Why Implement Endpoint Encryption?

James Christiansen
October 21,2013

CMS

Table of Contents

Endpoint Encryption

Part I – Why Implement Endpoint Encryption?

Introduction

The number of mobile devices has grown exponentially in the past few years and the typical organization has become reliant on the use of mobile devices as part of their overall business information technology. The reputation cost and operational expenses of a security breach can be devastating to an organization. A well implemented endpoint encryption solution must handle a laptop, mobile phone and tablet device encryption equally.

This white paper is provided in a three part series; Part I – "Selecting the Right Solution" focuses on the business case drivers for implementing an endpoint encryption solution. Part II – "Selecting the Right Solution" addresses the primary considerations selecting the right endpoint encryption solution, and Part III – "Successful Implementation" reviews best practices implementing an endpoint encryption solution.

Series Key Points

- Loss/Stolen endpoint devices are a leading source of security breaches. Implementing an effective endpoint encryption solution provides a safe harbor.
- Implement endpoint encryption to protect your intellectual property, protect your customers, and meet your regulatory requirements.
- Endpoint encryption solutions should conform to industry standards such as Trusted Security Group's OPAL[i] to protect your investment.
- Reviewing the solution for critical features will lead to more successful adoption across the organization.
- A systematic implementation increases the probability of a successful implementation and a satisfied user.

Why Implement Endpoint Encryption?

Implementing an endpoint encryption solution is a daunting task filled with potential disasters. Why then implement an endpoint encryption solution? The most significant loss U.S. companies' face is the loss of intellectual property (IP). Another source of concern is government mandates for protecting sensitive information. The disclosure laws require that anytime an endpoint with regulated data (PII, PHI, etc.) is lost or stolen you must disclose to the potential victims. The cost of protecting your IP, customers, managing the disclosure, mitigating the cause of the breach, and the potential regulatory fines and lawsuits more than justify the cost of deploying a world-class endpoint encryption solution.

The Law

The biggest seller of encryption is the news. Security breach notification laws have been enacted in most U.S. states since 2002 and each day security breach notices are in the news and costing the notifying company thousands to millions of dollars a year. In 2012 the average cost of a security breach in the U.S. was $5.4 million dollars excluding the "mega" breaches (breaches exceeding 100,000 records)[ii]. In most cases properly encrypted data is a "safe harbor" from breach notice. If the lost/stolen device is encrypted then your loss is limited to the depreciated cost of the corporate asset.

Government regulations such as Gramm-Leach-Bliley Act (GLBA), Federal Information Security Management Act (FISMA), Health Insurance Portability & Accountability Act 45 CFR 164.308 (HIPPA) and Sarbanes-Oxley (Section 302 & 404), and industry requirements such as the Payment Card Industry (PCI) standard require encryption of sensitive information. Some States within the U.S. have passed State level laws requiring encryption for sensitive information.

Risk Management

While encryption is required for safe harbor in many different regulations and industry standards such as PCI, it is also important to use encryption as part of your overall risk management program. Don't only encrypt data that is required by law also encrypt data that is sensitive to the business. A company that markets a software solution should encrypt its most important business asset – the software.

You are faced with the ongoing decision to provide full disc or file/folder encryption. In older computer systems the overhead of encryption could cause degradation of performance, but with more current technology the overhead of encryption in unperceivable. Given the improvements in technology the cost and risk of managing file/folder encryption far exceeds the additional cost for full-disk encryption. To minimize the risk of disclosure of sensitive information deploy a full disk encryption solution.

First Steps

Take Action Now: Regardless if the driving pressure is protection of the corporate assets, a "red" audit finding, or a requirement to meet a customer or regulatory demand. It is time to implement or expand your encryption deployments. Encryption is the only safe harbor for many of the government regulations. The cost of losing a fully encrypted endpoint device is limited to the depreciated capital value. The cost of a lost or stolen endpoint device that is unencrypted can be in the millions!

Policy: The first step is to design and implement a corporate wide policy requiring encryption. Make sure you are able to gain support for, and implement a new organization wide policy to encrypt sensitive data on all media. Each company will have their own definition of sensitive data but many of the government regulations require any data with Personally Identifiable Information (PII) and Protected Health Information (PHI) be encrypted.

Migrating Existing Users: There are a number of considerations when implementing an endpoint encryption solution that are discussed later in the paper. One of the biggest challenges is migrating a user from the current non-encrypted system to an encrypted system. The first time encrypting an endpoint for an existing user can take hours and be very frustrating for the user, and if the frustrated person is one of the key executives the project could end before it even gets started!

To migrate an existing user's endpoint consider using fully encrypted hard drive backup storage devices. How would that work? Simply plug the backup device into the user's system while he is working and the software will make a full encrypted copy of the primary system. The next day simply swap the drive in the backup system with the primary device and within minutes the user is up and running on the new fully encrypted hard drive! Make sure the old unencrypted hard drive is disposed of properly (wiped and repurposed or completely destroyed).

External backup drives and flash drives are a common area of security breach. When storing data on an external backup device or flash drive make sure the devices are encrypted.

Solution Type: Determining the best solution type that fits your business needs requires choosing between full disk encryption and file/folder encryption. There are advantages to each but with the computing power of the recent mobile devices the overhead of encryption is unnoticeable. With file/folder encryption the user is required to manage security of the information and can easily lead to sensitive data that is not encrypted on the hard drive. With full disk encryption everything is encrypted automatically and no management is required by the user. Full-disk encryption is simpler to implement and is the preferred solution for most companies.

Summary

The business drivers for implementing an endpoint encryption solution is a combination of legal and best practices in enterprise risk management. Get started now with a good policy and determining the requirements and migration strategy for your end users.

Part II of the series "Selecting the Right Solution" addresses the primary considerations when selecting the right endpoint encryption solution, and Part III – "Successful Implementation" reviews best practices implementing an endpoint encryption solution.

Endpoint Encryption

Part II – Selecting the Right Solution

Introduction

This is part two of a three part series on endpoint encryption. Part I of the series focused on the business case drivers for implementing an endpoint encryption solution. This article focuses on selecting the right solution and Part III – "Successful Implementation" of the series will review best practices implementing an endpoint encryption solution.

Series Key Points

- Loss/Stolen endpoint devices are a leading source of security breaches. Implementing an effective endpoint encryption solution provides a safe harbor.
- Implement endpoint encryption to protect your intellectual property, protect your customers, and meet your regulatory requirements.
- Endpoint encryption solutions should conform to industry standards such as Trusted Security Group's OPAL[iii] to protect your investment.
- Reviewing the solution for critical features will lead to more successful adoption across the organization.
- A systematic implementation increases the probability of a successful implementation and a satisfied user.

Selecting the Right Solution

When considering implementing endpoint encryption make sure to account for three core elements; people, processes and technology to support the business need. The technology is covered in the next section. People and process elements are covered in the implementation recommendations.

Evaluating the Technology Solution

As you are evaluating any technology solution you should consider six different aspects; Feature/Function, Usability, Integration, Interoperability, Cost, and Vendor Support/Viability.

Feature/Function: Below we will discuss the primary and secondary features of endpoint encryption. Depending on your own individual business requirements the feature set will vary in importance.

Usability: The usability will always be an important factor when selecting an endpoint encryption product. If the users find the solution cumbersome or prevent them from being productive you will get resistance in the deployment. A great endpoint solution will be transparent to the end-user.

Integration: The solution must integrate many different types of encryption and legacy technologies. It is likely some existing encryption technologies (e.g. BitLocker) have been deployed on some endpoints. The solution will need to be able to manage those devices during transition and support new technologies such as Self Encrypting Drives (SED).

Interoperability: The solution must be able to interoperate with your organizations core architectures and information technology standards. For example, if your users are on Apple products and the solution does not support Apple then it wouldn't make sense to purchase the product. Many large organizations lack a complete inventory of their end-users machines which will complicate the selection and deployment. With today's dynamic work force the solution with the widest interoperability including workstations, laptops, smartphones and tablets should be considered.

Cost: Total-cost-of-ownership is the entire cost of the solution including; license costs, maintenance, and support. A solution that is more expense to license but is more transparent for the users will cost less than a solution that causes a high number of help desk calls. There is a tradeoff between cost and usability/functionality of the solutions. Often usability will outweigh the cost, but for a smaller organization with limited budgets the cost may be the determining factor.

Evaluating the Solution Provider

Do not underestimate the value of selecting the right vendor. It is often a more critical than the feature/function of the product. Many vendors may be able to meet your minimum requirements for functions buy may not be able to support your organization in the geographic locations of your business.

Vendor Support: One of the key long term views of the product is the ability for the vendor to support the product across the geographic locations of the companies. For a multi-national company this can be one of the deciding factors. If you find the best product features at a great price but they cannot adequately support your organization it is better to turn to the next best supplier.

Vendor Viability: Is the vendor dedicated to providing solutions in this technology or is this a side-line business? Endpoint encryption is much too important to deploy from a vendor that this product is not core to the company. Over the long term it will not keep up with other solutions and runs the risk of being discontinued. The long-term financial health of the company should also be considered. Endpoint encryption is very strategic and difficult to switch to another provider if the vendor should become financially insolvent.

Endpoint Encryption Features

There are a number of features to consider when selecting an endpoint encryption solution. The best choice will be the one that is transparent to your users, integrates seamlessly with your technology, and is scalable/cost effective for your deployment.

Standard Features

There are a set of standard features that all endpoint encryption deployments will require:

Standard Encryption Algorithm: The solution should use one of the industry standard encryption algorithms (e.g. AES) certified by FIPS. Non-standard algorithms may not provide a safe harbor under the regulatory statutes and should be avoided.

Key Management: Not having a great key management system is like buying the best car alarm in the industry and then leaving the keys in the door. The weakest link in any encryption deployment is the key management system. Why try to break AES 128 bit encryption when you can easily gain access to the encryption keys through an ineffective key management system?

Solution Flexibility: The solution needs to work equally well in a standalone environment as when attached to the corporate network.

Full-Disk and File/Folder Encryption: The solution must have the ability to support full-disk encryption. The ability to support file/folder encryption is becoming less important as the underlying hardware has become fast enough to handle the overhead of encryption without degradation of response time for the user. However, for organizations with a lot of older legacy endpoints file/folder encryption may still be a core requirement.

Recommended Features

The following features are recommended to have a successful implementation of a long term solution.

Remote Storage: Most individuals require additional space to backup or store their information that is offline to their main system. Some users need large disk storage devices to transfer information from one location to another. The solution must provide the ability to transparently encrypt the data on to the mobile disk and then allow the authenticated user access to the data at the remote site. A great solution will allow encrypted backups to be used as the primary system in the event of a main system failure (e.g. system boot device crash) until the system disk can be restored.

Enterprise Management: The solution must include an enterprise management system that provides the ability to monitor the use of the system, provide proof that endpoint is encrypted, mange the global settings and deploy upgrades.

Single Sign-On: One of the key transparency qualities of great solution is the ability to carry the sign-on from the initial boot to the operating system to open the encryption. Nothing is more annoying for the end-user than needing to sign-on multiple times.

Data Mobility: Data is constantly moving and the number of devices and options are increasing. The ability to put data on USB drives, smartphones and tablets requires the encryption solution be fluid throughout the mobile data ecosystem of the user.

Mobile Device Encryption: Smartphones and tablets sales have exceeded the number of laptops in a typical organization today. An endpoint encryption solution must be able to manage encryption on mobile devices.

Removable Device Encryption: The solution is capable of encrypting removable devices such as USB devices using the same user interface, and has the ability to unlock the device (given proper credentials) on other computers without requiring additional software.

Remote Wipe: Lost/stolen devices represent an ongoing risk to the organization and a great solution should provide the ability to remotely wipe the system to further protect the information.

Summary

Selecting the right solution is critical to success of the project. Part I of the series defined the business drivers for implementing an endpoint encryption solution, getting started with a good policy, determining the requirements and migration strategy for your end users.

Selecting a solution that meets the business requirements is a strategic decision and implementing a solution that is compliant with industry encryption standards makes good business sense. The right solution is a combination of feature/function, usability, integration, interoperability and cost of the solution. Selection of the right solution provider is equally important. The vendor must provide support in the geographic areas that you do business. Selecting an endpoint encryption solution is a strategic decision and the long term viability of the vendor must be evaluated.

Part III – “Successful Implementation” reviews best practices implementing an endpoint encryption solution.

Endpoint Encryption

Part III – Successful Implementation

Introduction

This is part three of a three part series on endpoint encryption. Part I of the series focused on the business case drivers for implementing an endpoint encryption solution. Part II of the series provided a deep dive into selecting the right solution. This article focuses on the successful implementation of an endpoint encryption solution.

Series Key Points

- Loss/Stolen endpoint devices are a leading source of security breaches. Implementing an effective endpoint encryption solution provides a safe harbor.
- Implement endpoint encryption to protect your intellectual property, protect your customers, and meet your regulatory requirements.
- Endpoint encryption solutions should conform to industry standards such as Trusted Security Group's OPAL[iv] to protect your investment.
- Reviewing the solution for critical features will lead to more successful adoption across the organization.
- A systematic implementation increases the probability of a successful implementation and a satisfied user.

Successful Implementation

The successful implementation of any new business solution requires three primary elements; people, process and technology. We have looked closely at the technical requirements now we explore the people and process requirements.

People

Executive Support: The successful implementation of endpoint encryption requires a strong champion at the executive level. Expect initial resistance for the costs involved in implementing the solution and more resistance during product implementation. Even the most transparent endpoint encryption solution requires the user to make some changes in their processes. People inherently do not like change and will resist the changes required by the project. A strong executive will assist in supporting the implementation throughout the lifecycle.

Training and Awareness Plan: Paramount to any successful implementation of endpoint encryption is the training and awareness plan. However, the more transparent the solution the less required of the training program. The ultimate solution is completely transparent and requires no training or awareness for the end users.

Effective Communications: Use your internal information mechanisms (e.g. blogs, etc.) to support the need for encryption by showing losses of other companies for unencrypted data on laptop computers, mobile media, and tapes. Staff members that do not believe that encryption is important will resist the implementation and may even obstruct progress.

Process

Testing: Test each of the implementation scenarios to make sure the product is working properly. Equally important is to test the "negatives" by trying to break the program. Do a complete and partial recovery of the encrypted data and a key management system recovery. Once your organization is dependent on the solution you don't want to find out that you cannot recover!

Systematic Implementation: Plan out the implementation of your endpoint encryption program with success milestones no more than three months apart. It is best to start with non-critical or "friendly" staff first, often members of the IT team. Fine tune the training, help desk support, and communication plan during the initial deployment phase. Show success at each milestone and then move to the next phase.

Success Metrics: Map out the success metrics that are going to be used during the implementation phase. Start with simple metrics like IT Laptop pilot, then percentage of deployment across a wider audience. Measure helpdesk calls, satisfaction and response time for resolution.

Support: A key success factor is the ability to react quickly to any problems that arise. Expect the unexpected. Make sure the helpdesk staff are trained on the product and kept informed of each phase of the deployment. The solution provider technical staff contact information should be tested occasionally to make sure the support is there when you need it!

Solution Management: Once the system is up and running it is not time to forget and move onto another product. Make sure you have set up a process to keep the solution updated with any fixes and upgraded to new releases of the software. All the testing and recovery procedures need to be retested after upgrades and major enhancements.

Summary

Selecting the best product to meet the user requirements and a vendor that provides great support is meaningless unless a systematic implementation approach is taken. Part I of the series defined the business drivers for implementing an endpoint encryption solution, getting started with a good policy, determining the requirements and migration strategy for your end users. Part II provided the primary drivers of selecting the right technology and the importance of vendor support. This article provided the key considerations for a successful implementation using a combination of the people and processes.

Loss/Stolen endpoint devices are a leading source of security breaches and implementing an effective endpoint encryption solution provides a safe harbor. In addition, endpoint encryption makes business sense to protect intellectual property, protect your customers, and meet your regulatory requirements.

Selecting a solution that meets the business requirements is a strategic decision and implementing a solution that is compliant with industry encryption standards makes good business sense. The right solution is a combination of feature/function, usability, integration, interoperability and cost of the solution. Selection of the right solution provider is equally important. The vendor must provide support in the geographic areas of your business. Selecting an endpoint encryption solution is a strategic decision and the long term viability of the vendor must be evaluated.

A successful implementation requires strong executive support and having a champion on the project is critical. Start by designing an effective training and awareness plan that includes communication on the importance of the project and training the staff on how to use the product. Using a systematic approach to the implementation will reduce the impact to the organization and improve the chances of a successful project.

After the solution implementation is complete continue to monitor the usage of the system and user satisfaction. Stay in front of any problems quickly to avoid unnecessary dissatisfaction. Continue to monitor the viability of your solutions provider and provide active feedback on new features to make your implementation more successful.

Endnotes

[i] http://www.trustedcomputinggroup.org/resources/tcg_storage_security_subsystem_class_opal_version_100_revision_200

[ii] 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2013

[iii] http://www.trustedcomputinggroup.org/resources/tcg_storage_security_subsystem_class_opal_version_100_revision_200

[iv] http://www.trustedcomputinggroup.org/resources/tcg_storage_security_subsystem_class_opal_version_100_revision_200