CEQUENCE

Datasheet

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.

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, logging, 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

Cequence Bot Management Overview

Cequence protects an organization's web, mobile, and API applications from the full range of bot attacks to prevent data loss, theft, and fraud. Powered by an ML-based analytics engine that determines 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.

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

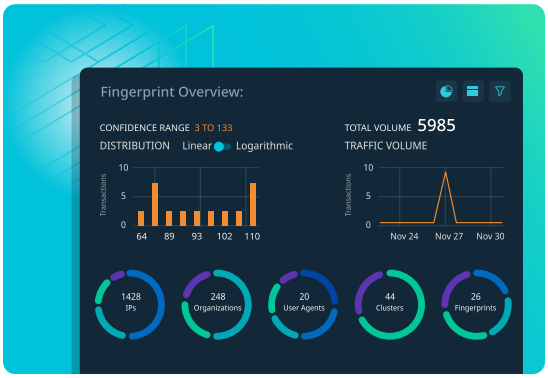
Sensitive data exposure

Gift card / loyalty program abuse

Fake account creation

Continuous Behavior-Based Threat Detection

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 requires no client-side or application integration, ensuring the broadest possible application and API protection.



AI and ML-Powered Bot Defense

Cequence leverages ML and AI throughout the entire UAP platform, from attack detection to mitigation. ML models enable accurate endpoint and threat classification, sensitive data detection, behavioral fingerprinting, and more. ML also powers Cequence's unique ability to detect malicious activity and autonomously create threat mitigation rules and policies that can be implemented automatically or after human review. Cequence protects authorized GenAI and agentic AI use in the enterprise and protects against unwanted scraping by AI bots and AI used by malicious actors for sophisticated attacks.

Rapid Time to Value

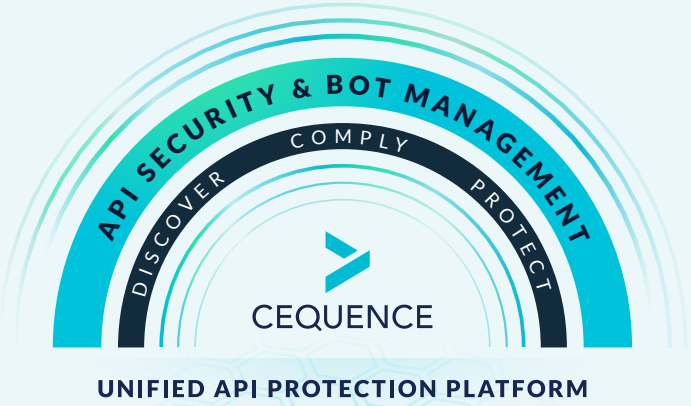
Cequence is easily deployed and immediately effective, with no application modification required. The solution features flexible SaaS, on-premises, and hybrid deployment options to meet the needs of any organization.

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. As traffic flows to APIs, activity matching those fraud policies is identified and blocked in real time and detailed information for analysis of each fraud campaign is provided. New policies can be created and out-of-the-box policies can be modified by the customer with no coding required.

Bot Management is Part of the Cequence Unified API Protection Platform

The Cequence Unified API Protection platform unites discovery, compliance, and protection to defend an organization's applications and APIs against attacks, business logic abuse, and fraud. 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 billions of user accounts and billions more daily API interactions.



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