aws | COHESITY

EBOOK

The Complete Guide to Backup as a Service (BaaS)

Modernize enterprise data backup and recovery with Cohesity and AWS

Protecting enterprise data has become imperative as ransomware threats and cybersecurity breaches are becoming more prevalent than ever before. As the IT landscape is growing more intricate and spanning on-premises, cloud, and hybrid environments, a backup and recovery solution is no longer a nice-to-have but an integral component of data management and security.

Cybercriminals have been evolving their methods over the years and have started targeting backup data, making it nearly impossible for businesses to restore their production environments. As cyber threats become more sophisticated, enterprises need to remain one step ahead of these evolving challenges by securing their mission-critical data with agile data backup and recovery solutions.

Let's take a look at how Cohesity and Amazon Web Services (AWS) together help organizations modernize their backup and recovery strategy.

Backup and Recovery Challenges Facing Modern Enterprises

As IT environments change, workforces become more distributed, and ransomware threats continue to grow, it is becoming clear that traditional backup and recovery solutions sometimes can't keep up.

Challenges of Traditional On-Premises Backup Solutions

Growing Costs

- Complex architecture
- Increasing renewal costs
- Expensive rip and replace
- Large data footprint
- Expensive data migration

Increasing Operational Overhead

- Infrastructure management
- Multi point products/UIs
- Disruptive upgrades
- Missed backup SLA
- Increased downtime

Data Vulnerability

- Large attack surface
- No immutability
- Lack of WORM (write once, read many)
- Lack of visibility
- Slow recovery

Growing Costs

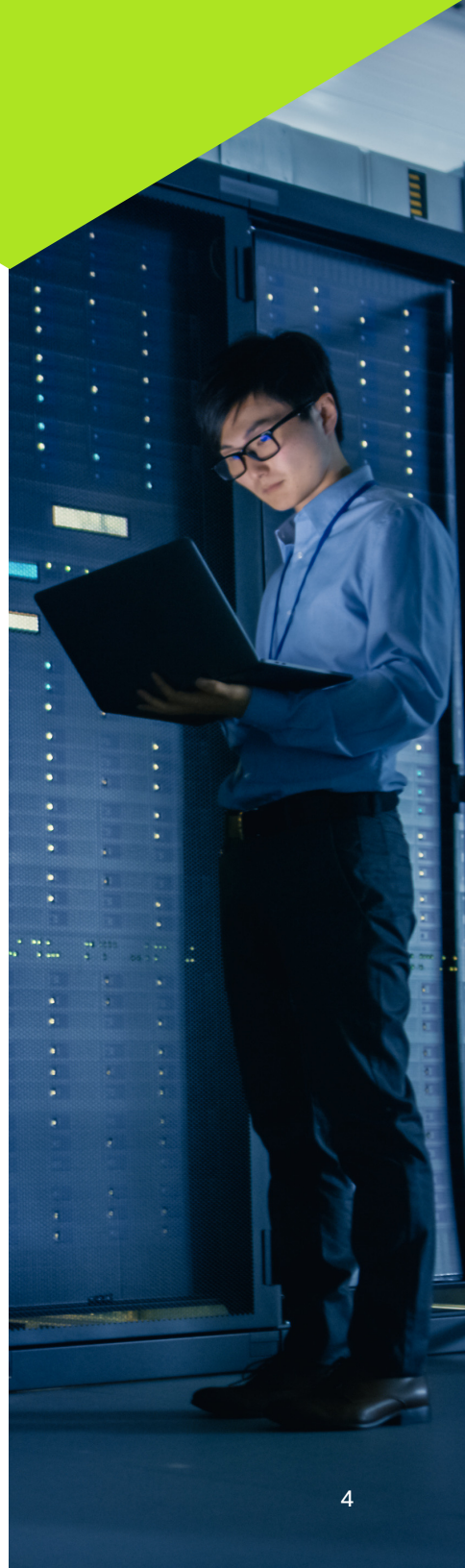
Maintenance and operating costs for traditional data backup and recovery solutions can be significant. Traditional hardware needs to be replaced every few years to take advantage of new technology, remain competitive and avoid any equipment failure. The costs associated here are not just for physical equipment but also include the labor and expertise of staff to complete the upgrades and migration.

Increasing Operational Overhead

IT environments are becoming more diverse and organizations are leveraging both on-premises, cloud and even edge deployments to meet their overall business needs and goals. In fact, in the recent survey, 80% of respondents stated they are taking on a hybrid approach and leveraging both on-premises and public cloud across their IT infrastructure[1]. As a result, the ability to backup and recover data across these complex environments is becoming even more challenging. Enterprises will often implement separate backup solutions for on-premises, cloud, and SaaS data. With these disparate solutions, significant stores of data are trapped in silos making it challenging to leverage data to generate tangible business value.

Ransomware Recovery

To bolster protection against cyberthreats, organizations need to ensure their backup data is ingested and stored in a separate environment. By creating a separate copy of data that is safely isolated, it becomes more difficult for cybercriminals to gain access if accounts get compromised. An effective backup and recovery solution will also ensure that backup data is immutable and utilizes effective identity and access management protocols which will prevent tampering, modification or deletion of backup data.



1. Adler, Brian. "Cloud Computing Trends: Flexera 2022 State of the Cloud Report." Flexera Blog, 21 Mar. 2022

Simply Better Backup with Cohesity DataProtect Delivered as a Service

Cohesity DataProtect delivered as a Service is a Backup as a Service (BaaS) managed by Cohesity and built on the reliable, secure cloud infrastructure of AWS. With DataProtect delivered as a Service, enterprises can take advantage of a backup and recovery solution that simplifies data backup for complex and dynamic workloads, eliminates data silos, safeguards data in increasingly distributed environments, and enhances protection against ransomware.

DataProtect delivered as a Service provides organizations with multi-faceted data protection that helps bolster the security, resiliency, and recoverability of enterprise data.

DataProtect Delivered as a Service Benefits

Address Supply Chain and Deployment Issues	Hybrid cloud backup made easy	Protect against ransomware
• Eliminate CapEx and procurement headaches	• True hybrid experience that simplifies management	• Secure backup data from production
• No infrastructure to manage	• Single UI for all services	• Immutability, multi-factor authentication (MFA) and encryption
• Scale and upgrade on-demand in minutes	• One solution to protect on-prem, cloud and SaaS workloads	• Anomaly detection finds clear data to recover from

aws | COHESITY

DataProtect delivered as a Service provides support for on-prem and SaaS applications including Microsoft 365 workloads, VMware, Hyper-V, NAS, SQL, Oracle and more. Often, native tools have default retention periods that might not always fulfill enterprise requirements. For example, the default retention period for Microsoft 365 data is typically 30 days, which might not meet the SLAs for some organizations. As a result, DataProtect delivered as a Service enables organizations to maintain compliance, improve SLAs, and enhance protection for a diverse range of workloads across the IT environment.

Cohesity and AWS: Better Together

Cohesity DataProtect delivered as a Service works with AWS to further enhance the security and recoverability of enterprise data. Cohesity DataProtect delivered as a Service also supports multiple AWS data sources including Amazon Elastic Compute Cloud (Amazon EC2), and Amazon Relational Database Service (Amazon RDS). The solution enables organizations to store backups of AWS native data in a separate tenant account that is managed and secured by Cohesity. Additionally, Cohesity DataProtect delivered as a Service leverages key management for self-managed or Amazon KMS keys, which allows administrators to create, delete and control keys that encrypt data stored in AWS.

Today's enterprises have a diverse range of workloads and data sources that are often dispersed across locations and environments. As data becomes more distributed and cyberthreats become more sophisticated, it's imperative for organizations to modernize enterprise data backup and recovery strategies with secure and agile solutions that enable organizations to remain one step ahead of evolving threats and protect the data that drives their business forward.

Sign up for a free trial of Cohesity DataProtect delivered as a Service

Cohesity is available in AWS Marketplace

Available in AWS Marketplace