TRACEABLE

WHITEPAPER

Banking on APIs: API Security for Financial Services

How To Take Control Of Your API Attack Surface, Protect Your Customers And Their Assets, And Maintain Compliance With API Security.

Table of Contents

Executive Summary

API Security for Financial Services: Why Now?

Financial services organizations including banks, payment providers, and fintech companies increasingly rely on APIs to power every part of their online services and consumer experience. This includes:

- Customer account creation
- User login and authentication
- Account and asset authentication
- Asset transfers between accounts and institutions
- Mobile deposits
- Payments
- And more...

As a security leader in a financial services organization, you have witnessed the explosion of APIs in your organization firsthand. Your organization's development teams are building, modifying, and integrating with APIs at a rapid pace - in many cases without proper security controls in place. This API sprawl has drastically altered your application's attack surface. Even if you are manually maintaining an inventory of your APIs, there is always the risk that unmanaged "shadow APIs" could introduce vulnerabilities to your application.

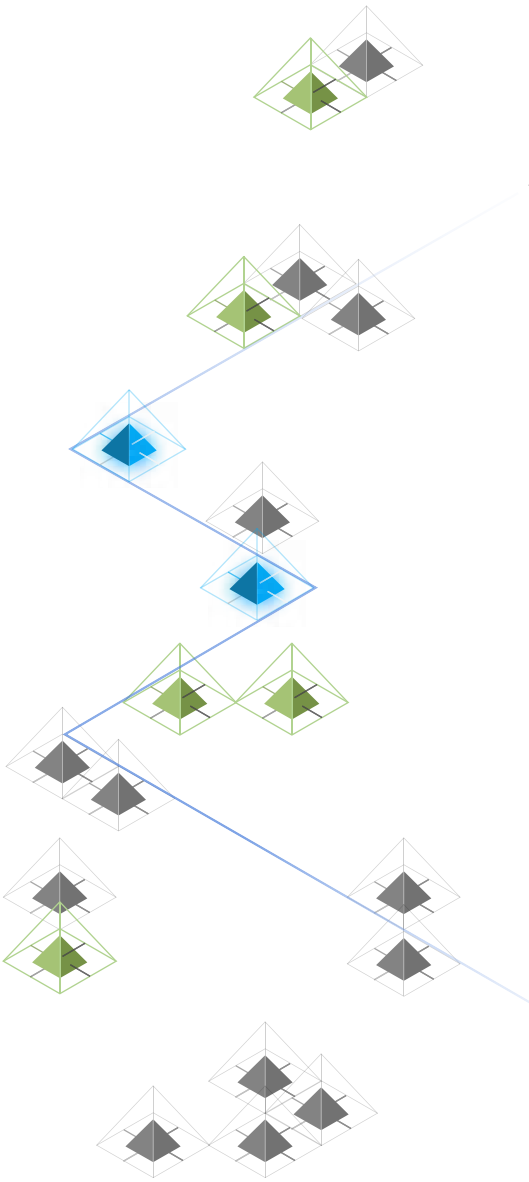
Financial Services APIs are Targeted

According to Gartner, APIs are now the most frequent attack vector, resulting in large-scale data breaches for enterprise web applications. Financial services APIs are a rich target for threat actors because they hold the keys to financial assets, account credentials, and sensitive data including PII and payment information protected under PCI-DSS. A successful attack on financial services APIs could have serious consequences for your organization such as a data breach, compliance violations, compromised user accounts, theft of assets, and reputational damage.

Compliance is Evolving

In recent years, regulations impacting the financial services industry have evolved to account for the new API attack surface. The FFIEC (Federal Financial Institutions Examination Council) addressed APIs security in an 2022 update to the Cybersecurity Resource Guide for Financial Institutions. This update explicitly calls out APIs as a separate attack surface in regulatory guidelines. The new FFIEC guidance requires a complete inventory of APIs and an audit of APIs as part of a risk assessment for digital banking and information systems. For payment processors and providers, achieving PCI-DSS 4.0 compliance requires organizations to install and maintain network security controls, maintain a vulnerability management program, and regularly monitor and test networks. API security can play a key role in each of these requirements.

With the challenges of API sprawl, an evolving regulatory landscape, and increasingly sophisticated threats, it's no wonder that API security is top of mind for security leaders in financial services organizations. In this guide, we'll dive deep into API security: why it's needed, what capabilities are essential, and how you can get started.



API Security Challenges for Financial Services

API Sprawl & Shadow APIs

Your development teams frequently update existing APIs, create new APIs, and integrate with 3rd party APIs. These changes expand your API attack surface and can potentially introduce vulnerabilities into your applications. It's your responsibility to secure that attack surface, but as the complexity of apps and the number of APIs grows, it is becoming harder and harder just to keep track of how many APIs exist, where they are in your applications, and what functions they serve. This is the root of API sprawl.

Maintaining an inventory of APIs is critical for API security. Like all other aspects of security, you can't secure what you can't see. Without an inventory, it's nearly impossible to ensure that you are adequately protecting your application from API-based threats. You need to know what APIs you have in order to conduct penetration tests and automated vulnerability testing, and to understand the security posture of your APIs in any comprehensive manner.

Unfortunately, it's no longer practical to maintain an inventory of APIs manually. In most organizations the speed of development is too fast and manual inventories are out of date too quickly. Even if you are particularly religious about updating the API inventory, it's impossible to know what you've missed with a manual inventory process. This can lead to "shadow APIs" that are unmanaged by security teams and potentially vulnerable. Major organizations including the Australian Telecom Optus have suffered data breaches due to vulnerable shadow APIs that were accidentally left exposed to the internet.

The challenges of API sprawl and shadow APIs are common to organizations across all industries, but in financial services the consequences are particularly high because of the sensitive data and assets you are tasked with protecting. Automated, continuous discovery and inventory of all types of APIs in your organization is just the first step towards protecting your APIs and securing your customers' data and assets.

API Fraud and Abuse

Digital fraud and abuse are among the most insidious types of API attacks impacting financial services organizations. Detecting fraud and abuse at the API layer is challenging because attackers often use legitimate credentials to access and manipulate data. This can make it difficult for traditional security solutions, which lack deep API data and long-term contextual awareness, to distinguish between legitimate and fraudulent activity. The challenge is particularly acute when an attack occurs over an extended period of time.

Fraud within APIs can take various forms depending on the API's specifics. However, broadly speaking, API based digital fraud and abuse attacks exploit legitimate functionality for the attacker's benefit. Examples include a race condition that allows a malicious user to continually top up a gift card with money, resource abuse where an attacker repeatedly signs up for a server hosting trial to mine crypto, identity fraud or account takeovers where a fraudster assumes another person's identity, or even internal fraud, where an employee collaborates with an external actor to bypass security controls. Most digital fraud and abuse attacks are specific to the enterprise they are targeting making them especially difficult to mitigate. Here are a few types of digital fraud and abuse that impact the financial services industry:

New Account Fraud

Banks, mobile payment apps, and credit card providers are all prime targets for new account fraud. New account fraud occurs when fraudsters register new accounts in order to abuse account resources or leverage the account for malicious purposes. In banking, fake accounts may be used to apply for a loan or access credits. In other fintech apps, fake accounts might be created to access rewards (e.g. promotional offers such as credit card points, free deposits, a free stock etc. offered for new registrations). New account fraud is often perpetrated at a large scale, but attackers have become increasingly sophisticated in how they carry out these attacks to bypass traditional detection. Attackers may use a combination of bots and real humans to carry out the attacks, making it harder to distinguish between fraudulent and legitimate user activity.

Account Takeover (ATO) Fraud

Account takeover (ATO) fraud occurs when fraudsters take over existing user accounts. The goal of these attacks is typically to transfer funds and assets out of the accounts to a third party account controlled by attackers. Account takeover can happen in many ways. Usually it begins with a compromise of user credentials. Fraudsters obtain credentials via a dark web data sale, brute force, or phishing campaigns that steal credentials via spoofed login pages. Account takeover can also happen when hackers exploit API vulnerabilities such as BOLA (broken object-level authorization).

Rewards Abuse

Reward abuse occurs when fraudsters seek to take advantage of free credits, discounts, points or other rewards. New account fraud and rewards abuse often work in tandem - when the reward is tied to new account creation, fraudsters create new accounts to obtain the reward. Rewards abuse can also happen when vulnerabilities allow for enumeration of coupon or discount codes.

Detecting Fraud and Abuse with API Security

Each type of fraud and abuse described above is perpetrated via APIs, specifically login and rewards APIs. Effective detection of these attacks requires complete API context: understanding the historical behavior in each API to identify anomalous activity, understanding the patterns of behavior seen in fraud and abuse attacks, and having intel on threat actors and IPs to monitor suspicious actors. By combining these signals, it's possible to distinguish between legitimate activity and fraudulent and abusive activity, and detect and block fraud and abuse in APIs.

Protecting Sensitive Data

Financial services companies handle large volumes of sensitive data on behalf of their customers and business partners. This data includes PII such as full names, addresses, social security numbers, credit scores, and bank account information, as well as payment and credit card data protected under PCI-DSS. It also includes account authentication information such as usernames, passwords, and phone numbers. As a security leader, this sensitive data is your most critical asset. As your application surface grows, understanding where sensitive data resides and having controls in place to monitor data flows and prevent data exfiltration is critical.

API sprawl can also lead to sensitive data sprawl without proper governance in place. APIs are the pipelines through which data flows into, within, and out of your application. Having visibility into sensitive data flows at the API level should be a key piece of your data governance program.

Data loss prevention (DLP) is a common solution for the detection and prevention of data exfiltration at the perimeter. DLP is typically done by monitoring network traffic and identifying sensitive data as it crosses the network gateway or edge. However, this is not an API native solution, and it was simply never designed to have visibility at the API layer, where sensitive data is in transit. Instead of detecting transmission over the network, a head-on approach must be used, protecting the data at its source, APIs.

Evolving Compliance Landscape

Banks, payment providers, fintech companies, and other financial services organizations are subject to compliance requirements including data protection regulations like GDPR and CCPA/CPRA, and industry-specific regulations including FFIEC and PCI-DSS 4.0.

API security can help organizations achieve and maintain compliance through several core capabilities:

- **Automatic discovery and cataloging of API endpoints:** This gives organizations a complete inventory of their APIs which is a requirement for FFIEC compliance, and provides the foundation for other key compliance requirements, such as risk assessment for APIs and vulnerability management for APIs.
- **API Risk Scoring:** The FFIEC cybersecurity assessment asks organizations to assess the risk of assets including APIs. API security tooling can provide up-to-date risk scoring for API endpoints based on their security posture, access, and sensitive data exposure.
- **Sensitive data tracking:** Local data protection laws like GDPR and CCPA/CPRA as well as regulations around specific data types like PCI-DSS require strong data governance programs for sensitive data. Part of good data governance is understanding where your sensitive data is stored and where it is flowing in your applications. API security can help with that by classifying sensitive data and monitoring where it is flowing both internally within your applications and externally to any 3rd party APIs. API security tools should also allow you to block exfiltration of data.

Context-Aware API Security with Traceable

Platform Overview

Traceable helps financial services organizations achieve API protection in a cloud-first, API-driven world. Traceable is the only intelligent and context-aware solution that powers complete API security – API discovery and posture management, API security testing, attack detection and threat hunting, and attack protection anywhere your APIs live. Traceable enables financial services organizations to minimize risk and maximize the value that APIs bring their customers.

The core of Traceable's API security platform is our API security data lake. Traceable collects and stores rich data about every API transaction in a queryable data lake to power detection, threat hunting, and investigation. This deep, historical API context combined with AI and ML-driven analysis capabilities enables Traceable to detect advanced attacks including low and slow attacks and API fraud and abuse campaigns that unfold over time.

API Discovery and Posture Management

Traceable's API catalog automatically and continuously discovers and builds an inventory of every API in your organization, including internal, private, public or externally exposed, rogue, shadow, partner, and 3rd party APIs. Traceable discovers and tracks changes to APIs via on-premise, cloud, in-code components, integrations with API management, network traffic endpoints, and even workloads via eBPF. This comprehensive and always up-to-date API catalog enables your organization to meet FFIEC requirements around maintaining an API inventory.

Traceable also provides a detailed API security posture analysis of the inherent risk of each API, allowing you to understand which APIs (or the sensitive data in the flow) are most vulnerable to attack or abuse. Traceable analyzes each API with respect to the likelihood of exploitation and its potential impact using API context that includes context such as if an API is external facing, vulnerability specifics, ease of discovery, sensitivity of data being passed, and more. Traceable can prevent sensitive data exposure by identifying API endpoints that handle sensitive data without appropriate authentication or encryption implemented, empowering you to reduce risk.

Traceable's API discovery and security posture management capabilities allow your security team to prioritize those APIs that have inadequate security controls protecting your organization from threats or abuse. The end result is a comprehensive view of your API attack surface designed to help your security and development teams quickly discover, prioritize, and fix API risks, and maintain compliance.

API Testing

Traceable empowers your security team to test and eliminate the risk of pushing vulnerable APIs into production environments by proactively assessing and testing your APIs using real context from active API traffic. Requiring zero configuration and no dependency on OpenAPI spec files or Postman collections, Traceable uses its extensive API security and operational context collected by the platform to discover vulnerabilities in APIs during the QA and security testing processes. Traceable API security testing comes with hundreds of out of the box plugins to test for countless vulnerabilities and can easily be extended by the customer. With Traceable, security and development teams have the ability to perform contextually informed API assessments and proactively discover API security vulnerabilities before attackers do.

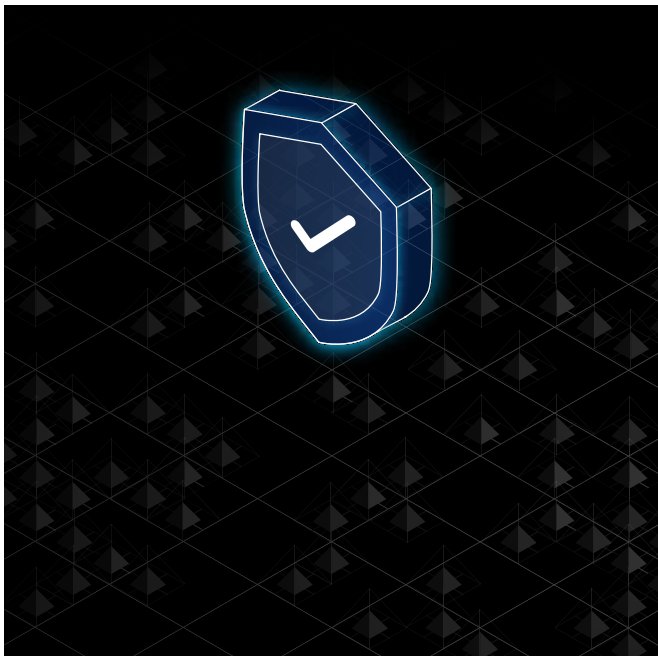
Attack Detection and Threat Hunting

With Traceable, you can identify, assess, and mitigate API security threats to your organization, reveal unknown attacks, and visualize user behavior analytics to uncover fraud and abuse. Traceable's attack detection capability provides a comprehensive set of security and API flow analytics that allows your SOC team, incident responders, and threat hunters, as well as red teams and blue teams, to find issues, detect threats, and mitigate attacks as they occur.

Traceable's attack detection and threat hunting capabilities provide a deep understanding of your environment via our API security data lake, where we analyze user-attributed transactions, request and response sequences, API data flows, code flows, and much more, allowing your security team to detect attacks and abnormal behaviors as they occur. This capability allows SOC teams and threat hunters to illuminate API targeted data breach, ransomware, abuse, fraud, or data exfiltration. Additionally, with the Traceable platform, security teams can not only discover attacks and threats, but also perform post-mortem reviews, and conduct forensics analysis for API security incidents.

API Attack, Fraud, and Abuse Protection

Using Traceable's contextual analysis of your APIs and the complete understanding of the inter-connectivity between the API activity, user activity, data flow, and code execution, Traceable automatically detects and blocks known and unknown API attacks, business logic abuse attacks, API fraud and abuse, as well as sensitive data exfiltration in your production environments. (ex: OWASP API top 10, fraud, credential stuffing, bot mitigation and more).



Traceable's deep data collection and analysis capabilities of API activity allow for additional protection against API fraud and abuse, and the ability to mitigate bot-based attacks. We don't only look at each individual API request or account in isolation. The Traceable platform correlates all collected API data based on many dimensions, including endpoint specifics, request parameters, network and API communication patterns, code and data flow, etc. This analysis provides you with a holistic view of how an actual attack may be distributed and organized and has progressed over time.

Appendix

TRACEABLE

CASE STUDY

Axos Bank's Journey to Comprehensive API Security with Traceable

Digital Bank Gains API Visibility, Streamlined Testing, And Protection Against Fraud And Abuse.

Executive Summary

As a pioneer in digital banking, Axos has been challenging the status quo of traditional financial services for more than two decades. Axos relies on APIs to provide innovative banking products and services to customers nationwide. With a focus on providing a superior online banking experience, Axos needed to ensure comprehensive API security that could keep pace with rapid innovation. Having relied upon external partners and manual pentesting to provide periodic assessments of their APIs, Axos determined it needed a solution that could provide continuous visibility and risk posture of all APIs, advanced automated testing to discover vulnerabilities pre-release, and rich analytics to incident detection and response.

Axos selected Traceable because it delivered the most comprehensive capabilities across API discovery, testing, and threat detection and response. With Traceable, Axos was able to discover and catalog every API across their enterprise, increasing visibility to 100%. Traceable's automated testing capabilities enabled Axos' security and engineering teams to discover 4x more vulnerabilities and streamline testing processes to deliver software faster and more securely. Finally, Traceable's API security data lake was an unmatched capability that other vendors couldn't provide, offering Axos's security team superior threat detection, investigation, and response.

Raghu Valipireddy

Chief Information Security Officer, Axos Bank

As CISO of Axos Bank, Raghu Valipireddy is responsible for overseeing and managing the information security strategies and policies of the organization, ensuring risk management, incident response, and compliance are all achieved while protecting customer's data and assets.

Case Study Highlights

Company

Axos, a digital bank, pioneered online banking two decades ago. Under CEO Gregory Garrabrants since 2007, the company transformed, shifting from white-label reliance to inhouse developed technology. Axos emphasizes constant innovation and expansion of banking products. Axos is committed to their API-driven approach, viewing it as central to their growth and technological innovation journey.

Challenge

- Limited API visibility leading to security blind spots
- Lack of API risk scoring and inability to prioritize testing and remediation for most vulnerable APIs
- Lack of historical API data and context to accurately detect fraudulent activity and ATO
- Lack of an API data lake to power incident investigation and response
- Previous API Protection Platform lacked API security data lake

API Security with Traceable

- API Visibility: Increased to 100%
- Risk scores available for 100% of APIs
- Vulnerability Discovery: 4x improvement compared to previous tools
- Detected attempted ATO
- Reduces time to test and fix vulnerabilities in APIs, resulting in faster releases

THE CHALLENGE

Life at Axos Bank Before Traceable

Incomplete Visibility and Context with WAF

As an API-centric company, Axos Bank's security team, led by CISO Raghu Valipireddy, was challenged to manage API sprawl and to comprehensively monitor all changes, updates, and data flows throughout their API ecosystem.
As a bank facing specific regulatory and operational requirements to secure their APIs, and obligations to their customers to protect their assets, the security team at Axos understood that comprehensive API visibility, protection, and analytics would be critical.

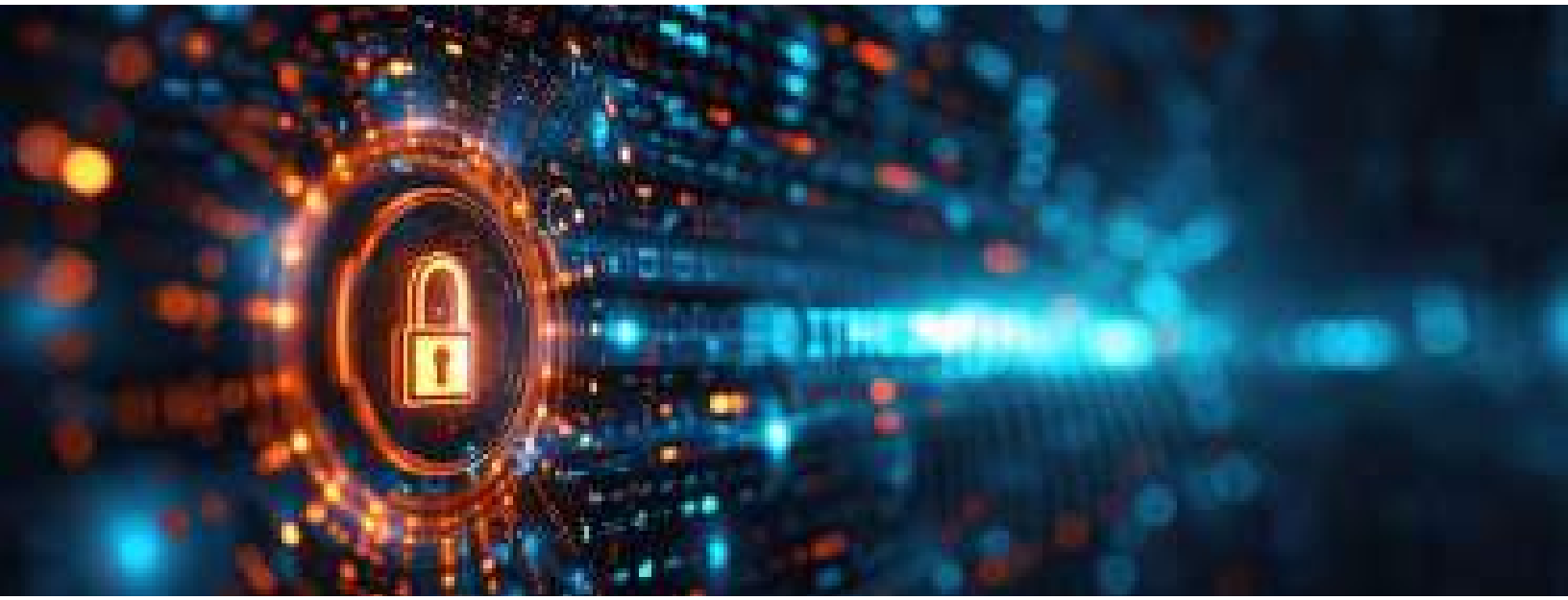
The WAF and gateway were the first step on Axos' journey to track and secure all API activity. The data that flowed through their API gateway and WAF provided a starting point for the team to speculate on potential risks and test for them, but could not provide the comprehensive API security capabilities they needed to detect and block more sophisticated attacks, such as digital fraud and abuse. These attacks often use legitimate credentials to access and manipulate data, making them difficult to detect without long-term contextual awareness.

> **"Initially we used an API Gateway and WAF, but this was only the first step to securing our APIs. We knew we needed to adopt a holistic API security platform.**

Inefficient API Penetration Testing

With limited security resources, Axos relied on external partners and penetration testing vendors to identify vulnerabilities within APIs. These efforts were largely manual. Without an API discovery and protection platform, the Axos Bank security team and their testing vendors lacked the prioritization necessary to ensure test coverage of all risky endpoints. Because Axos Bank is API-centric, with high traffic and frequent changes to their APIs, point in time penetration tests were no longer sufficient. They needed a way to continuously assess their API security posture and risk.

> **We needed a solution that would monitor all API activity around the clock, not just once a year. We needed something that would tell us what's good vs. bad on a frequent basis, to eliminate speculation and improve the efficacy of pentesting.**



Relying on third party penetration testing vendors also meant delays when shipping code to production. To speed up their software delivery process, the team needed a standardized, repeatable way to test APIs and identify vulnerabilities in house.

> **We had no way to do the required testing internally, it made it difficult to complete releases with consistent, standardized timing. We were waiting for external vendor testing, which is time-consuming and not comprehensive.**

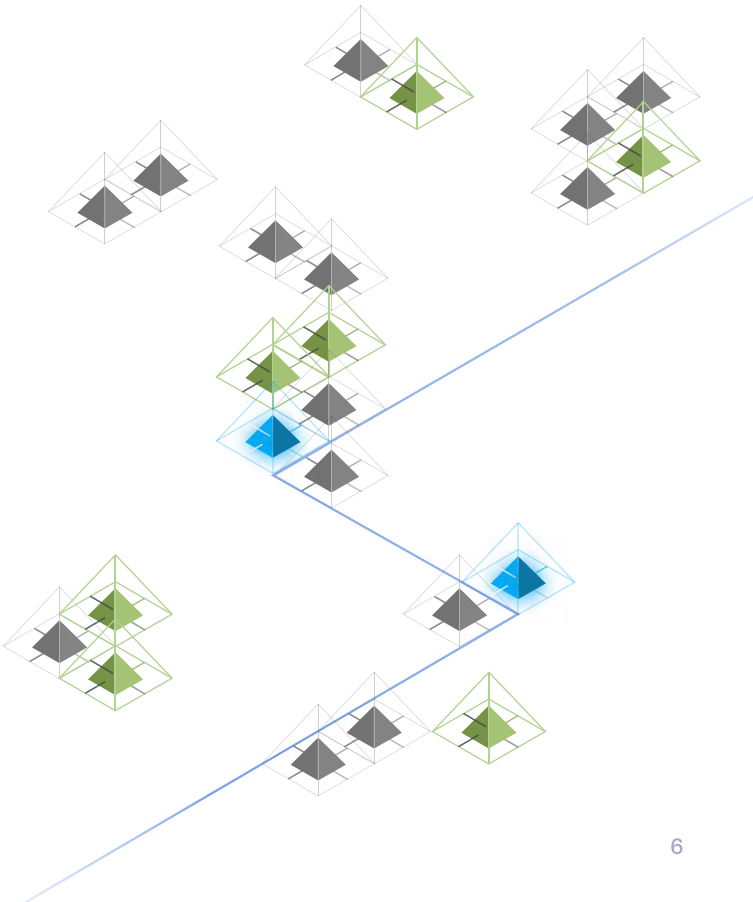
Ineffective Threat Detection with other API Security tools

The Axos team recognized the need for more consistent monitoring of their APIs, leading them to explore solutions that would monitor their APIs and accurately detect fraud and abuse attacks. Axos initially opted for a vendor solution that offered continuous automated API security testing, but they were only able to gain visibility into 25% of their APIs before running into challenges with the manual onboarding process. Some of the APIs lacked complete documentation that was needed to test outdated and infrequently used APIs. Further, this solution lacked an API discovery capability, making it impossible to identify blind spots.

Looking for another solution, they evaluated solutions from established API security vendors and selected a platform that was considered a leader. Upon implementing the platform, Axos achieved their first goal: a view traffic from all APIs, but its limitations became evident quickly. Protection against API attacks including digital fraud and abuse was a critical requirement for Axos. Attackers are continuously adapting and often changing their tactics, which makes detecting fraud and abuse at the API layer challenging. To gain the context required to detect these attacks, you need to collect comprehensive data about API activity over a long period. This platform lacked an API security data lake to store and analyze such data, making it impossible for Axos to get the long-term contextual awareness they needed to accurately distinguish between legitimate and fraudulent activity. The team realized they needed a data lake to power more advanced analytics so they could detect such malicious behavior.

> **“ We achieved API visibility, but it wasn’t enough. The absence of data lake capabilities meant that, while we could detect attacks, we still lacked the ability to examine similar past incidents. A data lake is crucial in order to perform analytics and enhance incident response capabilities when we detect fraud or abuse. We needed to do more.**

The team decided to reevaluate their options again. This time, the requirement for an API security data lake and advanced analytics for more accurate threat detection led them to Traceable.



THE TRANSFORMATION

Comprehensive API Security with Traceable

Valipireddy's team decided to move forward with a two-week Proof of Concept (POC) of Traceable. In that time, Axos Bank successfully implemented Traceable in production, achieving 90% API visibility. Finding that Traceable met their requirements: API discovery, protection, and analytics in the form of the API security data lake, Axos moved ahead with Traceable.

> **We realized that everything we were asking for was in Traceable. In those two weeks, we were not only able to stand up the product, but also showcase that all the requirements we had can be fulfilled using Traceable, specifically the critical data lake component.**

In the instances where the team at Axos requests changes or features from Traceable, they are live quickly.

> **Other products weren't as flexible. In terms of Traceable, we're seeing our feature requests and fixes delivered, which tells us that this is the partner we want to continue to work with.**

Traceable has revolutionized Axos Bank's API security approach, providing comprehensive API visibility, streamlined API testing, and higher confidence in API threat detection. With complete discovery and risk scoring for APIs, Axos has been able to focus penetration testing efforts and gain continuous insights into API security posture. Traceable's testing tools have streamlined collaboration between developers and security teams, resulting in faster and more secure releases. Finally, Traceable's rich analytics and API security data lake have powered detection, investigation, and response, improving Axos' ability to detect sophisticated attacks like fraud and account takeover (ATO) attempts.

API Security Data Lake Powers Investigation and Response

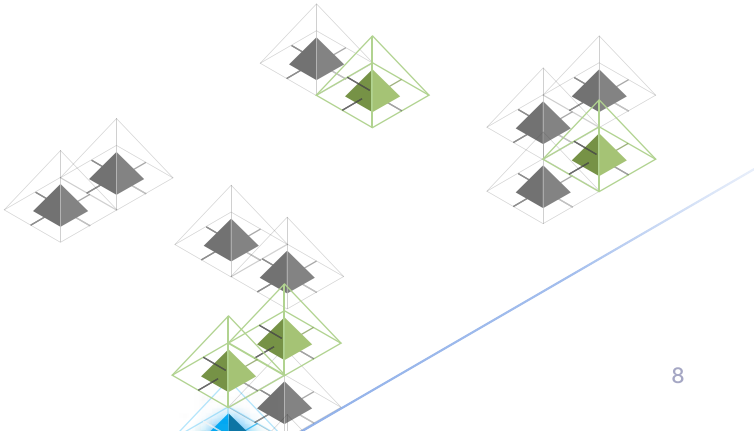
Axos Bank makes heavy use of Traceable's API security data lake to investigate suspicious activity flagged by Traceable's real-time threat detection. When a new threat is detected, the security team can explore past interactions from the same actor, enabling them to accurately identify threats and filter out the noise of false positives. The team is now confident they are taking action where needed.

> **With Traceable's data lake, we can go back in time and look at the historical telemetry of the API traffic. This allows our incident responders to generate all sorts of analytics that help them to gain critical context of the security incident and enables them to respond to incidents more precisely, without making any assumptions. This is exactly why the data lake is so important to our API security approach: we were somewhat blind in the past without the historical data. We are more confident now in our investigations.**

Continuous Risk Assessment

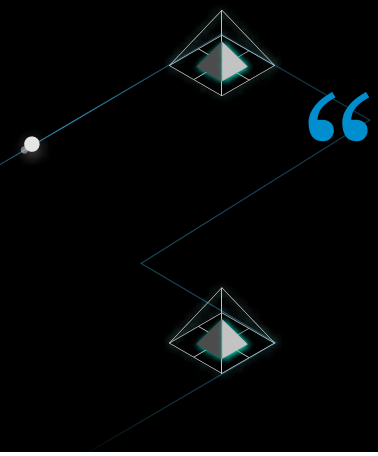
With Traceable, Axos went from having limited understanding of their API risk to having risk scores for 100% of their APIs, giving them a better sense of their overall API security posture. With this risk scoring and classification of endpoints, the team has dialed-in their penetration testing efforts, ensuring testers focus on what needs the most attention.

> **We modify our APIs daily, pentesting is not something that is agile enough to match this frequency. We use Traceable's risk grading to prioritize our pentesting efforts. We're able to tell pentesters exactly which APIs are considered risky, and we're not guessing.**



Streamlined API Testing Discovers Vulnerabilities Early

Historically, interaction between Axos Bank's security and engineering teams was primarily centered around annual or biannual code testing by penetration testers. However, increased focus on API security has required more consistent collaboration. Traceable has empowered the team to identify more opportunities to improve the security of APIs before they are live, sometimes uncovering weaknesses missed by professional penetration testers. This has resulted in a streamlined testing process and improved collaboration between security and development teams. Developers now proactively engage with the security team for testing and feedback, using Traceable to validate fixes before production releases.



> **Detecting vulnerabilities earlier with Traceable has streamlined our processes and increased the speed of addressing issues. This proactive approach, compared to waiting for traditional pen testing, has significantly accelerated our testing timeline. Consequently, our releases are not only more consistent but also follow a standardized and repeatable process.**

Fraud Detection

With Traceable, Axos can proactively identify and prevent fraudulent account creation, protecting not only their organization but their customers. Traceable analyzes Axos' API traffic patterns and applies sequence-based application fingerprinting using LLM models to identify indicators of fraud activity. Based on the traffic observed with this method, Traceable has pinpointed potential fraud for Axos.

> **Because we're so API heavy, we can see those fraud patterns in the APIs themselves, or in API traffic. Traceable's team is helping us identify potential fraud instances and threats by using the data aggregated in the data lake, applying LLM models that then provide us with a targeted list of potential fraudsters that are attempting to interact with us.**

ATO Prevention

Traceable's account takeover (ATO) detection capabilities solve a prevalent concern in the banking industry. While Axos Bank employs various solutions to safeguard against account takeovers, Traceable introduces a unique perspective, and has already enabled the team to more quickly identify attempted phishing-led ATO. Using Traceable, Axos successfully detected and thwarted incidents related to OTP violations, while thwarting additional ATO attempts through analytics. The detection capabilities provided by Traceable surpassed the bank's earlier experiences with other API security vendors, allowing Axos to remain at the cutting edge of API security, protecting their customers.

> **Traceable is putting a new spin on ATO protection for Axos and our customers, it's definitely well above and beyond what we have seen from other API security vendors, and is incredibly powerful.**

About Traceable

Traceable is the industry's leading API Security company that helps organizations achieve API protection in a cloud-first, API-driven world. With an API Data Lake at the core of the platform, Traceable is the only intelligent and context-aware solution that powers complete API security – security posture management, threat protection and threat management across the entire Software Development Lifecycle – enabling organizations to minimize risk and maximize the value that APIs bring to their customers.

To learn more about how API security can help your business, book a demo with a security expert.

www.traceable.ai

TRACEABLE_