



## McAfee Endpoint Encryption

(poprzednia nazwa SafeBoot® Encryption)

### Zabezpieczaj dane na komputerach stacjonarnych, laptopach, tabletach PC i palmtopach

Zabezpieczenie danych to priorytet numer jeden dla wszystkich dyrektorów ds. bezpieczeństwa informatycznego<sup>1</sup>. McAfee® Endpoint Encryption to skalowalne rozwiązanie zabezpieczające dla całej firmy wykorzystujące silne szyfrowanie oraz rygorystyczną kontrolę dostępu w celu uniemożliwienia nieupoważnionego dostępu do danych znajdujących się w komputerach stacjonarnych, laptopach, tabletach PC, smartfonach i palmtopach.

#### KLUCZOWE ZALETY

##### Silne szyfrowanie i kontrola dostępu

- Dzięki silnemu szyfrowaniu na poziomie dysku oraz silnemu uwierzytelnianiu przed zainicjowaniem systemu operacyjnego możesz chronić urządzenia w Twoim przedsiębiorstwie przed nieupoważnionym dostępem i wyciekami danych
- Przejrzyste szyfrowanie danych „w locie” w sposób niewidoczny dla użytkowników nie wymaga ich szkolenia
- Gwarancja, że wszystkie pliki i foldery pozostają zaszyfrowane przy każdym ich zapisie lub przeniesieniu

##### Zgodność z wewnętrznymi i zewnętrznymi zasadami polityki bezpieczeństwa

- Wdrażaj obowiązkową politykę bezpieczeństwa dla całej firmy
- Zapewnij zgodność z przepisami na temat ochrony danych osobowych
- Kontroluj dostęp użytkowników do aplikacji

##### Łatwe centralne zarządzanie i niższy łączny koszt posiadania

- Korzystaj z szerokiego zakresu możliwości centralnego zarządzania
- Synchronizuj i integruj to rozwiązanie z Active Directory, Novell, LDAP oraz PKI
- Korzystaj z możliwości pojedynczego logowania oraz obsługi popularnych kart elektronicznych i generatorów haseł (tokenów)
- System obsługuje wszystkie popularne języki, rodzaje klawiatur oraz systemy operacyjne Windows

##### Chroń swoje zasoby i markę

Niebezpieczeństwo utraty poufnych danych, łącznie z danymi na temat klientów i pracowników oraz dokumentacji biznesowej, stało się poważnym problemem dla wszystkich firm na całym świecie. W ankiecie przeprowadzonej w 2007 roku przez Ponemon Institute 85 procent respondentów potwierdziło, że w ich firmach miały miejsce przypadki złamania zabezpieczeń i wycieku danych<sup>2</sup>. Zgodnie z danymi Instytutu średnia wielkość kosztów ponoszonych w przypadku tego typu zdarzeń wynosiła 6,3 miliona dolarów<sup>3</sup>.

##### Maksymalne bezpieczeństwo danych dzięki szyfrowaniu na poziomie dysków twardej

Ochrona danych to podstawowy problem współczesnych organizacji. McAfee Endpoint Encryption umożliwia pełną ochronę krytycznych danych Twojej firmy. Rozwiązanie to wykorzystuje rygorystyczną kontrolę dostępu z uwierzytelnianiem przed zainicjowaniem systemu operacyjnego oraz algorytmy z rządową certyfikacją w celu szyfrowania danych na urządzeniach końcowych, tzn. komputerach stacjonarnych, laptopach, tabletach PC, smartfonach i palmtopach. Szyfrowanie i rozszyfrowywanie to proces niezauważalny dla użytkownika wykonywany „w locie” bez żadnego negatywnego wpływu na działanie urządzeń. McAfee Endpoint Encryption doskonale integruje się z istniejącymi systemami firmy i zapewnia sprawność operacyjną znacznie obniżając łączny koszt posiadania systemu.

##### Chroń pliki i foldery, gdziekolwiek się znajdują

Zdefiniuj, które pliki lub foldery mają być zaszyfrowane. McAfee Endpoint Encryption umożliwia administratorom definiowanie zawartości folderów, plików tworzonych przez dane aplikacje lub plików danego typu, które mają zostać zaszyfrowane. Grupy użytkowników otrzymują prawa dostępu do określonych plików i folderów, dzięki czemu mogą w bezpieczny sposób przekazywać je sobie w sieci.

Niezależnie od tego, gdzie dane zostaną zapisane lub przeniesione, są one przez cały czas zaszyfrowane za pomocą zaawansowanej technologii – Persistent Encryption Technology™. Jeśli nieupoważniony użytkownik wykona próbę zapisu pliku przeglądanego na laptopie na nieautoryzowane urządzenie zapisu danych, plik ten pozostanie zaszyfrowany i będzie niezdatny do użytku.

##### Zapewnienie zgodności z przepisami i niższy łączny koszt posiadania systemu

Uniemożliwaj wycieki danych gdziekolwiek znajdują się twoje dane oraz spełniaj wymagania przepisów prawnych, stosując pełny zakres rozwiązań zabezpieczających i szyfrujących, które są zarządzane za pomocą jednej centralnej konsoli. McAfee Endpoint Encryption zapewnia funkcje zarządzania centralnego obejmujące administrację, centralne wdrażanie, zdalne aktualizacje, zarządzanie wymaganą polityką bezpieczeństwa, narzędzia skryptowe, unieważnianie, odzyskiwanie danych, synchronizację itd. Rozbudowane funkcje raportowe pokazują, czy urządzenie było zaszyfrowane, gdy zostało zgubione lub ukradzione, co zapewnia zgodność z obowiązującymi przepisami. Obowiązkowe polityki bezpieczeństwa mogą być przejrzyste wdrażane przez administratorów. McAfee Endpoint Encryption obsługuje także pojedyncze logowanie oraz bezpieczne odzyskiwanie użytkownika offline.

<sup>1</sup> Ankieta Merrill Lynch z 2007 roku dla dyrektorów ds. bezpieczeństwa informatycznego.

<sup>2</sup> Ponemon Institute: „The Business Impact of Data Breach” (Wpływ utraty danych na działanie firmy), 2007.

<sup>3</sup> Ponemon Institute: badania roczne za 2007 r.: „Cost of a Data Breach” (Koszty utraty danych).

## WYMAGANIA SYSTEMOWE

### Komputery, laptopy i tablety PC w punktach końcowych

#### Systemy operacyjne

- Microsoft Vista (wszystkie wersje 32-bitowe i 64-bitowe)
- Microsoft Windows XP
- Microsoft Windows 2000
- Microsoft Windows Server 2003

#### Wymagania sprzętowe

- Procesor: zgodny z Pentium
- RAM: minimum 128 MB
- Wolne miejsce na dysku: dostępne 5-35 MB w zależności od lokalizacji i liczby urządzeń
- Podłączenie do sieci: TCP/IP do zdalnego dostępu

### Urządzenia mobilne

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

### Scentralizowane zarządzanie

#### Systemy operacyjne

- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003

#### Wymagania sprzętowe

- RAM: 128 MB; zalecane 512 MB
- Wolne miejsce na dysku: 200 MB
- Procesor: zgodny z Pentium

### Silne szyfrowanie i kontrola dostępu

Zapobiegaj nieautoryzowanemu dostępowi i korzystaniu z komputerów stacjonarnych, laptopów, tableatów PC, smartfonów i palmtopów wraz z danymi na ich dyskach twardych dzięki szyfrowaniu na poziomie dysków twardych.

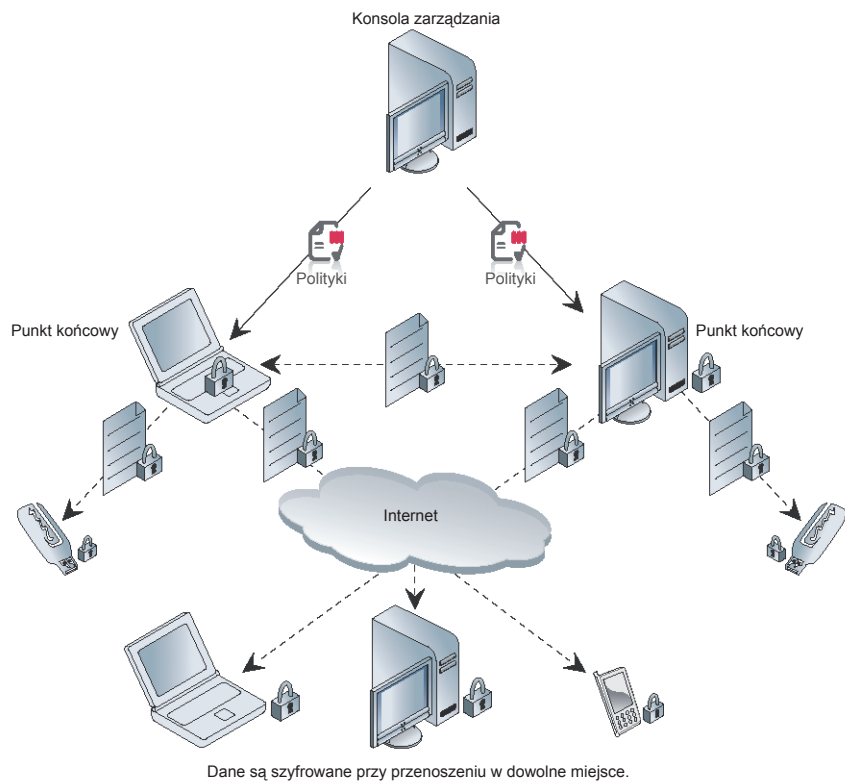
- Weryfikuj użytkownika i urządzenie przed uruchomieniem komputera z zastosowaniem dwuskładnikowego uwierzytelniania przed zainicjowaniem systemu operacyjnego dodatkowo do funkcji uwierzytelniania za pomocą hasła.
- Zyskaj niezrównaną ochronę za pomocą wiodącego w branży i wielokrotnie nagradzanego szyfrowania z wykorzystaniem silnych algorytmów, w tym AES-256 i RC5-1024.
- Szyfruj pliki w niezauważalny dla użytkownika sposób, który jednocześnie nie ma wpływu na codzienne działanie firmy ani nie wymaga specjalnego szkolenia użytkowników.
- Persistent Encryption Technology zagwarantuje, że wszystkie pliki i foldery pozostaną zaszyfrowane niezależnie od tego, gdzie zostały zapisane.

### Zapewnienie zgodności z wewnętrznymi i zewnętrznymi wymaganiami

- Dostępność pełnego audytu zapewniającego zgodność z podejściem „Safe Harbor”, które sprawia, że w przypadku zaszyfrowania danych zgubienie laptopa lub urządzenia USB nie powoduje wycieku danych ani publicznego ujawnienia informacji.
- Tworzenie i wymuszanie reguł bezpieczeństwa
- Można także określać, które typy plików lub folderów mają być szyfrowane bez udziału użytkownika końcowego.
- Korzystanie z certyfikacji FIPS 140-2 i Common Criteria EAL4.

### Łatwe scentralizowane zarządzanie i niższy łączny koszt posiadania

- Łatwe centralne zarządzanie oraz niższe łączne koszty posiadania systemu zapobiegają utracie danych przy wykorzystaniu pełnego zakresu rozwiązań zabezpieczających i szyfrujących, zarządzanych z jednej centralnej konsoli.
- Wykazuj zgodność z przepisami dotyczącymi ochrony danych osobowych oraz chroń swe zasoby i markę, zachowaj lojalność klientów i uzyskaj przewagę konkurencyjną.
- Z łatwością wdrażaj i zarządzaj politykami w całej firmie, oszczędzając w ten sposób czas i pieniądze.
- Zdalnie i bezpiecznie odzyskuj hasła oraz tokeny. Hasło użytkownika może zostać ponownie ustawione po wykonaniu słownej weryfikacji i autentykacji typu pytanie/odpowieź (Challenge/Response), co powoduje oszczędność czasu dla działu wsparcia technicznego.



### McAfee Endpoint Encryption

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 niezależne 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-ee-001-0108