CARBONITE

Carbonite: Complete data protection

All the strategic tools necessary to protect any type of data

Complete data protection

Data protection often seems like a clash between competing interests: the need to protect data, against the need to protect access to data. The challenge lies in deploying the right protection across the different systems and types of data, since they each require different forms of protection.

IT pros need confidence that the protection they deploy can:

- Ensure long-term survivability of historical data.
- Deliver data securely to different waypoints.
- Extend protection as environments change.

Carbonite offers a complete stack of tools for ensuring both the survivability and availability of data for various strategic purposes, including: information governance, regulatory compliance support, business intelligence, agility and user productivity. Carbonite backup, disaster recovery and high availability solutions—powered by EVault and DoubleTake technology—help more than 1.5 million customers protect their data. From simple, secure cloud backup and hybrid disaster recovery 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 resiliency

With the high rate of technology disruption today, it's increasingly 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 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 different protection than an intermediary. A repository stores historical data that's less urgent than other types of data but still necessary to protect. An intermediary system delivers critical services as well as actively changing data that users need to be able to access.

The question of the appropriate protection comes down to outcomes. Starting with outcomes, IT decision makers can easily eliminate solutions lacking the minimum feature set.

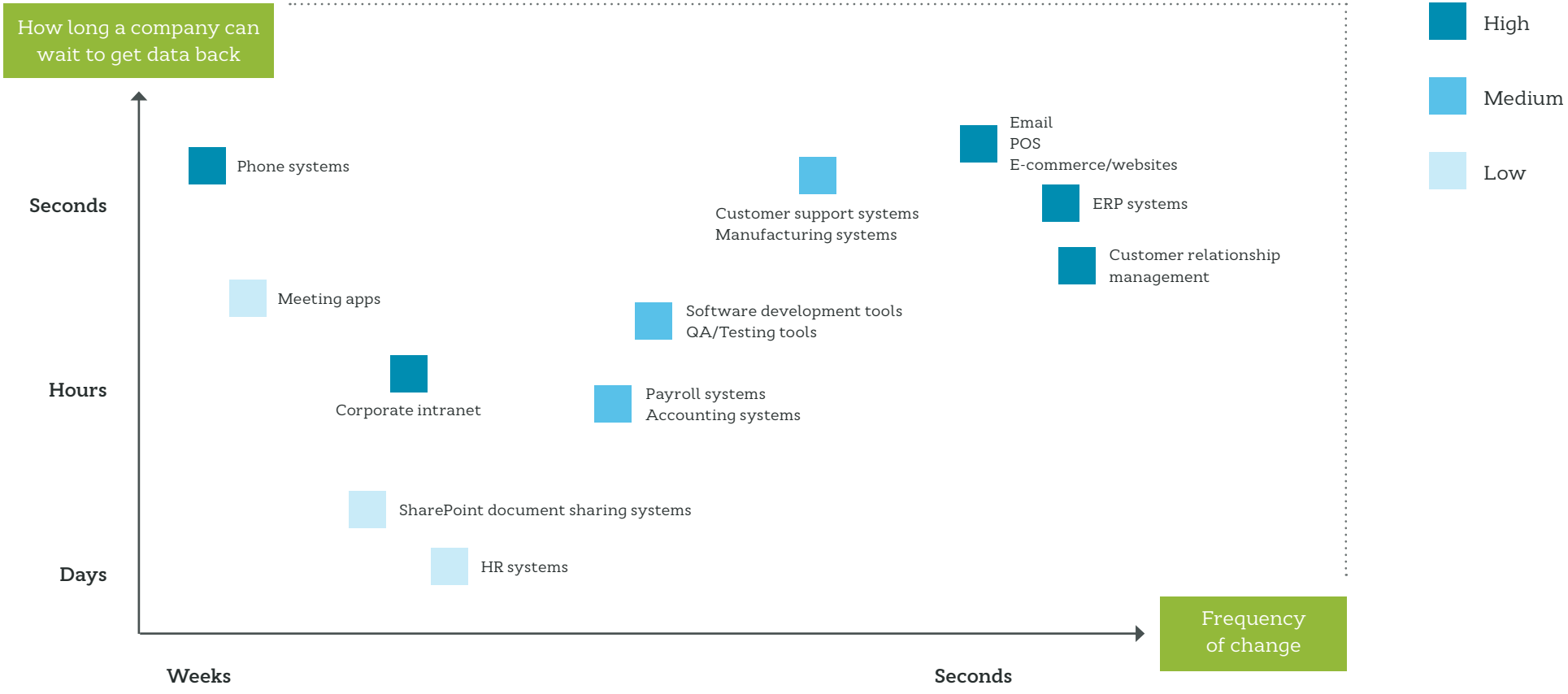
Specific outcomes businesses seek to control include:

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

Procedures and technology are additional factors. Rate of change and available bandwidth will determine the applicability of 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 resiliency

Aligning protection with urgency



Data-defined protection

Data-defined protection isn't new. But the lack of automated tools has 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—seem superficial and antiquated. The practices and procedures for data protection have evolved alongside mobile, cloud and virtual platforms. Businesses now have a complete spectrum of data-defined 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 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 establishing 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.

Data protection that's 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.

User productivity

Today's markets are highly competitive, mobile and global. To stay productive, users need always-on access to the most critical, high-value data in their organizations. Even small disruptions can be too costly for extremely time-sensitive data. Businesses need the option to automatically or manually fail over to an alternative, mirrored target with minimal disruption in service. A solution designed for productivity offers businesses advanced feature sets for ensuring always-on access to critical servers and applications in the event of a disruption to the production environment. Today, system complexity and distribution 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.

Data protection from Carbonite

Carbonite offers a complete portfolio of data protection solutions with multiple options for backup, high availability and data migration for all types of data, including heterogeneous environments and dispersed networks. Carbonite allows organizations to deploy a blended data protection strategy for any hardware, software or virtual platform. 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 Hybrid Backup

Carbonite Hybrid Backup *Powered by EVault* is a powerful disaster recovery 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

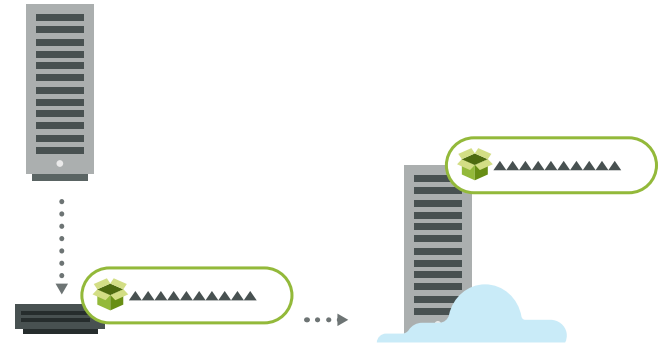
- Protect heterogeneous networks with a single solution
- Accelerate recovery time performance
- Ensure flexible daily and monthly recovery points
- Centralize protection for distributed environments

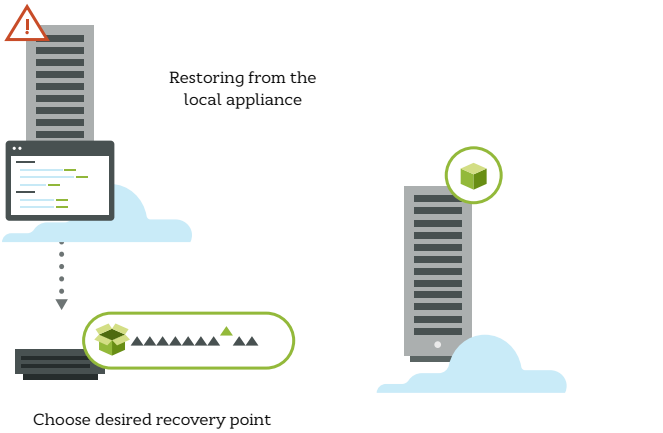
Carbonite Hybrid Backup is available as a software-only solution or as hardware with subscription pricing for reducing or eliminating capital expenditure (capex).

Feature detail

- System image and granular recovery options
- Advanced 256-bit private key encryption
- Dissimilar hardware restore
- Central management via browser-based portal

With fully customizable scheduling and retention settings, Carbonite Hybrid Backup gives businesses options for addressing the speed of recovery, the point in time they wish to recover from, storage footprint and network bandwidth.





Data protection from Carbonite

Carbonite Availability

Carbonite Availability *Powered by DoubleTake* 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

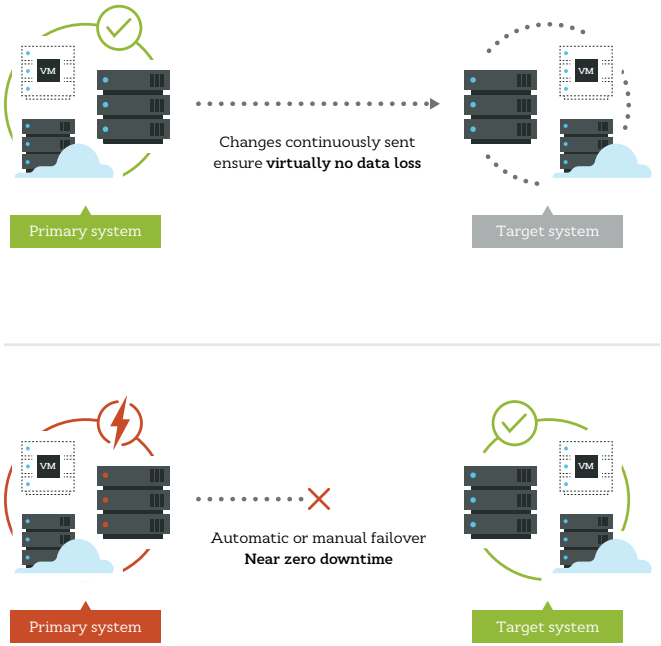
- Replicate any source data to any secondary target in real time
- Perform automatic or triggered failover with virtually no disruption in service
- Execute tests with live data to ensure cross-dependent functionality
- Simplify administrative tasks and eliminate disaster recovery fire drills

Carbonite Availability continuously replicates to the secondary target, eliminating the potential for data loss from changes that can occur post-snapshot. In the event of a disruption at the source, push-button or automated failover ensures uninterrupted access to application data from the secondary source.

Feature detail

- Real-time, byte-level replication for physical, virtual or cloud environments
- DNS mapping with automatic application dependency discovery
- Software development kit (SDK) for seamless integration via API

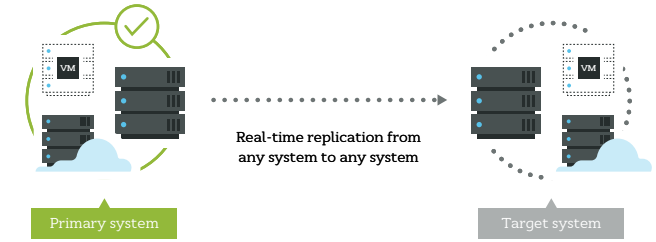
Once the issue is resolved, users fail back to the production environment, usually without noticing. The entire solution is managed through the console.

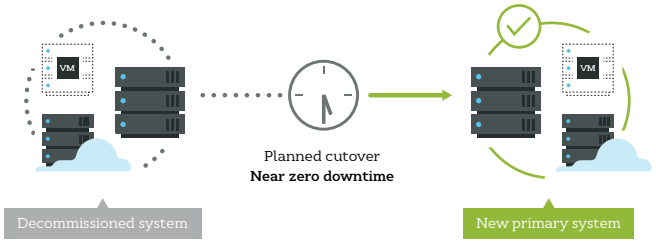


Data protection from Carbonite

Carbonite Move

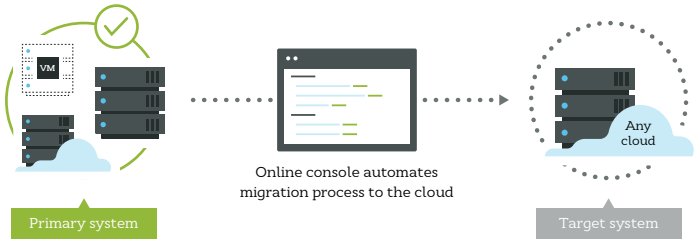
Carbonite Move *Powered by DoubleTake* automates data transfer in real time. It replicates the entire server, identifying and preserving cross-dependencies along the way. At cutover, it automates turning the target machine into the production machine. Move talks to the DNS servers, updates records and automatically redirects to the new server. Move allows end-to-end testing and full reporting that support both internal and external compliance. It uses byte-level replication to eliminate the risk of data loss for critical applications and data.

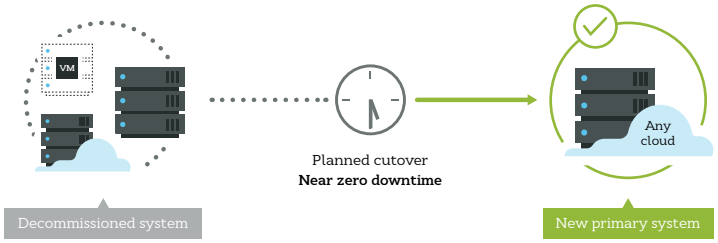




Carbonite Cloud Migration

Carbonite Cloud Migration *Powered by DoubleTake* offers superior flexibility for migrating between the major public cloud providers. Carbonite Cloud Migration is a point-specific solution that supports any production environment running in AWS, Azure, VMware or OpenStack. It automates the entire migration process, including licensing, discovery and orchestration, and handles virtual server configuration and customization from a central management console.

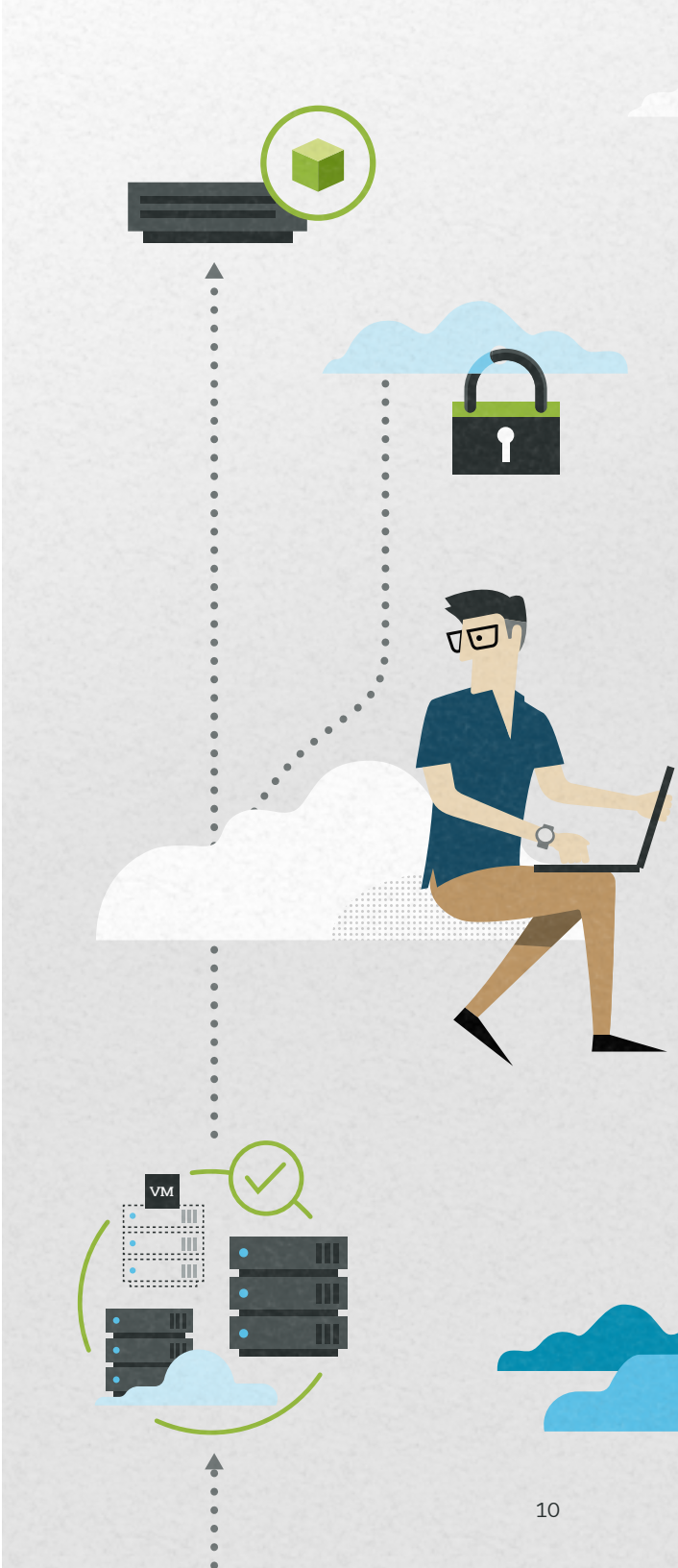




Deployment

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.
- **Data migration** – Deploy for hardware or platform upgrades, software patches and for changing vendors.

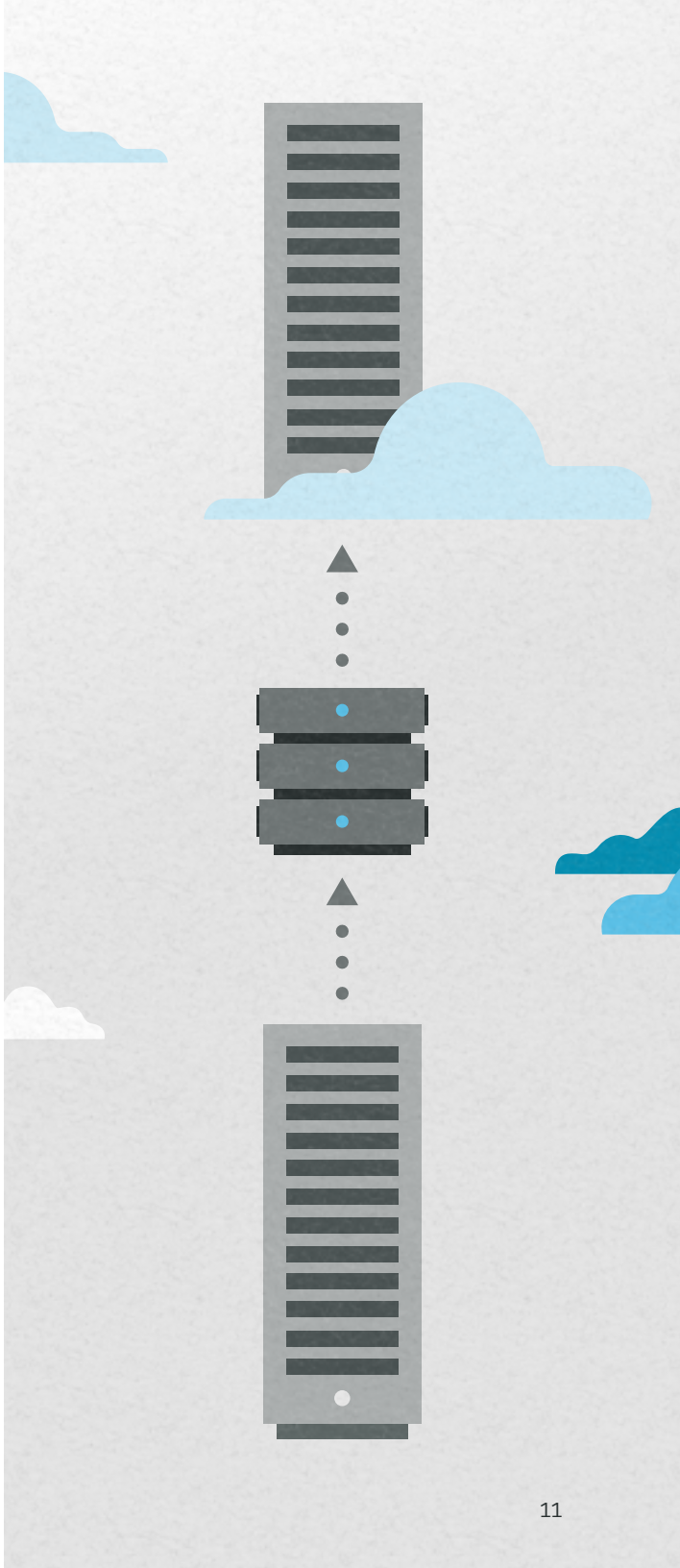


Deployment

Backup

To satisfy demands for document retention and recoverability, businesses should deploy backup for all types of data. Backup captures snapshots at periodic intervals and protects them according to a set retention schedule. A daily snapshot taken during off-peak hours and protected onsite will allow a business to perform rapid recovery from a specific point in time. A retention schedule consisting of the most recent snapshots—30 daily and 12 monthly—is usually sufficient to address most forms of data loss, including accidental deletions, hardware failures and malware. Large-scale interruptions like power outages, natural disasters and critical hardware failures, while less common, can be far more detrimental.

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. Because regional outages can affect both the backup and the original, cloud backup allows businesses to recover server data remotely. Recovery time using backup is typically measured in hours or days, depending on the scale of the disruption and the time it takes to resolve the underlying issue.

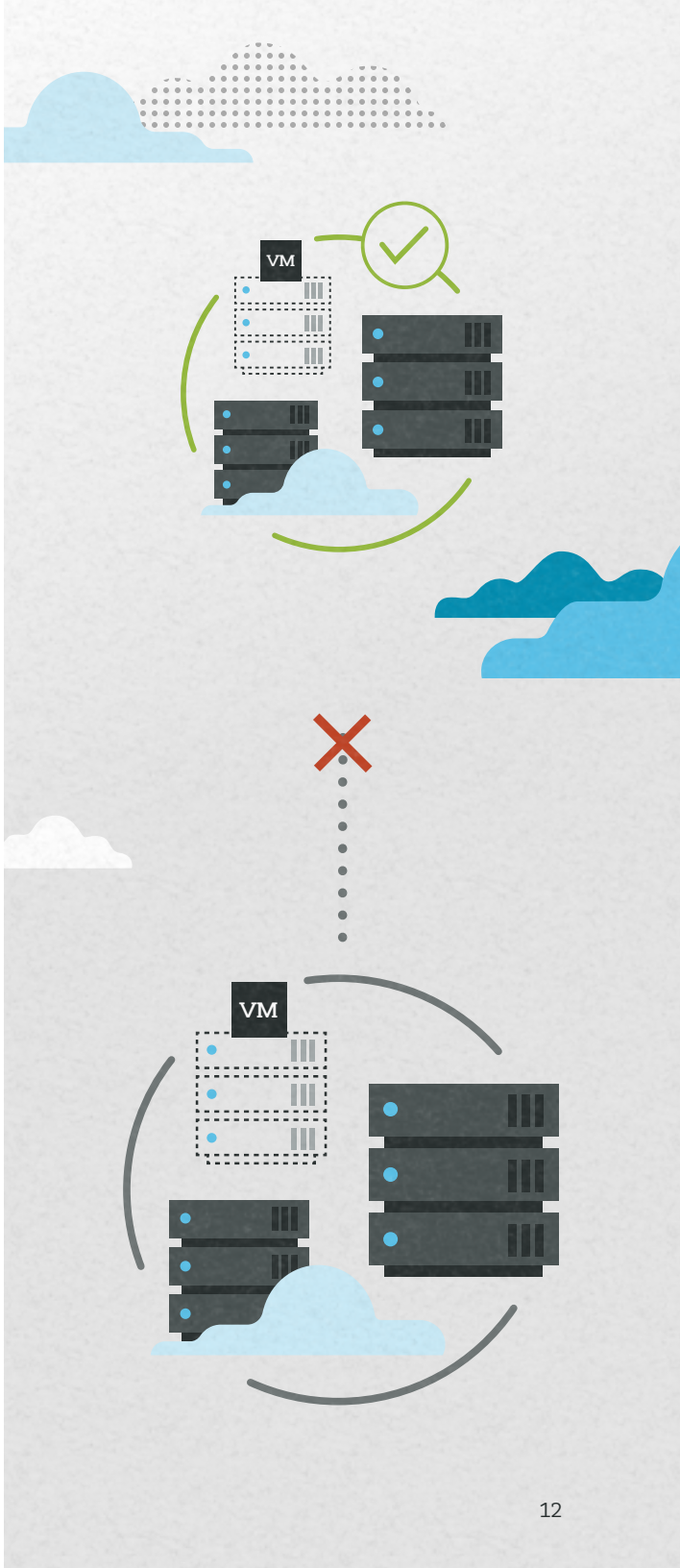


Deployment

High availability

Critical systems require urgent protection. An outage to an email server or transactional database could disrupt essential operations. This is where high availability comes in. High availability can share the same architectural structure as backup, with a copy onsite and one in the cloud. The difference lies in the frequency of replication, which has implications for system uptime and potential for data loss. A high availability solution mirrors server data in real time. If there's a server outage in a high availability environment, the secondary server becomes the source and users fail over to the replicated server. Recovery time in this scenario is measured in seconds. Workloads continue to run on the secondary system until the primary server is brought back online. The entire process can be automated or triggered.

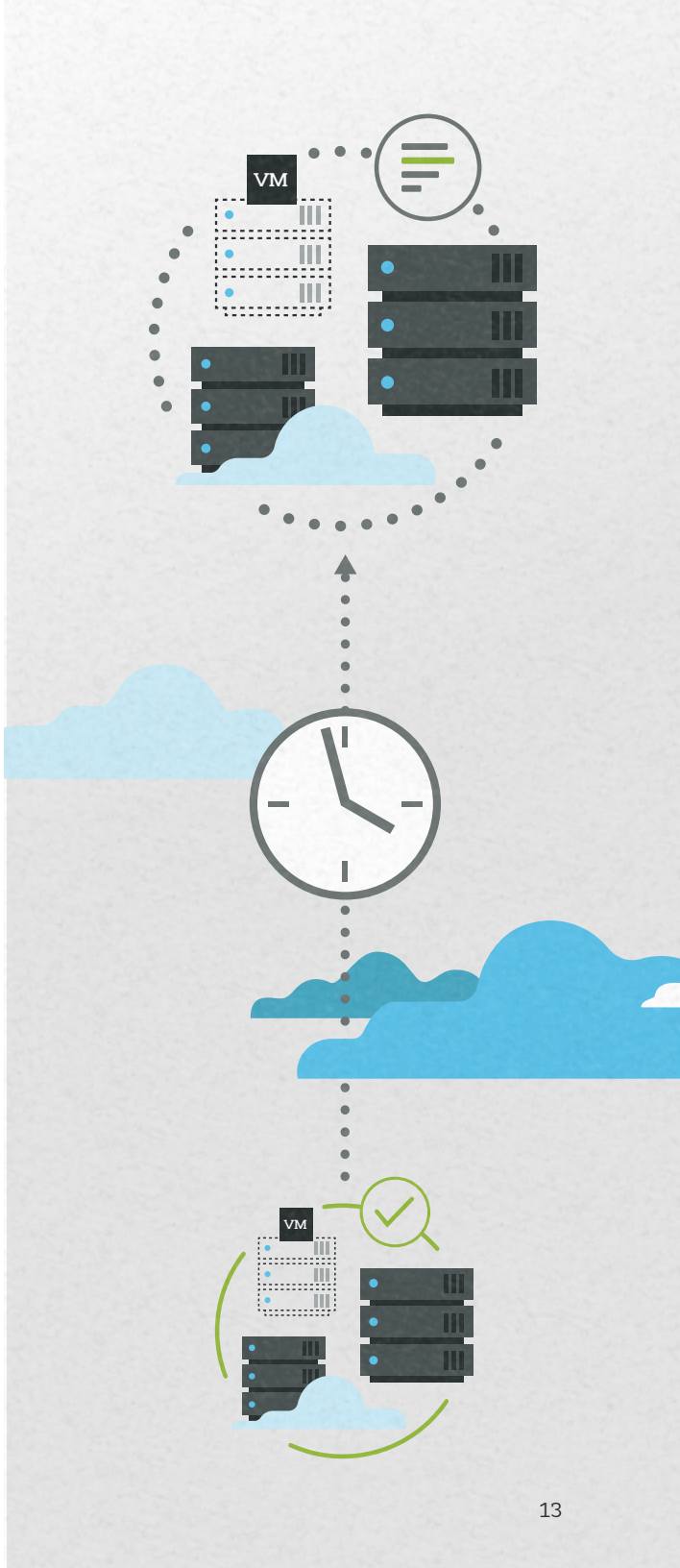
As with cloud backup, if both the primary and secondary servers are affected, the cloud target is available remotely until the onsite disruption is resolved. Since the replication process occurs in real time, a high availability solution can ensure zero or near-zero data loss. High availability also allows IT admins to perform test failovers using real-time data without disrupting users or asking staff to work irregular hours. Any time there's a change to network topology, IT can test performance with a high degree of confidence.



Deployment

Migration

Public cloud platforms like Amazon Web Services (AWS) and Microsoft Azure are disruptive 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 data protection 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.

With Carbonite, any size business in any industry can deploy a comprehensive data protection strategy for any type of data on any technology platform all from a single source.

Phone: 800-683-4667
Email: DataProtectionSales@carbonite.com

CARBONITE

[1] Enterprise Strategy Group, Why—and How—Organizations Need to Align Business Priorities and Data Protection Strategies, April 2017.