WHITE PAPER

Advancing Financial Services in Asia-Pacific with Robust API Security

Executive summary

According to the International Monetary Fund, the Asia-Pacific (APAC) region will continue to see significant economic growth — 4.2% in 2024. In the ever-evolving landscape of this growth, particularly in the financial services sector, application programming interfaces (APIs) have emerged as a central driving force behind the industry's digital transformation. APIs serve as the technological bridge that connects various components of banking systems, enabling a seamless exchange of data and functionality. They have revolutionized the way financial services are delivered, providing customers with a host of advantages.

The rapid growth in the use of APIs has not been without its challenges, as illustrated by the IDC prediction that security spending in APAC will reach US$55 billion by 2026. As financial institutions have expanded their digital offerings through APIs, they have inadvertently exposed themselves to a multitude of security vulnerabilities. This surge in API usage has led to an exponential increase in the potential attack surface for cybercriminals. Threat actors recognize the inherent value of financial data and have adapted their tactics to exploit these newly available entry points.

In response to this growing threat landscape, financial institutions have been compelled to invest heavily in cybersecurity measures. They are not only focused on safeguarding their own systems but also on protecting the sensitive data and assets of their customers. This has led to a heightened emphasis on threat detection, response strategies, and collaboration with industry peers and cybersecurity experts to mitigate the risks posed by cyberattacks.

The digital transformation in the APAC financial services industry, driven by APIs, is a testament to the industry's adaptability and commitment to meeting the evolving needs of customers. Nevertheless, as this transformation unfolds, the industry must remain vigilant in its efforts to fortify its cybersecurity posture, address security vulnerabilities, and ensure that the benefits of digital innovation are not overshadowed by the ever-present threat of cyberattacks.

The growing importance of APIs

The APAC region is experiencing a digital revolution in the financial services sector. APIs have been a driving force, facilitating an unprecedented level of convenience, speed, and security for customers seeking access to banking products and services. Customers now have a wide range of financial activities at their fingertips, from checking account balances and transferring funds to applying for loans and managing investments. This convenience has not only reshaped the customer experience but has also propelled the financial industry into the digital age. APIs have evolved from simple system-to-system communication tools into the backbone of internet traffic, supporting a wide array of applications and services.

According to a report by Polaris Market Research, the global open banking market size was valued at US$16.14 billion in 2021 and is projected to reach US$128.12 billion by 2030, growing at a compound annual growth rate of 26.8% during the forecast period. Polaris's research also highlighted the APAC region as the one that will experience the most growth over the forecast period. For the financial services industry in APAC to reap the benefits of the promise of open banking, there must be a concerted effort to meet the challenges of API security.

Leading the pack in the region is Singapore, with an API playbook published by the Monetary Authority of Singapore (MAS). In 2018, MAS also led the establishment of API Exchange (APIX), an initiative jointly formed with the World Bank Group's International Finance Corporation and the ASEAN Bankers Association. It is an online global marketplace and sandbox for collaboration between financial institutions and financial technology institutions.

Several other countries in Asia have long been working on initiatives to develop open banking. India has been working on improving financial inclusion for the large unbanked and underbanked population in that country.

One of the government's early initiatives was the unified payments interface in 2016, which allowed the general public to access bank accounts and execute transactions via authorized third parties using API protocols. In 2021, the Reserve Bank of India launched Account Aggregators, a framework that creates consent managers and allows consumers to digitally access and control their financial records and eases the process of data sharing with financial service providers.

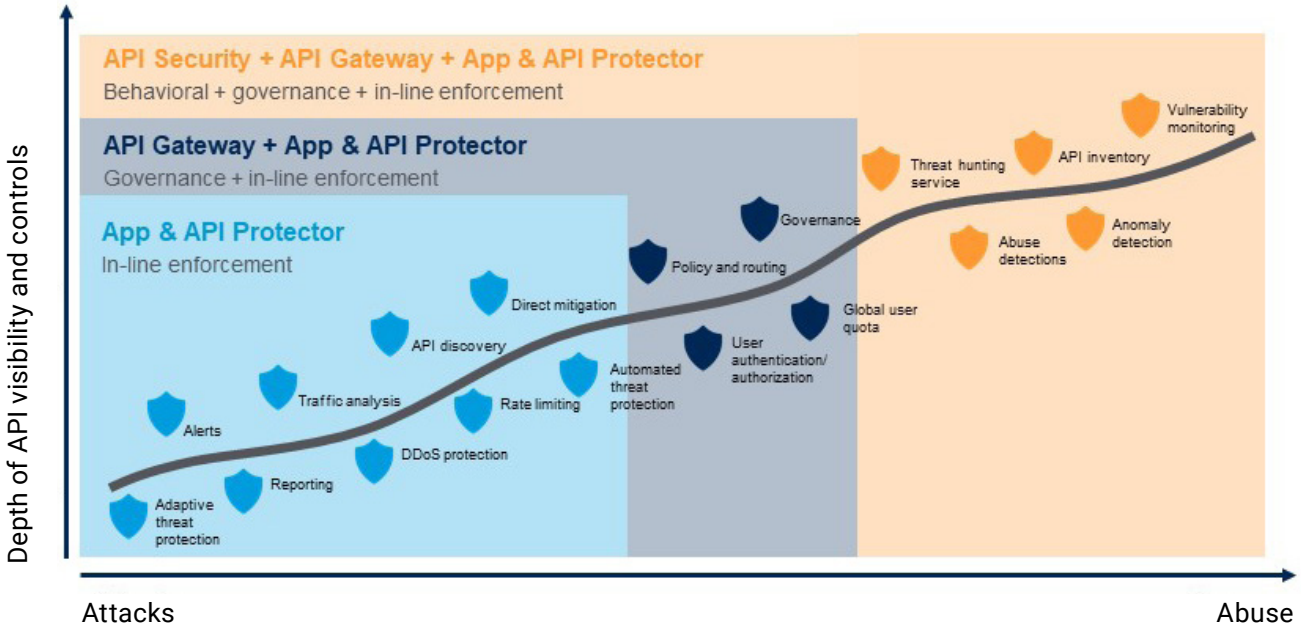
Even with this focus, the financial services industry in APAC continues to be one of the most attacked industries in the world, experiencing a growth in web application and API attacks by 36% from Q2 2022 to Q2 2023 — a staggering 3.7 billion attacks in 18 months. The APAC region, home to numerous financial hubs, has witnessed a sharp increase in web application and API attacks.

API-related threats in APAC

Web application and API attacks in the APAC region have risen dramatically, with a 248% increase in attacks from 2021 to 2022 for financial services. The vulnerabilities of APIs have led to numerous large scale, high-profile breaches, including the Optus data breach in Australia and the T-mobile API data breach in the United States These incidents underscore the need for robust API security solutions that go beyond guarding endpoints and checking credentials.

In this white paper, we will explore the strategies that can address this critical attack surface and secure APIs effectively. And we'll discuss how a proactive approach to API security can ensure compliance and data protection.

API attacks are evolving



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 prioritize security efforts effectively.

- **API abuse.** As digitization accelerates, the number of web attacks across APAC 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, presenting 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

Undetected and unreported attacks

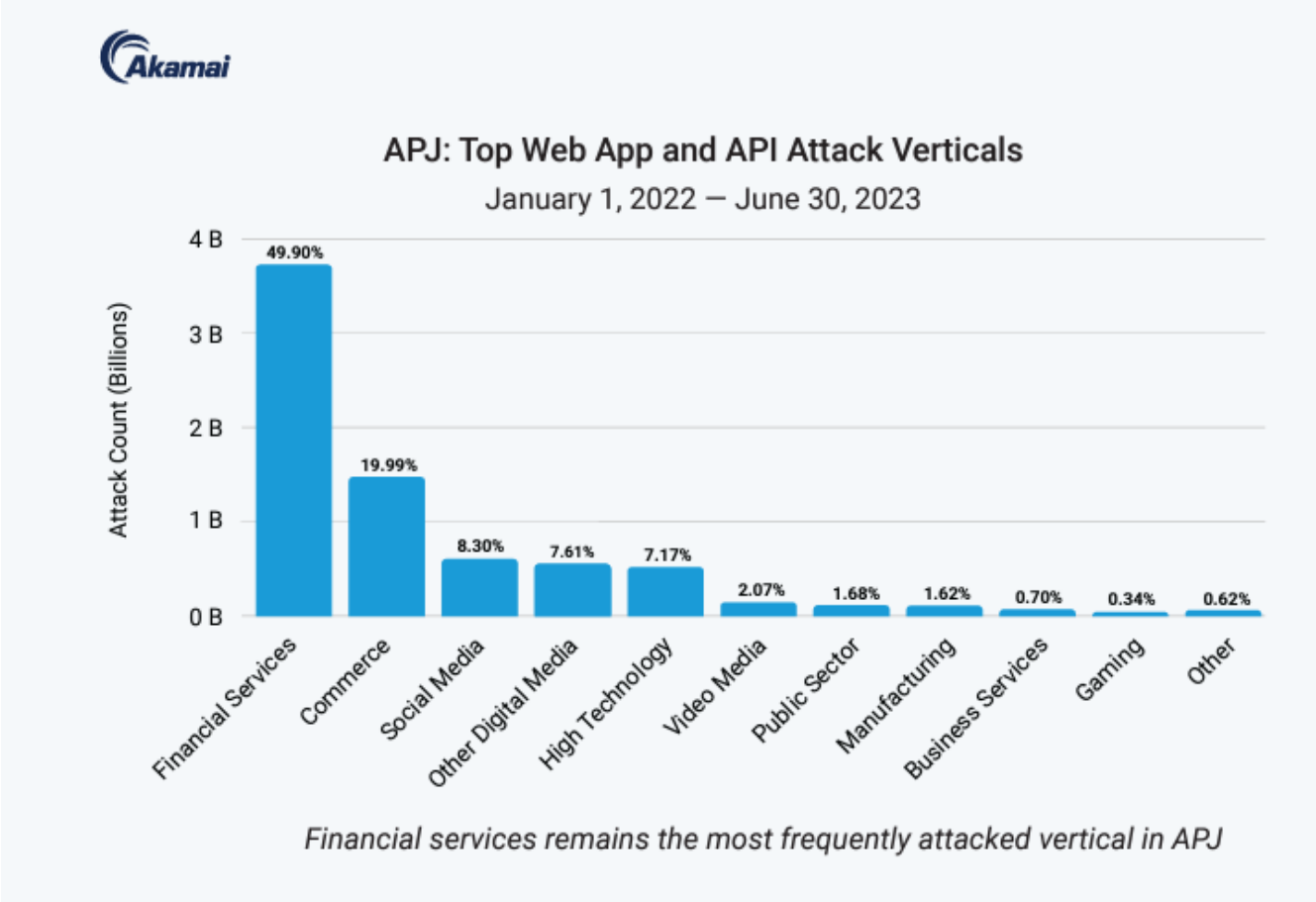
According to a recent SANS survey, API inventory remains a critical issue for financial institutions. Financial institutions may not even be aware of all the APIs within their infrastructure, creating a governance and security blind spot. This lack of visibility may be one of the key factors contributing 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.



Financial services remains the most frequently attacked vertical in APJ

Regulations and security

Financial institutions harnessing the power of APIs and other innovative technologies find themselves at the intersection of public policy and financial stability objectives. Within the diverse landscape of financial regulators in the APAC region, there exists a shared commitment to enhancing customer outcomes. The overarching goals are to expand the array of financial options, foster increased competition and accessibility, and promote financial inclusion. Regulatory bodies throughout the APAC region are striving to broaden the scope of financial services, benefiting both individuals and organizations.

According to the World Bank, a staggering 1.7 billion adults worldwide lack a bank account. Notably, the three countries with the largest percentages of unbanked individuals are situated in Asia, with China at 13% (approximately 225 million people), India at 11% (190 million people), and Indonesia at 6% (96 million people). This vast untapped market of unbanked and underbanked individuals and enterprises in the APAC region is estimated to range from US$55 billion to US$115 billion.

The role of regulations in API security

Regulations such as the Revised Payment Services Directive (PSD2) promote transparency by requiring traditional institutions to share data with external entities. These regulations aim to protect end users' data, privacy, and security. Financial institutions must adhere to these regulations while continuing to innovate.

While regulations foster data sharing, they also dictate how organizations must store and protect data and data access. Akamai solutions can help financial institutions comply with these regulations without hampering their innovation efforts.

6 steps to building a robust API security strategy

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

1. Collaborating with partners

Financial institutions and their security partners must collaborate closely, 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 attack surface's scope 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 Financial Services Information Sharing and Analysis Center (FS-ISAC) gives members the advantages of their intel platform, resources, and a trusted peer-to-peer network of experts to 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 in the APAC region. 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 the 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 at akamai.com/finserv

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn. Published 02/24