cuebiq

CASE STUDY

Cuebiq implements DevSecOps at scale with Prisma Cloud

paloalto® NETWORKS | Cybersecurity Partner of Choice

IN BRIEF

Customer	Industry	Products and Services
Cuebiq Inc.	Marketing and advertising	Clara
Organization Size	**Location**	**Website**
100	NY, USA	cuebiq.com

Challenge

Security team sought automation and integration.

Solution

Prisma® Cloud reduces manual tasks and extends visibility.

Results

+ Incorporates security in the CI/CD pipeline to discover and address flaws in containers before the issues go into production.
+ Integrates with existing SIEM, creating a central location for managing cloud-native security events.
+ Shortens time to remediation, using a single pane of glass to get a broader picture rooted in context. Realtime monitoring and risk prioritization speed up discovery and remediation dramatically.
+ Reduces task load for a security team by automating security controls, freeing them up to focus on higher priority tasks.

INTRODUCTION

Cuebiq's platform, Clara, uses location-based data to show how marketing activities influence consumer behavior. The company is at the forefront of industry privacy standards: Clara uses a future-proof privacy framework in its data collection and is one of the very first location providers to be certified by the Network Advertising Initiative (NAI), a leading privacy organization.

Cuebiq has a wealth of data that needs to be carefully protected, and new features are released regularly. Clara runs on Kubernetes®, and the team needed a dedicated tool to address container security.

CHALLENGE

Security team sought automation and integration

Cuebiq's security team is responsible for hardening, securing, and monitoring containers and Kubernetes. Together with Site Reliability Engineering (SRE), the team supports a DevOps organization of nearly 100 people.

The team needed a solution that could manage security risks with less manual effort, integrate with its existing security information and event management (SIEM) tool, and support the company's advance toward DevSecOps.

SOLUTION

Prisma Cloud reduces manual tasks and extends visibility

The security team uses Prisma Cloud as a primary tool in hardening the Kubernetes environment. Team members now run 10 scans per day to look for vulnerabilities, inspect traffic between containers, and block malicious requests.

Prisma Cloud allows the team to integrate security at every phase of development. With realtime monitoring, it's easy to discover and address any vulnerability or flaw before it goes into production. This, in turn, is helping the entire company move toward a DevSecOps culture and ultimately stay secure.

The team also appreciates simplified compliance in scanning for misconfigurations. Because certain security controls can be automated, management and remediation are easier for a team with many other responsibilities.

Cuebiq integrated the platform directly with its existing SIEM, creating a central location for all security events—a fundamental requirement of the security vendor search.

> “Prisma Cloud helps our company reach the concept of DevSecOps, where we assess security in every phase of development. If any vulnerability or flaw is discovered, we patch it before going into production.
>
> **— Head of Security, Cuebiq**

The head of security for Cuebiq says that Prisma Cloud provides “an incredible overall picture of everything developed in our environment. In a single pane of glass, we have everything under control.”

By adopting Prisma Cloud, Cuebiq shortened the overall time between vulnerability discovery and remediation the head of security and his team can now perform near-realtime assessment and gain better understanding of what needs to be done to fix any issues.

KEY BENEFITS

Prisma Cloud has helped Cuebiq in numerous ways, allowing the team to:

- **Incorporate security in the CI/CD pipeline** so they can discover and address any flaws in their containers before the issues go into production.
- **Integrate with existing SIEM**, creating a central location for managing cloud-native security events.
- **Shorten time to remediation** using a single pane of glass to get a broader picture rooted in context. Realtime monitoring and risk prioritization speed up discovery and remediation dramatically.
- **Reduce task load for a security team** by automating security controls, freeing them up to focus on higher priority tasks.

CONCLUSION

With Prisma Cloud, the Cuebiq engineering team can confidently identify and assess security vulnerabilities before putting code into production.

The head of security and the security team appreciate what Prisma Cloud has done for their current processes, and they're thrilled they don't have to manage multiple security tools anymore. In the near future, they also plan to assess the platform's forensic capabilities, using Incident Explorer and the timeline view of security audits to help them enhance their internal capabilities.

To learn more about how Prisma Cloud can support your security processes, visit paloaltonetworks.com/prisma/cloud.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_cs_cuebiq_021224