OPCITO TECHNOLOGIES

Enhancing security solutions for a Kubernetes-based security startup

About The Customer

The customer offers a Zero Trust cloud-native security and compliance solution that safeguards public and private cloud environments. This solution empowers organizations to proactively detect, prioritize, prevent, and mitigate advanced cloud-based threats.

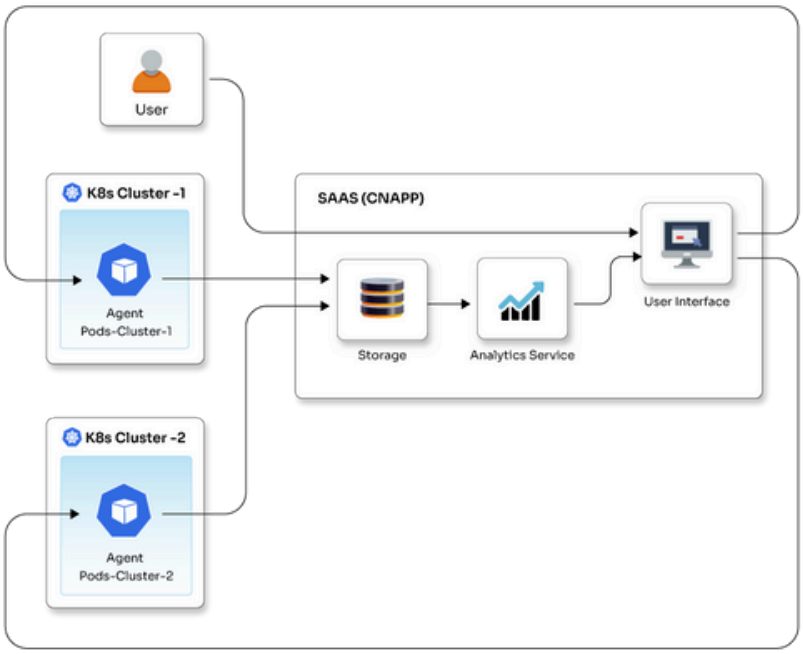
Business Challenge

The customer faced a complex set of challenges related to security and observability. Firstly, they needed to enhance the alerting capabilities of their existing security solutions to ensure prompt detection and response to threats. Secondly, they aimed to establish robust observability for APIs within their Kubernetes cluster, particularly those operating within a Service Mesh, to gain deeper insights into their application behavior and potential vulnerabilities. Lastly, they seeked to expand the capabilities of their product to seamlessly integrate with a variety of security solutions, providing a unified and comprehensive security posture.

How Opcito Helped

- **Enhanced security alerting:** Opcito's security product engineering experts extended the alerting mechanisms of security solutions to send security violation alerts to ElasticSearch. Implementing a system that integrates security alerts directly with ElasticSearch enabled real-time monitoring and analysis of security events. This improved incident response times by centralizing the alert management.
- **Integrated new security solutions:** Opcito's security product engineering team seamlessly incorporated advanced security tools to enhance the platform's defence mechanisms, providing a unified interface for managing multiple security solutions. This ensured compatibility and smooth operation with the existing infrastructure.
- **Real-time API observability: Opcito's team** leveraged WebAssembly (Wasm) to enhance the Envoy proxy in Istio for real-time API call monitoring. This enabled detailed observability and analysis of internal API traffic. Opcito further integrated this observability feature to ensure comprehensive insights into cluster activities.

India office +91 (20) 6712 4100 US office +1 (650) 772 4442



Technologies, Tools, and Platforms used

KUBERNETES
DOCKER
GOLANG, WASM
PYTHON, GCP
EBPF, AWS

Benefits

ENHANCED OBSERVABILITY OF API CALLS	This improvement enabled real-time visibility into API traffic within the Kubernetes cluster, facilitating proactive identification and resolution of potential issues.
PROVISIONED CONTINUOUS SECURITY INTEGRATION	The streamlined integration of new security solutions ensured a robust and adaptable security posture, keeping the platform protected against emerging threats.
IMPROVED MONITORING AND ALERTING	The enhanced monitoring and alerting mechanisms enabled efficient detection and response to security threats, minimizing potential damage and downtime.

About Opcito

At Opcito, we believe in designing transformational solutions for our customers, start-ups, and enterprises, with our ability to unify quality, reliability, and cost-effectiveness at any scale. Our core work culture focuses on adding material value to your products by leveraging best practices in DevOps, like continuous integration, continuous delivery, and automation, coupled with disruptive technologies like containers, serverless computing, and microservice-based architectures. We also believe in high standards for quality with a zero-bug policy and zero downtime deployment approach.

India office +91 (20) 6712 4100

US office +1 (650) 772 4442