

Help protect business data in transit and at rest—even beyond the enterprise network—without increasing IT complexity



IBM Data Security Services for endpoint data protection – PGP Corporation encryption software and support

Highlights

- ***Helps protect sensitive data on endpoint devices—including laptops, handhelds, and removable storage devices—against unauthorized exposure***
- ***Accelerates deployment and expand coverage as needed with a scalable platform***
- ***Reduces need for in-house security experts with IBM 24x7x365 support and professional services***

Protecting data across a growing number and variety of endpoints

Today data resides on a wide array of endpoints for both convenience and business efficiency. The endpoint devices that aid business operations—including laptops, USB flash drives, and personal digital assistants (PDAs)—can be lost, stolen, or accessed by unauthorized persons, exposing sensitive business data. You need to protect business data at rest, in motion, and in use, even beyond the enterprise network, without increasing IT complexity. IBM understands these concerns and now delivers award-winning endpoint encryption that combines the PGP® Encryption Platform from PGP

Corporation with purpose-built IBM Data Security Services. PGP Corporation encryption software and support provides a comprehensive solution that helps protect sensitive data across endpoints, removable storage media, and e-mail, against loss, theft, or unauthorized access.

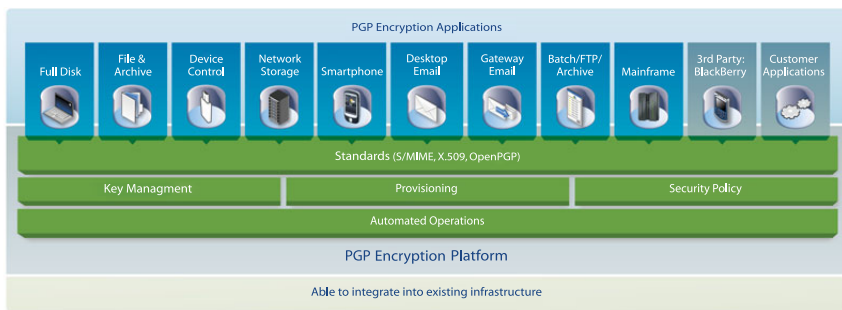
The IBM endpoint encryption solution builds security into the most commonly used applications, protecting data wherever it resides—from outbound e-mail, to file servers, to removable storage devices such as USB flash drives and PDAs. The solution helps organizations consistently enforce corporate and regulatory security policies.

Our endpoint encryption solution can help you:

- *Protect stored data even when an endpoint device is lost or stolen*
- *Enforce device-usage policy and protect data automatically to optimize data security while the data is in use on an endpoint device*
- *Monitor and control the use of external storage devices for storing and transporting data*
- *Safeguard e-mail where it is sent, as it travels, and where it is received*
- *Enable collaboration and maintain confidentiality on shared servers*
- *Cost-effectively manage policy and reporting for encryption applications and scale the solution as your needs grow*

Decreasing risk to data on endpoints with an enterprise encryption platform

Point encryption applications that protect only one type of data or one locale are rapidly being replaced by platform-based solutions that scale to provide a range of data security options, depending on where data is stored, how it is shared, and who needs access. The PGP Encryption Platform provides operational efficiencies and scalability to accommodate



PGP Encryption Platform

growth. Complementing PGP technology and software, IBM services assess requirements, design architecture, plan implementation, and manage deployment to configure data protection policies for your business needs.

As part of a complete data protection solution, IBM data security experts can deploy the PGP Encryption Platform. Multiple encryption applications can also leverage a single framework to help expedite deployment, reduce operational costs, and free administrative resources for other tasks. Multiple encryption applications on the platform extend the value proposition beyond the endpoint by helping to:

- *Provide secure e-mail protection at an enterprise gateway level*
- *Deliver file encryption on most well-known server operating system platforms (including mainframes)*

- *Leverage standards-based encryption key management and digital certificates that can be integrated for securing business transactions at the application layer*

The key technology components of the IBM endpoint encryption solution include:

- **PGP Universal™ Server**—delivers an extensible framework that supports scalable, centralized gateway and desktop encryption management, deployment automation, and policy enforcement across applications
- **PGP Whole Disk Encryption**—provides comprehensive, nonstop encryption to help protect files on desktops, laptops, and removable media, transparently securing all disk contents, including system and temporary files, and enabling quick, cost-effective protection for sensitive data

- **PGP NetShare**—enables teams to securely share documents on file servers by automatically and transparently encrypting files with granular group access policies
- **PGP Desktop Email**—secures e-mail communications between sender and recipient using centrally defined, policy-based encryption that leverages industry standards for interoperability and transparency
- **PGP Endpoint**—provides built-in security that detects, authorizes, and secures removable storage devices and media (such as USB drives, CDs, and DVDs)
- **PGP Universal Gateway Email**—delivers standards-based enterprise e-mail encryption and digital signatures without client software

Deploying a platform-driven encryption solution

Effective endpoint encryption solutions offer centralized management that controls policy and data access without requiring end users to make enforcement decisions, or burdening administrators with complicated and resource-intensive tasks.

All PGP endpoint encryption applications are managed through the award-winning, extensible PGP Encryption Platform, which enables phased deployment and capabilities such as:

- *Centralized policy and key management*
- *Support for Microsoft® Windows® and Apple® Mac OS X operating systems*
- *Centralized logging and auditing of encrypted devices*
- *Standards-based encryption of data at rest, in motion, and in use, even beyond the enterprise network*
- *Patented PGP Additional Decryption Key (ADK) technology provides access to data protected by lost or forgotten keys*

Realizing the full value of your encryption investment

IBM understands data security at the enterprise level. Our consultants and specialists have experience with a wide range of industry solutions and IT architectures to help enterprises

quickly adopt an endpoint encryption solution. Our professional support services include:

- **Requirements and Planning Workshop** to define business, IT, and compliance-related requirements and develop a high-level approach to deploying an encryption solution
- **Implementation and Policy Design Services** to provide project planning, architecture and design, policy design, component testing, pre-production testing, deployment assistance, help desk enablement and skills transfer during project deployment phase
- **Support Desk** to support all PGP software licensed and deployed in the solution with escalation to PGP Corporation for break/fix or other issues

Why IBM and PGP Corporation?

IBM and PGP Corporation come together to bring a comprehensive and transparent endpoint encryption solution to market. Clients can confidently deploy PGP Corporation's market-leading products by leveraging



IBM Global Services' experience, reach, and scale. The IBM endpoint encryption solution, powered by products from PGP Corporation, includes industry-leading technology, strategic consulting, and risk analysis, deployment services, support, and solution management.

For more information

To learn more about IBM Data Security Services for endpoint data protection – PGP Corporation encryption software and support, please contact your IBM representative or IBM Business Partner, or visit the following Web site: ibm.com/services

© Copyright IBM Corporation 2009

IBM Global Services
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
March 2009
All Rights Reserved

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product or service names may be trademarks or service marks of others. References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.



Recyclable, please recycle.