CEQUENCE

Datasheet

Cequence Unified API Protection for FinServ

Protecting Global Financial Services Organizations Against API Attacks

Financial services organizations were among the first to embrace mainframe computing, and are now leveraging applications, APIs and microservices to further business goals, like reducing cost and transaction friction, and providing customers with 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 scaping 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

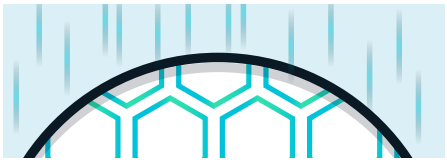
Today's security teams face unique, cross-functional challenges when it comes to protecting critical APIs and applications from cyber attacks.

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 security team visibility. Discoverable by attackers, unmanaged and unprotected APIs often contain critical vulnerabilities that lead to exploited applications and data breaches.

Maintain Good Posture

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



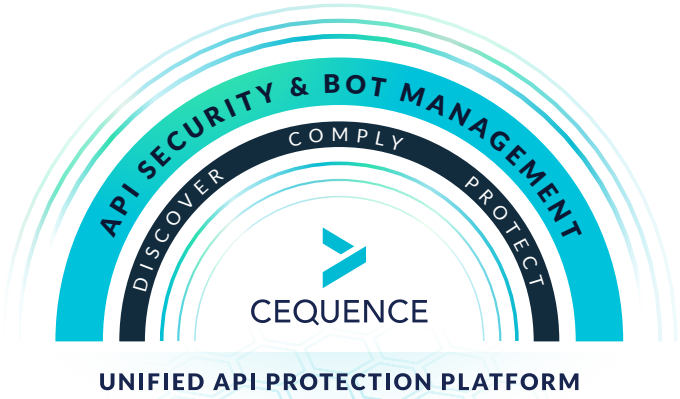
Protect the Core

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 API Protection Platform



To address these security challenges, the ideal solution must continuously engage in complete discovery of your entire API attack surface, including internal, external, and third-party APIs as well as edge, infrastructure, gateway, and hosting providers. Understanding your API risk posture, pinpointing which critical security vulnerabilities need remediation, while providing real-time protection that detects and blocks attacks *before* they reach your applications is crucial.

The Cequence solution is the only security offering that addresses all phases of your API protection lifecycle, discovers your entire API attack surface, eliminates unknown and unmitigated API security risks, and protects your applications and APIs from cyber attacks that lead to data loss, fraud, and business disruption.

The Cequence Unified API Protection platform enables customers to continuously reap the competitive and business advantages of secure applications and ubiquitous API connectivity. The Cequence solution 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. Learn more at **www.cequence.ai.**

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 servers, endpoints, and hosting providers so that security and compliance teams are aware of their existence.

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, automated bot activity, online fraud, OWASP API Security Top 10 attacks, and much more.

Protecting Top Global Financial Services Brands

$10T Business value protected

10B Daily API transactions secured

3B User accounts safeguarded

ADP · ALLIANT · AMERICAN EXPRESS · BANCO DO BRASIL · e-global · NAVY FEDERAL Credit Union · REGIONS · snap! finance

CEQUENCE

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