THREATX

DATA SHEET

Financial Services: Effectively Protect Open Banking and Financial APIs

Take a Protection-First Approach to Securing the APIs That Manage Your Customers' Financial Data

Many financial services institutions struggle to keep up with their expanding use of APIs and API-driven microservices. As the number of APIs expands, so does an organization's attack surface and risk exposure. This dependence on various APIs also complicates the organization's ability to secure dynamic environments and ensure they meet industry regulations. All in all, this creates the perfect storm for security professionals within financial services, many whom are already struggling to keep their customers' sensitive data protected.

Open Banking

Financial services, such as banking and insurance organizations, are increasingly adopting API-driven services into their applications. For example, Open Banking is one of the most popular API-powered systems used to share and exchange data between financial institutions. Open Banking's reliance on APIs makes it a top target for attackers due to the type of data being managed — payment information, banking account numbers, SSNs, physical addresses, and other user-identifiable data.

Keeping up With Regulations

As if protecting and managing an organization's growing API attack surface comprised of vulnerable APIs in micro-services or third-party libraries wasn't daunting enough alone, security professionals in financial services must also keep track of industry-specific data regulations, and ensure their organization is adhering to them. Regulations that might be required include; PCI DSS, PSDS Europe, NY DFS, GDPR, ISO/IEC 27001, and SOC.

ThreatX can help meet requirements such as:

PCI DDS 6.2: Develop custom software securely, including use of external APIs

PCI DSS 6.4: Protect public-facing web applications against attacks

PCI DSS 6.4.1: Deploy an automated solution for public-facing web applications that continually detects and prevents web-based attacks

PCI DSS 5.0: Protect all systems and networks from malicious software

PCI DSS 10.0: Log and monitor all access systems managing sensitive data

Each API Is a Target

The increased adoption of APIs in the financial industry and the responsibility to comply with cybersecurity requirements presents security professionals with a challenge to meet all the demands needed to secure their organization's web applications and APIs. Using third-party and open-source API services introduces complex vulnerabilities that attackers can use to access customers' account information, payment information, and personal identifiable data. Each API is a potential target, and attackers are dedicated to finding and exploiting data from any endpoint, using any tactic, to uncover any vulnerability they can.

Common Pain Points for Financial Services

Often, ThreatX's financial services customers struggle with managing credential stuffing attacks on their login pages, exploitation attempts on vulnerable third-party APIs, and API abuse. Protecting APIs is hard – and important. That's why it's crucial to know what requirements are at the top of your list when evaluating an API protection solution. ThreatX brings an API-native approach to AppSec that addresses the unique risks, challenges, and threats that financial institutions face every day.

These Include:

- Real-time detection and blocking of attacks
- API discovery and traffic observability
- Managed services and security operations

When we asked a Senior Manager of Platform Support in banking about why API security is important to them, they said:

"APIs are outdated, many are open source-based, and they introduce phenomenal risk and unreliability. That's why we employ a multi-layered protection scheme that utilizes in-house staff for scanning our own environment while a variety of managed service providers that specialized in threat detection and remediation cover that key area of concern."

Managing and maturing API security strategies has become the next essential step for many organizations but, most importantly, financial institutions.

see next page to learn how ThreatX can help »

Key Capabilities for Financial Services

Detect and Block Attacks in Real-Time

THREATX

ThreatX analyzes all inbound API traffic in real time, identifying and blocking attacks. This real-time monitoring enables ThreatX to execute advanced threat engagement techniques, such as IP fingerprinting, interrogation, and tar-pitting. These capabilities allow ThreatX to identify and stop the most complex attacks, including large-scale bots and DDoS-level threats.

Detect and Block Attacks in Real-Time

ThreatX analyzes all inbound API traffic in real time, identifying and blocking attacks. This real-time monitoring enables ThreatX to execute advanced threat engagement techniques, such as IP fingerprinting, interrogation, and tar-pitting. These capabilities allow ThreatX to identify and stop the most complex attacks, including large-scale bots and DDoS-level threats.

Enable Advanced Attack Forensics

Through advanced risk analysis, ThreatX can identify key attributes of an attack, such as attack patterns over time (e.g., low and slow); use of advanced evasion techniques; and details of the attack target. This insight enables security to understand the goals and nature of a threat to drive a more comprehensive security strategy.

Discover and Defend APIs

Because ThreatX examines all live traffic, the platform can identify APIs you may be unaware of, such as zombie and rogue APIs. For security professionals without a clear handle on their organization's API attack surface, these capabilities fill a critical gap in the security program.

Visualize API Attack Surface

In addition, the API discovery capabilities of ThreatX allow customers to visualize the entirety of the API attack surface. ThreatX's API dashboard provides a central view into legitimate, suspicious, and malicious requests hitting organizations APIs by analyzing and profiling actual traffic. ThreatX discovers and profiles API endpoints, providing users with enhanced visibility into legitimate, rogue and zombie APIs in production.

Partner With AppSec Experts

ThreatX provides Managed Services and Security Operations to ensure our customers get the highest protection possible by streamlining deployment with onboarding support, followed by immediate protection with dedicated resources focused on threat hunting, zero-day protection, and 1:1 AppSec expertise.

ThreatX protects your Open Banking and financial APIs and apps against API abuse, SQL injection, and botnet attacks while also providing zero-day coverage with our 24X7 SOC to act as an extension of your team.