OPEN BANKING AND APIS

API security in the banking and payments ecosystem

By Tari Schreider, strategic advisor, cybersecurity, Datos Insights

Around 2000 BCE (Before the Common Era), the first form of banks emerged in Assyria and Sumer when merchants extended grain loans to farmers. Over 4,000 years later, banking is very different, with the advent of digital loans and electronic payment processing. However, one constant has remained over 40 centuries; the world's economies cannot function without debt. Supplying the debt requires a digital economy operating around the clock, fueling over 60 major economic centres. The differential market advantage for banks is speed – those that can create, process and service loans fast win the day. This differential advantage comes from advanced applications based on generative AI. But these applications need to speak to one another as well as provide customers with a degree of control. The connective tissue of this digital economy is the application programming interfaces (APIs) that connect banking and payment processing applications. APIs are enabling the next generation of global banking and payment processing in the era of open banking.

APIs enable open banking

Open banking was born in the European Union with the 2018 Payment Services Directive (PSD2) and accelerated in the UK and Canada. Now it is on the precipice of adoption in the USA. If open banking is the future, understanding it is essential. Open banking provides third-party financial service providers access to consumer banking, transaction processing and financial intelligence data. It creates an unprecedented ecosystem where banks, credit unions and non-traditional financial entities share information through APIs that enable the networking of accounts and data across financial entities. Open banking is reshaping the financial industry.

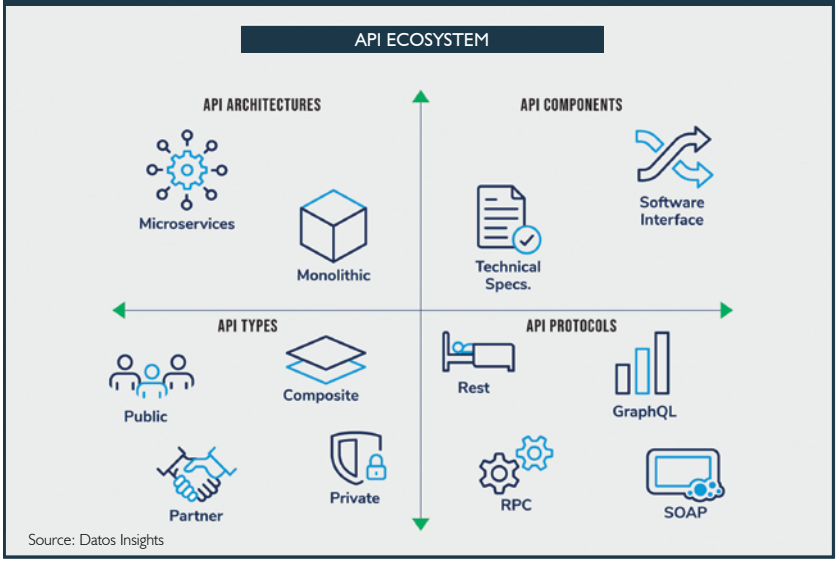
Once a customer grants consent, financial entities can allow access to and control of their personal and financial data to third-party service providers, most of which are fintech startups with purpose-built business models leveraging open banking. This data sharing occurs through APIs and access to massive data lakes. The power of aggregating data from many sources can be seen in its ability to provide enhanced customer profiles, including buying intents and purchasing sentiments. Toss in generative artificial intelligence and machine learning and you have the keys to the consumer kingdom. Open banking is busting down the walls of centralisation and ushering in the time of financial networking anywhere, anytime. With open banking, one can easily enrol in and de-enrol from financial services with a simple click.

Tari Schreider
Datos Insights

API sprawl is shockingly pervasive: today the average number of APIs organisations use is over 20,000. Lack of API management and oversight leads many organisations to promote APIs to production with known security issues. API sprawl creates a target-rich attack surface motivating hackers to develop an increasing number of zero-day API attacks.

Expansive ecosystem to protect

Making open banking work requires a complex ecosystem and orchestration of APIs



Source: Datos Insights

With great openness comes great risk

All this sounds pretty cool, right? It does, until it isn't, however. The promise of open banking can only be realised as long as it is secure. APIs serve as the lifeblood of open banking but are one of the most sought-after and compromised components in an attack by hackers. Datos Insights sees increasing data breaches as hackers focus on open banking APIs. In the USA, there are 4,135 FDIC-insured banks, most being small and generally having less rigorous cybersecurity control. Hackers gravitate to low-hanging fruit to initiate a compromise. With the potential for massive financial industry interconnectivity, the risk is real.

Open banking creates a risk trifecta where fraud, loss of privacy and data exfiltration come with the territory

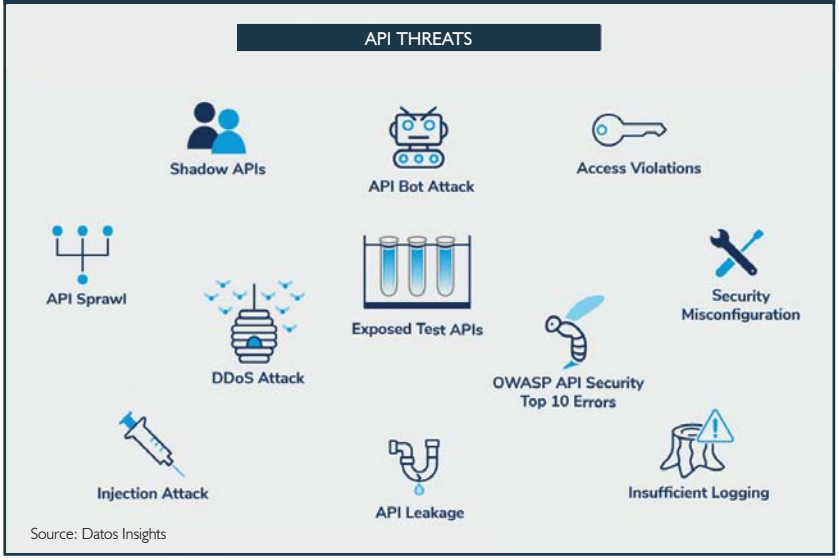
The threat of banking system compromise will move from the application to the API. Hackers have become adept at attacking banking customers' mobile apps, but the haul of illegal bounty is less than achieved through an API that, once compromised, is the gateway to great troves of customer financial data. Hackers will leverage open banking communication between a mesh of financial entities where the entity and the customer manage security. Guess which is the weakest link?

Threats are everywhere

API security is directly related to application security; subsequently, APIs have many of the same frailties of compromise as applications. APIs are critical because they transfer data between clients and servers connected over public networks, but there are many points of potential weakness that hackers can leverage to compromise APIs.

Many points of weakness

The top threats financial institutions face when using APIs



Source: Datos Insights

API exploitation is growing in frequency and sophistication, accounting for 1 billion compromised records. Zero-day attacks have led to single-event compromises of hundreds of millions of records.

Open banking creates a risk trifecta where fraud, loss of privacy and data exfiltration come with the territory. Hackers can trace the many APIs a single transaction can generate across many partners, looking for an easy access point to breach. Open banking leaves us with a huge attack surface to protect. Fortunately, we have a little time to prepare; open banking in the USA is still in its infancy, with most efforts being groundwork where financial entities negotiate bilateral agreements to share data. These agreements provide the why, but the detail is in the how. On top of that, the Consumer Financial Protection Bureau (CFPB) rule, part of Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act covering consumer access to financial records, is still flailing about in Congress.

Solving the API risk problem

An API security model is not unlike many other security models within organisations. APIs are exposed to the same threats and vulnerabilities as other components of an attack surface, but the context is different. An API security model typically includes six core components:

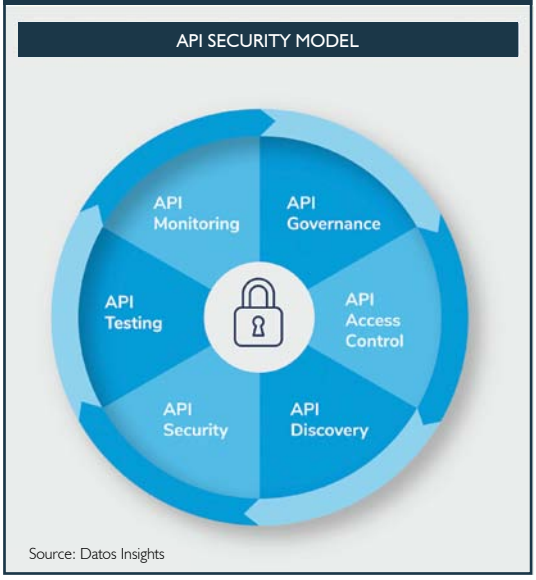
- API governance: APIs require proper management through standards, policies and procedures. Governance is used throughout the life cycle of an API, from design to retirement. Governance instils consistency across an API repository, ensuring APIs are built according to standard security practices. Poor governance leads to badly developed APIs, a lack of oversight and unreliable risk management.
- API access control: Only authorised users should have access to APIs and their functions. API access control is a combination of authentication and authorisation. Access lists, tokens, and identity and access management roles can all be used to control API access. A zero-trust architecture is incomplete without proper API access, authentication and authorisation. Two primary ways to

protect APIs include a single token string (i.e. a small hardware device providing unique authentication information) and basic authentication that uses a two-token string solution (i.e. username and password).

- API discovery: APIs must be discovered and inventoried to identify external API endpoints, orphan APIs, shadow APIs and API sprawl. Discovery must be automated and continuous to be effective. Discovered APIs should be evaluated for vulnerability and scored by risk level to understand which are most in danger of attack. Unknown APIs lead to unknown risks.
- API security: Preventing hacking by applying security protocols is essential to securing the API ecosystem. API security encompasses many aspects of security, from access control and runtime protection to API attack surface discovery. Contemporary models of API security understand its context and can properly execute discovery, apply runtime protection and react to attacks. Adhering to the recommended Open Web Application Security Project (OWASP) 10 API controls is a must practice.
- API testing: APIs must be tested to ensure the basic security requirements, including access, encryption and authentication, have been addressed. API testing should be included in any development, security and operations (DevSecOps) function. Security testing can be performed using DAST (dynamic application security testing) and SAST (static application security testing) solutions, purpose-built API security test benches and API security platforms.

FIs can use APIs securely

Model of an API security approach



Source: Datos Insights

- API monitoring: API data must be collected and analysed to track performance, availability, functionality and security state. Monitoring should track consumer interactions, data exchanges and third-party access using real-time data collection and analysis. Sampling monitoring is available.

With the move toward open banking, APIs are the future of the financial services industry; Datos Insights expects banks will likely double their API adoption in the next two to three years. Open banking has arrived in many countries in Asia, Europe and South America – and North America is on the threshold. The degree of adoption is predicated on regulations and cooperation, but one truth remains: APIs are the future, and secure APIs are a prerequisite. Deploying API security policies and a secure API architecture needs to start now. ■

Banks will likely double their API adoption in the next two to three years

NEW NAME, SAME COMMITMENT:
FOCUSED INSIGHTS, PERSONAL SERVICE, AND CUSTOMER IMPACT

Find out more about what Datos Insights can do for you.

datos-insights.com