

Trend Micro™

# Deep Security 7

## Ochrona serwerów i aplikacji dla dynamicznych centrów danych

Przedsiębiorstwa coraz częściej pracują online i przetwarzają coraz więcej danych, a aplikacje są coraz bardziej narażone na cyberataki niezależnie od zadań, do jakich są przeznaczone (połączenie z partnerami, personelem, dostawcami czy klientami). Te ukierunkowane zagrożenia są coraz większe i bardziej wyrafinowane, dlatego właściwe zabezpieczenie danych staje się coraz bardziej istotne każdego dnia. Firma potrzebuje bezkompromisowego bezpieczeństwa umożliwiającego modernizację centrów danych, w których stosowana jest wirtualizacja i usługi cloud computing, bez zmniejszania wydajności.

Firma Trend Micro oferuje zoptymalizowane i zintegrowane produkty, usługi i rozwiązania, zapewniające efektywną kosztowo ochronę ważnych danych i zmniejszenie ryzyka. Deep Security to oprogramowanie do kompleksowej ochrony serwerów i aplikacji, które umożliwia samoobronę środowiskom fizycznym, wirtualnym oraz środowiskom cloud computing. Bez względu na to, czy wdrażane jest jako oprogramowanie, urządzenie wirtualne, czy hybrydowo, rozwiązanie to redukuje koszty, ułatwia zarządzanie oraz nie zakłócając normalnej pracy wzmacnia ochronę maszyn wirtualnych. Oprogramowanie Deep Security spełnia także wiele wymogów dotyczących zgodności z przepisami, w tym sześć głównych wymogów zgodności z normą PCI, dzięki zaporze na poziomie warstwy aplikacji internetowej, systemom IDS/IPS, monitorowaniu integralności plików oraz segmentacji sieci.

### ARCHITEKTURA

- **Deep Security Virtual Appliance.** Nie zakłócając pracy wdraża reguły zabezpieczeń na maszynach wirtualnych VMware vSphere, stosowane do zapewnienia ochrony poprzez systemy wykrywania intruzów (IDS), usługi zapobiegania włamaniami (IPS), ochronę aplikacji internetowych, kontrolę aplikacji oraz ochronę za pomocą zapory sieciowej — we współdziałaniu z programem Deep Security Agent 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.
- **Centrum zabezpieczeń.** 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.

### WDRAŻANIE I INTEGRACJA

#### Szybka instalacja pozwala wykorzystać istniejące inwestycje w infrastrukturę informatyczną i zabezpieczenia

- Integracja maszyn wirtualnych VMware z oprogramowaniem VMware vCenter oraz ESX Server umożliwia importowanie informacji operacyjnych i firmowych do programu Deep Security Manager oraz zastosowanie drobiazgowo dokładnej ochrony w korporacyjnej infrastrukturze VMware.
- Integracja z interfejsami VMsafe™ umożliwia szybką instalację na serwerach ESX w postaci urządzenia wirtualnego w celu natychmiastowej ochrony w tle 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.
- Zarządzanie z możliwością konfigurowania zmniejsza lub eliminuje konieczność zmian w zaporze sieciowej, które zazwyczaj są potrzebne w przypadku systemów centralnego zarządzania. Umożliwia inicjowanie komunikacji programowi Manager lub Agent.
- Oprogramowanie agenta można łatwo zainstalować za pomocą standardowych mechanizmów dystrybucji oprogramowania, takich jak Microsoft® SMS, Novel Zenworks oraz Altiris

### GŁÓWNE KORZYŚCI

#### Zapobieganie naruszeniu bezpieczeństwa danych i występowaniu złośliwych w działaniu firmy

- Zapewnienie linii obrony na poziomie serwera fizycznego, wirtualnego lub w środowisku typu cloud.
- Ochrona przed znanymi i nieznanymi lukami w zabezpieczeniach w aplikacjach i systemach 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 sześcioma 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 usługi cloud computing poprzez połączenie zasobów serwerowych.
- Ułatwiona administracja dzięki zautomatyzowanemu zarządzaniu zdarzeniami związanymi z bezpieczeństwem.
- Zapewnienie ochrony przed lukami w zabezpieczeniach w celu określenia priorytetów bezpiecznego kodowania oraz ekonomicznej implementacji niezaplanych poprawek.
- Eliminacja kosztów instalacji oprogramowania na wielu klientach dzięki centralnemu zarządzaniu, wielofunkcyjnemu agentowi lub urządzeniu w wersji wirtualnej.

## MODUŁY DEEP SECURITY

### Dogłębne sprawdzanie pakietów danych

- Sprawdza ruch przychodzący i wychodzący pod kątem odchyłeń w protokołach, treści sygnalizującej atak lub przypadków naruszeń reguł.
- Działa w trybie wykrywania lub zapobiegania w celu ochrony systemów operacyjnych i eliminowania luk w zabezpieczeniach aplikacji w firmie.
- Chroni przed atakami na poziomie warstwy aplikacji, przed wstawianiem kodu do baz danych i wstawianiem skryptów na stronach.
- Dostarcza cennych danych, m.in. o sprawcy ataku, czasie ataku oraz o tym, jakie luki próbowano wykorzystać.
- Automatycznie powiadamia administratorów o zaistniałym zdarzeniu.

### 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, pocztę elektroniczną oraz serwery FTP.
- Inteligentne reguły zapewniają ochronę przed najnowszymi nieznanymi zagrożeniami atakującymi niewykryte luki, wykrywając nietypowe dane protokołu zawierające złośliwy kod.

### 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.
- Zapewnia elastyczne i praktyczne monitorowanie za pomocą raportów włączeń/wyłączeń, które można łatwo edytować.

### Ochrona aplikacji w sieci Web

- 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 przed lukami w zabezpieczeniach do momentu wprowadzenia poprawek w kodzie.

### Kontrola aplikacji

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

### Dwustronna zapora sieciowa

- Zmniejsza powierzchnię ataków serwerów fizycznych, serwerów w środowisku typu cloud oraz serwerów wirtualnych.
- Zarządza centralnie regułami zapory serwera, w tym szablonami dla popularnych typów serwerów.
- Udostępnia funkcje szczegółowego filtrowania (adresy IP oraz MAC, porty), reguły projektowe dla kart sieciowych, rozpoznawanie lokalizacji.
- Zapobiega atakom typu DoS i wykrywa skanowanie w celach rozpoznawczych.
- Obejmuje wszystkie protokoły oparte o IP (TCP, UDP, ICMP itd.) i wszystkie typy ramek (IP, ARP itd.).

### Kontrola dziennika

- Zbiera i analizuje wpisy dziennika systemu operacyjnego i aplikacji dotyczące zdarzeń związanych z bezpieczeństwem.
- 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 centralizowanego serwera dzienników w celu korelacji, raportowania i archiwizacji.
- Wykrywa podejrzane zachowania, gromadzi zdarzenia związane z bezpieczeństwem i działania administracyjne w centrum danych i tworzy zaawansowane reguły, wykorzystując składnię OSSEC.

## CHRONIONE PLATFORMY

### Microsoft® Windows®

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

### Solaris™

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

### System Linux

- Red Hat® Enterprise 3.0 (32-bitowy), 4.0, 5.0 (wersja 32-bitowa/64-bitowa)
- SUSE® Enterprise 9, 10 (wersja 32-bitowa)

### UNIX® \*

- AIX 5.3
- HP-UX® 10, 11i v2, 11i v3

\* Dostępne tylko monitorowanie spójności i kontrola dziennika

## WIRTUALIZACJA

- VMware®: Serwer VMware ESX (wirtualizowany system operacyjny)
- Citrix®: XenServer Guest VM
- Microsoft®: HyperV Guest VM
- Sun: Partycje Solaris 10 OS

## GLÓWNE CERTYFIKATY I KLUCZOWI PARTNERZY

- Common Criteria EAL 3+
- PCI Suitability Testing for HIPS (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

## MODUŁY DEEP SECURITY

Wymagania centrum danych	Dogłębne sprawdzanie pakietów danych			Zapora sieciowa	Monitorowanie spójności	Kontrola dziennika
	IDS/IPS	Ochrona aplikacji w sieci Web	Kontrola aplikacji			
Ochrona serwera	●			●	●	○
Bezpieczeństwo aplikacji w sieci Web	●	●			○	●
Bezpieczeństwo wirtualizacji	●	○		●	●	○
Wykrywanie podejrzanych zachowań	○		●	●	●	●
Bezpieczeństwo środowiska cloud computing	●	○		●	●	●
Raportowanie zgodności	○	●	○	○	●	●

● Zasadnicze ○ Korzystne



©2009 Trend Micro Incorporated. Wszelkie prawa zastrzeżone. Trend Micro, logo Trend Micro t-ball, OfficeScan i 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. [DS01DeepSecurity7\_091019PL]

www.trendmicro.com