InnovationSpotlight

Simplify Cloud Data Management with a Flexible As-a-Service Solution

By not having to run a secondary data center, Cohesity Data Management-as-a-Service can save agencies at least 60 percent on storage costs.

Federal agencies have had a challenging time during the pandemic.

And by nature, these agencies are set up for stability – not for rapid change.

Cloud data management can help federal IT teams with the stress of the move to remote work; the official mandate to adopt zero-trust; the pressure to embrace cloud to save costs; and technical worker shortages.

With advancing IT capabilities, agencies also have a complex data puzzle to solve. Some have multiple data sets across dozens of networks and several storage facilities. Cloud data management can help there as well.

Cohesity built its Data Management-as-a-Service (DMaaS) solution with those stressors in mind. Their solution runs Cohesity's Helios platform over Amazon Web Services (AWS), offering federal agencies a simplified "single-pane-of-glass" view into agency data. Additionally, DMaaS is in the process of completing FedRAMP authorization.

> **"By running DMaaS over AWS, an agency can size up or size down more frequently and benefit from that decision."**
>
> *Sean Phuphanich, Solution Architect, Public Sector, AWS*

"We allow agencies to come to the table with what they already have," said Ron Nixon, CTO and CISO for federal at Cohesity. "They just want us to manage the data so they can concentrate on using it. With Helios the real advantage is that it's all on the same user interface, so we eliminate the silos between management and use."

"By running DMaaS over AWS, an agency can size up or size down more frequently and benefit from that decision," explained Sean Phuphanich, a solution architect for the public sector at AWS. "So the customers buy storage closer to their actual need – and they save time and effort because they are not managing physical storage."

Phuphanich pointed to at least two cases of "strong economics" for federal customers using DMaaS.

First, many federal agencies operate at least two data centers, a main data center and a secondary site that functions mainly for disaster recovery and backup. Phuphanich said that by storing the data in the cloud, agencies can save roughly 60-to-90 percent by not having to run a second data center and still get similar or better RPO/RTO objectives.

Second, agencies can save big by changing from physical tape archiving to all digital cloud archiving, said Phuphanich. Agencies with long term archives due to compliance requirements can have three decades of physical tapes – it's often petabytes of data. Now consider the growth rate of data we will see for the next 30 years. These tapes are not as durable as cloud storage and not deduplicated. By changing data archiving from physical tape to cloud, it allows you to use highly durable Amazon S3 storage. With that increase in durability it allows you to use a strategy of long term incremental backups, Phuphanich said. Over time, the cost savings due to less storage usage can reach 90%.

The security angle

Cohesity's Nixon said there's also a strong security argument for agencies to consider DMaaS. By having the same standards, application programming interfaces (APIs), and certifications for compliance purposes, agencies using DMaaS will have a much more consistent environment that improves their overall security posture.

Because the DMaaS platform with Helios offers a great deal of flexibility, agencies can opt to get very granular

with their security controls. For example, Nixon said if the agency wants to manage security and governance, Cohesity can support that – DMaaS will take care of the backup and disaster recovery while supporting the other aspects the customer wants to own. "We specify all these arrangements in the contract so everyone's responsibility is clear: the customer, Cohesity, and AWS," added Nixon.

Helios also uses artificial intelligence (AI) to analyze anomalous behavior inside of the archives to make sure there's no malware. Nixon said Helios offers additional indicators of compromise (IoCs) within an agency's data so federal IT administrators are made aware of any potential threats.

Phuphanich added that in the past, backup was a "one-and-done" job. But when security gets added into the mix, it's more of a process that evolves.

"It's not uncommon to see organizations run one or two versions behind when it comes to updating the features and security of their software," Phuphanich said. "When you're talking about a Software as a Service (SaaS) model, Cohesity updates the features and security of their software, so the agency can maintain their normal one-and-done focus in terms of setting up backup, but the management gets moved away from that team. I have not seen many teams be able to consistently manage security updates on their own. So if they can use a SaaS solution like DMaaS, they can leap forward and get back on track."

An added security boost from FortKnox

Cohesity also offers FortKnox, a SaaS data isolation and recovery product that runs over AWS that improves cyber resiliency with an immutable copy of data in a Cohesity-managed cloud vault via a "virtual air gap." Think of the virtual air gap as data stored offsite in a "digital vault" that hackers can't infiltrate.

Nixon explains the real value to agencies facing today's threat landscape: by storing the data in the virtual air gap offsite, FortKnox offers added protection against ransomware because it's now not possible for the attackers to get to the archived data.

Ransomware has evolved to the point where the attackers don't just encrypt the victim's files. It's not a single attack, it's a campaign: First they exfiltrate data, then they delete the backup, and finally, the attackers encrypt the files so the organization gets forced into paying the ransom.

"What we're trying to do with this product is push this back to where the attackers were in the first place," Nixon explains. "With FortKnox, the attacker can't get to the archives or back ups you use to recover. This severely limits the impact, scope and length of the attack."

> **"With FortKnox, the attacker can't get to the archives or backups you use to recover. This severely limits the impact, scope and length of the attack."**
>
> *Ron Nixon, CTO and CISO for federal, Cohesity*

Here's how FortKnox works in real life: When security teams need to safely deposit data to the cloud vault or recover it quickly following an attack, Cohesity establishes a temporary and highly secure network connection that limits access to the isolated data by the attackers and unauthorized insiders, while simultaneously supporting business service-level agreements. The security team can manage the data without disrupting daily operations.

Other security benefits

There are a couple of other security benefits from DMaaS worth mentioning. Nixon said many agencies also like that they can integrate DMaaS into existing security tools. So if they use Splunk or Palo Alto Networks, they don't have to change their tools.

One final benefit: Because AWS has data centers globally, agencies no longer have to worry about natural disasters such as floods, hurricanes, or earthquakes. If something bad happens in a region where there's a federal data center, AWS will always have other systems they can call on – so agencies can keep working.

Talk about peace of mind.

To learn more on how the Cohesity and AWS DMaaS solution empowers Federal agencies to accelerate migrations, simplify hybrid cloud data management and eliminate silos visit www.cohesity.com/fed-dmaas