Case Study

aqua

Clarizen Secures Kubernetes-based Cloud Native Apps on Aws with Aqua Security

Customer Overview

Clarizen is a collaborative work management solution designed for people who value their time and for organizations that value cross-company engagement. With Clarizen, organizations can work the way they want to work and have real time-visibility into all their workstreams. This keeps teams focused on the things that matter, delivers results faster, and helps them exceed their company goals and customers' expectations. The company has thousands of customers across the globe and is widely regarded as the leader in collaborative project management.

The Challenge: Securing Kubernetes-Based Applications

In addition to its flagship SaaS solution, Clarizen One, the company has developed Clarizen Go, a more agile, lightweight SaaS solution for collaborative task management.

Clarizen Go was developed using a cloud-native approach, using containers. It is run and orchestrated using Amazon's Elastic Kubernetes Service (EKS) and keeps its container images on Amazon's Elastic Container Registry (ECR). Its agile development pipeline is managed using Bitbucket and Jenkins for continuous integration.

Since Clarizen Go handles sensitive customer data, a cardinal concern was adhering to compliance requirements such as SOC2 and GDPR and having best-in-class visibility and security controls. Due to the agile nature of development and wide usage patterns, the Clarizen team wanted to secure both the development pipeline as well as the runtime environment in AWS, in order to be able to detect issues as early as possible, and mitigate them before they present risks into the production environment.

> "Having granular visibility and observability of the entire application lifecycle from a security and compliance perspective was key," says Yuri Livshitz, Cloud Security Architect at Clarizen. "We wanted to be able to manage vulnerabilities and other issues in the pipeline as they happen."

The Solution

Clarizen canvassed the market for the leading cloud-native security solutions and chose Aqua for its fit with the team's requirements, its ability to secure the entire lifecycle from development to production, its advanced security feature set, and its broad platform support.

Yuri elaborates:

> "Our main security objective has been preventing data breaches. So we needed to tightly control the environment, focusing on preventive measures and least privilege enforcement. This in turn allows us to easily detect unauthorized access or activity."

Using Aqua, Clarizen was quickly able protect Clarizen Go according to best practices and establish security controls for the entire stack:

- Scan image builds within Jenkins to prevent vulnerabilities and malware from making their way into container images, and provide developers with immediate feedback for quick remediation;
- Enforce an image assurance policy, preventing images that do not meet the security and compliance criteria from deploying in production;
- Extend "secrets" (private keys, tokens) lifecycle management to containers, ensuring secure delivery of secrets to running containers while maintaining rotation and secrets management best practices;
- Monitor the Kubernetes and container runtime environment for suspicious behavior and ensuring that containers don't drift against their originating images.

> "One of the things we liked most about Aqua was its broad platform support, which enables us to future-proof our investment and give us flexibility in choosing how and where we run our applications moving forward." - Yuri Livshitz, Cloud Security Architect at Clarizen

aqua

AWS Services Leveraged

Clarizen runs the Clarizen Go application on Amazon EKS, using Amazon ECR to store and manage container images, and leveraging ancillary services such as AWS S3, AWS CloudWatch, and AWS ALB for load balancing.

Customer Benefits

By using the Aqua platform, Clarizen secures its container-based development pipeline, leveraging automation to reap the benefits of agile development without introducing unnecessary risk. Additionally, Clarizen has gained visibility into its Kubernetes-based production stack, keeping tabs on security issues as they emerge:

- Identifying issues early in the development cycle to ensure fast remediation, avoiding security incidents in production
- Preventing and monitoring unauthorized access to its containerized environment
- Ensuring that security and compliance best practices are continuously applied
- Protecting sensitive customer data, identifying and preventing breaches in real time

About Aqua

Aqua Security helps enterprises secure their cloud native, container-based and serverless applications from development to production. Aqua bridges the gap between DevOps and security, promoting business agility and accelerating digital transformation. Aqua's Cloud Native Security Platform provides full visibility and security automation across the entire application lifecycle, using a modern zero-touch approach to detect and prevent threats while simplifying regulatory compliance. Aqua customers include some of the world's largest organizations across sectors ranging from financial services to Internet giants, with global implementations spanning a broad range of cloud providers and on-premises technologies.

✉ contact@aquasec.com
www.aquasec.com
@AquaSecTeam
AquaSecTeam