

Trend Micro™

# Enterprise Security for Endpoints

Natychmiastowa ochrona, łatwiejsze zarządzanie i większa elastyczność dla punktów końcowych

W dzisiejszych czasach punkty końcowe są narażone na ponad 2000 nowych i unikalnych ataków złośliwego oprogramowania w ciągu godziny. Nawet częstsze aktualizowanie plików sygnatur nie pozwala stawić czoła takiej liczbie ataków. Ponadto zarządzanie coraz większymi plikami sygnatur spowalnia punkty końcowe i obciąża administratorów. Co więcej, większość rozwiązań służących do ochrony punktów końcowych nie jest w stanie nadążyć za dynamiką rozwoju współczesnych zagrożeń.

Rozwiązanie **Trend Micro Enterprise Security for Endpoints** zapewnia nową, rewolucyjną ochronę przed zagrożeniami — w sieci firmy i poza nią — łącząc światowej klasy narzędzie do walki ze złośliwym oprogramowaniem z ochroną działającą w tzw. chmurze, czyli otoczeniu sieciowym, obsługiwaną przez infrastrukturę Trend Micro™ Smart Protection Network™. Nowa technologia File Reputation (sprawdzanie reputacji plików) w programie OfficeScan przenosi ciężar zarządzania plikami sygnatur do otoczenia sieciowego, zwalniając zasoby systemowe punktów końcowych. Technologia Web Reputation (sprawdzanie reputacji stron internetowych) natomiast chroni punkty końcowe, blokując dostęp do szkodliwych stron internetowych. Enterprise Security for Endpoints stanowi jedno rozwiązanie zapewniające ochronę komputerów stacjonarnych, laptopów, serwerów plików oraz urządzeń smartphone. Elastyczna architektura z wykorzystaniem dodatków typu plug-in, wielowarstwowy system Host Intrusion Prevention oraz większa liczba obsługiwanych platform zapewnia lepszą ochronę, niższe koszty zarządzania i większą elastyczność rozwoju systemu zabezpieczeń.

## NAJWAŻNIEJSZE FUNKCJE

### Nowość! Technologia File Reputation (sprawdzanie reputacji plików)

- Zapytania dotyczące bezpieczeństwa pliku przed jego otwarciem
- Znaczna redukcja obciążenia zadaniami z zakresu zarządzania, jaki jest zwykle związany z rozwiązaniami opartymi na sygnaturach
- Natychmiastowa ochrona punktów końcowych w sieci firmy i poza nią
- Redukcja wpływu na wydajność i zasoby punktów końcowych
- Przekazywanie informacji o zagrożeniach do architektury Smart Protection Network, aby możliwe było szybsze ich sprawdzenie

### Technologia Web Reputation (sprawdzanie reputacji stron internetowych)

- Ochrona przed złośliwym oprogramowaniem internetowym, kradzieżą danych, zmniejszeniem wydajności oraz utratą reputacji
- Uniemożliwienie klientom i aplikacjom dostępu do szkodliwych lub zainfekowanych stron internetowych
- Ustalanie, które z milionów dynamicznie ocenianych witryn internetowych są bezpieczne
- Ochrona w czasie rzeczywistym każdej sieci, bez względu na typ połączenia

### Najlepsza ochrona przed złośliwym oprogramowaniem

- Ochrona przed wirusami, trojanami, robakami, programami spyware oraz ich nowymi wariantami, gdy tylko się pojawią
- Wykrywanie i usuwanie aktywnych i ukrytych rootkitów
- Zabezpieczenie skrzynek pocztowych punktów końcowych dzięki skanowaniu przychodzącej poczty e-mail POP3 i folderów programu Outlook
- Połączenie warstw sieci oraz aplikacji — system Host Intrusion Prevention System (HIPS) zapewnia ochronę przed najnowszymi zagrożeniami

- Ochrona nośników wymiennych zgodnie z zasadami firmowymi za pomocą technologii kontroli urządzeń

### Większa liczba obsługiwanych platform

- Bezproblemowa integracja z infrastrukturą firmy Microsoft® i możliwość bezpiecznej migracji do systemów Windows 7 oraz Windows Server 2008 R2
- Możliwość efektywnego korzystania z zasobów dzięki obsłudze środowisk wirtualnych oraz serwera Citrix Terminal
- Uproszczenie administrowania dzięki korzystaniu z Centrum zabezpieczeń systemu Windows
- Rozszerzenie ochrony na punkty końcowe, na których nie jest stosowany system Windows

### Łatwość zarządzania

- Automatyczne usuwanie z punktów końcowych złośliwego oprogramowania, a także ukrytych lub zablokowanych procesów i wpisów rejestru
- Łatwa integracja z usługą Active Directory w celu uzyskania i synchronizacji informacji o punktach końcowych i zgłaszania zgodności z zasadami
- Obsługa natywnego przetwarzania 64- i 32-bitowego w celu zoptymalizowania wydajności
- Możliwość scentralizowania zarządzania za pośrednictwem jednej konsoli internetowej

### Wydajna ochrona serwerów plików

- Uniemożliwienie rozprzestrzeniania się złośliwego oprogramowania w sieci dzięki blokadzie na poziomie serwera plików
- Skanowanie plików i archiwów oraz ewentualne wykrywanie i usuwanie złośliwego oprogramowania — w czasie rzeczywistym i przy minimalnym obciążeniu serwerów
- Uproszczenie wykonywania zadań dzięki skutecznemu systemowi automatyzacji czynności

## OPROGRAMOWANIE

### Elementy chronione

- Klienci
- Serwery
- Urządzenia przenośne

### Ochrona przed zagrożeniami

- Ochrona antywirusowa
- Ochrona przed spyware
- Ochrona przed rootkitami
- Zapora
- Ochrona przed zagrożeniami z Internetu
- System zapobiegania włamaniom

## GŁÓWNE KORZYŚCI

### Natychmiastowa ochrona

Eliminacja źródła infekcji dzięki blokadzie dostępu do złośliwych plików i stron internetowych

### Zmniejszone ryzyko biznesowe

Ochrona przed infekcjami, kradzieżami tożsamości, utratą danych, awariami urządzeń sieciowych, utratą wydajności oraz naruszeniem zgodności z przepisami

### Kompleksowa ochrona

Pakiet zapewniający pełną ochronę wszystkich typów punktów końcowych

### Niższe koszty generowane przez dział IT

Zmniejszenie nakładu pracy związanego z zarządzaniem środowiskiem IT dzięki technologii sprawdzania reputacji plików, integracji z systemami operacyjnymi Windows oraz obsłudze wirtualizacji

### Architektura z możliwością rozbudowy

Obsługa dodatków, które pozwalają zwiększyć możliwości w zakresie ochrony bez ponownego wdrażania całego rozwiązania

## MINIMALNE WYMAGANIA SYSTEMOWE

## Serwer zarządzania OfficeScan

- Microsoft® Windows® Server 2008, 2003, 2000; Microsoft Windows Storage Server 2003; Microsoft Cluster Server 2003
- Procesor Intel™ Pentium™ 800 MHz, 512 MB pamięci RAM, 1 GB wolnego miejsca na dysku

## Internetowa konsola zarządzania

- Procesor Intel Pentium 300 MHz (500 MHz w przypadku EMC Celerra), 128 MB pamięci RAM, 30 MB wolnego miejsca na dysku

## Obsługa wirtualizacji

- Microsoft Virtual Server 2005 R2 z dodatkiem SP1
- VMware™ ESX/ESXi Server 3.5 (Server Edition); VMware Server 1.0.3 (Server Edition); VMware Workstation i Workstation ACE Edition 6.0

## Ochrona klienta

## Windows® 2008

Procesor Intel™ Pentium™ 1 GHz (1,4 GHz w przypadku wersji 64-bitowej), procesor Intel x64, procesor AMD x64; 512 MB pamięci RAM; 350 MB wolnego miejsca na dysku

## Windows® Vista®

Procesor Intel™ Pentium™ 800 MHz, procesor Intel x64, procesor AMD x64, 1 GB pamięci RAM, 350 MB wolnego miejsca na dysku

## Windows® XP i 2003

Procesor Intel™ Pentium™ 300 MHz, procesor Intel x64, procesor AMD x64, 256 MB pamięci RAM, 350 MB wolnego miejsca na dysku

## Windows® 2000

Procesor Intel™ Pentium™ 300 MHz, 256 MB pamięci RAM, 350 MB wolnego miejsca na dysku

## Ochrona serwera

## Serwer Windows lub NetWare

- Windows Server 2003 Standard/Enterprise/Datacenter Edition; Microsoft Windows 2000 Professional/Server z dodatkiem SP1 lub nowszym; Windows Server 2003 64 bit; Windows Storage Server 2003 64 bit
- Novell NetWare 6.5: komputer klasy serwerowej z procesorem Pentium II lub AMD K7, 512 MB pamięci RAM, 500 MB wolnego miejsca na dysku
- Serwer antywirusowy/Serwer informacji: procesor Intel™ Pentium™ IV 2,5 GHz, procesor Intel 3,0 GHz EM64T lub 64-bitowy procesor AMD 2,0 GHz, 512 MB pamięci RAM, 500 MB wolnego miejsca na dysku
- W przypadku systemu Windows 2008 Standard/Enterprise/Datacenter Edition: 1 GB pamięci RAM, 500 MB wolnego miejsca na dysku

## Serwer Linux

- Red Hat™ Enterprise Linux 4 (AS, ES, WS, Desktop); Red Hat™ Enterprise Linux 5 (Server lub Desktop); Novell SuSE™ Linux Enterprise Server 10
- Procesor Intel™ Pentium™ II 266 MHz lub szybszy, procesor AMD™ Athlon™ lub szybszy, 256 MB pamięci RAM, 75 MB wolnego miejsca na dysku

## DODATKI DLA PROGRAMU OFFICESCAN

Aby zapewnić bezpieczeństwo, które pozostanie aktualne w przyszłości, program OfficeScan można łatwo dostosować do swoich potrzeb. Architektura dodatków zapewnia teraz i w przyszłości najlepszą ochronę, bez względu na to, gdzie i kiedy zostaną one zastosowane, oraz bez potrzeby ponownego wdrożenia całego rozwiązania.

- **Program Intrusion Defense Firewall:** oferuje aktywną ochronę w systemie HIPS oraz eliminowanie luk w zabezpieczeniach, zapewniając pełną ochronę i przestrzeganie zgodności z przepisami.
- **Program Mobile Security:** chroni dane i aplikacje za pomocą centralnie zarządzanych zabezpieczeń urządzeń smartphone i PDA, niezależnie od lokalizacji.
- **Ochrona komputerów Mac:** chroni klientów korzystających z komputerów Macintosh w sieci przed odwiedzaniem szkodliwych stron internetowych i dystrybucją złośliwego oprogramowania — nawet jeśli jest nieszkodliwe dla systemu Mac OS.

## UZUPEŁNIAJĄCE PRODUKTY I USŁUGI

- Rozwiązania InterScan™ Messaging Security
- Rozwiązania InterScan™ Web Security
- Usługi pomocy technicznej Premium firmy Trend Micro™



©2009 Trend Micro Incorporated. Wszelkie prawa zastrzeżone. Trend Micro, logo Trend Micro t-ball, InterScan, OfficeScan, ScanMail, Trend Micro Control Manager i Trend Micro Outbreak Prevention Services są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Trend Micro Incorporated. Pozostałe nazwy produktów i/lub firm mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi odpowiednich właścicieli. Informacje umieszczone w tym dokumencie mogą ulec zmianie bez wcześniejszego powiadomienia.  
[DS01\_ESE\_091204PL]

[www.trendmicro.com](http://www.trendmicro.com)