SOLUTION BRIEF

KEY BENEFITS

- Maximize protection to ensure no sensitive data is left unencrypted
- Implement strong cryptography to comply with various government and industry requirements
- Prioritize ease of use to reduce the burden on both end users and administrators
- Provide multiple options to enable the right mix of self-assisted and administrator-assisted recovery
- Ensure trusted data transactions to ensure confidentiality and authenticity in back-end systems

KEY FEATURES

- Architecture provides superior scalability for seamless adaptation to large enterprise environments
- Implement comprehensive endpoint encryption for laptops and removable media
- Automate key management and policy controls through Active Directory synchronization
- Enable single sign-on to eliminate the need for re-inputting multiple passwords
- Provide default and customized compliance reports for auditors and key stakeholders
- Centralize management of native OS encryption and Opal-compliant self-encrypting drives

Symantec by Broadcom

Protecting Against the Assumed Breach

Overview

One of the tenets of Zero Trust is to assume a breach. Despite deploying various security mechanisms and technologies to safeguard your data, adversaries may still gain unauthorized access. What is the next step? For most organizations today, the primary motivation behind implementing an encryption solution is to safeguard customer privacy and minimize the impact of potential data breaches. There is a heightened focus on data breaches due to the surge in cyber attacks and stricter data privacy regulations, leading to a significant increase in the number of data breaches. Furthermore, the volume of data requiring protection is growing at an alarming rate. In 2021, approximately 79 zettabytes of data were generated worldwide, and this is projected to double by 2025[1].

Regulatory requirements make encryption a necessity for many companies. Those needing to comply with regulations such as Continuous Diagnostics and Mitigation (CDM), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and the EU General Data Protection Regulation (GDPR) must implement an auditable encryption solution to protect the privacy of customer data. In the event of a data breach, organizations are often required to notify victims and governing bodies. However, with encryption in place, organizations can apply for Safe Harbor, eliminating the need to disclose the occurrence of a data breach.

Business Challenges

For today's mobile workforce, laptops, and removable media devices capable of storing gigabytes of data have granted the freedom to work from anywhere. However, this newfound flexibility brings an increased risk, lost or stolen devices could lead to a costly data breach. This risk is exacerbated by cloud sync and share services, allowing employees to inadvertently carry a significant amount of sensitive information.

Additionally, shared file servers have become central collaborative tools in today's workplace, with many companies offering cloud-based file-sharing options that enable users to access shared information from anywhere. Without proper protection, this shared data becomes an attractive target for malicious actors seeking sensitive information and an easy avenue for unintentional data leaks. Organizations must ensure that data stored and shared in this manner is secure and only accessible to authorized users for these tools to serve as genuine productivity enhancers.

Finally, data transfer and processing systems form the core of every organization, facilitating the exchange of large volumes of information between internal systems, suppliers, and customers. Legacy data transfer systems, in particular, are vulnerable to security breaches as traditional file transfer and email protocols lack built-in security measures.

Business Challenges (cont.)

In combination, these three scenarios pose challenges for organizations to adequately safeguard their data from accidental or malicious exposure. The Symantec® Encryption portfolio offers strategic solutions tailored to address these specific business challenges.

Solution Overview

The Symantec encryption portfolio offers flexible data protection through three primary offerings: PGP® Encryption Suite, Gateway Email Encryption, and PGP Command Line Encryption. Together, these solutions provide comprehensive coverage for data at rest, in use, or in motion. Moreover, the portfolio boasts robust management capabilities, including individual and group key management, automated policy controls, and out-of-the-box compliance-based reporting. Additionally, integration with Symantec Data Loss Prevention enhances protection by automatically encrypting sensitive data moved onto removable media devices or residing in emails, files, or folders.

PGP Encryption Suite

The PGP Encryption Suite offers a comprehensive set of capabilities to encrypt both *data at rest* and ***data in motion*** for endpoints. It includes the following products:

- **Endpoint Encryption:** Empowers the remote and mobile workforce to be productive from anywhere while ensuring the protection of sensitive data stored on their devices. This is achieved through robust full-disk and removable media encryption. Built on world-leading PGP encryption technology with an intuitive central management platform, it safeguards sensitive data from loss or theft. The system also aids administrators in proving that a device was encrypted in case it goes missing.
- **Desktop Email Encryption:** Automatically encrypts, decrypts, digitally signs, and verifies email messages based on individual or centrally managed policies. This client-level process ensures that communications remain secure before traversing internal networks or being stored in cloud repositories.
- **File Share Encryption:** Extends file server access controls to include strong end-to-end encryption. This allows content owners or administrators to specify access rights for specific groups, individuals, applications, or file locations. Administrators can set encryption policies, ensuring automatic encryption when data is produced from selected applications or sent to specific folders. Encrypted files and folders can be moved without compromising their encrypted status, ensuring only authorized users have access to sensitive data.
- **Key Management Server:** Centralizes the storage of encryption keys, eliminating the need to install them on every server for simplified management and support. Applications and servers securely access these keys by calling the key management server through a client, an API, or a client and API.
- **PGP Encryption Server Admin Console:** Provides an integrated management platform, enabling organizations to deploy and manage their endpoint encryption clients and policies efficiently from a single console.

Gateway Email Encryption

Employees rely on email to enhance productivity through collaboration. A perpetual concern for organizations is whether users are taking the necessary precautions to protect sensitive information, such as health records, financial data, or strategy documents, when transmitting it through email. The Symantec Desktop Email Encryption product is part of the PGP Encryption Suite discussed previously; however, we also offer an alternative email encryption solution called Symantec Gateway Email Encryption.

This product encrypts messages based on highly configurable encryption rules, eliminating the need for software installation on the client. The gateway facilitates the secure exchange of sensitive data outside an organization without requiring software installation or key exchange for encryption purposes. This secure data exchange is achieved through a feature called Web Email Protection, providing a secure web inbox hosted on the gateway server. Users can transmit secure content to recipients even if they lack PGP software. Copies of these messages are securely stored as PDFs on the gateway server. External recipients can enroll in the solution, granting them access to these emails through popular Internet browsers such as Chrome or Firefox.

Finally, the combination of Gateway Email Encryption with Symantec Messaging Gateway allows users to leverage the synergy of PGP encryption alongside the premier Symantec anti-virus, malware, and spam filtering. This integration enhances the security of email communications, providing protection against external threats.

PGP Command Line Encryption

For organizations requiring secure exchange of large volumes of information, PGP Command Line from Symantec offers easy and minimally disruptive protection for business-critical data. It can safeguard substantial amounts of information stored on servers, preventing unauthorized access. PGP Command Line ensures data security in automated processes, aiding organizations in regulatory compliance and protecting privacy and confidentiality. With availability on various platforms, PGP Command Line extends its protective measures to mission-critical data across the enterprise.

In contrast to alternative solutions, PGP Command Line excels in safeguarding data at rest, in motion, and in use, providing support for digital signatures to generate audit trails. Its seamless integration into virtually any automated process enhances security without significantly impacting existing business applications. The lifecycle of current business applications can be prolonged by incorporating security with minimal impact on the application itself. Additionally, new applications benefit from leveraging an established, proven cryptographic standard through a user-friendly interface.

Summary

The encryption portfolio from Symantec offers flexible data protection through a range of offerings, featuring the following competitive differentiators:

- **Protection throughout the data lifecycle:** The solution maintains data confidentiality during transit and at rest, even in the event of a server breach.
- **Ease of use:** The new, modern, web-based centralized management console facilitates the management of heterogeneous environments with a more scalable architecture.
- **Adherence to Zero Trust principles:** Assuming breach is a key tenet of Zero Trust, and encryption ensures that even in the event of a breach, data remains protected.
- **Meaningful security insights:** The solution provides robust reporting tools and dashboards, offering enhanced visibility and a high-level overview of the overall security posture at a glance. These include actionable and drill-down charts and KPIs (Key Performance Indicators).
- **Automated risk mitigation:** The solution automatically encrypts sensitive data based on policy, ensuring continuous protection.
- **Total cost of ownership:** The solution boasts a best-in-class total cost of ownership due to its quick deployment, user-friendly interface, and scalability.

For more information, please visit broadcom.com/symantec-encryption.

1. Big Data Statistics 2023: How Much Data is in The World? firstsiteguide.com/big-data-stats/

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

ENC-PAAB-SB100 January 17, 2024