



It's Time to Rethink How Your Data is Protected

Whether you're a large enterprise or small business, you have to be more vigilant than ever when it comes to protecting your confidential data. The threat landscape continues to grow more volatile, putting your data at risk. As you evaluate and seek to harden your security strategy in the face of these varied threats to your confidential data, you need to ensure encryption plays a major role in that strategy.

What is Encryption?

Encryption is the process of helping protect personal data by using a "secret code" to scramble it so that it cannot be read by anyone who doesn't have the code key. Today, vast amounts of personal information are managed online and stored in the cloud or on servers with an ongoing connection to the web. It's nearly impossible to do business of any kind without personal data ending up in a networked computer system, which is why it's important to know how to help keep that data private. Regulatory compliance, data privacy concerns and brand reputation often become powerful motivating factors for organizations to take advantage of encryption technologies.

Why is encryption important?

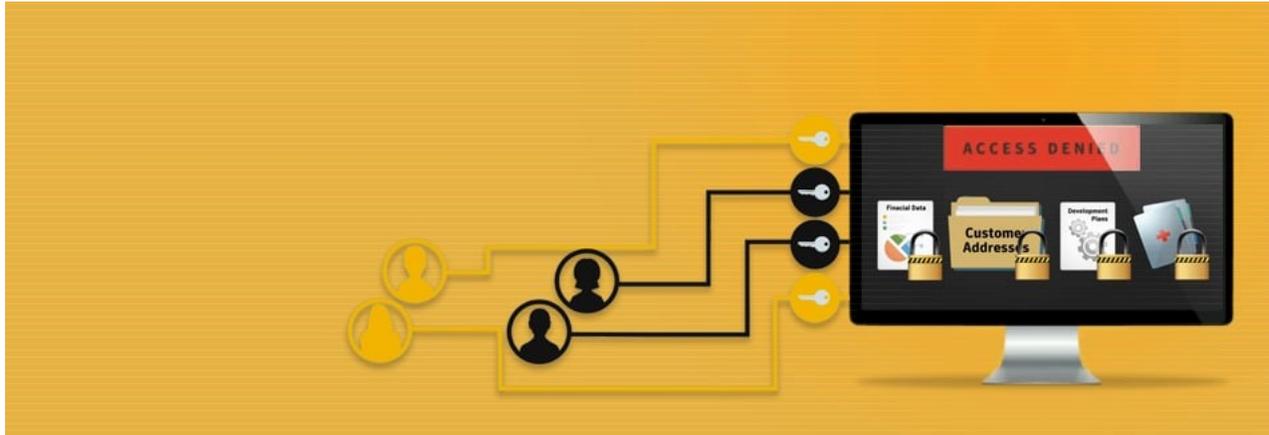
- Internet privacy concerns are real
Encryption helps protect privacy by turning personal information into “for your eyes only” messages intended only for the parties that need them — and no one else.
- Hacking is big business
Hackers aren’t just bored kids in a basement anymore. They’re big business, and in some cases, they’re multinational outfits. Large-scale data breaches that you may have heard about in the news demonstrate that people are out to steal personal information to fill their pockets.
- Regulations demand it
Encryption helps businesses stay compliant as well as helps protect the valuable data of their customers.

Symantec Encryption Offerings

To give you the flexibility and power you need to keep your sensitive data secure, Symantec provides you a family of robust and scalable encryption options that represent the widest variety of encryption offerings on the market.

- Symantec Endpoint Encryption
Built with PGP cryptographic technology, Symantec Endpoint Encryption delivers strong disk and removable media encryption with enterprise-class management, out-of-the-box compliance reports, and multiple key recovery options to maximize the protection of sensitive data on your endpoints.
- Symantec Email Encryption
To ensure only authorized individuals inside and outside of your organization can read the contents of your email messages, Symantec Gateway Email Encryption protects your outbound communications and Symantec Desktop Email Encryption provides end-to-end encryption and decryption of your internal communications from all your endpoints.
- Symantec File Share Encryption
To protect your sensitive data against accidental or malicious exposure of files as they multiply and travel, Symantec File Share Encryption automatically and transparently encrypts files and folders on file servers and shared network drives with drag and drop ease. Even though the strict rights and permissions you’ve implemented might not follow your files as they travel, the security of Symantec File Share Encryption will. Additionally, its Dropbox integration extends secure file sharing to the cloud.
- Symantec SSL Suite for Enterprise
To help you instill trust with your online users and customers, Symantec SSL Suite for Enterprise secures your websites and in-transit data with a robust

validation infrastructure that has experienced 100 percent uptime since 2004. It provides a variety of cost-effective SSL certificate options, administrative and discovery tools to centrally control lifecycle management of your SSL certificates, risk assessment and multiple algorithm options, including ECC, DSA, and RSA encryption.



PGP Command Line from Symantec

Because traditional file transfer and email protocols often lack built-in security, many legacy systems are vulnerable to security breaches. Symantec Command Line Encryption protects critical data to ensure confidentiality and authenticity in trusted data transactions. Powered by PGP technology, it integrates easily into existing business processes and protects information on servers from unauthorized access.

- Trusted data transactions – secures data in back-end systems to ensure confidentiality and authenticity in transactions
- Fast and flexible deployment – integrates easily into new and legacy business processes.
- Comprehensive protection – secures data at rest, data in motion, and data in use.
- Enterprise standard – leverages a common encryption application across enterprise systems.