

Cequence Solutions for Financial Services

Protecting Global Financial Services Organizations

Financial services organizations have long been at the forefront of technology adoption, building on microservices and cloud architectures that rely heavily on APIs to reduce costs and transaction friction while delivering new services. Those institutions now deploy AI agents to reconcile accounts, answer customers, and execute transactions, while customers and third parties use their own agents to interact with the organization. The rise in API use corresponds with an increase in API-origin data breaches compromising tens of millions of sensitive customer records, and every new agent adds another entity that needs visibility and control.

Regulators Expect Secure APIs and Governed AI Agents

Regulators and standards bodies continue to draft and update rules requiring secure APIs and protected sensitive data. The U.S. Consumer Financial Protection Bureau (CFPB) finalized an open banking rule under Section 1033 that favors secure APIs over screen scraping; the CFPB has since reopened the rule for reconsideration, but the shift toward API-based data sharing continues. The FFIEC has issued guidance on how covered entities should protect APIs, and NIST SP 800-204, PCI DSS version 4.0, and the U.S. Treasury Department all address how to securely develop, deploy, and use APIs. In Europe, the Payment Services Directive (PSD2) mandates that 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. AI oversight follows the same path: the EU AI Act classifies AI used for creditworthiness assessment as high-risk, and the New York Department of Financial Services (NYDFS) has issued guidance on AI cybersecurity risks. Security teams must prevent the misuse and abuse of business-critical APIs and govern the AI agents that use them.

Application, API, and Agent Security Challenges

Financial institutions face cross-functional challenges when it comes to protecting critical applications, APIs, and the AI agents that use them. The impact reaches well beyond IT and security: malicious bot attacks and ungoverned agent access affect digital banking, customer trust, fraud losses, regulatory standing, and more. Effective API security, bot management, and agentic AI governance programs protect the business and its customers.

Lift the Fog

APIs, MCP servers, and AI agents 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 and agents exist, where they are, who has access, and ensure they have accurate specifications and descriptions.

Maintain Good Posture

Security and development teams lack a clear and consistent picture of their security posture across the application portfolio and the agents connected to it. Knowing where a critical vulnerability, sensitive data exposure, business logic flaw, or over-permissioned agent creates risk lets security teams remediate pinpointed areas of risk.

Protect Applications and Data

Attackers constantly probe applications and APIs for any opportunity to exploit them and compromise the organization and its data, and an AI agent with valid credentials can still take actions outside its intended role. Detecting and stopping attacks and out-of-policy agent behavior in real time prevents 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 Platform

The Cequence Platform unites discovery, compliance, protection, and agentic AI governance to defend an organization's applications and APIs against attacks, business logic abuse, and fraud, and to give its AI agents secure, governed access to the systems they need. The Cequence Platform results in attack futility, failure, and fatigue for even the most relentless attackers while giving the institution a controlled path to agentic AI adoption. It significantly improves visibility and protection while reducing cost, minimizing fraud, data loss, non-compliance, and business disruption. The Cequence Platform delivers value in minutes rather than days or weeks and offers a flexible deployment model that requires no app instrumentation or modification.

API Attack Surface Discovery

Discover internal and external APIs | Identify AI agents in traffic | Alert and monitor changes

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

API Security Posture Management

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

Manage the 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. The same posture data shows which APIs are ready to expose to AI agents and which carry sensitive data that needs tighter controls first.

Bot Management, WAAP, and Fraud Prevention

Block application and API attacks | Prevent theft, business logic abuse, and fraud | Verify AI agents

Identify and mitigate bots and prevent fraud, protecting the 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. Behavioral analysis also separates legitimate AI agents, such as customer assistants and authorized aggregators, from malicious automation, so institutions can serve agentic traffic without opening a path for fraud.

Agentic AI Governance

Contain agent behavior | Enforce per-agent access | Audit every agent action

Agentic AI Governance focuses on keeping every AI agent within its intended role as it works against billing, account management, provisioning, SaaS applications, and more. The Cequence AI Gateway enforces agent containment in real time, preventing unauthorized actions and stopping agents from chaining individually authorized actions into unwanted outcomes. Agent Personas scope each agent to only the tools and data its role requires, and the MCP, API, and LLM registries limit agents to approved resources. Agent Behavior Protection stops activity that deviates from an agent's intended role, and the AI Gateway brokers authentication so agents never have direct access to backend credentials. Every agent action is logged for audit and regulatory review, and carriers can extend containment to new applications without writing code.

Application Protection and Agent Governance Reinforce Each Other

API Security provides posture management for enterprise APIs, reducing risk and hardening the APIs used by humans, bots, and AI agents alike. Bot Management evaluates the agents arriving from outside the institution, while the AI Gateway governs the agents the institution runs itself, so every human, bot, and agent interaction falls under one platform.

Protecting Top Global Financial Services Brands

10 Billion

Daily Application Interactions

4 Billion

User Accounts

1 in 15

Mobile Users Worldwide