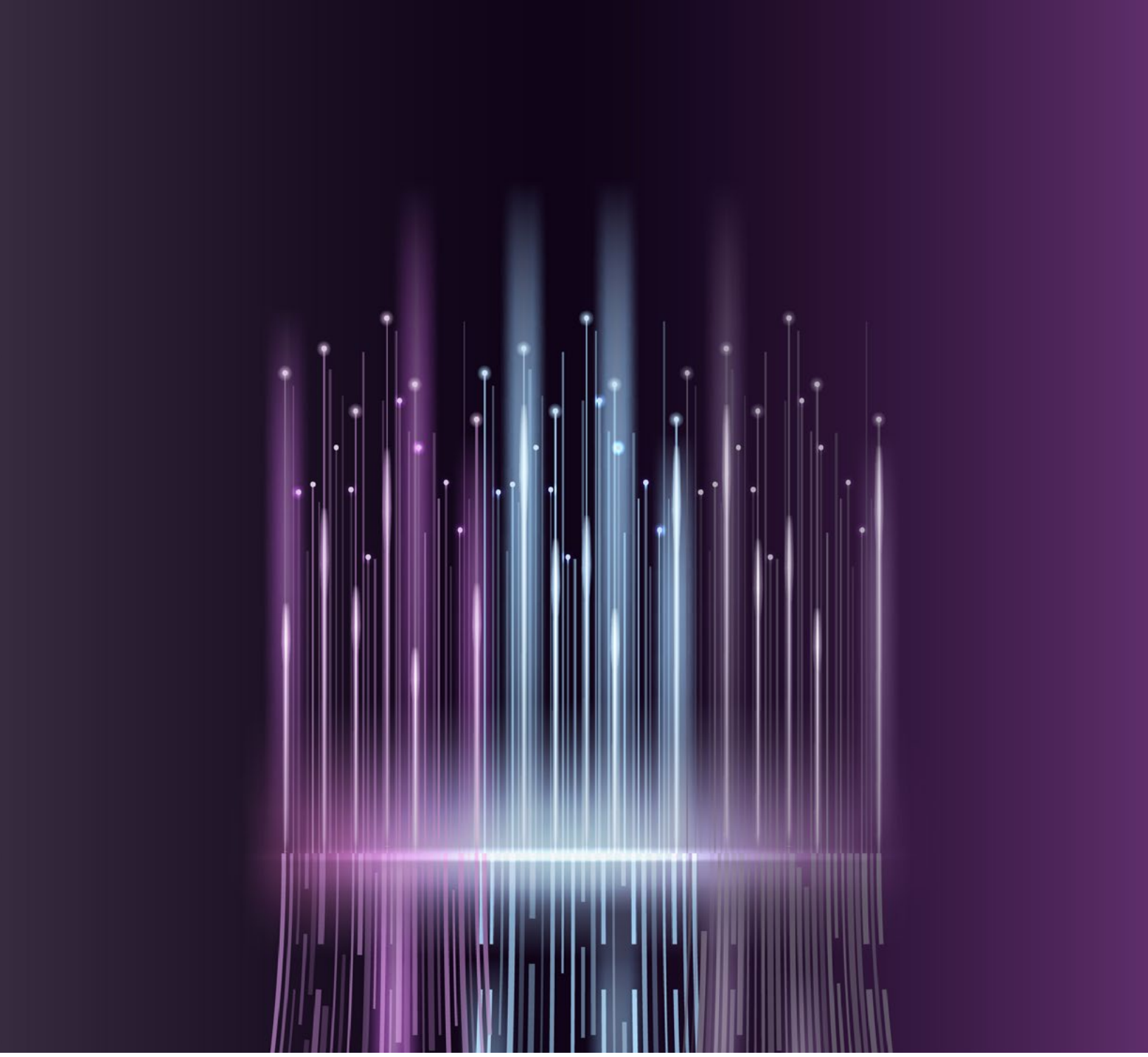


Cloud-Based Data Management: A Holistic Approach

MARKET TRENDS REPORT

govloop

COMMVAULT Public Sector

aws

Introduction

More government agencies than ever are backing up data to the cloud instead of relying solely on traditional on-premise data centers, citing cost savings, scalability and being reasonably satisfied with manageability, along with security being adequately addressed. But cloud-based backup and associated ability to restore from the cloud across the globe should afford more than reasonable satisfaction for managing and securing data. It should be about the ability that cloud provides to drastically improve data management by employing advancements in technology and best business practices.

At the federal level, the Federal Data Strategy — part of the President's Management Agenda — emphasizes the importance of being able to better leverage data as a strategic asset by improving data management to improve overall national security. State government initiatives are underway, too. According to the National Association of State CIOs (NASCIO), top priorities for 2020 include cloud services, along with data management and analytics.

Moving data to the cloud can be that important first step — or sometimes first stumble — toward effective data management, but migrating to the cloud doesn't solve all data management challenges. Despite the cloud, agencies today still grapple with compliance associated with fundamental visibility and data gathering, governance, monitoring, storage integration, and security. A holistic approach to data management, which enables agencies to more easily, effectively and securely manage data, is the best first step to building an operational plan to address our digital world's data challenges.

To understand how agencies can streamline and improve data management, GovLoop teamed with Commvault, a renowned industry leader providing comprehensive data management and protection across platforms, and Amazon Web Services, a provider of cloud services across all classification levels. This report will discuss the benefits of moving data to the cloud, and how agencies can do so in a way that addresses key issues around compliance, governance, manageability and security.

By the Numbers

53%

of government and public services organizations say data modernization is a key component of or reason for migrating to the cloud.

Source: Deloitte

49%

of public-sector IT leaders say their agencies use three to four products in the cloud to handle backups, archives, files and test/dev copies.

Source: Mass Data Fragmentation in the Cloud

32%

of organizations reported being able to realize tangible and measurable value from data.

Source: Accenture

#8

State CIOs ranked storage services #8 on its list of priorities for cloud migration.

Source: NASCIO

15 of 16

federal agencies reported significant benefits from acquiring cloud services.

Source: Government Accountability Office report

Top challenges in building sound data management:

- **Speeding up data analysis**
- **Integrating data**
- **Data-related skill gaps**

Source: CompTIA

89%

of federal IT leaders say cloud isn't providing as much benefit as it could because of data fragmentation in and across public clouds.

Source: Mass Data Fragmentation in the Cloud

35%

Five years ago, organizations had an average of 35% of data in cloud storage, vs. 52% today

Source: CompTIA

The Challenge: Managing Data Chaos

With pockets of data in multiple, unconnected repositories and formats, it has become much more difficult to understand where data is and how it is being used. This is a particularly thorny issue for government agencies, which often have complex information-sharing relationships with other agencies.

With a background in both federal and state government, David DeVries has experienced these challenges firsthand. As CIO at the Office of Personnel Management, for example, he saw how complicated it was to keep information from different parts of an employee's lifecycle separate, as the law requires, but also usable and sharable.

"During employees' active years, the agency manages the data — not only basic data, but things like background investigations. But when an employee retires, OPM takes over, managing retirement benefits," DeVries said. "So during an employee's lifetime, there may be multiple types of data that have to be kept separate for compliance reasons, yet it's also important to be able to look at that data holistically."

Lack of visibility into the location of data and how it is being used also can hide security threats and lead to performance degradation. A recent report from the SANS Institute found that many IT professionals consider lack of visibility and the complexity of managing data across infrastructures as major complications to effective security defense. Lack of visibility also leads to concerns about data privacy and the risk of exposing personally identifiable information and other sensitive data.

Compliance and data governance are also difficult in this environment. With separate data repositories, it can be particularly difficult to meet service-level agreements and agency requirements for security, privacy and data management.

The Solution: Holistic Data Management

The most effective way to address these issues is by managing data holistically. It's by far the best way to know what you have, where it is and that it's fully secure. Plus, agencies can govern that data in ways that comply with all requirements. It can no longer be simply delegated out to a business owner.

"Data is the lifeblood of an organization, from when the data is first created to the end of its natural lifecycle, when it is archived," said Richard Breakiron, Director of Strategic Initiatives for the Federal, Civilian and Intelligence Community at Commvault.

And it works. According to a recent report from IDC, holistic data management results in a 50% to 61% reduction in exposure to compliance or audit failures and a 44% decrease in annual spending on data infrastructure.

The first step to achieving holistic data management is embracing a multi-cloud environment with automated backup. This reduces costs, eliminates hardware and storage maintenance, and automates the process of moving data to different storage tiers and platforms throughout the data's lifecycle.

The next step is standardizing on a solution that provides centralized visibility, full integration with all data repositories and applications, a complete audit trail, automated data analysis, and advanced security capabilities.

In addition to solving data governance, compliance, security and storage challenges, holistic data management can help agencies make better use of advanced analytics, data sharing, artificial intelligence, machine learning and the Internet of Things.

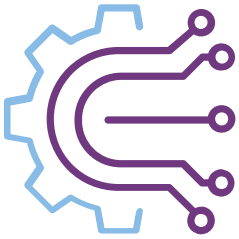
"The more access you have to more data sources, the better your analytics can get," Breakiron said.

Holistic data management also helps agencies prepare for the unexpected. When the COVID-19 crisis forced government employees to work from home, for example, agencies that already practice holistic data management were better positioned to make data available to workers as they shifted to working from home.

Best Practices

Take stock of what you have

You can't move what you don't see, so the first step in any data migration and management strategy is understanding what data you have, where it is stored and who has access to it. It's also important to understand the age and state of the data and associated applications; some older datasets and applications simply won't be compatible with the cloud.

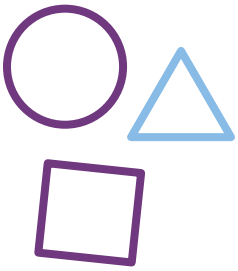


Automate, automate, automate

Manual processes such as scheduling backups or moving data to an archive take time and coordination, and they can lead to mistakes. Automating these procedures solves these problems because storage administrators receive alerts when issues arise, the system can detect new workloads and back them up, and administrators can create policies to automatically move datasets to the archive when they meet specific criteria. And by automating policy, agencies can help ensure that they stay in compliance.

Take advantage of expert guidance

Before taking any action, do your homework. In addition to talking to colleagues and vendors, take advantage of expert guidance from organizations such as Gartner and Forrester, which conduct research that may be valuable to your ultimate decision. For example, a recent Gartner report explains why organizations shouldn't rely on cloud providers' backup and recovery as their main solution. Most cloud providers provide backup and recovery services that don't have the important functions that organizations really need in a full backup and recovery solution, the report states.



Focus on simplicity

Simple is almost always better. For example, make sure you don't have to add new devices to accommodate various types of storage. Instead, choose something that works natively with the AWS storage environment and across all tiers. Make sure you have a simple view of all tiers and can put rules in place to automatically move data to different ones when it meets your criteria. Simplicity also means ensuring that your backup and recovery solution is optimized for both the cloud and heterogeneous on-premise environments. It also extends to tools; the more tools you use, the more complex and expensive it is to conduct backups. Streamline whenever possible, but don't compromise on the ability to protect, manage and monitor workloads across environments with a single, consolidated view.

"Data is the lifeblood of an organization, from when the data is first created to the end of its natural lifecycle, when it is archived."

Richard Breakiron, Director of Strategic Initiatives for the Federal, Civilian and Intelligence Community, Commvault

Case Study: Lending a Helping Hand, with the Help of Modern Technology

With a mission to help other countries reduce poverty, the Millennium Challenge Corporation (MCC) is in a unique position. This small, independent U.S. agency, created by Congress in 2004, has invested more than $14 billion in programs worldwide in areas such as agriculture, education, irrigation and transportation infrastructure.

That's important work, and it requires a solid infrastructure that keeps data safe and backed up and allows employees to access what they need, when they need it. But a legacy data infrastructure hampered MCC's ability to manage information.

The agency needed a modern data infrastructure with business continuity — and it couldn't cost more than the existing infrastructure to run and maintain. MCC had already taken steps away from a virtual environment to the cloud, but the agency's existing backup solution didn't work well in the cloud.

As part of the solution, MCC's IT team moved from its current VMware-hosted environment to Amazon Elastic Compute Cloud (EC2) and Simple Storage Service (S3) Glacier, and implemented Commvault's Complete Backup and Recovery. This combination of technology allowed MCC to securely and automatically back up, recover and archive across files, applications, databases and virtual machines. It also provided a full view of data storage locations and policy control management.

These changes have brought significant benefits. They cut backup storage needs by more than 25%, and backup requirements went from 90 days to six months. In addition, IT administrators no longer worry about whether all workloads will be backed up.

HOW COMMVAULT AND AWS HELP

Commvault's software-based technology data platform streamlines processes and operations, making it easier to manage data, eliminate downtime and reduce workload impact. With a centralized, web-based management interface, the holistic data platform provides a foundation for organizations to use and create value from their data whether it resides in the cloud, the data center, hybrid environments or on mobile devices.

Combining Commvault technology with AWS fosters a holistic, secure approach to data management. It includes protection for AWS-native workloads using agentless, agent and snapshot approaches; data migration and conversion from on-premise virtual machines and other cloud instances to AWS; application-consistent instance-level backups; storage tiering, deduplication and automatic power management of backup EC2 instances.

With Commvault you can quickly, securely and automatically manage data migration from your data center to the cloud or from public or private clouds to AWS, while improving utilization, availability and visibility into your data.

Commvault supports workloads across each of the AWS regions, including GovCloud, Secret, and Top Secret regions. This allows workloads to operate up to the secret U.S. security classification levels.

To learn more, visit www.commvault.com/supported-technologies/aws.

Conclusion

As government agencies embrace the cloud, they are better positioned to take advantage of the benefits that holistic data management provides, including the ability to more easily and securely share data, improve data governance and compliance, and enable more useful and comprehensive data analytics.

A holistic approach to data management should include, at the very least, fully automated backup, recovery and data protection. In addition, it should include global management, proactive monitoring and the ability to manage, monitor, and protect and report on all workloads across on-premise, multiple cloud accounts and regions from a single consolidated view.

The evolving work environment, the continuing need for information sharing, ever-changing regulations and cybersecurity threats, and the growing need for high-level analytics all make traditional methods of data management obsolete. In today's environment, holistic data management is simply good business; it helps ensure that agencies understand what they have, can use that information effectively and are well-positioned for whatever the future brings.

ABOUT COMMVAULT

Commvault provides customers with a comprehensive data management platform that enables data protection, workload migration, disaster recovery, and eDiscovery/compliance capabilities across on-premises environments and Amazon Web Services (AWS). Protect your data with the same policies and SLAs whether it's in your datacenter or in the cloud. Move your workloads to AWS with the click of a button with built-in migration & conversion tools. Test and orchestrate advanced disaster recovery scenarios with workflow automation for true 'DR on demand'. Control all your data – all from a single, secure, easy to use, web-based interface.

ABOUT AWS

With over 2,000 government agencies using AWS, we understand the requirements US government agencies have to balance economy and agility with security, compliance and reliability. In every instance, we have been among the first to solve government compliance challenges facing cloud computing and have consistently helped our customers navigate procurement and policy issues related to adoption of cloud computing. Cloud computing offers a pay-as-you-go model, delivering access to up-to-date technology resources that are managed by experts. Simply access AWS services over the internet, with no upfront costs (no capital investment), and pay only for the computing resources that you use, as your needs scale.

To learn more about AWS, please visit aws.amazon.com.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop