CEQUENCE

Datasheet

Cequence Unified API Protection for Telecom

Protecting global telecommunications organizations against application & API attacks

Introduction

A pioneering 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. Today, 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. 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 security teams face numerous challenges when it comes to protecting critical applications and APIs from cyber attacks.

First, 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, these unmanaged and unprotected APIs often contain critical vulnerabilities that can lead to exploited applications and data breaches.

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

Third, API applications are constantly probed by attackers seeking any opportunity to exploit an application and compromise your organization. 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?

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

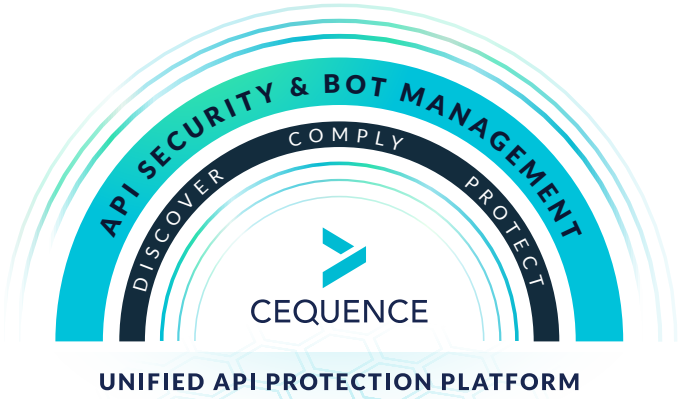
Protect Hype Sales

Prevent Account Takeover (ATO)

Prevent Device Activation Fraud

Prevent Device Port-In Fraud

The Cequence Unified 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 Telecommunication Brands

$10T Business value protected

8B Daily API transactions secured

3B User accounts safeguarded

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

CEQUENCE

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