MeriTalk
Improving the Outcomes of Government IT

REDSEAL

Solve the Cloud Security Conundrum With Deep Visibility Into Hybrid Environments

Prior to the COVID-19 pandemic, about 80 percent of Federal agencies were using more than one cloud platform[1], and 85 percent said the pandemic amplified the importance of moving to a hybrid cloud environment[2] in order to improve government resiliency. The Biden administration's May 2021 cybersecurity executive order[3] further amplified the push for cloud computing, as the president called on agencies to accelerate their movement to secure cloud services.

Multi-cloud can bring multiple benefits to agencies[4]:

- Increased performance
- Reduced risk
- Increased reliability
- Reduced cost
- Increased flexibility

Multiple Clouds Introduce Security Complexity

Multi-cloud also increases the complexity of cloud and hybrid environments, and as a result, can introduce security vulnerabilities, such as cloud resources that are exposed to the internet or don't comply with security mandates.

Federal IT leaders are working to address the security challenges inherent in multi-cloud adoption, but more than 40 percent say cybersecurity strategies are not evolving fast enough to keep pace with evolving multi-cloud environments[5].

Agencies face multiple stumbling blocks:

- A skills gap. Many agencies began their cloud journey with a single cloud provider. Now, their IT staff must learn how to manage and secure clouds from multiple providers, or they must hire experienced personnel

- Inter-cloud connections and data security. An agency may want to use Google Cloud Platform for an artificial intelligence application, for example, and connect it to Microsoft Azure so that developers using Azure can leverage the AI data. IT teams may have trouble connecting multiple clouds – or identifying cloud connections that should not be allowed. Security teams may not be familiar with the security controls of each cloud and how to configure them

- Visibility into the entire cloud and on-premises environment. As agencies move toward zero-trust architectures, they must identify everyone and every device on agency networks, determine what access permissions those people and devices have, and close security gaps. It's a massive task that often requires additional staff

- Management of tens or even hundreds of security tools, many of which are specific to one cloud

A series of steps can help agencies overcome these stumbling blocks:

- Leverage industry partners to help fill the skills gap

- Engage security and networking teams from the beginning. Embrace the concept of "shift left" to make security a part of the cloud development from the outset. Security and networking don't want to block cloud resources – intentionally or inadvertently. They want to enable cloud securely without negatively affecting the agency business or mission

1 Multi-Cloud Defense: Redefining the Cyber Playbook
2 Hybrid at Hyperspeed: Cloud Strategy for the New Reality of Government
3 Executive Order on Improving the Nation's Cybersecurity
4 Juggling the Clouds: What Are Agencies Learning?
5 Multi-Cloud Defense: Redefining the Cyber Playbook

- Implement technology tools that can provide broad and deep visibility into cloud and hybrid environments to ensure IT teams know who and what is on agency networks and can identify and remediate security vulnerabilities

Visibility Across the Entire Agency Environment Helps Close Security Vulnerabilities

In a recent study, 93 percent of Federal multi-cloud users said they have taken steps to improve visibility into their multi-cloud environments. However, just 37 percent said their current visibility is excellent[6]. As cloud deployments grow - bringing more subnets, instances, and security rules - it becomes hard to visualize the full cloud inventory and the access it provides to agency resources. As clouds connect to other clouds and physical networks, it becomes even more difficult to identify access permissions, misconfigurations that could expose cloud resources to the internet, and resources that attackers could reach.

The implications of visibility gaps are clear: Organizations with the most problematic visibility are experiencing twice as many cybersecurity incidents[7].

Greater cloud visibility has immediate benefits:

- Cost savings. Agencies can identify cloud resources that were spun up but aren't in use, or are underutilized
- Better cybersecurity. Agencies can't protect assets that they can't see. Improved visibility means IT and security teams can identify vulnerabilities faster and take corrective action
- Validation of compliance with security mandates, such as NIST security controls and Payment Card Industry Data Security Standard requirements

6 Multi-Cloud Defense: Redefining the Cyber Playbook

7 As IT Complexity Increases, Visibility Plummets

To realize these benefits, agencies need a cloud security solution that can identify:

- Exactly what resources exist and where they are, across public clouds, private clouds, and on premises infrastructure
- If any of those resources are unintentionally exposed to the internet
- What access is possible within and between clouds and on-premises environments
- The riskiest vulnerabilities in the cloud, so they can be remediated first
- Whether cloud deployments align with security best practices
- Whether cloud network segmentation policies are in place

RedSeal Provides the Broad and Deep Visibility Agencies Require

RedSeal's cloud security solution brings an agency's network environments – public clouds (AWS, Microsoft Azure, Google Cloud Platform, and Oracle Cloud), private clouds, and on-premises infrastructure – into a unified security architecture that enables IT teams to view and query the entire network for security risks.

The RedSeal platform benefits all IT professionals, regardless of their cloud expertise. It interprets access controls across multiple clouds and provides a dynamic visualization of the entire network so everyone can understand what is on the network and how it is configured, whether resources should be connected to each other or exposed to the internet, and why. It also integrates other security tools into a common platform, for a truly comprehensive view of the agency's assets, configurations, and potential vulnerabilities.

The result is better security – and efficiency. Previously, it could take hours or days to determine whether cloud resources should connect to each other. With RedSeal, IT teams can have that information in minutes and understand the severity of the risk, so they can prioritize remediation.

To learn more about RedSeal's cloud security solution, visit:

https://www.redseal.net/cloud-security/.