Panda
GateDefender **Integra**

Twoja pierwsza linia ochrony

Różnorodność i złożoność zagrożeń pochodzących z internetu sprawia, że konieczne jest skuteczne ich blokowanie zanim przenikną do wnętrza sieci firmowej.

Kompleksowa ochrona sieci firmowej

Panda GateDefender Integra jest wielofunkcyjnym urządzeniem zapewniającym ochronę sieci przed wszystkimi rodzajami zagrożeń w małej i średniej firmie. Łatwe w instalacji oraz administracji rozwiązanie umieszczane jest na styku sieci lokalnej z internetem. Zastosowanie ochrony w tej części infrastruktury IT skutecznie ją zabezpiecza, zmniejszając jednocześnie obciążenie serwerów i stacji roboczych.

Panda GateDefender Integra skutecznie chroni przed malwarem, spamem, umożliwia filtrowanie ruchu przychodzącego i wychodzącego oraz zapobiega włamaniom. Posiada intuicyjny, graficzny interfejs Administratora. Wykorzystanie innowacyjnej technologii Kolektywnej Inteligencji (przetwarzanie w chmurze) i modułów wiodących dostawców rozwiązań security (Cloudmark, Cobion, Snort) zapewnia wysoką skuteczność rozwiązania.

Obok funkcji ochronnych urządzenie może pełnić rolę Routera pozwalającego zarządzać ruchem wewnątrz organizacji, a także bramy VPN zapewniającej bezpieczne połączenie zdalnych użytkowników i oddziałów terenowych z centralą firmy.

Ochrona Antymalware
Ochrona plików oraz załączników poczty

Firewall
Zabezpieczenie sieci lokalnej

Ochrona Antyspam
Blokowanie niepożądanej korespondencji

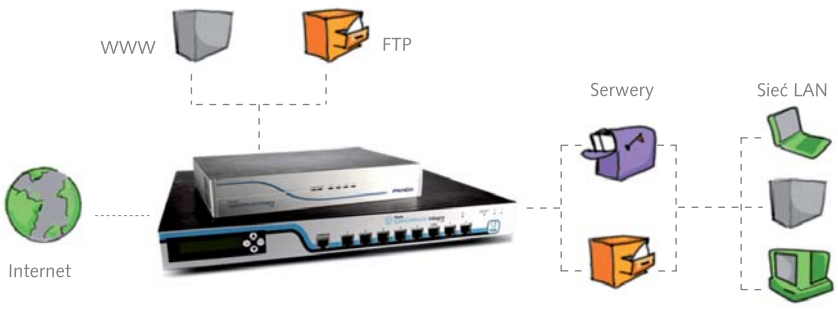
IPS
Analiza ruchu sieciowego

Filtrowanie ruchu SMTP/POP3
Skanowanie treści oraz załączników wiadomości pocztowych

VPN
Bezpieczny zdalny dostęp

Filtrowanie ruchu HTTP/FTP
Blokowanie treści pobieranych z internetu

Filtrowanie stron WWW
Blokowanie niepożądanych stron internetowych



Kompletna ochrona styku sieci firmowej z internetem.

Proaktywna ochrona zawartości.
Filtr treści poddaje analizie dane przychodzące i wychodzące z organizacji. Zabezpiecza sieć firmową przed wyciekiem poufnych informacji – funkcjonalność DLP (Data Loss Prevention).

Wysoka efektywność ochrony.
Obszerna baza reguł systemu IPS zawiera ponad 5000 zasad i wykorzystuje dodatkowy zbiór sygnatur złośliwego oprogramowania.

Brak limitów i nieograniczona ilość połączeń VPN.
Wysoka wydajność mechanizmów skanujących zainstalowanych w urządzeniu pozwala skanować pliki o dowolnej wielkości. Umożliwia też zestawienie dowolnej ilości tuneli VPN.

Główne zalety

- **Znaczne zmniejszenie obciążenia sieci.** Skuteczność wykrywania spamu na poziomie 98% redukuje obciążenie serwerów pocztowych, dodatkowo filtr treści oraz system IPS pozwalają wyeliminować niepożądany ruch sieciowy.
- **Wzrost wydajności pracowników.** Ograniczony dostęp do witryn WWW niezwiązanych z wykonywaną pracą wpływa na optymalizację wykorzystania pasma oraz zwiększa efektywność pracowników.
- **Redukcja kosztów operacyjnych.** Łatwa implementacja urządzenia, intuicyjna konsola zarządzania, automatyczne aktualizacje oraz system powiadomień pozwalają wyeliminować zbędne zaangażowanie personelu IT.
- **Regularne, automatyczne aktualizacje.** Reguły i sygnatury złośliwych programów, moduł IPS oraz filtr witryn internetowych aktualizowane są automatycznie co 90 minut, zaś reguły modułu Antyspam co minutę.

Panda GateDefender **Integra**	Zalecana liczba użytkowników	Przepustowość Firewall	Ilość gniazd sieciowych
GateDefender **Integra SB** 	Do 80 stacji	**400 Mbps**	4x 10/100/1000
GateDefender **Integra 300** 	Do 250 stacji	**850 Mbps**	8x 10/100/1000

Ochrona przed zagrożeniami ukrytymi w treści

Zabezpieczenie Antymalware

Rozwiązanie oferuje aktywną i pasywną ochronę przeciw wszelkim zagrożeniom transmitowanym za pomocą sześciu najszerzej stosowanych protokołów internetowych (HTTP, FTP, SMTP, POP3, IMAP4 i NNTP). Funkcja zapewnia ochronę przed: wirusami, robakami, oprogramowaniem szpiegującym, phishingiem, dialerami, narzędziami hakerskimi, trojanami, żartami i lukami bezpieczeństwa. Wbudowana heurystyka blokuje wirusy, na które nie ma jeszcze szczepionki.

Filtr zawartości

Moduł pozwala zblokować potencjalnie niebezpieczne treści w plikach skompresowanych, wykonywalnych, o formatach ActiveX itd. Daje możliwość oddzielnej konfiguracji ochrony protokołów pocztowych, grup wiadomości oraz transferu plików internetowych. Administrator może dowolnie konfigurować typy plików oraz rodzaje zawartości, które mają być odfiltrowane.

Zabezpieczenie Antyspam

Wszystkie wiadomości pocztowe są znakowane techniką wielofunkcyjnej analizy (Bayes, heurystyka, reguły Administratora). Niepożądana korespondencja może zostać wyeliminowana lub odpowiednio oznaczona zanim trafi do skrzynki odbiorczej adresata. Odbiorca oszczędza czas, który musiałby przeznaczyć na jej rozpoznanie. Ograniczenie zbędnej poczty zmniejsza także ruch w sieci.

Filtr witryn WWW

Administrator sieci może definiować kategorie nieproduktywnych witryn WWW oraz tworzyć własne listy stron, do których dostęp będzie udzielany lub blokowany. Dostęp do informacji o wykorzystywanych zasobach sieciowych organizacji pozwala zapobiegać przeglądaniu niepożądanych lub niebezpiecznych stron internetowych przez pracowników.

Ochrona przed zagrożeniami pochodzącymi z sieci

Zapora Firewall

Moduł odpowiada za blokowanie połączeń niezgodnych z ustaloną przez Administratora polityką bezpieczeństwa dzięki czemu zapewnia ochronę przed bezpośrednimi atakami z Internetu. Odpowiednia konfiguracja modułu sprawia, że filtrowaniu może podlegać także lokalny ruch sieciowy. Analiza ruchu realizowana jest dwupoziomowo:

1. **Statycznie (na poziomie sieci)**

   W oparciu o reguły dotyczące danych przychodzących i wychodzących, definiowane przez Administratora.

2. **Dynamicznie (na poziomie aplikacji)**

   Analiza stanu – monitorująca status i zawartość komunikacji podstawowej wszystkich protokołów oraz statusy, limity czasowe, ustanowione połączenia itp.

   Szczegółowa analiza pakietów – skanująca zawartość pakietów w celu analizy przesyłanych wiadomości.

Usługa VPN

Urządzenie umożliwia szyfrowanie danych, chroniąc transfer przed osobami niepowołanymi. Rozwiązanie działa w konfiguracjach host-host, host-sieć oraz sieć-sieć i obsługuje protokoły IPsec, SSL, L2TP oraz PPTP w trybie serwera oraz SSL i Ipsec w trybie klienta.

System zapobiegania włamaniom do sieci (IPS)

Detekcja zagrożeń opiera się na pliku znanych prób włamań (baza ponad 5000 reguł). System skanuje pakiety IP, ICMP, TCP i UDP. Administrator może określić próg czułości dla każdej ze stosowanych zasad i skonfigurować automatyczną blokadę wykrytych ataków redukując w ten sposób liczbę fałszywych alarmów.

Partner Panda Security