CARBONITE®
an opentext™ company

WEBROOT®
an opentext™ company

Carbonite Data Protection & Cyber Resilience

All the tools necessary to protect any type of data

Data Protection

Data protection is a balancing act between the need to protect data and the need to protect access to data. The trick lies with deploying the right protection across the different systems and types of data. IT pros need confidence that the protection they deploy can:

- Restore business data quickly and reliably
- Store and transmit data securely
- Extend protection as environments change
- Provide long-term survivability of historical data

This ability to protect data and preserve access to it during adverse events is called cyber resilience. Carbonite backup, disaster recovery and high availability solutions help businesses of all sizes and in every industry improve the resilience of their systems. From simple, secure cloud backup and disaster recovery as a service (DRaaS) to high availability and non-disruptive migration, Carbonite offers all the tools necessary to deploy a comprehensive data resiliency strategy for any type of data, on any system, across any distance.

Destination resilience

With the rapid pace of technology innovation today, it's common for data to be spread across a range of physical, virtual and cloud platforms, and across wider geographic distances. This heightens the need for aligning protection with urgency. By aligning data protection with urgency, businesses can ensure predetermined service levels for all types of data, eliminate unnecessary demands on internal resources, and maintain business agility, all at a lower total cost of ownership than with traditional solutions.

Determining factors

Several factors will determine the appropriate type of protection, including the nature of the system, the purpose of protection, and the procedures and technology available to achieve desired outcomes.

The nature of the source is a strong indicator for the type of protection it requires. A system that acts as a repository will require a lower level of protection than, say, a server hosting active, critical applications and data.

When determining protection, the ultimate decision comes down to outcomes. Starting with outcomes, IT decision makers can easily eliminate solutions lacking the minimum feature set.

Specific outcomes businesses seek to control include:

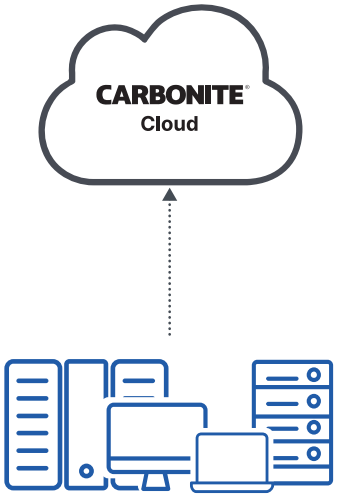
- System uptime
- Recovery speed
- Data survivability
- Document retention
- Discoverability
- Non-disruptive migration

Procedures and technology are additional factors. Rate of change and bandwidth will determine the need for periodic or real-time replication, or a blended approach that analysts now recommend.1 Geographic distribution of networks—combined with mixed physical, virtual and cloud deployments—also serve to increase complexity and demand for resources.

Destination resilience

Store

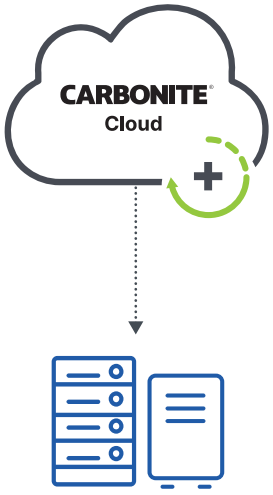
Backup of all data for servers and endpoints



Carbonite® Server
Carbonite® Endpoint
Carbonite® Backup for Microsoft 365

Restore

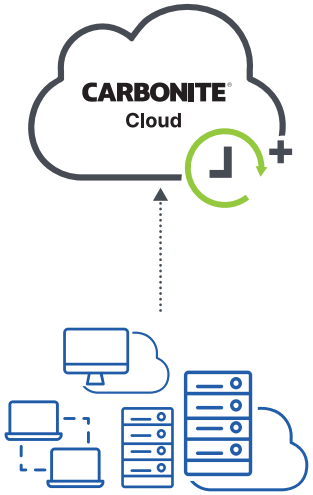
Local failover for servers and systems



Carbonite® Server
Carbonite® Endpoint
Carbonite® Backup for Microsoft 365

Rapid restore

Always-on access to critical systems that cannot afford downtime



Carbonite® Recover
Carbonite® Migrate
Carbonite® Availability

Data-defined protection

Data-defined protection isn't new. Historically, the lack of automated tools left the provisioning of protection subject to the clout of individual stakeholders. Today, traditional criteria for determining protection—such as business size or total data footprint—are less critical with today's scalable cloud infrastructure. The practices and procedures for data protection have evolved alongside mobile and cloud platforms. Businesses now have a complete spectrum of solutions to address critical needs for all types of data in any organization.

Information governance

Federal and industry regulations impose requirements for handling data that businesses must satisfy or risk compliance and certification. Requirements for record retention, email archiving and discoverability fall under the label of information governance. Traditional solutions were expensive, labor-intensive and prone to failure. Today, technology exists for ensuring the long-term survivability of semi-active or inactive data while reducing costs and improving the performance of more critical areas of protection. The ideal solution for archiving and document retention is one that automates backup to a secure target using low-cost, scalable storage.

Disaster recovery

Data loss becomes increasingly costly as organizations depend more on data to pursue strategic objectives. As organizations grow, so does the amount of data they generate. Modern infrastructures are more complex than those from just a few years ago. Today's environments support a wider range of operating systems, applications, physical servers, virtualized workloads and multi-cloud deployments, with networks extending beyond the central office. At the same time, risks are more pervasive. Malware and ransomware infections are on the rise, and businesses are increasingly targeted due to the value and sensitive nature of data. Backup is essential to mitigate these threats.

In a data-defined protection strategy, deployment aligns with predetermined objectives based-on the urgency of each system under protection. This affects scheduling, retention and the provisioning of onsite, offsite or hybrid protection. By protecting data at an offsite location in a separate FEMA zone from the source, organizations can ensure access to critical data if there's a disruption at the main location.

Service vs. purchase

Disaster recovery as a service (DRaaS) is an increasingly common option. With DRaaS, a third party provides a remotely hosted environment that mirrors production in real time. If there's an interruption at the source, the replica can be made available through either self-service or managed failover. All infrastructure and maintenance are the responsibility of the provider. Technology analysts predict the share of businesses using DRaaS will grow for small, medium and large organizations as the economics of the cloud continue to drive greater cost savings and scalability.

Whether an organization uses a traditional backup approach or DRaaS, any solution designed for recovery should provide simple procedures for restoring files, folders and full systems in the event of human error, hardware failures, malware and natural disasters. If a user becomes infected with a ransomware virus, an IT admin should be able to revert to an earlier, non-corrupt version without being forced to pay a ransom to cyber-criminals.

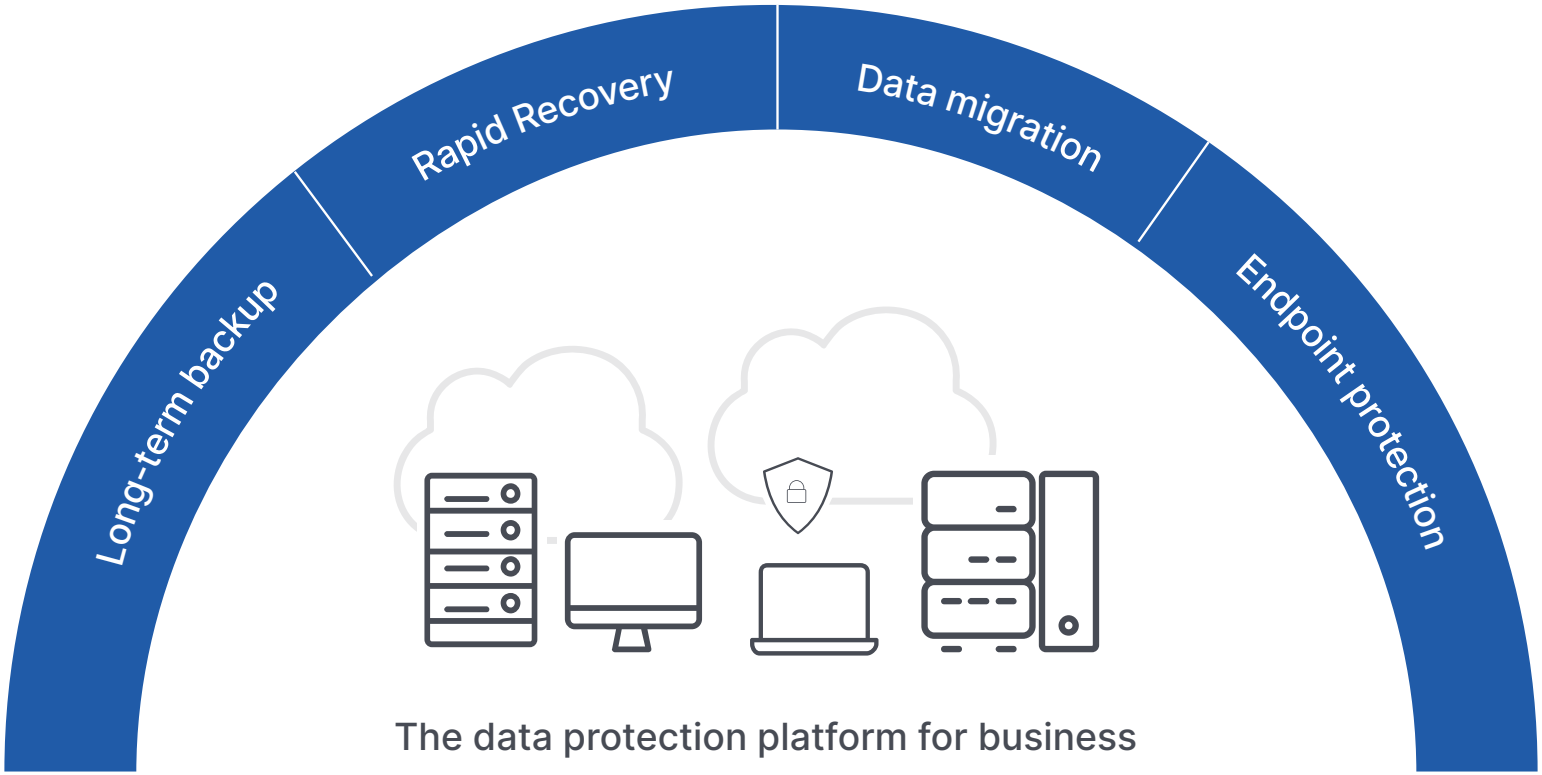
User productivity

Today's markets are highly competitive, mobile and global. To stay productive, users need always-on access to critical data. A lost or stolen laptop, coffee spill or server outage can be extremely costly for data-dependent organizations. IT departments need tools for protecting laptop and mobile data from common forms of data loss. And they need failover capabilities for when

a server or database experiences an outage. Data protection should offer businesses advanced feature sets for ensuring always-on access to critical data, servers and applications for any type of disruptive event. Today, system complexity and the mobile nature of the workforce necessitate a wide range of configuration options, including ground-to-cloud, cloud-to-ground, cloud-to cloud, one-to-many and many-to-one, to name a few.

Carbonite cyber resilience

The Carbonite Data Protection Platform delivers backup, high availability, DRaaS and data migration for all types of data, including heterogeneous environments and dispersed networks. Carbonite allows organizations to implement the right level of protection for each system in their network. All Carbonite solutions include complete documentation, online access to a user community and knowledge base, and award-winning global customer support from certified experts.



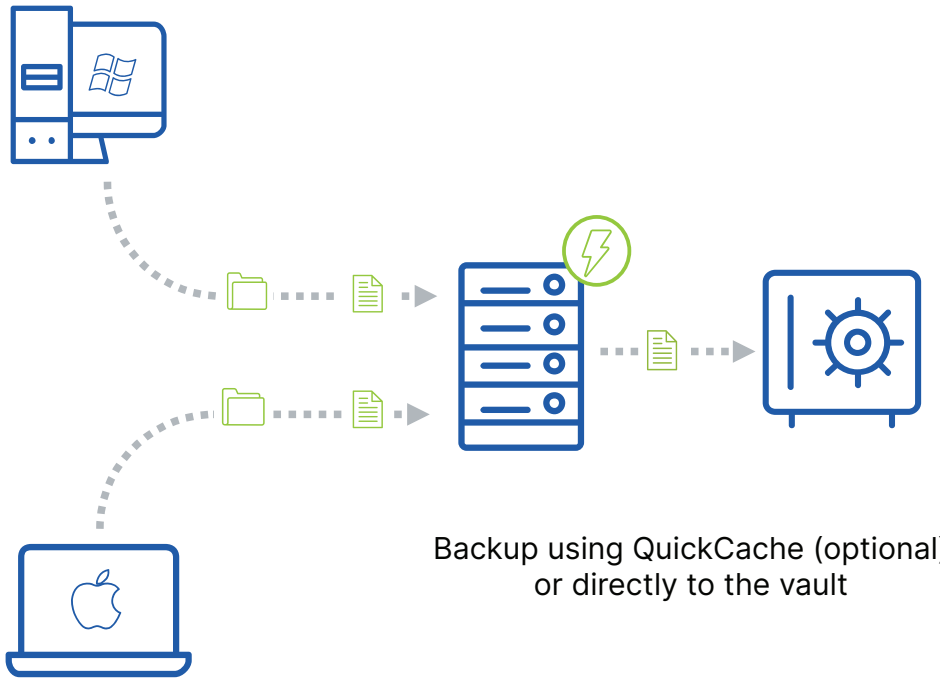
Carbonite cyber resilience

Carbonite® Endpoint

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.

Key features:

- 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, centralized deployment and management
- Centralized admin restore capabilities and flexible self-service options for end users
- Optional local cache to manage bandwidth consumption across distributed networks
- Global location tracking, remote wipe (remove data on command) and poison pill (remove data after specified off-line time)
- Powerful global deduplication of AES 256-bit encrypted data



Backup using QuickCache (optional) or directly to the vault

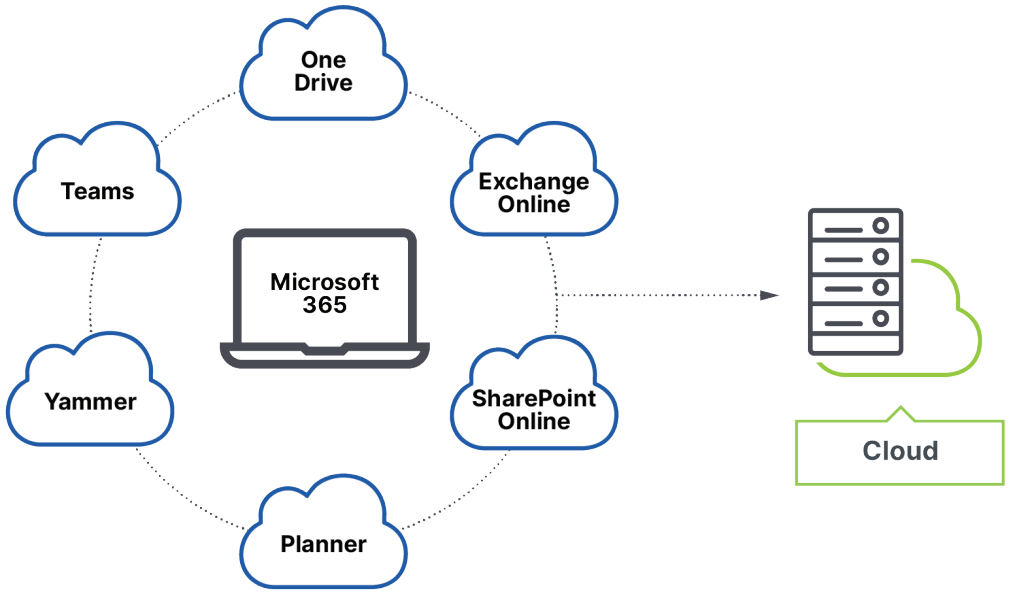
Carbonite cyber resilience

Carbonite® Backup for Microsoft 365

Carbonite Backup for Microsoft 365 is a comprehensive cloud backup solution that provides protection for Microsoft 365 data and applications. This complete solution helps protect against accidental deletions, overwriting, ransomware and other threats that Microsoft's backup and retention policies don't cover.

Key features:

- Protect the entire Microsoft 365 suite from large disasters and everyday data loss events
- Policy-controlled backups up to four times daily with flexible retention options
- Restore granular data, including mailboxes. conversations, projects and more
- Centralized control of backup data with audit trails, monitoring and alerts
- 24×7 service from Carbonite's tech support team



Carbonite cyber resilience

Carbonite® Server

Carbonite Server is a powerful solution that satisfies the need to protect the three types of data that comprise a multi-tier protection strategy: historical, semi-active and mission-critical. It also satisfies the need to protect data in two places: onsite and offsite. Onsite backup enables LAN-speed recovery of critical data, while offsite backup ensures a secondary copy persists in the event of a local failure, regional outage or natural disaster. Flexible options allow you to deploy the right level of protection for any type of data.

Key features:

- Protect heterogeneous networks with a single solution
- Centralize protection for distributed environments
- Accelerate recovery time performance
- System image and granular recovery options
- Optional failover to a local appliance for critical systems
- Advanced 256-bit private key encryption
- Dissimilar hardware restore
- Central management via browser-based portal

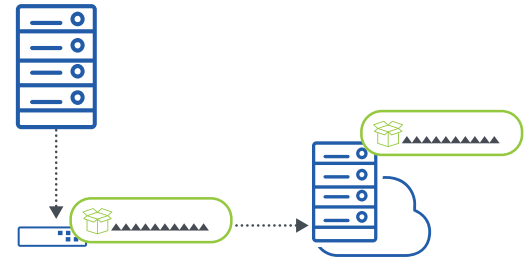
Carbonite Server is available as a software-only solution or as hardware with subscription pricing for reducing or eliminating capital expenditure (capex).

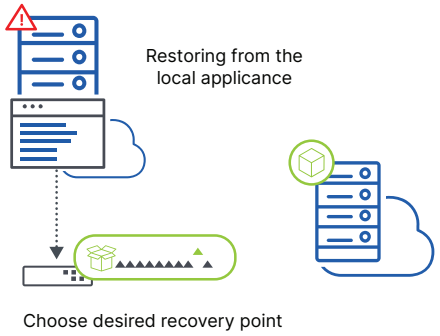
Carbonite® Server Rapid VM Restore

Carbonite Server is also available with simple point-and-click rapid VM recovery, which helps get mission-critical servers back in minutes.

Key features:

- Restore virtual machines (VM) to a vSphere host in your configured vCenter within minutes
- Migrate the VM to a permanent datastore anytime using the Portal
- Start a rapid VM recovery from the portal in a few clicks
- Migrate the VM back to production if desired
- The migrated VM keeps the old UUID so reseeds are not needed





Carbonite cyber resilience

Carbonite® Migrate

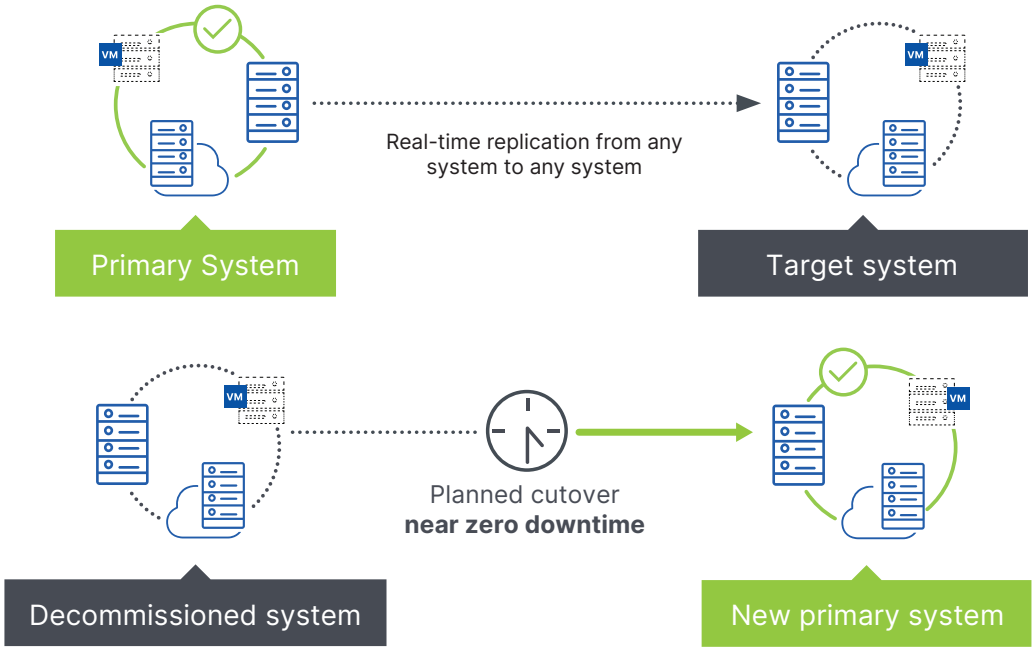
Carbonite® Migrate quickly and easily migrates physical, virtual and cloud workloads over any distance with minimal risk and near-zero downtime. The streamlined process automates and consolidates numerous manual and error-prone steps into just a few simple tasks, reducing the amount of work you need to do to reach your migration goals. Test cutovers can be performed anytime without impacting production systems.

Key features:

- 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

Target environments include:

- VMware vSphere
- VMware vCloud Director
- Amazon Web Services
- Microsoft Azure Classic
- Microsoft Azure Resource Manager
- Google Cloud



Carbonite cyber resilience

Carbonite® Recover

Carbonite Recover is a DRaaS offering that securely replicates critical systems from your primary environment to the cloud, ensuring that an up-to-date secondary copy is available for failover at any moment, minimizing downtime as well as costs. There's no need for a secondary data center. Carbonite handles all infrastructure and maintenance.

With Carbonite Recover, replication from the primary server to the cloud happens continuously at the byte level. The replica at the secondary cloud location is constantly synchronizing with the source, ensuring data stays current.

Key features:

- Recovery times and recovery points measured in minutes or seconds
- Orchestration for multi-tier applications, with boot order, scripting and automated discovery of systems in your environment
- Non-disruptive, self-service testing
- Bandwidth-optimized for limited network impact
- Built-in encryption, both at rest and in flight
- Broad platform support, including legacy systems such as iSeries and AIX

Carbonite® Availability

Carbonite Availability provides always-on protection for critical, time-sensitive data and applications. It creates a perfectly mirrored secondary copy that assumes responsibility for server workloads the moment there's a disruption to the primary source.

Key features:

- Replicate any source data to any secondary target in real time
- Perform automatic or triggered failover with virtually no disruption in service
- Execute tests with live data to ensure cross-dependent functionality
- Simplify administrative tasks and eliminate disaster recovery fire drills

Deployment

Businesses have more options than ever for blending data protection to form a holistic strategy:

- **Backup**

  Deploy across all systems for information governance and rapid recovery for both small-scale data loss and extreme adverse events.

- **High availability**

  Deploy for critical, time-sensitive systems requiring continuous or near-continuous operation.

- **DRaaS**

  Leverage our experts and infrastructure to keep a replica of critical systems on standby if there's ever an interruption at the source.

- **Data migration**

  Deploy for hardware or platform upgrades, software patches and for changing vendors.

Backup

Simply put, backup is the act of copying data so it can be restored if it is lost or corrupted. Modern server backup solutions take snapshots at periodic intervals, protecting them according to a set retention schedule. This allows businesses to perform rapid recovery from a specific point in time. Endpoint backup tools use a similar approach; however, they are optimized to protect many devices under a single, centralized platform.

Backup protection should allow IT to perform both simple file and folder restore as well as full-system recovery for the worst types of data loss. Businesses also need to create a second backup copy and store it at a secure, offsite location, such as the cloud. Cloud backup protects against regional outages that affect both primary and local backup data.

High availability

Critical systems require the highest level of protection. An outage to an email server or transactional database could disrupt essential operations. This is where high avasilability comes in. A high availability solution mirrors server data in real time. If there is a primary server outage, operations fail over to the secondary server within minutes or even seconds. Workloads continue to run on the secondary system until the primary server is brought back online. Extending this capability into the cloud allows operations to continue remotely until the onsite disruption is resolved.

Since the replication process occurs in real time, a high availability solution can ensure near-zero data loss. High availability also allows IT admins to perform test failovers without disrupting users or asking staff to work irregular hours. Anytime there's a change to network topology, IT can test performance with a high degree of confidence.

Deployment

DRaaS

Stagnant budgets are forcing IT departments to weigh investments more carefully and shift spending from capital expenditures to operational expenditures. With DRaaS, you don't need secondary hardware to store replicated data for recovery purposes. You can enjoy all the benefits of resilient IT without owning the hardware or being responsible for maintenance.

Many businesses have decided that, while their data is crucial for their success and survival, it's not necessary to invest in a secondary data center as a precaution. The emergence of cheap storage combined with advancements in data protection transforms the way IT decision-makers think about backup. It's now easier and more cost effective than ever to ensure high service levels for critical applications through a DRaaS provider while protecting secondary and archival systems with cloud or hybrid backup.

Migration

Public cloud platforms like Amazon Web Services (AWS) and Microsoft Azure are highly scalable technology innovations that help businesses lower expenditures and stretch resources further with less infrastructure. But if businesses can't migrate efficiently, it limits their ability to leverage new technology platforms and increases the risk of getting locked into a platform. This brings security into question as vulnerabilities emerge due to the absence of periodic software patches. Sooner or later, businesses will be forced to migrate as the platforms they're on are sunsetted. By onboarding the necessary resources to perform efficient, non-disruptive migration, businesses can ensure the success of migration projects and thereby protect long-term agility and competitiveness.

The cyber resilience sweet spot

A blended approach to data protection—with high availability combined with backup and non-disruptive data migration—gives IT decision-makers confidence in their ability to mitigate disruptions, preserve historical data and maintain business agility. It also simplifies administrative tasks and allows IT staff to focus on strategic initiatives. Organizations of all sizes wish to achieve this level of cyber resilience.

Carbonite's Data Protection Platform enables businesses to deploy comprehensive protection for any physical, virtual, cloud, legacy or heterogeneous environment. Contact us to learn more.

Contact us to learn more – Carbonite APAC

Phone: 1800 013 992

Email: carb-apac_sales_team@opentext.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.