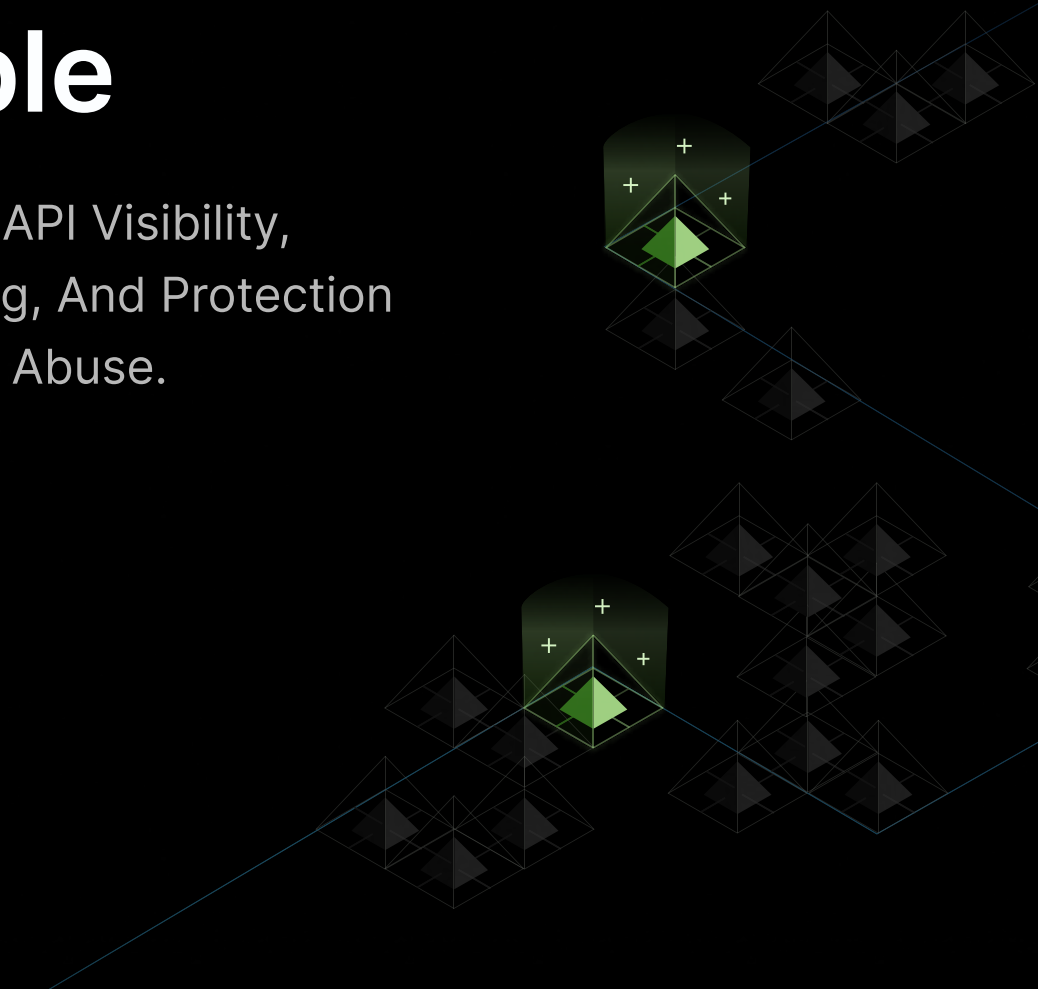
TRACEABLE

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.**

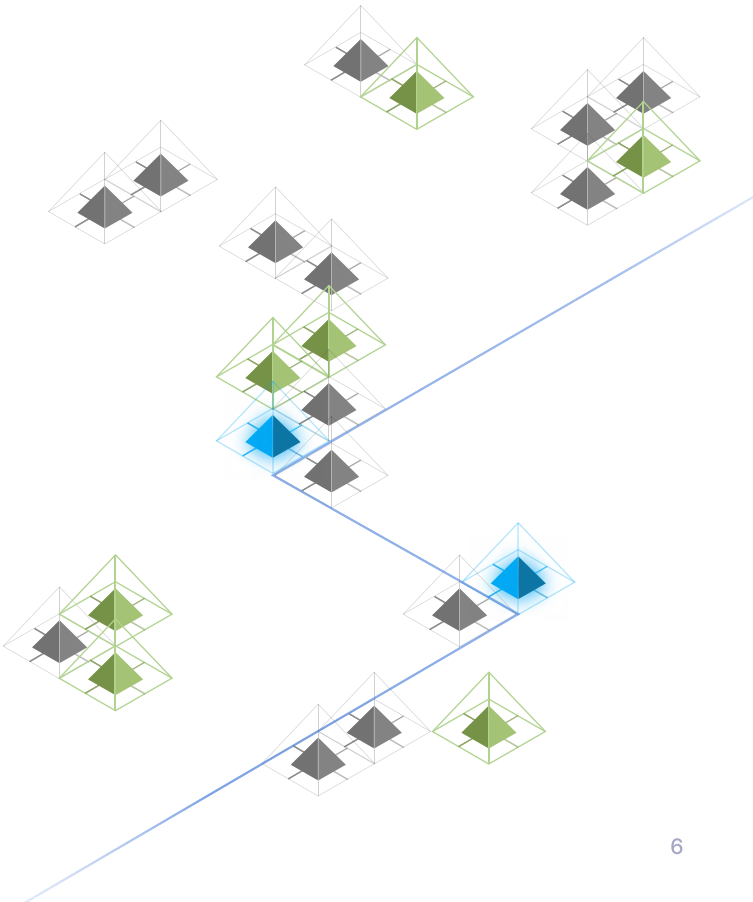
Ineffective Threat Detection with other API Security tools

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

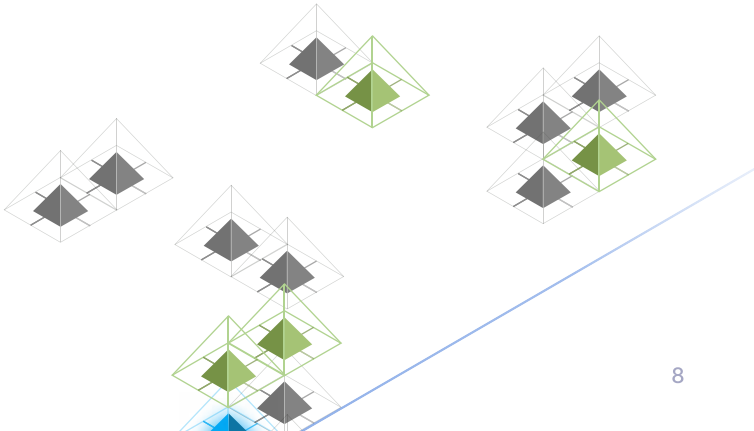
Axos Bank makes heavy use of Traceable's API security data lake to investigate suspicious activity flagged by Traceable's real-time threat detection. When a new threat is detected, the security team can explore past interactions from the same actor, enabling them to accurately identify threats and filter 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

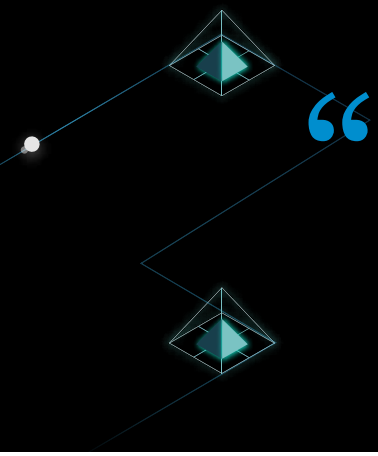
With Traceable, Axos went from having limited understanding of their API risk to having risk scores for 100% of their APIs, giving them a better sense of their overall API security posture. With this risk scoring and classification of endpoints, the team has dialed-in their penetration testing efforts,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