PRODUCT BRIEF

Endpoint Encryption

AT A GLANCE

Endpoint Encryption provides strong full-disk and removable media encryption to protect sensitive data from loss or theft.

KEY BENEFITS

- Maximize protection to ensure no files are left unencrypted
- Comply with government and industry requirements with strong cryptography
- Ease of use and multiple recovery options to reduce the burden on end users and administrators
- Consolidated encryption administration to reduce operations burden

KEY FEATURES

- Comprehensive endpoint encryption for mobile workforce, laptops, and removable media
- Architecture provides superior scalability to easily adapt to large enterprise environments
- Single sign-on to eliminate the need to re-input multiple passwords
- Multiple options to enable the correct mix of self-assisted recovery and administrator-assisted recovery
- Centralized management of native operating system encryption and Opal-compliant self-encrypting drives

Overview

Symantec® Endpoint Encryption combines strong full-disk and removable media encryption. Built on world-leading PGP® encryption technology with an intuitive central management platform, it protects sensitive data from loss or theft and helps administrators prove a device was encrypted should it go missing. Endpoint Encryption provides the following key features and benefits:

- Comprehensive endpoint encryption
- Strong cryptography
- User experience
- Enterprise class management

With these core features, Endpoint Encryption enables your remote and mobile workforce to be productive from anywhere, while protecting any sensitive data that may be stored on their devices. The solution also helps customers to maintain world-class security standards and simplify their workload.

Comprehensive Endpoint Encryption

During the initial encryption phase, Endpoint Encryption uses a FIPS 140-2 validated cryptographic module to encrypt each drive, sector by sector, ensuring that no files are left unencrypted for maximum protection. The solution also supports trusted platform module authentication with auto-login to prove a user's identity when they authenticate to their device. This authentication further helps provide security against threats such as firmware and ransomware attacks.

Strong Cryptography

Endpoint Encryption uses a FIPS 140-2 validated cryptographic module. This cryptographic module can help customers comply with a range of government and industry requirements such as Continuous Diagnostics and Mitigation, Payment Card Industry Data Security Standard, Health Insurance Portability and Accountability Act, and the EU General Data Protection Regulation. 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 the event if a data breach occurred.

User Experience

The following features improve the Endpoint Encryption user experience:

- **Single Sign-On:** Once encrypted, a user only needs to enter their passphrase to login to their device, and single sign-on technology passes them through to their main screen. As users access their encrypted data, decryption and re-encryption happens instantaneously, eliminating the need to enter another password for a seamless experience. Smart cards are also supported when stronger authentication is required.

User Experience (cont.)

- **Recovery Options:** Connectionless recovery is supported to allow users to access their data, even if the client has no connection to the server. To enable this, multiple recovery options are offered to allow the appropriate mix of self-recovery and help desk support. Local self-recovery enables users to set up knowledge-based question and answer challenges to regain entry to their data, while web-based help desk support features a one-time use token that the user can use to unlock their machine.
- **Bring Your Own Device:** Removable media enables remote users can leverage their personal devices while still protecting sensitive data. The types of removable data supports are USB drives, external hard drives, and CD, DVD and Blu-ray media.

Enterprise Class Management

Endpoint Encryption offers an integrated management platform to allow organizations to quickly deploy and manage the solution from a single console. Additionally, the following features are also provided to help organizations implement and manage the solution:

- **Active Directory Synchronization:** Administrators can sync user and group profiles with Active Directory to automate key management and policy controls across the organization, speeding deployments, and reducing administrative overhead. Additionally, devices that fail to connect to the network within a given timeframe can be locked out for extra security.
- **Seamless Upgrades:** Endpoint Encryption allows Windows Feature Updates to be installed within the need to decrypt beforehand.
- **Scalable Architecture:** Endpoint Encryption includes a robust management architecture that provides superior scalability. This scalability ensures that organizations can easily deploy the solution to large enterprise environments without significant operational burden.
- **Audit and Compliance Reports:** Organizations often struggle to prove compliance with regulators and auditors. Endpoint Encryption provides standard compliance reports that can be used as-is or easily customized to help ease the burden of proof to auditors and key stakeholders.
- **Heterogeneous Support:** Endpoint Encryption enables organizations to manage native operating system encryption, such as BitLocker and FileVault from its management console. Administrators can manage all endpoint encryption from a single console. Management capabilities have also been extended to provide support for Opal-compliant self-encrypting drives.

Integration with Data Loss Prevention

Enterprises continue to face data protection concerns from emerging privacy laws, targeted attacks, and digital transformations, but sensitive data is often transferred to unprotected devices through user error. Endpoint Encryption helps address this issue through integration with our industry-leading Symantec 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. When the 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, notifies the user, and gives them the option to encrypt the file before authorizing the transfer. This notification allows organizations to proactively prevent user error and ensure business continuity.

Summary

The current shift to remote work has only accelerated the trend to support Bring Your Own Device. Employees rely on mobility and anywhere, anytime access to stay productive. Unfortunately, sensitive or regulated data may be unknowingly synchronized from the cloud and stored on their devices, putting this data at risk if these devices are lost or stolen. Endpoint Encryption protects sensitive information and ensures regulatory compliance, by encrypting all files stored on these devices for maximum security.

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

BROADCOM®
connecting everything®

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

SEE-ENC-PB102 November 21, 2023