CARBONITE

At-Rest-Encryption

Carbonite Endpoint Backup delivers security with At-Rest-Encryption

Organizations today understand how critical it is to ensure that employee laptop data is properly encrypted while on the hard drive in the event that a laptop is lost or falls into the wrong hands. At-Rest-Encryption refers to the fact that the data is physically stored in an encrypted manner. At-Rest-Encryption works in conjunction with whole disk encryption.

Understanding encryption

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

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

Ensuring security for data at rest

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.

Once the laptop is unlocked and the system is up and running, all the data on the device is unprotected. Whole-disk encryption is especially problematic for laptops because they are often left "asleep" rather than being properly shut down. 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.

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.

Carbonite Endpoint Backup At-Rest-Encryption

- Can work standalone or in conjunction with FDE
- Is lightweight with no performance hit to the user
- Deletes any file from a laptop when a hacker tries to override a login password or perform a cold boot attack
- Leverages Windows EFS (Encrypting File System)
- Offers highest levels of encryption using AES 256

Contact Us

2 Ave de Lafayette
Boston, MA 02111
800-683-4667
DataProtectionSales@carbonite.com

© 2017 Carbonite, Inc. All rights reserved.

At-Rest-Encryption

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.

The Carbonite Endpoint Backup solution

The Carbonite solution 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 Backup:

- **Key management**: Uses the file- and folder-based encryption approach and takes it one step further with a smart approach to key management
- **Protect data on the move**: Enables follow-along encryption for data in motion
- **Encrypt and de-duplicate**: Employs a secure, automated key management process for backing up and restoring data that allows encryption and deduplication to work together
- **Easy deployment and enforcement**: 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, Carbonite Endpoint Backup can make your business more resilient.

Carbonite Endpoint Backup encryption in action

An executive at a financial services firm attending a conference discovers that her laptop has been stolen when she turned away to take a cell phone call. She immediately notifies IT at her firm that the laptop may have fallen into hostile hands because there is highly sensitive information about the company's performance on it.

Using Carbonite Endpoint Backup's security suite, IT is able to remotely delete all protected data on the executive's stolen laptop by an administrative command if the laptop connects to the internet or via a poison pill which can be scheduled via a policy.

At-Rest-Encryption gives the added protection of deleting protected files when a hacker tries to access the data by trying to crack the administrative passcode. With At-Rest-Encryption, files are also protected while the user is on unprotected wifi networks. Anyone trying to access the laptop will not be able to open any files that are protected with ARE as they won't have the correct encryption keys.

© 2017 Carbonite, Inc. All rights reserved.