

Cequence Platform

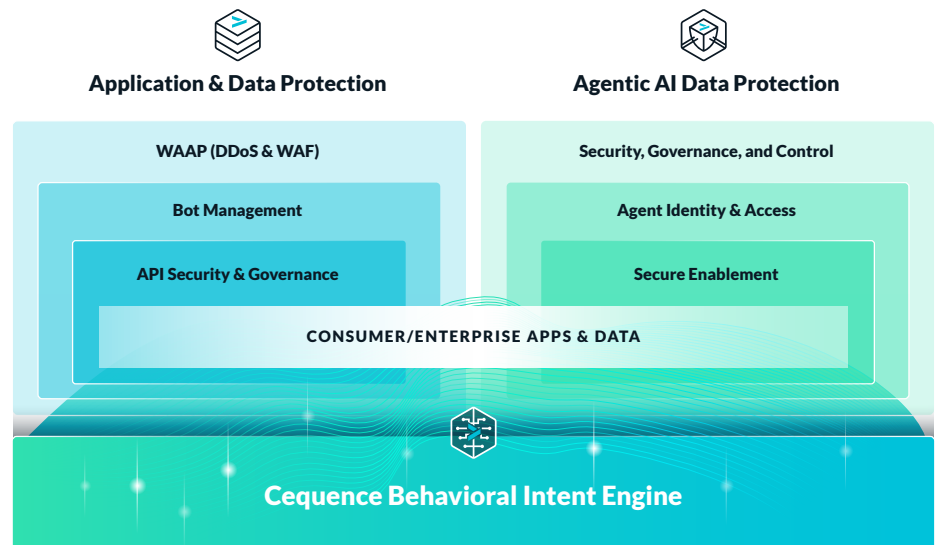
Behavioral Protection for Applications, APIs, and AI

The Attack Surface Keeps Growing

Cloud adoption, increasingly integrated systems, third-party supply chain dependencies, and the advent of AI have dramatically increased the enterprise attack surface, putting applications and data at risk. Applications and APIs continue to proliferate, AI enables bad actors to discover vulnerabilities and attack at machine speed, and rogue AI agents threaten to leak data and overstep their access. Organizations need a solution that enables them to realize the promise of AI-fueled productivity and growth while protecting their applications, APIs, and data from attacks, business logic abuse, and fraud.

The Unique Cequence Approach

Every application, API, and AI interaction reveals its intent through its behavior. Behavioral intent is the foundation of the Cequence platform. It profiles every user, bot, and agent interacting with your applications, APIs, and data, building digital identities that distinguish legitimate automation from malicious activity. That same capability now extends to agentic AI: Cequence applies behavioral analysis to agent-to-application traffic to enforce in real time what agents can do, what data they can access, and take action when their actions fall outside acceptable bounds.



Cequence Products



AI Gateway

Connecting and protecting agentic AI workflows



Bot Management

Protect applications and APIs from automated attacks and fraud



API Security

Discover, inventory, test, and secure your API endpoints



WAAP

Bot Management, API Security, WAF, and DDoS protection

Cequence AI Gateway enables organizations to make their applications and data accessible to AI agents easily and securely. It offers a central location for visibility and monitoring, trusted MCP, API, LLM, and skill registries, and company-vetted app catalog. The AI Gateway has built-in governance and guardrails to constrain agent behavior using capabilities that include least privilege access, rate-limiting, and sensitive data protection.

Based on zero trust principles, the AI Gateway provides continuous verification and validation of behavior at runtime. With these guardrails and controls in place, the AI Gateway enables organizations to swiftly innovate while respecting governance, going from prototype to production without incurring the technical debt and scalability limitations associated with basic solutions.

Cequence API Security is an AI-first solution that discovers, inventories, and tests APIs, providing comprehensive API security posture management. It discovers internal, external, and third-party APIs as well as edge, infrastructure, gateway, and hosting providers.

A combination of inside-out and outside-in discovery provides attack surface and internal API visibility and inventory. API Security autonomously identifies sensitive data traversing APIs and masks it at runtime, preventing unwanted exfiltration. API Security includes an AI Assistant to guide practitioners and a built-in MCP server to integrate with their internal agentic workflows.

Cequence Bot Management detects a wide range of automated attacks and enforces mitigation policies in real time to prevent data loss, theft, and fraud. Bot Management is network based, integrating with the infrastructure you already have, and requires no agents, JavaScript, or SDKs.

Behavioral fingerprints and multi-dimensional analytics provide a deep understanding of business context to identify and natively block attacks in real time. It mitigates a wide variety of cyberattacks including business logic attacks, exploits, automated bot activity, online fraud, and OWASP API Security Top 10 threats.

Cequence Web Application and API Protection (WAAP) combines Bot Management and API Security with WAF and DDoS protection in a single SaaS tenant.

Integrated components within a shared traffic pipeline eliminate the coverage gaps and routing inconsistencies that plague multi-vendor deployments. A single application protection portal spans WAF, bot management, and API security, reducing administrative complexity while maintaining consistent, coordinated defense across every application and API interaction.

Use Cases



Agentic AI Security and Governance

Visibility, monitoring, guardrails, and control for agentic AI workflows



No JavaScript or SDK Required

Deployment requires no application modification



Deployable Anywhere

On-premises, SaaS, or hybrid deployment



Prevent Bot Attacks

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



Not a Black Box

Immediate access to attack traffic, policies, and data enables quick response



Secure Agentic AI Enablement

Make enterprise and SaaS applications agent-ready – securely



Open Architecture

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



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 Platform Features

Behavioral Intelligence, Precise Identity

Cequence profiles user and entity behavior to establish rich digital identities, so organizations can enable productive agents without opening the door to malicious bots. It accurately distinguishes humans from bots, and between legitimate automation and threats. For an extra level of authentication, Cequence's Biometric Check can leverage a visitor's Secure Enclave on their device rather than adding unnecessary friction with a CAPTCHA.

Runtime Protection, Real-Time Response

Cequence operates at runtime, detecting attacks the moment they emerge and responding dynamically before damage is done. Rather than relying on static rules or after-the-fact analysis, the platform continuously evaluates live traffic to identify threats in real time and trigger immediate, precise countermeasures – keeping applications, APIs, and data protected without interrupting legitimate users.

Modular Architecture, Flexible Deployment

Cequence analyzes and protects more than 10 billion application and API interactions daily across some of the world's largest financial services, retail, and telecom organizations. Start with the Cequence products you need today and expand as your requirements grow. Fast, flexible deployment across SaaS, on-premises, and hybrid environments means the platform adapts to your infrastructure, not the other way around.

Unified Platform, Integrated Protection

The Cequence platform is built for integration from the ground up. Our native integration eliminates the blind spots and operational overhead of stitching together point solutions, and gives organizations a single, coherent defense across bot, API, and AI use cases.

"I don't want to have any interactions with threat actors on my edge — I want to push that perimeter out as far as I can. Cequence is able to intercept bad traffic from threat actors outside of our perimeter. With this capability, our threat posture has been significantly improved."

Maria Ng
CISO

