

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. In an era where cyber-attacks are growing and becoming increasingly sophisticated, it's not surprising to find that the number of data breaches has also grown exponentially. According to Symantec's Internet Security Threat Report, 2013 saw 62 percent more data breaches than the previous year, with at least 8 exposing over 10 million identities. Organizations are also paying more to recover. The average cost to a company affected by a breach was \$3.5 million dollars in 2013, 15 percent more than the previous year.

Regulatory requirements make encryption a necessity for many. Companies that need to comply with regulations such as PCI-DSS or HIPAA 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. Increasingly, employees are logging into corporate networks from hotel rooms, coffee shops and airports. With this freedom comes a much greater risk of devices with sensitive data being lost or stolen. For security administrators and executives, this means greater risk of a costly data breach. 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.

- **Maximum Protection** - During the initial encryption phase, Symantec Endpoint Encryption encrypts each drive, sector by sector, ensuring no files are left unencrypted for maximum protection.
- **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.
- **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 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.
- **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 (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 and folder encryption.

Endpoint Encryption	
Endpoint Encryption	<ul style="list-style-type: none"> • Full-disk and removable media encryption for laptops, desktops and servers.
Email Encryption	
Gateway Email Encryption	<ul style="list-style-type: none"> • Automated email encryption at the gateway based on highly configurable policies with no need for additional client software.
Desktop Email Encryption	<ul style="list-style-type: none"> • Email encryption immediately at the client, ensuring communications remain encrypted on internal networks.
File & Folder Encryption	
File Share Encryption	<ul style="list-style-type: none"> • Policy-enforced file encryption for collaborating teams.
PGP Command Line	<ul style="list-style-type: none"> • Automated encryption for file transfers and data-processing applications.

System Requirements

Server	Microsoft Windows Server 2012 R2, 2008 R2
Management Console & Client	Microsoft Windows Server 2012 R2, 2008 R2 Microsoft Windows 8.1, 8, 7
Directory Integration	Microsoft® Active Directory
More Detailed Requirements	http://www.symantec.com/docs/DOC7523

More Information

Visit our website

<http://go.symantec.com/encryption>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec protects the world's information, and is a global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com