

Cequence Unified Application Protection for FinServ

Protecting Global Financial Services Organizations Against API Attacks

Financial services organizations have long been on the cutting edge of technology and today leverage microservices and cloud architectures that lean heavily on APIs to reduce costs and transaction friction while providing compelling new services. Unfortunately, this rise in API use corresponds with an increase in API-origin data breaches, compromising tens of millions of sensitive customer records. The increased adoption of APIs requires a strengthening of security to protect open banking.

Regulators and standards bodies have taken note, drafting new and updating existing regulations and standards to ensure that APIs are secure and sensitive data is protected. The U.S. Consumer Financial Protection Bureau (CFPB) has proposed rules to accelerate the shift toward open banking, deprecating screen scraping in favor of APIs. The FFIEC has provided guidance on how covered entities should protect APIs. NIST SP 800-24, PCI DSS version 4.0, the U.S. Treasury Department, and other rule-making bodies leaning into Open Banking/Open Finance have also been floating requirements to securely develop, deploy, and use APIs. The European Payment Services Directive (PSD2) mandates banks share customer financial data with authorized third-party providers (TPPs) through secure APIs, and the Digital Operational Resilience Act (DORA) safeguards against operational and cybersecurity disruption. To ensure uninterrupted business success, security teams must prevent the misuse and abuse of these business-critical services that rely on APIs.

API Security and Bot Management Challenges

Today's organizations face unique, cross-functional challenges when it comes to protecting critical APIs and applications from cyberattacks. It's not just an IT or security problem; malicious bot attacks on applications and APIs can affect ecommerce, customer satisfaction, compliance, marketing and sales analytics, and more. Effective API security and bot management programs are necessary to protect the business and its customers.



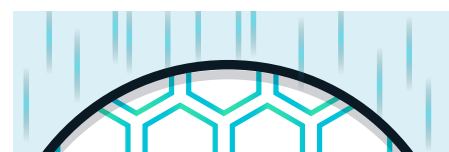
Lift the Fog

APIs are routinely developed and deployed by disparate teams at lightning speed across a mix of on-premises and cloud infrastructure, creating a "fog of war" that shrouds visibility. Teams must know what APIs exist, where they are, who has access, and ensure they have accurate specifications.



Maintain Good Posture

Security and development teams do not have a clear and consistent picture of their API security posture across their application portfolio. Understanding where a critical vulnerability, sensitive data exposure, or business logic flaw can be exploited enables security teams to remediate pinpointed areas of security risk.



Protect the Core

Applications and APIs are constantly probed by attackers seeking any opportunity to exploit them and compromise your organization and its data. The ability to detect and block attacks as they occur can prevent organizations from experiencing fraud, data exfiltration, and business disruption.

Financial Services Use Cases



Prevent Identity Breaches



Continuously Discover APIs



Quantify API Risk



Prevent Account Takeover (ATO)



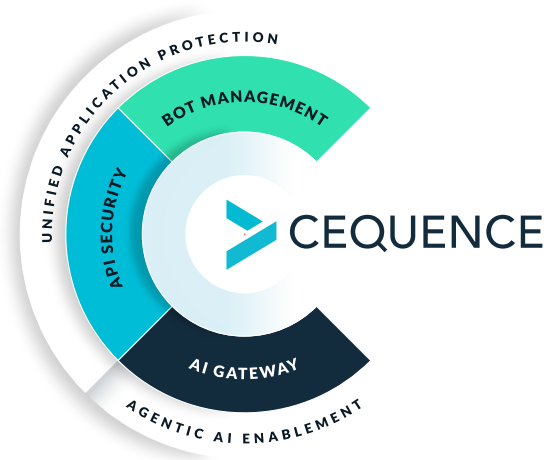
Avoid Aggregator Abuse



Prevent API Business Logic Abuse

The Cequence Unified Application Protection Platform

The Cequence Unified Application Protection (UAP) platform unites discovery, compliance, and protection to defend an organization's applications and APIs against attacks, business logic abuse, and fraud. Cequence UAP results in attack futility, failure, and fatigue for even the most relentless of attackers. It significantly improves visibility and protection while reducing cost, minimizing fraud, data loss, non-compliance, and business disruption. Cequence UAP delivers value in minutes rather than days or weeks and offers a flexible deployment model that requires no app instrumentation or modification.



DISCOVER

API Attack Surface Discovery

Discover internal and external APIs | Alert and monitor changes

Discover and inventory your organization's entire API footprint cataloging internal, external, and third-party APIs. Form a coherent picture of your publicly-accessible attack surface, giving you an attacker's view of your organization. Cequence continuously reveals new API hosts, endpoints, and hosting providers to keep security and compliance teams in the know.

COMPLY

API Security Posture Management

Monitor posture continuously | Test pre-production APIs | Remediate risks

Manage your organization's API security posture, ensuring its complete API footprint is compliant, conforming to specifications, security test requirements, and governance best practices. Autonomous API test creation identifies vulnerabilities and prevents sensitive data leakage prior to production.

PROTECT

Bot Management & Fraud Prevention

Block application & API attacks | Prevent theft, business logic abuse, fraud

Identify and mitigate bots and prevent fraud, protecting your organization and its applications from the full range of automated attacks. Requiring no agents, JavaScript, or SDKs, multi-dimensional behavioral fingerprints enable identification of even the most sophisticated attacks. Native, real-time blocking ensures protection against business logic attacks, exploits, malicious bots and AI agents, online fraud, OWASP API Security Top 10 attacks, and much more.

Works with Cequence AI Gateway

The Cequence AI Gateway enables agentic AI access to any internal, external, or SaaS application, in minutes, without coding. API Security can automatically create enhanced API specs that the AI Gateway uses to create MCP servers, eliminating significant manual effort.

Protecting Top Global Financial Services Brands

\$10T Business value protected

10B Daily API transactions secured

4B User accounts safeguarded



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

© 2025 Cequence Security, Inc. All rights reserved.

Cequence-UnifiedAPIProtectionFinserv-DS-20251027