Panda SecurityforBusiness

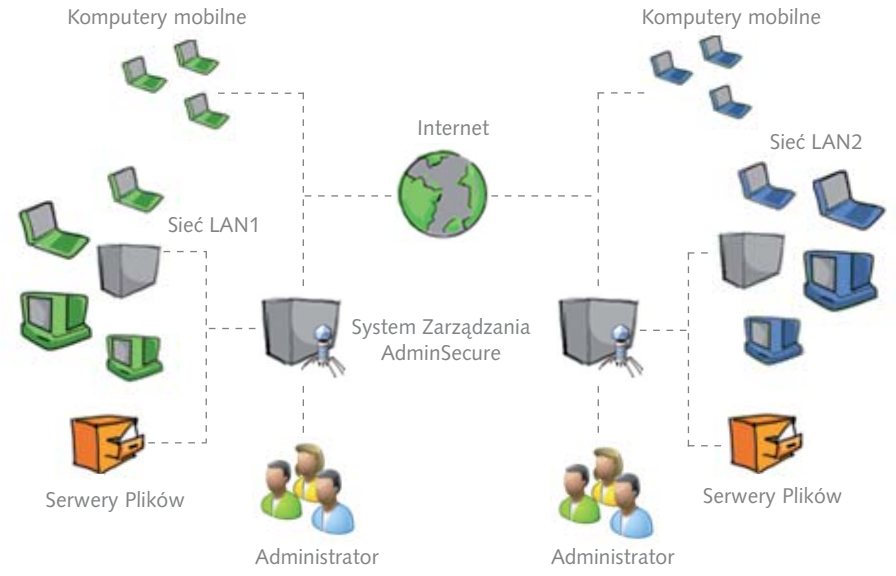
Więcej niż ochrona antywirusowa

Ponad 72% firm wykorzystujących oprogramowanie antywirusowe jest zainfekowanych. Tradycyjna ochrona antywirusowa dziś już nie wystarcza.

Panda Security for Business zawiera wszystkie niezbędne moduły zabezpieczeń stacji roboczych oraz serwerów plików: ochronę antymalware, system kontroli treści, personalny system firewall, system wykrywania ataków sieciowych (HIPS), system kontroli aplikacji, mechanizmy blokowania niepożądanych funkcji systemu operacyjnego oraz kontroli dostępu do zasobów sieciowych. Rozwiązanie wprowadza pełny system bezpieczeństwa, w średniej oraz dużej organizacji.

Panda Security for Business łączy tradycyjne metody analizy antywirusowej (prowadzone z wykorzystaniem baz sygnatur) z zaawansowanymi technikami analizy behawioralnej (TruPrevent) oraz innowacyjną technologią Kolektywnej Inteligencji (tzw. przetwarzania w chmurze). Połączenie różnych technik analizy zapewnia skuteczność ochrony przed znanymi oraz nowymi zagrożeniami na poziomie 99,9% (AV-Test XI.2009).

Administracja aplikacjami ochronnymi realizowana jest przy pomocy lokalnej konsoli zarządzającej AdminSecure. Skalowalny system pozwala na wdrożenie wydajnego mechanizmu administracji w sieciach składających się z 15 jak i 1500 komputerów. Intuicyjna w obsłudze konsola umożliwia szybkie i skuteczne zarządzanie siecią lokalną, jednostkami zdalnymi jak i poszczególnymi komputerami mobilnymi wchodzącymi w skład rozproszonej struktury sieci.



Wydajne zarządzania siecią lokalną, jednostkami zdalnymi oraz komputerami mobilnymi.

Ochrona Antymalware
Ochrona plików oraz załączników poczty

Ochrona Antyspam
Blokowanie niepożądanej korespondencji

Filtrowanie zawartości
Skanowanie wiadomości oraz plików

Kontrola aplikacji
Blokowanie niepożądanego oprogramowania

Kontrola dostępu do sieci
Blokowanie podejrzanych komputerów

Firewall
Zabezpieczenie zasobów lokalnych

HIPS (analiza pakietów)
Wykrywanie ataków sieciowych

Ochrona ruchu WWW
Bezpieczna komunikacja HTTP/FTP

Ochrona poczty
Bezpieczna komunikacja SMTP/POP3

Audyt bezpieczeństwa
Weryfikacja aktualnego poziomu ochrony

Główne zalety

- **Kontrola aplikacji oraz systemu.** Opatentowana technologia TruPrevent pozwala na blokowanie działania niepożądanych aplikacji takich jak BitTorrent, eMule, Gadu-Gadu, Skype. Umożliwia także blokowanie wybranych funkcji komputera (np. Bluetooth, WiFi, USB) podnosząc tym samym poziom bezpieczeństwa organizacji.
- **Automatyczny audyt bezpieczeństwa.** Cykliczny audyt bezpieczeństwa sieci, realizowany przez niezależny mechanizm skanujący, daje rzetelny obraz poziomu ochrony organizacji. Pozwala wykryć luki w systemie bezpieczeństwie oraz utajone infekcje.
- **Centralny system zarządzania.** Intuicyjna konsola administracyjna zapewnia kontrolę nad całym systemem bezpieczeństwa. Przejrzysty interfejs pozwala efektywnie realizować wszystkie zadania związane z instalacją oraz administracją ochrony firmowych stacji roboczych oraz serwerów.

Kompletna ochrona sieci

Ochrona Antymalware

Trzypoziomowy mechanizm (skanowania plików, ruchu HTTP, wiadomości pocztowych oraz komunikatorów internetowych) zapewnia ochronę przed wirusami, spyware, dialerami, żartami oraz narzędziami hakerskimi. Skanowanie heurystyczne skompresowanych lub nieposiadających rozszerzenia plików wraz z możliwością zablokowania plików zaszyfrowanych eliminuje potencjalne źródła infekcji.

Ochrona przed nowymi zagrożeniami

Połączenie techniki analizy heurystycznej (poszukiwanie podobieństw kodu) z technologiami TruPrevent (analiza zachowania procesów i aplikacji) oraz Kolektywną Inteligencją (analiza podejrzanych procesów i aplikacji na serwerach PandaLabs) zapewnia ochronę przed nieznanymi zagrożeniami. Pełne skanowanie odbywa się automatycznie i nie powoduje obciążenia stacji.

Ochrona Antyspam

Dwupoziomowa analiza wiadomości gwarantuje wysoką efektowność filtrowania poczty. Integracja z programem pocztowym pozwala na automatyczną klasyfikację i efektywne zarządzanie korespondencją niepożądaną przez Użytkownika. System analizy wiadomości pocztowych pozwala wyeliminować zbędne czynności pracowników firmy np. ręczne sortowanie korespondencji elektronicznej.

Zapora firewall oraz system HIPS

Inteligentny firewall pozwala definiować politykę dostępu do sieci na podstawie specjalnych polis bezpieczeństwa. Umożliwia blokowanie dowolnego ruchu sieciowego. Firewall jest zintegrowany z systemem analizy ruchu sieciowego (HIPS) dzięki czemu możliwe jest wykrywanie i blokowanie bezpośrednich ataków przeprowadzanych na stacje robocze lub serwery.

Filtrowanie Treści

System filtrowania treści monitoruje oraz blokuje niepożądany ruch internetowy. Administrator może wprowadzić filtr wszystkich plików multimedialnych (pliki video, pliki muzyczne, pliki graficzne) jak również blokadę określonego rodzaju plików np. PDF, EXE, ZIP, MP3. Blokowane są także podejrzane pliki, które stanowią zagrożenie dla bezpieczeństwa organizacji (m.in. pliki z niezgodnym formatem, zawierające zmodyfikowane lub powielone rozszerzenia). Mechanizm filtrowania podnosi poziom bezpieczeństwa organizacji oraz ogranicza obciążenie infrastruktury sieciowej.

Kontrola Aplikacji

Mechanizm kontroli aplikacji zwiększa efektywność zarządzania oprogramowaniem w firmie. Dzięki regułom bezpieczeństwa Administrator może przydzielać uprawnienia dostępu do sieci wybranym aplikacjom. Zablokowanie komunikatorów takich jak Gadu-Gadu, Skype lub aplikacji p2p jest proste i nie wymaga nieustannej aktualizacji reguł bezpieczeństwa.

Kontrola dostępu do sieci (blokowanie epidemii)

Funkcję kontroli dostępu do sieci potrafi wykryć i zablokować potencjalnie niebezpieczny komputer. Mechanizm blokuje stacje niespełniające określonych wymagań Administratora (np. brak aktualnej bądź aktywnej ochrony antywirusowej) lub te, na których wykryte zostało złośliwe oprogramowanie.

Bogata funkcjonalność systemu zarządzania

Scentralizowane zarządzanie

System zarządzania Panda AdminSecure pozwala na efektywne i centralne administrowanie całym systemem. Konsola zarządzająca umożliwia w czasie rzeczywistym monitorowanie aplikacji ochronnych, kontrolowanie poziomu bezpieczeństwa całej organizacji, wybranych stref lub poszczególnych stacji roboczych i serwerów plików. Dzięki modułowej budowie system zarządzania jest w pełni skalowalny. Istnieje możliwość jego dostosowania do infrastruktury sieciowej co znacznie ogranicza koszty wdrożenia.

Monitoring zdarzeń i alarmy w czasie rzeczywistym

Mechanizmy automatyzacji pracy Administratora zwiększają bezpieczeństwo firmy oraz stabilność pracy systemu. Monitorowanie statusu sieci oraz wydajności serwerów administracyjnych połączone jest z systemem wczesnego ostrzegania. W przypadku infekcji lub błędów Administrator zostaje natychmiast powiadomiony o zaistniałej sytuacji.

Szczegółowe raporty informacyjne

Wszystkie akcje podejmowane przez aplikacje ochronne jak również wszelkie zadania administracyjne są rejestrowane i przechowywane w systemie. W oparciu o zgromadzone dane, Administrator może generować raporty graficzne na potrzeby własne lub przełożonych. System automatyzacji pracy pozwala także na cykliczne generowanie i przesyłanie raportów na wskazany adres e-mail według ustalonego przez Administratora harmonogramu.

Cykliczny audyt bezpieczeństwa organizacji

Niezależny silnik Panda MalwareRadar pozwala przeprowadzać cykliczne, w pełni automatyczne audyty bezpieczeństwa stacji roboczych oraz serwerów. Wyszukuje luki systemowe oraz luki w zabezpieczeniach wskazując Administratorowi komputery zagrażające bezpieczeństwu organizacji. Szczegółowe raporty wzbogacane są o propozycje rozwiązań eliminujących luki w systemach ochrony.

Centralnie zarządzana kwarantanna

Podejrzane (lub uznane przez Administratora jako niebezpieczne) pliki są zabezpieczane w szyfrowanym katalogu kwarantanny. Administrator systemu za pośrednictwem konsoli AdminSecure ma możliwość zdalnego zarządzania kwarantanną każdej aplikacji ochronnej wchodzącej w skład systemu bezpieczeństwa. Istnieje możliwość połączenia systemu kwarantanny z mechanizmem automatycznego wysyłania podejrzanych plików do Laboratorium PandaLabs w celu ich analizy i dezynfekcji.

Integracja z Active Directory

Funkcja integracji z bazą Active Directory pozwala zautomatyzować proces instalacji oraz konfiguracji ochrony. Grupy komputerów prezentowane w konsoli Panda AdminSecure są wiernym odwzorowaniem kontenerów struktury domenowej, co pozwala na zachowanie spójności systemu ochrony z domenowymi polisami bezpieczeństwa.

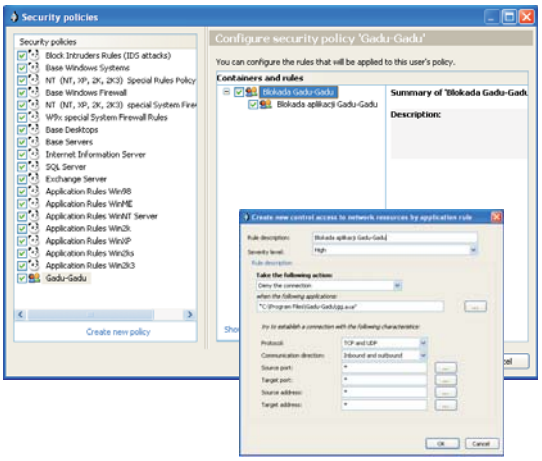
TruPrevent: Inteligentna analiza zachowań

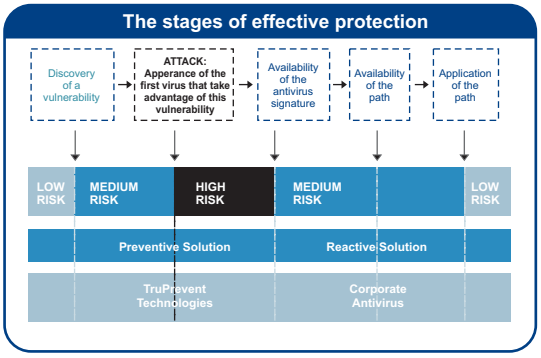
TruPrevent jest mechanizmem skutecznie wykrywającym i blokującym najnowsze wirusy bez potrzeby wcześniejszego ich przebadania w laboratoriach antywirusowych.

Typowe rozwiązania antywirusowe posiadają słaby punkt – muszą czekać, aż nowo wykryty wirus zostanie przeanalizowany i opracowana zostanie odpowiednia sygnatura. Tym samym nie chronią przed wirusami, które nie znajdują się w bazie sygnatur. Technologia TruPrevent wypełnia tę lukę w zabezpieczeniu przed wirusami - chroni komputer przed nieznanymi zagrożeniami.

Dzięki zaawansowanym technikom analizy behawioralnej TruPrevent potrafi wykryć niepożądane, groźne zachowanie kodu przed jego aktywacją i zablokować zagrożenie zanim nastąpią jakiekolwiek zmiany w systemie. Mechanizm ten analizuje zachowanie wszystkich programów, zezwalając lub blokując ich działanie.

Poza wykrywaniem nieznanych wirusów TruPrevent blokuje ataki sieciowe (takie jak przeprowadzane przez Sasser'a lub Blaster'a), próby włamań i penetracje zabezpieczeń, stanowiąc tym samym uzupełnienie dla rozwiązań typu firewall.





Wykorzystanie technologii TruPrevent:

- Redukuje ryzyko infekcji nowym, złośliwym oprogramowaniem.
- Eliminuje zagrożenie bezpośrednich ataków wykorzystujących luki w zabezpieczeniach oraz zaufanych aplikacjach.
- Podnosi poziom bezpieczeństwa blokując ataki hakerów, zagrożenia zero-day-exploit oraz kradzież poufnych informacji.

Panda Corporate Software Solutions - aplikacje ochronne		Panda Security For Business	Panda Security For Business with Exchange	Panda Security For Enterprise
Konsola Administracyjna	Panda AdminSecure	✓	✓	✓
TechTools	Panda MalwareRadar	✓	✓	✓
	Panda Security for Commandline	✓	✓	✓
Ochrona stacji roboczych i serwerów plików	Panda Security for Desktops	✓	✓	✓
	Panda Security for File Servers	✓	✓	✓
	Panda Security for Linux	✓	✓	✓
	Panda Security for Linux Servers	✓	✓	✓
Ochrona serwerów poczty	Panda Security for Exchange Servers		✓	✓
	Panda Security for Postfix			✓
	Panda Security for Qmail			✓
	Panda Security for Sendmail			✓
	Panda Security for Domino Servers			✓
Ochrona bram internetowych	Panda Security for ISA Servers			✓

Panda Corporate Software Solutions – funkcje ochronne		Panda Security For Business	Panda Security For Business with Exchange	Panda Security For Enterprise
Ochrona stacji roboczych oraz serwerów plików	Antivirus/ Antimalware	✓	✓	✓
	Firewall	✓	✓	✓
	Zapobieganie włamaniom (HIPS)	✓	✓	✓
	Antispam	✓	✓	✓
	Kontrola aplikacji	✓	✓	✓
	Współpraca z Cisco NAC	✓	✓	✓
	Niezależna funkcjonalność NAC	✓	✓	✓
	Audyt bezpieczeństwa	✓	✓	✓
Ochrona serwerów poczty	Antispam		✓	✓
	Antimalware		✓	✓
	Filtrowanie treści		✓	✓
	Ochrona bram SMPT			✓
Ochrona bram internetowych	HTTP/FTP antimalware			✓
	Content filtering			✓

Panda SecurityforBusiness

Więcej niż ochrona antywirusowa

Wymagania techniczne

Aplikacje ochronne

PANDA SECURITY FOR DESKTOPS

- Procesor: Pentium 300MHz
- Pamięć RAM: Pełen pakiet ochronny 512MB (Antywirus: 256MB)
- Dysk Twardy: 200 MB
- System Operacyjny: Windows 2000, XP, Vista, Windows 7 (32/64 bits), kompatybilność z WEPOS 1.1, WEPOS Ready 2009 oraz Tablet PC
- Technologia TruPrevent nie wspiera systemów 64 bitowych

PANDA SECURITY FOR FILE SERVERS

- Procesor: Pentium 300 Mhz
- Pamięć RAM: Pełen pakiet ochronny 512MB (Antywirus: 256MB)
- Dysk Twardy: 160 MB
- System Operacyjny: Windows NT 4.0 z SP6 (Domain Controller, SB Server, Terminal Server oraz Cluster), Windows Server 2000 Domain Controller, Terminal Server, SB Server oraz Cluster. Windows Server 2003 (32/ 64 bits) Enterprise Edition, SB Server, SP1, SP2 oraz Cluster, Windows Server 2003 R2(32/ 64 bits), Windows Server 2008 (32/ 64 bits), Windows SBS2008 (32/ 64 bits), Windows Server 2008 R2 (64 bits)
- Technologia TruPrevent nie wspiera systemów 64 bitowych

PANDA SECURITY FOR COMMANDLINE

- Procesor: Pentium/Athlon
- Pamięć RAM: 128 MB
- Dysk Twardy: 120 MB
- System Operacyjny: Debian 4 lub nowszy, Red Hat Enterprise 4 lub nowszy, Mandrake10.1/Mandriva 2006 lub nowszy, Ubuntu 6.06 lub nowszy, Fedora Core 5 lub nowszy, CentOS 4.6 lub nowszy, Windows NT/2000/XP, Windows Server 2003 (Enterprise Edition) /Vista

System zarządzania

SERWER ADMINISTRACYJNY

- Procesor: Pentium III 800 MHz.
- Pamięć RAM: 256 MB
- Dysk Twardy: 25 MB + 120 MB (bazy danych, sieć 100 komputerów)

SERWER REPOZYTORIUM

- Procesor: Pentium III 800 MHz
- Pamięć RAM: 128 MB
- Dysk Twardy: 520 MB

KONSOLA ADMINISTRACYJNA

- Procesor: Pentium II 266 MHz
- Pamięć RAM: 64 MB
- Dysk Twardy: 140 MB
- Internet Explorer 5.5
- Windows Installer 2.0

AGENT KOMUNIKACYJNY

- Procesor: Pentium 133 MHz
- Pamięć RAM: 64 MB
- Dysk twardy: 40 MB
- Internet Explorer 5.5
- System Operacyjny: Windows 2000/XP/XP 64 bits, Windows NT4 SP6 oraz Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64 bits, Windows Vista (32/ 64 bits), Windows Server 2008 (32/ 64 bits)

Certyfikaty i nagrody Panda Security

Partner Panda Security