MeriTalk
Improving the Outcomes
of Government IT

Underwritten by:
ViON
Building your enterprise solutions

Federal Cloud Growth Puts Spotlight on Proactive Multi-Cloud Security

With Federal government cloud spending on the rise, and four out of five Federal IT decision makers saying their agencies use multiple cloud platforms to satisfy different IT needs, cloud management capabilities are becoming more important than ever.

Tackling the complexity of multi-cloud security is easier said than done, and with the rise of ransomware and malware attacks infiltrating Federal remote networks and endpoint devices, few IT decision-makers are confident in their ability to keep all platforms secured.

Survey respondents said this concern stems from a host of challenges connected with multi-cloud management. Those include budget constraints, difficulty meeting Federal requirements, lack of a skilled workforce, and increased attack surfaces.

Agencies need to adjust their security models from a reactive stance to a proactive posture in order to identify and address security risks *before* attacks occur, rather than mitigate the impact after a breach.

Some reactive security methods such as firewalls and log shipping lead to a "lengthy threat remediation and/or recovery time," said Ray McCay, vice president of Solution Sales, ViON Corporation.

"I've heard of organizations taking six to 18 months from the original point of discovery to complete remediation and recovery back into operations," said McCay. "This is unacceptable. During this time there are potential open windows for attack, insider threat issues, and even sensitive data exfiltration and leveraged exploits."

It's a Process, Not a Product

To secure multi-cloud environments, it's important to first understand the difference between "the security of the cloud and the security in the cloud," said Eric Trexler, vice president of Global Governments and Critical Infrastructure, Forcepoint.

"Security is a process, not a product," said Trexler. "You can't buy a product from a cloud service provider that says you're secure. You need to work through it with security, with IT, with business operations, and see the cloud service provider as the integrator. There's a lot more to do and Federal IT teams need to think about it in that context."

Federal security regulations like the National Cross Domain Strategy Management Office (NCDSMO)'s Raise the Bar (RTB) guidelines boost the security architecture bar for Cross Domain Solutions beyond the National Institute of Standards and Technology (NIST) Risk Management Framework controls, and emphasize guard solutions that transfer data and files between segmented cloud networks.

In addition to utilizing proactive multi-cloud security methods, the Cybersecurity and Infrastructure Security Agency (CISA) released over 20 recommended strategies that organizations can take to strengthen cloud security practices against attackers, such as securing privileged access and focusing on threat awareness and training.

Putting the Human Front and Center

To combat advanced threats from malicious actors and reduce risk, the Department of Homeland Security (DHS) has embraced human-centric cybersecurity with zero trust security concepts to protect its multi-cloud environment. Human-centric security focuses less on the threat, and more on the people who are using the data and the data itself. With zero trust, an agency can better understand what they're doing with the data, the value of the data, and the risk equations associated with the data.

By implementing human-centric and zero trust security in their multi-cloud environments, the agency is focusing more on the data, said Luis Coronado, Jr., executive director, IT Operations, at DHS in a recent webinar.

With this new approach, the agency can track user activity within a particular document, "whether they're sending it out and sharing it and then once it goes out to that person, are they sharing it out? Are they trying to get around the ability for them to share it," explained Coronado, Jr.

As agencies move operations toward multi-cloud, they should evaluate the built-in tools that may exist within each cloud environment in addition to outside tools that can enable a human-centric cybersecurity.

"It allows our analysts to be able to focus on the things that matter, versus just constantly looking at a monitor and not really knowing what's going on," added Coronado.

As remote work remains prevalent and cloud migration increases, threats and attacks will continue to advance. But strengthening multi-cloud security doesn't have to be a difficult process when IT teams focus on your people, said Trexler.

The agencies who have had the most success migrating to cloud have a cloud management office of some sort, Trexler said, that manages cloud environments across the agency, provides visibility into what resources are available, and establishes a system of continuous monitoring.

With these tools in place, "you can focus on your people and see how they're working with the applications to better protect the business," added Trexler.

"There's a lot of IT in these equations," said Trexler. "When you break it down to people and data, it makes the [multi-cloud security] problem so much simpler."

Learn more.