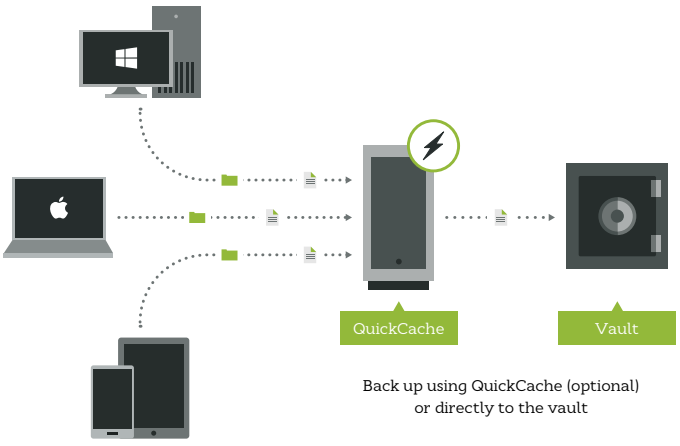
# Carbonite Endpoint Protection

## Protect your distributed workforce with enterprise-grade backup and archiving

Businesses looking to protect valuable data on laptops and other devices need to consider how widely distributed data has become thanks to greater workforce mobility. Protecting data from human error, malware and theft becomes more complicated when protection is spread across wide geographic distances and complex network topologies.

Carbonite Endpoint Protection is a hybrid cloud solution for endpoint backup and archiving that allows IT to mitigate data loss and data breach at the frontiers while maximizing network and end user performance.




### Flexible deployment

Our endpoint protection is engineered with central management and control features that simplify deployment while minimizing disruptions due to bandwidth restrictions or geographic dispersion of networks.

- **Maximum deployment flexibility**: Deploy Carbonite Endpoint Protection in the public cloud, a private cloud, on-premises in your own data center or a combination of all three.
- **Best-in-class public cloud options**: Take advantage of our relationships with Microsoft to deploy best-in-class enterprise public or private clouds.
- **Centralized management**: Centrally manage and restore user data and prevent breaches with audit trails, monitoring and alerts.

### Overview

- Enterprise-grade endpoint backup and archiving for the mobile workforce
- Maximum deployment flexibility and scalability for large, distributed organizations
- Intelligent global usage of bandwidth for fewer disruptions to users and the network

### Key Capabilities

- Policy controlled backups that don't interfere with end user productivity
- Support for laptop, tablet and smartphone data protection
- Global location tracking
- PC settings migration
- Secure, remote data access from any device, anywhere, anytime
- Quick, silent and centralized deployment & management
- Remote wipe and poison pill

# Carbonite Endpoint Protection

- **Extend to meet specific needs**: Customize the solution to meet your unique needs using the Carbonite Endpoint Protection API—including batch restores.

## Mitigate data loss and data breach

Carbonite Endpoint Protection protects mobile devices and data from internal and external threats while addressing regulatory requirements and the consequences of lost or stolen laptops and tablets.

- **Data encryption**: Data is encrypted before it leaves the device using 256-bit AES encryption at rest and Transport Layer Security (TLS/SSL).
- **Enterprise Key Controller**: Provides an extra layer of security and control for companies using the public cloud or a third party data center.
- **Secure data centers**: Deploy in state-of-the-art data centers that are SAS 70 Type II, SSAE 16 audited and ISO 27001 certified.
- **Data wipe**: Data can be wiped remotely with time-based policy triggers or on-demand when a device is lost or stolen.
- **Prepare for litigation**: Easily comply with legal hold requirements when facing litigation.

## Supported platforms

**Carbonite Endpoint Protection client**

- Windows 10, 8, 7
- Mac OS X 10.5 and later
- iOS 8 and later
- Android 4.1 and later

**Carbonite Endpoint Protection vault**

- Microsoft Azure
- Windows Server 2016, 2012 R2, 2008 R2
- SQL Server 2016, 2014, 2012, 2008 R2, 2008

## Maximize network and end user performance

Only Carbonite gives your organization the tools you need to manage global bandwidth usage intelligently so there's no disruption to network performance.

**Proven scale**: Leverage our proven scale to support employees in ROBO offices without adding headcount.

**Storage efficiency**: Save on storage without sacrificing security—even in a multi-tenant environment—with powerful global deduplication technology.

**QuickCache**: Use QuickCache to reduce or eliminate bandwidth consumption and accelerate time-to-protection. QuickCache is simple to install and centrally managed.

**Local cache**: Provide faster data restores and improve network traffic efficiency further by backing up encrypted data to a device's local cache. This means data can be restored without having to travel across your organization's WAN or LAN.

**Roamsmart**: Detect the user's network and turn off backup if their device is connected to an LTE, 4G or 3G mobile network to create a cost-effective and friction-free experience for employees.

## Contact us to learn more

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