PRESIDIO® FEDERAL

IBM Gold Partner

Protecting Federal Data in a Multi-Cloud World

Protecting federal data in a digital-first world doesn't have to be complicated.

Citizens can purchase cars, houses and even their daily groceries from the comfort of their homes. However, interacting with the government often lacks the same convenience — as government services are still predominantly paper-based. While some agencies like the Internal Revenue Service (IRS) are piloting new digital services, many government services remain inaccessible via the World Wide Web.

Shifting toward digital-first services is a gargantuan task for the federal government. Defining, designing and building cloud-native systems can take years. As such, many federal agencies look toward multi-cloud solutions as a way to simplify digital transformation.

"Cloud independence is essential to digital transformation," said Philip Carruthers, Cyber Domain Strategy Leader for IBM Public Sector. Multi-cloud solutions can speed up digital transformation, simplify deployment and provide teams with the flexibility needed to meet mission demands, all without being locked to a specific cloud service provider (CSP).

Though moving information from data center to cloud can cost agencies a small bit of control over service delivery for issues like up-time and bug patching, cloud-based solutions provide more benefits than drawbacks. For example, enhanced efficiency and greater flexibility are both documented benefits of leveraging cloud computing for service delivery.

As government leaders move applications and workloads to the cloud, now is the time to invest in a holistic cybersecurity strategy, connecting multi-cloud applications back to the core enterprise and understanding the risks associated with digital transformation.

Advanced persistent threats (APTs) aren't waiting for the government to secure data. In 2023, threat actors sought to leverage common vulnerabilities and exposures (CVEs) in multi-cloud environments.

"We see agencies buying software, pulling it out of the box, turning it on and then leaving it," Carruthers said. "In that situation, the question becomes, what APT have I left myself open to?"

Invest in the basics

APTs have a wealth of resources at their disposal. Exfiltrating federal data often becomes a game of what CVE could hackers exploit to gain access — a game that's now been simplified due to generative artificial intelligence (AI).

Agencies can fight back. Generative AI, while new, could be used by agencies to increase autonomous red teaming to close gaps in the environment. While AI and machine learning (ML) will help agencies defend against next-generation threats, leaders cannot forget that protecting federal data starts with investing in the basics.

"We've changed the conversation," Carruthers said. "We need to focus on doing the basics in cybersecurity first and then adding in and bringing along AI/ML capabilities."

Existing standards like NIST 800 53, OMB M-21-31 and Executive Order 14028 all focus on the need to secure federal systems using current capabilities and protocols. What's more is these directives underscore the importance of understanding who and what is on the network. Government leaders must shift from traditional, perimeter-based security to a more in-depth, intelligent form of sensing.

Intelligent forms of sensing, coupled with automation and continuous red teaming could help leaders address CVEs before APTs find their way onto the network, but investing in the basics is crucial. Government leaders must adopt zero trust models before onboarding emerging technologies.

Planning for a more secure future

Establishing robust zero trust models and building guidance for a multi-cloud environment are some of the immediate needs facing government agencies. Thankfully, there is a wealth of resources available that government agencies can leverage to learn how to enhance cybersecurity efforts on-premises and in the cloud.

In terms of mitigating existing risks, agencies should look toward partnering with industry leaders to better understand how a certain technology might impact their technology stack.

“Buying software, pulling it out of the box, turning it on and then leaving it isn’t the solution. You’ve got to get experts like Presidio Federal who can come in when you purchase software and help you plan that configuration,” Carruthers said. “You want to implement the configuration and then make sure it’s current and that the software revisions are taken care of and that if something’s changed in the environment, changes occur.”

As government leaders within the Security Operations Center (SOC) work toward building secure multi-cloud environments, policy leaders should focus on acquiring funding for future programs associated with emerging cybersecurity techniques.

At present the federal government does not have any plans, programs or government-wide funding associated with leveraging emerging technologies for cybersecurity efforts — certain directives exist but funding for deploying AI/ML or generative AI doesn’t.

To protect and defend the digital infrastructure of the United States, lawmakers must invest in cybersecurity at the speed and scale of the mission. Agencies simply cannot afford to wait. Executive leaders must have candid discussions with their SOC about the threats they face and the resources they need to effectively protect and defend data.

Unfortunately, countless original equipment manufacturers and small businesses clamor for the attention of federal decision-makers, making it difficult for leaders to sort through the noise.

By partnering with a trusted industry leader, agencies can cut through this noise to secure federal data and plan for multi-cloud solutions that fit the mission, vision, values, and goals of the organization. Together, securing federal data doesn’t have to be complicated.

“Protect your data at all costs and engage experts,” Carruthers said.

There is an urgent need for federal agencies to prioritize cybersecurity in multi-cloud environments. Connect with our team of experts at Presidio Federal and IBM today to discuss adopting a zero-trust model and integrate intelligent sensing to defend against cyberthreats.