Swish | Check Point SOFTWARE TECHNOLOGIES LTD.

The Cloud Conundrum: How Federal Agencies Can Stay Secure Amid Modernization

With more employees working from home and multiple cloud infrastructures at play, federal agencies are turning to adaptive cloud security solutions to keep systems and staff safe.

When it comes to cloud security, federal agencies can never be too careful. With sensitive information that can be compromised without the right security policies in place, organizations must take specific precautions to protect their information.

These security challenges have been heightened by increased cyberthreats over the past several months as malicious actors use the global health crisis as an opportunity to target first responders, healthcare facilities and government agencies. According to the FBI's Internet Crime Center (IC3), reports of cybercrime have quadrupled since the COVID-19 pandemic began.

Now, federal agencies are looking critically at their security infrastructure, employing advanced tools and technology to prevent these attacks as they navigate the IT realities of a more remote future. Here are the steps they need to take to get there.

Prioritize Cloud Security in the Age of Remote Work

With more federal employees teleworking, a growing number of agencies are moving to multicloud and hybrid environments that offer increased flexibility and scalability as IT needs change. With users working from various endpoints, IT leaders must move data deployed on-premises onto multiple clouds. As these resources become more readily available and accessible to users, securing the cloud is imperative to maintaining a productive remote workforce.

But deploying an effective cloud security model is easier said than done. According to a recent report from Check Point, Swish and Cybersecurity Insiders, 34% of security operations centers cite compliance as their biggest challenge to date. Meanwhile, 33% say the lack of visibility into security infrastructure makes it difficult to get things done. As more agencies move to multicloud environments, gaining visibility into the security of all of their cloud components becomes a greater challenge.

34%
of security operations centers cite compliance as their biggest challenge

33%
say the lack of visibility into security infrastructure makes it difficult to get things done

So, how can they achieve consistency across multiple environments? By leveraging adaptive cloud security tools that evolve as the cloud does.

"When you're dealing with so many cloud environments, it's critical to have security systems that offer complete visibility and oversight of everything you're working with," said Glen Deskin, head of engineering for Mid-Atlantic and Federal at Check Point Software Technologies. "And that's only possible with governance and compliance tools that allow you to monitor these cloud environments at a high level."

Maintain Consistency Across Platforms

Attaining this level of visibility and compliance is only possible with the right strategy. According to Deskin, agencies can begin working toward that goal by streamlining security across platforms. Agency leaders agree: In a recent report conducted by MeriTalk, 89% of federal IT decision-makers identified consistency across cloud platforms as a key priority for secure multicloud adoption.

Before they can reach this level of consistency, organizations must understand the different components they are using to support their security infrastructure.

“It’s as much about social maturity as it is about technology maturity. Think about how your teams work together. How they share information, collaborate and problem-solve. The key is working together to become experts on the tools and technologies that will improve security at your agency.”

SEAN APPLEGATE, CTO AT SWISH DATA

“One of the biggest challenges organizations face is the utilization of too many different products, technologies and vendors,” Deskin continued. “That may have worked in the past, but it doesn’t meet the security demands of today. In fact, studies show that the more products an agency implements, the less secure their infrastructure is.”

These disparate systems and technologies can also negatively impact how an agency manages threats. Products that aren’t integrated into a single workflow often rely on various threat intelligence platforms, which can complicate the process of detecting an attack and lead to inaccurate mitigation tactics.

Sean Applegate, CTO at Swish Data, says agencies can overcome these challenges by deploying shared threat intelligence across all of the various platforms.

“With shared threat intelligence, organizations can more effectively streamline their incident response,” he said. “More importantly, this approach enables security operations centers to see and react to threats as quickly as possible.”

Move from a Detection Mentality to a Prevention Mentality

Managing a successful cloud security infrastructure will also require federal IT leaders to be proactive about managing threats. That means going beyond detecting a potential security breach or responding to a threat. Instead, it will require them to design policies into their cloud security infrastructure that prevent attacks.

Applegate recommends integrating a universal, consolidated policy based on specific user access, which would allow agencies to effectively protect against threats by monitoring each user’s access.

“This type of policy is dynamic in nature, meaning it understands what type of device the user is accessing and where they are located,” he said. “It then applies specific security implementations to each platform the user has access to.”

But successful cloud security is about more than just technology — agencies must also ensure their staff knows how to use these tools effectively.

“It’s as much about social maturity as it is about technology maturity,” Applegate said. “Think about how your teams work together. How they share information, collaborate and problem-solve. The key is working together to become experts on the tools and technologies that will improve security at your agency.”

Find out how Check Point and Swish can help you modernize your cloud security infrastructure with CloudGuard. To learn more visit checkpoint.com and swishdata.com.