



PGP® Desktop Storage 9.5

Flexible Speicherverschlüsselung für Unternehmen

Teil der PGP® Encryption Platform

Schutz von Daten auf Laptops, Desktops und gemeinsam genutzten Dateiservern

PGP Desktop Storage ermöglicht mit PGP® Whole Disk Encryption die flexible, mehrschichtige Verschlüsselung zum Schutz von vertraulichen Dateien, die lokal auf Desktop- oder Laptopsystemen gespeichert sind. Mit PGP® NetShare können Dateien sicher gemeinsam mit ausgewählten Kollegen genutzt werden. Dieses Konzept gewährleistet, dass nur berechtigte Anwender Zugriff auf sensible Daten erhalten und dass die von Geschäftspartnern oder Behörden definierten Vorgaben zur Weitergabe und zum Schutz von Informationen erfüllt werden.

Vollständiger Laufwerksschutz

Mit PGP Whole Disk Encryption wird der gesamte Datenbestand eines Laptops, Desktops, externen Laufwerks oder USB-Flash-Laufwerks einschließlich der Boot-Sektoren sowie der System- und Auslagerungsdateien geschützt. Die Verschlüsselung ist für den Anwender transparent.

Durchgängige Dateiverschlüsselung auf Servern

PGP NetShare erweitert die Zugriffskontrolle für Dateiserver mit zuverlässiger durchgängiger Verschlüsselung. Sicherheitsadministratoren und Eigentümer von Daten konfigurieren die Zugriffsrechte einzelner Personen oder bestimmter Gruppen. Dokumente, Tabellenkalkulationen, Präsentationen, Video-, Audio- und Internet-Daten werden beim Speichern in einen geschützten Ordner automatisch verschlüsselt.

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

Nutzen für das Unternehmen

Anwenderfreundlichkeit

- Die Endanwender nutzen und schützen ihre lokal gespeicherten oder gemeinsam genutzten Daten, ohne neue Arbeitsabläufe einführen zu müssen.
- Eine Anwenderschulung ist nicht erforderlich.

Einfache Administration, vereinheitlichte Infrastruktur

- Die webbasierte Managementkonsole von PGP Universal™ Server ermöglicht die einfache Verwaltung von PGP Desktop Storage.
- Tools für eine reibungslose Installation und Datenwiederherstellung.
- Sicherheitsadministratoren legen Richtlinien fest, die zentral umgesetzt werden können.
- Der Einsatz von MSI-Standard-Softwarepaketen vereinfacht die Implementierung von vorkonfigurierten Clients.

Integration in die Unternehmensstruktur

- Keine Änderungen an der vorhandenen Speicher- und Netzwerkinfrastruktur erforderlich
- Nutzung vorhandener LDAP- und Microsoft Active Directory-Dienste für die zentrale Zuordnung von Sicherheitsrichtlinien zu Anwendergruppen

Vorteile für Arbeitsgruppen

Flexible, skalierbare Sicherheit

- Kostenwirksame, bedarfsabhängige Skalierung vom selektiven Datenschutz bis zur unternehmensweiten Implementierung.
- Die Dateneigentümer können Zugriffskontrollen für gemeinsam genutzte Daten selbst verwalten oder die Zugriffsadministration delegieren.
- Verschlüsselung und Entschlüsselung finden auf dem Client transparent statt. PGP Desktop Storage kann deshalb für mehrere tausend Anwender ausgelegt werden, ohne dass sich die Leistung von Systemen, Servern oder Netzwerken verschlechtert.

Merkmale und Funktionen

Neu: Schnellerer und verbesserter Schutz

Beschleunigung der Verschlüsselungsfunktionen, eine effektivere Nutzung des Prozessors und Schutzmechanismen für Stromausfälle verbessern die Bedienbarkeit für Anwender.

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.

Transparent für den Anwender

PGP NetShare-Anwender nutzen Dokumente wie zuvor, ohne ihre Arbeitsabläufe zu ändern oder Schulungen zu absolvieren.

Zentrale Verwaltung, Installation und Richtlinien

Die automatische Bereitstellung, Anwender- und Schlüsselverwaltung sowie die Umsetzung von Richtlinien für die Verschlüsselung von E-Mails, Festplatten und Netzwerkdateien erfolgt mit der Managementkonsole von PGP Universal Server.

Zuverlässiger Datenzugriff

Die von PGP Corporation patentierte Additional Decryption Key-Technologie (ADK) gewährleistet im Unternehmen den Zugriff auf verschlüsselte Daten.

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.

Funktionen bei zentraler Verwaltung

Zentral umgesetzte Sicherheitsrichtlinien

- Nutzung vorhandener LDAP- und Microsoft Active Directory-Dienste für die automatische Zuordnung von Richtlinien auf Basis von Gruppenattributen.
- Policy übernimmt die Umsetzung von Richtlinien für die Laufwerksverschlüsselung und verhindert, dass Anwender Laufwerke entschlüsseln oder die Software deinstallieren.
- Ermöglicht die Erstellung und Veränderung von Ressourcen, die durch PGP NetShare geschützt sind.

Ereignisprotokollierung

- Alle administrativen Vorgänge werden für Revisionen und Sicherheitsüberprüfungen in detaillierten Protokollen festgehalten.

Wiederherstellungspasswort

- Die automatische Rücksetzung des Wiederherstellungspassworts nach jeder Verwendung reduziert die administrativen Kosten.

Technische Daten

- Unterstützte Betriebssysteme
- Windows XP SP1 oder SP2
- Windows 2000 Professional SP4

Unterstützte Speichersysteme – PGP NetShare

- Windows-Dateifreigaben (SMB, CIFS und Samba)
- Lokal angeschlossene Festplattenlaufwerke (intern und extern)
- USB-Flash-Laufwerke

Sprachen

- Englisch
- Deutsch
- Japanisch

Authentifizierungsoptionen

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

Symmetrische Verschlüsselungsalgorithmen – PGP Whole Disk Encryption

- AES (256 bit)

Symmetrische Verschlüsselungsalgorithmen – PGP NetShare

- AES (256 bit) im EME-Modus

Zwei-Faktoren-Authentifizierung

Die aktuelle Liste der unterstützten Geräte finden Sie unter www.pgp.com/products/desktop_storage/tech_specs.html#smartcards

(Aktuelle Produktspezifikationen finden Sie unter www.pgp.com/products/desktop_storage/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

* 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.

