym zarządzaniem.

Rozwiązania McAfee do szyfrowania stacji końcowych

Wiodące w branży rozwiązania do ochrony danych firmy McAfee są dostępne w formie kluczowych komponentów pakietów zabezpieczeń McAfee w celu zapewnienia kompleksowej i niestandardowej ochrony, która spełnia dzisiejsze i przyszłe potrzeby przedsiębiorstw.

Rozwiązania szyfrujące	Kluczowe funkcje
Szyfrowanie dysku Pełne szyfrowanie dysków w laptopach oraz komputerach stacjonarnych PC z systemem Microsoft Windows zapobiega utracie poufnych danych, w szczególności z zagubionych lub skradzionych urządzeń.	<ul style="list-style-type: none">• Doskonała kontrola dostępu dzięki uwierzytelnianiu przed uruchomieniem systemu.• Zastosowanie certyfikowanych algorytmów szyfrujących klasy wojskowej (FIPS, Common Criteria).• Certyfikacja FIPS 140-2 oraz Common Criteria EAL2+ dla wdrożenia Intel Advanced Encryption Standard-New Instructions (AES-NI).• Automatyczne przejrzyste szyfrowanie bez ograniczania wydajności.• Obsługa mieszanych środowisk sprzętowych, łącznie z dyskami SSD.• Obsługa samoszyfrujących napędów Trusted Computing Group (TCG) Opal v1.0.• Lepsza wydajność wynikająca z obsługi technologii Intel AES-NI.
Ochrona plików i nośników wymiennych Wdrażane na poziomie polityki szyfrowanie plików, folderów i nośników wymiennych.	<ul style="list-style-type: none">• Zapewnienie przejrzystego, automatycznego i wdrażanego na poziomie polityki szyfrowania plików i folderów zapisanych lub współdzielonych na komputerach PC, serwerach plików, stacjach roboczych VDI, w e-mailach oraz na nośnikach wymiennych (napędy USB, płyty CD/DVD), a także w plikach ISO.• Uniemożliwienie nieupoważnionego dostępu do informacji na serwerach sieciowych i nośnikach wymiennych.• Zapewnienie mechanizmów współdzielenia kluczy, dzięki którym użytkownicy mogą bezpiecznie współdzielić pliki.• Odczyt i edycja zaszyfrowanych danych na nośnikach bez potrzeby instalowania dodatkowego oprogramowania; zapis danych przy zachowaniu szyfrowania.• Niezależność sprzętowa — możliwość ochrony nawet najtańszych nośników.
Zarządzanie natywnym szyfrowaniem Ochrona danych przy użyciu natywnego szyfrowania Apple (FileVault) na komputerach Mac oraz Microsoft (BitLocker) na komputerach z systemem Windows.	<ul style="list-style-type: none">• Dzięki oprogramowaniu McAfee ePO administratorzy sieci informatycznych mogą zabezpieczyć i zarządzać wszystkimi komputerami Mac z zainstalowanymi systemami OS X Mountain Lion, Mavericks oraz Yosemite, które obsługują Apple FileVault.• Dzięki oprogramowaniu McAfee ePO administratorzy sieci informatycznych mogą zabezpieczyć i zarządzać wszystkimi komputerami z zainstalowanymi systemami Windows 7 oraz 8, które obsługują Microsoft BitLocker.• Kompatybilność z jeszcze nieopublikowanymi poprawkami OS X, uaktualnieniami oraz aktualizacjami oprogramowania firmware Apple.• Mechanizm jednokrotnego logowania ze środowiska przed uruchomieniem FileVault bezpośrednio do OS X.• Aktualizacja z jednej głównej wersji OS X do kolejnej bez konieczności deszyfrowania i ponownego szyfrowania dysku.• Zarządzanie BitLocker w systemie Windows 7 i 8 bezpośrednio z oprogramowania McAfee ePO, bez potrzeby instalacji oddzielnego serwera Microsoft BitLocker Management and Administration (MBAM).

Gartner Magic Quadrant for Mobile Data Protection

Szyfrowanie punktów końcowych to ważna część procesu szyfrowania danych na urządzeniach przenośnych. Firma McAfee zdobywała najwięcej punktów w badaniach **Gartner Magic Quadrant for Mobile Data Protection** przez sześć kolejnych lat i zajmuje pierwsze miejsce pod względem możliwości wykonawczych oraz kompleksowości rozwiązań.¹

McAfee Drive Encryption

Rozwiązania firmy McAfee przeznaczone do szyfrowania dysków twardych chronią cenne dane na laptopach i komputerach stacjonarnych PC przy zastosowaniu pełnego szyfrowania napędu oraz doskonałej kontroli dostępu. Takie zdarzenie jak zagubienie lub kradzież komputera PC lub Mac z zaimplementowanymi funkcjami szyfrowania nie jest zwykle traktowane jako naruszenie zasad ochrony danych, ponieważ dane te są „nie do użycia, nie do odczytania lub nie do odszyfrowania przez nieupoważnione osoby”². Bez zastosowania szyfrowania lub możliwości potwierdzenia ochrony danych z konsoli zarządzającej największym problemem związanym z bezpieczeństwem jest możliwość naruszenia zasad ochrony danych poufnych. Naruszenie zasad ochrony poufnych danych firmy lub klienta może skutkować utratą własności intelektualnej, karami związanymi z brakiem zgodności z normami branżowymi lub z regulacjami itd.

Kluczowe funkcje

- Szyfrowanie wszystkich danych na komputerach PC
- Doskonała kontrola dostępu dzięki uwierzytelnianiu przed uruchomieniem systemu
- Zastosowanie certyfikowanych algorytmów szyfrujących klasy wojskowej (FIPS, Common Criteria)³
- Automatyczne przejrzyste szyfrowanie w tle
- Lepsza wydajność wynikająca z obsługi technologii Intel AES-NI⁴
- Obsługa środowisk z szyfrowaniem na bazie dedykowanego oprogramowania i sprzętu, łącznie z dyskami SSD oraz dyskami samoszyfrującymi⁵
- Automatyczna optymalizacja wdrażania procedur dla każdego klienta, niezależnie od tego, czy komputer PC wykorzystuje szyfrowanie na bazie oprogramowania lub sprzętu, czy jest to urządzenie nowe lub już działające w organizacji
- Obsługa uwierzytelniania wieloskładnikowego poprzez hasła oraz szeroki zakres obsługiwanych tokenów i kart inteligentnych⁶
- Uproszczona aktualizacja systemów operacyjnych (OS) z opcjonalną możliwością tymczasowego zawieszenia uwierzytelniania przed uruchomieniem systemu podczas wprowadzania poprawek do systemu operacyjnego, a także z możliwością wykonania kompleksowego „odświeżenia” systemu bez konieczności deszyfrowania i ponownego szyfrowania danych na komputerze PC⁷
- Współpraca z wybranymi narzędziami śledczymi innych producentów⁸

Korzyści

- **Wiele opcji zapisu i współdzielenia danych** — szyfrowanie danych na dyskach lokalnych, serwerach plików, nośnikach wymiennych i załącznikach do e-maili (niezależnie od tego, czy odbiorca posiada oprogramowanie szyfrujące McAfee) w celu zapewnienia opcji zapisu i współdzielenia danych spełniających szeroki zakres potrzeb.
- **Skalowalne szyfrowanie na bazie polityk** — funkcja szyfrowania jest automatycznie wdrażana zgodnie z firmową polityką bezpieczeństwa informacji, a jej ustawienia można dostosować do potrzeb jednostek, grup lub całych firm. Polityki szyfrowania są tworzone na podstawie oprogramowania McAfee ePO i można je przydzielać użytkownikom w oparciu o informacje uzyskane z Microsoft Active Directory. Klucze szyfrujące są generowane i zarządzane centralnie przez oprogramowanie McAfee ePO. Użytkownik nie może obchodzić procedur.
- **Automatyczne, zawsze aktywne szyfrowanie** — podczas transferu pomiędzy nośnikami danych dokumenty są stale zaszyfrowane, co zapewnia ich bezpieczeństwo bez interwencji użytkownika. Informacje na temat szyfrowania są przenoszone wraz z plikiem w jego „nagłówku”. Pliki są szyfrowane podczas ich tworzenia, co zapobiega utracie ukrytych danych, np. poprzez tymczasowe pliki z tekstem zwykłym oraz pliki stron systemu (pamięć wirtualna z dysku twardego). Szyfrowanie jest zachowane podczas kopiowania, przenoszenia oraz edycji plików na obsługiwanych nośnikach.
- **Proste rozwiązanie dla użytkownika końcowego** — zaszyfrowane pliki mają oryginalne rozszerzenia i dla upoważnionego użytkownika końcowego wyglądają jak „normalne” pliki przy zachowaniu minimalnej ingerencji. Funkcja uwierzytelniania użytkownika jest w pełni zintegrowana z procesem logowania do systemu Microsoft Windows, co oznacza, że każdy token uwierzytelniający wykorzystywany do logowania do Windows jest automatycznie obsługiwany przez plik i funkcję ochrony nośników wymiennych, co zapewnia bardzo przejrzyste i proste rozwiązanie dla użytkownika.
- **Szczegółowa elastyczność** — szczegółowe opcje szyfrowania poszczególnych dokumentów, całych folderów, lokalizacji i/lub typów plików zapewniają bardziej skuteczny wybór cennych danych do szyfrowania w oparciu o obowiązujące procedury, a także możliwość szyfrowania indywidualnych plików na żądanie użytkownika.
- **Współdzielenie zaszyfrowanych dokumentów** — upoważnieni użytkownicy lub grupy użytkowników mogą z łatwością współdzielić zaszyfrowane dokumenty przy użyciu funkcji scentralizowanego zarządzania kluczami oferowanej przez oprogramowanie McAfee ePO. Proces szyfrowania i deszyfrowania odbywa się „na bieżąco” po stronie klienta podczas otwierania i zapisywania chronionych dokumentów. Pliki samorozpakowujące można stosować w załącznikach do e-maili, a odbiorca nie musi instalować żadnego oprogramowania szyfrującego w celu odczytania zaszyfrowanego załącznika, co znacznie zwiększa wygodę obsługi.
- **Szyfrowanie nośników wymiennych** — wszystkie dane (lub ich części) na standardowych, dostępnych na rynku nośnikach USB lub innych tego typu urządzeniach można szyfrować, modyfikować i zapisywać na urządzeniach z oddzielnym uwierzytelnieniem i zachowanym szyfrowaniem, bez potrzeby instalowania dodatkowego oprogramowania lub posiadania lokalnych praw administracyjnych na danym hoście. Dzięki wbudowanej funkcji usuwania żadne pliki nie pozostają na stacji.
- **Wielopoziomowe i łatwe w konfiguracji zabezpieczenia** — użytkownik może stosować metody uwierzytelniania (hasło, karty inteligentne CAC lub PIV), a także metody odzyskiwania danych. Firma McAfee oferuje także oddzielnie zaszyfrowane sprzętowo napędy flash USB i dyski twarde.

File and Removable Media Protection

Typowe zastosowania

Szyfrowanie plików i folderów

- Chcę automatycznie szyfrować wszystkie pliki Microsoft Excel zapisane na laptopie.
- Chcę szyfrować wszystkie pliki zapisane w określonym folderze na laptopie.

Współdzielenie w sieci

- Chcę w przejrzysty sposób szyfrować dany folder sieciowy i zapewnić do niego dostęp tylko dla zespołu działu HR.

Szyfrowanie nośników wymiennych

- Chcę blokować kopiowanie plików na niezasyfrowane napędy wymienne.
- Chcę odczytać dane z zaszyfrowanego urządzenia na komputerze domowym bez zainstalowanego oprogramowania McAfee.
- Chcę umożliwiać dostęp do zaszyfrowanych urządzeń tylko dla osób należących do mojej organizacji.

Pliki samorozpakowujące

- Chcę wysyłać zaszyfrowane załączniki w wiadomościach e-mail do współpracownika oraz umożliwiać mu do nich dostęp bez konieczności instalowania oprogramowania.

File and Removable Media Protection

Funkcje ochrony plików i nośników wymiennych zapewniają automatyczne, przejrzyste i zgodne z obowiązującą polityką szyfrowanie plików i folderów zapisanych lub współdzielonych na komputerach PC, serwerach plików, w e-mailach i na nośnikach wymiennych (np. na napędach USB i płytach CD/DVD).

Korzyści

- **Ochrona nośników wymiennych** — dostępne na rynku urządzenia USB są niewielkie i tanie, co oznacza, że łatwo je zgubić. Szyfrowanie w oparciu o obowiązującą politykę oraz oprogramowanie McAfee ePO umożliwia szybkie i łatwe wdrożenie procedur szyfrowania w całej organizacji w odniesieniu do nośników wymiennych, aby ograniczyć ryzyko utraty danych. Szyfrowanie nośników wymiennych wciąż zapewnia do nich dostęp dla upoważnionych właścicieli poza organizacją, co nie ogranicza możliwości ich przenoszenia.
- **Ochrona lokalnych danych** — zabezpieczenie plików i nośników wymiennych zapewnia dodatkowy poziom ochrony dla komputerów PC i zapisanych na nich poufnych danych, niezależnie do tego, czy dany komputer jest włączony, czy wyłączony.
- **Ochrona danych współdzielonych w sieci** — jeśli cyberprzestępca dostanie się do sieci, indywidualnie szyfrowane pliki i foldery stanowią kolejną warstwę zabezpieczeń, ponieważ zawarte w nich dane są nie do odczytania i nie do użytku przez nieupoważnione osoby. Można także umieszczać indywidualnie zaszyfrowane pliki w indywidualnie szyfrowanych folderach, aby jeszcze bardziej zwiększyć poziom ochrony.
- **Bezpieczne współdzielenie danych ze stronami trzecimi** — podczas współpracy z partnerami, wykonawcami lub innymi podmiotami zewnętrznymi można korzystać z zaszyfrowanych plików i folderów, aby współdzielić poufne dane firmy, własność intelektualną lub duże ilości danych łącznie z plikami ISO, w sposób dostosowany do okoliczności.

Zarządzanie natywnym szyfrowaniem

Funkcja zarządzania natywnym szyfrowaniem umożliwia klientom zarządzanie funkcją natywnego szyfrowania oferowaną przez Apple FileVault w systemie OS X oraz Microsoft BitLocker w Windows, bezpośrednio z oprogramowania McAfee ePO.

Kluczowe funkcje dla systemów Mac

- Zarządzanie FileVault na dowolnym sprzęcie Mac obsługującym systemy OS X Mountain Lion, Mavericks lub Yosemite, bezpośrednio z oprogramowania McAfee ePO.
- Wdrażanie standardowej procedury złożoności haseł dla lokalnych użytkowników OS X.
- Przekazywanie informacji na temat zachowania zgodności w różnych raportach i panelach kontrolnych dostępnych w oprogramowaniu McAfee ePO.
- Dostarczanie klucza przywracania danych FileVault w przypadku konieczności odzyskania danych do wykorzystania narzędzi przywracania dostarczonych przez Apple.
- Umożliwienie administratorom ręcznego importu kluczy przywracania danych FileVault, po tym jak użytkownicy uruchomili już ręcznie FileVault.
- Raport zawierający dowody na zgodność z regulacjami w przypadku zagubienia lub kradzieży laptopa.

Zalety dla systemów Mac

- Możliwość przejścia na kolejną wersję systemu OS X bez konieczności deszyfrowania i ponownego szyfrowania napędu.
- Możliwość jednokrotnego logowania ze środowiska przed uruchomieniem FileVault bezpośrednio do OS X.
- Kompatybilność z jeszcze nieopublikowanymi poprawkami OS X, uaktualnieniami oraz aktualizacjami oprogramowania firmware Apple.
- Wsparcie dla nowego, wchodzącego dopiero na rynek sprzętu Apple.
- Dział informatyczny może wdrażać procedury zabezpieczania hasłami dla OS X.
- Pełna kompatybilność przed uruchomieniem dla wszystkich języków obsługiwanych przez Apple.
- Obsługa nowego trybu BYOD, w którym urządzenie nie jest zarządzane, lecz stan jego zgodności jest zgłaszany w oprogramowaniu McAfee ePO (dobre rozwiązanie dla firm wdrożeniowych).
- Prosta administracja i zarządzanie.

Kluczowe funkcje dla systemów Windows

- Zarządzanie Microsoft BitLocker na sprzęcie obsługiwany przez Windows 7 lub 8, bezpośrednio z oprogramowania McAfee ePO.
- Wsparcie dla Trusted Platform Module (TPM) 1.2 i 2.0.
- Zgodność z wymaganiami FIPS 140-2.
- Obsługa Microsoft eDrive.
- Wygodny interfejs użytkownika do zarządzania FileVault i BitLocker.
- Dostarczanie klucza przywracania danych BitLocker w przypadku konieczności odzyskania danych.
- Przekazywanie informacji na temat zachowania zgodności w różnych raportach i panelach kontrolnych dostępnych w oprogramowaniu McAfee ePO.

Zalety dla systemów Windows

- Zarządzanie BitLocker z oprogramowania McAfee ePO, bez konieczności stosowania oddzielnego serwera Microsoft BitLocker.
- Management and Administration (MBAM).
- Portal samoobsługowy umożliwia użytkownikom przywracanie sprawności ich maszyn.
- Kompatybilność z jeszcze nieopublikowanymi poprawkami systemu Windows oraz aktualizacjami publikowanymi przez Microsoft.
- Wsparcie dla nowego, wchodzącego dopiero na rynek sprzętu Microsoft.
- Wsparcie dla certyfikowanych urządzeń Windows To Go.
- Obsługa trybu BYOD, w którym urządzenie nie jest zarządzane, lecz stan jego zgodności jest zgłaszany w oprogramowaniu McAfee ePO (dobre rozwiązanie dla firm wdrożeniowych).
- Prosta administracja i zarządzanie.

Zintegrowane, scentralizowane zarządzanie poprzez oprogramowanie McAfee ePO

Wielokrotnie nagradzana konsola zarządzająca - oprogramowanie McAfee ePO umożliwia scentralizowane wdrażanie, zarządzanie, administrowanie współdzieloną polityką, odzyskiwanie haseł, monitorowanie, raportowanie, wykonywanie audytów oraz potwierdzenie ochrony. Oprogramowanie McAfee ePO współpracuje z rozwiązaniami w zakresie szyfrowania, ochrony przed utratą danych (DLP) oraz innymi produktami firmy McAfee w celu ułatwienia zarządzania, zapewnienia konsekwentnej ochrony, pełnego wglądu i niskiego całkowitego kosztu posiadania (TCO). Użytkownik może w pełni polegać na tych funkcjach zarządzania bezpieczeństwem.

Kluczowe funkcje

Skalowalność klasy korporacyjnej

- Wydajne wykorzystanie serwera w największych instalacjach.

Uproszczone wdrażanie

- Niższe administracyjne koszty ogólne wynikające z zastosowania pojedynczej konsoli oraz wspólnego agenta administracyjnego dla produktów zabezpieczających dane i punkty końcowe.
- Określenie niechronionych komputerów PC i Mac, a następnie wdrażanie agenta oprogramowania McAfee ePO w celu ochrony tych komputerów zgodnie z obowiązującymi procedurami.
- Kontrole pod kątem niekompatybilnych produktów przed aktywacją klienta McAfee oraz dostarczanie raportów na temat stanu stacji poprzez platformę McAfee ePO.
- Możliwość zdalnej „bezdotykowej” migracji z systemu Microsoft Windows XP do Microsoft Windows 7. Podczas tego procesu dane użytkownika są zachowywane, a maszyna jest cały czas zaszyfrowana.

Współdzielona infrastruktura

- Obsługa mieszanych środowisk szyfrowania, która umożliwia organizacjom stworzenie jednej polityki bezpieczeństwa i infrastruktury zarządzania dla całego środowiska, niezależnie od tego, czy szyfrowanie odbywa się na bazie oprogramowania, czy sprzętu.
- Współdzielenie zadań, polityk oraz infrastruktury zarządzania, niezależnie od tego, które narzędzia szyfrowania zostały wdrożone.

Omówienie rozwiązania

Łatwe w dostosowaniu, szczegółowe polityki

- Konfiguracja polityk per użytkownik (indywidualny użytkownik, współdzielone przez grupy lub cała firma), PC/Mac, lub serwer.
- Możliwość definiowania nowej procedury szyfrowania na dowolnym poziomie organizacji w odpowiedzi na konkretny przypadek użycia.
- Możliwość wykorzystania skryptów do personalizacji szerokiego zakresu zadań zarządzania, np. zarządzania użytkownikami i hasłami.⁹
- Opcjonalna, oparta na politykach blokada zasobów pomiędzy komputerem PC a siecią w przypadku braku komunikacji z siecią firmową.

Dedykowane Panele kontrolne oraz szerokie funkcje raportowania

- Zapis wszystkich informacji na temat audytów i zapisów w dziennikach w konsoli oprogramowania McAfee ePO.
- Generowanie standardowych i niestandardowych raportów na temat całej sieci zarządzanej przez McAfee ePO.

Przydatne w działaniu operacyjnym raporty tworzone przy użyciu konsoli oprogramowania McAfee ePO oraz innych rozwiązań

- Doskonałe narzędzia odzyskiwania danych, łącznie z narzędziami do samodzielnego odzyskiwania danych przez użytkownika.
- Możliwość natychmiastowego podjęcia działań na podstawie raportu w celu wykonania zadań w określonych systemach lub rozwiązania problemów.
- Możliwość wykorzystania funkcji wykrywania niedozwolonych systemów oferowanej przez konsolę oprogramowania McAfee ePO w celu określenia, które maszyny są niezabezpieczone, nawet w przypadku, gdy żaden agent McAfee nie działa na danej maszynie.
- Raport Forrester Research z marca 2010 r. stwierdził, że zastrzeżona wiedza oraz tajemnice firmowe są dwukrotnie cenniejsze od danych depozytowych (np. dane kart płatniczych lub dokumentacja medyczna).¹⁰ Firma McAfee zapewnia doskonałe funkcje kontroli dostępu i szyfrowania w połączeniu z odpowiednim zarządzaniem i potwierdzeniem ochrony, aby firmy mogły mieć pewność, że ich dane są stale bezpieczne.

Rozwiązania firmy McAfee do ochrony danych zapewniają kompleksową ochronę przy zintegrowanym i scentralizowanym zarządzaniu. Te konfigurowalne rozwiązania już dziś ułatwiają organizacjom ochronę dużych ilości danych biznesowych i związanych z zapewnianiem zgodności z regulacjami, a możliwość ich rozbudowania zapewnia także spełnienie przyszłych zmieniających się potrzeb w tym zakresie. Firma McAfee dostarcza rozwiązania do ochrony danych, które umożliwiają użytkownikom skupienie się na tym, na czym znają się oni najlepiej, tzn. na odpowiednim prowadzeniu swej działalności.

Więcej informacji na temat rozwiązań firmy McAfee do szyfrowania punktów końcowych i zarządzania można uzyskać na stronie www.mcafee.com/dataprotection, lub pod numerem telefonu **00800 122 55624**.

1. *Gartner Magic Quadrant for Mobile Data Protection*, wrzesień, 2013 r.: <http://www.mcafee.com/us/independent-reports/gartner-mq-mobile-data-protection.aspx>

2. Publikacja w Rejestrze Federalnym, 24 sierpnia 2009 r. Hhs.gov.

3. Obsługiwane przez McAfee Drive Encryption, tylko na komputerach PC.

4. jak wyżej.

5. jak wyżej.

6. jak wyżej.

7. jak wyżej.

8. Obsługiwane przez McAfee Drive Encryption, tylko na komputerach PC. Rozwiązania śledcze zewnętrznych dostawców dostępne za dodatkową opłatą.

9. Obsługiwane przez McAfee Drive Encryption, tylko na komputerach PC.

10. *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest in Cybercrime Currency*, McAfee 2011.

Intel oraz logo Intel są zastrzeżonymi znakami towarowymi firmy Intel Corporation w Stanach Zjednoczonych i/lub innych krajach. McAfee, logo McAfee, ePolicy Orchestrator oraz McAfee ePO 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.

Copyright © 2014 McAfee, Inc. 61232brf_ep-encryption_0714_fnl_ETMG



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