

Cyber Resilience

From the Edge to the Cloud

Promoting Cyber Resilience with End-to-End Protection and Data Security

With advanced security for computers, servers, and other endpoint devices, plus backup and recovery services, your days worrying about losing mission-critical data are over.

Powerful protection. Easy recovery. That's how Carbonite and Webroot empower cyber resilient businesses to be fearless in the face of cybercrime and data loss. Together, these solutions ensure businesses remain up and running, no matter what comes their way.

The Carbonite & Webroot Portfolio

Carbonite[®] Endpoint

Carbonite Endpoint is a comprehensive, automatic backup solution for all your endpoint devices and the data that resides on them. Carbonite Endpoint simplifies the administrative tasks associated with deploying protection across an entire organization, no matter the size, distribution, or sophistication of the environment.

With Carbonite[®] Endpoint, organizations can better protect valuable data on employee devices, mitigate data loss and data breaches, and restore lost data quickly. It gives businesses an enhanced data resilience strategy through best-in-class protection to reduce risk from ransomware, user errors, and lost or stolen devices.

Carbonite[®] Backup for Microsoft[®] 365

Carbonite Backup for Microsoft 365 offers comprehensive backup of all Microsoft 365 applications to ensure data protection and, if needed, recovery. Centralized management allows you to create granular policies for what should be protected, as well as run backups up to four times per day, with flexible retention options.

You'll be able to restore granular data, including mailboxes, conversations, projects and more, as well as perform site-level rollback to easily restore lost data. This cloud-to-cloud backup solution helps businesses deploy the same robust data protection for cloud apps as they do for physical, on-premises devices and data.

Carbonite[®] Server

All businesses need a straightforward, comprehensive backup and recovery solution that keeps data secure, minimizes downtime and protects company operations. Carbonite Server is a reliable, all-in-one, server backup and recovery solution for physical, virtual and legacy systems. Advanced features include:



Carbonite and Webroot are creating the most comprehensive online security offering available anywhere. Together, we have the ability to fight cybercrime and protect users from the loss of priceless data.

We're committed to becoming your one-stop shop for business cyber resilience through cybersecurity, data protection and recovery. Our current offerings include:

- Carbonite[®] Server
- Carbonite[®] Endpoint
- Carbonite[®] Backup for Microsoft[®] 365
- Carbonite[®] Migrate
- Carbonite[®] Recover
- Carbonite[®] Availability
- Carbonite Safe[®]
- Webroot[®] Business Endpoint Protection
- Webroot[®] DNS Protection
- Webroot[®] Security Awareness Training
- Webroot BrightCloud[®] Threat Intelligence Services

- Secure local and cloud backup with optional hardware, all from one vendor
- Cloud failover with push-button failback for critical systems
- Granular recovery (files, folders, Exchange, SharePoint, SQL, Active Directory, Oracle DB)
- Forever incremental backups with flexible retention options—up to seven years

Carbonite® Migrate

Carbonite Migrate quickly and easily migrates physical, virtual and cloud workloads with minimal risk and near-zero downtime. The streamlined process automates and consolidates numerous steps into just a few simple tasks, reducing the amount of work necessary to reach your migration goals. Features include:

- Structured, repeatable migration with near-zero downtime
- Highly automated process that eliminates common risks and streamlines migrations
- Freedom from lock-in to a specific cloud, hypervisor or piece of hardware

Carbonite® Recover

Carbonite Recover is a DRaaS offering that securely replicates critical systems from a primary environment to the Carbonite cloud. This ensures an up-to-date secondary copy is available for failover at any moment, minimizing downtime as well as costs. Features include:

- Recovery times measured in minutes and recovery points in seconds, reducing the risks of lost productivity and revenue
- Continuous, real-time replication for always-on data protection
- Non-disruptive, self-service testing
- Bandwidth-optimized for limited network impact

Carbonite® Availability

Carbonite Availability enables organizations to maintain the highest availability of their Windows® and Linux servers by preventing downtime and data loss. Continuous, byte-level replication maintains a secondary copy without taxing the primary system or network bandwidth. Advanced features include:

- Continuous replication that minimizes data loss
- Incredibly fast failovers that minimize downtime
- Platform support for physical, virtual and cloud-based systems
- Automatic failover triggered by threshold monitors

Carbonite Safe®

Automatically back up computers and servers to the cloud with options to protect files locally for faster recovery. Carbonite Safe is designed to scale from consumers and home offices to small businesses with one or more servers.

Webroot® BrightCloud Threat Intelligence

The Webroot® Platform is the architecture that informs every layer of our solutions for consumers and businesses, as well as our BrightCloud® Threat Intelligence Services for technology partners, which include:

- Web Classification & Web Reputation
- IP Reputation
- Real-Time Anti-Phishing
- Mobile Security SDK
- File Reputation
- Streaming Malware Detection

Webroot® Business Endpoint Protection

The foundation of an advanced cyber resilience strategy is highly effective multi-vector protection and prevention. Cyber resilience starts by stopping the attacks aimed at endpoints and their users. Advanced, next-generation, and automated, Webroot Business Endpoint Protection:

- Stops malware, ransomware, known and unknown infections
- Protects against file-based and fileless scripts, APTs, exploits, and evasive attacks
- Stops phishing and users identity and credential theft
- Automatically remediates and returns local endpoint drives to pre-infected state without reimaging

Webroot® DNS Protection

Every business uses the internet, and every internet connection uses DNS. Unless you privately and securely filter all DNS requests, your business is at risk. The next layer of a comprehensive cyber resilience strategy must be domain layer security that can provide both privacy and security by supporting DNS over HTTPS (DoH). Webroot DNS Protection:

- Automatically filters DNS and DoH requests to malicious and dangerous domains, blocking 88% of known malware before it can hit your network or endpoints*
- Provides private DNS resolvers in Google Cloud™ to stop internet usage request surveillance by bad actors, or those mining data for profit
- Provides network, IP address, and user policy management over bandwidth and unproductive or non-compliant internet access, using 80 URL categories
- Uses the most timely, accurate and reliable DNS filtering intelligence backed by the Webroot BrightCloud® Web Classification Service

Webroot® Security Awareness Training

When users unwittingly divulge sensitive information, or click on the wrong link, criminals can bypass layers of security and successfully breach networks. That's why cyber resilience demands cyber-awareness. Highly automated Webroot Security Awareness Training delivers measurable results with the minimum of effort through:

- Continuous education programs that combine micro-learning, phishing simulations with effectiveness measurement and executive reporting
- Specialty compliance courses for PCI, HIPAA, GDPR and more
- Courseware and phishing templates that are continuously updated so they're relevant and effective at educating users and modifying behaviors
- Proven effectiveness at reducing click rates and minimizing security incidents

Next Steps

For more information about Carbonite and Webroot products, visit [webroot.com](https://www.webroot.com) and [carbonite.com](https://www.carbonite.com).

Contact us to learn more – Carbonite US

Phone: 877-542-8637

Email: carb-data_protection_sales@opentext.com

Contact us to learn more – Webroot US

Email: wr-enterprise@opentext.com

Phone: +1 800 772 9383

* Based on Webroot's internal testing and threats identified by Webroot after scanning real-world network traffic.

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](https://www.carbonite.com) and [webroot.com](https://www.webroot.com).