



PGP® Endpoint 4.3

Verhindert Datenverlust bei Verwendung
von Wechseldatenträgern und mobilen Geräten

Teil der PGP® Encryption Platform

Vorteile

- **Einfacher, automatischer Betrieb** – Ermöglicht eine sichere und autorisierte Verwendung von Wechseldatenträgern ohne Änderung der Arbeitsabläufe des Endanwenders und ohne Produktivitätsverlust.
- **Erweiterte Sicherheitsrichtlinien** – Erweitert die Sicherheitsrichtlinien für die Geräteverwendung über USB-, FireWire-, WiFi- und Bluetooth-Verbindungen, verschlüsselt automatisch und richtliniengesteuert die auf Wechseldatenträgern gespeicherten Daten; protokolliert bei Bedarf die Verwendung und liefert Compliance-Nachweise.
- **Schnellere Bereitstellung** – Verringerter Zeitbedarf für Einrichtung bedeutet schnelleren Schutz für das Unternehmen ohne Änderung der Arbeitsabläufe für den Benutzer und unter Beibehaltung der vorhandenen Verzeichnisstruktur.
- **Verringerte Betriebskosten** – Durch schnelle Bereitstellung, einfache Bedienung, zentrale Verwaltung und automatische Umsetzung von Sicherheitsrichtlinien.

PGP-Kunden im Fokus

„Bei unseren Angebotsvergleichen kamen wir zu dem Schluss, dass die Produkte der PGP Corporation die für uns optimale Datenschutzlösung anbieten.“

Alex Clonaris
IT-Sicherheitsexperte
Henry Davis York

Integrierte Datenverschlüsselung und Umsetzung von Geräterichtlinien für Wechseldatenträger

Wechseldatenträger (wie zum Beispiel USB-Sticks und CD/DVD-Laufwerke) und mobile Verbindungstechnologien (wie WiFi, FireWire und Bluetooth) werden auch im Unternehmensbereich immer beliebter. Sie sind praktisch, erhöhen die Produktivität, stellen das Unternehmen aber auch vor neue Sicherheitsrisiken. Die auf diesen mobilen Endpunktgeräten und -medien gespeicherten Daten beinhalten gegebenenfalls geistiges Eigentum oder vertrauliche Kundendaten.

Die unternehmensinternen Regelungen und der Ausbildungsstand der Mitarbeiter reichen gegebenenfalls nicht aus, um die Daten ausreichend gegen absichtliche oder versehentliche Preisgabe durch Unternehmensangehörige zu schützen. Die Preisgabe vertraulicher Daten aufgrund von Verlust oder Diebstahl eines mobilen Geräts oder Wechseldatenträgers kann zu finanziellen Einbußen, juristischen Komplikationen und Rufschädigungen führen.

PGP® Endpoint bietet eine integrierte Sicherheit, die mobile Geräte und Wechseldatenträger (wie zum Beispiel USB-Geräte, CDs und DVDs) erkennt, autorisiert und sichert. Diese Sicherheitslösung setzt zentrale definierte Richtlinien zur Geräteverwendung um und verhindert Datenverluste bei Netzwerkverbindungen und Verbindungen zu Peripheriegeräten (zum Beispiel über Bluetooth, WiFi und FireWire). PGP Endpoint hilft Unternehmensdaten sicherer zu machen und überwacht den Austausch von Daten zwischen Endpunktgeräten und dem Netzwerk.

Mit der PGP Encryption Platform kompatibel

PGP Endpoint ist ein Teil von PGP Encryption Platform. PGP Encryption Platform bildet den unternehmensweiten Rahmen und die Architektur für das Management gemeinsamer Datennutzung durch Benutzer, zur Verwaltung von Schlüsseln und Richtlinien sowie für die Bereitstellung automatisierter plattform-, system- und anwendungsübergreifender, integrierter Verschlüsselungsanwendungen. In Kombination mit PGP® Whole Disk Encryption stellt PGP Endpoint eine integrierte Lösung zur Vermeidung von Endpunkt-Datenverlusten in Unternehmen dar.

Umsetzen von Sicherheitsrichtlinien

PGP Endpoint schützt und sichert Daten am Speicherort und bei der Übertragung. Das Umsetzen der Sicherheitsrichtlinien eines Unternehmens mit PGP Endpoint hat folgende Vorteile:

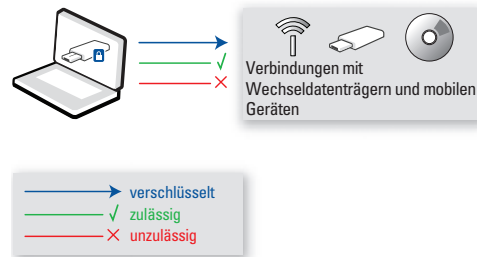
- **Granulare Medienbenutzungsrichtlinien** – Unerlaubte Geräte werden gesperrt. Unternehmensübliche Medien wie zum Beispiel CDs und DVDs können autorisiert und zulässige Zugriffs- und Verschlüsselungsarten sowie weitere Parameter festgelegt werden; Zugriffslisten zum Festlegen von Benutzerberechtigungen.
- **Prüfpfade** – Compliance durch Protokollierung aller Geräteverwendungen; optionale Aufzeichnung aller zwischen Geräten und Netzwerk ausgetauschten Daten.
- **Präziser Schutz von Dateien und Daten** – Blockieren von PS/2- und USB-Keyloggern; Festlegen zulässiger Dateitypen; Festlegen von Höchstgrenzen für Datenübertragungen.
- **Remote-Benutzer und nicht verbundene Benutzer** – Umsetzen von Richtlinien auch bei Nichtverfügbarkeit von Netzwerkverbindungen.
- **Flexible Verschlüsselungsmöglichkeiten** – Verwaltung der Datenverschlüsselung auf Wechseldatenträgern mit flexiblen Optionen (zentral festgelegte Richtlinien oder je nach Benutzungszeitpunkt) Integration mit PGP Whole Disk Encryption.
- **Schutz von Benutzeranwendungen** – Die zusätzlich erhältliche Option Application Control ermöglicht die richtlinien-gesteuerte Kontrolle von Anwendungen. Application Control schützt Endpunkte vor Malware, Spyware, Zero-Day-Angriffen und unerwünschter oder unlizenzierter Software.

Einfache automatische Funktionsweise

Mit PGP Endpoint sind Daten auf mobilen Geräten ohne zusätzlichen Aufwand für den Anwender automatisch geschützt.

- **Geräteerkennung und Datenschutz „in Echtzeit“** – Automatische Erkennung von Geräten ohne Unterbrechung für den Anwender.
- **Flexible Benutzerberechtigungen** – Vermindertes Risiko der Verwendung unautorisierter Geräte ohne Beeinträchtigung der Anwenderflexibilität. Vielfältige Einstellmöglichkeiten für Benutzerberechtigungen wie zum Beispiel Art des Zugriffs und spezifische Geräteverwendung.

PGP und das PGP-Logo sind eingetragene Marken der PGP Corporation. Die Produkt- und Markennamen in diesem Schriftstück sind evtl. Markenzeichen oder eingetragene Markenzeichen ihrer jeweiligen Besitzer. Alle solchen Markenzeichen oder eingetragenen Markenzeichen sind alleiniges Eigentum ihrer jeweiligen Besitzer.



Verhindert Datenverlust am Endpunkt.

Schnellere Bereitstellung

Schnelle und einfache Bereitstellung von PGP Endpoint im Unternehmen durch folgende Funktionen:

- **Automatische Installation** – Keine Administratoreingriffe zur Bereitstellung erforderlich; verwendet Microsoft® MSI.
- **Nutzung vorhandener Verzeichnisdienste** – Transparente Einstellung von Benutzer- und Geräte Richtlinien über vorhandene Microsoft Windows® Active Directory- oder Novell® eDirectory™-Infrastrukturen.

Geringere Betriebskosten

PGP Endpoint verringert den Arbeits- und Zeitaufwand für die Bereitstellung, Schulungskosten für Endanwender entfallen und die IT-Abteilung wird nicht stärker durch telefonische Anfragen belastet. Mit PGP Endpoint können Unternehmen ihre Sicherheitsrichtlinien für Anwender und Verschlüsselung zentral verwalten und die bei Verwendung ungleichartiger Verschlüsselungslösungen entstehenden Betriebskosten reduzieren.

Zentralisierte Verwaltung

PGP Endpoint wird über den PGP Endpoint Administrations-server zentral verwaltet. Die Vorteile:

- **Anwender- und Geräteverwaltung** – Möglichkeit zur Festlegung granularer Richtlinien mit vielfachen Anwender- und Geräteoptionen.
- **Wiederherstellung und temporäre Authentifizierung** – Zahlreiche Aussperrungs- und Wiederherstellungsoptionen einschließlich temporärer Benutzerberechtigungen.
- **Unabhängig von der Infrastruktur** – Kann in praktisch jedem Netzwerk eingesetzt werden – unabhängig von der Komplexität des Netzwerks oder der Anzahl der Anwender.

Technische Spezifikationen

PGP Endpoint unterstützt Windows 2000 Professional (SP4 oder höher), Windows XP (SP2 oder höher) und Windows Vista® (32- und 64-Bit-Editionen). Eine vollständige Aufzählung der technischen Spezifikationen finden Sie unter www.pgp.com.



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
EPTDSDE081009