The Dawn of Security as Code

MARKET TRENDS REPORT

govloop

JHC TECHNOLOGY
Cloud. Simplified.™

Introduction

Government agencies taking their IT infrastructures to the cloud are realizing that their approach to security must change.

Cloud computing – coupled with advances in mobile computing and the Internet of Things (IoT) – has allowed organizations to greatly extend their networks' reach while adding speed, efficiency and access to data from multiple sources. But hackers have also reaped many of the same advantages. Attacks now come from more directions faster than ever, leaving agencies with less time to identify, analyze and react to them.

To keep their data, applications and operations protected, agencies need to execute their security procedures in as close to real time as possible. And that ability requires software that's built from the ground up for the job.

To explain how to do this, GovLoop talked with Matt Jordan, Vice President of JHC Technology, a cloud and IT solutions provider for government and commercial clients. In this report, we discuss how agencies can take advantage of Agile development to deploy new software more quickly and with security woven into the process at every step.

With the goal of securing software from the start, IT development is seeing the dawn of Security as Code.

"The risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing as security threats continue to evolve and become more sophisticated."

Government Accountability Office

BY THE NUMBERS:
Cybersecurity Remains Front and Center

#1

The rank of Security and Risk Management on state chief information officers' (CIOs) list of Top 10 Priorities for 2019. Governance, budget and resource requirements, and security frameworks topped the list of goals.

#2

The rank of Cloud Services on the list of top priorities, with cloud strategy, proper selection of service and deployment models, and scalable and elastic capabilities among the goals.

#1

Rank of budget shortfalls among state CIOs' top cybersecurity concerns in every NASCIO survey since 2010.

69%

Number of federal agencies who report that less than half of their cloud service providers are certified under the Federal Risk and Authorization Management Program (FedRAMP), a governmentwide program that provides a standardized approach to cloud security.

55%

Number of federal agencies that "strongly embrace" cloud.

8.9%

of the fiscal 2018 federal IT budget funds provisioned services, such as cloud computing.

5-25%

The percentage of IT budget that federal agencies spend on cybersecurity by U.S. federal agencies.

28%

The percentage of IT budgets spent on cybersecurity in the U.S. private sector

Sources: NASCIO, 2018 Deloitte-NASCIO Cybersecurity Study, 2019 Ponemon Survey on Cloud Adoption Across Federal Government Agencies

THE CHALLENGE: Mitigating Cloud's Vulnerabilities

A cloud infrastructure delivers many benefits, but it also expands an organization's attack surface and introduces a wide range of potential vulnerabilities, especially with the growing prevalence of mobile and IoT devices.

Cloud is not just another platform, but one that ultimately can transform how agencies think about the development and delivery of IT services. Cloud increasingly goes hand in hand with Agile software development and DevOps practices. The latter combines software development and IT operations practices, which shortens system deployment and provides continuous delivery with high software quality.

This growing complexity has good intentions, but it can also leave agencies struggling to adapt their existing cybersecurity strategies.

Increasing complexity is all the more challenging because agencies at all levels of government remain a favorite target of malicious actors. Incidents such as the 2015 hack of the federal Office of Personnel Management, which resulted in the loss of more than 21 million records, have garnered much attention, but state and municipal governments have often been in the crosshairs as well. A list of the largest government cyberattacks in recent years, for instance, includes California's and Georgia's secretaries of state, Los Angeles County, and Washington's Department of Fish and Wildlife. State and local governments also were the victims of almost two-thirds of all ransomware attacks, according to a 2019 study by Barracuda Networks.

Unfortunately, cloud implementations can introduce problems if not done properly. Poorly secured and configured cloud databases were a major contributor to security breaches in 2019, with poor configuration alone behind the loss of more than 70 million leaked or stolen records, according to Symantec's 2019 Internet Security Threat Report.

The bottom line is that today's cloud-based networks have created an environment far removed from traditional on-premises computing. A new approach that starts with secure code is needed.

THE SOLUTION: Bake Security Into Code

The best approach to cloud security is not based in the cloud, but in the concept of Security as Code.

Security as Code creates a foundation for DevSecOps, which brings security into the Agile development process at the ground floor. It incorporates security as a fundamental component of development tools and workflows. DevSecOps also uses a similar approach to collaboration through constant testing and continuous delivery.

This process shortens the feedback loop, accelerating the speed with which developers can respond to stakeholder requirements with new releases – often several times daily, as opposed to once weekly or even a few times each year, as with traditional methods.

Security as Code adds security "from the first word of design," said Matt Jordan, Vice President of JHC Technology. And because it's delivered through an automated build, test and deploy process, it's consistent in all of its implementations.

Security as Code also reflects how the cloud works, with agencies relying on automated processes. "Developers need to code and deploy workloads using test driven security," JHC Technology Evangelist Michael Bryant added. "Security is part of code quality."

The result is a more comprehensive, flexible cybersecurity that's woven into the software – and the IT infrastructure – from the get-go, with source code analysis and validation performed continuously. And infrastructure is deployed as code, making it auto-scaling, self-healing and trending toward 100% uptime.

Having security that's "baked in" rather than bolted on afterward has been a mantra of IT officials in government and every other sector for years, but the realities have lagged behind the ideals. Security as Code puts those ideals into practice. It's automated, repeatable, highly scalable and portable from the start.

BEST PRACTICES:
Good Governance Rules

1. Develop a Cloud Policy

It all starts with a good plan. Agencies need a cloud policy that covers steps from acquisition to implementation, and addresses the three models of cloud computing: Infrastructure-, Platform- and Software-as-a-Service. Security is an essential component of a good policy; Security as Code builds it into the foundation.

2. Adopt a Governance Framework

In the realm of cloud and Agile development, a good plan means strong governance. Governance establishes a framework covering the people, practices and technology standards at each step along the way to an agency's goals. The collaboration, constant testing and other elements of DevSecOps put many cooks in the kitchen; a strong governance plan, with secure code at the core, establishes procedures that ensure that the process does not become too convoluted.

3. Establish a Cloud Center of Excellence

As part of the governance plan, agencies should establish a Cloud Center of Excellence (CCoE), a cross-functional team that centralizes and coordinates cloud strategy. CCoEs set repeatable policies, reference architectures, frameworks and procedures for development teams to follow. They also can establish contracts with easy-to-use base frameworks. Agencies can order from those contracts according to their business needs.

4. Find an Experienced Industry Partner

Cloud transitions can be complex, and no agency has the necessary expertise in every area. Agencies should look for partners with experience in making the transition and ask about specifics, such as a potential partner's familiarity with the tools and technologies that will be used. The ability to implement Security as Code should be included in the criteria. An agency should ensure its cloud and security vendor is among the top tiers of partnership within the chosen CSP, helping to ensure that the partner has the requisite experience, familiarity, past performance, and relationships to carry projects forward.

HOW JHC CAN HELP

JHC Technology has supported federal, state and local governments with new, innovative technologies – including cloud services from Amazon Web Services, Microsoft Azure, Office 365, and Google Cloud Platform and G Suite – since 2010.

JHC's approach to Security as Code builds on Agile strategies and DevOps Infrastructure as Code, in which servers, databases, virtual machines and other infrastructure components are provisioned and managed via source code. It produces reliable and repeatable environments with each use, avoiding the traditional manual processes that often result in unique environments that can't be reproduced.

The company has worked with a range of federal, state and local government clients, helping them comply with FedRAMP; the Federal Information Security Management Act, a framework for protecting government information and systems; and other compliance standards. JHC has helped agencies implement security methodologies such as zero trust cybersecurity, vulnerability and risk assessments, and configuration assessments. JHC Technology has a extensive experience on enterprise and agency level cloud migration, DevSecOps, managed services, Infrastructure and Security as Code, and cost optimization to meet business and technical drivers.

To learn more, visit www.jhctechnology.com or email sales@jhctechnology.com.

Conclusion

Government agencies moving to the cloud must trust that they can protect their network and data by identifying and responding quickly to inevitable attacks. Agencies, particularly at the state and local levels, often don't have the budgets or security experts to handle every aspect of managing and providing the security for their workloads. By making security part of the design in an Agile process built on automation, constant testing and continuous delivery, Security as Code can pave the way for the most comprehensive, efficient, resilient and cost-effective cloud cybersecurity.

JHC TECHNOLOGY
Cloud. Simplified.™

ABOUT JHC

JHC Technology, a "born with the cloud" company, has been delivering cloud solutions for nearly a decade. At JHC Technology, security is built into our DNA. JHC understand the present compliance landscape, the need for codified and repeatable deployments with security baked in, and how to construct cloud solutions that can evolve to meet future compliance standards. We implement security as code for our customers by paving the way for the most comprehensive, efficient, resilient and cost-effective cloud cybersecurity.

Our goal at JHC Technology is to ensure trust within state, local and federal government agencies. Explore our website to discover how our team of architects can design your environment with built-in security while meeting organizational and industry requirements.

govloop

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.

govloop

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

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

www.govloop.com
@GovLoop