

January 2005

---

# PGP<sup>®</sup> White Paper

## Top 10 Reasons: Why PGP Corporation?



## Introduction

There are many strategies and products that protect an organization's technology infrastructure, but only one for protecting digital information. **Encryption**—the business standard for securing email, stored data, corporate databases, mobile devices, and server-to-server communications—protects the data itself by scrambling it in a way only the intended recipient can decipher. Encryption is becoming an important component of a comprehensive enterprise security solution for several key reasons:

- **Most confidential corporate information is stored digitally** – Encrypting the data itself is the only way to ensure the highest level of security.
- **Email is everywhere, making protecting confidential information harder** – Encryption follows the data, protecting it at rest as well as in transit.
- **Regulations and corporate risk officers are demanding encryption of critical data** – Encrypting such data avoids loss of proprietary information, reduces the risk of litigation, and provides customers assurance that their personal data is secure.

Consequently, more and more companies are using encryption to secure private, confidential, and proprietary information wherever it resides. There are many types of encryption solutions available today, and sorting through these options requires organizations to understand their specific needs, objectives, desired functionality, and existing email system and corporate infrastructure. Although building effective cryptographic solutions is a difficult task that few vendors have successfully executed, selecting a vendor does not have to be as hard.

This white paper will describe what questions to ask when selecting an encryption vendor, including the top 10 qualifications to look for and potential problems if a vendor does not meet these requirements. The paper will also delineate what differentiates PGP Corporation from other security, secure-messaging, and encryption vendors.

## Top 10 Reasons: Why PGP Corporation?

When choosing an encryption solution, organizations should consider both the specific security functionality required as well as the viability, expertise, and reputation of the vendor. Following are the top 10 reasons why organizations should choose PGP Corporation as their preferred encryption vendor.

1. **Proven & vetted technology** – Desirable products are those that have been tested through long-term use of more than 10 years by organizations, individuals, and cryptography experts; proven their effectiveness in real-world situations; and verified vendor claims regarding functionality.

### **PGP Corporation:**

- Creates solutions based on mature encryption technology that has been proven effective and used by millions—including enterprises, government agencies, individuals, and cryptographers—for the last 14 years.

- Is the only commercial software vendor that publishes source code for peer review, ensuring the integrity of its encryption implementation and demonstrating there are no “back doors”<sup>1</sup> that could compromise data security.
- Has a long history as a leader with a worldwide reputation in the security industry.

**Other vendors:**

- Lack relevant, practical experience that includes years of product testing and consistent use of products in enterprise settings.
- Create proprietary solutions or products based on “revolutionary” new crypto algorithms for which source code is unavailable.
  - As a result, companies do not know exactly how or if these products will encrypt data.
  - Because product code is not available for review, there is also an increased risk of flawed code and potential “back doors.”
- Do not have a long history of building and deploying encryption solutions and may lack the experience necessary to create effective products.

- 2. Based on industry standards** – Choosing products based on current industry standards ensures interoperability with other products based on the same standards, maximizes investments in existing infrastructure technologies and products, and provides the highest level of security.

**PGP Corporation:**

- Supports all popular key and certificates formats, including the most common standards: OpenPGP, S/MIME, PGP/MIME, X.509, and FIPS 140-2 (a standard used by the U.S. federal government).
- Creates encryption technology that is considered the de facto standard for email security.
- Counts 90% of the Fortune<sup>®</sup> 100 and 74% of the Forbes<sup>®</sup> International 100 as customers, ensuring interoperability with other organizations and business partners already using PGP solutions.
- Benefits from decades of research by scientists, cryptographers, and IT specialists who are constantly reviewing and updating the core set of PGP encryption algorithms and how they are implemented.
- Adopts the latest research to ensure the strongest encryption available is incorporated in PGP products.

**Other vendors:**

- May base solutions on non-standard formats and use older encryption approaches (called “symmetric” solutions<sup>2</sup>) that rely on a single key to encrypt/decrypt information, compromising security.

---

<sup>1</sup> A “back door” is a means of accessing a computer program or system that bypasses security mechanisms. Whether installed as an administrative tool by programmers or as a means of attack by hackers, a back door is a security risk because there are always individuals looking for vulnerabilities to exploit.

<sup>2</sup> Symmetric key systems allow a recipient to use the same key to unlock or decrypt the encrypted file that the sender used. Although this approach provides much faster encryption and decryption than the two-key approach (called “asymmetric” encryption), management and distribution of symmetric keys can often be cumbersome and insecure.

- May use proprietary formats that require business partners and vendors to change existing encryption solutions or to purchase their solution to ensure interoperability.

- 3. Integrates with the existing email system or partner email systems** – Solutions based on open standards for public key formats and nonproprietary technologies will ensure the widest compatibility among deployments. Products based on plug-in architectures are usually designed for purposes other than security, lack support, and change frequently, making interoperability problematic.

**PGP Corporation:**

- Only employs encryption that supports industry-standard messaging protocols and de facto messaging standards.

**Other vendors:**

- Develop more expensive and complex solutions that rely on plug-ins<sup>3</sup> for interoperability and requiring IT support when these applications are modified or upgraded.

- 4. Integrated & comprehensive product suite** – Vendors that offer a unified encryption suite are more likely to have a long-term product roadmap based on a single product architecture that emphasizes interoperability and ease of use.

**PGP Corporation:**

- Offers an integrated suite of encryption products that share keys and a unified product architecture, simplifying deployment, maintenance, and support.
- Provides a broad product line that meets most security needs to encrypt email, disks, and batch/file transfers.
- Has a long-term vision that includes a comprehensive product roadmap, demonstrating a continued investment in and continued support of PGP encryption products.
- Has a sole focus on encryption that enables the development of complex encryption solutions too difficult for vendors that do not specialize in encryption to build.

**Other vendors:**

- Offer solutions that do not interoperate, share keys, or are not part of a product roadmap, making deployment difficult and integration with installed products potentially risky.
- Sell only one or two point solutions, requiring companies to use multiple vendors to address their encryption needs.

- 5. Flexibility to achieve multiple levels of security** – Most enterprises have indicated that granular policy options are a high priority to help meet corporate encryption needs for users who need to determine when and how to apply security policy to email as well as users who may not understand encryption or know how to apply it. At the same time, enterprises also need two-way policy enforcement so that outgoing messages sent securely are returned encrypted and not “in the clear.”

---

<sup>3</sup> Plug-ins are hardware or software modules that “plug into” another system and add a specific feature or service to it.

**PGP Corporation:**

- Develops products that support different policies for different users and classes of data: transparent and automated for most users, desktop for power users, end-to-end protection inside the company, and gateway protection for external security.
- PGP products take into account tradeoffs between highest security and ease of use, allowing policy to be extended to external users.
  - Automatic policy options can be based on domain, recipient, or even on keywords when interoperating with mail transfer agents (MTAs) such as Clearswift™ or IronPort™ Systems.
  - Several options are available for secure communications with recipients that do not have an installed encryption solution.

**Other vendors:**

- Offer “all-or-nothing” solutions that do not provide granular security or two-way policy enforcement, making it impossible to achieve a satisfactory level of security.
- Push “one-size-fits-all” solutions that are not flexible enough to accommodate a range of internal and external encryption needs.

- 6. Simple & automatic key management** – Managing the keys required to encrypt data can be cumbersome, limiting deployment of encryption to a few individuals within the company. Most companies need scalable solutions that meet the needs of all employees as well as external business partners and vendors.

**PGP Corporation:**

- Bases its suite of encryptions solutions on an innovative architecture that automatically manages keys and digital signatures.
  - PGP Universal, a server-based solution, automatically, creates, revokes, and maintains keys for company employees as well as automatically providing solutions for external partners without keys.
  - This scalable, cost-effective product architecture frees IT staff from repetitive tasks such as key generation, eliminates the need for routine human intervention, and lowers costs while providing security for the extended enterprise.
- Provides solutions that scale from 100 employees to 100,000 employees and easily extend to company vendors and suppliers.

**Other vendors:**

- Offer market solutions that require manual management of keys and digital signatures.
- Do not offer industry-standard solutions for recipients without keys.

- 7. Digital signatures & encryption for authentication** – Authentication is the process of verifying that the sender of an email is who he/she claims to be as well as that the email's contents have not been altered in transit. Although encryption can be used to establish the identity of a sender, based on the sender's unique private key, authentication is not its main objective. Verifying the identity of the sender is usually done by use of a digital signature.

**PGP Corporation:**

- Offers a suite of products that provide digital signature capability as well as strong encryption, enabling users to authenticate senders and verify the integrity of messages.

**Other vendors:**

- Provide only encryption or digital signatures, not both.

- 8. Integrates with anti-virus, anti-spam, and content filtering solutions** – “Email hygiene” includes all the activities required to keep an organization’s email system up and running and clean: virus, spam, and content blocking plus securing email through encryption and digital signatures. These technologies must interoperate seamlessly to address potential threats to email system stability, security, and productivity.

**PGP Corporation:**

- Develops best-of-breed encryption solutions that are tested for interoperability with installed security solutions to maximize investments.
- Provides joint configurations for leading MTA partners such as Clearswift™ and IronPort™ Systems.
- Partners with leading point solution vendors such as Symantec™ to offer solutions that streamline IT management through an integrated management console.

**Other vendors:**

- Offer a standalone solution with separate security policies and operating requirements that complicate management and require more resources.
- Provide solutions that require user training and support, additional IT personnel or resources, or recurring costs (such as digital certificates).

- 9. Can recover lost keys** – Security regulations such as Sarbanes-Oxley increasingly require corporate access to encrypted data even if the key owner is unable or unwilling to provide the private key. Organizations should only consider encryption solutions that offer advanced key features such as Additional Decryption Key (ADK), key reconstruction, and key splitting that ensure policy-defined access to proprietary corporate information.

**PGP Corporation:**

- Provides solutions that feature patented Additional Decryption Key (ADK) options for easy data recovery when required by security policy or regulations.

**Other vendors:**

- Utilize approaches that require trading security for reliability such as encryption based on simple key escrow/key backup, which can create risk and violate security policy.

- 10. Financial viability** – Enterprises want to work with vendors that have strong financial positions, ensuring they will become long-term infrastructure partners and have the resources to invest in continued product and business development as well as customer support.

**PGP Corporation:**

- Sold its email, disk, mobile, and FTP/batch encryption solutions to more than 30,000 companies in the 2 years between August 2002 (when it became an independent company) and August 2004.
- Booked in excess of \$30 million in GAAP orders in the same 2-year period.

- Added more than 50 PGP Universal corporate customers worldwide that together have purchased licenses for more than 50,000 internal email users in the first 6 months of availability.
- Has a broad international reach, including a strong presence in both North America and Europe.

**Other vendors:**

- Have few reference customers and only a limited number of successful product deployments.
- Lack the breadth of product line to respond to customers' demands for solutions that meet all their encryption needs.
- Must spend time and energy consistently raising new capital and are unable to devote the resources necessary to product innovation and development.
- Do not have an international presence in Europe as well as North America.

**PGP Corporation**

3460 West Bayshore Road

Palo Alto, CA 94303 USA

Tel: +1 650 319 9000

Fax: +1 650 319 9001

Sales: +1 877 228 9747

Support: [www.pgpsupport.com](http://www.pgpsupport.com)

[www.pgp.com](http://www.pgp.com)

© 2004 PGP Corporation

All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form by any means without the prior written approval of PGP Corporation.

The information described in this document may be protected by one or more U.S. patents, foreign patents, or pending applications.

PGP is a registered trademark 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.

The information in this document is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors.

Changes to this document may be made at any time without notice.