Symantec Endpoint Encryption, Powered by PGP™ Technology

Data Sheet: Encryption

Protect Your Customers and Your Organization

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 cyber-attacks, and stronger data privacy regulations, with the number of data breaches having grown exponentially. In 2015, half a billion personal records were stolen or lost, according to the Symantec 2016 Internet Security Threat Report Vol.21 (ISTR). Organizations are paying significant sums to recover from breaches, with the average cost due to a breach now standing at $3.6 million dollars (Ponemon Cost of Data Breach Study, 2017)

Regulatory requirements make encryption a necessity for many. Companies that need to comply with regulations such as PCI- DSS, HIPAA and 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.

Comprehensive Endpoint Encryption

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 *'synch and share'* services allow employees to unknowingly carry a large amount of sensitive information. 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.

- **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. Symantec Endpoint Encryption supports TPM authentication with Auto-logon to protect against changes to the computer system state.
- **Strong cryptography –** Symantec Endpoint Encryption uses a FIPS 140-2 validated cryptographic module. This can help customers comply with a range of government and industry requirements like 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).
- **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 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 help- desk support for their users. Local self-recovery allows users to set up customizable questions and answers to regain entry while web based help-desk 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.

- **Flexible Removable Media –** Removable media users can access their data on any Windows or Mac system, even if encryption isn't 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.

- **Scalable –** Improved management architecture provides superior scalability over previous platforms and easily adapts to large enterprise environments.
- **Automated –** 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. For extra security, devices that fail to connect to the network within a given timeframe can be locked out.
- **Robust Reporting –** Compliance reports can be used out-of-the-box or customized to help ease the burden of proof to auditors and key stakeholders.
- **Heterogeneous Encryption –** Management capabilities have been extended to provide support for native OS encryption (BitLocker and FileVault) and Opal compliant self-encrypting drives.

Increased Security with Symantec Data Loss Prevention

Often, sensitive data is 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.

Additional Encryption Options

With Symantec, your security solution doesn't stop with just endpoint encryption. Organizations can take advantage of the broadest encryption portfolio on the market and protect other channels with solutions such as email and file & folder encryption.

Endpoint Encryption	
Endpoint Encryption	Full-disk and removable media encryption for laptops, desktops and servers.
Email Encryption	
Gateway Email Encryption	Automated email encryption at the gateway based on highly configurable policies with no need for additional client software.
Desktop Email Encryption	Email encryption immediately at the client, ensuring communications remain encrypted on internal networks.

File & Folder Encryption	
File Share Encryption	Policy-enforced file encryption for collaborating teams.
PGP Command Line	Automated encryption for file transfers and data-processing applications.

System Requirements

Server	Microsoft Windows Server 2016, 2012 R2, 2008 R2
Management Console & Client	Microsoft Windows Server 2016, 2012 R2, 2008 R2 Microsoft Windows 10, 8.1, 8, 7
Directory Integration	Microsoft® Active Directory
More Detailed Requirements	http://www.symantec.com/docs/DOC9497