CEQUENCE SECURITY

CUSTOMER CASE STUDY

API Risk Analysis Helps Maintain Regulatory Compliance

CUSTOMER CHALLENGE

Potential Compliance Violations

Like most financial services organizations, this (anonymous) customer is increasingly using APIs to deliver their core products and services. Extending beyond standard APIs used to move money (FDX) or integrate with aggregator partners, APIs within this organization are now primary application components. When exposed to the public – purposely or inadvertently – they raise a variety of security challenges ranging from regulatory compliance associated with sensitive data sharing, to application business logic abuse and automated bot attacks. Like many large organizations, this customer takes a distributed approach to application and API development, with different business groups working in parallel to publish their APIs. While they have a well-defined process for API publication, risks still exist:

- APIs may be published outside of the defined process (shadow APIs)
- They may not adhere to the defined API specification
- Internal APIs may be inadvertently made public, potentially exposing sensitive data
- Older, deprecated, or unmanaged APIs may be able to be discovered by threat actors

This customer quickly came to the conclusion that they needed a way to fully understand their API footprint and then use that information to confirm their security and regulatory compliance posture. Already using Cequence API Spartan, they evaluated API Sentinel, for runtime API visibility and monitoring. The evaluation quickly turned into a production deployment when API Sentinel validated their concerns – shadow APIs had been discovered.

THE SOLUTION

Negating Sensitive Data Leakage Risks

Deployed as a modern Kubernetes application, API Sentinel is integrated with their existing load balancers to collect all external APIs. Longer term, they will take advantage of API Sentinel's ability to integrate with multiple elements of their API management infrastructure (API Gateways, ingress controllers, proxies) to collect API intelligence on internal APIs as well as external.

The immediate benefit was the creation of a centralized inventory of all APIs – from the edge to the data center. The visibility also provides traffic statistics – including usage and information about where the traffic was coming from. Any API that exhibited anomalous spikes, or a questionable location was investigated further using API Spartan. If the additional analysis warranted further action, API Spartan policies were updated to protect the API from malicious activity.

CUSTOMER PROFILE

Large, global financial services company that provides both consumer and commercial products and services.

Outcomes with API Sentinel

- Discover APIs potentially leaking sensitive data
- Visibility into API source and destination
- Improved collaboration and accelerated API security maturity

API Sentinel provides runtime visibility into all of this customers' APIs by continually evaluating traffic passing through the API management infrastructure. All discovered APIs, shadow or otherwise, are confirmed to have a business owner within API Sentinel for tracking and management purposes. APIs are then analyzed for possible sensitive data leakage, a potential compliance violation and a significant security gap. API Sentinel will also help assess other risk factors associated with weak authentication, use of encryption, compliance with API specifications, and customer defined concerns such as the presence of PII, PCI or other sensitive data.

For this customer, the analysis for sensitive data leakage and where the information might be going (IP address) is critically important. API Sentinel performs a runtime assessment of the API, looking specifically for credit card or social security numbers using predefined data patterns. Any API discovered to be leaking data, are displayed in a sensitive data dashboard for visual analysis and rapid response that automatically sends an alert to or email to appropriate parties to ensure the issue is addressed. Other APIs found to be in high risk are flagged for development and then translated into API Spartan security policies to ensure the risk is negated once the API is published.

> "The ability to analyze APIs at runtime to discover possible sensitive data leakage is unique to API Sentinel. We can quickly see if APIs are doing what is intended.
>
> Chief Data Officer,
> Large FSI Customer

THE RESULTS

Better Security, Improved Collaboration

API Sentinel is helping this customer eliminate possible compliance violations caused by APIs that may be exposing sensitive data. More importantly, the edge-to-data center API visibility and ownership tracking is driving collaboration between security, development and the business groups, speeding the maturity of their API security program – a critical requirement to keep their customers' data secure and private.