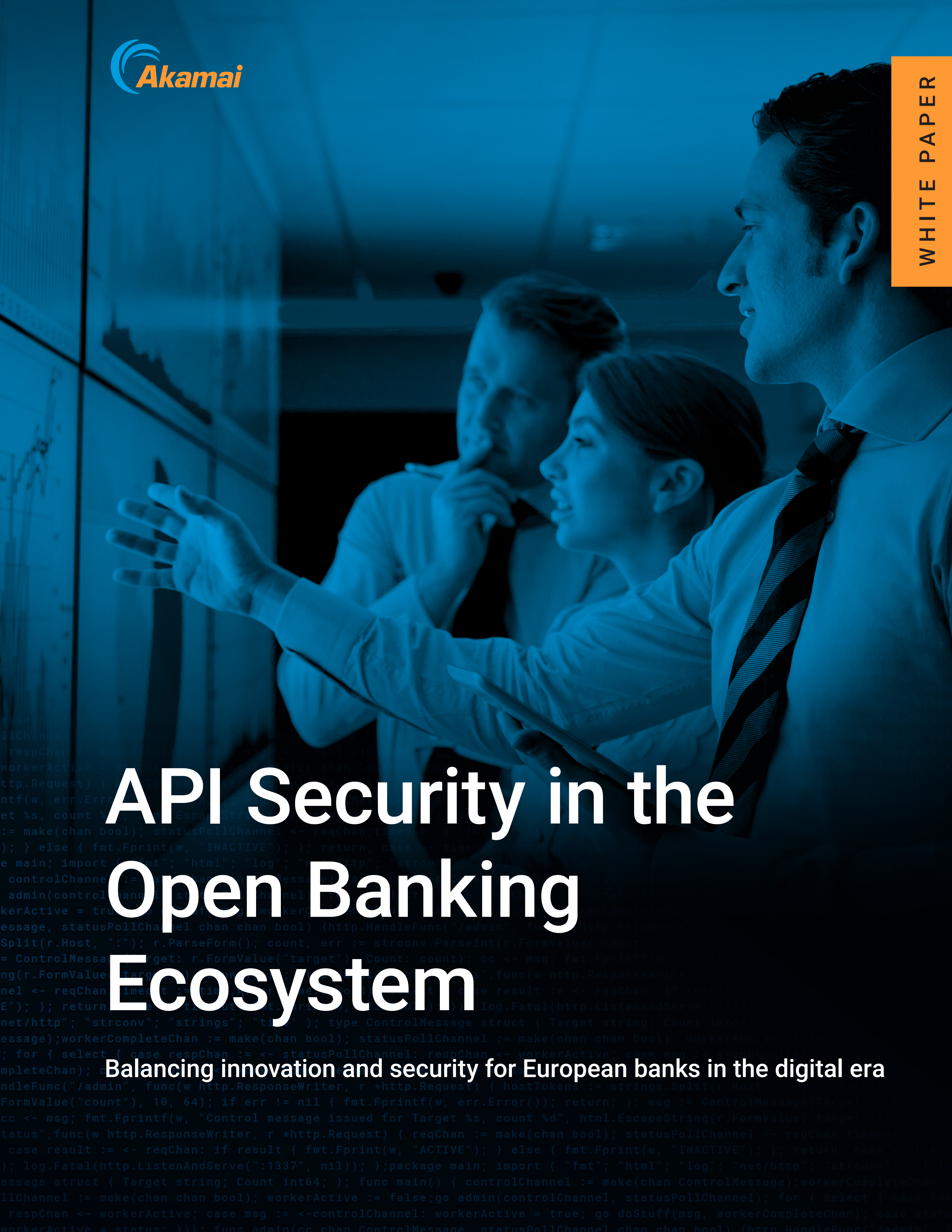


WHITE PAPER

API Security in the Open Banking Ecosystem

Balancing innovation and security for European banks in the digital era

Executive summary

In 2023, banks in Europe, Middle East, and Africa (EMEA) enjoyed significant profitability, and that is expected to persist into the upcoming year. Application programming interfaces (APIs), which constitute 31% of all web traffic, have been instrumental in this growth, facilitating various services like banking transactions, remote cheque deposit, and GPS-assisted automated teller machine locations, along with third-party services. However, the rapid adoption of APIs has expanded the cyberthreat landscape, prompting substantial cybersecurity investments by financial institutions.

The European Union's revised Payment Services Directive (PSD2) and the anticipated PSD3 have played a pivotal role in shaping data exchanges between traditional banks and fintechs. Regulatory Technical Standards (RTS) enforce secure API usage, incorporating strong customer authentication (SCA) and common and secure open standards of communication (SCA-RTS). PSD2, although primarily focused on payments, has propelled the term "open banking" in the United Kingdom, emphasising the sharing of customer-permissioned account data and paving the way for broader "open finance" solutions. At the heart of these open finance solutions lie APIs.

The ongoing digital transformation in EMEA's financial services industry, driven by APIs, showcases the industry's adaptability and commitment to meeting evolving customer needs. However, as this transformation unfolds, vigilance is essential to fortify cybersecurity, address vulnerabilities, and ensure that the benefits of digital innovation prevail over the ever-present threat of cyberattacks. McKinsey reports major banks are planning to allocate 14% to API programs, reflecting the surge in API usage and prompting substantial cybersecurity investments. Financial institutions now prioritise safeguarding internal systems and protecting customer data and assets, emphasising a focus on threat detection, response strategies, and collaboration to effectively counter cyber risks.

The growing importance of APIs

EMEA is experiencing a digital revolution based on the desire to provide more efficient and tailor-made services and products to their financial services customers. APIs play a pivotal role, 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, evolving from simple communication tools, have become the backbone of internet traffic, supporting various applications.

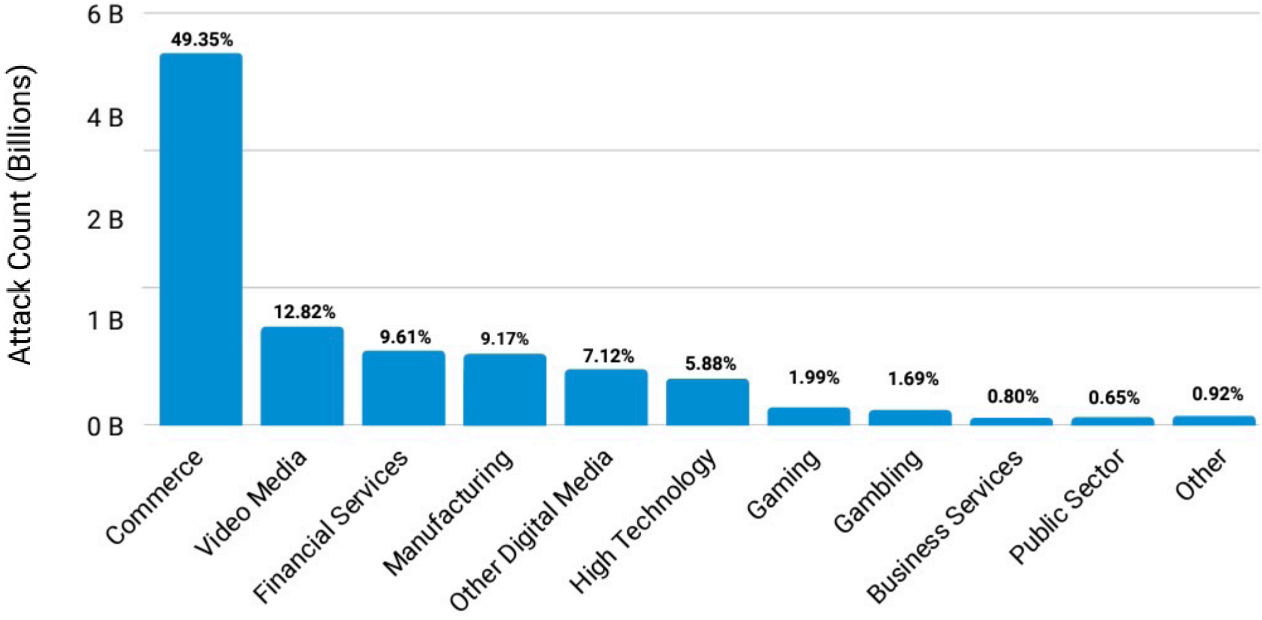
According to Allied Market Research, the European open banking market reached US$6.14 billion in 2020 and is expected to soar to US$48.30 billion by 2030, with a 23.18% compound annual growth rate from 2021 to 2030. Initiatives like the Open Bank Project, led by Berlin-based TESOBE, accelerate this adoption. Collaborating with more than 40 banks globally, the Open Bank Project empowers banks to offer third-party apps and services to customers through an open API and app store. In France, consolidation around the STET API, provided by the Systèmes technologiques d'échange et de traitement (STET) clearinghouse, is helping the implementation of open banking payments. APIs are at the forefront of rapidly reshaping the financial landscape across EMEA and the rest of the world.

API-related threats in EMEA

The financial services industry emerges as the third-most-targeted sector in the EMEA region; it's the target of almost 10% of the onslaught of web application and API attacks between January 2022 and June 2023. This translates to a staggering 1 billion of the total 11 billion web attacks across EMEA's industries, which signifies a significant 119% increase year over year from Q2 2022 to Q2 2023. By delving deeper, we find that the United Kingdom led with 59.2% of web application attacks, experiencing the highest year-over-year growth at 79%, followed by the Netherlands at 16.2%, and then Germany at 10.7%.

EMEA: Top Web App and API Verticals

January 1, 2022 — June 30, 2023



Financial services is the third-most frequently attacked vertical in EMEA

Key API security risks

APIs can be vulnerable to a wide range of security risks, which can lead to data breaches, unauthorised 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 cataloguing APIs across the organisation 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 on 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 prioritise security efforts effectively.

- **API abuse.** As digitisation accelerates, the number of web attacks across EMEA 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 unauthorised access to sensitive information.

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

API security challenges

API inventory

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 catalogue them comprehensively.

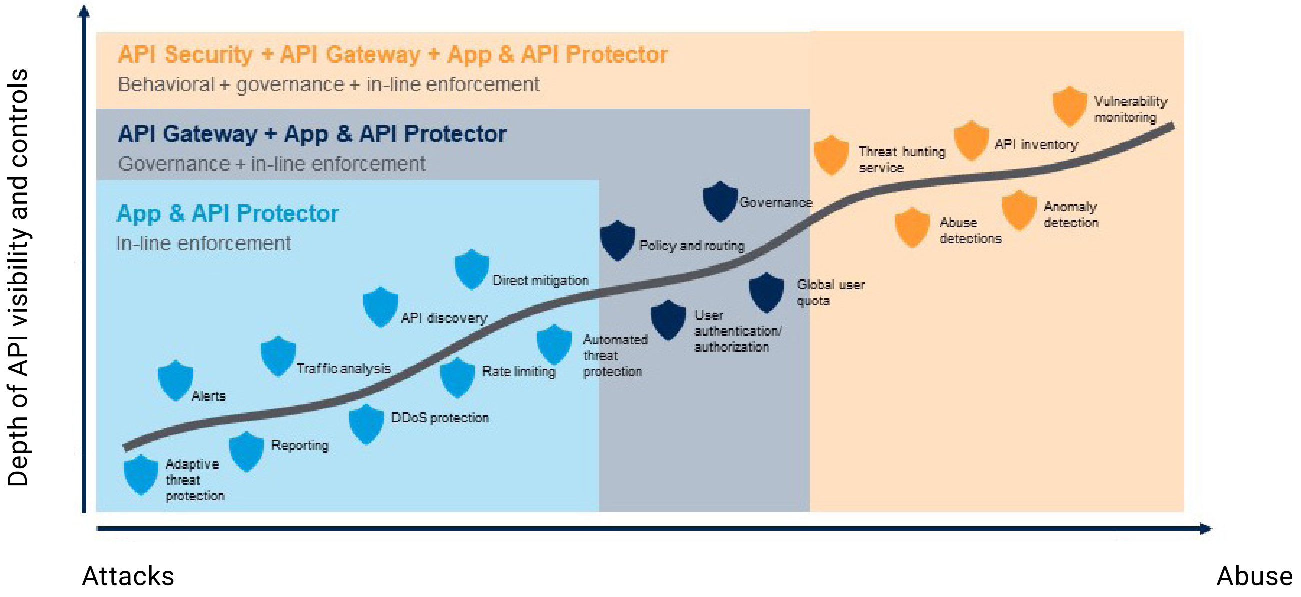
The impact of disruptive API attacks

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


API Security + API Gateway + App & API Protector
Behavioral + governance + in-line enforcement
API Gateway + App & API Protector
Governance + in-line enforcement
App & API Protector
In-line enforcement
Vulnerability monitoring
Threat hunting service
API inventory
Governance
Anomaly detection
Abuse detections
Policy and routing
Direct mitigation
Global user quota
API discovery
User authentication/ authorization
Automated threat protection
Traffic analysis
Rate limiting
Alerts
DDoS protection
Reporting
Adaptive threat protection
Depth of API visibility and controls
Attacks
Abuse

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 throughout EMEA are striving to broaden the scope of financial services, which will benefit both individuals and organisations.

The role of regulations in API security

Regulations like PSD2 (and, soon, PSD3) promote transparency by mandating that traditional institutions share data with external entities, prioritising end users' data, privacy, and security. Financial institutions must uphold these regulations while actively pursuing innovation.

While regulations promote data sharing, they also specify how organisations store and safeguard data. Financial institutions require a technology partner that ensures regulatory compliance without hindering innovation. Such a partner should address concerns regarding API quality and provide authorities with tools to assess dedicated API interfaces from banks and other financial entities.

According to the European Banking Authority, "The experience gained from implementing PSD2 highlights the absence of a single API standard, resulting in varied API solutions across the EU. This poses significant challenges for third-party service providers, necessitating substantial efforts to connect to different Account Servicing Payment Service Providers' APIs and adapt connections to evolving APIs." The expectation is that PSD3 will incorporate the lessons learned from PSD2.

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 defence 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 cataloguing APIs

The first step in securing APIs is discovering and cataloguing them across the organisation. 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 behavioural detection

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

5. Prioritising OWASP Top 10 controls

Financial institutions should prioritise 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) 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 organisations 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 EMEA. 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 towards the edge, moving away from an organisation's infrastructure and closer to the digital touchpoints where customers engage with 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 organisation.

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 01/24.