



End-to-End-Verschlüsselung von E-Mail.

### PGP®-Kunden im Fokus

BAE Systems, ein führender, transatlantischer Rüstungskonzern, verwendet PGP® Desktop Email zum Schutz seiner internen und externen Datenkommunikation und zur Freigabe von Projektinformationen an Kunden.

### Vorteile

- **Unkomplizierte, automatische Funktionsweise** – Datenschutz ohne zusätzlichen Aufwand für den Anwender.
- **Richtlinienumsetzung** – Automatische Umsetzung des Datenschutzes anhand zentral verwalteter Richtlinien.
- **Schnellere Bereitstellung** – Durchgehende Verschlüsselung von E-Mails bei Verwendung der vorhandenen Infrastruktur.
- **Verringerte Betriebskosten** – durch zentralisierte automatische Verschlüsselungsrichtlinien für E-Mails

### Schutz vertraulicher Informationen in E-Mails mit Lösung für Desktop-PCs

E-Mail hat sich zum weltweit wichtigsten Kommunikationssystem für Unternehmen entwickelt, denn es ermöglicht ein effizientes Arbeiten mit Kunden, Lieferanten und Geschäftspartnern. Leider stellen ungeschützte E-Mails ein beträchtliches Risiko für die höchst vertraulichen Daten eines Unternehmens dar: Kundendaten, Finanzdaten und Geschäftsgeheimnisse. Wenn solche Informationen in falsche Hände gelangen, kann es zu finanziellen Verlusten, juristischen Problemen und zur Rufschädigung kommen.

PGP® Desktop Email ist eine automatische, transparente Verschlüsselungslösung zum Schutz der internen und externen vertraulichen E-Mail-Kommunikation von Unternehmen. Mit PGP® Desktop Email können Unternehmen das Risiko des Datenmissbrauchs minimieren und die gesetzlichen Datenschutzbestimmungen sowie die Anforderungen von Geschäftspartnern erfüllen.

### Leistungsstarke End-to-End-Verschlüsselung von E-Mails

PGP® Desktop Email stellt umfassende Verschlüsselungsfunktionen zum Schutz der gesamten E-Mail-Kommunikation eines Unternehmens in einer einzigen, benutzerfreundlichen und leicht zu verwaltenden Lösung bereit. Ermöglicht Unternehmen den automatischen Schutz der gesamten E-Mail-Kommunikation zwischen dem E-Mail-Programm des Absenders und dem des Empfängers, also auf allen Zwischenstationen, durch Verschlüsselung anhand zentral definierter Richtlinien. PGP® Desktop Email unterstützt alle wichtigen E-Mail-Sicherheitsstandards und arbeitet nahtlos mit den bei E-Mail-Empfängern verbreitetsten E-Mail-Sicherheitslösungen zusammen. Für Empfänger ohne E-Mail-Sicherheit kann der Absender Dokumente mit PGP® Zip oder PGP® SDA (selbstentschlüsselndes Archiv) verschlüsseln und als normale E-Mail-Dateianlage zusenden.

### Mit der PGP® Encryption Platform kompatibel

PGP® Desktop Email ist mit der PGP® Encryption Platform kompatibel, die den strategischen Rahmen für das Management der gemeinsamen Datennutzung durch Anwender, zur Verwaltung von Richtlinien und für die Bereitstellung automatisierter plattform-, system- und anwendungsübergreifender, integrierter Verschlüsselungsanwendungen bildet. So können die vorhandenen Richtlinien, Anwender, Schlüssel, und Konfigurationen mit PGP® Universal™ Server verwaltet werden, um die Bereitstellung und Richtlinienumsetzung zu beschleunigen. PGP® Desktop Email kann auch in Kombination mit anderen PGP-Verschlüsselungsanwendungen verwendet werden, um mehrere Sicherheitsebenen zu schaffen.

## Einfache automatische Funktionsweise

Sobald PGP® Desktop Email bereitgestellt ist, wird die Verschlüsselung vollkommen transparent durchgeführt – die Anwender können einfach wie gewohnt weiterarbeiten. Die Nachrichten werden automatisch geschützt. So kann der Anwender nie vergessen, E-Mails und Anhänge zu schützen.

- **Automatische Messaging-Sicherheit** – Automatische Verschlüsselung, Entschlüsselung sowie digitale Signierung und Verifizierung von E-Mail-Nachrichten nach individuell definierten oder zentral verwalteten Richtlinien.
- **Softwareunabhängige, sichere E-Mail-Zustellung** – Wenn PGP® Desktop Email mit PGP® Universal™ Gateway Email im Einsatz ist, werden Nachrichten auch sicher an externe Anwender zugestellt, die über keine Software mit E-Mail-Verschlüsselung verfügen.
- **Viele Möglichkeiten zum Schutz von Daten** – Schutz vertraulicher Daten mit PGP® Zip, PGP SDA (selbstentschlüsselndes Archiv) und PGP® Virtual Disk.
- **Sicheres Löschen von Dateien** – Entfernt zuverlässig und endgültig alle Spuren vertraulicher Daten von Laufwerken.

## Umsetzen von Sicherheitsrichtlinien

E-Mail-Richtlinien können für Absender, einzelne Empfänger, Empfängerdomänen, Schlüsselwörter oder Inhalte definiert werden, sodass vertrauliche Nachrichten automatisch ohne zusätzlichen Aufwand für den Anwender geschützt werden. Diese Richtlinien können mit der Verwaltungskonsolle von PGP® Universal Server definiert und überwacht werden.

- **Kontrolle der Offline-Richtlinie** – Administratoren können jetzt Richtlinien für Offline-Nutzer erstellen, die dann beim Versand von E-Mails angewendet werden, wenn der PGP® Universal Server nicht von PGP® Desktop erreicht werden kann.
- **Client-Bedienelemente** – Legen Sie fest, welche Funktionen am Client-PC aktiviert, für den Benutzer sichtbar sind und durchgesetzt werden. Hierzu zählen auch optionale Schaltflächen für das manuelle Verschlüsseln und Signieren.
- **Erweiterte Authentifizierungsoptionen** – Zwei-Faktor-Authentifizierung mit Smartcards (z.B. RSA SID800).

## Schnellere Bereitstellung

PGP® Universal Server in Kombination mit PGP® Desktop Email erlaubt die Erstellung, Umsetzung und Aktualisierung von Sicherheitsrichtlinien in Echtzeit. So wird der zum Bereitstellen der umfassenden Datenverschlüsselung benötigte Zeit- und Arbeitsaufwand verringert. Durchgehend verschlüsselte E-Mail-Kommunikation.

**Beschleunigter Bereitstellungsprozess** – Schnellere Bereitstellung durch automatische Installation und Konfiguration.

## Geringere Betriebskosten

Für PGP® Desktop Email benötigen Endanwender keine spezielle Schulung. Dadurch beschleunigt sich die Bereitstellung, Kosten für Schulungen werden verringert und eine Zunahme der Anrufe bei der telefonischen Beratung wird vermieden.

## Verwaltung mit PGP® Universal Server

PGP® Desktop Email kann zentral bereitgestellt und verwaltet werden, wenn es zusammen mit PGP® Universal Server verwendet wird (optional). Dies ermöglicht es Unternehmen, auf einfache Weise unternehmensweite Datensicherheitsrichtlinien einzurichten und umzusetzen.

- **Zentralisierte Umsetzung von Sicherheitsrichtlinien** – Automatische Umsetzung von Sicherheitsrichtlinien für vertrauliche Daten und E-Mails anhand eines Verzeichnisdienstes.
- **Erweiterbarer Schutz** – Ermöglicht die Verwaltung von PGP® Support Package for BlackBerry®, PGP® Mobile oder anderer Anwendungen, die mit der PGP® Encryption Platform kompatibel sind.

## Technische Spezifikationen

Eine vollständige Aufzählung der technischen Spezifikationen finden Sie auf [www.pgp.de](http://www.pgp.de).



[www.pgp.de](http://www.pgp.de)

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 solche Marken oder eingetragenen Marken sind alleiniges Eigentum der jeweiligen Inhaber. © PGP Corporation.

DTEMSDE