

Cequence Bot Management

Bot Detection, Mitigation, and Fraud Prevention

Bots, both good and bad, generate almost half of all web traffic today. Malicious bots used to primarily target websites and applications, but today they often bypass apps and target APIs directly. The ubiquity of APIs combined with their accessibility, ease of use, and flexibility have made them a top target for threat actors. Even properly-coded APIs can be subject to business logic abuse as part of a large-scale account takeover (ATO) or shopping bot campaign. Mass fake account creation and content scraping efforts are regularly executed against applications and their APIs. Organizations need a solution that detects and prevents automated attacks against their applications and APIs, is easy to deploy, and is immediately effective.

Cequence Bot Management Overview

Cequence protects an organization's web, mobile, and API applications from the full range of bot attacks — both conventional and AI-enhanced — to prevent data loss, theft, and fraud. Powered by an ML-based analytics engine that analyzes behavior in real time if application and API transactions are malicious or legitimate, it natively mitigates attacks and eliminates harmful business impacts such as downtime, brand damage, skewed sales analytics, and increased infrastructure costs.

Bot Management Features

No Application Modification or Customer Friction

Cequence's network-based approach precludes the need for agents or any application modification such as JavaScript or mobile SDK integration. This approach eliminates customer friction induced by bot-prevention methods such as CAPTCHAs and extends coverage to all applications and APIs, and not just those that can be instrumented. Network-based protection eliminates the development and testing effort required by app instrumentation, saving time and expense.

Bot Management at a Glance

- ✓ **No CAPTCHA Needed** — network-based approach requires no agents, JavaScript, or SDK integration
- ✓ **Native Mitigation** — attack identification and blocking without relying on third-party infrastructure such as WAFs
- ✓ **Robust Mitigation Options** — blocking, rate limiting, header injection, and deception
- ✓ **Flexible Deployment Model** — supports on-premises, SaaS, and hybrid
- ✓ **API Fraud Prevention** — customizable, granular policies for organization-specific use cases

Organizations may not even know they have a bot problem; bots are simply a way to automate attacks at scale. Cequence detects and mitigates a variety of attack types, including:



Account takeover (ATO)



BOLA vulnerabilities



Flash sales, hype sales, and sneaker drops



Sensitive data exposure



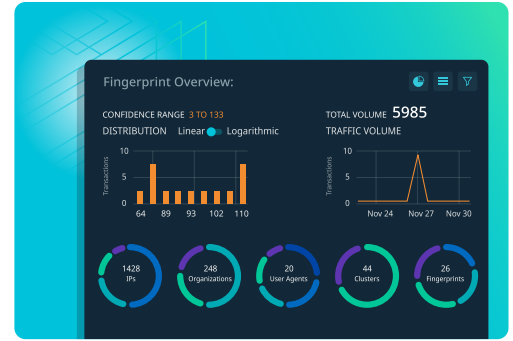
Gift card / loyalty program abuse



Fake account creation

Continuous Behavior-Based Threat Detection and Response

Cequence's ML-based analytics engine analyzes behavioral intent across web, mobile, and API traffic, identifying legitimate and malicious traffic based on behavior, not just IP addresses. Using this analysis, the solution develops behavioral fingerprints that continuously track sophisticated attacks, even as adversaries retool to avoid detection. This approach is highly effective and works against both conventional and AI-powered bot attacks.



Real-Time Mitigation

Cequence uses AI to detect attacks and autonomously creates threat mitigation rules and policies that can be implemented automatically or after human review. Native mitigation occurs in real time and options include blocking, rate limiting, header injection, and deception.



Friction-Free User Verification

Traditional bot defenses have hit their limits. ML models now solve image-based CAPTCHA challenges with higher accuracy than the average human, and SMS farms exploit carrier infrastructure to intercept one-time codes at scale. Cequence's Biometric Check takes a different approach: instead of presenting a puzzle or sending a code, it redirects suspicious sessions to the device's native authentication prompt, whether that's Face ID, Touch ID, or Windows Hello. The result is silent, sub-second verification that confirms a real person is behind the request without adding any friction to the user journey.

Rapid Time to Value

Cequence is easily deployed and immediately effective, with no application modification required. The solution features flexible SaaS, on-premises, and hybrid deployment options to meet the needs of any organization.



Fraud Prevention Tailored to Your Business

Cequence Bot Management also includes fraud prevention capabilities that support customizable, granular policies for fraud prevention use cases specific to your business and vertical. Activity matching those fraud policies is identified and blocked in real time and detailed information for analysis of each fraud campaign is provided.

Works with Cequence AI Gateway

The Cequence AI Gateway enables secure agentic AI access to any internal, external, or SaaS application, in minutes, without coding. Bot Management ensures that enterprise applications and APIs are protected from malicious agents.

Bot Management is Part of the Cequence Platform

The Cequence platform provides secure agentic AI enablement while protecting web, mobile, API, and AI channels from attacks, business logic abuse, and fraud. A deep understanding of user, entity, and agent behavior makes Cequence uniquely qualified to safely and securely enable agentic AI access, allowing enterprises to unlock the promise of AI-fueled productivity and growth. Cequence's platform gives organizations the security, governance, and control they need to maximize focus on their true mission.

