

Trend Micro™

Deep Security 7.5

Ochrona serwerów i aplikacji dla dynamicznych centrów danych

Przedsiębiorstwa coraz częściej pracują online i przetwarzają coraz więcej danych związanych z połączeniami z partnerami, pracownikami, dostawcami czy klientami, a aplikacje są coraz bardziej narażone na cyberataki. Te ukierunkowane zagrożenia są coraz większe i bardziej wyrafinowane, zatem wymagania dotyczące właściwego zabezpieczenia danych stają się coraz bardziej rygorystyczne. Firmy potrzebują bezwzględnie bezpieczeństwa, które umożliwi modernizację centrów danych, w których stosowana jest wirtualizacja i usługi cloud computing, bez zmniejszania ich wydajności.

Rozwiązanie Trend Micro Deep Security zapewnia zaawansowane zabezpieczenie serwerów fizycznych, wirtualnych i pracujących w otoczeniu sieciowym oraz maszyn wirtualnych. Bez względu na to, czy wdrażane w postaci oprogramowania, urządzeń wirtualnych lub w ramach podejścia hybrydowego, rozwiązanie to redukuje koszty, ułatwia zarządzanie oraz zapewnia silną ochronę wirtualnych maszyn bez wdrożonego agenta. Rozwiązanie Deep Security, łączące wiele modułów ochrony w jednym, skonsolidowanym rozwiązaniu, spełnia także wiele wymagań dotyczących zgodności, w tym siedem głównych wymagań zgodności ze standardem PCI.

ARCHITEKTURA

NOWOŚĆ! Deep Security Virtual Appliance. Nie zakłócając pracy wdraża reguły zabezpieczeń na maszynach wirtualnych VMware vSphere, co umożliwia ochronę przed złośliwym oprogramowaniem bez konieczności wdrażania agentów oraz zapewnia ochronę poprzez systemy wykrywania intruzów (IDS), usługi zapobiegania włamaniom (IPS), ochronę aplikacji internetowych, kontrolę aplikacji oraz ochronę za pomocą zapory sieciowej — we współdziałaniu z programem Deep Security Agent, jeśli jest taka potrzeba, w celu monitorowania spójności i kontroli dziennika.

Deep Security Agent. Ten niewielki element oprogramowania, zainstalowany na chronionym serwerze lub maszynie wirtualnej, wdraża reguły zabezpieczeń centrum danych (IDS/IPS, ochrona aplikacji internetowych, kontrola aplikacji, zaporę sieciową, monitorowanie spójności oraz kontrola dziennika).

Deep Security Manager. Zaawansowane scentralizowane zarządzanie umożliwia administratorom tworzenie profili ochrony i zastosowanie ich na serwerach, monitorowanie ostrzeżeń i działań zapobiegawczych podejmowanych w odpowiedzi na zagrożenia, przesyłanie aktualizacji zabezpieczeń do serwerów oraz tworzenie raportów. Nowa funkcja oznaczania zdarzeń ułatwia zarządzanie dużą liczbą zdarzeń.

Security Center. Nasz wykwalifikowany zespół specjalistów do spraw zabezpieczeń pomaga użytkownikom zabezpieczyć się przed najnowszymi zagrożeniami, tworząc i dostarczając aktualizacje zabezpieczeń chroniące przed nowo odkrytymi zagrożeniami. Portal dla klientów zapewnia dostęp do aktualizacji programu Deep Security Manager.

Smart Protection Network. Rozwiązanie Deep Security jest zintegrowane z infrastrukturą bezpieczeństwa nowej generacji, działającą w otoczeniu sieciowym. Dzięki temu zapewnia ochronę przed pojawiającymi się zagrożeniami w czasie rzeczywistym, poprzez ciągłą ocenę i porównanie informacji o zagrożeniach i reputacji witryn, źródeł poczty elektronicznej i plików.

WDRAŻANIE I INTEGRACJA

Szybki proces wdrożenia pozwala wykorzystać istniejące inwestycje w infrastrukturę informatyczną i zabezpieczenia

- Integracja z interfejsami API rozwiązań vShield Endpoint oraz VMsafe™, a także VMware vCenter umożliwia szybkie wdrożenie na serwerach ESX w postaci urządzeń wirtualnych w celu natychmiastowej i niezakłócającej pracy ochrony maszyn wirtualnych vSphere.
- Szczegółowe dane dotyczące zdarzeń związanych z bezpieczeństwem na poziomie serwera są dostarczane do systemu SIEM, w tym ArcSight™, Intellictics, NetIQ, RSA Envision, Q1Labs, Loglogic, a także innych systemów poprzez wiele opcji integracji.
- Integracja katalogów w skali całego przedsiębiorstwa łącznie z usługą Microsoft Active Directory.
- Oprogramowanie agenta można łatwo zainstalować za pomocą standardowych mechanizmów dystrybucji oprogramowania, takich jak Microsoft® SMS, Novell Zenworks oraz Altiris.

GŁÓWNE KORZYŚCI

Zapobieganie naruszeniu bezpieczeństwa danych i występowaniu zakłóceń w działaniu firmy

- Zapewnienie linii obrony na poziomie serwera fizycznego, wirtualnego lub w otoczeniu sieciowym
- Ochrona przed znanymi i nieznanymi lukami w zabezpieczeniach aplikacji i systemów operacyjnych
- Ochrona aplikacji w sieci przed wstawianiem kodu do baz danych SQL i atakami sieciowymi za pośrednictwem skryptów
- Blokowanie ataków na systemy przedsiębiorstwa
- Identyfikowanie podejrzanych działań i zachowań, co umożliwia aktywne przeciwdziałanie

Pomoc w zapewnieniu zgodności z normą PCI oraz innymi przepisami i standardami

- Zgodność z siedmioma głównymi standardami ochrony danych PCI oraz wieloma innymi wymogami przepisów prawnych
- Dostarczanie szczegółowych raportów, które można łatwo kontrolować, zawierających informacje na temat udaremnionych ataków oraz stanu zgodności z zasadami bezpieczeństwa
- Zmniejszenie nakładu pracy i oszczędność czasu potrzebnego na przeprowadzenie audytu

Zmniejszenie kosztów operacyjnych

- Optymalizacja oszczędności kosztów wynikających z wirtualizacji lub środowiska cloud computing poprzez połączenie zasobów serwerowych
- Uprozczone zarządzanie środowisk serwerów i maszyn wirtualnych przez zapewnienie mechanizmów zabezpieczających przed złośliwym oprogramowaniem i innych mechanizmów zabezpieczeń w konfiguracji bez wdrożonych agentów
- Ułatwiona administracja dzięki zautomatyzowanemu zarządzaniu zdarzeniami związanymi z bezpieczeństwem na wszystkich serwerach
- Zapewnienie ochrony przed lukami w zabezpieczeniach w celu określenia priorytetów bezpiecznego kodowania oraz ekonomicznej implementacji niezaplanowanych poprawek
- Eliminacja kosztów instalacji oprogramowania na wielu klientach dzięki centralnemu zarządzaniu, wielofunkcyjnemu agentowi lub urządzeniu w wersji wirtualnej

MODUŁY DEEP SECURITY

NOWOŚĆ! Ochrona środowisk VMware przed złośliwym oprogramowaniem bez wdrażania agenta

- Integracja nowych interfejsów API VMware vShield Endpoint do ochrony maszyn wirtualnych VMware przed wirusami, spyware, trojanami i innym złośliwym oprogramowaniem przy zerowym obciążeniu systemu.
- Optymalizacja operacji zabezpieczających w celu uniknięcia przeciążeń związanych z zabezpieczeniami często występujących przy skanowaniu całego systemu i aktualizacjach sygnatur.
- Ochrona odporna na penetrację przez zaawansowane ataki dzięki odizolowaniu złośliwego oprogramowania od zabezpieczeń przed złośliwym oprogramowaniem.

Zaawansowana kontrola pakietów danych

- Sprawdza ruch przychodzący i wychodzący pod kątem odchyłeń w protokołach, naruszeń reguł lub treści sygnalizującej atak.
- Działa w trybie wykrywania lub zapobiegania w celu ochrony systemów operacyjnych i eliminowania luk w zabezpieczeniach aplikacji w firmie.
- Dostarcza automatyczne powiadomienia o sprawcy ataku, czasie ataku oraz o tym, jakie luki próbowano wykorzystać.

Wykrywanie intruzów i ochrona

- Chroni przed znanymi i najnowszymi atakami, zabezpieczając przed nieograniczonym wykorzystywaniem znanych luk.
- Automatycznie w ciągu kilku godzin zapewnia ochronę przed nowo wykrytymi zagrożeniami, obejmuje ochroną tysiące serwerów w ciągu kilku minut bez konieczności ponownego uruchamiania systemu.
- Obejmuje natychmiastową ochroną ponad 100 aplikacji, bazy danych, serwery internetowe, e-mail oraz serwery FTP.

Ochrona aplikacji internetowych

- Zapewnia zgodność z przepisami (PCI DSS 6.6), aby chronić aplikacje internetowe i przetwarzane za ich pomocą dane.
- Zabezpiecza przed wstawianiem kodu do baz danych SQL, wstawianiem skryptów na stronach i innymi lukami w zabezpieczeniach aplikacji internetowych.
- Zapewnia ochronę luk w zabezpieczeniach do momentu wprowadzenia poprawek w kodzie.

Kontrola aplikacji

- Zapewnia szczegółowy wgląd w aplikacje uzyskujące dostęp do sieci lub kontrolę nad nimi.
- W celu identyfikacji złośliwego oprogramowania uzyskującego dostęp do sieci wykorzystuje reguły kontroli aplikacji.
- Zmniejsza ryzyko ataków na serwery.

Dwustronna zapora sieciowa z analizą stanów połączeń

- Zmniejsza narażony na atak obszar serwerów fizycznych, wirtualnych i działających w otoczeniu sieciowym poprzez precyzyjne filtrowanie, projektowanie odrębnych reguł dla poszczególnych sieci i zmianę działania w zależności od lokalizacji dla wszystkich protokołów opartych na IP i typów ramek.
- Zarządza centralnie regułami zapory serwera, w tym szablonami dla popularnych typów serwerów.
- Zapobiega atakom typu DoS i wykrywa skanowanie w celach rozpoznawczych.

Monitorowanie spójności

- Monitoruje krytyczne pliki systemu operacyjnego i aplikacji, takie jak katalogi, klucze rejestru i wartości, w celu wykrywania szkodliwych i nieoczekiwanych zmian.
- Wykrywa modyfikacje istniejących systemów plików oraz przypadki utworzenia nowych plików i zgłasza je w czasie rzeczywistym.
- Oferuje wykrywanie na żądanie, wykrywanie zaplanowane lub w czasie rzeczywistym, sprawdza właściwości plików (PCI 10.5.5) i monitoruje określone katalogi.

Kontrola dziennika

- Zbiera i analizuje wpisy dziennika systemu operacyjnego i aplikacji dotyczące podejrzanych zachowań, zdarzeń związanych z bezpieczeństwem i zdarzeń administracyjnych z całego centrum danych.
- Zapewnia zgodność z przepisami (PCI DSS 10.6), aby zoptymalizować identyfikację ważnych zdarzeń związanych z bezpieczeństwem znajdujących się w wielu wpisach w dzienniku.
- Przekazuje zdarzenia do systemu SIEM lub scentralizowanego serwera dzienników w celu korelacji, raportowania i archiwizacji.

CHRONIONE PLATFORMY

Microsoft® Windows®

- 2000 (wersja 32-bitowa)
- XP (wersja 32-bitowa/64-bitowa)
- XP Embedded
- Windows 7 (wersja 32-bitowa/64-bitowa)
- Windows Vista (wersja 32-bitowa/64-bitowa)
- Windows Server 2003 (wersja 32-bitowa/64-bitowa)
- Windows Server 2008 (wersja 32-bitowa/64-bitowa)
- Windows Server 2008 R2 (wersja 64-bitowa)

Solaris™

- System operacyjny: 8, 9, 10 (platforma 64-bitowa SPARC), 10 (wersja 64-bitowa x86)

System Linux

- Red Hat® Enterprise 4.0, 5.0 (wersja 32-bitowa/64-bitowa)
- SUSE® Enterprise 10, 11 (wersja 32-bitowa/64-bitowa)

UNIX®*

- AIX 5.3, 6.1
- HP-UX® 10, 11i v2/v3

* Dostępne tylko monitorowanie spójności i kontrola dziennika.

WIRTUALIZACJA

- **Urządzenie wirtualne:** VMware vSphere 4.1
- **VMware®:** VMware ESX 4.1 Server (wirtualizowany system operacyjny)
- **Citrix®:** XenServer
- **Microsoft®:** HyperV
- **Sun:** Pojemniki Solaris 10 (Solaris 10 Containers)

GLÓWNE CERTYFIKATY I KLUCZOWI PARTNERZY

- Common Criteria EAL 3+ (EAL 4 w trakcie)
- Certyfikat spełniania norm PCI (PCI Suitability Testing for HIPS) firmy NSS Labs
- Wirtualizacja VMware
- Program ochrony aplikacji firmy Microsoft
- Certyfikowany partner firmy Microsoft
- Novell
- Współpraca z firmą Oracle
- Współpraca biznesowa z firmą HP
- Certyfikat zgodności z systemem Red Hat

Wymagania centrum danych	Zaawansowana kontrola pakietów danych			Zapora sieciowa	Monitorowanie spójności	Kontrola dziennika	NOWOŚĆ! Zabezpieczenia przed złośliwym oprogramowaniem
	IDS/IPS	Ochrona aplikacji internetowych	Kontrola aplikacji				
Ochrona serwera	●			●	●	○	●
Bezpieczeństwo aplikacji internetowych	●	●			○	●	
Zabezpieczenia wirtualizacji	●	○		●	●	○	●
Wykrywanie podejrzanych zachowań	○		●	●	●	●	
Bezpieczeństwo środowiska cloud computing	●	○		●	●	●	●
Raportowanie zgodności	○	●	○	○	●	●	
Oparte na agentach	●	●	●	●	●	●	
Urządzenie wirtualne	●	●	●	●			●

● Niezbędne ○ Korzystne



©2010 Trend Micro Incorporated. Wszelkie prawa zastrzeżone. Trend Micro, logo t-ball firmy Trend Micro, OfficeScan oraz Trend Micro Control Manager 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 zawarte w niniejszym dokumencie mogą ulec zmianie bez powiadomienia. [DS03DeepSecurity7.5_100721PL]

www.trendmicro.com