CARBONITE® ENDPOINT

CARBONITE® an opentext™ company | WEBROOT® an opentext™ company

3 secrets to data encryption

Tools and tips for preventing unwanted access to confidential data

Best practices bring results

Workforce mobility places serious demands on IT teams when it comes to protecting laptop data. With data spread across the organization, and between different locations and systems around the world, keeping it secure from unwanted access becomes increasingly challenging. To simplify this seemingly impossible task, companies should observe a few data protection best practices—in particular, those related to managing encryption keys. Incorporating these best practices into your IT organization offers a number of advantages:

- Reducing total data storage needs
- Getting more out of your existing IT budgets
- Freeing your team to work on more value-added projects

Protecting laptop data at all times

Protecting digital assets and complying with regulations are high priorities for IT organizations. It necessitates following the highest available encryption standards within your data center, as well as implementing a backup policy that helps maintain business continuity. This white paper outlines five areas to consider:

- Ensuring security for data at rest
- Ensuring security for data in motion
- Enabling security for backed up and restored data
- Pairing encryption with secure data deduplication
- Facilitating IT management and support

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 U.S. 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.

Encrypting data is relatively easy, especially now that encryption standards are 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 becomes exceedingly hard to manage the large number of cryptographically random encryption keys.

Some solutions use a derived key approach involving 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 remembering the password, keeping it private and changing it at regular intervals. Unfortunately, passwords are easy to guess. Another approach is to keep the key in a storage center to decrypt the data when you need it. In this case, anyone who has access to the servers would have a copy of the key list and could use it to decrypt the data.

To increase your company’s laptop security, do the following:

- Generate multiple keys, so that if a single key is compromised, only a subset of data is exposed
- Ensure data encryption is at least 256-bit so your keys are of sufficient length
- Use cryptographically random encryption keys—not derived keys—to realize the full strength of the encryption process

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. 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 to 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 may increase help desk call rates.

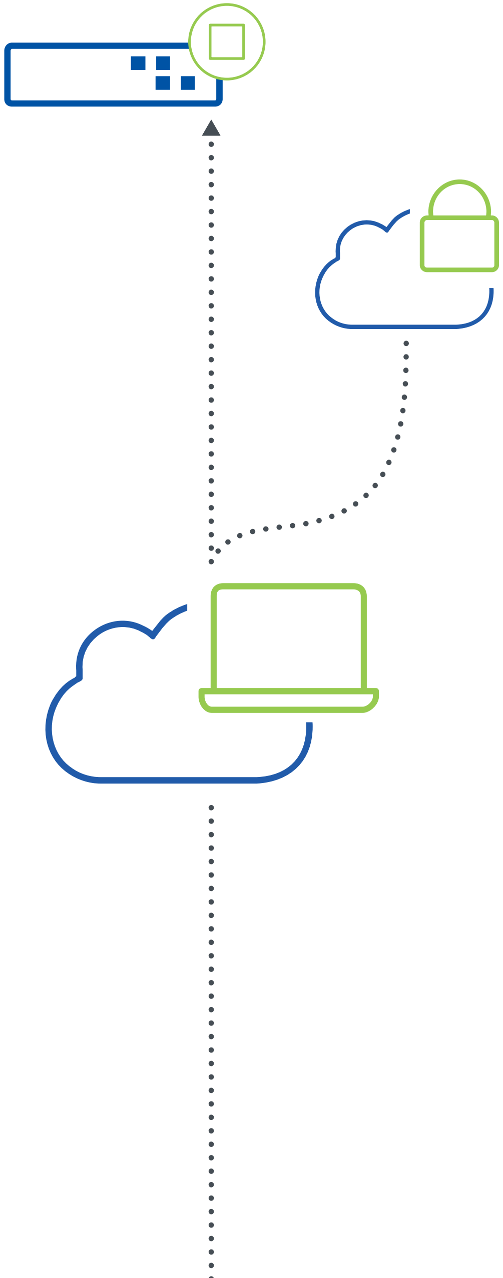
Best practice #1:
Use file- and folder-based encryption

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.

The encryption method is transparent to employees, who no longer have 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.

There's still the issue of protecting data while it's in transit. One glaring vulnerability that almost all organizations face is the employee practice of copying files to USB drives. Whether data in motion exists on a compact storage device or a wide area network, organizations need a solution that protects data whenever it's moving from one waypoint to another.



Best practice #2:
Establish security at every step

End-to-end security is achieved by first defining read-write access permissions for the different ports on employee laptops. This procedure is sometimes called device control. After you have set your device access control permissions, consider 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 is encrypted before it leaves the laptop. You also want to ensure the transmission is secure, using transport layer security (TLS/SSL). If you don’t do both, your corporate data will be exposed at either end of the process.

Another consideration is making sure that data stored in backup is properly encrypted. Storing encrypted data presents challenges for IT organizations because traditionally, 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 forces IT to 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 gaps in security. 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 #3: Practice scalable key management

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.

The way in which the key is managed is critical to enabling data to be restored when the original laptop is not available. In the event of a lost or stolen device, 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.

Bonus tip: Find an end-to-end solution

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 integrates 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.

Incorporating encryption best practices into your comprehensive IT security plan can reduce your data storage needs and simplify your IT encryption management processes. Carbonite answers this call with an end-to-end approach to encryption and keys—from key generation to key management to key storage.

Specifically, Carbonite Endpoint Protection uses file- and folder-based encryption and takes it one step further with a smart approach to key management:

- It enables port access control and follow-along encryption for data in motion
- It employs a secure, automated key management process for backing up and restoring data that allows encryption and deduplication to work together
- It incorporates all these security features into a friction-free solution that will result in easy deployment and enforcement—and fewer help desk requests

Conclusion

With this broad range of functionality, Carbonite Endpoint Protection can make your business more resilient. Your IT department can maintain 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.

Contact us to learn more – Carbonite US

Phone: 877-542-8637

Email: carb-data_protection_sales@opentext.com

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.