



# PGP Universal™ Gateway Email 2.5

Sichere E-Mail-Kommunikation ohne Client-Software

Teil der PGP® Encryption Platform

## Vertraulichkeit von E-Mails durch zentral definierte Richtlinien gewährleisten

PGP Universal Gateway Email verschlüsselt E-Mails zentral und standardbasiert, um die Kommunikation mit Kunden und Partnern zu sichern. E-Mails werden nach detailliert konfigurierbaren Regeln verschlüsselt, um sie außerhalb des Unternehmensnetzwerks zu schützen. PGP Universal Gateway Email erfordert keine Schulungen oder zusätzliche Software seitens des Empfängers.

### Richtlinien automatisch umsetzen

- Prüfung der ankommenden und abgehenden E-Mails
- Umsetzung zentral definierter Richtlinien für die E-Mail-Verschlüsselung
- Automatische Verschlüsselung ohne Eingriff des Anwenders

### Einfache Anpassung an veränderte Revisionsanforderungen und gesetzliche Bestimmungen

Wie beim Schutz geistigen Eigentums werden auch die Revisions- und Compliance-Anforderungen immer strenger. Mit PGP Universal Gateway Email implementieren Administratoren schnell und ohne Aufwand neue Richtlinien zur Kontrolle des E-Mail-Verkehrs und der Verschlüsselung.

- Richtlinien können entweder für alle Anwender gelten oder auf genaue Gruppen, E-Mail-Anwendungen, Absender und Empfänger eingegrenzt werden.
- Nachrichten an interne und externe Empfänger sowie interne Microsoft Exchange-Verteilerlisten werden den Richtlinien entsprechend verarbeitet.

### Externe Empfänger sicher erreichen

PGP Universal Gateway Email passt sich automatisch an die verfügbaren Mittel des Empfängers an und übermittelt Nachrichten auf sicherem Weg. Für Empfänger ohne Verschlüsselungssoftware gilt:

- PGP Universal™ Web Messenger stellt vertrauliche E-Mails über eine sichere Website zur Verfügung.
- Wenn Nachrichten auf dem Desktop verschlüsselt werden sollen, kann PGP Universal™ Satellite sehr schnell und einfach installiert werden. Diese Anwendung stellt sicher, dass E-Mails in beide Richtungen automatisch geschützt werden.

- Nachrichten an Empfänger mit mehreren PGP-Applikation werden einzelnen verarbeitet und geschützt.
- Die Verwaltung von Anwendern und Schlüsseln erfolgen automatisch und ohne Eingriff des Endanwenders.

### PGP Encryption Platform

Mit der PGP® Encryption Platform verfügt ein Unternehmen über das Grundgerüst für die strategische Verschlüsselung. Das Management gemeinsam genutzter Anwenderdaten, die Richtlinienverwaltung und die Bereitstellung erfolgen dabei anwendungsübergreifend und automatisch. Die Anwendung PGP Universal Gateway basiert ebenfalls auf der PGP Encryption Platform und ermöglicht die Nutzung vorhandener Richtlinien, Anwender, Schlüssel und Konfigurationen, womit sich die Implementierung und die Umsetzung von Richtlinien zusätzlich beschleunigt. PGP Universal Gateway Email kann in Kombination mit anderen neuen oder vorhandenen PGP® Desktop Email-Installationen eingesetzt werden, um verschiedene E-Mail-Sicherheits Ebenen abzudecken.

## Nutzen für das Unternehmen

### Kundendaten und geistiges Eigentum schützen

PGP Universal Gateway Email schützt E-Mails außerhalb des Unternehmensnetzwerks.

- Als Kriterien für die Verschlüsselung von Nachrichten können der Inhalt, der Absender, der Empfänger und andere Merkmale der Nachricht dienen.
- Die Integration mit Spam- und Content-Filtern ist möglich.

### Mehr Sicherheit ohne Produktivitätsverluste

Unternehmen sollten auch die potenziellen Seiteneffekte einer neuen Anwendung beachten. PGP Universal Gateway Email schützt Nachrichten nach Richtlinien, ohne die Arbeitsweise oder Produktivität des internen Anwenders zu beeinflussen.

- Empfänger außerhalb des Unternehmens können E-Mails mit den gewohnten E-Mail-Programmen oder einem Browser abrufen.
- Helpdesk-Anfragen werden durch einen hohen Grad an Benutzerfreundlichkeit und Automatisierung stark verringert

## Integration in bestehende Compliance-Lösungen

PGP Universal Gateway integriert sich in vorhandene Compliance-Lösungen zur Kontrolle abgehender Nachrichten und nutzt die bestehenden Richtlinien und Prozesse dieser Anwendungen.

## Vorteile für Geschäftspartner

### Mehr Vertrauen und Datenschutz, gleiche Kosten und Komplexität

- Unterstützung zweier global etablierter Standards für E-Mail-Verschlüsselung: OpenPGP und S/MIME
- Gleiche Arbeitsschritte für Anwender bei unveränderter Produktivität
- Keine Investitionen in neue Software, Hardware oder Schulungen seitens Kunden oder Geschäftspartner.

## Merkmale und Funktionen

### Neu: Erweiterte Verschlüsselungsrichtlinien

Mit der erweiterten Mail Policy-Engine von PGP Universal™ Server lassen sich Nachrichten nach Inhalt, Übertragungsmethode, Absender, Empfänger und andere Kriterien verschlüsseln.

- Die erweiterte Mail Policy-Engine gibt Administratoren eine differenzierte Kontrolle des E-Mail-Verkehrs und der Verschlüsselung.
- Für PGP Universal Gateway Email definierte Richtlinien können durchgängig angewendet werden, zum Beispiel auf PGP Desktop Email-Clients.

### Neu: Erweitertes Clustering für Hochverfügbarkeit

Mehrere PGP Universal Server können zu einem Cluster zusammengefasst werden, um Richtlinienaktualisierungen von PGP Universal Web Messenger und Nachrichten innerhalb des gesamten Unternehmens sowie für Kunden und Geschäftspartner hoch verfügbar zu machen.

### Neu: Integration von E-Mail-Archiven

PGP Universal Gateway Email kann in führende E-Mail-Archivlösungen integriert werden.

### PGP Universal Web Messenger

PGP Universal Gateway Email bietet eine Richtlinienoption zum sicheren Senden und Empfangen von Nachrichten über einen Browser.

## PGP Universal Satellite

Anwender können auch ihr bestehendes E-Mail-Programm zum Empfang von sicheren Nachrichten nutzen möchten, indem sie PGP Universal Satellite installieren. Außerdem erfüllt diese Option die Anforderung der Verschlüsselung auf auf Desktop-Ebene.

### Optional: Symantec AntiVirus™ Scan Engine

PGP Universal Gateway Email kann die Symantec AntiVirus Scan Engine einbinden, um E-Mails auf Viren zu prüfen.

## Technische Daten

### Systemvoraussetzungen

- PGP-Software: PGP Universal Server 2.5
- Hardware: Aktuelle Informationen zu unterstützten Hardwarekonfigurationen finden Sie unter [www.pgp.com/products/universal\\_gateway\\_email/tech\\_specs.html](http://www.pgp.com/products/universal_gateway_email/tech_specs.html)
- Virtualisierung: VMware ESX Server

### Messaging-Sicherheitsstandards

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

### Schlüssel- und Zertifikatsverwaltung

- OpenPGP
- X.509 v3

### Unterstützte Messaging-Protokolle

- POP/POPS
- IMAP/IMAPS
- SMTP/SMTPS
- STARTTLS für POP/IMAP/SMTP

### Unterstützte E-Mail-Server

- Microsoft Exchange Server 2003 SP1
- Microsoft Exchange Server 2000 SP3
- Lotus Domino Server 6.5, Domino Server 5.0.11
- Stalker CommuniGate 5.0

(Aktuelle Produktspezifikationen finden Sie unter [www.pgp.com/products/universal\\_gateway\\_email/tech\\_specs.html](http://www.pgp.com/products/universal_gateway_email/tech_specs.html))

PGP und das PGP-Logo sind eingetragene Marken der PGP Corporation. Die in diesem Dokument erwähnten Produkt- und Markennamen sind Marken oder eingetragene Marken der jeweiligen Eigentümer. Alle solchen Marken oder eingetragenen Marken sind alleiniges Eigentum der jeweiligen Inhaber.

