



# PGP® Universal™ Gateway Email 9.6

Bezpieczna poczta elektroniczna bez oprogramowania klienckiego

Part of the PGP® Encryption Platform

## Ochrona poufności poczty elektronicznej dzięki centralnie zdefiniowanej polityce bezpieczeństwa

PGP Universal Gateway Email zapewnia centralnie zarządzaną, opartą na standardach szyfrację poczty elektronicznej, która chroni komunikację firmy z klientami i partnerami. W oparciu o konfigurowane reguły szyfrowania, e-maile są zabezpieczane w chwili, kiedy wchodzą lub opuszczają sieć korporacyjną. PGP Universal Gateway Email rozszerza firmową politykę bezpieczeństwa poczty elektronicznej na jej odbiorców bez potrzeby przeprowadzania specjalnych szkoleń lub instalacji dodatkowego oprogramowania.

### Automatycznie wymuszona polityka

- Sprawdza e-maile wchodzące i wychodzące z organizacji
- Stosuje centralnie zdefiniowaną politykę do szyfrowania poczty elektronicznej
- Przeprowadza szyfrowanie automatycznie, bez udziału użytkowników

### Dostosowanie do wymagań audytorów i przepisów prawa

Ponieważ przepisy dotyczące ochrony własności intelektualnej i wymagania audytorów mogą się zmieniać, PGP Universal Gateway Email pozwala administratorom szybko i łatwo wprowadzać nowe polityki bezpieczeństwa i kontrolować sposoby szyfrowania poczty.

- Polityki mogą dotyczyć grup, aplikacji pocztowych, nadawców lub adresatów wiadomości lub mogą być wąsko zdefiniowane według szczególnych wymagań.
- Wiadomości do odbiorców wewnętrznych i zewnętrznych wraz z listami dystrybucyjnymi serwera Microsoft Exchange podlegają niezauważalnym dla użytkowników procesom zdefiniowanym przez politykę bezpieczeństwa.

### Rozszerzenie polityki bezpiecznej komunikacji poza organizację

PGP Universal Gateway Email automatycznie dostosowuje się do możliwości odbiorcy, jednocześnie dostarczając wiadomość zgodnie z polityką bezpieczeństwa. Adresatom, którzy nie mają zainstalowanego oprogramowania szyfrującego:

- PGP Universal™ Web Messenger dostarcza zabezpieczoną wiadomość przez interfejs webowy;
- Jeżeli polityka wymaga zabezpieczenia wiadomości na komputerze odbiorcy, można szybko zainstalować PGP Universal™ Satellite,

który zaszyfruje wiadomość zgodnie z polityką;

- Wiadomości wysyłane do użytkowników, którzy mają inne narzędzia szyfrujące są zabezpieczane w sposób indywidualny;
- Konfiguracja, tworzenie kont i zarządzanie kluczami odbywają się automatycznie i w sposób niezauważalny dla użytkowników.

### 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 Universal Gateway Email jako element tej platformy używa tych samych kluczy, definicji użytkowników, konfiguracji dla przyspieszenia wdrożenia i łatwiejszego zarządzania całością komponentów szyfrujących. PGP Universal Gateway Email może być użyty w kombinacji z dowolnym innym produktem PGP zapewniając wielostopniowe bezpieczeństwo w przedsiębiorstwie.

## Korzyści w firmie

### Ochrona danych klientów i własności intelektualnej

Dzięki PGP Universal Gateway Email organizacje mogą chronić wiadomości poczty elektronicznej, kiedy wchodzą i opuszczają sieć korporacyjną

- Szyfruje wiadomości w oparciu o ich treść, nadawcę, odbiorcę i inne parametry, które określają wiadomość poufną
- Integruje się z rozwiązaniami stosowanymi przez strony trzecie

### Rozszerzenie bezpieczeństwa bez wpływu na produktywność

Potencjalny wpływ wdrożenia nowego rozwiązania na działalność firmy jest poważnym problemem. PGP Universal Gateway Email zabezpiecza pocztę zgodnie ze zdefiniowaną polityką bezpieczeństwa nie wymagając zmiany zachowań użytkowników i nie wywierając wpływu na produktywność.

- Odbiorcy zewnętrzni mogą odbierać wiadomości za pomocą dotychczasowo używanego oprogramowania pocztowego i przeglądarki WWW.
- Niewidoczne i bezobsługowe działanie aplikacji zapobiega zwiększeniu liczby zapytań do helpdesku.

# PGP® Universal™ Gateway Email 9.6

## Bezpieczna poczta elektroniczna bez oprogramowania klienckiego

### Ochrona dotychczasowych inwestycji

PGP Universal Gateway Email integruje się z rozwiązaniami innych producentów, dzięki czemu działając zgodnie z dotychczasowymi politykami i procesami zabezpiecza wiadomości wchodzące i wychodzące z organizacji.

## Korzyści dla partnerów biznesowych

### Prywatność i zaufanie bez dodatkowych kosztów i komplikacji

- Wspiera dwa globalne standardy szyfrowania poczty: OpenPGP i S/MIME
- Nie wpływa na produktywność użytkowników
- Nie wymaga od partnerów biznesowych żadnych inwestycji w nowy sprzęt lub oprogramowanie, ani szkoleń

## Cechy produktu

### Rozszerzone możliwości polityki szyfrowania

Dzięki rozszerzonym narzędziom zawartym w PGP Universal™ Server, polityki szyfrowania mogą być dostosowywane w oparciu o zawartość wiadomości, metodę dostarczenia, nadawcę, odbiorcę i inne parametry

- Rozszerzone możliwości silnika Mail Policy zwiększają zakres kontroli przepływu poczty i szyfrowania
- Polityki zdefiniowane dla PGP Universal Gateway Email mogą być przenoszone w dół na stacje robocze z zainstalowanym PGP Desktop Email

### Ciągłość pracy dzięki klastrowaniu

Kilka serwerów PGP Universal Server można połączyć w klastr, podnosząc niezawodność rozwiązania. Gwarantuje to ciągłość pracy przy aktualizacji polityk bezpieczeństwa, przekazywaniu wiadomości poprzez PGP Universal Web Messenger, zarówno wewnątrz organizacji, jak i na zewnątrz.

### Archiwizacja poczty

PGP Universal Gateway Email integruje się z wiodącymi rozwiązaniami do archiwizacji poczty.

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

### PGP Universal Web Messenger

PGP Universal Gateway Email umożliwia wysyłanie i odbieranie bezpiecznych wiadomości przez przeglądarkę WWW.

### PGP Universal Satellite

PGP Universal Satellite to aplikacja przeznaczona dla użytkowników, którzy preferują używanie dotychczasowego klienta pocztowego, lub gdy polityka bezpieczeństwa wymaga szyfrowania e-maili na stacji klienckiej.

### Opcja: Symantec AntiVirus™ Scan Engine

Istnieje możliwość integracji produktu Symantec Antivirus Scan Engine jako dodatkowego komponentu.

## Specyfikacje techniczne

### Wymagania systemowe

- Oprogramowanie PGP: PGP Universal Server 2.6
- Sprzęt: Aktualna lista wspieranych urządzeń znajduje się na stronie: [www.pgp.com/products/universal\\_gateway\\_email/tech\\_specs.html](http://www.pgp.com/products/universal_gateway_email/tech_specs.html)
- Wirtualizacja: VMware ESX Server

### Standardy bezpieczeństwa poczty elektronicznej

- PGP/MIME RFC 3156
- OpenPGP RFC 2440
- S/MIME v3 RFC 2633

### Zarządzanie kluczami i certyfikatami

- OpenPGP
- X.509 v3

### Protokoły pocztowe

- POP/POPS
- IMAP/IMAPS
- SMTP/SMTSPS
- SMARTTLS dla POP/IMAP/SMTP

### Wspierane serwery pocztowe

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2003 SP2
- Microsoft Exchange Server 2000 SP3
- Lotus Domino Server 7.0.1, 6.5 lub 5.0.11

(aktualne dane techniczne produktu znajdują się na stronie [www.pgp.com/products/universal\\_gateway\\_email/tech\\_specs.html](http://www.pgp.com/products/universal_gateway_email/tech_specs.html))



Veracomp jest wyłącznym dystrybutorem rozwiązań PGP na terenie Polski. Prowadzi sprzedaż wyłącznie za pośrednictwem Partnerów handlowych.  
[www.veracomp.pl/pgp](http://www.veracomp.pl/pgp)  
tel. (12) 25 25 555, fax: (12) 25 25 500

