CEQUENCE

Solution Brief

Protecting Financial Services APIs From Automated Attacks

Driven by the move towards modular applications and mobile device ubiquity, the financial services industry (banks, credit unions, credit card, and financial technology) were early API adopters as a means of engaging users with equal efficiency through a mobile app or a browser while fostering a vast third-party ecosystem. The reason for the early adoption is simple – APIs provide speed and flexibility for developers. Validating that APIs are the development tool of choice, the Cequence CQ Prime threat research team found that 14.4 billion or 70% of the 21.1 billion application requests analyzed during the second-half, 2021 were API-based. In the same time period, the research team found that 80% of mitigated traffic was API-based, a finding that confirms the notion that attackers love APIs as much as developers.

Financial Services Targeted by API-based Account Takeovers

Industry research by BCG Digital states that financial services organizations are 300 times as likely as other companies to be targeted by a cyberattack. Attackers view the assets held and programs provided by the financial services industry as highly coveted targets, using a variety of techniques to execute account takeovers (ATOs) against APIs that often result in theft or fraud:

Shadow and zombie APIs

Attackers use open source tools to find and attack APIs that are unknown to and unmanaged by organizations. These APIs, commonly referred to as shadow or zombie APIs, are often insecure and favored by attackers. Shadow APIs are a rapidly growing problem, as documented by Gartner who state that by 2025 less than 50% of enterprise APIs will be managed, as explosive growth in APIs surpasses the capabilities of API management tools. This industry statistic is further validated by CQ Prime, finding that roughly 30%, or 5 billion of the 16.7 billion attacks mitigated in the first-half 2022 targeted shadow APIs.

Exploit API coding errors

Alternatively, analysis may uncover and exploit API coding errors that expose too much data, provide access to sensitive data, rely on weak authentication, or allow unfettered access to user data.

Target perfectly coded APIs

Attackers analyze perfectly-coded APIs to understand how they work, then use commercially available attack tools combined with the billions of readily available stolen credentials to launch automated high-volume attacks.

ATOs impact many different business groups including security, fraud, compliance, IT infrastructure, PR, and marketing. With nearly 1 in 4 consumers falling victim to ATO in 2023 (Federal Trade Commission), the financial impact for the business ranges from $290 (Juniper Research) and nine hours of investigative work to $311 (FTC).

Traditional API Security for Financial Services Falls Short

Organizations using first-generation bot detection products to address automated attacks against their applications and APIs are met with limited success due in part to these solutions' client-based (JavaScript and mobile SDK) approach. The client-less nature of APIs means that first-generation bot solutions have limited access to telemetry data and other information needed to determine if the intent of a transaction is malicious or not. Without this capability, policy enforcement and visibility are by definition inconsistent across the organization's multitude of application endpoints – web, mobile, and, most critically, supporting APIs.

Compounding the ineffectiveness of bot detection offerings is the fact that security teams lack the visibility and defensive capabilities needed to reduce the risks introduced by dramatically increasing API use. Many organizations believe that compliance with PCI or SOC 2 and a shift-left, DevOps approach is sufficient to protect APIs. The problem with these approaches is that they don't require comprehensive API discovery, and only know about APIs the organization is already aware of. Shadow and zombie APIs and their vulnerabilities go undiscovered and unaddressed.

Even if all APIs are discovered and known, attackers can still masquerade as customers performing legitimate transactions to steal data or commit fraud. Traditional approaches that use WAFs or API gateways depend on easily evadable detection, lack the real-time ability to discern good from bad API activity and are reliant on static, least common denominator protection spread across multiple technology components.

Solution: Cequence Unified API Protection

The Cequence Unified API Protection solution takes a comprehensive approach to securing financial services APIs by addressing each of the key API security lifecycle phases. Using a full-spectrum approach ensures that all your APIs are discovered, analyzed for hidden risks, and protected from automated threats and vulnerability exploits.

Outside-in discovery

Viewing an organization's API attack surface from a threat actor perspective to reveal the unknown.

Inside-out inventory

Performing a comprehensive API inventory, including all existing APIs and connections.

Compliance monitoring

Keeping APIs in compliance with specifications such as the OpenAPI framework, standards including the OWASP API Security Top 10, and regulations like PCI DSS ensures high API code quality, consistency, and governance.

Ongoing API testing

Integrating API protection into development, which shifts API security left within the organization, so risky code doesn't go live.

Threat detection

Continuously scanning for threats and malicious activity, including subtle business logic abuses that has not yet been observed.

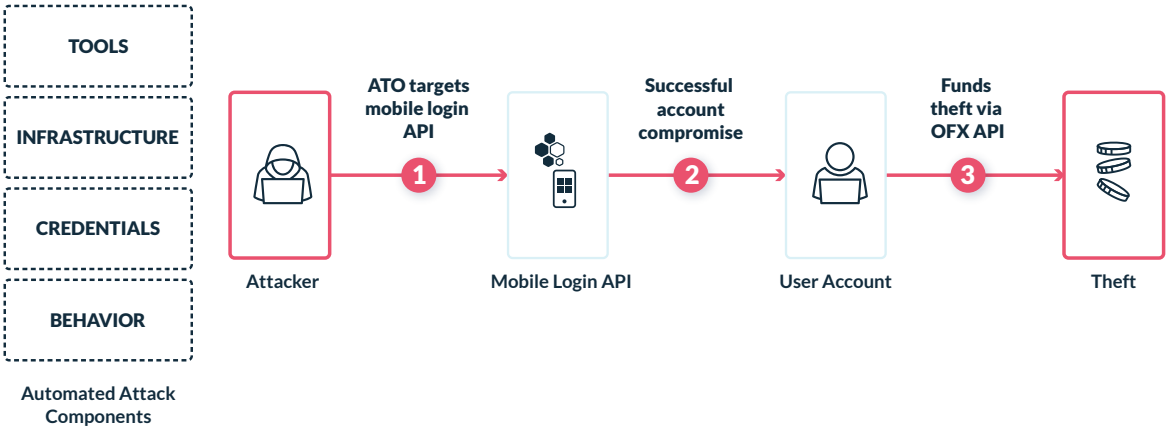
Threat prevention

Employing real-time countermeasures such as alerts, blocking, and even deception, without needing additional third-party tools.

Unified API Protection is different from fragmented or incomplete API protection offerings because it's a methodology designed to account for multiple types of risk, across every phase of the API protection lifecycle.

Customer Spotlight: Fortune 100 Financial Services Company

At a Fortune 100 financial services organization attackers analyzed the firm's mobile application to fully understand how the login API worked. They then used known tools, malicious infrastructure, and readily available (stolen) credentials to launch a sophisticated ATO campaign. When they met resistance, the attackers quickly shifted behaviors to continue their onslaught. If a malicious login attempt was successful, they would proceed to transfer funds to their own (fake) account using the OFX API, the financial services industry standard fund transfer protocol. Faced with mounting fraud, customer dissatisfaction, and an API-first development methodology, the customer turned to the Cequence Unified API Protection (UAP) solution to stop the attacks.



UAP detects ATO attempts using an advanced ML-based analytics engine that automatically discovers API, web, and mobile application endpoints to build an intuitive site map for visibility and policy-based protection. Predefined policies based on the largest API threat database available dynamically determines the intent of each transaction request. When malicious activity is detected, the customer could natively enable mitigation policies using multiple response options such as blocking, rate limiting, or deception. The agentless, ML-based approach of the UAP helped them achieve the following results:

- Significantly reduce their organization's API attack surface
- Prevent patterns of misuse that led to fraud and user dissatisfaction
- Automatically protect newly-deployed web applications and APIs
- Unify protection for public-facing web, mobile, and API-based applications

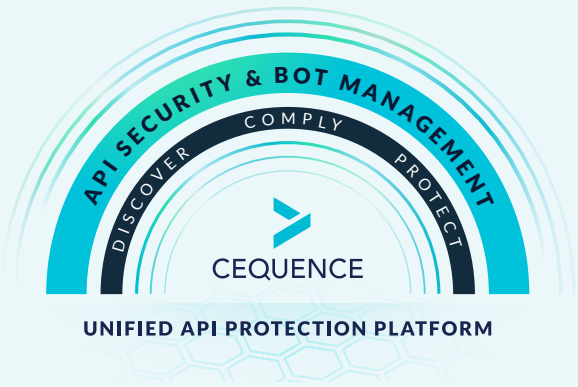
Today, the customer is using Cequence UAP to protect more than 50 public-facing applications, preventing fraud and theft associated with ATOs.

Get an attacker's view into your organization with a **Free API Security Assessment**.

The Cequence Advantage

The Cequence Unified API Protection platform is the only solution that addresses the entire API lifecycle, discovering the complete attack surface, managing the API security posture, and detecting and mitigating attacks.

Cequence enables customers to reap the competitive and business advantages of secure, ubiquitous API connectivity. The Cequence solution induces attack futility, failure, and fatigue for even the most relentless of attackers, improving visibility and protection while reducing cost, minimizing fraud, data loss, non-compliance, and business disruption. Learn more at **cequence.ai**.



CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai