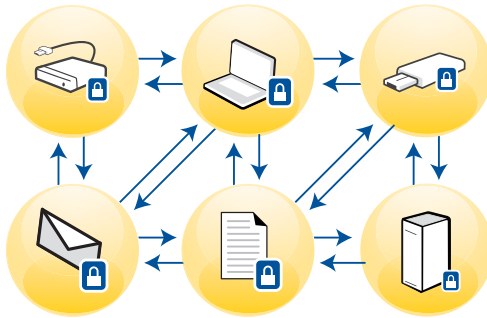
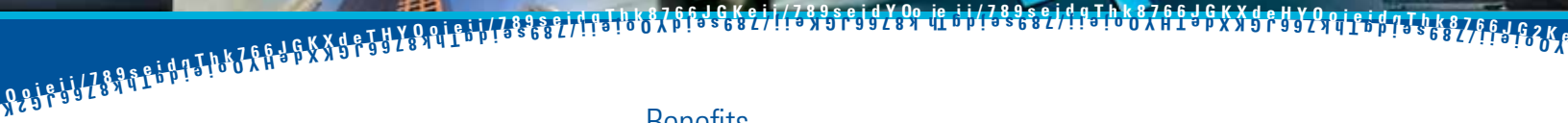




PGP® Desktop Corporate

Flexible email and storage encryption for distributed professionals



Protection for disks, files, and email.

Benefits

- **Easy, automatic operation** – Protects data without changing the user experience.
- **Enforced security policies** – Automatically enforce email and data protection with centrally managed policies.
- **Accelerated deployment** – Achieves end-to-end email and data encryption integrating with the existing infrastructure.
- **Reduced operation costs** – Result from centrally automating email encryption policies.

Secure confidential data in email, on laptops and desktops, and shared on file servers

Email, mobile computers, and file servers have quickly emerged as industry-standard tools for increasing communication, user productivity, and collaboration. Unfortunately, unprotected email, files, and devices pose a critical risk to an enterprise's most sensitive data: customer information, financial data, trade secrets, and other proprietary information. Exposure of this data can result in financial loss, legal ramifications, and brand damage.

PGP® Desktop Corporate provides flexible, multilayered encryption using PGP® Desktop Email and PGP® Whole Disk Encryption to secure confidential data in email and in files stored on local desktop or laptop systems and using PGP® NetShare to securely share files with selected colleagues. This approach ensures that only authorized users can access sensitive data, fulfilling partner and regulatory requirements for information partitioning and security.

- **PGP Desktop Email** – Delivers all of the encryption functionality necessary for protecting an organization's email communications in a single, easy-to-use and easy-to-manage solution.
- **PGP Whole Disk Encryption** – Locks down the entire contents of a laptop, desktop, external drive, or USB flash drive, including boot sectors, system, and swap files.
- **PGP NetShare** – Extends file server access controls to include strong end-to-end encryption, allowing content owners or security administrators to specify access rights for groups or individuals.

PGP® Encryption Platform–Enabled

PGP Desktop Corporate is a PGP Encryption Platform–enabled application. The PGP Encryption Platform provides a strategic enterprise encryption framework for shared user management, policy, and provisioning, automated across multiple, integrated encryption applications. As a PGP Encryption Platform–enabled application, PGP Desktop Corporate can be used with PGP Universal™ Server to manage existing policies, users, keys, and configurations, expediting deployment and policy enforcement. PGP Desktop Corporate can also be used in combination with other PGP® encryption applications to provide multiple layers of security.

PGP® Customer Spotlight

Global relocation services company SIRVA chose PGP® Whole Disk Encryption to secure laptops and mobile devices along with PGP® Desktop Email and PGP Universal™ Gateway Email to secure communications internally and with customers and partners.

Easy, Automatic Operation

Once PGP® Desktop Corporate is deployed, its operation is completely transparent—users simply continue to work as usual. The software automatically protects email and local and shared information according to policy, ensuring that users never forget to secure confidential data.

- **Single sign-on** – Provides simplified login experience using existing Windows' password.
- **Encryption that follows the file** – Ensures that files stay encrypted locally, on the server, and in backups.
- **Automatic messaging security** – Automatically encrypts, decrypts, digitally signs, and verifies email messages according to individual or centrally managed policies.

Enforced Security Policies

Security policy configured in PGP Universal™ Server ensures that data and email messages are secured automatically, without requiring changes in user behavior.

- **Protect data by application policy** – Enforce encryption for desktop applications, securing documents wherever stored or used.
- **Expanded device security policy** – Limit access to systems after failed pre-boot authentication login attempts.
- **Client controls** – Enable the organization to better meet security requirements by locking down which features are enabled, visible to the user, and enforced.
- **Status logging & reporting** – Tracks and reports on the state of protection in the organization to satisfy regulatory requirements and help prevent a data breach.
- **Strong authentication options** – Perform pre-boot authentication using smart cards such as the RSA SID800.

Accelerated Deployment

Used together, PGP Desktop Corporate and PGP Universal Server's unified management console establish, enforce, and update security policy in real time. This combination reduces the time and effort required to deploy comprehensive data encryption.

Reduced Operation Costs

With PGP Desktop Corporate, no special training is required for end users. This approach accelerates deployment time, reduces training costs, and avoids any increase in help desk calls.

- **Flexible, scalable security** – Scale to thousands of users without degrading system, server, or network performance.

PGP Universal Server Management

PGP Desktop Corporate can be centrally deployed and managed when used with PGP Universal Server (optional), enabling organizations to easily set and enforce data security policies throughout the enterprise.

- **Centrally enforced security policy** – Automatically enforces protection of sensitive data and email using security policies driven by an existing corporate directory.
- **Extensible protection** – Allows management of any other PGP® Encryption Platform-enabled application.

Technical Specifications

For complete technical specifications, please visit www.pgp.com.



www.pgp.com

© 2010 PGP Corporation. PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners.

DTCORPDS100113