



Trend Micro™

Core Protection for Virtual Machines

Rozwiązanie zaprojektowane specjalnie do ochrony środowisk VMware

Wirtualizacja serwerów zwiększa wydajność centrów danych, ale również stanowi wyzwanie dla bezpieczeństwa środowiska informatycznego. Tradycyjne rozwiązania z zakresu bezpieczeństwa, stosowane w środowiskach fizycznych, nie są w stanie w pełni chronić środowisk wirtualnych, które są szczególnie narażone na atak, gdy maszyny wirtualne (VM) są w stanie uśpienia lub trybie offline, ponieważ nie mogą one wówczas być chronione przy pomocy skanera antywirusowego i aktualizacji sygnatur. Również działanie zabezpieczeń, pochłaniające znaczne ilości zasobów, takie jak zaplanowane skanowanie systemu, mogą znacznie obniżyć wydajność pracy hosta systemów wirtualnych, szczególnie w przypadku równoczesnego sprawdzania wielu maszyn wirtualnych. Aby w pełni docenić korzyści finansowe i wydajność związaną z wirtualizacją, przedsiębiorstwom niezbędne są rozwiązania stworzone specjalnie w celu ochrony zasobów w wysoce zwirtualizowanych centrach danych.

Rozwiązanie **Trend Micro™ Core Protection for Virtual Machines** umożliwia przedsiębiorstwom uzyskiwanie korzyści finansowych płynących z wirtualizacji bez obniżania bezpieczeństwa centrum danych. Zaprojektowane specjalnie z myślą o środowiskach VMware ESX/ESXi, zapewnia ono ochronę aktywnych oraz znajdujących się w stanie uśpienia maszyn wirtualnych, korzystając z interfejsów API VMsafe. Jest to ochrona wielowarstwowa, oparta na użyciu wyspecjalizowanych, skanujących maszyn wirtualnych, współpracujących w czasie rzeczywistym z działającymi na każdej maszynie wirtualnej agentami ochrony.

NAJWAŻNIEJSZE FUNKCJE

Optymalizacja pod kątem środowisk wirtualnych

- Eliminacja luk w zabezpieczeniach, charakterystycznych dla środowisk wirtualnych.
- Ochrona maszyn wirtualnych aktywnych lub będących w stanie uśpienia za pomocą architektury zabezpieczeń, specjalnie przystosowanej do takich środowisk.
- Większa wydajność maszyn wirtualnych dzięki uruchamianiu procesów zużywających znaczną ilość zasobów, takich jak pełne skanowanie systemu, z osobnego wirtualnego serwera skanowania.
- Ochrona przed rozprzestrzenieniem się zagrożeń poprzez automatyczne skanowanie nowych maszyn wirtualnych.

Światowej klasy ochrona przed złośliwym oprogramowaniem

- Ochrona maszyn wirtualnych w stanie uśpienia oraz gwarancja pełnej aktualizacji zabezpieczeń w celu zapewnienia gotowości w momencie wznowienia pracy.
- Ochrona przed złośliwym oprogramowaniem, unikającym wykrycia przez odinstalowywanie, ograniczanie działania oraz niedozwolone modyfikowanie ochrony antywirusowej.
- Dodatkowa odporność na zagrożenia, dzięki uruchamianiu agenta skanowania na innej maszynie wirtualnej niż skanowana.

Uproszczone zarządzanie

- Integracja z infrastrukturą zarządzania VMware, zmniejszająca złożoność administrowania zabezpieczeniami w środowiskach wirtualnych.
- Stała komunikacja z konsolą zarządzania VMware vCenter, zapewniająca komplet aktualnych informacji o stanie maszyn wirtualnych.
- Automatyczne zlecenie skanowania zabezpieczeń na każdej nowej maszynie wirtualnej, ułatwiające ochronę rozbudowanej infrastruktury maszyn wirtualnych.
- Zarządzanie skanowaniem i aktualizacją sygnatur dla maszyn wirtualnych znajdujących się w stanie uśpienia bez potrzeby ich aktywowania.
- Optymalizacja wymagającego znacznych zasobów pełnego skanowania systemu bez konieczności rekonfiguracji.

Łatwość wdrażania

- Łatwość wdrożenia w środowiskach korzystających z oprogramowania Trend Micro OfficeScan.
- Możliwość centralnego zarządzania z tej samej konsoli programu OfficeScan, która jest używana do zarządzania komputerami stacjonarnymi i serwerami fizycznymi.
- Wygoda korzystania z programu OfficeScan lokalnie na każdej maszynie wirtualnej oraz pełnego skanowania zdalnych systemów za pomocą oprogramowania Core Protection for Virtual Machines.

OPROGRAMOWANIE ZABEZPIECZAJĄCE ŚRODOWISKA WIRTUALNE

Punkty ochrony

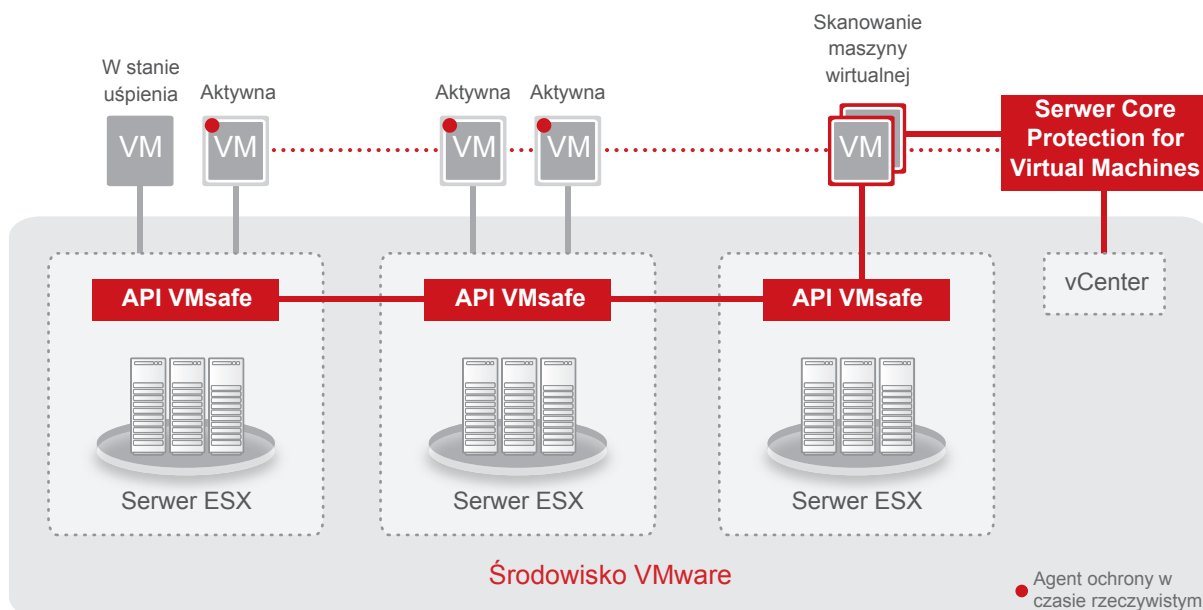
- Maszyny wirtualne

Ochrona przed zagrożeniami

- Zagrożenia internetowe
- Wirusy i robaki
- Trojany

GLÓWNE KORZYŚCI

- Ochrona maszyn wirtualnych, zarówno aktywnych jak i w stanie uśpienia
- Optymalizacja wydajności i maksymalizacja czasu pracy bez uszczerbku dla bezpieczeństwa
- Odporność agenta skanowania na działanie złośliwego oprogramowania
- Zmniejszenie złożoności zarządzania środowiskami wirtualnymi
- Pełna współpraca z oprogramowaniem OfficeScan



Rozwiązanie **Trend Micro Core Protection for Virtual Machines** zabezpiecza środowiska wirtualne przed zagrożeniami nowej generacji, specyficznymi dla tego typu architektury.

WYMAGANIA SYSTEMOWE

Serwer	
System operacyjny	Microsoft™ Windows™ Server 2003 lub 2003 R2 Enterprise Edition w wersji 32-bitowej z dodatkiem Service Pack 1 lub 2
Sprzęt	Procesor 800 MHz, 512 MB pamięci RAM, 1 GB wolnego miejsca na dysku twardym, karta sieciowa
Serwer WWW	Microsoft Internet Information Server (IIS) — na komputerze z systemem Windows Server 2003: wersja 6.0
Konsola internetowa	Procesor 300 MHz, 128 MB pamięci RAM, 30 MB wolnego miejsca na dysku twardym, przeglądarka Microsoft Internet Explorer™ w wersji 6.0 lub Microsoft Internet Explorer™ w wersji 7.0
Agent skanowania	
System operacyjny	System operacyjny Microsoft Windows XP Professional w wersji 32-bitowej, Microsoft Windows Server 2003 lub 2003 R2 Enterprise Edition w wersji 32-bitowej
Sprzęt	Procesor 300 MHz, 256 MB pamięci RAM (512 MB w przypadku agentów aktualizacji), 200 GB wolnego miejsca na dysku twardym (700 MB w przypadku agentów aktualizacji), karta sieciowa
Agent ochrony w czasie rzeczywistym	
System operacyjny	System operacyjny Microsoft Windows 2000 Server, Windows XP Professional w wersji 32-bitowej, Windows Server 2003 (lub 2003 R2) w wersji 32-bitowej, Microsoft Windows Server 2003 (lub 2003 R2) w wersji 64-bitowej, Windows Server 2008, Windows Vista Enterprise w wersji 32-bitowej, Windows Vista Business w wersji 64-bitowej
Właściwości maszyny wirtualnej	1 procesor, 128 MB pamięci RAM, 200 MB wolnego miejsca na dysku twardym, karta sieciowa w technologii VMware
Obsługiwane platformy	
VMware	VMware VI3 (ESX 3.5, ESXi, vCenter 2.5), vSphere 4.0

Uwaga: do korzystania z rozwiązania Core Protection for Virtual Machines jest niezbędne oprogramowanie VMware vCenter.

PRODUKTY UZUPEŁNIAJĄCE

Bezpieczeństwo serwerów

- Deep Security
- ServerProtect

Endpoint Security

- OfficeScan Client/Server Edition

Produkty zapewniające bezpieczeństwo w sieci Web

- InterScan™ Web Security Virtual Appliance

Produkty ochrony komunikacji

- InterScan™ Messaging Security Virtual Appliance



©2009 Trend Micro Incorporated. Wszelkie prawa zastrzeżone. Trend Micro, logo t-ball firmy Trend Micro oraz TrendLabs 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. [DS01CPVM_090622IT]

www.trendmicro.com