Aqua Stops Cloud Native Attacks. Guaranteed.

Aqua prevents them before they happen, and we stop them when they happen. We "Aquarantee" it.

Containers, Kubernetes, Cloud and DevOps Pipelines (collectively called "cloud native" technologies) are in every department and most agencies.

Do you know how to protect them?

Speed Meets Security

To tackle the ever-changing needs of government and to better serve the public, federal agencies need to become more agile. Cloud Native provides the agility needed for modern application development and deployment. With technology that enables faster development and provides the means to experiment, iterate and learn, cloud native has been taking the world by storm.

Tsvi Korren
Field CTO
Aqua Security

Gartner estimates that by 2025, 95% of apps will be deployed on cloud native platforms. This transformation has been disruptive in many ways: just ask anybody who has been tasked to overhaul their application portfolio to be cloud first. But the biggest disruption and impediment to wide adoption is security.

For starters, in Cloud Native, 70-90% of any given piece of software comes from open source, which makes it hard to track and authorize software component for use. Furthermore, older security tools do not work well in cloud native environments. Lacking both visibility inside workloads and altogether missing both integration and understanding into the contextual nature of scalable clouds, they provide poor information and often unable to reliably respond to attacks. Attackers are taking note. They are evolving their capabilities to target cloud native environments. Since developing in cloud native cannot be avoided, agencies must act fast to lock down the development cycle and to actively protect cloud native assets.

Modernizing Security For Cloud Native

Security continues to be one of the top challenges for cloud and cloud native adoption according to the Cloud Security Alliance 2022 "Top Cloud Threats to Cloud Computing report.

This will not change until both security practices and tools provide the dedicated capabilities and controls required for cloud native applications. Agencies can use the mandates in EO 14028 as a guide to building a security program for cloud native that covers, among others, these specific capabilities:

- Identifying and remediating vulnerabilities, misconfigurations, and embedded sensitive data
- Zero trust in workload acceptance, with preauthorization
- Identifying incidents in containers, Kubernetes, functions, and cloud
- Provide contextual data for investigation and remediation
- Safeguarding the security and integrity of the software supply chain
- Expedite incident response with automatic blocking and disruption of attacks.

> Through 2025, 99% of cloud security failures will be the customer's fault.
>
> – Gartner, October 10, 2019

How Does Aqua Help Government?

We Stop Cloud Native Attacks. Guaranteed

As the largest pure-play cloud native security company, Aqua helps customers, both public and private sector, unlock innovation and build the future of their applications. **We detect, prioritize, and reduce risk — all in a single, unified platform.**

The Aqua Platform is the industry's most integrated Cloud Native Application Protection Platform (which Gartner coined as CNAPP), prioritizing risk and automating prevention, detection, and response across the entire application and infrastructure lifecycles. Aqua's CNAPP helps federal agencies address, comply, and benefit from Executive Order (EO) 14028 and OMB M-22-09, as well as other cybersecurity requirements.

By enabling software supply chain hygiene, zero trust acceptance and access, and active workload protection, agencies can rapidly and securely embark on cloud native adoption agencywide. We also offer government organizations supplemental staffing resources and DevSecOps expertise with security as the top priority.

The Industry's Only $1M Cloud Native Protection Warranty

Aqua is so confident that it will stop cloud native attacks on your agency that **it provides the industry's only $1 Million Cloud Native Protection Warranty**, the "Aquarantee".

Purchase and deploy the Aqua platform to all your production workloads. Maintain the platform to Aqua best practice standards. If your protected cloud native applications are successfully attacked, we will back it up with up to $1 Million. This is how we partner with you to prove that Aqua has the most comprehensive and capable platform on the market to protect your cloud native assets.

If your agency is just starting your cloud native journey, Aqua can get you up and running quickly and provide you the visibility you need across the application lifecycle. Detect, prioritize, and secure everything that runs in your cloud. When you are ready, step up to real-time protection from attacks. Detect and surgically respond across your cloud native assets while you keep your agency running.

All of this from one vendor, with one platform, Aqua. ■

Connect with a security expert: https://www.aquasec.com/solutions/federal/