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; websites work better, suffer less downtime, and are able to serve an ever-growing number of visitors. 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 more easily automate attacks. Ready-made 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 in order to commit fraud or steal sensitive information. Many API attacks mask themselves as legitimate transactions, making it difficult to determine what activity to block

Increased Regulatory Pressures

In addition to security concerns, maturation of the regulatory environment has clarified requirements and increased penalties for non-compliance. Commonly-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. The Federal Financial Institutions Examination Council (FFIEC) has established security guidelines and addressed API security specifically in its most recent Authentication and Access guidance.

70% of application requests
come from API transactions[1]

53% orgs impacted
by three or more API attacks per month[2]

80% of traffic
found to be malicious and blocked[3]

Early Bot Mitigation Techniques

The proliferation of APIs necessitated security solutions that could protect them from a new generation of attackers, and Web Application Firewalls (WAFs) were initially the tool of choice.

However, since WAFs prevent attacks by blocking specific IP addresses, attackers can easily bypass them by spreading their attacks across millions of IP addresses available through bulletproof proxy vendors. Another mitigation technique frequently utilized is geo-fencing, which also can be easily bypassed using residential IP addresses to blend in with customer traffic. Additionally, WAF signatures are often used to look for suspicious HTTP headers, but today's attacker tools can successfully mimic real browsers.

Another common bot mitigation technique employs JavaScript or SDKs to integrate data collection capabilities into web pages and mobile applications. CAPTCHA is likely the most well-known of these types of mitigations. However, these techniques can have a significant impact on application load times, user experience, and development time, not to mention the fact that APIs cannot be protected in this manner.

1 https://www.cequence.ai/wp-content/uploads/2022/02/Cequence_Infographic_APIs-tool-of-choice-for-devops-target-of-choice-for-attackers.pdf
2 https://www.cequence.ai/wp-content/uploads/2022/12/PulseSurvey_Balancing_APIBusinessValue_and_Security.pdf
3 https://www.cequence.ai/blog/api-security/api-threat-research-validates-robust-api-security/

Adversaries have evolved as well, with advanced attackers quickly moving beyond simple site scraping bots and into custom-made attack platforms. APIs are well defined "doorways" into modern systems and applications, requiring more sophisticated and holistic mitigation and protection methods.

The Evolution of API Protection

Clearly, a new approach is needed – one that provides protection and defense throughout the entire API lifecycle. The ideal solution must discover every API an organization has – managed and unmanaged, known and unknown, external and internal. Then, it must enable 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:

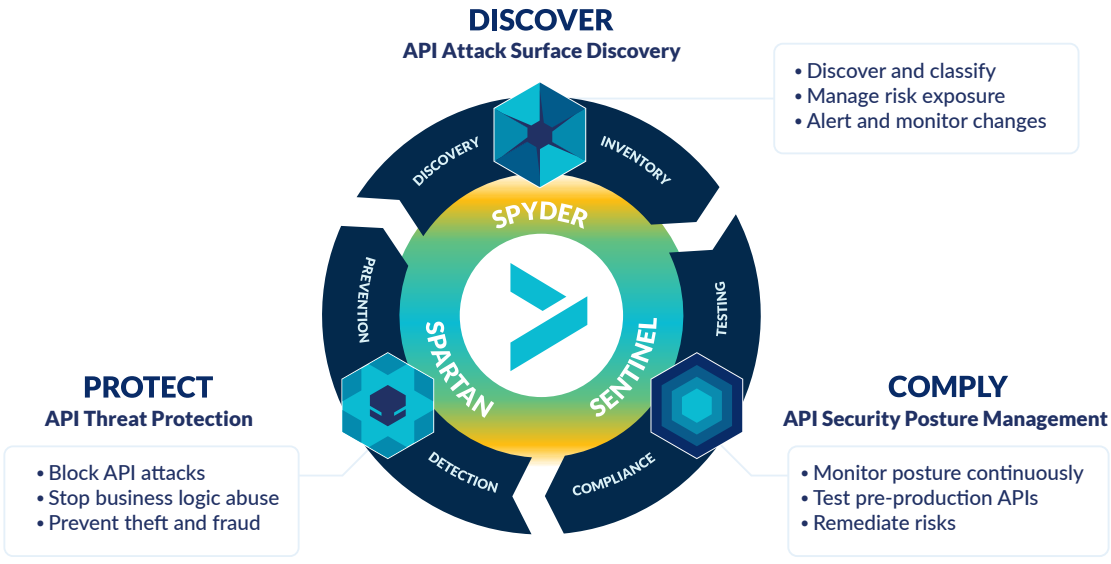
- Provide fast time to value, including rapid deployment
- Be agile, responsive, and resilient to adversary re-tooling
- Analyze large amounts of data to infer behavioral anomalies, enabling the solution to evolve with attacks
- Become easier to implement, preferably in a way that did not require infrastructure changes or code-level integrations
- Protect APIs for web and mobile applications as well as modern APIs for cloud- and microservices-based architectures

Cequence Unified API Protection

The Cequence Unified API Protection platform discovers all your APIs, flags risks for remediation, and detects and mitigates sophisticated threats in real time. The result is complete protection from API threats that cause data loss, theft, fraud, and business disruption.

The Cequence solution offers a unique approach to bot management, utilizing multi-dimensional machine learning (ML) techniques to analyze user behavior without client-side or application integration. Cequence scrutinizes behavioral intent consistently across API, web, and mobile traffic, detecting legitimate and malicious bots based on their behavior determined by machine learning rather than their IP address range or other easily falsified criteria. The result is highly effective API and web application protection from the full range of automated attacks including the OWASP Top 10 API Security and Web Application Security Risks.

Cequence protects against bots immediately upon deployment with hundreds of customizable rules based on common behavioral traits of automated attacks. The machine learning engine analyzes traffic to improve attack detection and evolve with sophisticated attacks, even as they retool to avoid detection. This approach eliminates the need for JavaScript and mobile SDK integration and associated development time and page load delays. Additionally, protection is extended to all traffic and not limited to applications and infrastructure that support application-specific toolkits. Cequence's platform integrates with your existing enterprise infrastructure, including SIEMs, web application firewalls, and enterprise ticketing systems.



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 blocking attacks.

Other solutions claim to block attacks, but most provide varying levels of detection and then rely on other solutions such as Web Application Firewalls (WAFs) to provide actual blocking and mitigation. Cequence provides native detection and blocking as part of the platform's complete API security lifecycle management.

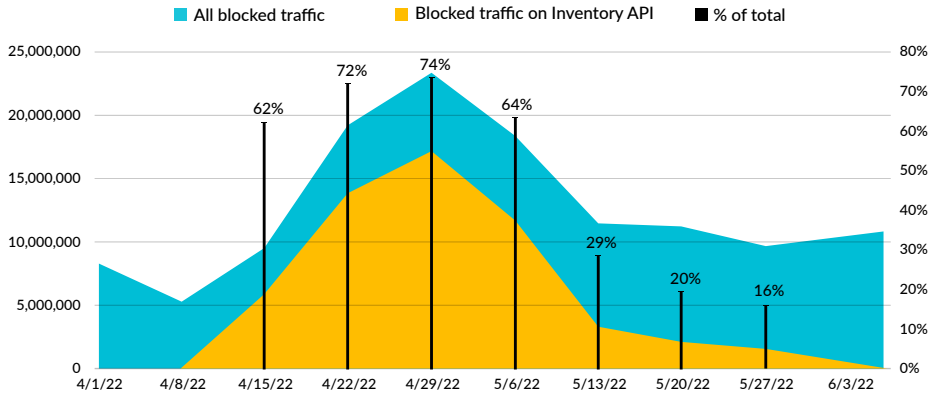
Cequence also offers a managed threat protection service staffed by experienced data science and cybersecurity experts. This service can be utilized for the tuning of ML models, policy updates, creating application-specific rules, and to supplement existing staff during business-critical events such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

Ulta Beauty and Cequence Block API-based Enumeration Attacks

Ulta Beauty experienced a persistent, high-volume inventory API scraping attack with an uncertain goal but a clear threat, such as enabling physical shoplifting opportunities by mapping store inventory. The attack was executed against a third-party API causing local inventory search API traffic to spike 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:

- High-quality, residential proxy IP addresses were used to make IP blocking at the edge difficult
- 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 CTI team to put policies in place 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 Cequence Bot Management Features

- **Deployment flexibility**
  on-premises, SaaS, and Hybrid
- **Zero application integration**
  no JavaScript or mobile SDK required
- **Privacy-friendly and omni-channel ready**
  no collection of user or device telemetry
- **Complete data protection**
  all data stays within customer's secure perimeter
- **High visibility and control**
  not a "black box"; 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

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 Security, who worked closely together to identify the attack and behaviors and respond with effective blocking policies.

The Cequence Unified API Protection platform 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**.