CARBONITE
an opentext company

BUYER'S GUIDE:
ENDPOINT PROTECTION

Key features to look for in an endpoint backup solution

Comprehensive Protection

Endpoint users generate a high volume of sensitive company data. Protecting it is a top strategic objective for IT. An essential part of data protection strategy includes flexible recovery options that allow IT administrators to maintain user productivity without draining help desk resources. That's why businesses need a purpose-built backup solution. Today, top-performing endpoint protection combines robust backup and recovery capabilities, for both devices and cloud platforms, with additional security features – like legal hold and remote wipe – that allow businesses to better control the large volume of data their users generate.

Consider how many identical copies of the same file are shared throughout an organization. When duplicate data lands in storage, it needs to be deduplicated to avoid storage bloat. But since the data lands in an encrypted state, deduplicating it can potentially leave data vulnerable. For businesses in regulated industries, this is a dealbreaker.

This guide focuses on how to identify, evaluate and implement endpoint backup that delivers on the top objectives for today's IT professionals.

Endpoint protection myths

Myth: My endpoint data is secure because I have anti-virus software.

Fact: Anti-virus is essential for detecting known virus signatures, but cybercriminals use evasive tactics that help them circumvent anti-virus software. Carbonite helps you get clean files back if and when an advanced threat penetrates your perimeter defense.

Myth: Online storage is an effective substitute for computer backup.

Fact: Online storage is a consumer product that is not engineered with the complete feature set businesses need to protect their data.

What to look for in endpoint protection

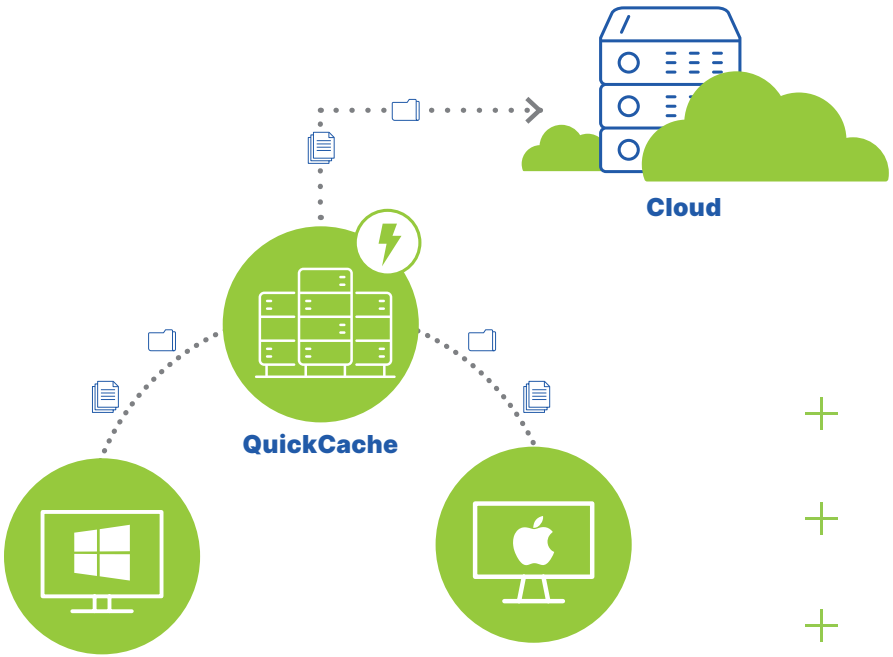
What	Why
Flexible deployment	Host your data anywhere. Know your organization's requirements for on-premise vs. cloud and data sovereignty needs.
Customizable implementation	Protect all endpoints globally. Look for backup that allows you to use existing IT tools and tailor your implementation specifically to your needs.
Device track/remote wipe	Keep company data out of the hands of cyber criminals and hackers. Locate employees and devices during emergencies.
Central management	Manage endpoint protection from a single pane of glass, set and manage policies, execute restores, check backup health and status, and set alerts.
Global deduplication	Reduce backup-related WAN traffic and backup sizes. Shrink storage by eliminating redundant data.
Legal hold	Lock backups so relevant files cannot be deleted. Look for a solution that silently implements this control and continues backing up in this state.
Administrative restore	Perform file recovery remotely so users can continue to access important files and data.
Self restore	Reduce help desk tickets by giving users the ability to perform simple file and folder recovery.

Buying tips

Businesses have a wide range of needs when it comes to protecting endpoints. Regulatory considerations demand high levels of security with no compromises, but deploying and enforcing policies for highly mobile devices makes the task of managing protection increasingly complex. Carbonite solves many of these issues through the use of advanced security features to encrypt, track and secure data at every step in the process so data never exists in an unencrypted state.

The Carbonite advantage

Carbonite® Endpoint offers advanced endpoint security for distributed workforces. Silent deployment, global deduplication and flexible deployment options help protect against data loss without user disruption or bandwidth strain.



Features and Benefits

Key features and benefits:

- Policy-controlled backups that don't interfere with end-user productivity
- Flexible deployment options—back up to our cloud, the public cloud or onsite
- Quick, silent and centralized deployment and management
- Centralized admin restore capabilities and flexible self-service options for end users
- Powerful global deduplication of AES 256-bit encrypted data
- Optional local cache to minimize bandwidth consumption across distributed networks
- Global location tracking, remote wipe (remove data on command) and poison pill (remove data after specified off-line time)

To learn how Carbonite® Endpoint can help safeguard your company and your workforce from data loss and ransomware, start a free, 30-day trial today.

Contact us to learn more

Data Protection Sales

Phone: +1 (877) 542-8637
Email: DataProtectionSales@carbonite.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.

CARBONITE
an opentext company