



PGP® Whole Disk Encryption 9.9

Aktiver Schutz vertraulicher Daten auf Laufwerken und Wechselmedien

teil der PGP® Encryption Platform

Vorteile

- **Schneller, automatischer Betrieb** – Datenschutz ohne zusätzlichen Aufwand für den Anwender.
- **Richtlinienumsetzung** – Automatische Umsetzung des Datenschutzes anhand zentral verwalteter Richtlinien.
- **Beschleunigte Bereitstellung** – vollständige Laufwerksverschlüsselung mit der vorhandenen Infrastruktur.
- **Verringerte Betriebskosten** – durch zentralisierte automatische Verschlüsselungsrichtlinien.

PGP-Kunden im Fokus

Continental Corporation, ein führender, deutscher Automobilzulieferer, schützt E-Mails an Kunden mit PGP® Desktop Email und vertrauliche Daten auf 6.000 Laptops mit PGP® Whole Disk Encryption.

Umfassende Festplattenverschlüsselung für Desktop-PCs, Laptops und Wechselmedien

Mobile Computer entwickeln sich zunehmend zum Standardwerkzeug in Unternehmen und steigern die Produktivität der Anwender. Gerade weil diese Geräte so leicht zu transportieren sind, nimmt aber auch die Gefahr von Verlusten und Diebstählen zu. Wenn dadurch vertrauliche Daten in falsche Hände gelangen, kann es zu finanziellen Verlusten, juristischen Problemen und Rufschädigung kommen.

PGP Whole Disk Encryption ermöglicht Unternehmen umfassende und permanente Laufwerksverschlüsselung zum schnellen und kosteneffizienten Datenschutz auf PCs, Laptops und Wechselmedien. Die mit PGP Whole Disk Encryption verschlüsselten Daten sind dauerhaft gegen unberechtigten Zugriff geschützt. Das bedeutet hohe Sicherheit für geistiges Eigentum, Kunden- und Partnerdaten sowie Markenwert.

PGP Whole Disk Encryption kann optional mit PGP Universal™ Server kombiniert werden. Mit PGP Universal Server können Sicherheitsrichtlinien für unterschiedliche Anwendergruppen direkt aus vorhandenen Personallisten zentral definiert und umgesetzt werden. Die integrierten Funktionen zur zentralisierten Berichterstellung und Protokollierung liefern umfassende Informationen über den Status der mit PGP Whole Disk Encryption im Unternehmen erreichten Datensicherheit und vereinfachen die Einhaltung von Compliance- und Revisionsanforderungen.

Schutz ganzer Datenträger

PGP Whole Disk Encryption verschlüsselt den gesamten Inhalt von Laptop- und Desktop-Computern, externen Laufwerken und USB-Flash-Laufwerken einschließlich der Boot-Sektoren und System- und Swap-Dateien. Die Verschlüsselung wird – unbemerkt vom Anwender – im Hintergrund durchgeführt, sodass die Daten jederzeit automatisch geschützt sind.

Mit der PGP Encryption Platform kompatibel

PGP Whole Disk Encryption 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 Whole Disk Encryption kann auch in Kombination mit anderen PGP-Verschlüsselungsanwendungen verwendet werden, um mehrere Sicherheitsebenen zu schaffen.

Einfache automatische Funktionsweise

Sobald PGP Whole Disk Encryption bereitgestellt ist, wird die Verschlüsselung vollkommen transparent im Hintergrund durchgeführt – die Anwender können einfach wie gewohnt weiterarbeiten.

Die Software ver- und entschlüsselt die Daten in Echtzeit. Dadurch ist permanenter Datenschutz ohne Änderung der gewohnten Arbeitsabläufe des Anwenders gewährleistet.

- **Single Sign-on** – Vereinfachte Anmeldung mit vorhandenem Windows-Passwort.
- **Neu: Erweiterte Unterstützung für länderspezifische Tastaturen** – Unterstützung für 30 länderspezifische Tastaturbelegungen bei der Pre-Boot-Authentifizierung.
- **Viele Möglichkeiten zum Schützen von Daten** – Schutz von vertraulichen Daten mit PGP® Zip, PGP® SDA (selbstentschlüsselndes Archiv) und PGP® Virtual Disk.
- **Sicheres Löschen von Dateien** – Zuverlässiges, endgültiges und spurloses Entfernen vertraulicher Daten von Laufwerken.

Umsetzen von Sicherheitsrichtlinien

Die in PGP Universal Server konfigurierten Sicherheitsrichtlinien stellen sicher, dass sowohl lokale Datenträger als auch Wechselmedien verschlüsselt werden, sodass alle Daten auch dann, wenn sie auf leicht verlierbaren Geräten transportiert werden, sicher vor unbefugtem Zugriff sind.

- **Neu: Erweiterte Gerätesicherheitskontrolle** – Eingeschränkter Zugriff auf Systeme nach fehlgeschlagenen Pre-Boot-Anmeldeversuchen.
- **Neu: PGP® Endpoint Integration möglich** – Die Kombination von Festplattenverschlüsselung und Gerätekontrolle senkt das Risiko einer Datenlücke deutlich.
- **Erweiterte Kontrolle** – Anforderungen werden besser umgesetzt, da festgelegt werden kann, welche Funktionen für den Anwender verfügbar, sichtbar und obligatorisch sind.
- **Erweiterte Berichterstellung** – Überprüfung und Berichterstellung zum Datenschutzstatus, um bestehende Vorschriften einzuhalten und Datenmissbrauch vorzubeugen.
- **Erweiterte Authentifizierungsoptionen** – Authentifizierungsmöglichkeiten vor dem Laden des Betriebssystems mit Smartcards (zum Beispiel RSA SID800).
- **TPM (Trusted Platform Module)-Unterstützung** – Schützt Verschlüsselungsschlüssel vor unbefugtem Zugriff.

Schnellere Bereitstellung

Wenn PGP Whole Disk Encryption in Kombination mit der einheitlichen Verwaltungskonsole von PGP Universal Server eingesetzt wird, können Sicherheitsrichtlinien in Echtzeit erstellt, umgesetzt und aktualisiert werden. Durch diese Kombination wird der zum Bereitstellen der Laufwerksverschlüsselung benötigte Zeit- und Arbeitsaufwand verringert.



Umfassender Schutz für lokale und Netzwerk-Medien.

Neu: Beschleunigter Bereitstellungsvorgang – Schnellere Bereitstellung durch automatische Installation und Konfiguration.

Geringere Betriebskosten

Für PGP Whole Disk Encryption 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 Whole Disk Encryption 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 vorhandener Personallisten.
- **Wiederherstellungspasswort** – Automatisches Generieren und Speichern eines eindeutigen, einmal verwendbaren Wiederherstellungspassworts, um den autorisierten Zugriff auf verschlüsselte Daten sicherzustellen.
- **Erweiterbarer Schutz** – Ermöglicht das Verwalten von PGP® NetShare oder sonstiger Anwendungen der PGP Encryption Plattform.

Technische Spezifikationen

PGP Whole Disk Encryption unterstützt Windows Vista (alle 32- und 64-Bit-Editionen), Windows XP (SP1, SP2 und SP3), Windows 2000 Professional (SP4) und Mac OS X 10.4 (Intel). Eine vollständige Aufzählung der technischen Spezifikationen finden Sie auf www.pgp.com.

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
www.pgp.com

PGP Corporation Hauptsitz
Tel: +1 650 319 9000

PGP (GB) Ltd.
Tel: +44 (0)20 8606 6000

PGP Deutschland AG
Tel: +49 69 838310 0

PGP Japan K.K.
Tel: +81 03 4360 8308

© 2008 PGP Corporation
WDEDSDE081009