CEQUENCE

DATASHEET

# Cequence Unified Application Protection for Telecom

## Protecting global telecommunications organizations against application, API, and AI attacks

A consistent early adopter of technology, the telecommunications industry was among the first to embrace APIs and microservices to further business goals, like reducing cost and transaction friction, increasing visibility, and providing customers with compelling new services. Internal carrier services like billing, account management, and payments, along with external integration with third-party service providers like Apple, Netflix, Hulu, etc. all depend on APIs. Today, we also see organizations moving to take advantage of agentic AI. To ensure uninterrupted business success, security teams must prevent the misuse and abuse of these business-critical services.

## Application and API Security Challenges

Today's organizations face unique, cross-functional challenges when it comes to protecting critical applications and APIs from cyberattacks. It's not just an IT or security problem; malicious bot attacks on applications and APIs can affect ecommerce, customer satisfaction, marketing and sales analytics, and more.

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. Failing to do so allows attackers to discover unmanaged and unprotected APIs containing critical vulnerabilities that can lead to exploited applications and data breaches.

Further, 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 work with development teams to remediate pinpointed areas of security risk.

Last, 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.

## Security leaders are now asking fundamental questions:

1. How many APIs do I have and where are they?
2. What risks do my APIs pose?
3. How can I protect *all* of my applications and APIs from abuse and attack?
4. Are my applications and APIs under attack?

Answering these questions is critical to a robust security program, a task made more difficult due to the nature of business. New product launches, organic growth, and acquisitions all require a solution capable of keeping up with this constant change.

## Telecommunications Use Cases

**Mitigate SIM Swaps**

**Reduce CPNI Leakage**

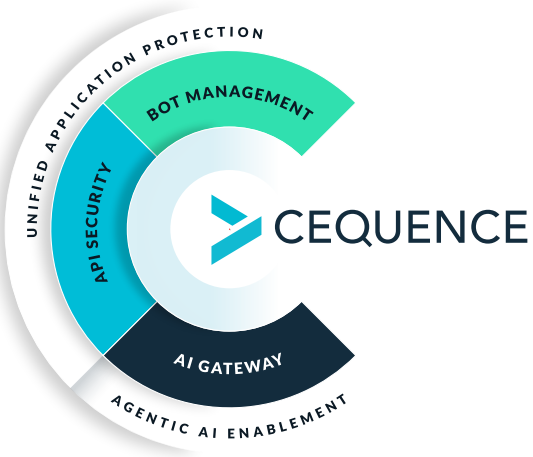
**Protect Hype Sales**

**Prevent Account Takeover (ATO)**

**Prevent Device Activation Fraud**

**Prevent Device Port-In Fraud**

# 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 Telecommunication Brands

**$10T** Business value protected

**8B** Daily API transactions secured

**4B** User accounts safeguarded

T-Mobile · verizon · Telstra · one.nz · Telia · e& · TURKCELL

CEQUENCE

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