Best Practices Guide - May 2010

Top Five Recommendations for Encrypting Laptop Data

Best Practices Guide

By Datacastle
May 2010

Contents

Executive Summary 1
Protecting Laptop Data at All Times 1
Understanding the "Key" to Encryption Best Practices 2
Best Practices for Encrypting Laptop Data 3-6

Top Five Recommendations for Encrypting Laptop Data

Best Practices Guide - May 2010

Executive Summary

Today's highly mobile workforce is placing new demands on IT teams when it comes to protecting laptop data. To guard this corporate data at all times, companies can follow a number of data protection and encryption best practices, especially related to how encryption keys are managed. Incorporating these best practices into your IT organization can reduce data storage needs, get more out of your existing IT budgets and free your team to work on more value-added projects.

Protecting Laptop Data at All Times

Protecting your company's growing digital assets and complying with regulations is one of your top IT priorities. To do this, you are probably following the highest available encryption standards within your data center. You likely have a backup policy that you enforce to help maintain business continuity. And, as a server-centric organization, you may even have a policy that prohibits employees from keeping sensitive information on their laptops. After all, with a highly mobile workforce, some of your company's most critical data assets are on these laptops—at the edge of your network.

However, end user-dependant policies can only do so much to protect data. If a data breach occurs at the edge, your customers, investors and fellow employees will be most concerned about the exposure, not comforted that you have reprimanded an employee for not following the data policy in place.

Fortunately, there are a number of encryption best practices you can take to help project your company's laptop data at all times—at rest, in motion, during back up, and in restoration if a laptop is lost or stolen.

This paper outlines five areas to consider in data protection, as well as best practices to ensure your data is as secure as it can possibly be. These five areas are:

– Ensuring security for data at rest.

– Facilitating security for data in motion.

– Enabling security for backed up and restored data.

– Pairing encryption with secure data deduplication.

– Easing IT management and support.

Understanding the "Key" to Encryption Best Practices

Before delving into the best practices, it's important to understand the process of encryption and the questions it brings up around key management.

In its simplest definition, encryption uses an algorithm to convert data into an unreadable state, which can then be unlocked with a key and converted back into a readable state. Standards like the US government-approved 256-bit Advanced Encryption Standard (AES) specify which algorithm to use and how keys should be generated. The output is a cryptographically random encryption key that can then be used to encrypt or decrypt the data when needed.

As it turns out, encrypting data is relatively easy to do, especially now that encryption standards are being built into laptops and operating systems. However, key management—the way in which keys are generated, processed and managed—is significantly more difficult. For example, if you comply with the 256-bit AES standard, apply it to corporate data, and scale it across 100 or 1,000 or 100,000 employees, it can become exceedingly hard to manage the large number of cryptographically random encryption keys.

Some prevailing market solutions have skirted this issue by taking a derived key approach. The most common option is to use a password, which translates into a 128-bit or 256-bit key that is used to encrypt and decrypt the data. This method relies on employees with laptops to remember the password, keep it private and change it at regular intervals per your IT policy. Unfortunately, passwords can also be easy to guess.

Other Web-based market solutions take a stored key approach, keeping the key in a storage center to decrypt the data when you need it on the Web site. In this case, anyone who has access to the servers would have a copy of the key list to your data and could decrypt it. Clearly, this approach is not providing the full measure of security available.

To increase your company's laptop security, remember to use:

- Multiple keys across your data sets so that if a single key is compromised, only a subset of your data is exposed.
- At least 256-bit keys so your keys are of sufficient length.
- Cryptographically random encryption keys, rather than derived keys, to realize the full strength of the encryption process.

Best Practices for Encrypting Laptop Data

Since key management is the crux to making a solution secure and private, it is important to think about the ways your encryption keys are being generated, processed and managed. Following are five scenarios to consider along with forward-thinking best practices you can adopt to make sure all of your data is protected—all of the time.

Ensuring security for data at rest

The first step is to make sure that your employees' laptop data is properly encrypted while on the hard drive. This will help keep it safe if a laptop is lost or falls into the wrong hands.

The traditional method for securing data on a laptop hard drive is whole-disk encryption. Software installed on the device works to encrypt the applications, operating system and disk all the way down at the hardware level. To use a laptop with whole-disk encryption, employees often must provide a password as soon as they turn on the device, known as a pre-boot authentication, and then a second separate password to authenticate to the operating system.

One of the downsides of whole-disk encryption is that once the laptop is unlocked and the system is up and running, all the data on the device is unprotected. Other people using the laptop or coming in over the network through background processes like malware can access the at-rest data on the laptop in an unencrypted way.

Another issue is performance. Encrypting and decrypting every piece of data takes time, which slows down the machine and can annoy on-the-go employees. Yet another downside is relying on employee behavior as it relates to policy enforcement. For example, some employees may not activate the boot-level password for fear of getting locked out of the system. A final issue is deployment; whole-disk encryption solutions can be difficult to deploy, require more set up time, and can increase help desk call rates.

Best Practice #1

The more advanced and performance-friendly alternative is file- and folder-based encryption. This flexible method encrypts data as it is stored on the laptop and decrypts it when an employee opens an application file, which greatly reduces the performance penalty. File- and folder-based encryption also ensures that data is protected whether the laptop is on or off.

Equally important, the encryption method is transparent to employees, not requiring them to remember additional passwords to secure sensitive data on their laptops. This will curtail employee resistance and minimize IT help desk calls to request password changes.

Managing this approach is easy at the IT level, too. File- and folder-based encryption is straightforward to deploy and support. IT administrators can use policy-based granularity to select specific files and folders to encrypt as employees use them on the laptop. By using automatic policy-based enforcement, rather than employee behavior-based enforcement, you gain much greater protection and security.

Facilitating security for data in motion

The next area to consider relates to encryption factors around data in motion. If you are going to allow employees to copy files to USB drives or burn data to CD/DVD ROM drives, make sure you are using an encryption solution that follows with the files as they are being copied off the laptop and onto the portable media.

Best practice #2

Ironically, the first thing to do when securing data in motion does not relate to encryption. Instead, you start by defining the read/write access permissions for the different ports on the employee's laptop. This procedure is sometimes also called device control.

After you have set your device access control permissions, then you can turn your attention to how data is protected in transit. To do this, create a policy to minimize data leaks—known as data leak prevention (DLP)—so that you are using strong encryption on data being transferred through the ports that you allow to be used.

One of the most commonly overlooked areas for protecting data in motion is when data is being moved for backup purposes. In this case, you first need to ensure that data being moved is encrypted before it leaves the laptop. Secondly, you also want to ensure the transmission is secure while the data is in transit by using a secure sockets layer (SSL). If you don't do both, your corporate data will be exposed at either end of the process.

Enabling security for backed up and restored data

The third area to consider is making sure that data in back up is properly encrypted, with a secure transmission and a lock-tight storage facility. As described above, the derived and stored key approaches have limitations that can leave your corporate data at risk. The answer lies in how the keys are managed.

A related area comes into play when an employee loses a laptop or a hard drive goes haywire. It is best from a support-cost perspective to allow employees to recover data themselves in a self-service manner. However, when facilitating this, you need to make sure that the employee or their new laptop is properly authenticated to IT. In addition, if the data needed to be encrypted in the first place, when it is recovered to the new laptop, it should also be forced to be in an encrypted state.

Best practice #3

The best way to ensure that your corporate data stays private and secure during back up is to generate and manage cryptographically random keys in a scalable way. Similarly, the way in which the key is managed is critical to enabling data to be restored when the original laptop is not available.

In addition, in a recover situation, remember that you do not want old data left on the stolen laptop. Ideally, the data on the laptop should have been encrypted so the first thing you would do is destroy the key, and then the data on the lost laptop, either through a command or a timed poison pill. This step removes the thief's greatest asset in trying to gain access to the lost data—time. Such digital shredding should also be done so that the data is not retrievable using disk recovery tools.

Pairing encryption with secure data deduplication

The fourth area to think about is how encryption impacts the amount of data you have to store. More than likely, your corporate data is stacking up at a rapid pace—and that's driving up your data center storage costs in the process. To address this, you may use data deduplication, whether on the client-side (laptop) or the target-side (storage location), to eliminate duplicate data blocks, and thus have less data to store.

However, traditional data deduplication and encryption work at odds with one another. Data that is encrypted using different encryption keys looks random and thus cannot be deduplicated. This incompatibility leaves you in a data backup bind as you have to falsely decide which is more important: security or storage budgets.

One workaround used by most backup vendors is to decrypt the data, perform data deduplication and then re-encrypt the data, but this process leaves your corporate data vulnerable in the unencrypted state gaps. The key also has to be known and thus is equally vulnerable. Another option is to perform data deduplication across encrypted data by sharing one key across all employees, but this makes the solution only as strong as a single key. Neither choice is optimal.

Best Practice #4

Secure, automated key management makes it possible for encryption and data deduplication to work together. The best way to do this is to complete the encryption process up front and then run data deduplication on the encrypted data using a secure key escrow system. This breakthrough concept allows you to gain the storage cost benefits of data deduplication with the strong protection realized by multiple, cryptographically random encryption keys.

Easing IT management and support

The last encryption area for you to assess comes down to manageability—for both your company and your IT team. Yet all too often, ease of use is sacrificed for a secure encryption solution. The reality is that the more friction your employees experience, the more likely they will work around the security solution. Conversely, the more friction-free your encryption solution, the greater the adoption rate, which leads to better overall security for your company.

Best Practice #5

The best way to deliver on the data security and privacy promise is to find an end-to-end solution that is easy to deploy (ideally a silent install) and integrate with your existing desktop management infrastructure. Most of all, you need a friction-free solution that minimizes forgotten passwords and keeps your IT help desk team focused on more important priorities.

Datacastle Solution Encompasses Best Practices

Incorporating these five encryption best practices into your comprehensive IT security plan can reduce your data storage needs and simplify your IT encryption management processes.

The Datacastle solution answers this call with an end-to-end approach to encryption and keys—from key generation, to key management, to key storage.

Specifically, Datacastle RED (Resilient Endpoint Data):

– Uses the file- and folder-based encryption approach and takes it one step further with a smart approach to key management.

– Enables port access control and follow-along encryption for data in motion.

– Employs a secure, automated key management process for backing up and restoring data that allows encryption and deduplication to work together.

– Brings all these security features into a friction-free solution that will result in easy deployment and enforcement—and fewer help desk requests.

With this broad range of functionality, Datacastle RED can make your business more resilient. Now your IT department can help keep control of corporate data assets and meet regulatory requirements while allowing your company's highly mobile employees to be as productive and effective as possible.

Learn More

To learn more about Datacastle RED, please visit our website at www.datacastlecorp.com, email us at info@datacastlecorp.com, call us at (425) 996-9684 or follow us on Twitter @Datacastle.

About Datacastle

Datacastle makes an organization's mobile workforce resilient to the unexpected. Listed in Gartner's Hype Cycle for Storage Technologies, 2009, Datacastle RED turns vulnerable business information into a resilient, managed business asset. Datacastle empowers IT to enforce data policies and exceed compliance requirements. For more information, visit http://www.datacastlecorp.com.