



# PGP® Desktop Professional 9.5

Umfassende Verschlüsselung für Desktop- und Laptop-Computer

Teil der PGP® Encryption Platform

## Daten auf Anwendersystemen schützen

PGP Desktop Professional bietet ein umfassendes Paket von Verschlüsselungslösungen zum Schutz von sensiblen Daten in E-Mails, Instant Messages und auf Festplatten oder Wechsel-datenträgern. PGP Desktop Professional gewährleistet, dass vertrauliche Informationen geschützt und dass von Geschäftspartnern oder Behörden definierte Vorgaben zur Weitergabe und zum Schutz von Informationen erfüllt werden.

### Schutz für Festplatten, Datenträger und Dateien

PGP Desktop Professional umfasst die Anwendung PGP® Whole Disk Encryption. Damit wird der gesamte Datenbestand eines Laptops, Desktops, externen Laufwerks oder USB-Flash-Laufwerks einschließlich der Boot-Sektoren sowie der System- und Auslagerungsdateien geschützt.

### Sicheres Messaging

PGP Desktop Professional bietet Verschlüsselung für E-Mails und Instant Messaging zwischen Anwendern von AOL® Instant Messenger™ (AIM), damit Kommunikation vertraulich bleibt.

### Flexible Implementierungsoptionen

PGP Desktop Professional lässt sich als Einzelplatzinstallation in kleineren Unternehmen oder für gefährdete Anwender in größeren Unternehmen mit minimalem Zeitaufwand installieren. Wenn die Sicherheitsanforderungen steigen, können vorhandene Anwender problemlos in eine zentral verwaltete Architektur übernommen werden, ohne die Anwender zu beeinträchtigen.

### 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 Desktop Professional basiert ebenfalls auf der PGP Encryption Platform und ermöglicht die Nutzung vorhandener Anwender, Schlüssel und Konfigurationen, womit sich die Installation und die Umsetzung von Richtlinien zusätzlich beschleunigt. PGP Desktop Professional kann in Kombination mit anderen PGP-Verschlüsselungslösungen eingesetzt werden, um verschiedene Sicherheitsebenen abzudecken.

## Nutzen für das Unternehmen

### Schnelle Implementierung

- Der Einsatz von MSI-Standard-Softwarepaketen vereinfacht die Installation von vorkonfigurierten Clients.
- Die automatische Installation mithilfe von standardisierten Mechanismen zur Softwareverteilung minimiert den Aufwand für den Endanwender und reduziert die Häufigkeit von Helpdesk-Anfragen.

### Zentrale Sicherheitsrichtlinien statt individueller Entscheidungen

- Die Verschlüsselungsrichtlinien für E-Mails und Festplatten können zentral erstellt und umgesetzt werden. Daten werden damit automatisch geschützt, ohne dass sich der Anwender an neue Verfahren gewöhnen muss.
- Die Verschlüsselung von gesamten Festplatten, die Passwortregeln und weitere Sicherheitsrichtlinien können ebenfalls zentral konfiguriert und umgesetzt werden.

### Verringerte Betriebs- und Wartungskosten

- Die vereinheitlichte webbasierte Managementkonsole von PGP Universal™ Server bietet vereinfachte und intuitive Funktionen für die Richtlinien- und Client-Verwaltung.
- Automatische Updates werden direkt vom PGP Universal Server bezogen, so dass keine zusätzlichen Installationspakete erstellt und implementiert werden müssen.

### Zuverlässiger Zugriff auf geschützte Daten

Die von PGP Corporation patentierte Additional Decryption Key-Technologie (ADK) ermöglicht Unternehmen den Zugriff auf geschützte Daten ohne Verwendung von Master-Passwörtern oder geteilten Schlüsseln.

## Vorteile für Arbeitsgruppen

### Anmeldung mehrerer Anwender an einer Workstation

Mehrere Anwender können mit individuellen Authentifizierungsdaten auf dasselbe verschlüsselte Laufwerk zugreifen.

## Einfacher, unkomplizierter Betrieb

Mit Kontextmenüs und einer intuitiven Anwendungsoberfläche lässt sich PGP Whole Disk Encryption sehr einfach bedienen.

## Merkmale und Funktionen

### Neu: Integrierte Windows-Anmeldung

Die integrierte Anmeldung an Microsoft Windows erlaubt die Synchronisation von Passwörtern. Es ermöglicht so eine strikte Umsetzung der Richtlinien für Windows-Domain-Passwörter, ohne die Windows-Anmeldedaten zu verändern.

### Neu: Selbsterweiternde PGP Virtual Disk-Laufwerke

Selbsterweiternde PGP Virtual Disk-Laufwerke vergrößern sich automatisch, wenn der Datenbestand wächst.

### Neu: Partitionsorientierte Verschlüsselung

Mit PGP Whole Disk Encryption können Anwender bestimmte Festplattenpartitionen verschlüsseln. So ist die Software mit Systemen kompatibel, auf denen mehrere Betriebssysteme installiert sind oder eine spezielle Wiederherstellungspartition eingerichtet ist.

### Daten weitergeben oder gemeinsam nutzen

Mit PGP® Virtual Disk, PGP® Zip und PGP® Self-Decrypting Archive lassen sich verschlüsselte, vom Speichermedium unabhängige Datenpakete erstellen, in denen bestimmte Dateien transportiert und zur gemeinsamen Nutzung weitergegeben werden können.

### Sicheres Löschen von Dateien

PGP Shredder und PGP Wipe entfernen Dateien endgültig.

## Funktionen bei zentraler Verwaltung

### Zentral definierte Sicherheitsrichtlinien

- Mail Policy sorgt für die Umsetzung von Richtlinien für die E-Mail-Verschlüsselung und für digitale Signaturen.
- Policy übernimmt die Umsetzung von Richtlinien für die Laufwerksverschlüsselung und verhindert, dass Anwender Laufwerke entschlüsseln oder die Software deinstallieren.
- Nutzung vorhandener LDAP- und Microsoft Active Directory-Dienste für die automatische Zuordnung von Richtlinien auf Basis von Anwendergruppenattributen.

### Ereignisprotokollierung

- Alle administrativen Vorgänge werden für Revisionen und Sicherheitsüberprüfungen protokolliert.

## Wiederherstellungspasswort

- Einmal verwendbare Wiederherstellungspasswörter helfen bei der Remote-Unterstützung.

### Technische Daten

#### Unterstützte Betriebssysteme

- Windows XP SP1 oder SP2
- Windows 2000 Professional SP4
- Mac OS X 10.4 (Universal Binary – Intel und PPC)\*

#### Sprachen

- Englisch
- Deutsch
- Japanisch

#### Authentifizierungsoptionen

- OpenPGP-Schlüssel (RFC 2440)
- X.509-Zertifikate

#### Zwei-Faktoren-Authentifizierung

Die aktuelle Liste der unterstützten Geräte finden Sie unter [www.pgp.com/products/desktop\\_pro/tech\\_specs.html#smartcards](http://www.pgp.com/products/desktop_pro/tech_specs.html#smartcards)

#### Messaging-Protokolle

- POP3
- IMAP
- SMTP
- MAPI
- Lotus Notes

#### Messaging-Sicherheitsstandards

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

#### Unterstützte E-Mail-Clients

- Microsoft Outlook XP SP3, Outlook 2003 SP2, Outlook 2000 SP3, Outlook Express 6, Entourage 2004
- Lotus Notes 5.0.11 und 6.2 für Windows
- Mozilla Thunderbird 1.5
- Qualcomm Eudora 6.2 und 7 für Windows
- Apple Mail 2.1

#### Symmetrische Verschlüsselungsalgorithmen – PGP Whole Disk Encryption

- AES (256 bit)

(Aktuelle Produktspezifikationen finden Sie unter [www.pgp.com/products/desktop\\_pro/tech\\_specs.html](http://www.pgp.com/products/desktop_pro/tech_specs.html))

#### Voraussetzungen für die zentrale Verwaltung

- PGP Universal Server 2.5.\*\* Weitere Informationen zu PGP Universal Server finden Sie unter [www.pgp.com/products/universal\\_server/tech\\_specs.html](http://www.pgp.com/products/universal_server/tech_specs.html)

\* Unter Mac OS X wird PGP Whole Disk Encryption nur für Laufwerke unterstützt, die nicht für den Systemstart verwendet werden.

\*\* PGP Universal Server erfordert einen dedizierten Server.

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.

