CEQUENCE

Solution Brief

Cequence Bot Management

APIs and Bot Management

In the past decade, extensive infrastructure changes have swept through organizations as part of digital transformation. Monolithic web and mobile applications were modularized and broken down into microservices that provide the same business logic through APIs, and the advent of cloud environments such as Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP) led to further infrastructure dispersion. These changes offered businesses unprecedented infrastructure flexibility and scalability; web applications work better, suffer less downtime, and are able to serve an ever-growing number of users. However, these changes also reduced infrastructure visibility for security and IT teams and increased the overall attack surface.

APIs are now the common method by which disparate applications communicate with each other, especially between vendors and organizations; they are easy to use, flexible, and fast. While this makes it much easier to integrate and share data between applications, it also enables adversaries to easily automate attacks at massive scale with networks of malicious bots. Ready-made bot attack toolkits have become extremely sophisticated, and the trove of stolen credentials available on the internet has streamlined the ability for adversaries to abuse business logic and take over accounts to commit fraud or steal sensitive information. Many API attacks mask themselves as legitimate transactions, making it difficult to determine which activity to block.

71%

of organizations use APIs to connect applications to API workloads

78%

of organizations expect over half of their applications to use APIs by 2027

33%

of organizations have experienced multiple API-related security attacks

Source: *Enterprise Strategy Group, "API Security from Development to Runtime"*

Increased Regulatory Pressure

In addition to security concerns, maturation of the regulatory environment has clarified requirements and increased penalties for non-compliance. Well-known regulations such as HIPAA and PCI DSS require systems that process Personal Identifiable Information (PII) to be compliant and protect consumers against fraud and privacy violations. Some regulations call out API protection specifically; for example, the Federal Financial Institutions Examination Council (FFIEC) has established security guidelines and addressed API security specifically in its most recent Authentication and Access guidance.

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.

Web 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

Gathering 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.

SIM swapping

Compromising user accounts with unauthorized SIM swaps.

Traditional Bot Mitigation Techniques

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."

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.

The Evolution of API Protection Against Malicious Bots

Adversaries continue to evolve, quickly moving beyond simple site-scraping bots and onto custom-made attack platforms. APIs are well defined "doorways" into modern systems and applications, requiring more sophisticated and holistic mitigation and protection methods. The ideal solution must discover every API an organization has – internal, external, third-party, managed and unmanaged, known and unknown. It must employ API security posture management through risk analysis, API specification compliance evaluation, and vulnerability testing. Finally, the solution must provide blocking and mitigation to prevent targeted attacks, business logic abuse, and fraud.

The best solutions deliver the following benefits:

- Deploy rapidly and easily with fast time to value
- Protect applications and APIs without requiring infrastructure changes or code-level integrations such as CAPTCHAs
- Be agile, responsive, and resilient to adversary re-tooling
- Intelligently identify behavioral anomalies and evolve with attacks
- Provide broad coverage for APIs for web and mobile applications as well as those for cloud- and microservices-based architectures

Cequence Unified API Protection

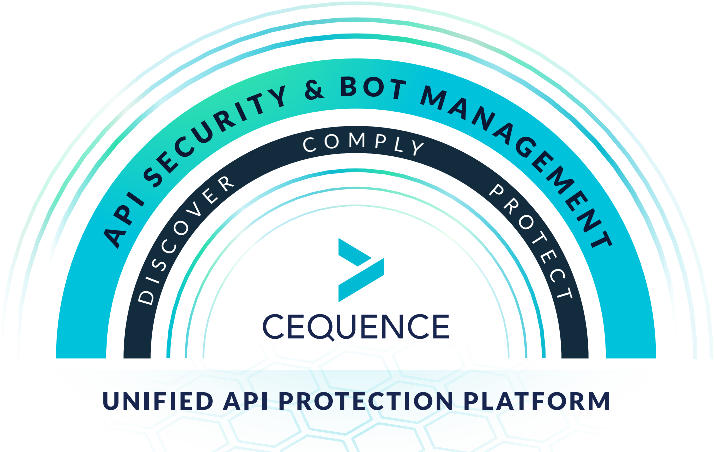
The Cequence Unified API Protection platform unites API security and bot management, offering discovery, compliance, and protection for all applications and APIs.

ML-Powered Behavioral Fingerprinting

Cequence offers a unique approach to bot management, utilizing multi-dimensional machine learning (ML) techniques to identify anomalous behavior without client-side or application integration. Cequence scrutinizes behavioral intent across API, web, 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 criteria. The result is highly effective API and web application 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


API SECURITY & BOT MANAGEMENT
DISCOVER
COMPLY
PROTECT
CEQUENCE
UNIFIED API PROTECTION PLATFORM

The Cequence Unified API Protection platform is the only solution that addresses the entire API lifecycle: discovering the complete attack surface, managing the API security posture, and detecting and mitigating attacks.

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.

Other API security 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, including blocking, as part of the platform's complete API security lifecycle management.

Other bot management solutions rely on instrumenting each application, which is time consuming and leaves APIs unprotected. Cequence's network-based deployment offers protection for all APIs without involving development teams for code or SDK integration.

AI and ML-Powered Bot Defense

Cequence leverages ML and AI throughout the entire UAP platform, from attack detection to automated 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 defends against unwanted scraping by AI bots and AI used by malicious actors for sophisticated attacks.

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.

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.

Key Cequence Bot Management Features

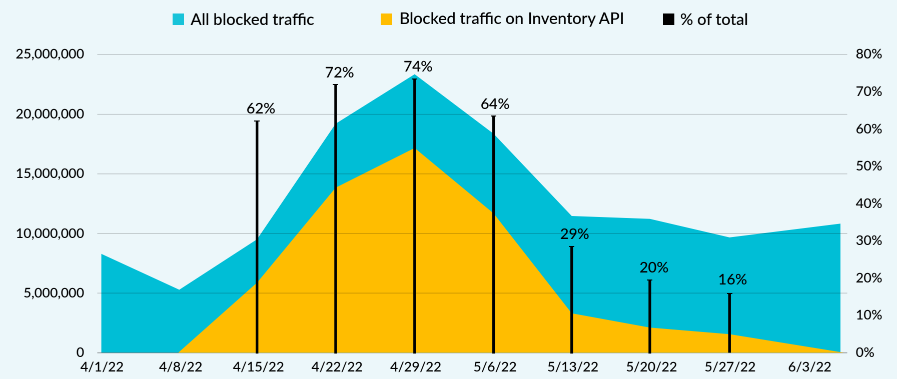
- ✓ **Deployment flexibility**
  On-premises, SaaS, or hybrid
- ✓ **No application modification**
  No server- or client-side agents, JavaScript, or SDK integration required
- ✓ **High visibility and control**
  Not a "black box"; users can drill into incident forensics
- ✓ **Application content-aware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

Case Study: Ulta Beauty and Cequence Block API-based Enumeration Attacks

Ulta Beauty experienced a persistent, high-volume inventory API 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
- Web APIs were targeted initially, quickly pivoting to mobile APIs which provided similar information

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.



At the height of the attack, Cequence-enabled policies were blocking upwards of 17M requests.

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.

The Cequence Advantage

Cequence enables customers to reap the competitive and business advantages of secure, ubiquitous API connectivity. The Cequence solution induces attack futility, failure, and fatigue for even the most relentless of attackers and improves visibility and protection while reducing cost, minimizing fraud, data loss, non-compliance, and business disruption. Learn more at **cequence.ai**.