SOLUTION BRIEF

ENCRYPTION PROTECTS AGAINST THE ASSUMED BREACH

KEY BENEFITS

- Maximize protection to ensure no files are left unencrypted
- Strong cryptography to comply with a range of government and industry requirements
- Ease of use to reduce burden on end users and administrators
- Multiple options to enable the right mix of self-assisted and administrator-assisted recovery
- Trusted data transactions to ensure confidentiality and authenticity in back-end systems

KEY FEATURES

- Architecture provides superior scalability to easily adapt to large enterprise environments
- Comprehensive endpoint encryption for laptops and removable media
- Automate key management and policy controls with Active Directory synchronization
- Single sign-on to eliminate the need to re-input multiple passwords
- Default and customized compliance reports to with auditors and key stakeholders
- Centralized management of native OS encryption and Opal-compliant self-encrypting drives

In a world with increasing regulations to safeguard customer and sensitive data, encryption provides the data protection necessary to address privacy mandates and lessen the impact of the assumed breach.

Overview

One of the tenets of Zero Trust is to assume breach. Despite all of the security mechanisms and technologies you have deployed to protect your data, the bad guys have gotten in. What now? For most organizations today, the primary driver behind deploying an encryption solution is to protect customer privacy and lessen the impact of a potential data breach. There is increased focus on data breaches, both as a result of the growth in cyberattacks, and stronger data privacy regulations, with the number of data breaches having grown exponentially. In 2021, IBM found that customer Personally Identified Information (PII) was the most common type of record lost from a breach, and that customer PII was the costliest type of data lost or stolen at $180 per record lost (IBM Cost of a Data Breach, 2021).

Regulatory requirements make encryption a necessity for many. Companies that need 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 have an auditable encryption solution in place to protect the privacy of customer data. In many cases, when a data breach occurs, organizations must notify victims and governing bodies of what happened. With encryption in place, organizations can apply for Safe Harbor, removing the need to disclose if a data breach occurred.

Business Challenges

For today's mobile workforce, laptops and removable media devices capable of storing gigabytes of data have provided the freedom of being able to work from anywhere. With this freedom comes an increased risk that lost or stolen devices will result in a costly data breach, particularly as cloud *sync and share* services allow employees to unknowingly carry a large amount of sensitive information.

Additionally, shared file servers have emerged as central collaborative tools in today's workplace and many companies now offer cloud based file sharing, enabling users to access shared information anywhere. Without proper protection, this shared data presents an easy target for those looking to maliciously gain sensitive information and an easy way for sensitive data to accidently leak. Organizations must have confidence that data stored and shared in this way is secure and only accessible to authorized users if they are to be used as true productivity tools.

Finally, data transfer and processing systems are at the heart of every organization, exchanging large volumes of information between internal systems, suppliers, and customers. Legacy data transfer systems are especially prone to security breaches because traditional file transfer and email protocols have no built-in security.

Combined, these three scenarios make it difficult for organizations to adequately protect their data from accidental or malicious exposure. The Symantec® Encryption portfolio contains strategic solutions that address these business challenges.

Solution Overview

The Symantec Encryption portfolio provides flexible data protection through a range of offerings, which include endpoint, file and folder, and email encryption. Integration with Symantec Data Loss Prevention delivers added protection by automatically encrypting sensitive data being moved onto removable media devices or residing in emails and files or folders. Additionally, robust management features include individual and group key management, automated policy controls, and out-of-the-box, compliance-based reporting.

PROTECT SENSITIVE DATA STORED ON LAPTOPS, WORKSTATIONS, AND REMOVABLE MEDIA.

Endpoint Encryption

Symantec Endpoint Encryption combines strong full-disk and removable media encryption with an intuitive central management platform to protect sensitive data from loss or theft, and help administrators prove a device was encrypted should it go missing.

The key features and benefits of Symantec Endpoint Encryption are as follows:

- **Maximize Protection** – During the initial encryption phase, Symantec Endpoint Encryption encrypts each drive, sector by sector, ensuring no files are left unencrypted for maximum protection as well as protecting the boot loader of the system.
- **Enhanced Security** – Symantec Endpoint Encryption supports TPM authentication with Auto-logon to protect against changes to the computer system state as well aiding in Windows updates.
- **Strong cryptography** – Symantec Endpoint Encryption uses a FIPS 140-2 validated cryptographic module. This module can help customers comply with a range of government and industry requirements like CDM, PCI DSS, HIPAA, and GDPR.
- **Ease of Use** – Once encrypted, a user need only enter their passphrase once and single-sign-on technology passes them through to their main screen, eliminating the need to re-input multiple passwords. As users access their information, decryption and re-encryption happen instantaneously for a seamless experience. Smart cards are also supported for when you require additional user authentication.
- **Multiple Recovery Options** – Multiple recovery options allow organizations to find the right mix of self-recovery and helpdesk support for their users: Local self-recovery allows users to set up customizable questions and answers to regain entry; Web-based helpdesk support features a one-time use token that the user can insert into their machine. As an added security measure, this token changes after every use. Connectionless Recovery allows a machine with Drive Encryption to be recovered even if it has never checked into the encryption management server
- **Flexible Removable Media** – Removable media users can access their data on any Windows or Mac system, even if encryption is not installed on the machine they are using. Symantec Endpoint Encryption supports various types of removable media, including USB drives, external hard drives, and CD/DVD/Blu-ray media.
- **Enterprise Class Management** – Automation and key management are critical to success when implementing an encryption solution. Symantec Endpoint Encryption offers an integrated management platform to allow organizations to quickly deploy and manage their endpoint encryption solution from a single console.
- **Heterogeneous Encryption** – Management capabilities have been extended to provide support for native OS encryption (BitLocker and FileVault) and Opal compliant self-encrypting drives.

Finally, sensitive data is often transferred to unprotected devices due to user error. Symantec Endpoint Encryption helps address this issue through integration with our industry leading Data Loss Prevention (DLP) solution. As users accumulate information on laptops and desktops, DLP scans this data, flagging sensitive content and monitoring user activity on and off the network. If a user attempts to move sensitive material to a removable device, instead of simply blocking the transfer, and potentially frustrating the user, DLP logs the action. Then, through a customizable prompt, employees can be notified that they are attempting to move a sensitive file. Users are then given the option to encrypt the file before authorizing the transfer, allowing organizations to proactively prevent user error and ensure business continuity, all while helping educate employees on security best practices.

ENABLE COLLABORATION AND PROTECT SENSITIVE DATA WHEREVER IT GOES AND RESIDES—EVEN IN THE CLOUD.

Email Encryption

Employees rely on email to increase productivity through collaboration. A constant concern for organizations is whether users are taking the necessary precautions to protect sensitive information such as health records, financial information, or strategy documents over email. By utilizing Symantec Email Encryption, your sensitive data can be protected wherever it goes and wherever it resides—even in the cloud. Email encryption includes the following features:

- **Desktop Email Encryption** – Automatically encrypts, decrypts, digitally signs, and verifies messages according to individual or centrally managed policies. Email is encrypted immediately at the client, ensuring communications are secure before hitting internal networks or stored in the cloud. Compatible with: macOS and Microsoft® Windows®
- **Gateway Email Encryption** – Messages are encrypted according to highly configurable encryption rules, with no need for software to be installed on the client.

Not every organization is the same, and different departments may require different levels of security. Centralized management allows administrators to organize keys and policies per user or group from a single web-based console and sync these with Active Directory. Seamless integration with existing standards-based email encryption solutions such as OpenPGP and S/MIME continue to simplify administrative headaches.

Finally, when recipients do not have their own email encryption solutions, Gateway Email Encryption provides the following options:

- **PDF Messenger**, which enables users to send secure content to recipients who do not have PGP software installed using Portable Document Format (PDF). The PGP Server can provide the storage of copies of messages sent as Secure PDFs on the PGP Server. This option allows recipients to access the stored messages through Web Email Protection.
- **Web Email Protection**, which allows an organization to exchange sensitive data in a secure manner without the need to install any software or exchange any keys for encryption. This is done with a secure web inbox similarly designed to exchange information with only the organization hosting this service. Once a user is enrolled to a Web Email Protection account, any further email sent to the user from the organization is accessed through an internet browser, such as Chrome or Firefox.

Both of these features enable safe and secure communications without the recipient needing to install any additional software to read the secured content.

RESTRICT ACCESS SO ONLY AUTHORIZED USERS CAN VIEW ENCRYPTED DATA ON SERVERS.

File and Folder Encryption

Symantec File Share Encryption extends file server access controls to include strong end-to-end encryption, allowing content owners or administrators to specify access rights for specific groups, individuals, applications, or file locations.

With File Share Encryption, authorized users can save and share encrypted files, with no change to their applications or business practices. Administrators are able to set encryption policy so content such as documents, spreadsheets, presentations, video, and audio are automatically encrypted when produced from selected applications or sent to specific folders. Once encrypted, files and folders can be moved without jeopardizing their encrypted status, ensuring only authorized users have access to sensitive data.

Additionally, by combining File Share Encryption with Symantec Data Loss Prevention, organizations are able to solve the problem of exposed data on desktops, laptops, network, and cloud servers. Data Loss Prevention Endpoint Prevent integrates with Symantec File Share Encryption to automatically encrypt files as a protection measure. This limits the potential of a data breach and ensures data protection policies are consistently applied without requiring staff to take special action. The Encryption Insight integration with Symantec Data Loss Prevention Network Discover helps organizations inspect files previously protected by Symantec File Share Encryption in order to discover confidential information.

INTEGRATE ENCRYPTION OF SENSITIVE DATA INTO ANY AUTOMATED PROCESS.

SYMANTEC ENCRYPTION IS QUICK TO DEPLOY, EASY-TO-USE, AND PROVIDES THE END-TO-END DATA PROTECTION NEEDED TO ADHERE TO ZERO TRUST PRINCIPLES.

PGP Command Line Encryption

For organizations that need to securely exchange large volumes of information, PGP Command Line from Symantec can protect business-critical data easily and with little impact on existing systems. PGP Command Line can also be used to protect large volumes of information stored on servers from unauthorized access.

PGP Command Line secures data in automated processes, helping organizations comply with regulations and protect privacy and confidentiality. Available on many platforms, PGP Command Line secures mission critical data across the enterprise. Unlike alternative solutions, PGP Command Line helps protect data at rest, in motion, and in use with support for digital signatures to generate audit trails.

PGP Command Line can be integrated in virtually any automated process. The lifecycle of existing business applications can be extended by adding security with little impact on the application itself. New applications benefit from leveraging an established, proven cryptographic standard using a straightforward interface.

Summary

The encryption portfolio from Symantec provides flexible data protection through a range of offerings and provides the following competitive differentiators:

- **Protection throughout the data lifecycle** – The solution keeps data confidential while in transit and at rest, even if the server is breached.
- **Ease of User** – The new modern web-based centralized management console helps manage your heterogeneous environment with better scale out architecture.
- **Adhere to Zero Trust Principles** – Assume breach is one of the three tenets of Zero Trust. Encryption can ensure that when a breach occurs, data is still protected.
- **Meaningful security insights** – The solution provides robust reporting tools and dashboards that provide better visibility and a high-level view of the overall security posture at a glance with actionable and drill down charts and KPIs (Key Performance Indicators).
- **Automated risk mitigation** – The solution automatically encrypts sensitive data based on policy to ensure that it is protected.
- **Total cost of ownership** – The solution offers best in class total cost of ownership because the solution is quick to deploy, easy-to-use, and scalable.

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