

Panda Managed Office Protection

Zmień oprogramowanie antywirusowe
na rozwiązanie Security as a Service



Obsługa produktów antywirusowych wymaga od małych i średnich firm zbyt wiele czasu i wysiłku

Małe i średnie firmy dobrze wiedzą, że są narażone na takie samo **ryzyko** i podlegają takim samym **prawom** co wielkie organizacje. Rosnąca liczba zagrożeń sprawia, że wymagania tych firm w odniesieniu do zabezpieczeń zyskały złożony charakter. Tymczasem w wielu przypadkach **ograniczone zasoby**, jakimi firmy te dysponują, nie wystarczają, aby osiągnąć wysoki poziom bezpieczeństwa.

Małe i średnie organizacje zmuszone są ponosić wydatki na zakup dodatkowego sprzętu oraz licencji **oprogramowania**, a także koszty zatrudnienia wykwalifikowanego **personelu**, którego jedynym zadaniem jest zapewnienie wysokiego poziomu bezpieczeństwa.

Panda Managed Office Protection to rozwiązanie przeznaczone w szczególności dla organizacji, które chcą uniknąć podobnych problemów.

Rozwiązanie: Panda Managed Office Protection

Panda Managed Office Protection to usługa abonamentowa działająca w oparciu o interfejs www, która pozwala wyeliminować koszty zakupu i obsługi sprzętu, utrzymania personelu i wykorzystania zasobów związanych z zastosowaniem rozwiązań antywirusowych przeznaczonych dla małych i średnich firm.

Usługa udostępniana na zasadzie hostingu oferuje łatwą w użyciu **konsolę www**, która umożliwia organizacjom zarządzanie zabezpieczeniami przez cały czas i z dowolnego miejsca, co stanowi znaczące ułatwienie. **Panda Managed Office Protection** pozwala na zdalną instalację i zarządzanie, dzięki czemu stanowi idealne rozwiązanie dla oddziałów wielkich organizacji, które nie są podłączone do sieci LAN. W takim wypadku usługa pozwala uniknąć dodatkowych kosztów związanych z rozbudową infrastruktury.

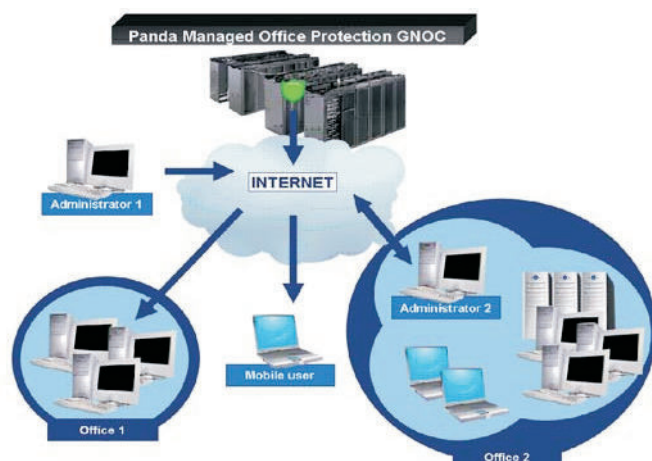
Usługa typu **Security as a Service** (bezpieczeństwo jako usługa) dla małych i średnich firm jest dostępna przez www i jako portal administracyjny, który umożliwia **przekazanie** (jeżeli okaże się to konieczne) zarządzania bezpieczeństwem do usługodawcy.

Panda Managed Office Protection uzupełniono szczegółowymi **kontrolami** złośliwego oprogramowania, które korzystają z technologii **Kolektywnej Inteligencji**.

Zamów subskrypcję usługi i pozbaź się kłopotów z wyspecjalizowanymi urządzeniami antywirusowymi, oprogramowaniem oraz zatrudnianiem personelu obsługi technicznej.

„Panda Managed Office Protection to idealne narzędzie typu Software as a Service (oprogramowanie jako usługa) stworzone dla działów IT i dostawców usług zarządzanych takich jak my. Pozwala nam zarządzać i generować raporty dla naszych klientów praktycznie z dowolnego miejsca dzięki scentralizowanej konsoli www oraz przeprowadzać aktualizacje, o ile dostępne jest połączenie z Internetem. Jestem przekonany, że Panda Security dysponuje najlepszym obecnie zabezpieczeniem na rynku, oferującym przy okazji niezawodną pomoc techniczną”.

Johnerick Cintrón, Ingeniero de redes, Strategic Network Consulting



„Potrzebowaliśmy produktu takiego jak Panda Managed Office Protection. Narzędzie to pomoże nam zredukować koszty związane z wyjazdami służbowymi. W naszym przypadku jest to szczególnie istotne, ponieważ do tej pory musieliśmy przemieszczać się w obrębie całego kraju. Scentralizowana konsola administracyjna umożliwia między innymi monitorowanie statusu wszystkich zainstalowanych licencji, podgląd komunikatów z ostrzeżeniami oraz przeprowadzanie niestandardowych instalacji”
Informática Notarial

Johnerick Cintrón, Ingeniero de redes,
Strategic Network Consulting

Główne zalety

- **Ograniczenie do minimum kosztów operacyjnych.** Brak konieczności inwestowania w rozwój infrastruktury. Umożliwia firmom przekazanie obsługi zabezpieczeń wyspecjalizowanym usługodawcom.
- **Ułatwienie obsługi.** Łatwa w użyciu scentralizowana konsola www, umożliwiająca wdrażanie i administrację zabezpieczeniami także w zdalnych oddziałach firmy.
- **Redukcja strat wydajności.** Aktualizacje nie wymagające ingerencji użytkownika i modernizacje ograniczające do minimum wykorzystanie pasma pozwalają skupić się na innych właściwych celach firmy.
- **Udoskonalone zarządzanie ryzykiem.** Pulpit nawigacyjny dostarcza w czasie rzeczywistym informacje na temat działań związanych z wykrywaniem oraz udostępnia wyniki cyklicznych kontroli bezpieczeństwa całej sieci.
- **Gwarancja ciągłości funkcjonowania firmy.** Usługa o wysokim stopniu dostępności, świadczona w formie hostingu, oferuje 24-godzinny pomoc techniczną przez 7 dni w tygodniu, wykorzystującą najnowsze technologie i pliki sygnatur.
- **Zapobieganie kradzieżom tożsamości** dzięki skutecznej identyfikacji ukrytego złośliwego oprogramowania, które odpowiada za przecieki poufnych informacji poza organizację.

Główne funkcje

- **Proaktywna ochrona** przed znanymi i nieznanymi zagrożeniami, a także przed zagrożeniami ukrytymi, w tym ochrona **plików i poczty, zabezpieczenie przeglądark i komunikatorów internetowych**.
- **Firewall oraz system HIPS z możliwością zarządzania**, które mogą być obsługiwane centralnie lub lokalnie w zależności od potrzeb administratora.
- **Usługa szczegółowych kontroli złośliwego oprogramowania** umożliwiająca cykliczne oszacowywanie statusu całej sieci.
- **Konsola administracyjna www** dla potrzeb zarządzania wszystkimi zabezpieczeniami, także w zdalnych oddziałach firmy.
- **Zautomatyzowane modernizacje/aktualizacje P2P.** Stacje robocze mogą aktualizować lub modernizować zainstalowane zabezpieczenia, łącząc się z najbliższym komputerem, co pozwala zminimalizować wykorzystanie przepustowości.
- **Ochrona w oparciu o profile** umożliwiające przypisanie różnych zasad lub profili zabezpieczeń różnym użytkownikom w zależności od potrzeb organizacji.
- **Zarządzanie przekazywaniem administracji** umożliwiającej organizacjom dokonanie podziału zadań administracyjnych między innych uprawnionych użytkowników.
- **Elastyczna instalacja.** Oferuje różne opcje wdrażania usługi, z lub bez konieczności interwencji użytkownika.
- **Codziennie raporty przesyłane pocztą elektroniczną.** Konfigurowalne raporty na temat działań związanych z wykrywaniem oraz na temat procesów aktualizacji.

PANDA
SECURITY

One step ahead.

Proaktywna ochrona przed nieznanym złośliwym oprogramowaniem

Proaktywna ochrona stacji roboczych i serwerów przed znanymi i nieznanymi zagrożeniami, a także przed zagrożeniami **ukrytymi**. Obejmuje również technologie **heurystyczne** oraz ochronę **plików, poczty, przeglądarek i komunikatorów internetowych**, w niewielkim stopniu wykorzystując zasoby systemu.

Firewall z możliwością zarządzania

Firewalle mogą być zarządzane centralnie za pomocą konsoli www lub **lokalnie** (z punktów końcowych) z wykorzystaniem konsoli lokalnej w sytuacji, gdy administrator przekazuje ich obsługę użytkownikom. Firewall oferuje filtrowanie aplikacji, filtrowanie **dostępu do sieci**, system **IPS** (Intrusion Prevention System), blokowanie **wirusów sieciowych** oraz konfigurację w oparciu o strefy.

Usługa szczegółowych kontroli złośliwego oprogramowania

Panda Managed Office Protection zawiera narzędzie **Malware Radar**. To usługa **kontroli** złośliwego oprogramowania, która cyklicznie szacuje status sieci. Malware Radar **sporządza raporty** i umożliwia **zautomatyzowanie** procesu neutralizacji zagrożeń.

Konsola administracyjna www

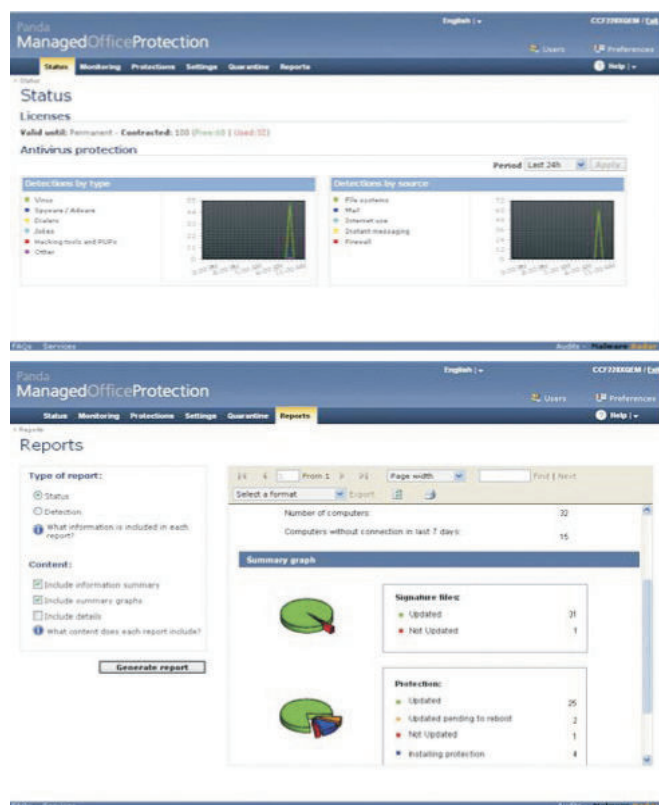
Wystarczy przeglądarka internetowa, aby administratorzy mogli **bez trudu**, a zarazem w scentralizowany sposób zarządzać zabezpieczeniami antywirusowymi i firewallami na wszystkich stacjach roboczych, także na tych, które znajdują się w **zdalnych oddziałach** firmy, nie podłączonych do sieci LAN. Nie jest wymagana rozbudowa infrastruktury, ani zatrudnianie personelu do obsługi zabezpieczeń.

Aktualizacje / modernizacje P2P

Stacje robocze będą aktualizować lub modernizować zainstalowane zabezpieczenia, łącząc się z **najbliższym komputerem** i korzystając z technologii **P2P**, co pozwoli zminimalizować wykorzystanie przepustowości. Jeżeli pakiet aktualizacyjny nie zostanie odnaleziony w sieci LAN, stacja robocza pobierze je z serwera Pandy za pośrednictwem Internetu.

Ochrona w oparciu o profile

Funkcja ta umożliwi administratorom przypisywanie różnych **zasad** lub **profilu** zabezpieczeń różnym użytkownikom lub grupom w zależności od potrzeb organizacji.



Zarządzanie przekazywaniem administracji

Umożliwia administratorowi dokonanie **podziału zadań administracyjnych** między innych uprawnionych użytkowników poprzez przydzielenie im komputerów, do których będą mogli uzyskać dostęp.

Elastyczna instalacja

Administratorzy dysponują różnymi opcjami umożliwiającymi wdrażanie zabezpieczeń, z lub bez konieczności interwencji użytkownika. Aby uniknąć konieczności angażowania użytkowników, stworzono **narzędzie dystrybucyjne**, które umożliwia wdrażanie zabezpieczeń w wybranych punktach końcowych w sposób **niewidoczny dla użytkowników**.

Codziennie raporty przesyłane pocztą elektroniczną

Raporty pozwalają na konfigurowanie, udostępniając informacje na temat wykrytych i wyeliminowanych **złośliwych programów** oraz tych, które są zlokalizowane w **kwartantach**, a także **statusu** procesów aktualizacji. Ponadto raporty można wyeksportować do plików tekstowych, a także zapisać w formacie XML, HTML lub Excel. Raporty dają także możliwość **zaplanowania** ich przesłania za pośrednictwem poczty elektronicznej.

Zautomatyzowane modernizacje / aktualizacje

Zautomatyzowane **modernizacje / aktualizacje** zabezpieczające przed atakami typu zero-day. **Częstotliwość** przeprowadzania aktualizacji może być konfigurowana przez administratora za pomocą scentralizowanej konsoli www. Istnieje także możliwość przeprowadzania aktualizacji **na żądanie**.

„Szczególnie ważna była dla nas możliwość oferowania usług zarządzanych zdalnie, a które są aktualizowane w sposób ciągły, jak to ma miejsce w przypadku Panda Managed Office Protection. Pozwoliło to nam natychmiastowo reagować na wszelkie problemy związane z bezpieczeństwem. Funkcja sporządzania raportów wykorzystująca interfejs www okazała się szczególnie skuteczna podczas usprawniania naszych procesów i umożliwiła dostarczanie szczegółowych analiz problemów związanych z bezpieczeństwem, mających szczególne znaczenie dla pracowników administracyjnych naszych klientów”.

Sean Lentner, Principal Partner, Lentner Technology Integrators.

Wymagania techniczne

Konsola www:

- Połączenie z Internetem
- Internet Explorer 6.0 lub nowszy
- Platforma Microsoft lub Linux

Stacje robocze / serwery plików:

- Przynajmniej jedna (jeden) musi posiadać połączenie internetowe
- Procesor Pentium 300 MHz (lub szybszy)
- Windows 2000 WS/Server, 2003, XP, Vista 32- i 64-bitowy, 2008
- 512 MB RAM
- Wolne miejsce na dysku twardym: 130 MB

Narzędzie dystrybucyjne:

- Pentium II 266 MHz (lub szybszy)
- Windows 2000 WS/Server, 2003, XP, Vista 32- i 64-bitowy, 2008
- 512 MB RAM
- Wolne miejsce na dysku twardym: 20 MB
- Windows Installer 2.0

Certyfikaty przyznane Panda Security



Czy Twój komputer jest zainfekowany? Sprawdź na witrynie www.infectedornot.com
Pobierz wersję testową Panda Managed Office Protection.

PANDA
SECURITY