CASE STUDY

CEQUENCE SECURITY

Reducing API Sprawl with Inventory Tracking and Risk Assessment

Customer Challenge: A Lack of Visibility

Like most organizations that have been using APIs for many years, this (anonymous) customer came to the realization that they had a bad case of API sprawl caused by a distributed development process and numerous acquisitions. With the understanding that you cannot protect what you cannot see, they went through a manual inventory and risk assessment effort. The API information collected was valuable, uncovering shadow APIs while providing details on a set of risk categories, but the manual data collection process took too long - they needed it to be real-time and the process of collecting it needed to be scalable.

The Solution: Runtime Discovery and Inventory

The customer evaluated multiple API security offerings and chose Cequence API Sentinel for several reasons. API Sentinel performs a continuous runtime inventory to ensure they have a full view of their API footprint, which numbers in the thousands. The inventory includes API traffic patterns, including geographic source and destination, organization and ISP that can be used to determine if there is potential malicious activity. The API visibility includes both external and internal APIs, a unique API Sentinel capability that is enabled through a Kubernetes-based network agent that ties into Apigee for API visibility at the edge and as the deployment expands, it will tie into their service mesh environment for discovery of internal APIs.

In addition to providing an up-to-the-minute inventory, API Sentinel provided immediate value as soon as it was deployed. The specification conformance assessment discovered several APIs that were out of conformance with the uploaded specification which dictated that only HTTP GETs be accepted, but some of the APIs were accepting HTTP POSTs as well. The discovery was quickly remediated by application development, eliminating any potential security risk. Additional risk assessment criteria include discovery of sensitive data exfiltration, usage of weak authentication and custom risk categories. The manually generated risk assessment done previously will be used to create custom risk categories which will allow them to quickly analyze their APIs to discover and remediate potential security gaps.

Results: Improved Visibility and Stronger Security Posture

The deployment flexibility has enabled the customer to gain a handle on all of their APIs and they are using API Sentinel as their centralized API visibility and risk assessment dashboard. The customer also chose to purchase Bot Defense, which they use to remediate any potential malicious activity and prevent sophisticated bot attacks against their mobile, web apps and APIs.

Customer Profile

Large, global telecom service provider.

Outcomes with API Sentinel

- **Realtime inventory and traffic analysis** of internal and external APIs
- **Deployable across any of their data center** or cloud environments
- **Custom risk categorization** easily translated into security policy

© 2021 Cequence Security, Inc. › 100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-408-978-3258 › info@cequence.ai › www.cequence.ai › All rights reserved. Part# EN01305-01