CEQUENCE

Cequence Security Corporate Overview

Founded in 2014, Cequence Security pioneered API security and bot management, protecting the applications and APIs that organizations depend on from attacks, business logic abuse, and fraud. Our unique Unified API Protection platform unites discovery, compliance, and protection capabilities, providing unmatched real-time security in the face of sophisticated threats. Demonstrating value in minutes rather than days or weeks, Cequence offers a flexible deployment model that requires no app instrumentation or modification. Cequence solutions scale to meet the demands of the largest and most demanding private and public sector organizations, protecting more than 10 billion daily API interactions and 4 billion user accounts. The company is venture-backed and is headquartered in Santa Clara, California, USA with personnel located globally.

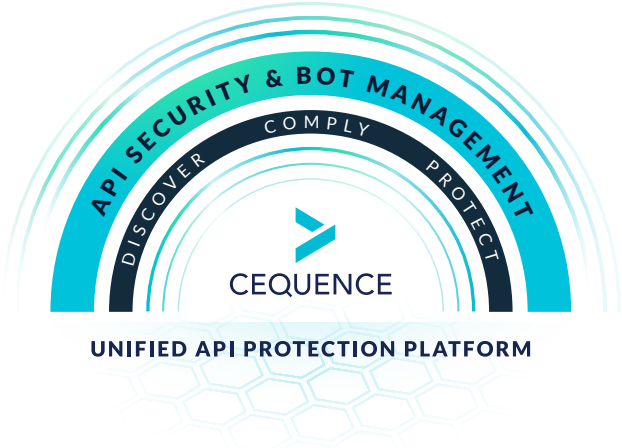
DELL Technologies CAPITAL · HarbourVest · Hewlett Packard Enterprise · ICON VENTURES · kpn · MENLO VENTURES · Prosperity7 · SANABIL INVESTMENTS · SHASTA · TITANIUM VENTURES · T-MOBILE VENTURES

The Problem: Applications and APIs at Risk

Digital transformation, leveraging the cloud, and escalating use of artificial intelligence (AI) have conspired to cause organizations and their applications to depend on an exploding volume of internal, external, and third-party APIs. This new and often hidden attack surface broadly enables two types of security incidents – automated attacks against an organization's public-facing applications and API coding errors that can introduce threats such as those outlined in the OWASP API Security Top 10.

Traditional approaches to preventing these attacks often require multiple point solutions that are largely ineffective and are hard to manage. What's needed is an innovative, ML-based platform that provides complete visibility into an organization's applications and APIs and with actionable intelligence to protect this modern infrastructure in real time.

The rise of AI brings powerful new business benefits, but also significant risk. AI runs on APIs, and organizations require API protection solutions that can discover AI use and assess its adherence to relevant governance and compliance while ensuring sensitive data, intellectual property, and machine learning (ML) models are properly protected.



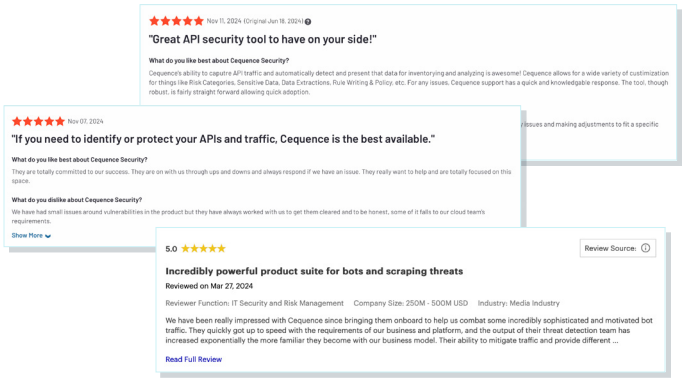
The Solution: Cequence Unified API Protection Platform

The Cequence Unified API Protection (UAP) platform solves these challenges with the only offering that unifies runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to consistently detect and protect against dynamically-evolving online attacks.

- Cequence Bot Management detects threats and attacks, including business logic abuse, enforcing mitigation policies in real time with a range of response options including blocking, rate limiting, header injection, and deception.
- Our API Security offering integrates with your API management infrastructure to identify, inventory, analyze, and test your APIs enabling the discovery and mitigation of API coding errors before they are published or exploited by attackers. Sensitive data is autonomously identified, appropriately masked, preventing inappropriate exfiltration.
- Cequence makes use of ML and AI throughout the UAP platform, from attack detection to automated mitigation. Customizable machine learning models analyze application and API transactions resulting in a unique behavioral fingerprint that determines malicious or benign intent. Findings are then used for policy enforcement or exported via a REST-based API to an existing security infrastructure component.
- Cequence also safeguards authorized GenAI and agentic AI use and defends against unwanted AI bot scraping as well as AI-enabled attacks.

aws PARTNER

- AWS Security Competency
- AWS Retail Competency
- AWS WAF Ready
- AWS CloudFront Ready
- AWS Marketplace Seller



Our Customers

Cequence customers broadly span industry verticals with concentration in retail, telecommunications, and financial services markets where applications and APIs are heavily used and represent prized targets for bad actors. In many cases we have been chosen as a replacement for an existing solution that has failed to prevent malicious attacks. Don't take our word for it – check out what our customers are saying in their Gartner Peer Insights and G2 reviews.

The Cequence Difference

The Cequence UAP platform is the most comprehensive offering available, unifying runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to consistently detect and protect against ever-evolving online attacks without the development and deployment friction associated with alternative offerings.

Application & API Discovery
Automatically discovers APIs across web, mobile, and API applications

No JavaScript or SDK Required
Deployment requires no application modification

Deployable Anywhere
On-premises, SaaS, or hybrid deployment

Open Architecture
Import data to enhance findings, export data to SIEMs, WAFs, to improve workflow

Not a Black Box
Immediate access to attack traffic, policies, and data enables quick response

ML-Powered Platform
Predefined and customizable rules detect and block malicious activity

Prevent Bot Attacks
Provides effective attack defense across all web, mobile, and API apps

Prevent Vulnerability Exploits
Prevent zero-day attacks and address OWASP API Security Top 10 and PCI DSS requirements

API Inventory and Risk Assessment
Inventory internal, external, and third-party APIs, continually assessing risk

Prevent Sensitive Data Leakage
Automatically identifies and masks sensitive data and prevents exfiltration

CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai
© 2025 Cequence Security, Inc. All rights reserved.