CARBONITE

Executive guide to data protection

© 2017 Carbonite, Inc. All rights reserved.

Guide to data protection

Data protection often seems like a clash between competing interests: the need to protect data, and the need to protect access to data. The challenge lies in deploying the right protection across the different systems and types of data, since businesses have different objectives depending on the nature of the data.

Determining factors

The question of the appropriate protection comes down to outcomes. Starting with outcomes, decision makers can easily eliminate solutions lacking the minimum feature set. Specific outcomes businesses seek to control include:

- System uptime
- Recovery speed (RTO/RPO)
- Data survivability
- Document retention
- Discoverability
- Non-disruptive migration

Business benefits of aligning protection with type of data:

- Achieve predetermined recovery objectives for different types of data
- Eliminate unnecessary demands on internal resources
- Maintain business agility
- Reduce total cost of ownership

© 2017 Carbonite, Inc. All rights reserved.

Data-defined protection

Data-defined protection isn't new. But 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.

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.

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. And the threats of natural disasters, such as floods, have become more common and widespread.

In a data-defined protection strategy, deployment aligns with predetermined objectives establishing the urgency of each system under 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.

© 2017 Carbonite, Inc. All rights reserved.

Data protection deployment

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

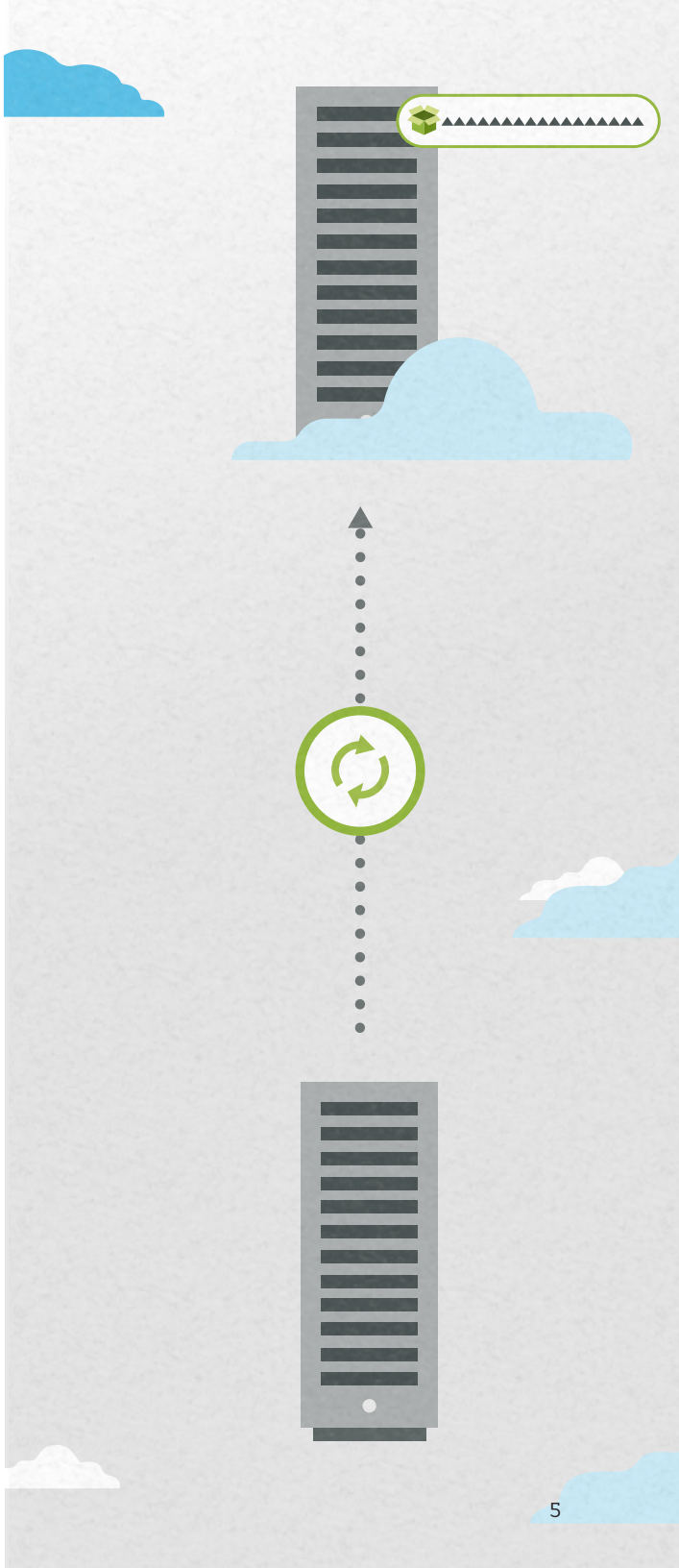
- **Backup** – Deploy across all systems for information governance and rapid recovery for both small-scale data loss and extreme adverse events.
- **High availability** – Deploy for critical, time-sensitive systems requiring continuous or near-continuous operation.
- **Data migration** – Deploy for hardware or platform upgrades, software patches and for changing vendors.

© 2017 Carbonite, Inc. All rights reserved.

Data protection 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 in 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.

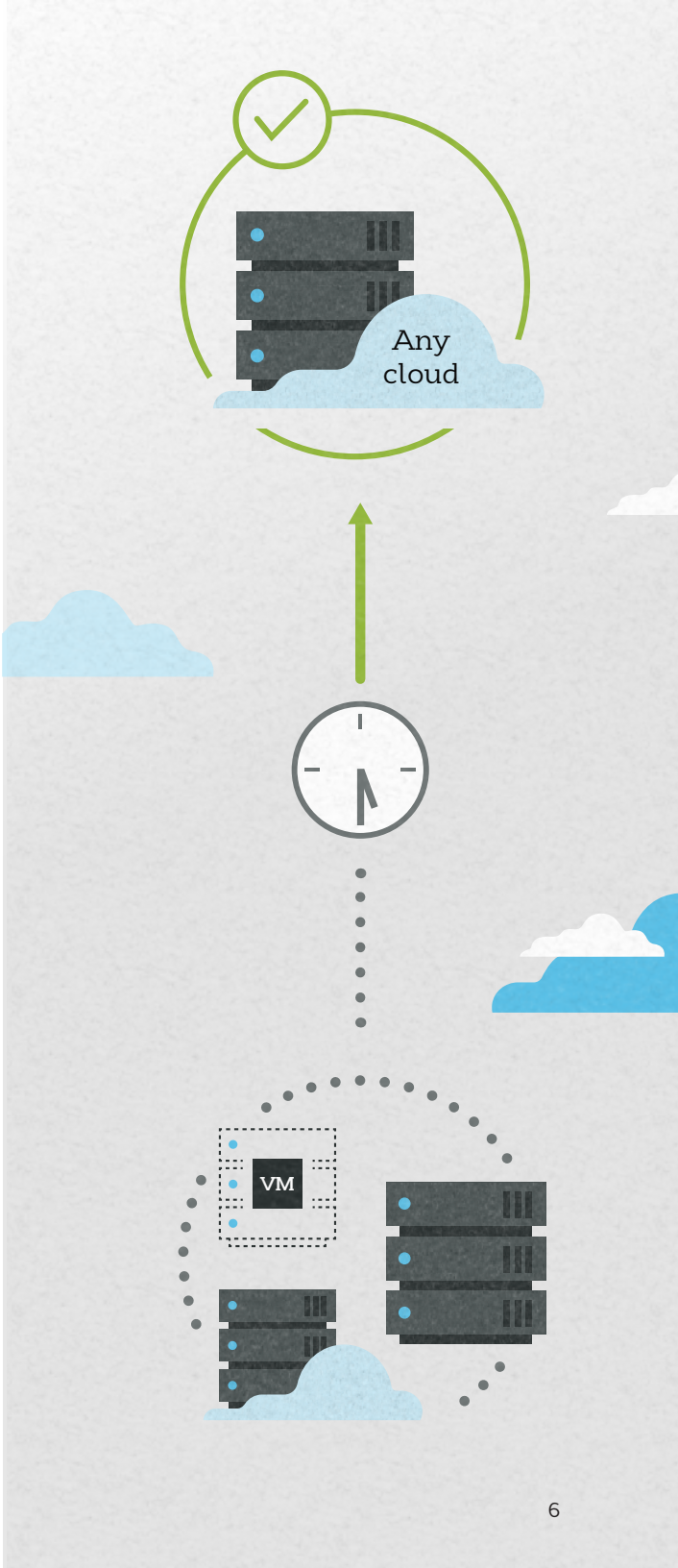


© 2017 Carbonite, Inc. All rights reserved.

Data protection deployment

Migration

Public cloud platforms like Amazon Web Services (AWS) and Microsoft Azure are disruptive technology innovations, which are helping businesses of all sizes 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 and vendor. No business stakeholder wants to feel as if they can't leverage the public cloud offering that works best for them, or change providers. By onboarding the necessary resources to perform efficient, non-disruptive migration, businesses can enable the success of migration projects and thereby ensure long-term agility and competitiveness.



© 2017 Carbonite, Inc. All rights reserved.

Data protection deployment

High availability

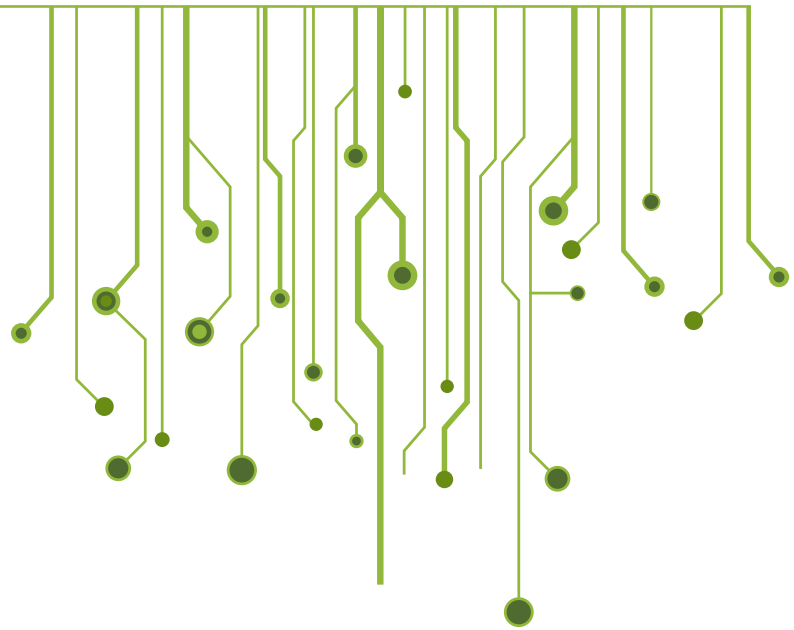
Critical systems require urgent protection. An outage to an email server or transactional database could disrupt essential operations. This is where high availability comes in. High availability can share the same architectural structure as backup, with a copy onsite and one in the cloud. The difference lies is 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 manually 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 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.

© 2017 Carbonite, Inc. All rights reserved.

The data protection sweet spot

A blended approach to data protection—high availability combined with backup and non-disruptive data migration—provides decision makers confidence in their ability to mitigate disruptions, preserve historical data and maintain business agility. It also simplifies administrative tasks, and allows staff to focus on more strategic initiatives and ways to leverage data as a competitive asset.

Learn more about Carbonite data protection solutions today.



Contact us

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

CARBONITE

© 2017 Carbonite, Inc. All rights reserved.