Zatrudnij **Deep Security** do automatycznej ochrony Twoich serwerów

Dbanie o właściwy poziom zabezpieczeń przed cyberzagrożeniami powinno być w dzisiejszych czasach traktowane priorytetowo. Być może zapewnienie bezpieczeństwa oznacza dla Ciebie konieczność zmierzenia się z wieloma problemami, m.in.:

- Brak czasu na podjęcie odpowiednich środków zabezpieczających
- Ograniczone zasoby ludzkie, które mogłyby skutecznie zadbać o cyberbezpieczeństwo
- Korzystanie ze starych, niewspieranych przez producenta, systemów operacyjnych
- Utrata ciągłości biznesowej w związku z pracami prowadzonymi na środowisku serwerowym
- Opracowanie kompleksowej strategii działań, chroniącej przed wszelkiego rodzaju zagrożeniami.

Jeśli tak, to naszym rozwiązaniem dla Ciebie jest **Deep Security japońskiej firmy Trend Micro**. Pod tą nazwą kryje się zestaw kilku narzędzi przeznaczonych do ochrony serwerów: fizycznych (bare metal), wirtualnych, chmurowych i kontenerowych. Deep Security to:

- **Elastyczne rozwiązanie** umożliwiające dostosowanie poziomu ochrony do aktualnych potrzeb, możliwość wyboru odpowiadającej konfiguracji trzech modułów
- **Automatyczna ochrona** serwerów w czasie rzeczywistym, bez obciążania maszyny
- **Zarządzanie politykami** bezpieczeństwa za pomocą intuicyjnej konsoli.

Korzyści z wdrożenia:

- **Minimalizacja czynnika ludzkiego** – możliwość uniknięcia zaniedbań, np. nieprzeprowadzenia aktualizacji systemu/aplikacji na czas, nieumyślnego uruchomienia złośliwego oprogramowania.

- **Bieżąca kontrola zabezpieczeń** – możliwość generowania raportów działania zabezpieczeń w dowolnym momencie. Możliwość zmiany polityk bezpieczeństwa na bardziej restrykcyjne lub łagodne.

- **Automatyzacja procesów zapewniających cyberbezpieczeństwo** – odciążenie działów IT, które mogą skupić się na innych działaniach. Pomocne zarówno w firmach z mniejszymi, często jednoosobowymi działami IT, jak i w takich, które dysponują rozbudowanymi środowiskami serwerowymi, wymagającymi ochrony.

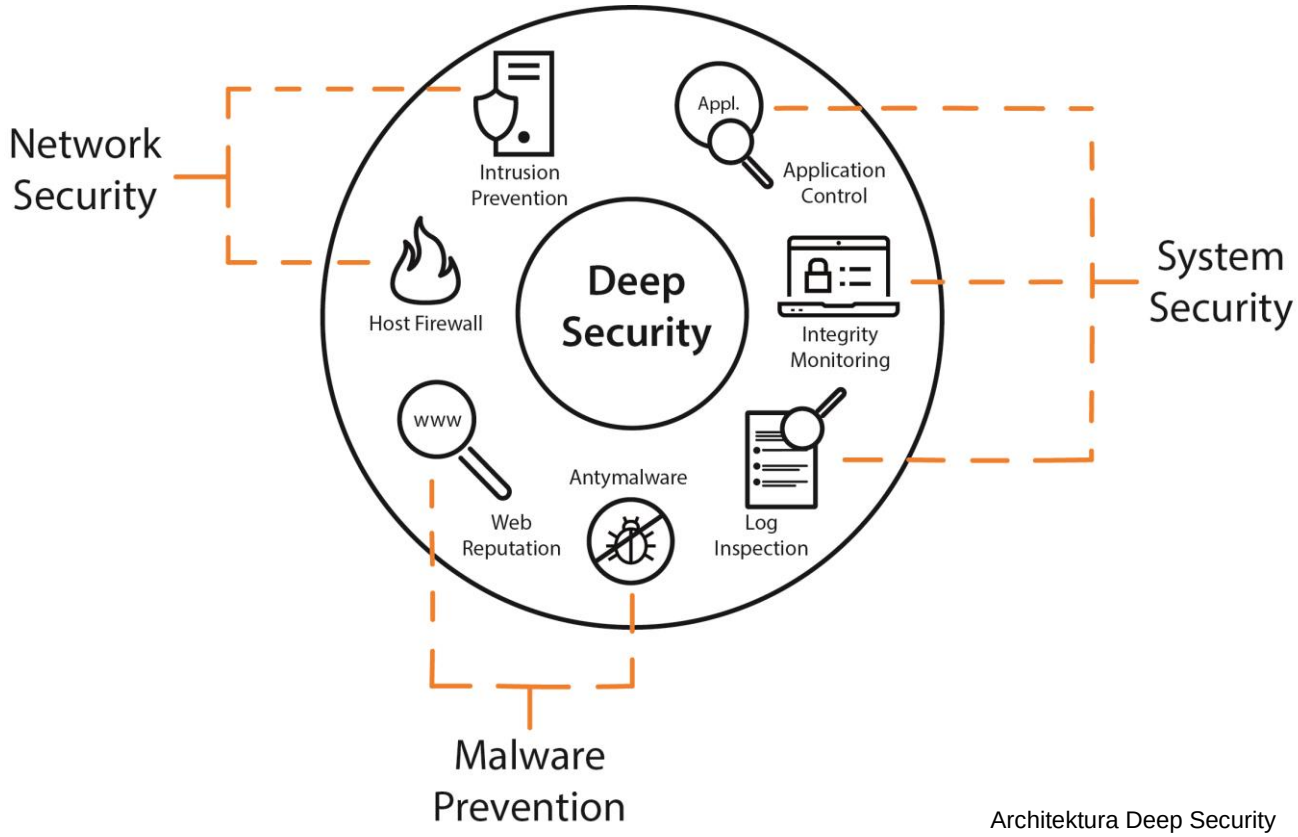
- **Łatwe zarządzanie** – wygodna konsola zarządzająca, ulokowana w profesjonalnym Atman Data Center WAW-1. Zarządzanie wszystkimi narzędziami Deep Security z jednego miejsca. Ponadto zapewniony materiał onboardingowy oraz wiedza specjalistów.

- **Ciągłość działania** – brak konieczności wyłączania/restartowania serwerów w celu załatania luk bezpieczeństwa systemów operacyjnych i aplikacji.

- **Kompleksowe rozwiązanie** – Deep Security chroni przed lukami w zabezpieczeniach, złośliwym oprogramowaniem i podejrzanymi działaniami w środowisku serwerowym.

ATM S.A., ul. Grochowska 21a, 04-186 Warszawa
tel. 22 51 56 100, info@atman.pl

www.atman.pl



Architektura Deep Security

Moduł Network Security – składa się z dwóch narzędzi: Firewall i Intrusion Prevention, zapewnia ochronę przed atakami sieciowymi i lukami bezpieczeństwa systemów i aplikacji.

Firewall

- Elastyczna i konfigurowalna zapora chroniąca punkty końcowe sieci
- W momencie instalacji modułu jest nieaktywna

Intrusion Prevention (Virtual Patching)

Wirtualne patchowanie w sposób automatyczny chroni serwer przed zagrożeniami związanymi z nieaktualizowanym oprogramowaniem, poprzez „nakładanie" patchy (łatek) do czasu wykonania aktualizacji:

- Chroni serwery, które nie mają wgranych aktualizacji wydanych przez producenta (Windows, Linux)
- Ma zastosowanie przy webserwerach, silnikach bazodanowych, frameworkach
- Chroni serwery pracujące na starych systemach operacyjnych, które nie mają już wsparcia producenta i oficjalnych aktualizacji (Windows 2003, Windows 2008 Server, Debian 6 itp.)
- Dzięki uruchamianemu raz na dobę skanerowi rekomendacji zapewnia stale najświeższą bazę danych nowych podatnościach
- Eliminuje problem przestojów w działaniu serwerów i nieprzeprowadzenia aktualizacji na czas

Czy wiesz, że?

61 dni – średnio o tyle szybciej klienci Deep Security otrzymują „łatę bezpieczeństwa" w porównaniu do osób korzystających z aktualizacji pochodzących od producenta. Często od momentu wykrycia podatności do przeprowadzenia ataku mija zaledwie kilka godzin lub dni. W tym przypadku czas reakcji ma ogromne znaczenie!

Deep Security

Moduł Malware Prevention – składa się z dwóch narzędzi: Web Reputation i Antymalware, zapewnia ochronę przed złośliwym oprogramowaniem i zainfekowanymi witrynami.

Web Reputation
Skanuje witryny w poszukiwaniu złośliwego kodu i kategoryzuje treść na stronie. Poprzez tę analizę narzędzie zezwala bądź blokuje wejście na witrynę.

Antymalware
chroni przed każdym rodzajem złośliwego oprogramowania, w tym m.in.:

- **Spyware** – złośliwe oprogramowanie szpiegujące, które potajemnie obserwuje działania użytkownika komputera bez jego zgody i zgłasza je autorowi oprogramowania. Zazwyczaj jest nieświadomie pobierane podczas instalacji legalnych aplikacji bądź otwarcie zainfekowanych załączników w mailach.
- **Keylogge**r – oprogramowanie, które rejestruje naciśnięcia klawiszy użytkownika na klawiaturze i wysyła je do hackera, który w ten sposób wchodzi w posiadanie poufnych informacji, loginów, haseł.
- **Ransomware** – oprogramowanie, które blokuje/szyfruje urządzenie i dane oraz żąda okupu. Jedno z częściej używanych narzędzi przez cyberprzestępców.

Czy wiesz, że?
Uznaje się, że przeciętny antywirus jest w stanie wychwycić tylko 45% wszystkich ataków. Antymalware to zdecydowanie bardziej skuteczne rozwiązanie.

Moduł System Security – składa się z trzech narzędzi: Application Control, Integrity Monitoring, Log Inspection, wykrywa podejrzane działanie na serwerze.

Application Control
Uniemożliwia uruchomienie złośliwego oprogramowania, stale monitorując zmiany na chronionych serwerach. Blokuje pliki i skrypty zidentyfikowane jako nieznane.

Integrity Monitoring
Skanuje serwer w poszukiwaniu nieoczekiwanych zmian wartości kluczy rejestru, zainstalowanego oprogramowania, plików. Narzędzie wykrywa zmiany i informuje o nich użytkownika.

Log inspection
Narzędzie pozwala wychwycić incydenty bezpieczeństwa np. błędy aplikacji, zamknięcia systemu, nadmierną liczba logowań, zmiany polityk.

Zobacz, jak niewiele kosztuje bezpieczeństwo Twoich serwerów:

Moduł	Koszt
Network Security (Intrusion Prevention, Firewall)	**75 zł/miesiąc/serwer**
Malware Prevention (Antymalware, Web Reputation)	**40 zł/miesiąc/serwer**
System Security (Application Control, Integrity Monitoring, Log Inspection)	**75 zł/miesiąc/serwer**
Wszystkie moduły	**160 zł/miesiąc/serwer**