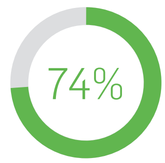
SOPHOS
Security made simple.

Deciphering the Code: A Simple Guide to Encryption

By **Anthony Merry**, Director of Product Management - Data Protection

A business's success is increasingly dependent on its ability to leverage its data. Whether it's achieving top-line growth or improving the bottom line, businesses rely on data to boost sales, drive product innovation, target market customers, and gain competitive advantage. Your data is valuable, but in the wrong hands it could hurt you.

Data breaches are in the headlines almost every day, yet only a small percentage of cyberattacks target the big organizations like Sony, Anthem, or the US government. If you're a small or mid-sized business (SMB), your data is under attack too. Over 700 million records were compromised in 2014, and 53% of confirmed data loss incidents are in organizations of less than 1000 users[i], according to a report by Verizon[1]. No business or institution anywhere in the world is immune to data theft, regardless of geography, size and industry.



of small businesses had a security breach in 2015[2]

So much of IT security is focused on protecting physical things—servers, desktops and laptops, mobile devices—but businesses should think more about how to protect the valuable data on those computers. With the proliferation of data and the need to access data from anywhere at any time, encryption is rapidly emerging as the best place to start your security strategy.

Despite the cold, hard facts of SMBs' vulnerability to data breaches and accidental data loss, many are slow to adopt encryption. Why? In part, it's because encryption has long been shrouded in myths, including:

- Encryption is too complex to install or manage
- Encryption hurts performance of laptops, desktops, servers and applications
- On top of these common myths, the demands of implementing a data protection plan that includes encryption can cause confusion, such as the following examples:
- Do you need to use encryption everywhere data is found—on disks, files, folders, removable devices, mobile devices, and cloud storage?
- What are the best practices for implementing encryption?
- How can you protect all your important data without slowing the business down?

This whitepaper aims to dispel the fear and confusion surrounding encryption. It demonstrates how organizations can move forward with an encryption strategy in a manner that is simple, practical and achievable. So let's start by setting the record straight on a few myths.

[i] Where size of organizations is known

Encryption myths

Myth: Only businesses that have compliance requirements where encryption is mandated by law need to use encryption.

Truth: For any type of organization, data has value and needs to be protected. That may be customer information (names, emails, credit card information), internal finance or competitive information, employee information, intellectual property, and more. Simply put, data is currency—it has value and should be protected as such. Companies should always encrypt sensitive data, whether they are legally obligated to or not.

Myth: Encryption is too complicated and requires too many resources.

Truth: Data encryption can be very simple to implement and manage. The key is to understand the types of data you need to encrypt, where it lives and who should have access to it.

Myth: Encryption will kill database and application performance.

Truth: Performance of applications, databases, servers, and networks is a top priority of IT and end users. When designed and implemented properly, encryption can not only protect the critical data running through those systems, but its presence can have minimal impact on performance that is imperceptible to users.

Myth: Encryption doesn't make data stored in the cloud more secure.

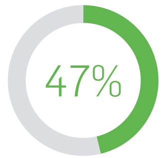
Truth: Storing encrypted data in the cloud is more secure than storing non-encrypted data in the cloud. Do you know where cloud data is stored? Who truly has access to it? The answers to these questions underscore the reason that all data that is sent to the cloud should be encrypted, with the encryption keys controlled by you.

Myth: Encrypting data is more important than key management.

Truth: Encryption without careful key management is pointless. Too many organizations fail to manage their encryption keys, either storing them on the same server as the encrypted data or allowing a cloud provider to manage them. You wouldn't want to lock your car and leave the keys in the door.

Myth: If your data is encrypted, it can't be stolen.

Truth: Encryption doesn't stop data loss or theft. But it does keep data safe by making it unreadable and unusable. Choose an encryption solution that provides proof that your data was indeed encrypted.



of data breaches are due to malicious/criminal attack, up from 42% last year[3]

Understanding encryption: How it works

Encryption is a method of scrambling messages in a format that is unreadable by unauthorized users. Cryptography—the art and science behind encryption—uses algorithms to turn readable data (plaintext) into unreadable format (ciphertext).

Without getting too deep into the details, it's helpful to think about it like this: when you encrypt data you are storing it like you would money in a safe—you need a key to unlock the safe to get the money out.

There are loads of ways to use encryption, but for organizations concerned about data loss, two very important areas to understand are full-disk encryption and file-level encryption.

Full-disk encryption

Full-disk encryption (FDE) is the encryption of an entire disk

Full-disk encryption (FDE) is the encryption of an entire disk, not just specific files, at the sector level below the File System. In other words, all the contents of your device's physical hard drive are encrypted.

FDE offers the most protection when the device is powered off (not turned on or in sleep mode), offering what is known as protection of data "at rest." FDE is considered the first line of defense in a data protection strategy, primarily aimed at keeping your data secure in the event that a device is lost or stolen.

With FDE, any files that you save on a computer or digital device with will be encrypted (protected) automatically. However, as soon as a file leaves the disk (say you send it via email, or copy it to removable media or to the cloud), it will not be protected anymore by FDE.

File encryption

File encryption is the encryption of specific files only

File encryption is the encryption of specific files only. Let us say you have two documents on your computer, you can choose to encrypt one but not the other. Unlike disk encryption, which automatically encrypts everything that is written to the disk, with file encryption, you need to set up rules and policies to determine what type of files to encrypt.

Unlike FDE, encrypted files remain encrypted after leaving the boundary of the disk or the device. You can share an encrypted file via email and it will still be secure. The same is true if you copy an encrypted file to removable media and to the cloud. This is also sometimes referred to as protection of data in use and data in transit.

With file encryption, you will want to set rules to make things easier—for example, you could make sure that all Word documents are encrypted by default, but not images.

What data should you encrypt?

You need to think a bit more about what data you want to encrypt and why.

Typically, this includes employee/HR data, financial records, customer information, point-of sales data, health information and anything else that can be useful to an attacker. At times, regulatory compliance requirements like those defined by PCI, HIPAA, PIPEDA, and more, require you to encrypt data.

However, if you only encrypt what you consider to be your most top secret data, encryption can act as an indicator to attackers that that data is important. Encrypting as much as you can removes that indicator from attackers.

Implementing an Encryption Strategy

According to a Ponemon Institute report[4], when respondents were asked what the biggest challenges in planning and executing a data encryption strategy were:

56%	said discovering where sensitive data resides in the organization
34%	stated classifying which data to encrypt
15%	rated training users to use encryption appropriately as the most challenging

Encryption is the foundation of any data protection strategy. Before you can put your strategy into an actionable plan, you need to answer the following questions:

1. **How does data flow into and out of your organization?** Do you receive emails with file attachments, or send them out? Do you receive data on USB sticks or other forms of removable media? How does your organization store and share large amounts of data internally and externally? Do you use cloud based storage services like DropBox, Box, OneDrive, etc.? What about mobile devices and tablets? According to a Sophos survey, an average technology user carries 2.9 devices. How do you rein in the wide range of devices that have access to enterprise data? You should look for an encryption solution that is built to adapt to the way you use data and how data flows within an organization.

Use case example: With more and more SMBs using cloud storage, you need a solution that secures cloud-based data sharing and provides you with custody of your encryption keys.

You need a data encryption solution that protects your data wherever users need to access it, without complicating things for the end user. It must be like a guardian angel, with the user not really being aware it is actually there.

2. **How does your organization and your people make use of data?** What are their workflows and how do they go about making their day-to-day jobs more productive? What tools, devices or apps do they use and do any of those present a possible vector for data loss?

3. **Who has access to your data?** This topic can be both an ethical and regulatory discussion. In some situations, users should not ethically have access to certain data (e.g., HR and payroll data). Worldwide, there are some data protection laws that stipulate only those who need data to perform their tasks should have access to it; everyone else should be denied. Do your employees have access to just the data they need to do their job, or do they have access to data they do not need?

Use case example: IT administrators tend to have unlimited access to data and IT infrastructure. Does the IT administrator need access to everyone's HR data, or access to the legal department's documents about the latest court case? In a public company, should people outside of the finance department have access to the latest financial figures?

4. **Where is your data?** Centralized and mostly contained in a data center? Completely hosted in the Cloud? Sitting on employee laptops and mobile devices? According to a Tech Pro Research survey, 74% of organizations are either allowing or planning to allow their employees to bring their devices to their office for business use (BYOD). Employees are also taking their work home and working on the go. They are carrying sensitive corporate data on their devices, increasing the risk of data leaks or compliance breaches. Think how easy it would be to access confidential information about your organization if an employee's smartphone gets stolen or misplaced.

   Every organization is different, so there is no one-size-fits all data protection strategy. Your data protection plan must be based on your business, the type of data your business works with and generates, local/industry regulations, and the size of your business.

   Even though many of these decisions are specific to your business, there is one constant across all companies—you need to educate employees.

   Employees need to understand how to comply with a clearly defined data protection plan and how to use encryption. They must be clearly told which data they have access to, how this data needs to be accessed and how they can protect this data. Most importantly, you need to ensure that you can both offer and manage encryption in such a way that it doesn't impact the organization's workflows. People are naturally resistant to change, so your data protection plan should include provisions for education and training.

Choosing a Solution

When asked to rate the most important features of encryption technology solutions[5]:

53%	rated system performance and latency as the most important
51%	rated integration with other security tools highest
51%	rated management of keys as being the highest priority

Below are some key aspects to keep in mind while choosing the right encryption solution for your organization:

Usability: An encryption solution needs to be simple yet comprehensive. Your encryption product should be easy to set up and deploy, with an intuitive management console.

Multi-platform: Find a solution that covers all types of encryption, including for multiple operating systems like Windows, Mac, Android, iOS.

Adaptability: You ideally want a solution that protects your data without interrupting your organization's workflow and impacting productivity. Your encryption solution should adapt to your organization's workflow and not the other way around.

Independent endorsement: Make sure whatever company you choose for your encryption needs provides ample support and has strong third party endorsements from industry analysts, reviewers and customers.

Scalability: As you grow your business, you need an encryption solution that scales with your business. It should also allow for simple key management and enforcement of your data protection policy.

Proof of compliance: In the event that the worst happens, you need to be able to show that your data was protected. If you work in a vertical or location that has specific data protection laws or regulations, auditors will require proof that the data was encrypted.

Introducing Sophos SafeGuard Encryption

Sophos SafeGuard is the most complete data protection solution on the market today, protecting data on multiple devices and operating systems. Whether your data resides on a laptop, a mobile device, or is being collaborated upon via the cloud or other file sharing methods, SafeGuard Encryption is built to match your organizational workflow and processes without slowing down productivity.

Sophos SafeGuard provides the best encryption solution on the market today:

- 'The Breakout Star' in Forrester Encryption Wave 2015[6]
- A Gartner Magic Quadrant Leader for last 6 years[7]
- 2014 TechTarget Readers' Choice Award for the Best Encryption Solution 2014
- Independent tests show Sophos Encryption is faster with lowest performance impact

Highlights:

- Supports both Full-Disk Encryption and File Encryption
- Secures sensitive data wherever it is stored (at rest, in use and in transit), with minimal impact on performance. Regardless of whether it is stored on laptops, USB devices, network shares or cloud (DropBox, Box, OneDrive, etc.), your data is protected.
- Allow users to remain productive, in the office or on the road, by allowing them to view and edit encrypted files on smartphones and tablets.
- Central console helps define and manage data protection efficiently.
- Simplifies regulatory compliance through policy enforcement and reporting, providing proof of compliance where necessary. It helps you conveniently comply with data protection regulations like HIPAA, etc.
- Convenient key management allowing authorized users to share data securely and easily.
- Data is protected across multiple platforms, allowing employees to have the freedom of choice for a device and form factor that suits their daily requirements (Windows, OS X, iOS and Android)

Conclusion

Too many SMBs don't use encryption because of the idea that encryption is just too complicated. But encryption is actually rather simple—when your data is encrypted, it is protected, as it is unreadable if lost or stolen.

The need for encryption has never been greater. Mobile working, the increasing sophistication of cybercrime, and the growing black market for data, all mean sensitive information is more at risk than ever before.

Implementing a data protection strategy based on encryption starts with understanding why you need encryption and how it can work for you. By implementing a simple encryption solution, you can rest easy knowing your data is always protected.

Disclaimer

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

1. Verizon. (2015). 2015 Data Breach Investigations Report
2. PwC. (2015). 2015 Information Security Breaches Survey
3. Ponemon Institute. (2015). 2015 Cost of Data Breach Study: Global Analysis
4. Ponemon Institute. (2015). 2015 Global Encryption & Key Management Trends Study
5. Ponemon Institute. (2015). 2015 Global Encryption & Key Management Trends Study
6. Forrester Research, The Forrester Wave™: Endpoint Encryption, Q1 2015, by Chris Sherman, January 16, 2015
7. Gartner Magic Quadrant for Mobile Data Protection, John Girard, 8 September 2014

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2015-07-30 WP-NA (MP)