How to Take Control of Your Cloud Operations

MARKET TRENDS REPORT

govloop

E-INFOSOL LLC
INNOVATIVE SECURE IT SERVICES & GREEN SOLUTIONS

aws

Introduction

With the speed and relative ease of implementing cloud services, federal agencies' cloud infrastructures can quickly grow bigger than their ability to control them. Over time, agencies can feel overwhelmed by hybrid and multi-cloud environments.

There are fundamental differences in how cloud infrastructures operate compared with on-premises networks. Currently, cloud infrastructures are growing fast due to DevOps software development and the continuous integration/continuous delivery (CI/CD) pipeline. Yet this scenario often leaves IT teams understaffed and without the expertise to manage every facet of their agency's operations. IT staff can lack visibility into all the applications and services running in the infrastructure, as well as all of the various identities with access. The attack surface grows, creating new layers of vulnerabilities.

Agencies, which are moving increasingly to the cloud because of its many advantages and the mandates of the government's Cloud Smart policy, need to take a comprehensive approach to managing cloud services in order to reap the benefits.

To learn more about cloud services management, GovLoop collaborated on this report with E-INFOSOL, a service-disabled and veteran-owned small business that specializes in secure IT services, including cloud. This report will look at the specific challenges agencies face in managing their growing cloud operations and the tools they can use to bring them under control.

$7.8 billion

is the projected amount of federal spending on cloud computing in 2022.

91%

of federal agencies have all, most or some systems and solutions in the cloud.

45%

of federal agencies currently store citizen and mission data in the cloud.

68%

of all malware downloads in the second quarter of 2021 were delivered from cloud apps.

Agencies Seek to Gain Control Over the Ever-Expanding Cloud

Challenge: Fast Growth, Complexity Hinder Management

Cloud infrastructures can grow in size and complexity too quickly for IT teams to keep up, expanding the attack surface in ways that aren't always apparent without a clear, full view of critical assets, software services, microservices and other features of the cloud. Trying to secure services after they've gone into production can be complicated, though that may be the only approach teams have at their disposal.

"Security needs to be embedded upfront, and that isn't always the case," said Chad Thomas, E-INFOSOL's Chief Security Officer. "Sometimes the users get out ahead of the architects."

The most acute pain points in managing cloud infrastructures include:

Lack of visibility. Agencies' ability to manage the consumption of cloud services is hindered by not having a clear view of their enterprises. They don't always know what services are being used or what the rates of usage are, and are blind to the use of shadow IT. It can affect efficiency, resulting in unexpected costs while creating new security vulnerabilities, particularly with regard to the surge in ransomware.

Cloud misconfiguration. Among the biggest sources of cloud vulnerabilities are misconfigurations, involving anything from loosely defined access controls or ports to Docker application programming interfaces and unrestricted storage buckets. This is the biggest fear of many organizations, and one of the areas where manpower and skills shortages come into play.

Blanket privileges. Another major source of trouble is the rampant and over permissioning of accounts (including non-human accounts) that may be convenient for employees to build and deploy, but give unfettered access to attackers who compromise a user's credentials.

Account provisioning/resource provisioning. Managing access to resources, as well as the deployment and operation of software and hardware resources, is a huge burden for IT employees, and it's only getting heavier as the customer's cloud usage grows. Agencies suffer from a lack of automation and standard processes.

90%

of organizations are vulnerable to breaches because of cloud misconfigurations.

61%

of breaches involve compromised credentials.

72%

of credential-related breaches involve privilege abuse.

25%

of agencies reported an accidental cloud leak in 2020.

The Solution: Cloud Services Management

Cloud services management brings oversight and orchestration to cloud operations, with a comprehensive approach that covers planning and designing cloud systems, streamlining operations through better visibility and automated tools, and maintaining control of services by ensuring that security, spending and compliance goals are met.

"Cost, security, identity, control," said Fredy Pesante, Co-Founder and CEO of E-INFOSOL. "Everything starts with managing all aspects of [the] cloud."

Agencies are successful when they establish an identity strategy for the cloud and a network strategy for the cloud, said Robert Szot, Chief Cloud Architect for E-INFOSOL. A management plan, for example, will help make security a part of development and operations so that new services aren't let loose into the environment before security has been reviewed and addressed. This is the idea behind DevSecOps, in which the development, security and operations teams collaborate throughout the development process.

"You need to put some thought into it before you just start clicking buttons in the cloud and creating things," he said.

Cloud services management offers a lot of benefits for agencies, including:

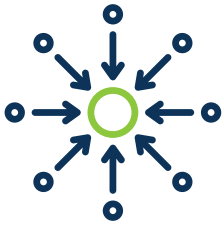
Performance. By providing better control over services and identities, cloud services management increases responsiveness and efficiency. "The cloud highlights the need for a new type of skill set, with heavy automation and heavy scripting," Szot said. Automated tools handle operations, maintenance and other tasks that cannot be done by hand at scale, such as managing containerized microservices deployed in the infrastructure.

Lowered costs. Increased visibility and automation can help agencies maintain control of temporary resources and abandoned services (such as test services) that are still running on the network, saving money on abandoned or unnecessary services and reducing cloud sprawl.

Scalability on demand. Rather than building for peak periods that can't always be predicted, cloud services management can quickly scale up or down depending on demand, which also reduces costs. Take advantage of managed services and serverless offerings from the cloud service providers to put more of the undifferentiated heavy lifts on them.

Compliance. Effective management will incorporate reporting, auditing and other controls into the operations, helping agencies maintain security and FedRAMP compliance.

Best Practices in Cloud Services Management

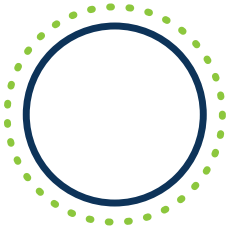


Centralized Management

When operating at the scale of the cloud, centralized management is essential. Managing access to services and enforcing controls such as least privilege can't effectively be done on a platform-by-platform or application-by-application basis. Because everything in the cloud is interconnected, management must be enforced centrally rather than distributed.

Security First

Cloud providers prioritize security for their services, but agencies using the cloud are exposing their networks to different environments and networks, as well as the malicious actors who populate the internet. Agencies should be sure to conduct security assessments before enabling any services, implement controls during development and continuously monitor both for security and compliance. It's also important to educate the workforce, especially developers who aren't necessarily worried about how the different aspects of the cloud can expose data.



Establish Cloud Boundary Protections

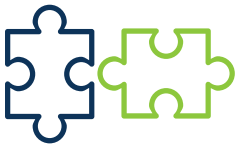
Internal vulnerabilities are important in security, but the initial line of defense is still the external boundary. "What the first focus should be is on boundary protection," Szot said. Whether it involves identity and access management, accreditation or networking, boundaries are where threat actors will first encounter the cloud infrastructure, so securing those boundaries is essential. Agencies also need to secure communications between external and internal systems and have the capability to initiate automated remediations for non-compliant resource configurations. E-INFOSOL practices a lot of defense in depth, and while protecting the edge will never go away, the company encourages agencies to think of protecting the layers with Security Groups/NACL.

Use Automation

Managing the speed and scale of the cloud isn't possible without automated tools, which can provide visibility, help manage accounts and services, scale services depending on demand, enforce security policies and meet federal compliance mandates. They also are particularly useful in conducting assessments of services. If aligned with the controls and standards outlined in the National Institute of Standards and Technology's (NIST) SP 800-53, those assessments can help agencies obtain an authority to operate.

Establish a Cloud Center of Excellence

A center of excellence, preferably established at the start of an agency's migration, will help ensure that cloud implementations adhere to the agency's cloud strategy.



Build a Culture of Collaboration

Starting with buy-in from leadership, agencies should ensure that units within the organization, such as operations and security teams, understand one another's priorities and share the same goals.

Cloud Service Management Puts Agencies in Control

A federal agency migrating operations to the cloud is going to gain speed and scalability in fielding its services, but it will also encounter difficulties in managing operations, especially as its infrastructure incorporates multiple cloud providers and hybrid arrangements of on-premises and public cloud systems.

In this new environment, an agency most likely won't have the staff or skills to manage every aspect of the cloud. It can lose sight of all the identities on the network and all the services it has running, which increases costs and creates a host of new vulnerabilities in an expanding attack surface. It also can lose track of meeting the compliance requirements necessary to maintain its authority to operate.

By implementing a cloud services management system, agencies gain visibility into the infrastructure and exercise control over network identities, privileges and cloud services. They can better enforce security policies, meet compliance mandates and control costs through greater efficiency. Cloud services management also delivers speed and efficiency that would not be possible otherwise, as automated tools perform tasks in minutes or seconds that would have taken an IT team weeks or longer.

Agencies' cloud services additionally become more responsive, able to scale up or down with demand or provide specific services when requested.

Agencies that have implemented cloud services management have found that it effectively allows their services to perform the way they want them to.

HOW E-INFOSOL CAN HELP

E-INFOSOL has extensive experience in successfully helping agencies with a variety of technology implementations, including migrating and managing operations in the cloud, having worked with agencies such as the FAA, NASA, and the departments of Justice, Defense, and Homeland Security.

An Amazon Web Services (AWS) advanced consulting partner, E-INFOSOL specializes in cloud migrations, program management, networking, cloud identity and access management, automated account provisioning services and software development. With cloud services management, the company brings a comprehensive set of tools and services to help agencies get control over their cloud infrastructures, enhancing security, reducing operational costs and enabling the scalability and responsiveness that agencies need to do their jobs.

"We provide you a day-one capability through standard and automated processes," said Pesante. "And we provide centralized management of your cloud services, with the end result of actually providing mission impact."

Learn more: e-infosol.com

Conclusion

Cloud services management provides a comprehensive approach to planning, migrating, implementing and operating a cloud environment. By employing automated tools, it can deliver visibility into the infrastructure and control over the different functions within the cloud, from managing identities to providing in-depth security.

Cloud services management increases efficiency – curtailing the overspending that frequently plagues cloud operations – helps make IT staff more effective and gives agencies the means to readily meet compliance mandates. Above all, it enables agencies to use the cloud to securely and effectively perform their missions.

ABOUT E-INFOSOL

E-INFOSOL is a Service-Disabled and Veteran-Owned Small Business (SDVOSB) located in the Washington, D.C. metropolitan area. We specialize in building modern and tailored solutions to support our customers' mission. As a mission-first organization, we deliver Subject Matter Expertise (SME) in cloud computing, virtualization, cyber security, software development and data services. We support the Intelligence Community, Department of Defense, Federal Law Enforcement, Civilian Agencies and the Private Sector.

Learn more: e-infosol.com

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop