Securing Federal Cloud Infrastructure with Cloud Security Posture Management

As agencies adopt mandated cloud security requirements, they’re looking for a platform that can unify compliance and cybersecurity.

The federal push to cloud is an ongoing journey, and security remains a key component of cloud adoption. In fact, the Cybersecurity and Infrastructure Security Agency’s (CISA) Cloud Security Technical Reference Architecture v.2 strengthened its guidance to meet cybersecurity standards in the administration’s “Improving the Nation’s Cybersecurity” Executive Order.

The reference introduces the concept of Cloud Security Posture Management, and how capabilities associated with CSPM can facilitate the implementation of zero trust architectures. To discuss CSPM implementation, threat detection, data security, visibility and more, members of government and industry recently spoke at a FedInsider panel to share their expertise.

FEDERAL CLOUD SECURITY BEST PRACTICES IN ACTION

As agencies continue to implement their cloud strategies, they’re turning to known cybersecurity best practices to identify and remediate risks in the cloud. While many of these practices weren’t known years ago when the U.S. Citizenship and Immigration Services (USCIS) first began implementing cloud, its Chief Information Security Officer Shane Barney said the agency has since adopted strategies in response to the cloud to enhance its security program operations.

“It’s driving more threat hunting, the threat modeling, and how you operate the security organization,” Barney said. Rather than just adhering to compliance, USCIS had to rethink how security is applied to advance cloud capabilities.

“There’s a lot of automation we employ, and one of the things that comes out of the cloud is the unbelievable amount of data that flows from it,” he said. Ten terabytes of log data a day drove changes in USCIS’ workforce, so Barney said they took a developer mindset. “Because, if your infrastructure and your environment is code, then your security needs to be code too,” he said.

USCIS changed how it trained its workforce, including operations, which was critical for integration of risk-based approaches to managing and governing its cloud presence. It was important everyone understood how to react, respond and monitor in case of an incident. “As you move forward in the cloud, embracing a risk-based model is absolutely critical,” Barney said.

IN NEED OF A UNIFIED CLOUD SECURITY APPROACH

CISA’s TRA v.2 intends to bridge that gap between cybersecurity and compliance, which Jeffrey Lush, chief information officer for the U.S. Air Force’s Air University, said should be the same. “The bottom line is how we manage and sustain this for the long haul,” he added.

The reference includes adopting a security model that includes zero trust, security management and sustainment. “It becomes a very interesting model,” Lush said.

From an industry perspective, Brian Davis, federal district sales manager for Prisma Cloud at Palo Alto Networks, said he’s focused on ensuring secure and compliant effective management of federal cloud footprints.

“We are leveraging cutting-edge technology, processes and approaches to reduce the burden of maintaining a cloud security architecture,” Davis said. This approach can be done across single, hybrid and multi-cloud environments, integrating previously disparate teams across...
agencies. This way, technology is being leveraged to bring together development and security operations.

And when it comes to CSPM, it’s about bringing together visibility, compliance, governance, threat detection and response, as well as data security and integrity.

CLOUD SECURITY POSTURE MANAGEMENT
Davis said agencies are looking to CSPM because they need a single solution to support all versions of their cloud infrastructure, with a unified view of the entire cloud footprint with customizable policies and compliance standards.

“What can you get out of the box that will check and take care of all of that, and take it off your plate so that you can focus on threat hunting and going after more advanced scenarios?” Davis asked. The answer is prebuilt and customizable policy options that are extremely important to agencies, and for the entire service pipeline. CSPM extends that from code to cloud.

In terms of visibility, CSPM platforms also provide machine learning-powered, intelligence-based detection and visibility with contextual insight so agencies can effectively address misconfigurations and vulnerabilities. For instance, Palo Alto Networks’ CSPM platform ingests security logs and other third-party integrations to create advanced analysis and detect known and unknown threats. It can aggregate, analyze and sort through data for the user – alerting them to anything out of the ordinary.

CSPM can also detect misconfigurations of security groups with an automated system of policies to ensure users adhere to identity access management policies. If the system doesn’t meet the minimum password requirement, for instance, “It should be stopped automatically, if possible, and then made a high priority for your teams to be able to respond to it,” Davis said.

And visibility, Barney added, is also critical for protecting assets. “You need to determine when that asset is operating outside of what you would consider normal for that role. That is really what it’s about – determining that norm and figuring out where things are different.”

INTEGRATING CSPM & AUTOMATION TO SECURE FEDERAL CLOUD ENVIRONMENTS
Visibility is a foundational piece from which agencies can build and grow their capabilities, according to Davis. From there, agencies can automate security flaws like trusted IP addresses that are exposed so that IT managers can focus on more important tasks.

“It starts with visibility to automation and having technology support the people on your team to be able to offload the heavy lifting and really get down to the stuff that is really valuable,” Davis said.

Barney said a major benefit to visibility and automated monitoring is quick detection and response to incidents. “The cloud environment is a data heavy environment – especially for security teams,” he said. “So, investing heavily in security information early on is important.”

CSPM also loops in zero trust applicability. Davis said zero trust is about identity, devices, networks and data. CSPM is an application configuration that monitors activity in real time so that IT managers can investigate with context, come up with a decision and respond as quickly as possible to any incident, misconfiguration or threat.

It also helps with identity management, a big component of zero trust, Davis said. As a platform, CSPM enables automated monitoring, validation and compliance specifically tied to many areas of zero trust. So it can act as a powerful assistant as agencies move along that long road towards fully implementing a zero trust architecture, Davis added.