COHESITY

ActualTech MEDIA

Multicloud Data Protection and Recovery

Lawrence Miller

- ✓ Modern Data Management Challenges
- ✓ Multicloud Data Protection and Recovery Use Cases
- ✓ Requirements for a Multicloud Data Protection and Recovery Solution

IN THIS PAPER

Data is crucial for modern businesses, and its loss due to ransomware, hardware failure, or other issues can cripple operations. Effective data backup and recovery are essential to mitigate these risks. This tech brief highlights the challenges and solutions in data management, especially in multicloud environments.

Highlights include:

- Multicloud architectures, while beneficial, complicate data management and protection.
- Essential features for modern data protection include cloud-native support, instant recovery, and cyber resilience.

CONTENTS

Data is the lifeblood of every modern business, but what happens when your data is gone? Whether it's ransomware, a denial-of-service (DoS) attack, a malicious insider, a hardware malfunction, or an honest mistake, when your data is gone your business can't function. Given the business-critical nature of data today, you need to ensure you can quickly and effectively back up and recover your data.

In this tech brief, you'll learn about data management challenges, multicloud data protection and recovery use cases, and the capabilities and features you need in a modern data protection and recovery solution.

Modern Data Management Challenges

Despite knowing how important protecting their data is, organizations struggle to do so because of complex IT infrastructures, data silos, and explosive data growth. Part of this is due to organizations developing a patchwork of data protection tools and products to address different use cases. It is also driven by legacy solutions that have grown expensive to maintain and aren't always interoperable with new technologies. Instead, many companies are adopting cloud-first strategies with multicloud infrastructures.

Despite knowing how important protecting their data is, organizations struggle to do so because of complex IT infrastructures, data silos, and explosive data growth.

In a multicloud architecture, an organization uses two or more cloud computing services from different cloud providers in order to improve their disaster recovery capabilities, leverage best-of-breed technologies, optimize application workloads, and reduce risk. However, it is not without its drawbacks—87% of organizations adopting a multicloud strategy, say managing multicloud has become one of the top three cloud challenges for enterprises.

Why? Sometimes, multicloud architectures have emerged unintentionally as a result of decentralized IT management and pervasive shadow IT, rather than a deliberate strategy. For example, your human resources department may be using a Software-as-a-Service (SaaS) application for payroll, your DevOps teams may prefer to build applications on Amazon Web Services (AWS), and your IT department may be managing your core infrastructure in Microsoft Azure. Other times, they are deliberate, but by nature, multicloud strategies result in data in separate locations. Regardless of whether they were intentional or not, data is everywhere. This increases IT complexity, leading to data protection and security challenges.

Another source of data growth and complexity is data democratization—that is, making all data and data types readily available to all business users, rather than adopting the least privilege security principle—which creates more data management challenges. As organizations quickly move to launch their own artificial intelligence (AI) initiatives, data volumes will continue to grow exponentially, and putting data everywhere in disparate point products deployed across multicloud and hybrid architectures, will continue to be increasingly problematic.

What organizations need is a modern data protection and recovery solution that protects systems and workloads across on-premises and hybrid multicloud environments that is fully integrated, provides granular backup and instant recovery capabilities, strengthens cyber resilience, detects threats, and enables rapid recovery from cyberattacks. It's a single unified solution for data management and protection that will service business use cases today and in the future.

What organizations need is a modern data protection and recovery solution that is cloud-native, fully integrated, provides granular backup and instant recovery capabilities, strengthens cyber resilience, detects threats, and enables rapid recovery from cyberattacks.

Multicloud Data Protection and Recovery Use Cases

Multicloud data protection and recovery supports many use cases. Some of the most common include:

- **Backup and recovery.** You can lose data in a variety of ways, malicious and not, which is why a critical first step to recovery is backing up your data. It is important to have a process and a tool for creating and storing copies of data in a secure location to protect against loss or damage.

- **Data security and compliance.** Different industries have different rules for how you can handle data. For example, General Data Protection Regulation (GDPR) applies to any business controlling or processing the personally identifiable information (PII) of European Union residents. Businesses who fail to manage their data in accordance with their industry's regulations could face legal, monetary, and financial repercussions.

- **Ransomware protection, detection, and recovery.** The most effective defense against ransomware is a good, immutable backup of your data that enables rapid recovery—without paying a ransom. However, you should also put a strategy in place to ensure an effective response. Align your strategy with a framework, like NIST, to ensure you're following cybersecurity best practices and have robust protection, detection, and recovery capabilities for your data.

- **Long-term retention and archival.** For businesses that generate new data regularly, but need to retain existing data, data archiving is critical because it enables organizations to quickly retrieve both types. In certain industries, retaining data for longer periods of time is required for compliance and regulatory reasons.

- **Disaster recovery and business continuity.** In our fast-moving, "always-on" business world, downtime hurts both your reputation and bottom line. Organizations must be able to meet increasingly stringent maximum tolerable downtime (MTD) requirements, recovery time objectives (RTOs), and recovery point objectives (RPOs), to ensure their business can quickly and fully recover from an outage or other major event.

Requirements for a Multicloud Data Protection and Recovery Solution

As data becomes more valuable to organizations, a modern data protection and recovery solution for multicloud is essential. Key requirements include:

- **Unified management.** A single unified solution enables global management across multicloud, hybrid, and on-premises environments at scale. It should act as an intelligent global assistant, detecting potential ransomware attacks, helping you identify anomalies and making corresponding remediation recommendations, such as for additional capacity planning.

- **Protection for on-premises, cloud, and SaaS data.** Data is everywhere today. Modern data protection and recovery must protect your data wherever it exists, whether it is on-premises, spanning multicloud and hybrid environments, or in SaaS applications. Look for flexible on-premises and cloud deployment options that can be self-managed or managed "as-a-Service."

- **Instant mass data restore.** Threat actors attempt to exfiltrate or destroy as much of our data as possible, so you need a way to quickly recover all of your data. Look for a solution that keeps snapshots fully hydrated to improve recovery times so it can provide the ability to restore hundreds of VMs, large databases, and large volumes of unstructured data instantly, at scale, to any point in time and location.

- **Cyber recovery.** Verify the integrity of your backups to identify a "clean" recovery point, for example, in the event of a ransomware attack that targets backups. Look for a solution that can enable you to confidently restore data at a granular level.

- **Unlimited scalability.** Eliminate complex, risky, and costly on-premises forklift upgrades and easily scale your solution without disruption. Look for a scale-out, hyperscale architecture and distributed file system that provides global search capabilities and helps reduce your data and storage footprint with global variable-length deduplication and compression.

As data becomes more valuable to organizations, a modern data protection and recovery solution for multicloud is essential.

Customer Story

Ausenco Strengthens Security and Cuts Management Time with Cohesity DataProtect Delivered as a Service

A multinational engineering and consulting services provider, Ausenco backs up 100 TB of critical Microsoft 365 (M365) data for its more than 3,000 employees. The previous backup solution—Veeam software on self-managed cloud infrastructure—no longer met the company's security needs and took 20 hours/week to manage. By switching to Cohesity DataProtect delivered as a service, Ausenco reclaimed 20 hours/week previously spent managing backup infrastructure, introduced 4-hour service-level agreements (SLAs) for file recovery, and obtained the immutable backups required for cyber insurance and peace of mind. All without additional costs.

CHALLENGE

Ausenco's engineering and consulting services business is growing—especially among mining companies experiencing soaring demand for battery metals. The company backs up 100 TB of critical M365 data for its more than 3,000 employees. "Microsoft provides some data protection built-in, but not enough for our business," says Kalpesh Bhathella, Ausenco's Director of Operational Services. "We retain some SharePoint and OneDrive files indefinitely, and can't afford to lose them to cyberattacks."

Until 2022, Ausenco's IT team backed up M365 data with Veeam software, using infrastructure as a service (IaaS) from Amazon Web Services (AWS). But managing the infrastructure and software was brutal, consuming 50% of one IT administrator's time. Another shortcoming: taking immutable backup copies, a must-have to recover from cyberattacks, would require more infrastructure and more management time. "Security is top of mind for us," Bhathella says. "Prospective customers always ask about it, and lately they also want to know if we have cyber insurance. We needed immutable copies, but without more management burden."

SOLUTION

After evaluating Cohesity and Rubrik, Ausenco selected Cohesity DataProtect delivered as a service, which provides backup and recovery capabilities for software as a service (SaaS) like M365 as well as other cloud or on-premises data Ausenco might add later. "We liked the idea of a fully-managed cloud service because self-managing infrastructure makes no sense in this day and age if IT is not your core business," Bhathella says. "And only Cohesity creates immutable backups by default."

The Cohesity cloud service was up and running quickly in approximately 2 weeks. The IT team rarely has to think about it anymore. "After initial configuration, Cohesity just worked," Bhathella says. "On the rare occasions when we've needed support, Cohesity figured it out right away. We've never had to escalate."

OUTCOME

For Ausenco, the top benefit of the Cohesity solution is a stronger security posture. "We do everything we can to prevent cyberattacks, but having the ability to restore clean M365 data from Cohesity's immutable backup copies means we have a solid fallback. Storing immutable backups offsite also helped us qualify for cyber insurance, which prospective customers ask about."

Stronger security costs less, not more. "The savings from not having to pay monthly fees for cloud infrastructure fully paid for Cohesity DataProtect delivered as a service," says Bhathella. "On top of that, we're saving the 20 hours a week we used to spend tuning and managing our backup software and cloud infrastructure." The team member who used to devote 50% of their time managing backups can now spend that time on higher-value digital transformational work. And together with Ausenco's other cybersecurity measures, immutable backups helped the company qualify for favorable rates on its cyber insurance policy.

For the first time, Ausenco is offering a 4-hour SLAs for M365 email or file recovery—a big hit with the company's busy engineering, consulting, and operations teams. "With our old backup solution, restoring a lost Exchange, SharePoint, or OneDrive file could take weeks because our IT admin had to comb through hundreds of backups just to find it," Bhathella says. "Cohesity's search engine is like the Google of backups. We just enter a filename or phrase, and a list pops up. The file we're looking for is often right on top."

Now Ausenco is preparing to use Cohesity DataProtect delivered as a service to protect other workloads besides M365, including on-prem and AWS virtual machines. For extra resilience Bhathella plans to back up certain workloads on Microsoft Azure—a hybrid cloud setup. The IT team will be able to view and manage backups and restores in any cloud from the same Cohesity interface, enjoying a unified management experience.

As Bhathella sums it up, "With Cohesity DataProtect delivered as a service we have everything we need to protect any kind of data as our business grows: immutable backups, fast restores, and great support—all without having to worry about infrastructure management."

The key benefits achieved by adopting Cohesity's solutions are:

- **Immutable copies—a requirement for cyber insurance**
- **Up to 99% faster restoration of M365 email and file restores—4 hours instead of 2 weeks**
- **20 hours/week management time saved**
- **Zero additional expense**

LEARN MORE

Visit https://www.cohesity.com/solutions/backup-and-recovery to learn more about modern data protection and recovery solutions, and download Protect, recover, and get more from your data: A guide to selecting an AI-powered data security and management platform.

COHESITY