Carbonite Endpoint encryption

Carbonite Endpoint combines top encryption technologies to keep data secure at all times

Businesses can't afford compromises when it comes to the security of data stored on company devices. If a laptop is lost or stolen and the data becomes accessible to the wrong people, the consequences could be devastating. That's why it's critical that businesses use encryption to protect data while it's at rest on a laptop or mobile device.

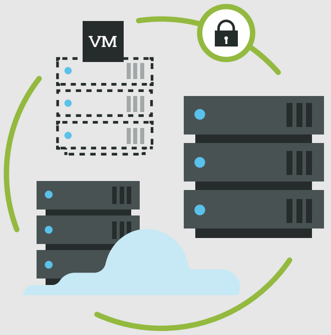
Encryption overview

Most encryption technologies use an algorithm to convert data into an unreadable state. To unlock it, the user needs the digital key that converts the data back to a readable state. The traditional method for securing data on a laptop is full-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 full-disk encryption, employees often must provide a password as soon as they turn on the device, and then again to authenticate the operating system.

Once the laptop is unlocked and the system is up and running, all the data on the device is unprotected. Full-disk encryption is especially problematic for laptops, since they're 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

An alternative method for securing the data 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, who don't have to remember additional passwords to secure sensitive data on their laptops. This reduces employee resistance and minimizes IT help desk calls to reset passwords.



Key security features of Carbonite Endpoint:

- Works as standalone encryption or in conjunction with full-disk encryption
- Lightweight with no performance impact
- 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)
- AES 256-bit encryption for data at rest

Carbonite Endpoint encryption

Carbonite Endpoint

Carbonite uses file- and folder-based encryption and takes it a step further. Our endpoint backup solution employs a secure, automated key management process for backing up and restoring data that allows encryption and deduplication to work together. With advanced transport layer security (TLS) for data in flight, Carbonite ensures that data remains encrypted at all times: at rest on the hard drive, in transit and during the global client-side deduplication process. Carbonite Endpoint brings all these security features together in a friction-free solution that results in easy deployment and enforcement, and fewer help desk requests.

Carbonite 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 the Carbonite Endpoint 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 policy.

Carbonite Endpoint can also delete files when a hacker tries to access the data by trying to crack the administrative passcode. With Carbonite, files remain protected if the user is using unprotected Wi-Fi networks. Anyone trying to access the laptop will not be able to open any files since they won't have the correct encryption keys.

Contact Us

Phone: 877-542-8637
Email: DataProtectionSales@carbonite.com