SOPHOS
Security made simple.

Encryption Buyers Guide

Organizations today face the dual challenges of keeping data safe without affecting user productivity. Encryption is widely regarded as one of the most effective ways to protect information from attackers – yet many organizations have shied away from comprehensive encryption because the technology was too complicated or taxing for end users. But things are changing.

Security companies have developed tools that make it easy to encrypt data, with streamlined mechanisms that make it virtually transparent to the end user. It is now possible to effortlessly protect corporate information wherever it goes, whether on Windows or Macs, laptops, files uploaded to the cloud, network shares, USB sticks, etc.

This buyers guide details the factors you should consider when evaluating the different options. Its goal is to help you select the right encryption solution for your organization – one that offers data protection, without impacting the flow of business.

How to Use This Guide

This guide details the capabilities to look for when evaluating endpoint encryption solutions. It is separated into specific encryption features – full-disk encryption, file and folder encryption, mobile, etc. – for ease of use. It also includes key questions to ask vendors to help you identify which solution best meets your requirements.

Why Use Encryption?

Simply put, encryption makes data unusable in the wrong hands. By applying the latest cryptographic techniques, organizations gain peace of mind that attackers can't access critical information, even if they compromise data stores.

Compliance requirements across industries and geographies with penalties for breaches that lead to data compromises make it necessary to encrypt data. Something as simple as a lost USB stick carrying customer records could potentially put the whole business at risk for regulatory fines, loss of customer goodwill and damage to the brand.

More importantly, however, are the risk reduction benefits that encryption offers. Thieves steal devices such as laptops and smartphones. People leave iPads in pockets on the back of airplane seats and USB sticks everywhere.

Employees snoop in file shares they shouldn't really see. Driven by the rise of mobile devices, data is finding its way onto third-party cloud storage by the gigabyte – with or without company approval. But the speed of business today dictates that IT does not and should not get in the way of data portability. This leaves IT in a difficult position. You must allow data to freely move from device to device so users can access that data from anywhere at anytime. At the same time, if mistakes are made, the business must not be severely affected by unencrypted data compromises. Thus, any organization with compliance demands must consider data encryption a necessary precaution to keep up with regulators. In fact, the argument can be made that organizations in any industry should consider encryption a solid investment for protecting intellectual property and trade secrets. In today's world, every company is a technology company, from the baker to the banker; data is the currency of today's business.

Ultimately, encryption technology should be easy to integrate into a centralized IT workflow and easy to work in sync with corporate policies. More importantly, correctly deployed encryption should be seamless for the end user, no matter what type of file, device or storage the user needs to access.

Evaluating Solutions

Centralized management and control

Encryption solutions are available from many different sources. The ability to manage, control and report on the effectiveness of the solution is vital to the success of the overall project. When considering an encryption solution, review the individual pieces of data and how they are to be protected, and also ensure that you can centrally manage the policies and keys that enforce the protection. Client computers must be able to check in, report on their status and receive policies in return from the outside world, without relying on virtual private network (VPN) connectivity.

Keeping the responsibilities of administrators in line with their duties is also vital, as is auditing their actions. You must understand who has done what in your environment, and restrict access to sensitive areas according to roles.

With data disclosure laws becoming stricter, costly, and highly publicized, you need a consistent set of policies and management practices in place. Therefore, centralized management architecture is the key to the successful rollout of any encryption solution.

Centralized Management and Control		
Capability to look for	**Description**	**What to ask your vendor**
Centralized key and policy management	Managing encryption keys and policies centrally for all devices and platforms	Do you have a central solution to manage all necessary encryption keys and policies? Can you manage all encrypted devices?
Role-based administration	Administrator roles should provide only the privileges they need for their areas of responsibility	Can you separate duties from AD administrators, allowing specific security officers to be created and then restrict their area of control?
Auditable management functions	All activities performed in the management console must be recorded for future audit	Does your solution record who, for example, changed a policy, assigned keys to users, created security officers and provided recovery passwords?
Global client/server communication	Clients should be able to communicate with the encryption solution wherever they are in the world	Does you solution provide a reliable and secure communication method that does not require users to be connected to the corporate network, either directly or by VPN, without loss of functionality?
Reporting	Provide a mechanism to see the encryption status of your organization from a single console, regardless of operating system	Does your system provide a mechanism to report on all devices protected by the solution?
Proof of Compliance	Provide a mechanism to provide a proof of compliance report in the event of lost or stolen devices or data	Does your system give you the ability to prove that data was encrypted when it was lost or stolen?

Full-Disk Encryption (FDE)

Full-disk encryption protects against loss and stolen device use cases. It's primary responsibility is protection of data at rest; meaning when the device is powered off. Encompassing the entire disk or volume, from operating system to program files all the way down to temp files; it is the first line of cryptographic defense. In the past, third-party encryption technologies offered less nimble FDE options for devices, but the latest operating systems offer it natively. These built-in FDE technologies perform better and offer greater stability with a wide range of hardware with the added benefit of removing both hardware and operating system incompatibilities. Third party FDE options can suffer greatly from both, leading to an increased workload for both Administrators and Support staff.

In spite of these improvements and the performance gains attained from them, many security firms still override these built-in FDE options in favor of proprietary options that fit into an overarching endpoint encryption package. Ideally, though, an organization should be able to take advantage of built-in encryption within a centrally managed encryption suite. The solution should be able to cover gaps where built-in, full-disk encryption isn't enough protection – such as for legacy operating systems or file and folder encryption – while making it easy for IT to track encryption keys, and who has access to which data.

Full-Disk Encryption (FDE)		
Capability to look for	**Description**	**What to ask your vendor**
BitLocker support	Microsoft's built-in FDE technology	Do you support the Windows native encryption engine? If not, What is the impact of your solution on: • Boot time • System performance during runtime • How do you stay current with new hardware to ensure that your third-party encryption works on all new hardware? • How do you handle major and minor OS Upgrades? • What benefit does your solution provide over native encryption solutions?
FileVault 2 support	Apple's built-in FDE technology	Do you support the OS X native encryption engine? If not, What is the impact of your solution on: • Boot time • System performance during runtime • How do you stay current with new hardware to ensure that your third-party encryption works on all new hardware? • How do you handle Apple Extensible Firmware Interface and firmware updates? • How do you handle major OS upgrades? • What benefit does your solution provide over native encryption solutions?

File Encryption

File encryption offers further flexibility in protecting data on running systems. This is a second line of cryptographic defense, which sits on top of FDE. The primary responsibility for file encryption is the protection of data in use, and in transit. This type of encryption includes protection of data on removable media like USB drives, CDs/DVDs (yes, they all still exist), network file shares and information stored in the cloud.

With today's workforce becoming mobile and the corporate perimeter quickly vanishing, storing and sharing data via smartphones, tablets, the cloud, etc., is the new norm. Consider your own users – how many of them access company data on their mobile device (emails, files, etc.) and how much of your company data is shared on cloud-based storage services? While this improves the ease and simplicity of sharing data both inside and outside an organization, it also poses a threat in that confidential information may be exposed inadvertently. It also raises the question of "Where is your data?" and this can have a compliance impact in some geographies.

Encryption of cloud-based storage lets your organization's staff use public cloud storage services, as it offers more inaccessibility of data than a cloud provider would. Organizations need an encryption solution that can safely shield sensitive data from attackers' eyes. Files that go out to such services must be encrypted.

Mobile encryption features should allow your organization to encrypt all of the data stored on a device, while offering a safe way to access already-encrypted files stored on file shares or cloud storage.

In the case of removable media, a solid encryption solution will make it possible to easily share data on both approved and non-approved devices or among approved users on Windows or Macs while prohibiting unauthorized access, should the removable device be lost or stolen.

Meanwhile, encryption of file shares makes it easy to enforce role-based access to information. For example, encryption keys used for securing sensitive salary documents would be held by only human resources personnel, protecting IT administrators from accidentally accessing this sensitive data during the course of day-to-day activities.

In addition, a file encryption solution must work across multiple devices and operating systems. Your users will access data on a wide range of devices, during the course of their day-to-day activities. The ability to both access and encrypt files on those devices becomes imperative to not only protecting your data, but also for allowing users to remain productive.

File Encryption		
Capability to look for	**Description**	**What to ask your vendor**
Encryption for multiple endpoints (mobile devices, laptops, tablets, cloud, etc.)	Cross platform support. There is no point in only half of your business being able to access encrypted data	Is your solution cross platform? Does it work on Windows, OS X, iOS and Android? Can I access encrypted data on a mobile device such as a mobile phone or tablet?
Provide access for mobile devices to encrypted data stored on the device or in the cloud, regardless of device	An application for accessing encrypted data stored in the cloud from iOS, Android, Windows and Mac systems	Can you protect data being shared in the cloud among users, while allowing them access to work on different operating systems and hardware platforms?
Encryption of removable media devices	Protection for data on USB devices, CDs, DVDs, etc.	Does your solution provide a mechanism to encrypt data being placed on removable media with the option to leave existing data intact (e.g., not affect users' personal information)?
Encryption for network files shares	Protection for sensitive data stores authorized to be seen by only selective users	How do you prevent data from being accessed via elevated privileges or accidentally by privileged users?
Encryption for cloud storage	Protection for data stored in private, hybrid or public clouds	How can users access encrypted data stored in a cloud-based service from any device they use?

Comparing Solutions

Specific needs for your organization

Depending on your industry and geography, standards and compliance needs may change over time. Encryption is the de facto standard for meeting the strict data protection guidelines laid out by most regulators, but the specific encryption needs may vary depending on business drivers and existing technology deployments.

You're encouraged to use the above questions as a good way to benchmark encryption solutions based on your specific needs.

Ease of use/ease of deployment

Old perceptions about encryption's once-difficult nature may still linger, but the truth is that many of today's encryption suites have advanced beyond previous limitations. As you evaluate encryption solutions, consider how easy the technology is to use for two distinct populations within the business: end users and IT administrators.

More importantly, end users should be able to communicate, share data and collaborate without even being aware that the encryption is working. IT administrators should be able to roll out the technology without long deployment times. In the end, you should seek encryption that just works.

Future-proofing your encryption solution

Older encryption technologies were built with perimeter-centric security regimes in mind. Future-proof your encryption investments by seeking a platform that can handle yesterday's operating systems yet still easily incorporate the latest in native encryption capabilities.

The platform should also be able to accommodate sharing and portability by covering encryption of the removable drives, mobile devices and cloud storage options that today's employees depend on to collaborate and be productive.

Users today want to access corporate information from more places than ever: laptops, smartphones, cloud storage, network shares, USB sticks, etc. Choose encryption solutions that make it easy to stay compliant, that are able to prove it, and protect sensitive data across all platforms without getting in the way of your users.

Introducing Sophos SafeGuard_

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.

The following chart compares Sophos SafeGuard to other vendors key encryption capabilities.

	Sophos	Symantec	Microsoft	Intel Security (McAfee)	WinMagic Data Security
Full Disk Encryption (FDE) Windows XP, Vista, 7, 8, 10	✔	✔	✔	Limited	✔
Full Disk encryption OS X	✔	✔	✔	✗	✔
Utilizes Native FDE where available – Windows & OSX	✔	✔	✔	Limited	✔
File Encryption – Windows and OS X	✔	Limited	Limited	Limited	Limited
Removable media encryption – Windows and OS X	✔	Limited	Limited	Limited	✔
Cloud Storage Encryption – Windows and OS X	✔	✗	Limited	✗	Limited
Access Encrypted Data on Mobile devices	✔	✗	✗	Limited	✗
Single Management console	✔	✗	✔	✗	✔
Gartner MQ leader	✔	✗	✔	✗	✗

Conclusion

Users today want to access corporate information from more places than ever: laptops, smartphones, cloud storage, network shares, USB sticks, etc. Choose an encryption solution that makes it easy to stay compliant, that are able to prove it, and protects sensitive data across all platforms without getting in the way of your users.

Additional Reading

For further information about encryption, including links to some of the documents mentioned in this whitepaper, please see below.

Deciphering the Code: A Simple Guide to Encryption

This whitepaper aims to dispel the fear and confusion surrounding encryption.

Gartner Magic Quadrant for Mobile Data Protection

Gartner has recognized us as a Leader in the Magic Quadrant for Mobile Data Protection for the sixth year in a row.

Forrester Wave – Endpoint Encryption

Forrester Research, Inc. has recognized Sophos as a Leader in The Forrester Wave™: Endpoint Encryption, Q1 2015* report, calling Sophos its "breakout star" for 2015.

Security Readers' Choice Awards 2014: Encryption products

We're proud to announce that Sophos SafeGuard Enterprise has been awarded the 2014 TechTarget Readers' Choice Award for the best encryption solution.

Tolly Report: Encryption Speed and Performance test

Performance tests conducted by the independent testing firm Tolly show that Sophos SafeGuard Encryption is the fastest solution for disk encryption, with the lowest impact on performance for boot-up and in sleep/hibernate/wake tests.

Sophos SafeGuard Enterprise

Register for a free 30-day evaluation at sophos.com/free-trials

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

Oxford, UK | Boston, USA

2015-08-19 BG-NA (RG)

SOPHOS