FEDInsider

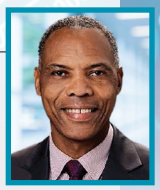
4 Things to Focus on in 2021 to Improve Multi-Cloud Data Protection

Contributors:

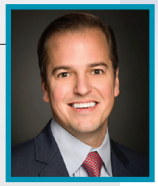
- **Jeff Lush**
  Chief Information Officer, United States Air Force Air University

- **Vijay D'Souza**
  Director IT & Cybersecurity Team, U.S. Government Accountability Office (GAO)

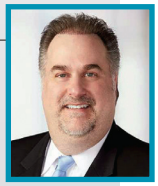
- **Greg Edwards, Ph.D.**
  Sr. Advisor to the CIO, FEMA



- **Justin Ciaccio**
  Director of DoD, SLED & Commercial Sales, ViON Corporation



- **Cameron Chehreh**
  Chief Technology Officer & VP, Federal Systems Dell Technologies



Federal IT leaders are taking an aggressive approach to cloud adoption with more than 75% of federal agencies now working in a multicloud environment. As the past year has demonstrated, the flexibility of cloud has been instrumental in enabling new ways of working. Many agencies were able to seamlessly shift to remote working overnight in the wake of the pandemic. However, with this change came a renewed focus on concerns about data security, privacy and confidentiality issues, especially surrounding the data that employees are accessing on the edge.

We spoke to a panel of federal government IT experts recently to hear their insights into how agencies can improve their security posture in a multicloud world. Below are four recommendations they shared that you could also focus on in 2021.

Ride the New Wave of Government Modernization

The Biden administration has proposed increasing the budget of the Technology Modernization Fund (TMF) from $25 million to $9 billion – a more than 3,000% increase. This includes funds in the COVID-19 relief plan, plus another $1 billion targeted to improve security monitoring and incident response. Funds can also be used for hiring IT experts and expanding GSA technology programs.

"I would encourage agencies to utilize these funds to refactor their applications that are running on proprietary technology," says Justin Ciaccio, director of sales, ViON Corporation. "There are companies out there that will take your mainframe workload while you work to refactor your software to get onto different platforms."

Agencies can borrow from the TMF to redesign their applications, upgrade or phase out the proprietary technology, and then migrate the applications to a new cloud platform. The savings from cutting maintenance costs on outdated IT infrastructure, reducing spend on software licenses, and lowering operational expenses can then be used to repay the TMF loan. Anyway you look at it, the time to modernize is now.

Focus On Your Security Responsibilities for All Cloud Deployments

One key issue they identified by the Government Accountability Office as a barrier to implementing cloud solutions at agencies was a lack of clarity regarding security responsibilities. According to a GAO report on FedRAMP deployments, many agencies were unclear about their security responsibilities compared to those taken on by their cloud providers.

One way to help the situation is to standardize security requirements so that agencies can use the same template regardless of what kind of cloud is being created or what cloud provider is being used. By focusing on and defining agency security responsibilities, it eliminates any surprises or vulnerabilities down the road.

"The extent to which you can try to standardize your security requirements will make it easier for both federal and state agencies to implement," says Vijay D'Souza, director, IT and cybersecurity issues, GAO.

To further standardize and simply deployments, Cameron Chehreh, CTO and vice president of Dell EMC Federal, says there are three rules to follow when determining the structure of a multicloud environment. They include:

- The law of economics: consider where the workload needs to sit and how it connects to any legacy infrastructure and the cost associated with where that data resides. Does that workload belong in the public cloud or on-prem? How often will I be accessing it and what are the costs associated with that.

- The law of physics: computers are only so fast, so determine how much power and capacity is needed to provide end users a quality experience with any given application.

- The law of the land: address all the statutory or regulatory and compliance requirements and how they affect where the data and the workloads reside, and plan your cloud deployment accordingly.

Leverage Cloud Services to Improve Your Security Posture

When thinking of how to protect data, it all starts with how end users access information and applications. Through such technologies as software-defined networks, it becomes possible to push things like software-based firewalls closer to the workloads and shape network traffic in a sustainable way. Many agencies are finding that moving their transactions and services to a cloud or multicloud environment actually helps reduce the security workload automatically.

"First of all, you have to get all of your stuff to the cloud, and that's quite a feat," says Jeffrey Lush, CIO, U.S. Air Force Air University, the service's center for professional military education. "But once it's moved, we also have reduced our security threat."

Lush explained that most of the cloud deployments at the Air University are done to keep his ATOs current. However, there is nothing wrong with taking advantage of the established barriers within the cloud to gain extra cybersecurity protection.

For example, with cloud services, "you can look at the work environment where users are logging in from and control what access they have to data based on that location," says Dell's Chehreh. "If I can determine someone is logging in from their favorite coffee shop, they may only get access to certain prescriptive workloads. When I detect they're on their home network, a better, more private setting, I can release access to more data and applications."

Ensure Data Security in a Mobile Cloud Environment

The future work environment requires that agencies utilize cloud applications and mobile services– not in the coffee shop sense, but capabilities that can be extended beyond normal boundaries. For example, there are many requirements for field work or communications in an active DOD theatre. This sort of scenario applies to the military services and other federal agencies, such as the Federal Emergency Management Agency and the Department of Defense. When a disaster strikes – hurricanes, wildfires, flooding, blizzards, or anything a region may face – a big part of FEMA's response is establishing secure communications and connectivity. The initial effort is to extend federal connectivity to the location, which provides network resilience.

"We can use the empty backbone to reach out to those brick and mortar sites that might be near a disaster location," says Dr. Gregory Edwards, senior advisor to OCIO, FEMA. "If we need to go further, we release our mobile emergency response vehicle. With this mobile service in place, we establish diverse communication paths into that location, back to the headquarters, back to our on-premise data center, and back to our cloud data centers. We talk in terms of extending our data centers to that edge."

Federal agencies are increasingly adopting Cloud Smart recommendations to accelerate cloud adoption and improve their security posture across the enterprise. With an increased focus in 2021 on technology modernization within the federal government, it's the perfect time to look at what steps you can take to protect your data and leverage the advantages of a multicloud world.

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
www.FedInsider.com
@FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

ViON
196 Van Buren Street, Suite 300
Herndon VA 20170
Contact: Justin Ciaccio

(571) 353-6000
info@vion.com
www.vion.com
@vion-corporation_2
@ViONcorp