

## Case Study

# API Risk Analysis Helps Maintain Regulatory Compliance

## The Challenge Maintaining Compliance

Like most financial services organizations, this Cequence customer is increasingly using APIs to deliver their core products and services. Extending beyond standard APIs used to move money using the Financial Data Exchange (FDX) or integrating with aggregator partners, APIs 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. 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:

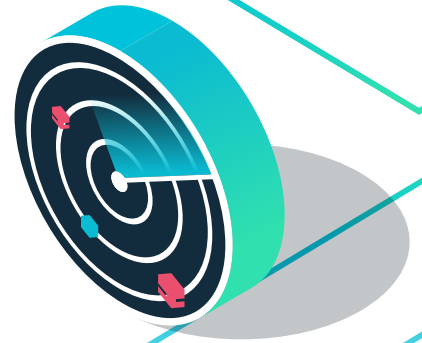
- APIs may be published outside of the defined process (shadow APIs)
- They may not adhere to the defined API specification
- Internal APIs may be inadvertently made public, potentially exposing sensitive data
- Older, deprecated, or unmanaged APIs may be discovered by threat actors

This customer quickly determined 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 Bot Management, they evaluated Cequence API Security for runtime API visibility and monitoring. The evaluation quickly turned into a production deployment when Cequence validated their concerns – shadow APIs had been discovered.

## The Solution Negating Sensitive Data Leakage Risks

Deployed as a modern Kubernetes application, API Security integrated with the customer's existing load balancers to identify all external APIs. 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. If the additional analysis warranted further action, Cequence Bot Management policies are updated to protect the API from malicious activity.

Cequence provides runtime visibility into all APIs by continually evaluating traffic passing through the API management infrastructure. All discovered APIs, shadow or otherwise, are confirmed to have a business owner for tracking and management purposes. APIs are also analyzed for possible sensitive data leakage, a potential compliance violation and a significant security gap. Cequence also helps 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.



## Customer Profile

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

## Outcomes

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

For this customer, the analysis for sensitive data leakage and where the information might be going, such as to a specific external IP address, is critically important. Cequence 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 security policies to ensure the risk is negated once the API is published.

## The Results

### Better Security, Improved Collaboration

Cequence helped 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.

**“The ability to analyze APIs at runtime to discover possible sensitive data leakage is unique to Cequence. We can quickly see if APIs are doing what is intended.”**

Chief Data Officer  
Large FSI Customer