



# McAfee Total Protection for Data

## Kompleksowa ochrona krytycznych danych

W ostatnich latach na pierwsze strony gazet często trafiały informacje o kradzieży poufnych danych dotyczących klientów różnych przedsiębiorstw. Wielokrotnie były one po prostu wynoszone z firmy na laptopie lub innym przenośnym urządzeniu. Firmy tracące w ten sposób dane mogą być później narażone na poważne konsekwencje, np. ustawowe kary, publiczne ujawnienie informacji, narażenie na szwank wizerunku marki, utrata zaufania klientów oraz straty finansowe. W 2007 r. średnie koszty poniesione przez firmy z powodu utraty danych wyniosły 6,3 mln \$<sup>1</sup>.

W dzisiejszym świecie z wszechobecnym Internetem oraz gwałtownie rosnącą liczbą urządzeń przenośnych ochrona poufnych informacji dotyczących klientów oraz własności intelektualnej musi być najważniejszym priorytetem każdej firmy.

### KLUCZOWE ZALETY

#### Zapobieganie utracie danych (DLP)

- Możliwość wdrożenia centralnie zarządzanej polityki bezpieczeństwa mającej na celu kontrolowanie dostępu, wykorzystania i przenoszenia poufnych danych przez pracowników

#### Szyfrowanie urządzeń wykorzystywanych w firmach

- Szyfrowanie dysków twardych w połączeniu ze skuteczną kontrolą w celu zapewnienia ochrony poufnych danych na wszystkich stacjach roboczych

#### Skuteczne szyfrowanie plików i folderów

- Możliwość korzystania z automatycznego, przejrzystego systemu szyfrowania plików i folderów „w locie”, zanim zostaną one rozprowadzone w organizacji

#### Konsola centralnego zarządzania

- Możliwość określenia firmowej polityki bezpieczeństwa kontrolującej proces szyfrowania, monitorowania i ochrony poufnych danych
- Uproszczenie zarządzania, oszczędność czasu i ograniczenie konieczności szkoleń w celu zwiększenia zwrotu z inwestycji (ROI) i obniżenia kosztów użytkowania systemu (TCO)

#### Zaawansowana funkcja sprawozdań i audytów

- Monitorowanie zdarzeń w czasie rzeczywistym i generowanie szczegółowych sprawozdań
- Możliwość wykazania audytorom, członkom zarządu oraz innym interesariuszom, że w firma działa zgodnie z przepisami wewnętrznymi i ustawowymi

### McAfee Total Protection for Data

McAfee® Total Protection for Data to najbardziej kompleksowe w branży rozwiązanie chroniące poufne dane. Niezawodne szyfrowanie, uwierzytelnianie, funkcje zapobiegania utracie danych oraz środki ochrony zgodne z określoną polityką w dowolnym miejscu i czasie uniemożliwiają nieupoważniony dostęp do poufnych danych oraz ich wyprowadzenie.

#### Zapobieganie utracie danych

Zapobieganie utracie danych zaczyna się od ulepszenia widoczności danych oraz usprawnienia kontroli nawet nad ukrytymi danymi. McAfee Total Protection for Data umożliwia wdrożenie i stosowanie firmowych polityk bezpieczeństwa regulujących i ograniczających sposoby wykorzystywania oraz przenoszenia poufnych informacji przy użyciu standardowych kanałów, np. poczta e-mail, IM, wydruki i USB. Nieważne, czy informacje te są w biurze, w domu lub w podróży – masz nad nimi całkowitą kontrolę.

#### Szyfrowanie na poziomie sprzętu

Zabezpieczaj poufne dane za pomocą rozwiązania zabezpieczającego dla firm. Total Protection for Data wykorzystuje szyfrowanie dysków twardych, które w połączeniu z rygorystyczną kontrolą dostępu dzięki dwuskładnikowemu uwierzytelnianiu przed zainicjowaniem systemu operacyjnego, uniemożliwia nieautoryzowany dostęp do poufnych danych we wszystkich stacjach roboczych, łącznie z laptopami, komputerami kieszonkowymi, smartfonami itd.

#### Skuteczne i przejrzyste szyfrowanie plików i folderów

Określone pliki i foldery są zawsze szyfrowane niezależnie od tego, czy są one edytowane, kopiowane lub zapisywane na takich urządzeniach, jak komputery stacjonarne, laptopy, komputery kieszonkowe, smartfony itd. Total Protection for Data oferuje funkcje szyfrowania zawartości, które automatycznie i przejrzysto szyfrują „w locie” wybrane pliki i foldery, zanim zostaną one rozprowadzone w organizacji. Można także tworzyć i wdrażać centralne polityki dotyczące indywidualnych użytkowników oraz ich grup mające na celu szyfrowanie określonych plików i folderów bez interakcji użytkownika.

#### Scentralizowane zarządzanie zabezpieczeniami oraz zaawansowana funkcja raportowania

Integracja rozwiązania Total Protection for Data z aplikacją ePolicy Orchestrator® (ePO™) jest planowana na rok 2008<sup>2</sup>. Połączenie to umożliwi stosowanie scentralizowanego zarządzania zabezpieczeniami w oparciu o określoną politykę. Dodatkowo zapewni ono także zaawansowane funkcje raportowania umożliwiające spełnienie rygorystycznych wymagań rządowych i branżowych dotyczących prywatności, zapewnienie ochrony danych osobowych zgodnej z podejściem „Safe Harbor” oraz wykazywanie zgodności na potrzeby wewnętrznych i zewnętrznych audytorów, członków zarządu oraz innych kluczowych uprawnionych podmiotów.

<sup>1</sup> Na podstawie badań Ponemon Institute 2007 „Cost of Data Breach” (Koszty utraty danych).

<sup>2</sup> Informacje podane na niniejszej kartce danych na temat przyszłych produktów nie mogą być traktowane jako wiążące przy podejmowaniu decyzji dotyczących ich zakupu.

## WYMAGANIA SYSTEMOWE

### ePO Server

#### Systemy operacyjne

- Microsoft Server 2003 SP1, 2003 R2

#### Wymagania sprzętowe

- Wolne miejsce na dysku: 250 MB
- RAM: 512 MB  
1 GB RAM (zalecane)
- Procesor – Intel Pentium II lub wyższy – minimum 450 MHz

### Punkty końcowe – komputery stacjonarne i laptopy

#### Systemy operacyjne

- Microsoft Vista\* (wszystkie wersje 32- i 64-bitowe)
- Microsoft Windows XP Professional SP1 lub wyższy
- Microsoft Windows 2000 SP4 lub wyższy

\* Dostępne dla DLP w 2008 roku<sup>2</sup>.

#### Wymagania sprzętowe

- Procesor: Pentium III 1 GHz lub wyższy
- RAM: zalecane 512 MB
- Wolne miejsce na dysku: minimum 200 MB
- Podłączenie do sieci: TCP/IP do zdalnego dostępu

### Punkty końcowe Windows Mobile

#### Systemy operacyjne

- Microsoft Windows Mobile 6.0 for Smartphone
- Microsoft Windows Mobile 6.0 for PDA
- Microsoft Windows Mobile 5.0 for Smartphone
- Microsoft Windows Mobile 5.0 for Pocket PC

#### Wymagania sprzętowe

- Procesor: minimum 195 MHz
- RAM: 64 MB
- Podłączenie do sieci: TCP/IP do zdalnej administracji oraz Activesync 4.5 lub wyższa wersja do przewodowej instalacji/aktualizacji polityki

## Funkcje

### Zapobieganie utracie danych

- Kontroluj, jak użytkownicy wysyłają dane, uzyskują do nich dostęp oraz drukują je w sieci, poprzez aplikacje na urządzenia do przechowywania danych: pocztę e-mail, pocztę przeglądaną za pomocą przeglądarki WWW, aplikacje „peer-to-peer”, IM, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, CD, DVD, drukarki, faksy oraz przenośne urządzenia do przechowywania danych.
- Uniemożliwaj wyciekaniu danych w wyniku działania koni trojańskich, robaków oraz aplikacji do udostępnienia plików kradnących informacje na temat tożsamości pracowników.
- Chroń wszystkie informacje, formaty i dane pochodne nawet wówczas, gdy dane są modyfikowane, kopiowane, wklejane, kompresowane lub szyfrowane, nie zakłócając jednocześnie codziennej pracy.

### Szyfrowanie sprzętowe dla firm

- Automatycznie szyfruj całe urządzenia w sposób niewymagający interwencji użytkowników lub ich odpowiedniego wykształcenia, bez wpływu na zasoby systemowe.
- Korzystaj z szyfrowania dysków twardych przy użyciu wielu standardowych algorytmów, łącznie z AES-256 i RC5-1024.
- Za pomocą rygorystycznego wieloskładnikowego uwierzytelniania określaj i weryfikuj autoryzowanych użytkowników.

### Skuteczne szyfrowanie plików i folderów

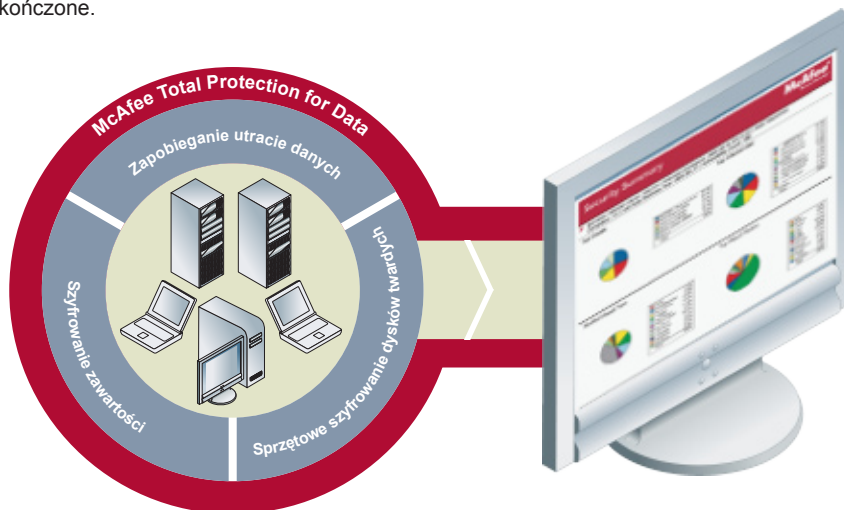
- Chronione pliki przez cały czas pozostają zaszyfrowane dzięki automatycznemu dodawaniu do nich nagłówka przenoszonych wraz z nimi.
- Zabezpieczaj pliki i foldery, niezależnie od tego, gdzie zostały zapisane, np. na lokalnych dyskach twardych, serwerach plików, urządzeniach przenośnych lub nawet w załącznikach wiadomości e-mail.

### Konsola scentralizowanego zarządzania

- Korzystaj z ePO w celu określania filtrowania, monitorowania i blokowania nieupoważnionego dostępu do poufnych danych w odniesieniu do ich zawartości.
- Zarządzaj sprzętowym szyfrowaniem dysków twardych, plików i folderów, stosuj politykę kontroli i zarządzania uaktualnieniami systemu operacyjnego, odzyskuj utracone klucze i spełniaj ustawowe wymagania dotyczące zgodności z przepisami i standardami.
- Synchronizuj własne polityki bezpieczeństwa z Active Directory, Novell NDS, PKI itd.

### Zaawansowana funkcja sprawozdań i audytów

- Wykorzystuj kompleksowe funkcje audytowe w celu wykazania, że urządzenia zostały odpowiednio zaszyfrowane.
- Prowadź dziennik transakcji danymi, aby zarejestrować takie informacje, jak dane nadawcy i odbiorcy, terminy, dowody dotyczące danych, datę i godzinę ostatniego udanego logowania, datę i godzinę ostatniej otrzymanej aktualizacji oraz informacje na temat tego, czy szyfrowanie zostało pomyślnie zakończone.



### McAfee Total Protection for Data

Więcej informacji na temat ochrony danych znajduje się na stronie [www.mcafee.com/data\\_protection](http://www.mcafee.com/data_protection).

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, [www.mcafee.com](http://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. 1-dp-tpd-001-0108