

Cequence Bot Management

Bot Detection, Mitigation, and Fraud Prevention

Every digital experience your customers have, whether on a web application, a mobile app, or an embedded third-party service, runs on a foundation of APIs, microservices, and cloud infrastructure. Organizations depend on this architecture to serve users at scale, integrate third-party services, and push new capabilities to market without friction. But the same properties that make it powerful – modularity, openness, and ubiquitous connectivity – make it an attractive target. The attack surface expands with every new endpoint, every new integration, and every new AI-powered workflow the business adopts.

Automated bot attacks exploit that expanded attack surface. Adversaries no longer target applications one at a time; they attack web apps, mobile apps, APIs, and the microservices beneath them, using automation that mimics legitimate user behavior well enough to bypass conventional defenses. Pre-built attack toolkits are commoditized. Stolen credentials are readily available and cheap. And now, AI arms attackers with capabilities that adapt in real time to evade detection faster than a human ever could.

The New Threat: LLM Bot Scraping and AI-Powered Attacks

AI has introduced a new class of automated threat that conventional bot defenses were never designed to handle. Large language model (LLM) providers and AI agent frameworks send crawlers and scrapers across the web and into application endpoints to harvest training data, retrieve real-time context, and execute tasks on behalf of users. Most of these bots arrive with accurate user-agent strings and behave like browsers, making signature-based detection useless. Some, however, operate under fraudulent or absent identification, scraping proprietary content, pricing data, product catalogs, and customer-facing APIs without authorization, at scale.

Bot attacks are now AI-enhanced. Attackers use AI to generate synthetic behavioral patterns that defeat traditional bot detection. AI-powered attack platforms vary timing, session depth, click patterns, and navigation paths to mimic the profile of human users. They solve CAPTCHAs automatically, retool in response to detection signals, and optimize attack parameters mid-campaign. All at machine speed.

Cequence Bot Management – Behavioral Detection and Response

What separates Cequence from every other approach is behavioral intent analysis. Rather than asking “Is this a known bad IP address?” or “Does this request match a known attack signature?”, Cequence asks: “What is this traffic trying to do?” Multi-dimensional machine learning models analyze behavior across the full application and API traffic flow, distinguishing legitimate use from malicious automation based on intent, not identity. Modern attackers route through trusted residential proxies, rotate through millions of IP addresses, and use AI to generate requests that look indistinguishable from real users at the packet level. Cequence’s behavioral intent engine cuts through all of that to accurately detect malicious activity, regardless of attack volume.

Bot Management in the AI Era

Behavioral analysis has been the foundation of the Cequence platform from inception, and that approach maintains effectiveness in the era of AI. Cequence identifies unauthorized AI crawlers and LLM scraping bots by what they do, not just what they claim to be. The same engine that detects credential stuffing and account takeover detects AI-driven enumeration, data harvesting, and business logic abuse, and does so without requiring any changes to your applications or infrastructure. Cequence also protects authorized generative AI and agentic AI deployments in the enterprise, ensuring that the AI your organization runs is secured from abuse and that your data is not feeding someone else's model.

Common Bot Management Use Cases

Account takeover (ATO)



Using stolen credentials to gain unauthorized access to accounts.

Credential stuffing



Using stolen credentials to access accounts and services.

Content Scraping



Scraping sensitive financial data, impacting market decisions.

Flash sales, hype sales, and sneaker drops



Mass purchasing high-demand products quickly for resale.

Sensitive data exposure



Exfiltrating sensitive data exposed by APIs for nefarious purposes.

Gift card / loyalty program abuse



Brute-forcing card object combinations to find valid gift cards or loyalty program details.

Business logic abuse



Exploiting intended app or API functionality

SIM swapping



Compromising user accounts with unauthorized SIM swaps.

Traditional Bot Mitigation Techniques Fall Short

Web Application Firewalls

The proliferation of web applications necessitated security solutions that could protect them from a new generation of attackers, leading to the adoption of Web Application Firewalls (WAFs). However, WAFs prevent attacks by blocking specific IP addresses, and attackers often bypass them by spreading their attacks across millions of IP addresses available through bulletproof proxies. WAF geo-fencing defenses are often evaded using residential IP addresses that blend in with legitimate customer traffic. WAFs also look for suspicious HTTP headers, but today's attacker tools easily mimic real browsers and "user agents." WAFs are a useful tool for a defense-in-depth strategy, but are insufficient as a standalone control.

CAPTCHAs and SDKs

Another common bot mitigation technique employs JavaScript or SDKs integrated into web pages, applications, and mobile applications. CAPTCHA is likely the most well-known of these types of mitigations. However, these techniques are easily bypassed by attackers, particularly in the age of AI. CAPTCHAs often have a significant impact on user experience, application load times, and require development and QA time to implement and test.

Cequence Bot Management Key Features

Industry-Leading Bot Detection

Unlike legacy bot solutions, Cequence identifies anomalous behavior through network-based detection and multi-dimensional ML, with no client-side or application integration required. Cequence analyzes behavior across web, API, and mobile traffic, differentiating between legitimate and malicious bots based on behaviors and other criteria rather than simply their IP address or other easily falsified identifier. The result is highly effective application and API protection from the full range of automated attacks including and beyond the OWASP API Security Top 10.

Fast Time to Value

Cequence protects against bots immediately upon deployment with hundreds of customizable rules based on common behavioral traits of automated attacks. The ML engine analyzes traffic to detect attacks and track them as they evolve, even as adversaries retool to avoid detection. This approach eliminates the need for JavaScript and mobile SDK integration and associated customer friction, development time, and page load delays. Additionally, protection is extended to all traffic and not limited to applications and infrastructure that have been modified. Cequence's platform integrates with your existing enterprise infrastructure, including SIEMs, web application firewalls, and enterprise ticketing systems.

Real-Time Mitigation

Other bot defense solutions claim to block attacks, but most provide varying levels of detection and rely on third-party solutions such as Web Application Firewalls (WAFs) to provide only basic IP blocking. Cequence provides native detection and robust mitigation options including blocking, logging, rate limiting, header injection, and deception.

Friction-Free User Verification

CAPTCHA and SMS codes do not reliably separate humans from bots – ML models solve image challenges more accurately than most users, and SMS farms exploit carrier vulnerabilities at scale. Cequence's Biometric Check routes suspicious traffic to a user's native biometric authentication such as Face ID, Touch ID, or a Windows Hello prompt instead, confirming a real person is present in under a second with no puzzles, no codes, and no conversion-killing friction.

Fraud Prevention

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, malicious 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. Detailed incident forensics provides transaction analysis with key insights into fraudulent and malicious activities.

Key Cequence Bot Management Features

- ✓ **Deployment flexibility**
On-premises, SaaS, or hybrid
- ✓ **No application modification**
No server- or client-side agents, JavaScript, or SDK integration required
- ✓ **High visibility and control**
Not a "black box"; users can drill into incident forensics
- ✓ **Application content-aware protection**
Inspects entire application flow
- ✓ **Detects and prevents fraud**
Absent in traditional bot management products
- ✓ **Privacy-friendly**
No collection of user or device telemetry
- ✓ **Complete data protection**
All data stays within customer's secure perimeter

Managed Threat Protection Service

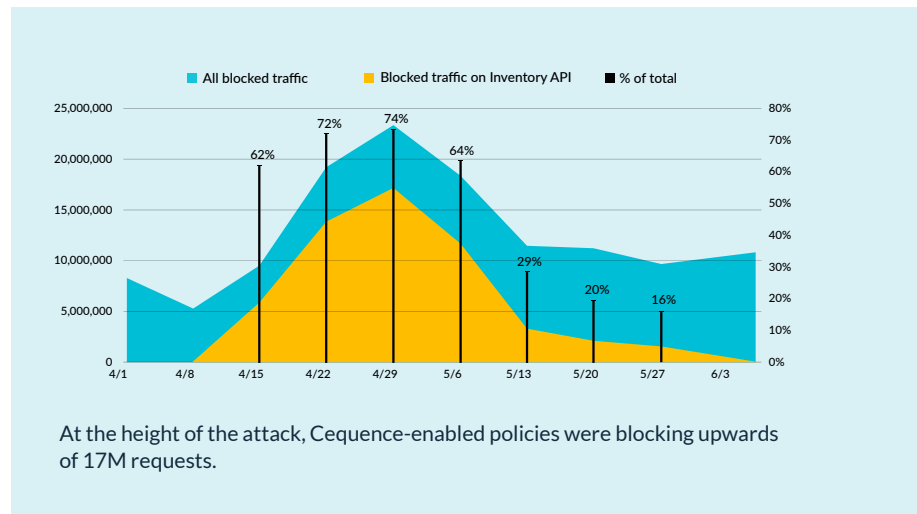
Cequence also offers a managed threat protection service staffed by experienced data science and cybersecurity experts. This service can be utilized for the optional tuning of ML models, policy updates, creating application-specific rules, and to supplement existing staff during business-critical events such as product launches and flash sales.

Case Study: Ulta Beauty and Cequence Block Enumeration Attacks

Ulta Beauty experienced a persistent, high-volume inventory scraping attack with the apparent goal of enabling shoplifting opportunities by mapping physical store inventory. The attack caused local inventory search API traffic to increase up to 700 times normal volumes, rotating through more than 153,000 unique product and SKU combinations across 61,000 zip codes. The attack exhibited the following characteristics:

- Trusted, residential proxy IP addresses were used to make IP-based blocking ineffective
- The attack enumerated ZIP codes to find high concentrations of specific, high-value products
- Attackers targeted web APIs first, then pivoted to mobile APIs

Cequence assisted the Ulta Beauty team with creating policies that successfully blocked 85.9M total requests resulting in at least \$80,000 saved in infrastructure and loss prevention.



Key to the successful mitigation and ongoing prevention of this attack were the rapid response and teamwork between Ulta Beauty's Cyberthreat Intelligence Team and Cequence, identifying the attack behavior and responding with effective blocking policies.

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. Learn more at cequence.ai.

