CARBONITE an opentext company | WEBROOT an opentext company

Buyer's Guide

Carbonite® Server

What to look for when protecting servers from downtime and data loss

Server Protection

Data-driven businesses have multi-faceted needs when it comes to protecting server data. With different types of data present in their systems, different feature sets will be required when considering a backup solution. For time-sensitive data, speed of recovery will be a primary consideration. For archival data, retention scheduling will be paramount.

Decision makers have a number of options when it comes to deploying protection on these systems. This makes it feasible to align protection with the type of data they're looking to protect. According a report from Enterprise Strategy Group (ESG), businesses now employ a number of technologies to protect the different systems and types of data within their networks, including:[1]

- Backup and recovery software
- Replication software with failover and orchestration features
- Applications with built-in mirroring and failover features
- Virtualized and cloud-based systems with rapid scalability

But how do businesses know which data protection solutions offer the features and functionality they need? To answer the question, we put together this buyer's guide. It explores the underlying technology behind the most common forms of server protection. It also includes critical features to look out for, and the benefits they promise for businesses.

Backup, recovery and resiliency

Server backup today is just one facet of a multi-tier strategy for protecting server data and—more critically—access to server data. As businesses realize data loss is inevitable, they have begun to recognize the importance of recovery when determining how to protect servers. It's now widely understood by businesses that backup is only useful if it's part of a streamlined restore process that meets critical requirements for recovery time and, in the example of ransomware and cybertheft, recovery point.

This explains why there's been a broad shift from tape-based backup to technologies that facilitate rapid and flexible restore options.

Periodic backups enable businesses to recover clean copies of data when the originals are lost or become infected. Locally stored backups help businesses and service providers ensure rapid recovery for many of the common data loss scenarios businesses face, including server outages, accidental deletions and overwriting.

Additionally, by replicating server data to a secondary location—such as the cloud—it gives businesses and service providers another option for recovering data when the local source is offline or not operational for whatever reason.

Some systems are so critical to the business that even tiny disruptions in service will result in serious, irreparable harm. For these high priority systems, businesses need highly reliable mechanisms in place for ensuring continuous operation while minimizing the amount of human intervention necessary.

This level of protection requires a highly efficient means for maintaining a secondary instance of the server; one that doesn't impose excess burdens or otherwise interfere with critical data traveling over the network. When an outage on a high priority server occurs, an automated mechanism is required to redirect traffic to the secondary environment. Automatic or triggered failover, while not necessary for less critical systems, is essential for maintaining access for top-tier systems. Fortunately for businesses—and for business data—modern forms of protection have evolved to meet the different strategic objectives businesses have when securing different types of data.

Server resilience myths

Myth: Data protection solutions like backup and disaster recovery are too expensive.

Fact: Compared to the business costs associated with lost data and downtime, data protection solutions are a bargain. Integrated solutions can now offer economies of scale and reduce administrative overhead, making comprehensive disaster recovery far more attainable.

Myth: I have to use legacy backup technology on my legacy systems. It's too risky to update the server or the backup.

Fact: Legacy systems are still widely used for handling highly sensitive and confidential financial data. Additionally, federal and industry regulations often require specific safeguards for protecting this data for specified periods of time. Given the criticality of data on these types of systems, having a purpose-built backup solution is essential.

Myth: Cloud-hosted server backup and disaster recovery is an enterprise-level solution that most businesses don't need or can't afford.

Fact: It's never been easier to maintain a perfectly synchronized replica server in the cloud for use in cloud-based disaster recovery. The combination of a highly efficient mirroring process—like byte-level replication—and automatic failover to a secondary server target makes cloud-based disaster recovery a very real and achievable possibility for almost any business.

What to look for in server protection

What	Why
Hybrid deployment	Server data should be duplicated both onsite and offsite (such as cloud) to enable rapid recovery from a local source and facilitate remote recovery for network outages.
Flexible retention (enabling point-in-time recovery)	The ability to revert back to an earlier state can simplify recovery efforts and thwart ransomware and other malicious cyber threats.
Broad platform support and robust application protection	Broad platform compatibility ensures both legacy and modern systems remain secure, while eliminating the need to procure multiple solutions to protect all your systems and applications.
Ease of use	Backup and retention policy controls, automation and APIs save time and money.
Monitoring and reporting	Status monitoring and reporting enable administrators to verify whether backups are working properly. The dashboard should give clear indicators of failed jobs and options for proactive alerts.
Rapid restore	Server protection should give administrators the ability to restore files, application data or entire servers quickly, using the restore mechanism that makes sense for the specific failure (failover locally, mount virtual, download from the cloud, etc.).
Non-disruptive testing	Having a secondary cloud environment that mirrors the source in real time enables businesses to keep critical systems and applications online anytime there's an interruption at the source. Best-in-class solutions include orchestration for multi-tier applications, with boot order and script points.
Cloud failover	24/7 support and professional services from initial deployment to testing to failover and failback can simplify onboarding of solutions and ensure proper deployment.
Customer supporrt	24/7 support and professional services from initial deployment to testing to failover and failback can simplify onboarding of solutions and ensure proper deployment.

Buying tips

One of the challenges IT decision makers face when considering server protection is finding a solution that protects physical, virtual and legacy systems. The struggle lies in balancing performance features with overall system compatibility, along with the needs of the business. Some IT managers combine several different solutions, as certain features and functionality become table stakes. But combining solutions only serves to add complexity to an already sprawling architecture. An ideal solution offers broad flexibility in terms of the types of systems it supports as well as the network topology over which it's deployed. This includes flexible deployment for both physical and virtual systems as well as flexible configuration, both onsite and at a cloud target or offsite datacenter. It also includes flexible features that enable IT organizations to implement different facets of a multi-tier data protection strategy, such as periodic snapshotting for scheduled retention and cloud failover for continuous operations.

The Carbonite advantage

Carbonite Server is a simple, all-in-one server protection solution for physical, virtual and legacy systems. Deployed in your onsite environment, it stores copies on a local target as well as in the cloud. The software, cloud service and even optional onsite hardware are fully integrated and backed by the award-winning Carbonite support team.

Key features and benefits:

- Easy, reliable server backup and recovery for virtual, physical and legacy systems
- Secure local and cloud backup with optional, integrated hardware
- Flexible recovery options including rapid local failover and granular restore of files, folders and application data
- Optional cloud failover for critical systems that require near-zero downtime
- Compressed, deduplicated, forever-incremental backups
- Expansive platform support—over 200 operating system versions, applications and platforms
- Recover virtual machines in minutes regardless of the VM size
- Recover entire systems (including operating system, data and applications) with bare metal restore
- End-to-end encryption—AES 256-bit private key encryption and TLS/SSL transport security
- On-boarding and recovery support from our certified experts, 24×7

Operating systems and hypervisors

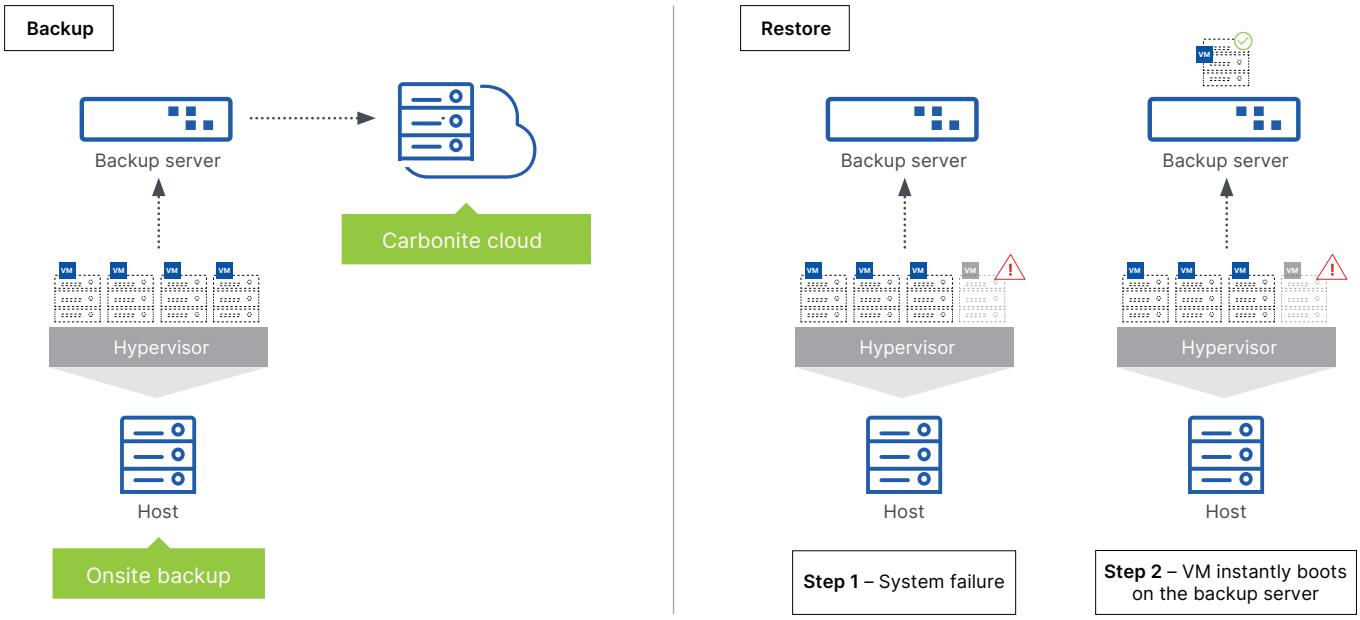
- Windows
- Linux
- VMware and Hyper-V (agentless)
- Oracle
- IBM AIX
- HP-UX
- Solaris
- IBM iSeries

Application-aware agent plug-ins

- Microsoft SQL
- Microsoft SharePoint
- Microsoft Exchange
- OracleDB

Granular recovery

- Files/folders
- Microsoft Exchange
- Microsoft SQL databases and tables
- Microsoft SharePoint
- Microsoft Active Directory



Contact us to learn more – Carbonite US
Phone: 877-542-8637
Email: carb-data_protection_sales@opentext.com

[1] ESG Master Survey, Real-world SLAs and Availability Requirements, May 2018

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.