Akamai Customer Story

Top U.S. Bank Secures API Traffic and Gains Visibility

Maintaining stringent regulatory compliance with unprecedented visibility into its API attack surface

The banking industry has undergone a significant transformation in recent years, driven by the adoption of application programming interfaces (APIs). This proliferation of APIs has enabled banks to leverage new opportunities, enhance customer experiences, and drive business growth.

APIs have played a crucial role in enabling seamless integration between different systems and applications within the banking ecosystem. By exposing their services and data through APIs, banks can now collaborate with third-party developers, fintech startups, and other financial institutions to create innovative solutions and expand their offerings. However, despite these clear advantages, exposing APIs doesn't come without some risk.

API security risks can pose significant threats to the confidentiality, integrity, and availability of an API. These risks include unauthorized access, injection attacks, denial-of-service attacks, insecure data transmission, insufficient authorization and privilege escalation, lack of input validation, insecure storage of credentials, and inadequate logging and monitoring. To address these risks, this banking leader engaged with Noname Security (now an Akamai company).

Maintaining compliance

In the financial services industry, compliance with regulations is of utmost importance to ensuring fair and transparent practices, protecting consumers, and maintaining the integrity of the financial system. Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations

Banking Leader

Location

United States

Industry

Financial Services

Solution

Akamai API Security

Key Impacts

- Strengthened regulatory compliance
- Integrated with F5 production environment
- Provided continuous API identification

Akamai

require financial institutions to verify the identity of their customers, assess potential risks associated with money laundering and terrorist financing, and report suspicious activities.

Other regulations include the Payment Card Industry Data Security Standard (PCI DSS), which is a set of security standards established by major credit card companies to protect cardholder data. These regulations are just the tip of the iceberg when financial regulations are concerned. For this reason, knowing what data is traversing through its APIs was crucial to the financial services leader.

The company needed to understand, manage, and mitigate risk by improving the overall visibility of its API ecosystem — with emphasis on API discovery, data classification, vulnerability, and anomaly detection. It also prioritized integration with its F5 production environment.

Uncovering its API footprint

The Noname API Security Platform (now part of Akamai API Security) provided visibility into API traffic transmitted to and from the customer network as well as within it. The Akamai API Security engine analyzed the traffic and discovered all of the financial service leader's APIs. Real-time traffic analysis identified new APIs and changes in existing APIs, and the data was recorded and updated in the customer's dashboard.

Because the platform does not rely on agents or sidecars — and because it integrates with the cloud infrastructure — it sees every API, regardless of whether the API is registered with an API gateway. Internal and external APIs, legacy APIs (those that predate the API gateway), and shadow or rogue APIs (those not routed through a gateway) were all discovered, providing the customer with unprecedented visibility into the API attack surface.

Looking ahead

The banking leader uses a set of criteria to evaluate the success of its API security. One of these, which Akamai is providing support for, is rapid triaging. A key objective is determining how to analyze the severity of each finding, which would enable the SOC to rapidly evaluate, triage, and respond to an alert.

 | Published 08/24