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 Backup

Carbonite Endpoint Backup is a comprehensive, automatic backup solution for all your endpoint devices and the data that resides on them. It 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 Backup, 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® Server Backup

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

- 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:

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 onestop shop for business cyber resilience through cybersecurity, data protection and recovery. Our current offerings include:

- Carbonite® Endpoint Backup
- Carbonite® Server Backup
- Carbonite® Migrate
- Carbonite® Recover
- Carbonite® Availability
- Carbonite™ Cloud-to-Cloud Backup
- Carbonite™ Information Archiving
- Webroot® Business Endpoint Protection
- Webroot® DNS Protection
- Webroot® Security Awareness Training
- Webroot™ Advanced Email Encryption powered by Zix™
- Webroot™ Email Message Privacy
- Webroot™ Email Continuity
- Webroot™ Email Threat Protection
- BrightCloud® Threat Intelligence Services

- 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 disaster recovery as a service (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™ Cloud-to-Cloud Backup

Carbonite™ Cloud-to-Cloud Backup offers comprehensive backup and recovery of SaaS applications and boasts central management, granular restore, rapid recovery and flexible retention options. Our purpose-built backup solution ensures IT administrators can recover as much or as little SaaS application data, as necessary.

- Automate backups of Microsoft 365, Google Workspace, Salesforce, Box and Dropbox
- Protect against ransomware, malware, data loss and data breach
- Flexibly search and recover items, mailboxes or sites at any granular level
- Easily recover data with point-in-time recovery
- Browse daily snapshots and run searches
- Feel more secure with full redundancy
- Store more with unlimited storage and retention

Carbonite™ Information Archiving

Information Archiving provides an easy-to-use, secure and unified information archive and eDiscovery service that simplifies management of historical email and electronic communication data. Carbonite Information Archiving helps you easily adapt and comply with changing regulations including HIPAA, FCC, FOIA, FDIC, SEC, PCI DSS, FINRA, GDPR, GoBD and more.

- Unlimited cloud-based storage and eDiscovery for over 50 different sources of communication
- SimplyShare technology that enables you to share datasets with third parties – without external hard drives or SFTP sites
- Flexible search capabilities such as proactive glossary scanning, data classification, message flagging, attachment OCR scanning and content indexing
- Time-based retention policies that can be applied to everyone, specific users or customizable groups
- Role-based access controls to enhance security

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

Webroot™ Advanced Email Encryption powered by Zix™

Advanced Email Encryption removes the hassle of encrypting email and gives teams the peace of mind that sensitive data sent via email is secure. Using advanced content filters, emails and attachments are scanned automatically and any message containing sensitive information is encrypted for delivery.

- Industry-specific policies detect information in email subject, body and attachments
- Help customers achieve governance, risk and compliance (GRC) best practices
- Policy-builder to select the right combination of filters for your customers' industry

Webroot™ Email Message Privacy

Webroot's Email Message Privacy makes it simple to send and receive secure messages, request, or provide legally valid electronic signatures and share large files up to 100 GB directly from a user's existing email address. It all happens with real-time message tracking and control.

- No infrastructure investment, simple integration into existing mailbox and other communication channels
- Avoid loss of productivity associated with recipient's inbox size restrictions
- Send multiple large files (up to 100 GB each) simultaneously
- Allows easy and secure message exchange and file sharing that meets compliance requirements
- Full tracking visibility and rights management of messages

Webroot™ Email Continuity

Webroot's Email Continuity is an integral part of our cyber resilience solutions and ensures continuous availability of company email for 30 days despite outages. This ensures positive end user experiences without embarrassing non-delivery notifications and maintains employee productivity.

- Works automatically – no additional hardware or software required
- Keeps organizational email accessible across all devices, despite outages
- Maintains productivity via failsafe protection for your email service
- Provides access to the last 30 days of inbound messages during an outage
- Prevents embarrassing non-delivery notifications to your customers
- Automatic inbox synchronization upon main email server or service restoration

Webroot™ Advanced Email Threat Protection

Webroot Advanced Email Threat Protection provides multi-layered filtering for both inbound and outbound emails that permits legitimate email while automatically blocking malicious threats such as phishing, ransomware, impersonation, BEC and spam-type messages.

- Attachment quarantine performs forensic analysis on attachments in a secure, cloud-based sandbox environment.
- Link protection rewrites links to safe versions and performs time-of-click analysis on the destination address.
- Message retraction (for Microsoft 365) enhances incident response with the ability to retract malicious emails already delivered to users' inboxes.
- 24/7/365 live threat analyst team constantly identifies new threats, updating the system and providing warnings.

BrightCloud® Threat Intelligence Services

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

CARBONITE® + WEBROOT®

Carbonite and Webroot, OpenText Security Solutions, 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.