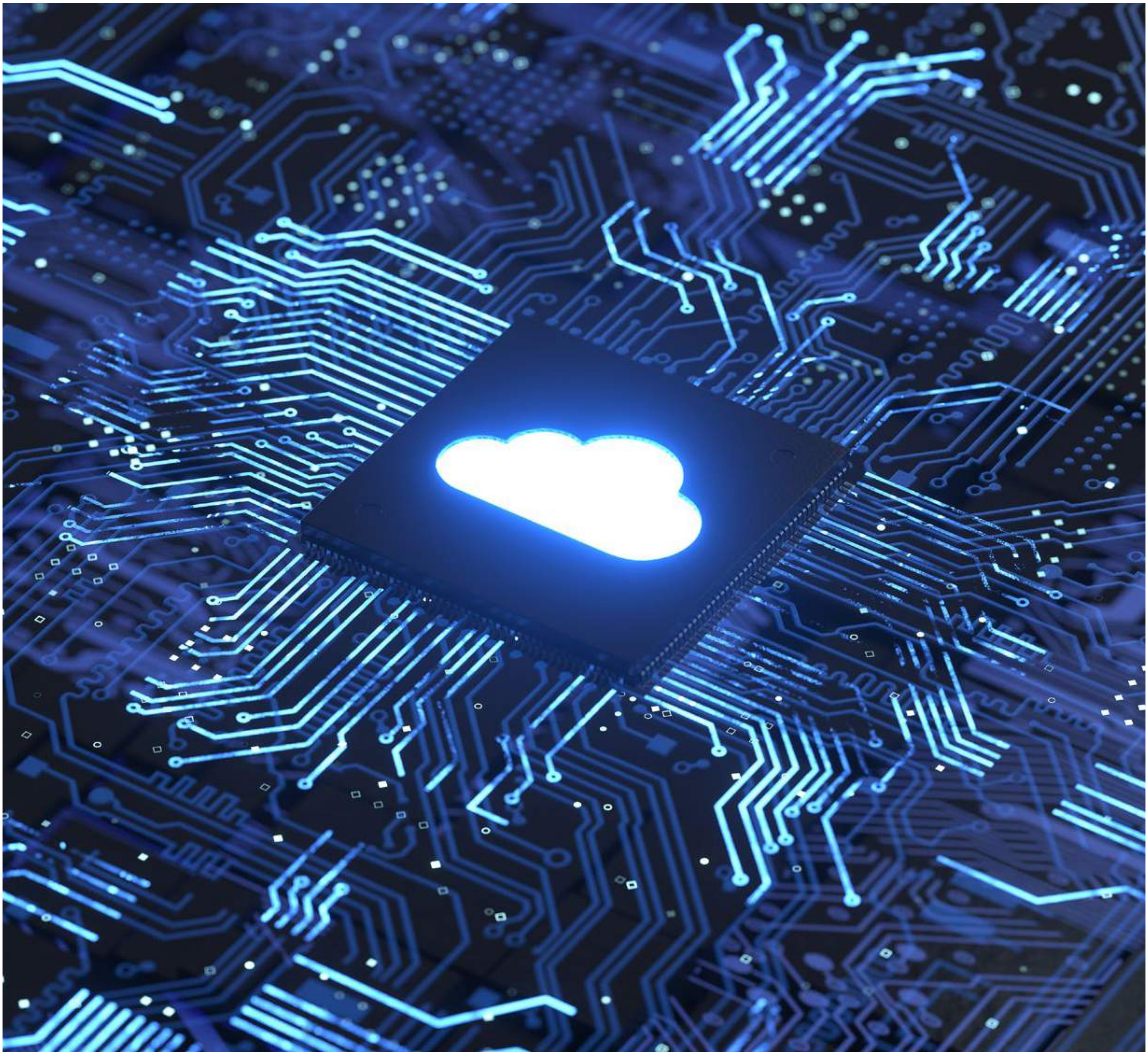

Navigating the Security Challenges of Cloud-Native Operations

MARKET TRENDS REPORT

Executive Summary

After years of increasing the adoption of cloud services, federal agencies are taking the next step: embracing cloud-native applications and the DevOps approach of bridging software development and IT operations to build them. In contrast to cloud-enabled applications, which typically were ported from on-premises servers to cloud services for cost and operational benefits, cloud-native applications are built and deployed in the cloud. They use containers and microservices architectures, which promise quicker application development and delivery, along with greater flexibility.

By adopting DevOps principles and cloud-native application development pipelines that build on reusable artifacts as container image building blocks, agencies have begun realizing benefits including faster development, improved user experience, easier management, higher reliability and lower costs – mostly because of the efficiencies that reuse of existing components across multiple container images affords.

Although the benefits are compelling, cloud-native architectures also introduce new types of security risks and potential sources of vulnerabilities for DevOps teams to address as part of their workflows and processes. Existing approaches to application security are not designed for this new paradigm. Instead, DevOps **teams need a new approach that helps them better identify where potential risks exist and enables them to integrate vulnerability management into their development and delivery pipelines.**

To learn more about how agencies can navigate the security challenges of cloud-native infrastructure, GovLoop teamed with Aqua Security, which helps organizations build and deploy applications that are secure by design without compromising functionality, security or compliance.

By The Numbers

6.5 million

The number of cloud-native developers worldwide

4 million

The number of developers using serverless architectures and cloud functions

14%

of funding earmarked for IT in federal agencies is spent on cloud security

35%

of public-sector employees said they had sacrificed mobile security while working at home to get their jobs done

81%

of public-sector organizations now include and/or define a zero-trust approach to cybersecurity

160

The average number of attacks against honeypots per day during the first half of 2020, a significantly higher number than the previous six months

92%

of organizations now use containers in production

95%

of attacks are designed to hijack resources vs. 5% designed to launch network denial-of-service attacks (based on an analysis of 16,371 attacks occurring between June 2019 and July 2020)

How Cloud-Native Disrupts Traditional Security Practices

Challenge: **A Different Kind of Architecture**

There is a big difference between securing traditional applications with dedicated infrastructure and securing dynamic cloud-native apps based on containers and running in a microservices architecture. Traditional security practices simply aren't designed for this environment, and they won't protect cloud-native apps effectively. Here's why:

- Cloud-native applications are developed incrementally, with continuous streams of code that are constantly updated and deployed into the environment. This creates a large attack surface of known and unknown vulnerabilities.
- Traditional applications always have a virtual machine (VM) or server attached, so they retain the same IP address and location at all times. Cloud-native applications have no permanence of location, with no clear perimeters. Every component is independently and automatically spun up or down, multiplied, spun down in one place and spun up in another. That means security must follow application services, wherever they are.
- The conventional method of securing applications focuses on identifying and mitigating code vulnerabilities before they're exploitable. For example, security policy might require fixing all critical vulnerabilities before moving an application to production. But analyzing the relative risk and criticality for thousands of vulnerabilities is time-consuming and difficult. The lack of prioritization when dealing with a proliferation of vulnerabilities in the cloud-native supply chain and infrastructure slows development and does not position DevOps teams to mitigate overall risk.

Solution: **A Risk-Based Approach**

When it comes to cloud-native applications, security can't be an afterthought. Instead of relying on bolted-on solutions and approaches, security must be integrated into the continuous integration and continuous development (CI/CD) pipeline.

It starts by taking a risk-based approach to cloud-native development, which allows DevOps teams to detect, evaluate and fix vulnerabilities in the artifact pipeline as an integrated component of the development process and maintain ongoing monitoring of how containers behave once deployed.

"Everybody runs tens or hundreds of thousands of vulnerabilities at any given moment, and the risk-based approach allows you to prioritize," explained Rani Osnat, Vice President of Strategy at Aqua. "By using a risk-based approach that includes scoring to assess how dangerous each vulnerability is, you can understand which poses the biggest risk and should be handled first."

A comprehensive risk-based approach includes:

- Shifting security controls into the development pipeline and focusing on the artifact pipeline to ensure that risks are evaluated and mitigated before code goes into production. Without this change, organizations are more likely to face a large attack surface at runtime that's too complex to understand and mitigate.
- Establishing an "acceptance gate" that ensures that customizable policies address all security risks and vulnerabilities, and allows security teams to evaluate containers in a sandboxed environment for risks such as supply-chain attacks before they are deployed.
- Having a plan for "drift prevention" — detecting changes to apps and containers that cause them to fall out of compliance with security requirements.

Adopting a risk-based approach is critical, but it's not the complete solution. It's much better when combined with layers of security that move beyond detection and assessment to remediation or mitigation. For example, in cases where you can't or don't want to remediate, you might choose to create a runtime control that detects, prevents and tracks the exploit for specific vulnerabilities.

Together, these steps create a full lifecycle approach to security starting with development and continuing through deployment to runtime. It ensures that nothing too risky flows through, while allowing organizations to prioritize and remediate what they can, accept or mitigate what they can't, and once running, easily detect and stop events.

Best Practices for Cloud-Native Security

Get on the same page. Disagreements among the DevOps, security and engineering teams can derail a project. For instance, if the security team doesn't fully understand the methods DevOps is using, they might insist on using a different methodology – one that doesn't work well for a cloud-native application. If the security team insists that the DevOps team compile and run a cloud-native application as if it were a traditional application, much of the benefit will be lost. In other cases, decision-makers may insist on a traditional model of how security works with applications – looking only at runtime or not considering development, for example. This may result in a situation in which the system addresses only a subset of the risks.

Look beyond the low-hanging fruit. It's not unusual for security staff to focus on known vulnerabilities in cloud-native applications instead of looking deeper. That's not wrong, Osnat says, but it doesn't go far enough. "If that's all you're looking at, you could easily miss zero-day attacks that aren't focused on vulnerabilities, insider abuse or user mistakes in exposing infrastructure. Not everything is related to vulnerabilities," Osnat said.

Know your strengths and limitations. If your agency doesn't have enough skilled developers, that will impact how quickly the organization can transform, how well applications are designed and how effectively new security measures are implemented. If that's the case, there are two options: Bring in trusted third parties to help or build up the team and create reference architectures and blueprints. In both cases, it pays to go slowly, starting with one application. Once you see that it's working well, you can more easily replicate them to other applications and groups.

Don't look for a one-size-fits-all approach. No matter the intention, chances are your agency will end up with several types of environments – different flavors of Kubernetes, different pipelines, different clouds. That's fine, Osnat says, but managing a multi-cloud, multi-platform environment requires a strong, unified platform. "If you're running one application on [Amazon Web Services] and another application on [Microsoft] Azure, the security postures will be different because you're using different tools," he explained. "You don't want to have to do the work twice or create security workarounds when you want to migrate. You want it to be transparent and consistent."

Case study: Slow and Steady Wins the Race

In 2015, when many organizations hadn't even heard of cloud-native computing, one of the country's largest organizations was heading in just that direction. The idea grew out of discussions about what it needed from its mission-critical applications, such as the ability to update applications frequently and run them in an orchestrated environment.

This made it clear that the way forward was embracing DevOps and cloud-native application development. At the same time, the group understood that this change would require a new approach to security.

Once the decision was made, the organization got started. After scanning containers and images in its pipeline to detect and manage vulnerabilities, the security division began exercising deployment controls and runtime protection capabilities, activating more preventative runtime controls over time. All told, it took the group about three years to build the capability from the ground up.

At the same time, the organization addressed the security changes required to smooth cloud-native application development. By implementing cloud-centric container security and vulnerability management tools, the IT staff was assured full visibility and tracking capabilities.

By systematically and proactively switching its approach to cloud-native development and adapting its security practices to keep pace, the organization avoided many of the issues that others experience during major changes: slowdowns, scalability problems and rejection from security or compliance officers when seeking to deploy something new.

HOW AQUA SECURITY HELPS

Focused squarely on cloud-native security, Aqua helps organizations prevent, detect, respond and automate across the entire application life cycle. The Aqua Cloud-Native Security Platform helps security teams stop threats and vulnerabilities, empowering DevOps to detect issues early and fix them quickly. The platform includes:

Vulnerability scanning and management: Minimizes the attack surface of cloud-native applications, detecting vulnerabilities, embedded secrets and other security issues during the development cycle.

- Continuously scans registries, container images and serverless function stores to detect and identify known vulnerabilities, hidden malware, embedded credentials and secrets, open source license issues, configuration errors, and over-provisioned permissions
- Identifies vulnerabilities by container image layer
- Automatically evaluates risk-related contextual factors to generate a complete list of vulnerabilities that can be refined based on factors such as exploitability, severity and whether the workloads are running

Dynamic threat analysis: Detects and mitigates advanced threats and unknown malware in container images using a secure container sandbox.

- Exposes hidden malware in CI builds and registries
- Provides detailed, actionable data on anomalous container behavior
- Maps suspicious network activity
- Allows the security operations and forensics teams to see the entire kill chain before attacks happen

Workload run time protection: Configure and enforce runtime controls that apply to all containers, functions and VMs, permitting only legitimate behaviors and preventing several types of privilege abuse, suspicious behaviors and attack vectors.

- Aqua's Vulnerability Shield detects and prevents attacks that target known vulnerabilities to generate runtime policies that can detect and block access to vulnerable components in containers.
- The Drift Prevention feature prevents any attempt to alter workloads in runtime — detects and prevents any change to running workloads, as compared to their originating images or artifacts.

Learn more:
Aqua Security Cloud Native Security Platform

Conclusion

Contrary to popular belief, cloud-native applications are not less secure by design than traditional applications. In fact, it's the other way around: Developing applications in a cloud-native environment allows IT teams to improve security, increase granularity protection and significantly improve visibility.

The key to achieving that security is integrating security into the application development pipeline, from start to finish. With a system that allows for customizable policies, agencies also can make sure to address all security risks and vulnerabilities, even as policies and risks change. Finally, it's important to embed an effective method for remediating and mitigating threats. Taking these steps will ensure that agencies can gain the benefits of cloud-native applications while avoiding the risks that can occur from a continually changing environment.

ABOUT AQUA

Aqua Security is the largest pure-play cloud native security company, providing customers the freedom to innovate and run their businesses with minimal friction. The Aqua Cloud Native Security Platform provides prevention, detection, and response automation across the entire application lifecycle to secure the build, secure cloud infrastructure and secure running workloads wherever they are deployed.

For more information please visit www.aquasec.com/

ABOUT CARAHSOFT

Carahsoft is the trusted government IT solutions provider, combining technological expertise with a thorough understanding of the government procurement process to help public sector organizations select and implement the best solution at the best possible value. As a top-ranked GSA Schedule Contract holder, Carahsoft is the largest government partner, serving as the master government aggregator for many of its best-of-breed vendors and driving value for an extensive ecosystem of IT manufacturers, resellers, system integrators, and consulting partners. Our dedicated solutions teams support proactive sales, marketing, and delivery of strategic solutions to help improve the efficiency and productivity of government IT.

For more information please visit www.carahsoft.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.

govloop

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

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

www.govloop.com
@GovLoop