



PGP® Desktop Email 9.6

Szyfrowanie poczty elektronicznej dla komputerów stacjonarnych i przenośnych

Part of the PGP® Encryption Platform

Bezpieczeństwo poufnych danych w poczcie elektronicznej na stacjach klienckich z centralnym zarządzaniem

PGP Desktop Email oferuje przedsiębiorstwom automatyczne i transparentne dla użytkownika rozwiązanie, które nieustannie zabezpiecza poufne informacje w poczcie elektronicznej. Dzięki tej aplikacji organizacje mogą chronić swoje poufne informacje spełniając wymagania swoich partnerów oraz przepisów prawa dotyczące bezpieczeństwa informacji.

Niezawodna ochrona

PGP Desktop Email zapewnia wszystkie funkcje szyfrowania, które są niezbędne dla zabezpieczenia komunikacji elektronicznej w organizacji za pomocą jednego prostego w obsłudze i zarządzaniu rozwiązania, które chroni pocztę od serwera nadawcy do serwera odbiorcy we wszystkich punktach pomiędzy nimi wykorzystując centralnie zdefiniowane, bazujące na politykach bezpieczeństwa szyfrowanie danych. Wysyłając wiadomość do użytkownika, który nie ma zainstalowanej aplikacji PGP Desktop Email, można zaszyfrować wybrane dokumenty jako archiwum używając PGP® Zip lub PGP® Self-Decrypting Archive i wysłać je jako standardowe załączniki.

Korzyści w firmie

Całkowicie zautomatyzowana instalacja i zarządzanie

- Współpracuje z popularnymi elementami infrastruktury e-mail i protokołami
- Wszelchstronnie chroni informacje bez zaburzania dotychczasowych praktyk biznesowych
- Dostarcza narzędzia umożliwiające szybkie wdrożenie PGP Desktop Email u użytkowników
- Wykorzystanie standardowych plików MSI ułatwia wdrożenie wstępnie skonfigurowanych klientów

Prosta, automatyczna obsługa

Po instalacji PGP Desktop Email pracownicy mogą wrócić do swych zwykłych zajęć. Oprogramowanie automatycznie szyfruje, rozszyfrowuje, podpisuje elektronicznie i weryfikuje wiadomości zgodnie z polityką bezpieczeństwa, zapewniając, że żaden z użytkowników nigdy nie zapomni zabezpieczyć poczty.

Wymuszona polityka bezpieczeństwa niezależna od indywidualnych decyzji

Polityka dotycząca bezpieczeństwa poczty elektronicznej może być oparta na nadawcy, indywidualnym odbiorcy, domenie odbiorcy, słowie kluczowym lub zawartości. Wiadomości są szyfrowane automatycznie, bez udziału użytkownika. Zasady polityki bezpieczeństwa mogą być ustanowione i audytowane za pomocą platformy zarządzającej PGP Universal Server.

Redukcja kosztów i szybkie wdrożenie

Dzięki wyeliminowaniu potrzeby uczenia się obsługi różnych interfejsów do zarządzania i oszczędności czasu przy instalacji, zarządzaniu i obsłudze wielu konsol zarządzających i serwerów, wdrożenie PGP Desktop Email jest szybkie i pozwala zredukować koszty operacyjne przedsiębiorstwa.

Wsparcie platformy szyfrującej PGP

Platforma szyfrująca PGP (PGP® Encryption Platform) dostarcza mechanizmów do współdzielenia definicji użytkowników, zasobów, polityk bezpieczeństwa w obrębie wielu aplikacji szyfrujących. PGP Desktop Email jako element tej platformy używa tych samych kluczy, definicji użytkowników, konfiguracji dla przyspieszenia wdrożenia i łatwiejszego zarządzania całością komponentów szyfrujących. PGP Desktop Email może być użyty w kombinacji z dowolnym innym produktem PGP zapewniając wielostopniowe bezpieczeństwo w przedsiębiorstwie.

PGP® Desktop Email 9.6

Szyfrowanie poczty elektronicznej dla komputerów stacjonarnych i przenośnych

Cechy produktu

Nowość: Wsparcie dla systemu Windows Vista

PGP Desktop Email wspiera teraz wszystkie 32-bitowe edycje nowego systemu operacyjnego Microsoft Vista.

Automatyczna ochrona poczty

PGP Desktop Email automatycznie szyfruje, rozszyfrowuje, podpisuje elektronicznie i weryfikuje wiadomości zgodnie z indywidualnie lub centralnie zarządzaną polityką. Szyfrowanie wiadomości tekstowych (Instant Messaging) zapewnia bezpieczeństwo komunikacji przy używaniu oprogramowania AOL® Instant Messenger™ (AIM).

Centralne zarządzanie, wdrożenie i polityki bezpieczeństwa

Automatyczne aktualizacje, zarządzanie użytkownikami i kluczami i polityką bezpieczeństwa obejmujące dyski, nośniki, pocztę i pliki sieciowe przebiega z poziomu platformy zarządzającej PGP Universal Server. Bazujące na rolach uprawnienia administratorów umożliwiają precyzyjny podział ich obowiązków.

Zabezpieczony dostęp do danych

Opatentowana technologia PGP Additional Decryption Key (ADK) zapewnia bezpieczny dostęp do zaszyfrowanych danych w przypadku zgubienia klucza szyfrującego lub gdy taki dostęp jest wymagany przepisami prawa.

Wiele sposobów współdzielenia danych

Użytkownicy mogą tworzyć szyfrowane kontenery (archiwa) danych w celu transportu i współdzielenia danych przy użyciu PGP® Virtual Disk, PGP® Zip i PGP® Self-Decrypting Archive, bez względu na typ nośnika danych.

- PGP Virtual Disk – tworzy szyfrowane wolumeny danych oferując zabezpieczoną przestrzeń dyskową
- PGP Zip – tworzy w jednym kroku szyfrowane bezpieczne archiwum danych
- PGP Self-Decrypting Archive – wykonywalny plik z zaszyfrowanym archiwum danych, który może być rozszyfrowany i rozpakowany bez produktu PGP® Desktop; idealny dla użytkowników nie posiadających PGP (tylko wersja Windows)

Bezpieczne usuwanie plików

PGP® Shredder i PGP® Wipe umożliwiają bezpieczne, całkowite i trwałe usuwanie plików z dysku.

Różne sposoby uwierzytelniania

PGP Desktop Email może być zabezpieczony kluczem PGP lub certyfikatem X.509 i wspiera istniejący system kluczy. Wsparcie dla kart i tokenów umożliwia wielostopniowe uwierzytelnianie administratorów i użytkowników.

PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners

Specyfikacje techniczne

Wspierane systemy operacyjne

- Windows Vista (wszystkie edycje 32-bitowe)
- Windows XP SP1 lub SP2
- Windows XP Tablet PC Edition 2005 (wymagana klawiatura)
- Windows 2000 Professional SP4
- Windows 2003 Server SP1
- Mac OS X 10.4 (Universal Binary – Intel & PPC)

Wersje językowe

- Angielska
- Niemiecka
- Japońska

Opcje uwierzytelniania

- Open PGP RFC 2440 keys
- X.509 keys

Uwierzytelnianie 2-stopniowe

Aktualna lista wspieranych urządzeń znajduje się na stronie www.pgp.com/products/desktop_email/tech_specs.html#smart-cards.

Protokoły pocztowe

- POP3
- IMAP
- SMTP
- MAPI
- Lotus Notes

Standardy bezpieczeństwa poczty elektronicznej

- PGP/MIME RFC 3156
- OpenPGP RFC 2440
- S/MIME v3 RFC 2633
- X.509 v3

Wspierane programy pocztowe

- Microsoft Outlook 2007, Outlook XP SP3, Outlook 2003 SP2, Outlook 2000 SP3, Windows Mail 6, Outlook Express 6, Entourage 2004
- Lotus Notes 5.0.11, 6.2, 7.0.1 dla Windows
- Mozilla 1.7
- Mozilla Thunderbird 1.5
- Qualcomm Eudora 6.2 & 7 dla Windows
- Apple Mail 2.1
- Novell GroupWise 6.5.1 lub późniejszy

Wspierane programy IM

- AOL Instant Messenger 5.5-5.9.x dla Windows
- AOL Instant Messenger 4.7 dla Mac OS X
- Trillian 2.2-3.1 dla Windows
- Apple iChat 2.1 I 3.1 dla Mac OS X

(aktualne dane techniczne produktu znajdują się na stronie www.pgp.com/products/desktop_email/tech_specs.html)

Wymagania systemu centralnego zarządzania

• PGP Universal Server 2.6 (wymagany jest dedykowany serwer), więcej informacji znajduje się na stronie www.pgp.com/products/universal_server/tech_specs.html

