Akamai

WHITE PAPER

API Security in Financial Services

Mitigating risks and ensuring trust

Executive summary

In the rapidly evolving landscape of the U.S. financial services industry, a subtle yet crucial struggle persists between traditional banking institutions and emerging fintech companies. Despite substantial global growth in open banking, the United States lags in its adoption, primarily because of the reluctance of traditional banks to cooperate with fintechs. This hesitancy to cooperate arises from tangible fraud risks associated with sharing sensitive banking information across unsecured networks.

Fintech companies, aiming to address the perceived risks, have turned to application programming interfaces (APIs) as a key to securely and efficiently exchanging consumer-permissioned data. However, the limited promotion of fidelity between banks and third parties within the U.S. banking infrastructure leaves the industry dependent on unsafe screen scraping technologies and an uncoordinated API landscape.

The U.S. financial sector urgently needs to shift from screen scraping to API-only innovation and align with the global trend toward open banking integration. The current utilization of a mere 36 unique APIs in the United States, compared with the United Kingdom's 196 and Germany's 80, underscores the inadequacy of the existing approach.

Financial aggregators present significant challenges, enticing customers with consolidated financial data while simultaneously posing cybersecurity risks. There is a need to transition toward secure APIs, urging financial institutions to enhance their understanding and management of application traffic. North American financial institutions must prioritize API security, navigate the challenges of screen scraping, and embrace standardized practices to strengthen their cyber defenses.

The growing importance of APIs

APIs are becoming an increasingly important part of banking and finance technology. Today, consumers prefer to bank digitally, with 78% of Americans saying they'd rather bank via a mobile app or a web browser. APIs play a pivotal role in digital banking, offering unparalleled convenience, speed, and security for customers who access banking products. APIs allow third-party applications to connect with a bank's tools, services, and valuable assets, streamlining connections for both parties. Customers now enjoy a broad range of financial activities, which has transformed the customer experience and propelled the financial industry into the digital age. APIs, which evolved from simple communication tools, have become the backbone of internet traffic, supporting various applications.

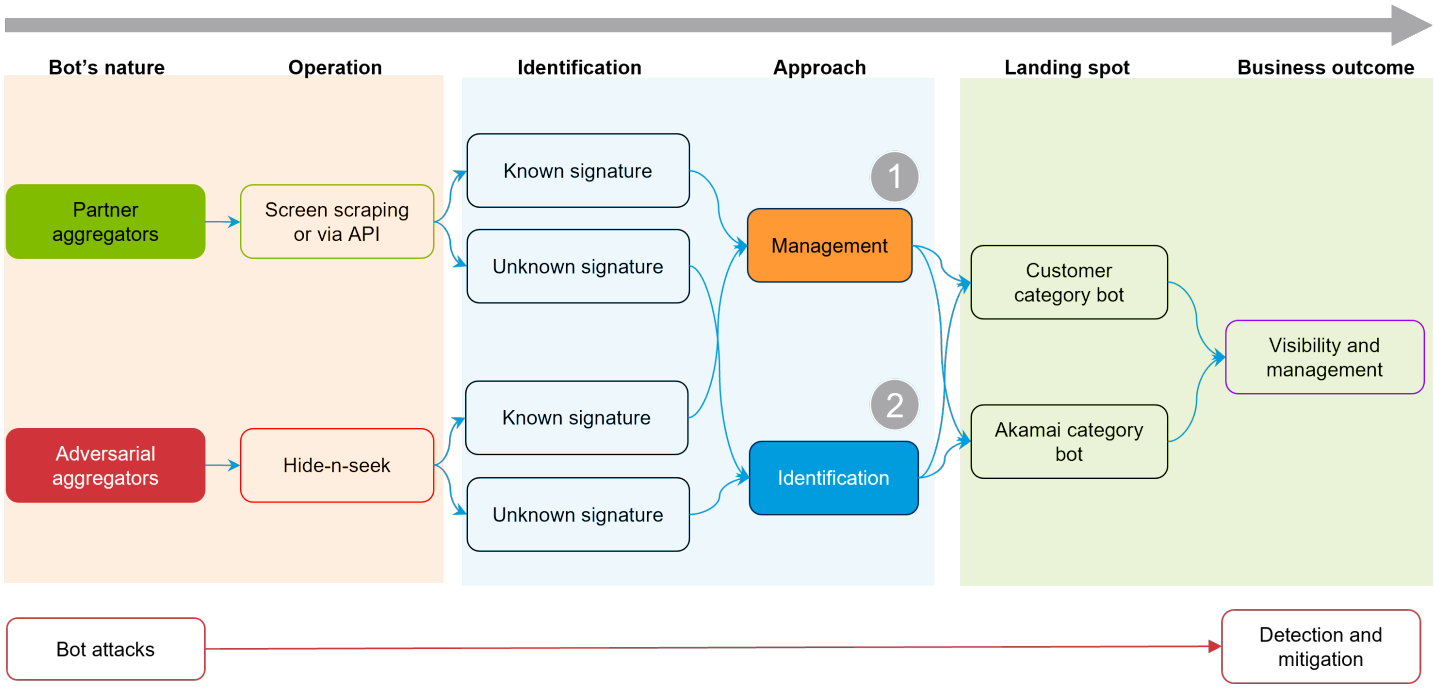
API workflows for aggregators

Financial data aggregators (FDAs) play a crucial role in the financial services industry by securely consolidating and providing access to a customer's financial information from various sources, such as banks, credit card companies, and investment accounts. This aggregation enables users to have a comprehensive view of their financial health through a single platform or application, streamlining financial management and planning processes. FDAs offer convenience and efficiency to customers and have become an integral part of modern fintech solutions.

However, the rise of FDAs has also brought about challenges, particularly with the surge in bot traffic in the financial services sector. Automated software programs called bots are increasingly used by cybercriminals to target FDAs and exploit vulnerabilities in their systems. These malicious bots attempt to

gain unauthorized access to customer accounts, extract sensitive financial data, and perform fraudulent activities. The sheer volume of bot traffic creates a significant burden on the FDA's infrastructure, leading to performance issues, potential data breaches, and concerns over data privacy and security. As the sophistication of bots continues to evolve, financial institutions and FDAs face a constant battle to detect and mitigate these attacks effectively, while ensuring uninterrupted service to legitimate users. Striking the right balance between offering seamless customer experiences and enforcing stringent security measures has become the paramount challenge in the financial services industry. Regulatory compliance, customer trust, and the reputation of financial institutions are all on the line, necessitating a proactive approach in implementing robust bot detection and prevention strategies.

Operationalize aggregator strategy



API-related threats in North America

API abuse poses unique challenges for financial institutions that extend beyond web application and API protection (WAAP). These challenges encompass discovering APIs across diverse landscapes, determining risk posture, understanding normal behavior, and identifying potential abuse.

A significant concern in the financial sector is the lack of visibility into API ecosystems and the absence of an enterprise-wide API inventory. API gateways, designed primarily for authorization, authentication, and rate limiting, lack security detection capabilities.

Financial institutions traditionally focus on north-south (command and control and exfiltration) traffic, but APIs differ by exposing core business functions externally, eliminating the need for classical kill chain steps. Identifying and cataloging APIs becomes increasingly complex because of API sprawl, which includes shadow APIs, zombie APIs, legacy APIs, orphaned APIs, and rogue APIs. Institutions must prioritize important APIs based on business impact and compliance violations, behavior monitoring, and serious misuse and criminal activity mitigation.

The absence of monitoring for abuse is a critical issue, as even seemingly flawless APIs can be exploited. For example, the abuse of new account credentials may lead to fraudulent account creation or unauthorized access to free credits. API scraping emerges as a substantial risk for financial institutions, equivalent to a modern data breach. This process, often low and slow, poses challenges in detection and necessitates API behavior monitoring.

In the context of accepted API traffic passing through WAAP products and gateways, questions arise regarding the monitoring of this traffic. Allowlisted traffic can bypass WAAP or API gateway controls, potentially exposing poorly configured rogue APIs to the internet without undergoing scrutiny. Internal east-west API traffic also circumvents these controls. API security addresses these challenges by collecting API activity data from any WAAP or gateway and sending it to a centralized data lake for comprehensive monitoring. It operates like a traffic camera by recording all API activity and performing behavioral analysis to enhance security measures.

Key API security risks

APIs can be vulnerable to a wide range of security risks, which can lead to data breaches, unauthorized access, and other forms of abuse. Key API security risks include shadow APIs, vulnerable APIs, API abuse, oversharing of sensitive information, and credential stuffing attacks.

- **Shadow APIs**. In many financial institutions, no single person or team is responsible for managing all APIs. This lack of oversight creates a significant security gap. Discovering and cataloging APIs across the organization is crucial to governing and securing them. It is important to bridge the gap between developers and security teams and detect shadow APIs in their environment. Ongoing discovery keeps you updated about newly discovered APIs or changes to existing ones, which can eliminate shadow APIs.

- **Vulnerable APIs.** Once APIs are discovered, financial institutions must assess their risk posture and identify vulnerabilities, especially for those carrying sensitive data. This step is vital to prioritizing security efforts effectively.

- **API abuse.** As digitization accelerates, the number of web attacks across North America continues to rise. Threat actors relentlessly target APIs, requiring robust security measures to thwart abuse and misuse.

- **Oversharing of sensitive information.** Modern apps often overshare sensitive data, which presents a new attack vector. Attackers can intercept traffic and gain unauthorized access to sensitive information.

- **Credential stuffing attacks.** Threat actors are targeting financial institutions using APIs to automate credential stuffing attacks.

API security challenges

API attacks are evolving, and today's security challenges include the lack of visibility into API inventory, the impact of disruptive API attacks, and the rapid growth of API traffic.

API inventory

According to a 2023 SANS survey, API inventory remains a critical issue for financial institutions. Financial institutions may not even be aware of all the APIs within their infrastructure, creating a governance and security blind spot. This lack of visibility may be one of the key factors contributing to the fact that API attacks often go undetected and unreported. The first step in securing APIs is to discover and catalog them comprehensively.

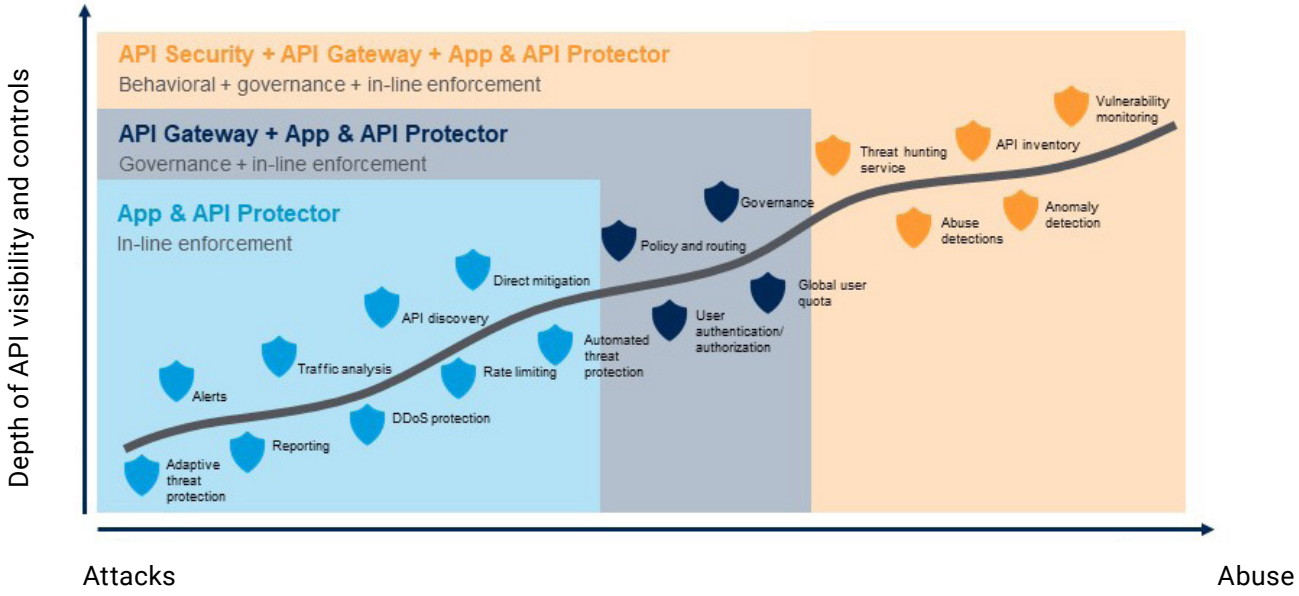
The impact of disruptive API attacks

Disruptions in the availability of web applications and APIs can significantly impact customer satisfaction and brand loyalty. With the increasing adoption of a digital-first approach, APIs have become even more critical for the success of financial institutions, especially in the context of open banking that has been embraced by fintech companies and traditional banks.

Rapid growth in API traffic

API traffic in the financial sector has experienced rapid growth, with traffic volume increasing into the triple digits. This growth challenges security controls to keep up with the evolving landscape of API-related threats.

API attacks are evolving



Regulations and security

Financial institutions that harness the power of APIs and other innovative technologies find themselves at the intersection of public policy and financial stability objectives. The important role of APIs in enhancing customer outcomes has made them the default connectivity and data exchange method within modern financial services environments, and they will continue to be so in the future. The overarching goals are to expand the array of financial options, foster increased competition and accessibility, and promote financial inclusion. Regulatory bodies are striving to broaden the scope of financial services, which will benefit both individuals and organizations.

The role of regulations in API security

The regulatory landscape plays a pivotal role in shaping and securing API practices within the financial sector. The Consumer Financial Protection Bureau's proposed rule exemplifies a commitment to fostering competition and consumer empowerment by mandating free access to personal financial data for sharing among financial firms. However, the lack of comprehensive regulations poses a hurdle to the widespread adoption of open banking in the United States.

Recognized standards like the Open Financial Exchange (OFX) and the creation of the Financial Data Exchange (FDX) by the Financial Services Information Sharing and Analysis Center (FS-ISAC) emphasize the importance of structured frameworks in improving data exchange. Regulatory bodies such as the Office of the Superintendent of Financial Institutions, which regulates federally regulated financial institutions, play a crucial role in guiding data-sharing practices and ensuring the security and integrity of financial data. Akamai solutions emerge as a key enabler, facilitating compliance with regulations while simultaneously addressing API quality concerns. By providing financial institutions with the tools needed to evaluate dedicated API interfaces, Akamai supports both regulatory adherence and ongoing innovation in the financial sector.

6 steps to building a robust API security strategy

The strategy of preventing API-based attacks by guarding endpoints and checking credentials is no longer enough. Today, a robust API security strategy must include the following six steps.

1. Collaborating with partners

Financial institutions and their security partners must collaborate closely by aligning people, processes, and technologies to establish a robust defense against API security risks. This collaboration includes development teams, network and security operation teams, identity teams, risk managers, security architects, and legal/compliance teams.

2. Discovering and cataloging APIs

The first step in securing APIs is discovering and cataloging them across the organization. This process allows security engineers to understand the scope of the attack surface and the potential exposure of sensitive information.

3. Testing vulnerability and assessing risk

Once APIs are discovered, financial institutions must conduct vulnerability tests and risk assessments to identify and address vulnerabilities in a timely manner. This process should be integrated into API development and upgrade cycles to ensure ongoing security.

4. Implementing behavioral detection

API protections are critical components of the overall application security framework. Behavioral detection is a key strategy to prevent vulnerable APIs from being exploited. This approach involves continuous monitoring and analyzing of API behavior to identify potential threats.

5. Prioritizing OWASP Top 10 controls

Financial institutions should prioritize the Open Worldwide Application Security Project (OWASP) Top 10 API Security Risks to ensure comprehensive protection. These controls cover the most critical vulnerabilities and attack vectors that affect APIs.

OWASP API Top 10 coverage by Akamai

- ☑ **API1:2023 — Broken Object Level Authorization:** BOLA vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs.
- ☑ **API2:2023 — Broken Authentication:** BA refers to broad vulnerabilities in the authentication process, exposing the system to attackers that can exploit these weaknesses to compromise API object protection.
- ☑ **API3:2023 — Broken Object Property Level Authorization:** BOPLA is a security flaw where an API endpoint unnecessarily exposes more data properties than required for its function, neglecting the principle of least privilege.
- ☑ **API4:2023 — Unrestricted Resource Consumption:** This is a type of vulnerability, sometimes called API resource exhaustion, where APIs do not limit the number of requests or the volume of data they serve within a given time.
- ☑ **API5:2023 — Broken Function Level Authorization:** BFLA can occur when access control models for API endpoints are incorrectly implemented.
- ☑ **API6:2023 — Unrestricted Access to Sensitive Business Flows:** This risk arises when an API exposes critical operations like business logic without sufficient access control.
- ☑ **API7:2023 — Server Side Request Forgery:** SSRF allows an attacker to induce the server-side application to make HTTPS requests to an arbitrary domain of the attacker's choosing.
- ☑ **API8:2023 — Security Misconfiguration:** This refers to the improper setup of security controls, which can leave a system vulnerable to attacks.
- ☑ **API9:2023 — Improper Inventory Management:** This is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including deprecated, legacy, and/or outdated APIs — may be left unpatched and vulnerable to attack.
- ☑ **API10:2023 — Unsafe Consumption of APIs:** This refers to the risks associated with the use of third-party APIs without putting proper security measures in place.

6. Learning from peers

Financial institutions should learn from their peers and share best practices. Membership in the FS-ISAC enables financial institutions to take advantage of their intel platform, resources, and trusted peer-to-peer network of experts to help anticipate, mitigate, and respond to cyberthreats. A clear understanding of how other organizations address API security challenges can help enhance security measures for the industry as a whole.

Conclusion

In this era of rapid digital transformation and widespread API adoption — which was designed to facilitate flexible, swift, and cost-effective integration across a wide spectrum of software, devices, and data sources — safeguarding APIs is of paramount importance for financial institutions. Nonetheless, API security presents a complex juggling act, involving various features, functions, and demands of the business. Neglecting API security can lead to severe consequences, including cyberattacks, data breaches, regulatory infractions, and damage to an institution's reputation.

Our data indicates that API functionality ranks among the top targets for threat actors who continuously evolve and adapt their methods of attack. Therefore, it is imperative that API security shifts toward the edge, moving away from your infrastructure and closer to the digital touchpoints where customers engage with your data and applications. This strategic adjustment is crucial to ensuring robust protection for your digital assets.

Learn more about Akamai for financial services. Or reach out to your Akamai contact to further discuss this topic and how it applies to your organization.