leidos

The Cloud Conundrum

Addressing the Risks and Rewards of a Hybrid IT Environment

On February 8, 2011, the Obama Administration released **a document** that would revolutionize the way government agencies store and process data: The Federal Cloud Computing Strategy called for agencies to adopt a "Cloud First" approach to "maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost."

Almost a decade later, the Office of Management and Budget agreed that this strategy was due for an upgrade. While "Cloud First" empowered agencies to adopt cloud-based solutions, it left many with more questions than answers. A **newer iteration** of the Federal Cloud Computing Strategy, known as "Cloud Smart," promises to answer common questions by equipping IT leaders with the tools they need to navigate the nuances of modern cloud adoption.

Still, many agencies are unsure about what cloud environment is right for them. Hybrid and multi-cloud environments, for example, offer flexibility and scalability to meet today's complex challenges.

"Given everything that happened last year, the need for remote access was quickly enabled by moving to the cloud," says Lakshmi Ashok, vice president of enterprise management at Leidos. "Each cloud provider has their own unique [capabilities]. So why not move to the [hybrid] cloud ... to get the best of breed, adopting optimum services [from each]."

Ashok, who has spent over 20 years delivering IT services and solutions to agencies across the federal government, explains that hybrid and multi-cloud environments offer both opportunities and risks.

"There are multiple areas we need to be cognizant of as related to providing end-to-end security in the cloud, especially based on zero trust principles," she explains.

However, with the proper frameworks in place, IT leaders can manage these security challenges and confidently move toward a hybrid cloud environment.

Hybrid and multi-cloud environments offer flexibility and scalability to meet today's complex challenges, but they also present some significant security risks. With the proper frameworks in place, IT leaders can manage these security challenges.

What You See Isn't Always What You Get

One of the most prevalent challenges of hybrid cloud adoption among IT leaders is limited visibility into the enterprise, says Ashok.

"The lack of consistent tooling and consistent control in a hybrid environment makes it very, very difficult to not only react to what's happening but actually be proactive," she explains. "It inhibits rapid decision making, especially when a security incident occurs."

“Given everything that happened last year, the need for remote access was quickly enabled by moving to the cloud.”

Lakshmi Ashok
Vice President
Enterprise Management
Leidos

Learn more about how Leidos is building solutions for secure cloud adoption.

leidos

The good news? There are ways around this visibility roadblock. In fact, Ashok and her team at Leidos have created enterprise-wide dashboards on a standard open framework to enable end-to-end visibility of incidents. These solutions, paired with artificial intelligence, aim to reduce the noise when it comes to alerts so that IT analysts can isolate root causes and stop threats in their tracks.

Educating the Workforce

Before organizations can employ specific solutions and capabilities, they must arm their personnel with the knowledge and expertise to address these complex challenges. Although “the cloud” has been around for decades, Ashok notes that many organizations still don’t have a solid understanding of what it actually means for their mission. That’s especially true in instances of a shared responsibility model, where security responsibilities fall on both cloud providers and their users.

“Cloud service providers offer security solutions up to a certain level, and then we need to manage [and] secure the [operating system], the network, applications, identities and so on and so forth. And this varies for whether we’re doing infrastructure-as-a-service platform or software-as-a-service,” Ashok explains.

Failure to comprehend this shared responsibility model can lead to a number of severe consequences, such as breach of non-compliance and increased costs. Ashok recalls one user, for instance, that exposed thousands of sensitive DOD records when they incorrectly secured an **Amazon Simple Storage Service**. Moving forward, to prevent these instances from occurring, Ashok recommends building guardrails, such as secure landing zones, with policies that can counter common mistakes — intentional or not.

A Place for Cloud Security in the Future of Work

There’s a new generation entering the IT workforce, and they’re bringing with them new ideas and mindsets. For example, recent studies show that, in general, members of Gen-Z **value independence** at work more than other age groups.

“They want flexibility, they want the ability to self-service,” Ashok says. And, with an increasingly remote and hybrid workforce, this independent mindset is becoming the new norm. While this move toward independent work offers many benefits (more control over one’s schedule, for one), it can also prove detrimental for security.

“This increasingly independent work structure leads to shadow IT outside of typical IT governance, where staff members are using systems and software that IT teams haven’t approved,” Ashok explains. “This opens the door to security vulnerabilities.”

Proactively implementing security protections, however, can help mitigate these challenges.

“Putting [in place] the right guardrails, while ensuring a good customer experience and giving independence to users is vital to success,” says Ashok.