Carbonite Endpoint

Protect critical data on desktops, laptops and tablets

Conversation starters

Protect against ransomware, accidental deletions and lost or stolen devices.

Provide easy-to-use solutions for a mobile workforce

Easy add-on sale in an underserved market

Protect your accounts from competitors

Endpoints are vulnerable

Imagine a CFO is using their laptop on a flight, and they decide to slip the device into the seat's back pocket during the flight. Later, the plane lands and the CFO heads for home, forgetting the device on the plane. Do your customers have a way to restore critical data on that missing device? Could you prevent that data from falling into the wrong hands?

Frequent endpoint upgrades

New laptops come with an operating system pre-installed, but how do you transfer application data and system preferences? The Carbonite endpoint solution can help. You can deploy a new endpoint device and migrate the entire operating system, including system preferences, with a few simple steps.

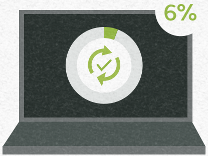
Endpoint vulnerabilties

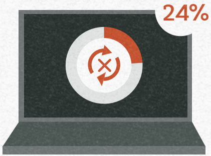
Loss or theft

According to the Ponemon Institute, over 600,000 laptops are lost or stolen at US airports each year.

User mistakes

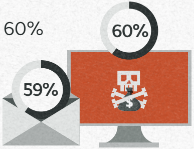
According to a 2018 Harris Poll, only 6% of laptops are backed up on a daily basis and 24% have never been backed up.





Ransomware

According to Osterman Research, 60% of attacks impact endpoint data, and 59% of cyberattacks start via an email link or attachment.



Mobility

Endpoints are harder to protect than servers. They are easily lost and stolen because they are mobile. Plus they can be turned off, put to sleep, and disconnected from the Internet. Effective endpoint protection requires intelligent use of available bandwidth and sensitivity to how the laptop is being used when the backup starts to execute, so user productivity is not impacted.

Carbonite is built on four pillars:

Power, Simplicity, Value and Security.

- 250+ petabytes of data under Carbonite management
- 24,000+ global partners, VARs and MSPs
- 435K customers with 90%+ customer satisfaction

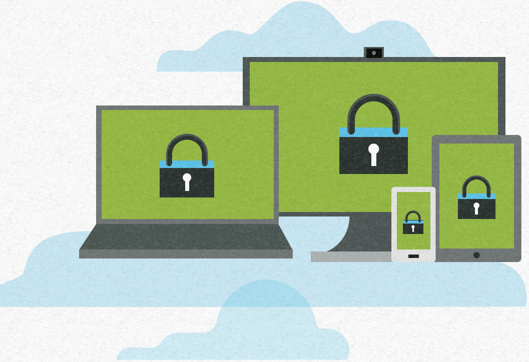
Carbonite data protection solutions deliver strategic value to businesses and provide peace of mind for IT pros faced with increasing threats to their organizational data.

Carbonite Endpoint is a cloud-hosted solution that provides a simple client installation and lessens IT burden.

Unique features:

- **Simple deployment –** Automated, silent, centralized installation and operation securely over public and private networks
- **Client-side global deduplication –** Reduces backup-related WAN traffic by up to 98% during business hours
- **Policy-controlled backups –** As often as every minute
- **Advanced admin control –** Legal hold visible to administrators only and admin-driven restore functionality
- **Secure protection –** 256-bit AES encryption in motion and at rest, and mitigation features like global location tracking, remote data wipe and poison pill
- **Incremental Restore –** Only recovers new or changed files. Ideal for recovering from ransomware and device migration

Key talking points for Carbonite Endpoint



Carbonite Endpoint: Easy-to-use, efficient, secure

Automatic backup to centralized repository

Many customers will tell you they are “doing nothing” when it comes to endpoint protection. This means users devise their own schemes, which scatter data outside their designated protection storage.

Carbonite centralizes endpoint protection storage to a single cloud repository.

Lower networking impact

Backing up many laptops at the same time can flood the network. Solutions need to automatically load balance, deduplicate, and offload backups to a local cache. Efficiency also enables more frequent backups – as often as every minute.

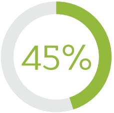
Carbonite automatically prioritizes and load balances endpoint backups, easily manages thousands of endpoints and accelerates backup and recovery.

Secure

Business and enterprise class endpoint protection solutions must be secure. And security is more than encryption. Organizations require Active Directory/LDAP integration, location tracking with remote wipe, enterprise key management, and client-side deduplication.

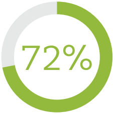
Carbonite Endpoint provides tight integration with AD/LDAP, location tracking and remote wipe. Unlike some other solutions, its deduplication works on encrypted data.

Endpoint Protection: numbers that matter



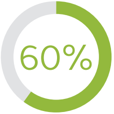
of business data is on devices that organizations can’t control.

Gartner



of employees use unauthorized free file-sharing services.

Workshare



of ransomware attacks impact endpoint data.

Osterman Research

How are you protecting endpoints today?

“File Sync and Share (FSS) is our backup”

File sync and share is not backup. It does not provide an immutable copy. Restoring from previous versions is a manual task.

“We leave it to users”

Since 30% of data on endpoints is unique to that endpoint, if a user leaves with their laptop or deletes their data, the organization loses that data.

“We rely on file history/Time Machine”

Because there is no image-level protection, files need to be individually found and restored. There is no centralized data protection repository.

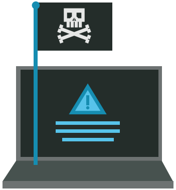
“We’re not doing anything”

Most organizations assume that implementing an endpoint backup strategy is difficult and time consuming. Carbonite Endpoint makes it easy with silent deployment, centralized admin console, admin restore and self-service recovery.

Discovery questions

What will you do if a laptop is lost or stolen?

According to Gartner Inc., a laptop is stolen every 53 seconds. Organizations need to make sure that the stolen laptop isn't used to access corporate data. Carbonite Endpoint provides global tracking, remote wipe and poison pill.



Do you have a ransomware recovery plan for endpoints?

Most organizations focus on recovering their servers from a ransomware attack, but endpoints are on the front lines and have the biggest risk of being infected. According to Osterman Research, 60% of ransomware attacks impact endpoint data. Carbonite Endpoint can back up laptops as frequently as every minute and our incremental recovery feature is an ideal way to recover from a ransomware attack.

Are you doing nothing because you feel it is too difficult?

The thought of protecting 50, 100 or 1,000 laptops can be daunting, but Carbonite's silent installation and operation make it easy. It gives IT the ability to set global data protection policies. There is no on-premises hardware requirement, so no space has to be made in the data center.

How does File Sync and Share, when used alone, fall short?

- Lacks automation, requires manual recovery
- No IT oversight
- No organization-wide data capture
- Unable to do a complete system restore, including user profiles
- Limited search for specific file versions
- Weak or no remote wipe
- No legal hold

Why you need both File Sync and Share and endpoint backup

No recovery from data corruption

If data is corrupted, that corrupted file is instantly synced and shared with all devices. In some cases, FSS has a versioning feature that allows you to recover an uncorrupted version, but each file must be discovered and copied manually.

Ransomware is a good example of how large numbers of files can be corrupted. Recovering clean files from FSS after a ransomware infection can be very time consuming.

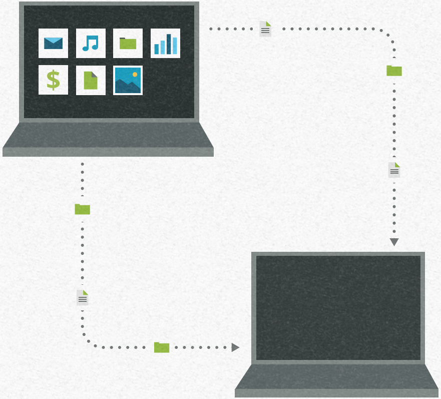
No centralized data capture

If users select their own FSS services, business data is being stored without IT oversight. If they leave the organization and delete their data, it may never be recovered.

No full system recovery

In the event of a hardware failure or system loss, file sync and share will not restore system state, user settings or applications.

How will you migrate data to new laptops?



Steps to configure new laptops:

1. Connect laptop to network
2. Install organizational software like security, VPN, etc.
3. Install applications
4. Configure organizational preferences
5. Configure user custom preferences
6. Have user log in to system
7. Restore user data. If FSS then user must be present to authenticate to their FSS account

Four simple steps to Carbonite Endpoint:

1. Connect laptop to network
2. Install Carbonite client on laptop
3. Trigger restore from administration console
4. Reboot laptop and send to user

Requirements for preventing data loss

- Centralized backup storage
- Incremental backup and recovery of endpoint data
- Automated backup
- Remote management and silent deployment
- Endpoint backup as frequent as every minute
- Advanced security features

How to prevent endpoint data loss with Carbonite Endpoint

Carbonite Endpoint recovers data types ranging from a single file to a full directory or an entire laptop.

Carbonite Endpoint reduces the risk of human error by automatically and transparently backing up user devices. Our agent is so lightweight the user won’t even notice the backup is occurring.

Carbonite Endpoint makes it easy to deploy the software across dozens, hundreds and even thousands of endpoints with our silent deployment technology.

Carbonite Endpoint’s flexible policy controls enable IT admins to control how often users and groups are backed up.

Carbonite Endpoint advanced security features provide device tracking, remote wipe and legal hold.

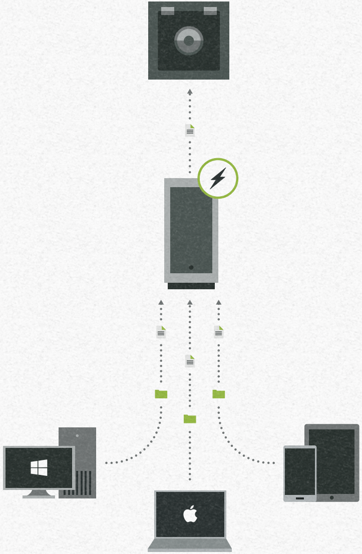
How to deploy Carbonite Endpoint

STEP 1 Establish a centrally managed vault in Carbonite's Microsoft Azure-hosted vault.

STEP 2 Silently deploy Carbonite software on computers, laptops and tablets.

STEP 3 Back up distributed devices using the local cache or directly to the vault.

STEP 4 Recover or remotely wipe data if a device is lost or stolen.



Carbonite operates a control framework based on adherence to SOC 2 Type 2 standards.

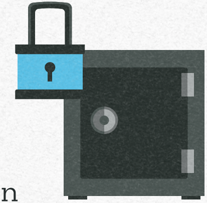
Carbonite Endpoint supports compliance with several industry-standard regulations, including:

HIPAA

FERPA

GLBA

Additionally, Carbonite adheres to PCI-compliant processes for customer payment transactions.



Security, privacy and comprehensive protection

Carbonite takes many steps to safeguard the integrity of data and prevent unauthorized access to information maintained on behalf of customers.

These protections cover information security and privacy, including governance, infrastructure, physical security, data handling and operations.

As part of Carbonite’s continuing commitment to risk management, controls such as authentication, monitoring, auditing and encryption are built into the design, implementation and day-to-day practices of our operating environment.

These measures are designed to avoid corruption or loss of data, prevent unknown or unauthorized access to systems and information, and above all, to comprehensively protect the critical data customers entrust to us.

Case Study: Diamond Foods

“If we lose important data on employee laptops, it has a direct impact on our bottom line.”

– **Kentrell Davis**, Senior Client Support Services Analyst at Diamond Foods.

Like most other companies, Diamond Foods’ critical files and folders don’t just live on servers – they live on endpoints. The company installed Carbonite Endpoint on 350 employee endpoints.

Davis relies on point-in-time restore to not only recover from accidental deletions but also to protect against employee turnover. “It also helps us maintain our institutional knowledge when employees leave,” he said. “We archive everyone’s endpoint data to ensure employee turnover doesn’t impact our business continuity.”

CARBONITE®

an opentext™ company

carbonite.com