White Paper

Keeping Your Private Data Secure

Symantec™

Norton™ SECURED
powered by Symantec

Keeping Your Private Data Secure

Contents

Keeping Your Private Data Secure

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. In the latest Symantec Internet Security Threat Report, the total number of reported breaches grew by 62 percent over the previous year, with the number of identities exposed due to those breaches quadrupling to more than 5 million. But your data is not at risk just to hackers. Accidental exposure and device theft/loss accounted for 56 percent of those breach incidents.[1]

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. That necessity is confirmed by the wide-spread reliance that government agencies place on security encryption to protect their own sensitive information. In fact, the National Institute of Standards and Technology (NIST) mandates that U.S. government agencies must employ end-to-end encryption for data-in-transit. The reason is clear. If your data is encrypted, it's still protected in the event of a breach.

Why Encryption?

Regulatory compliance, data privacy concerns and brand reputation often become powerful motivating factors for organizations to take advantage of encryption technologies. For example, the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to employ encryption for the transmission and storage of all non-public personal information. Health Insurance Portability and Accountability Act (HIPAA) specifies encryption requirements for health care organizations in regards to the transmission and storage of protected health information (PHI). The Payment Card Industry's Data Security Standard (PCI DSS) has strict requirements on how merchants need to employ encryption in order to protect stored cardholder data. Those are just a few regulations that include encryption requirements for securing data.

In addition, the majority of the states in the U.S. have enacted Safe Harbor Laws that protect organizations if they use strong encryption like the NIST Advanced Encryption Standards (AES). If such an encryption compliant organization falls victim to a breach, the Safe Harbor Laws free them from the obligation to provide notice of the breach to customers. These encryption friendly laws help organizations maintain a positive brand image and reputation, which in turn can enable them to avoid negative impacts to potential sales and strategic relationships.

Even when organizations aren't compelled by regulatory compliance to implement encryption, many recognize encryption as a vital best practice for safeguarding sensitive information and maintaining data privacy. In its analysis of nearly 500 breaches in the first half of 2014, the Online Trust Alliance (OTA) determined 93 percent of those breaches could have been avoided if organizations had implemented simple controls and security best practices. Three of the seven best practices prescribed by OTA involved encryption, including a combination of SSL implementations for in-transit data, encryption of all sensitive data at rest, and encryption of wireless communications.

[1] Symantec Internet Security Threat Report 2014

Obstacles to Encryption

Despite encryption's effectiveness at keeping sensitive data safe, far too many organizations fail to take advantage of its data privacy and security benefits. Others might employ encryption to a limited degree within their organization, but not to the full extent necessary to adequately safeguard their sensitive data and communications. The reasons for non- or under-utilization of encryption vary, but often it's due to unfounded encryption misperceptions.

One such misperception is encryption is too expensive. For example, there is a mistaken belief that end-to-end encryption of the online user experience (also known as Always-On SSL) increases web operational overhead and costs, resulting in a need for additional hardware investments. While the use of Always-On SSL will exact a degree of network latency, "researchers at Google performed extensive research on the computational load associated with Always-On SSL, and determined that for their high-volume site, there was no need for additional hardware to implement in their IT ecosystem."[2] In cases where encryption might have an impact on performance or operational costs, it's typically due to the organization failing to follow best practices or not leveraging a solution with adequate management capabilities. The point is if you don't make encryption a budgetary priority and a vital part of your overall security strategy your data will remain at risk.

Another obstacle to encryption deployment is that some believe encryption solutions are difficult to deploy and manage. Advanced solutions make encryption easy to employ with centralized and policy-based management. Others worry employing encryption will lead to increase help-desk calls, especially for those with users with a history of forgetting passwords. Those worries can easily be relieved with solutions that offer in addition to centralized management, multiple key/password recovery options, including self-help recovery.

Misperceptions that have often stood as obstacles to encryption adoption shouldn't stand in your way when it comes to protecting your data. It's no longer a question of, "Does your organization need encryption?" You can't afford not to leverage encryption. The real question you need to ask is, "How does encryption need to play a role in the various aspects of your overall security and risk management strategy?"

Approaches to Encryption

While you don't need to employ encryption everywhere within your infrastructure, you do need to consider how you can best leverage encryption wherever your sensitive data resides and flows. With that in mind, you can break down your encryption approach into four main categories.

- Endpoint Encryption
- File and Folder Encryption
- Email Encryption
- Secure Socket Layer (SSL) Encryption

[2] Rick Andrews, "Always-On SSL, Part 1," CA Security Council (16 January 2014, https://casecurity.org/2014/01/16/always-on-ssl-part-i/

Endpoint Encryption
To protect data-at-rest from loss or theft, endpoint encryption solutions typically fall under the following three categories of securing sensitive data:

- Drive encryption
- Removable media encryption
- Mobile encryption

Drive Encryption
Sometimes referred to as full disk encryption or whole disk encryption, drive encryption is perhaps the most traditional form of encryption for protecting data at rest. Drive encryption solutions encrypt the entire hard drive, including the operating system, applications, drivers, and user data. By encrypting data on a hard drive sector by sector, all data on the device becomes unreadable and unusable except to its authorized users.

Even though drive encryption requires you to deploy and manage an encryption client on every end user device, the advanced management capabilities of mature solutions significantly minimize that effort. More importantly, drive encryption provides the most effective and comprehensive method to keep data secure in the event of stolen or lost end user devices. The November 2014 Gartner report entitled *Comparing Encryption Technologies and Solutions for Data Protection on Endpoints* details the strengths and weaknesses of drive encryption, as well as those of other encryption solutions.

Removable Media Encryption
Removable media encryption addresses the encryption needs of sensitive data found on USB drives, removable hard drives, DVD's, and other portable storage devices. These solutions automatically encrypt data transferred to removable storage devices. As a result, if any of these storage devices get lost or stolen, the sensitive data will remain secure. When evaluating endpoint encryption offerings it's best to consider those that inherently provide both drive encryption and removable media encryption.

Mobile Encryption
Mobile encryption offerings cater specifically to the need to encrypt data stored on mobile devices. In addition to encryption of on-device data storage, some mobile encryption solutions provide extra protections that prevent data leakage. These extra protections might include policy-driven cut-and-paste controls or controls that prevent data from being opened or accessed from non-approved apps.

Other Endpoint Encryption Technologies
Encryption technologies constantly advance. In the area of endpoint encryption, some device manufacturers – especially those in the mobile arena – have begun to make encryption an inherent aspect of the device OS such that all user data

will be encrypted by default. With the encryption engine built into the OS, these encryption offerings can address interoperability and OS patching issues some third-party solutions occasionally experience. However, native OS encryption offerings lack the means to provide central management of encryption keys and user policies. You would need to still leverage the management capabilities of a traditional software based encryption solution to effectively use native OS encryption.

In terms of other technology advancements, some hard disk manufacturers have begun offering self-encrypting hard drives that automatically encrypt all data on the drive. While self-encrypting hard drive technology has made significant progress over the past several years, the adoption of industry standards has been slow and the technology itself is still relatively new with limited real-use vetting of its security strength. However, as advancements in the technology continue, it promises to provide another beneficial option for endpoint encryption.

File and Folder Encryption

While sometimes offered as part of an endpoint encryption offering, file and folder encryption encrypts designated files and folders on a device. This can include desktops, laptops, shared network drives and even cloud storage, such as Dropbox. When a file or folder is copied, archived or shared with other users, the encryption will follow the file or folder such that only authorized users can gain access its data. Authorized users can use and open the encrypted files in applications just as they normally would.

Depending on the specific file and folder encryption solution, you might have a variety of options for how files or folders are designated for encryption. The most common of these is to allow you to specify that all data within a particular folder will be automatically encrypted. A second option is to allow you to specify the encryption of certain individual files. Another powerful option is to specify that any files created by a particular application will automatically be encrypted upon creation.

File and folder encryption facilitates secure collaboration where team members or specific sets of individuals within an organization need to share sensitive information. Sensitive files that need to be shared can be individually encrypted or placed in an encrypted shared folder to ensure only authorized individuals can view the material.

Email Encryption

Email encryption helps you ensure sensitive communications can only be read by their intended recipients and that your employees and business partners can collaborate and communicate in a secure manner. Email encryption should be viewed as an additional layer of protection that is complementary to endpoint encryption rather than as an alternative to endpoint encryption.

Depending on your email implementation and usage, there are three main approaches to email encryption to consider.

- Desktop Email Encryption
- Gateway Email Encryption
- Mobile Email Encryption

Desktop Email Encryption
Desktop email encryption automatically encrypts email messages before they leave the client device, ensuring the contents of email messages remain encrypted in transit, on the mail server, backup server and storage systems. This type of email encryption is used primarily for internal communications and is ideal for organizations that outsource their email to a cloud service (i.e., Microsoft Office 365) since it encrypts email messages before they reach the cloud mail server. This prevents third-party cloud service providers from being able to read any confidential information contained within your email messages. Desktop email encryption needs to be installed on each endpoint device that needs to take advantage of the solution.

Gateway Email Encryption
Gateway email encryption encrypts email once it reaches the email gateway server and before it leaves your network boundaries. This type of email encryption is primarily used for protecting external communications since it does not provide internal email protection. Gateway email encryption has the advantage of not requiring the installation of any encryption software on your client machines since all encryption takes place on your email gateway server. Additionally, some gateway email encryption offerings have the added benefit of being able to integrate with data loss protection solutions.

Mobile Email Encryption
As the name suggests, mobile email encryption encrypts email messages that mobile devices send and receive. Sometimes provided as an extension to desktop email encryption, mobile email encryption eliminates the need to use a separate web portal to secure outgoing and incoming messages. It transparently lets you send and receive encrypted email just as you would normal email.

Secure Socket Layer (SSL) Encryption
With its ability to secure data transfers between web browsers and web servers, Secure Socket Layer (SSL) encryption has become the defacto standard for instilling trust with online users and customers. Initially, many organizations primarily used SSL to encrypt information users supplied for web login or authentication activities. Overtime, the usage of SSL has expanded to encrypt the transfer of any online data organizations wanted to secure.

More recently, the dramatic rise of man-in-the-middle attacks used by cyber criminals to hijack accounts has caused organizations to realize the need to employ SSL encryption from the start to the end of all web sessions. This start-to-end or end-to-end encryption is also known as Always-on SSL. Always-on SSL is supported

as a best practice by leading industry players including Google, Microsoft, PayPal, Facebook, Twitter and Symantec. Additionally, NIST now mandates the use of end-to-end SSL encryption by certain government organizations.

In addition to encryption of online data, SSL ensures the authenticity of a web server's identity. This provides users assurance that they are submitting their information to your actual web site or organization, and not to a criminal operated web site masquerading as you. Additionally, the visibility of SSL protection on your website has the ability to enhance your reputation and build greater trust with your online customers and partners, which can drive higher online traffic and business.

When considering SSL offerings it's important to realize that not all Certificate Authorities (CAs) are created equal. First of all, the underlying role of a Certificate Authority is to act as a trusted third-party that both you and your web users can trust. With that in mind, it's important to choose a Certificate Authority with a proven industry history of being reputable, as well as having a strong brand that conveys trust. Additionally, you need a Certificate Authority with extensive root ubiquity (preferably 100% ubiquity) to ensure that the SSL certificates they issue have wide spread browser support.

Encryption Best Practices

To further maximize your encryption efforts and minimize the impact on your productivity and budget, you need to look for the following capabilities when evaluating encryption solutions:

Centrally Managed Encryption – You need to be able to easily deploy encryption across your workforce, manage individual and group encryption keys, manage and set encryption policies, and report and audit encryption status. While some solutions might appear to have a free or low- cost benefit, you'll pay much more in time and effort without a centrally managed encryption solution.

Multiple Key-Recovery Options – For endpoint encryption, multiple key-recovery options are a must to minimize help desk calls and ensure productivity of your staff and users. This includes local self-recovery for users, whole disk recovery options administrators can provide users to unlock their devices, and an Additional Decryption Key (ADK) an organization can apply across its entire encryption implementation for emergency decryption purposes.

Data Loss Prevention Integration – Integration between your encryption and data loss prevention solutions can help ensure the encryption of sensitive data before it's transferred via email, shared folders or removable media.

SSL Specific Requirements – You need to be able to employ SSL throughout your entire process flow. This requires a comprehensive certificate lifecycle management solution to help track and deploy SSL certificates efficiently. Other aspects to demand include a reputable Certificate Authority with strong security practices

and infrastructure, a wide range of SSL certificates (i.e., Extended Validation, OV, SANs, and Wildcard), algorithm options in addition to RSA (i.e., ECC and DSA), 100% root ubiquity, rapid OCSP lookups, and a globally trusted brand that will instill confidence with your customers.

Just as with any security initiative, a successful encryption deployment requires appropriate employee awareness and ongoing training. This includes having well-documented and properly implemented encryption policies you apply to all sensitive data in your organization, regardless of where it resides and how it's transmitted.

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.

Maximize Your Data Security

Whether you're driven by the need to be compliant, nurture customer loyalty, maintain your brand reputation, or keep your competitive edge, securing your sensitive data must be a top priority. The technology advancements and wide variety of deployment options that encryption offers make it more cost-effective

and easier than ever to maximize the protection of your confidential customer information, intellectual property and other private data.

As a global leader in security, Symantec offers a wide array of powerful encryption solutions to keep your digital interactions safe, your online information protected, and your customers, employees and partners connected with their apps, websites and devices in a trusted and secure manner.

Visit Symantec Encryption and Symantec SSL Suite for Enterprise to learn more about how encryption solutions from Symantec can keep your data private and secure when at-rest, on the move, or in the cloud.

More Information

Encryption:

Visit our website

http://www.symantec.com/encryption

To speak with a Product Specialist:

1-800-240-2275

Website Security & SSL:

Visit our websites

North America: http://go.symantec.com/managed-pki-for-ssl
EMEA: http://www.symantec.co.uk/managed-pki-for-ssl
APAC: http://www.symantec.com/en/aa/ssl-certificates/managed-pki-ssl

Follow us on Facebook
Chat with us on Twitter @nortonsecured
Join the discussion at Website Security Solutions Forum

To speak with or contact a Product Specialist

SSL North America: +1(866) 893-6565 or +1(520) 477-3135; SSL_EnterpriseSales_NA@symantec.com
U.K. and Ireland: +0800 032 2101; sslsales-uk@symantec.com
Rest of EMEA: +353 1 793 9053 or +41 (0) 26 429 7929; sslsales-ch@symantec.com
Asia Pacific: +61 3 9674 5500; ssl_sales_APAC@symantec.com

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 the 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 industry leading expertise in protecting data, identities, and interactions gives our customer's confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com

Symantec™

Norton™ SECURED
powered by Symantec

21349382
UID: 242/02/15