

Cequence Unified Application Protection for Public Sector

Securing federal agencies and public sector organizations against application and API attacks

As the U.S. Federal Government and broader public sector moves towards more modern architectures, they are prey to the same threats faced by the private sector, perhaps even more so due to the sensitivity and value of their data they handle.

In order to protect your organization, security teams must prevent application and API attacks that can lead to data loss, fraud, and business disruption. Security teams often lack the visibility, testing, and defense capabilities needed to protect their applications and APIs from today's sophisticated attacks. The Cequence Unified Application Protection (UAP) solution addresses every phase of your API security lifecycle, can be deployed quickly without intrusive agents, instrumentation or application modification, and scales easily.

CASE STUDY

Navy Federal Credit Union Blocks Scammers

As the nation's largest mortgage service provider, NFCU is constantly under attack from bots trying to access and transfer assets from customer accounts and apply for loans using stolen identities.

Key outcomes with Cequence Unified Application Protection solution:

- Successfully blocked 8M+ account takeover requests missed by their existing bot mitigation provider
- Identified and stopped fraud attempts carried out across multiple channels (APIs and web applications)
- Protected all NFCU user accounts from fraud, data loss, and account takeover

CASE STUDY

Global Telecom Lack of API Visibility

This global telecom organization had a bad case of API sprawl with a distributed development process and numerous corporate acquisitions contributing to the issue. Understanding that you cannot protect what you cannot see, they went through a manual API inventory and risk assessment effort. While the information collected was valuable, uncovering shadow APIs while providing details on a set of risk categories, it was a manual effort that took far too long. They needed it to be in real time and the process of collecting it needed to be scalable.

Key outcomes with Cequence Unified Application Protection solution:

- Estimated 5,000+ APIs, but discovered over 18,000 within hours
- Reduced attack surface by retiring old shadow APIs and moving internal APIs behind their network perimeter
- Built custom policies to track clients using APIs that respond with sensitive information to ensure unauthorized users were blocked

Mission-critical differentiators

Proven Scalability and Reliability

- Cequence protects more than 10 billion daily API interactions and 4 billion user accounts with 99.99% platform availability and near-zero latency
- No application or API changes required, stopping attacks within 15 minutes of onboarding

Flexible Deployment Models

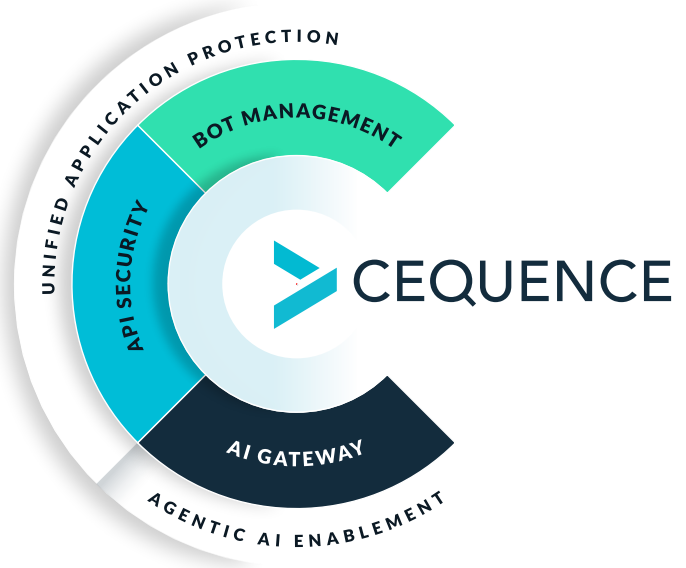
- Deploys and scales quickly and easily without intrusive instrumentation
- Containerized form factor allows for easy deployments across cloud and on-premises locations

Integrated API Security and Bot Management Platform

- Detect and prevent attacks across applications and APIs
- Network-based approach enables comprehensive, risk-based protection
- Threat and Entity Based Analytics autonomously detects attacks and creates mitigation rules

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.