

# data protection Is What Matters

*Traditional security measures aren't defending your business from costly breaches. Only enterprise data protection focuses on what matters most: your data.*

It happens all the time. Moreover, IT executives can no longer ignore it. All it takes is a lost laptop or USB flash drive, a disgruntled or criminal employee, or a breach to some other part of your security efforts, and critical data about your business, your partners, or your customers is in the wrong hands. The direct costs can be substantial, but the indirect costs — brand damage and loss of business — can be even worse. What's most frightening is that these kinds of scenarios are now commonplace, yet the forces arrayed against IT security only seem to grow more potent each day.

Georges Clemenceau, the prime minister of France during World War I, once warned, “*War is too important to be left to the generals.*” One can say the same thing regarding enterprise security. With the data at the heart of every business under threat, security is too important to be left to traditional approaches such as firewalls and intrusion prevention systems. Instead of merely building fences and patrolling perimeters, organizations are discovering that protecting data in the modern enterprise requires a comprehensive approach: Enterprise Data Protection.

Enterprise Data Protection integrates technologies that manage data, control data access, detect data at risk and protect data. With Enterprise Data Protection, security is built in, starting with data creation and following data as it is modified, transferred, stored, and archived. At the core of this approach is the protection of data using encryption, everywhere it goes.

Why encrypt? Data is vulnerable when traditional access barriers fail, either through an insider or an outside party. Then, customer data,

partner data, and your data move beyond your control. A recent study conducted by The Ponemon Institute found that data losses and security breaches caused extensive, measurable and far-ranging costs at 31 representative companies. Total costs averaged \$182 per lost customer record, and the average total



cost per reporting company was \$4.8 million per breach, rising to a high of \$22 million.

That's why data security must be built in. Enterprise Data Protection is four technology solutions working together:

- **Protecting Data** — Standards-based encryption enables a data-centric approach to security. Encryption locks down and remains with data wherever it goes, making it accessible only to authorized users.
- **Detecting Risk** — Solutions for data-leakage prevention search for data at risk, identify risks, and help IT executives develop strategies to mitigate exposure and enforce policies.
- **Controlling Access** — Authentication, including hardware tokens/smart cards and identity management, ensures that only authorized users can access data.
- **Managing Data** — Data must be available and redundant throughout its lifecycle. Storage management, backup, and archive solutions provide

a layer that helps keep data accessible even in the event of a disaster or system malfunction.

Building on these data management and access controls, Enterprise Data Protection secures your data by identifying any data at risk and automatically embedding data protection.

And it works. For example, as part of its commitment to protecting customer privacy, H&R Block, the tax-preparation industry giant, decided that encryption technology from PGP was critical to achieving its Enterprise Data Protection strategy. “From a compliance standpoint, we have a significant number of regulatory and corporate compliance drivers, including IRS guidelines, the Gramm-Leach-Bliley Act, plus California Senate

company, we promise our customers that we’ll keep their information private. We need to make sure we keep this vow because otherwise, we risk losing the customer’s trust,” say Ken Juneau, AVP, Director of Distributed Systems.

### Encryption Makes Enterprise Data Protection Work

Encryption answers the challenge of balancing productivity and security. Although encryption of one kind or another has been a part of information technology practices for a long time, it is just now entering mainstream usage. Compelled to meet industry and government regulations and the expectations of customers and partners, businesses of all kinds now find that only encryption offers the

*As new security risks and threats develop, the inherent protection of data encryption reduces the need to rush to implement a patchwork of inefficient fixes.*

Bill 1386 and similar breach-notification laws in more than 30 states,” says Dr. Daniel Fluke, senior project manager at H&R Block. His team took a straightforward approach to tackling the problem, implementing fully automated encryption for branches and knowledge workers.

### Meeting the Business Challenge

It’s ironic that the things that make business data so vulnerable — powerful productivity applications and mobility — are the very things that CIOs recognize as crucial to business success. Today, employees have access to more data, more often, than ever before. And they use it to stay competitive. However, according to the recent Yankee Group Report, “Zen and the Art of Rogue Employee Management”, enterprise IT is facing a potentially hazardous mix of secured and unsecured applications in the enterprise as consumer products such as instant messaging and personal computing devices gain popularity and escape oversight by IT. In this environment, traditional, “siloed” approaches to security are both costly and ineffective.

The challenge: how to keep employees productive and creative — able to access data when and where they want it — while still maintaining and even strengthening security.

A user of the PGP® Encryption Platform, American National Insurance Company (ANICO) faces this challenge each day. “As an insurance

security wherever data goes. That capability is why the core of any Enterprise Data Protection strategy is the protection of data with seamless, transparent and automatic encryption, applied immediately, wherever and whenever needed.

“Today, security is an integral part of the basic IT infrastructure,” says Thomas Goschütz, CTO Corporate Center, at global media company Bertelsmann. His company has made security an integral part of its business strategy and focuses on protecting data to reduce enterprise risk. “From an enterprise perspective, the protection of the information itself has become important,” says Goschütz.

With data security built in, IT can continually develop new, more proactive, redundant means of protecting data for particular applications. As new security risks and threats develop, the inherent protection of data encryption reduces the need to rush to implement a patchwork of inefficient fixes. Both end users and administrators become more productive, because data remains accessible and built-in security thwarts new threats. Most importantly, Enterprise Data Protection strategies marry policy and protection, improving the possibility of achieving comprehensive audit and regulatory compliance.

Central to this approach is the use of encryption, which provides the most fundamental

level of data security, substituting cryptographically secured data for unprotected data.

Continental Corporation, a leading automotive industry supplier based in Germany, relies on mobile data but understands the risks it presents. The company has selected the PGP Encryption Platform to secure proprietary and confidential information. It has implemented PGP Universal™ Server for centralized management of its encryption applications. It is also rolling out PGP Whole Disk Encryption to protect its mobile data. Thomas Ullrich, chief security officer at Continental, noted, “Today’s notebooks are small, are taken outside the company’s perimeters, and potentially contain sensitive data such as financial reports, personnel information, or technical blueprints. We decided we needed to protect all 6,000 laptops in the global enterprise.”

Although encryption might sound complex or daunting, in the case of PGP solutions, it is anything but. PGP solutions automatically

centrally managed solution. This approach controls policy and data access without requiring end users to make enforcement decisions, and it relieves administrators of complicated, resource-intensive tasks. This comprehensive approach also increases usability. It unites security and data and eliminates the risks associated with manual security decision making.

### Inside Enterprise Data Protection

Enterprise Data Protection consists of four complementary solutions working together to protect, detect, access and manage your data.

At the core of Enterprise Data Protection is the need to protect data itself. Standards-based encryption is the key to a data-focused approach to security. Encryption locks down and follows data wherever it goes, making it accessible only to authorized users. Centralized management with automated key and policy management enables scalability of enterprise data protection. This approach makes encryption interoperable,

*Enterprise Data Protection automatically detects when data is at risk and secures data using persistent protection, which works inside and outside the enterprise.*

protect data when an employee creates a spreadsheet on a desktop system inside the company firewall or at a remote location on a company laptop. PGP solutions locally encrypt information. Similarly, when teams collaborate remotely, policies allow only authorized users access to encrypted data.

Data protection extends beyond traditional enterprise perimeters. For instance, if a spreadsheet containing sensitive customer data is mistakenly or maliciously sent to an outside party, the enterprise data protection system detects a potential data breach. With enterprise data protection, data leakage prevention solutions can enforce corporate security policies to automatically encrypt sensitive files to authorized recipients. Messages remain encrypted while stored on recipient email servers or when downloaded to laptops.

Enterprise Data Protection automatically detects when data is at risk and secures data using persistent protection, which works inside and outside the enterprise. And the easiest way to implement Enterprise Data Protection is with a

transparent to users, and flexible enough to respond as new data security needs emerge. Enterprise data management also ensures that data is accessible today and in the future, as required by data retention policies.

Then, as data moves in and out of the enterprise, data-leakage prevention solutions—the detect function—search for data at risk. From this process, IT decision makers can adjust their strategies to reduce exposure.

Authentication tools, including hardware tokens or smart cards and identity management solutions, have a role, ensuring proper access so that only authorized individuals reach the data. Strong authentication can play an important role through to the “protect” layer.

Ensuring business continuity requires that data is available and redundant throughout its life cycle, from creation to archive. This manage function includes storage management, backup and archive solutions to ensure the efficient use of storage and access to data in the event of a disaster or system malfunction.

## Strategic Approach: The PGP Encryption Platform and Enterprise Data Protection

To help business stay competitive, IT organizations must participate in how organizations design new operational models, diversify globally, and develop closer relationships up and down the value chain to achieve greater profitability. At the same time, IT is responsible for increasing system security to meet compliance requirements and protect brand equity. The PGP Encryption Platform is the foundation of Enterprise Data Protection. The PGP Encryption platform allows businesses to cost-effectively deploy and manage multiple encryption applications, saving capital and human resources for other value-added activities. This strategic approach to encryption as noted in the “Encryption and Key Management” report from Aberdeen Research, increases data protection while reducing mistakes and operational inefficiencies.

The PGP Encryption Platform and integrated applications differ from other encryption approaches, including suites or sets of applications. With the PGP Encryption Platform, businesses can select from a range of centrally managed encryption solutions and

deploy and maintain these applications, and reduces the overall investment needed for effective information security. In addition, key management is automated and built-in across multiple applications, ensuring a seamless user experience while protecting corporate access to encrypted data.

### Security: Too Important to Ignore

Policy, automation and encryption are essential for successful enterprise data protection. Inconsistently applied or ill-defined policies may differ across applications or users, forcing administrators to focus reducing the level of risk mitigation. Over the long term, the direct costs associated with managing multiple applications and the indirect costs of lost productivity can outweigh even the potential financial consequences of a data breach.

Regardless of the business driver, encryption is fundamental to protecting data wherever it goes. Whether lost or stolen, encrypted data is useless to anyone but an authorized user, even if someone violates access controls. This level of critical protection is why more than 30 U.S. states provide safe harbor from mandated consumer notification

*In countries such as the U.K., where the need for breach mitigation is just emerging, protecting brand and reputation is the major reason that enterprises adopt encryption solutions.*

build a comprehensive encryption strategy on a single platform. Based on unified key management and policy, the PGP Encryption Platform offers the broadest set of integrated applications for enterprise data security. The platform enables organizations to meet current needs and expand as security requirements change for email, laptops, desktops, instant messaging, PDAs, FTP, bulk data transfers, backups, and shared files on network storage. By implementing the PGP Encryption Platform, organizations can reduce security infrastructure complexity, lower maintenance costs, and realize a strong return on investment.

In contrast to traditional, “siloed” approaches to security, which tend to incur growing costs from acquisition through to deployment and maintenance, the PGP Encryption Platform simplifies deployment of multiple, centrally managed encryption applications. This capability decreases the incremental cost and effort required to

in the event of a data breach involving encrypted data. In countries such as the U.K., where the need for breach mitigation is just emerging, protecting brand and reputation is the major reason that enterprises adopt encryption solutions.

Just as war is too important to be left to the generals, security is too important to be left to the hodgepodge methods of yesterday. The Enterprise Data Protection approach led by PGP Corporation now allows IT staff to focus on business needs without making security a separate project or an afterthought. Instead, security is built in: protecting, detecting risk, controlling access, and managing data. As the foundation of a comprehensive, strategic enterprise data protection solution, PGP encryption solutions protect data. ■

*For more information on enterprise data protection, go to: [www.pgp.com/edp](http://www.pgp.com/edp)*