4 Ways Cloud Makes the Best Platform for Disaster Recovery

MARKET TRENDS REPORT

govloop COHESITY aws

Introduction

As federal agencies continue their surge into cloud computing environments for everything from internal messaging to edge applications, some are keeping one foot planted in on-premises infrastructure for disaster recovery. With the idea that should cloud services evaporate in a crisis, they'll still have good old iron to fall back on.

That hardtack insurance policy is inefficient and unnecessary, particularly with so much being run in the cloud and at the network edge. Maintaining infrastructure and facilities, and hot/warm/cold locations in the event of an emergency is an expensive proposition, and their response can be slow, cumbersome and incomplete. Those physical resources are also vulnerable to the same type of disasters, such as fire or flood, that can befall primary data centers.

A managed cloud infrastructure offers significant technical and financial advantages during disruptions. It has the flexibility, scalability and accessibility to enable agencies to adjust quickly to a changing environment, and an on-demand model that saves on expenses before, during and after an emergency.

On-premises operations aren't dead. Of course, there are still instances where agencies can keep things in-house. But disaster recovery (DR) and business continuity (BC) in hybrid and multi-cloud environments are more efficient with cloud-based management that supports recovery from on-premises to the edge.

To learn more about how agencies can reap the many benefits of cloud-based DR and business continuity, GovLoop teamed with Cohesity and Amazon Web Services (AWS), which provide a full range of services, including DR, as part of a single-platform solution for cloud management. This report will discuss the challenges agencies face with disaster recovery and business continuity and how a cloud-based solution solves those problems.

By the Numbers

"[The Homeland Security Department] had not been able to implement a disaster recovery capability because it would cost over $1.5 million to build and maintain a second active network environment. Moving to the cloud enabled the agency to implement this capability for significantly less cost."

– GAO report, April 2019

The cloud carries the load

75%

of enterprise workloads globally will be processed outside of a traditional data center or cloud by 2025.

Source: Gartner

Agencies starting to follow suit

42%

of federal agencies use software-as-a-service (SaaS) for at least 30% of mission-critical resources

Source: Ponemon

Agencies are going to hybrid environments...

31%

of federal agencies are currently using a combination of public and on-premises/ private clouds

43%

expect to be using a combination in the future

Source: Ponemon

...And utilizing multiple cloud providers

44%

of federal agency respondents are currently using multiple public cloud providers

57%

expect to be using multiple providers in the future

Source: Ponemon

The Challenge: On-Prem DR Can't Keep Up With the Cloud

Disaster response involves several stages covering preparedness, the response to an emergency, mitigation of its effects and recovery. At the center of those stages is critical information that must be backed up, replicated and accessible. The data, which is the lifeblood of agency missions, must be readily available if agencies are to respond swiftly to a crisis and mitigate its impact. It's also essential to maintaining business continuity, whether that involves internal operations or administering relief programs.

Cloud platforms evolve swiftly, and best-of-breed solutions come and go, "but we can absolutely bank on the fact that your data is really your strategic asset," said Steve Grewal, Federal Chief Technology Officer (CTO) at Cohesity. "No matter what your mission space is, it's really all about the data. We say, 'Data is the new oil.'"

Agencies need unfettered access to that data across a unified fabric, whether working on-premises or at the edge, said Grewal, who spent more than 15 years as a federal information technology official, most recently as Deputy Chief Information Officer (CIO) of the General Services Administration (GSA), before joining Cohesity.

"The plumbing and stitching can change, but as long as you have that data layer under control and managed efficiently, the rest can be postured around that," he said.

Even in normal, non-emergency environments, however, managing that data can be complicated. Cloud architectures unify a lot of an agency's dispersed operations, but the propagation of cloud systems adds complexity.

An example of this is creating data silos generated by different formats, new services and multiple locations. If not effectively managed, it compounds the mass data fragmentation that already exists within legacy backup, storage and data management infrastructure, making swift retrieval a challenge.

The Solution: Cloud-Based, Enterprise-Grade DR

The government has no shortage of data, and an increasing amount of it resides in the cloud, making a cloud-based solution that integrates and manages that data from the start is optimal for DR. A cloud-based, enterprise-grade DR solution offers agencies a lot of benefits. Here are four of them.

Accessibility. A cloud-based DR solution offers near-instant recovery from the core to cloud to edge and back again. One of its main advantages is accessibility. Hot/warm/cold sites make up on-premises DR systems. These sites slow down physical recovery, and include some data stored offsite and/or on tape, which can be difficult and time-consuming to retrieve.

Policy-based management. A cloud-based solution that provides policy-based management of backups and replication securely across multiple clouds not only gives agencies digital long-term retention and quick access but can integrate that data so agencies can put it to use.

Integration. A software-defined platform provides native integration, consolidating data and infrastructure across its services, while working in a hybrid environment that involves both on-premises and cloud systems.

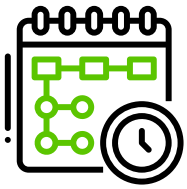
Elasticity/Scalability. Agencies haven't had the elasticity that comes with an on-demand model with traditional approaches;. Scaling systems can suffer from procurement processes that slow things down, as well as from guesswork involved in predicting demand, which can result in agencies under- or overprovisioning.

"Historically, there has been no quick way for agencies to expand on the fly. I think this COVID-19 situation demonstrates how important that is," Grewal said.

On-demand services can accommodate the peaks and valleys of activity as a crisis plays out. And it pays off when services are no longer needed, since they can disappear, unlike hardware. "Once things start to resume and you don't have a need for X number of simultaneous users and that kind of capacity, then you can scale back down," Grewal said. "And I think that is the biggest benefit that agencies will start to experience."

Best Practices: Unifying Data Management

An effective cloud-based DR/BC solution will have several consistent features. These include policy-based automation (including for testing), interoperability with multiple clouds, flexible replication, strong security and verifiable service-level agreements (SLAs). Agencies adopting a DR/BC solution should also hew to five best practices.

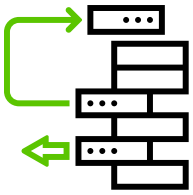


I. Plan for recovery

A governance plan that includes detailed steps for recovery and business continuity will ensure a smooth transition. The Homeland Security Department's guidelines for IT disaster recovery recommend that developing DR and BC plans together, emphasizing strategies for IT systems, applications and data. A plan focused on performing an agency's mission regardless of circumstances can prioritize recovery steps. Examples of this are identifying systems that cannot afford any downtime, specifying backup and retrieval procedures, and designating recovery teams.

2. Know your data

Agencies can start by assessing the types of data they have (i.e., structured, unstructured, in-house and social) and where it's currently stored. They should also learn about the compliance and privacy requirements for that data. Classifying data also will help inform risk assessments to ensure that DR procedures don't create vulnerabilities.



3. Integrate for agility

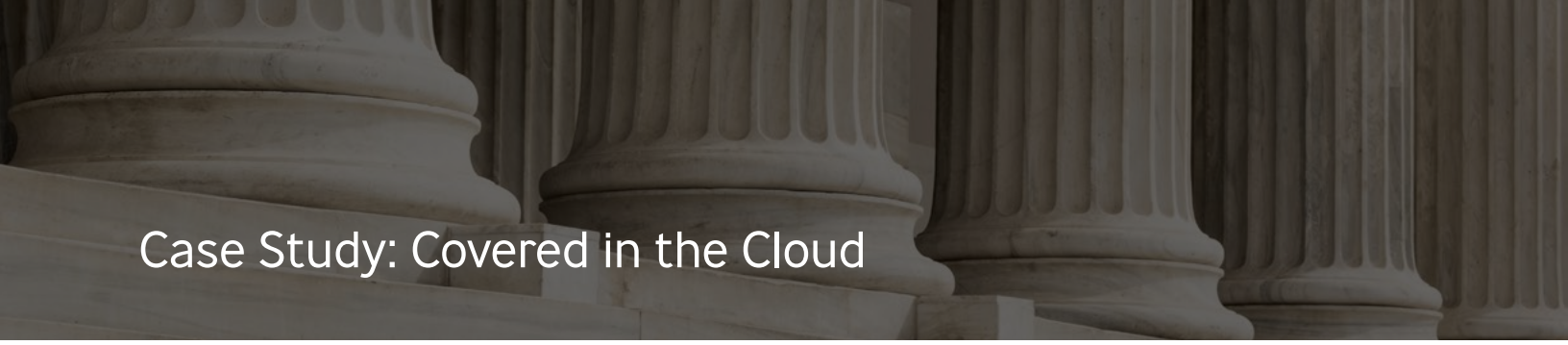
Choose a platform built for multi-cloud environments. It should be able to seamlessly replicate data across the environment, from on-premises core systems to public clouds and the edge, using cloud-native integrations. It should be able to seamlessly convert on-premises virtual machines (VMs) to the cloud, and consolidate management of data both on-premises and in the cloud on a single platform. Ease-of-use, as well as low network latency, should not be overlooked.

4. Follow policy

Policy-based automation will increase the efficiency of backups and replication in hybrid environments, allowing for faster response to and recovery from emergencies. It can simplify the management of distributed systems, better enabling integration, configurations and testing. And it can ensure that DR procedures adhere to an agency's disaster recovery plan.

5. Reimagine data management

Cloud computing has opened up new avenues for IT operations and data use, while adding some complexities to the network. Traditional, on-premises approaches to DR can't keep up. Agencies can move to simplify and automate data management with global visibility and provide direct access to data for third-party apps for security, insights and new innovations. Native integration with multiple cloud providers can solve data fragmentation problems, easily support hybrid environments, and enhance management by putting it into a unified platform and interface. By taking a path toward multi-cloud efficiency, agencies also can streamline their ability to recover from disruptions from virtually any incident – physical or cyber.



Case Study: Covered in the Cloud

Federal agencies have been making moves to the cloud for DR.

For example, one federal agency saw a need to move on from its legacy IT infrastructure. Itlacked DR capabilities and had legacy systems that were driving the agency into "technical debt," according to the agency's chief technology officer, speaking at an event last year focused on government cloud use.

Like other organizations, this agency had a troubled history of attempting to modernize systems in isolation, separated from the rest of the infrastructure. And like others, IT leaders found that this piecemeal approach didn't work effectively, in part because it ignored that system's interconnections with the agency's other systems.

This time around, the agency decided to take a comprehensive approach, upgrading a large chunk of its infrastructure. In the process, it paid off technical debt accumulated over 10, or even 20, years of maintaining older systems while neglecting to invest in new IT, the CTO said.

That led to adopting a cloud solution with AWS that integrates core systems and is future-proofed with continuous integration and deployment, and automated testing. It also enables the agency to implement an efficient DR operation that wasn't possible with its legacy systems. The move has paid off for the agency, according to the CTO, who noted that government data centers can't deliver the same security, scalability and efficiency that agencies can get in the cloud.

HOW COHESITY ON AWS CAN HELP

Cohesity on AWS can help you by simplifying your ability to address compliance, cost and speed of recovery objectives and let you stay focused on your mission. Cohesity provides a single, software-defined data platform and user interface that runs natively on AWS.

Data Protection & Rapid Recovery: Cohesity's hyperconverged, web-scale platform simplifies operations and eliminates silos while providing near-instant search and recovery for several Global 2000 companies and federal agencies, improving RTOs by using the DataPlatform indexing engine which enables rapid search-and-recover capabilities. Amazon S3 provides a resilient, secure and cost-effective storage location with 99.999999999% durability.

Compliance: The Defense Department (DoD), Intelligence Community and other federal agencies use AWS extensively by for cloud services due. AWS meets a robust set of federal and global compliance standards that can help agenciesdeploy new solutions faster. Itincludes Federal Risk and Authorization Management Program (FedRAMP) medium, FedRAMP high, and provisional authorizations under the DoD Security Requirements Guide (SRG) to provide services up to Impact Level 6, for Secret information. Cohesity's support for encryption in transit and at rest, near-instant search, and audit capabilities further help you protect and manage your data.

Savings: Cohesity on AWS can dramatically reduce total cost of ownership (TCO). Cohesity's data platform can replicate data from an on-premises cluster to the public cloud taking advantage of economies of scale. Raw storage costs are reduced by up to 96% with the Cohesity platform using intelligent storage tiering and optimal use of Amazon S3 storage classes (S3-IA, S3 One Zone, S3 Glacier, and S3 Glacier Deep Archive) for long retention at the lowest cost. Cohesity saves you time by managing everything through a simple to use interface, easy to deploy, features like near-instant search and recovery, and policy-based automation.

To learn more visit: www.cohesity.com/aws.

Conclusion

Disruptions caused by disasters and other events invariably are unexpected. They can result from anything, including cyber or physical attacks, natural disasters or public health emergencies. Regardless of the cause, agencies need to respond swiftly and surely to retrieve data and restore and maintain operations as close to immediately as possible. With so much of agencies' data in the cloud, cloud-based DR needs to work in concert with business continuity plans and agencies' policies.

While on-premises DR plans rely on local hardware for backup and recovery, cloud-based DR does not. It uses Cohesity and AWS to provide the speed, agility, scalability, compliance and cost-effectiveness that ensures integrated, efficient IT management from on-premises servers to the cloud and out to the edge of the Internet of Things (IoT). It can be a complex undertaking, but the right partnerships and the rewards of a software-defined infrastructure will be worth it — now and in the future.

ABOUT COHESITY

Cohesity eliminates mass data fragmentation with a single data management platform that radically simplifies the way organizations protect, manage, and extract value from their data. This web-scale platform spans clouds and data centers and uniquely enables organizations to run apps on the same platform, all managed from a single GUI.

To learn more, visit www.cohesity.com/solution/government

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