Protecting APIs, Web Apps, and Mobile Apps from Bot Attacks and API Abuse

Protect Your APIs at the Edge

As monolithic web applications have moved to the cloud, APIs have become the common method by which applications communicate. However, they're also a broad new vector for automated attacks which are quite sophisticated and difficult to differentiate from legitimate traffic. Attacks can result in data theft, fraud, increased cloud and bandwidth costs, and more. Amazon Web Services (AWS) and AWS Partner Cequence Security have partnered to deliver a robust solution that improves application performance and security.

The API Protection Lifecycle

DISCOVER

How many APIs do I have?

Organizations must be able to discover and inventory all APIs, including their unknown attack surface. Most organizations are unaware of how many shadow, hidden, deprecated, and third-party APIs they have, where they are deployed, and whether they're protected.

COMPLY

What is my API risk exposure?

APIs must be tested for vulnerabilities and assessed for risk, checking for sensitive data exposure while ensuring compliance with relevant API specifications. A rigorous compliance regimen helps protect against vulnerabilities that can be exploited by bad actors.

PROTECT

Am I protected from attacks?

APIs are prime targets for automated attacks and business logic abuse. It's crucial to not only inform, but take action, leveraging threat intelligence to quickly detect and natively block malicious activity rather than relying on other infrastructure that isn't equipped to handle this at scale.

Features

API Bot & Abuse Management

Detects and prevents sophisticated automated API and bot attacks, including business logic abuse, using hundreds of ML rules that leverage an API threat database containing billions of malicious behaviors, IP addresses, and organizations. Agentless, no-integration approach to threat protection eliminates the need for JavaScript or SDK integration. Native, policy-based response options ensure that any detected attack is blocked in real time, without relying on third-party WAFs, API gateways, or load balancers for mitigation.

API Discovery

Cequence provides a runtime inventory of public and private APIs, the origin of API requestors, and helps organizations discover shadow APIs including undocumented endpoints or private APIs that are publicly available. Cequence identifies risky APIs, including those using weak authentication, do not conform to their latest specification, are communicating sensitive information such as PII or PCI data, as well as other vulnerabilities outlined in the OWASP API Security Top 10.

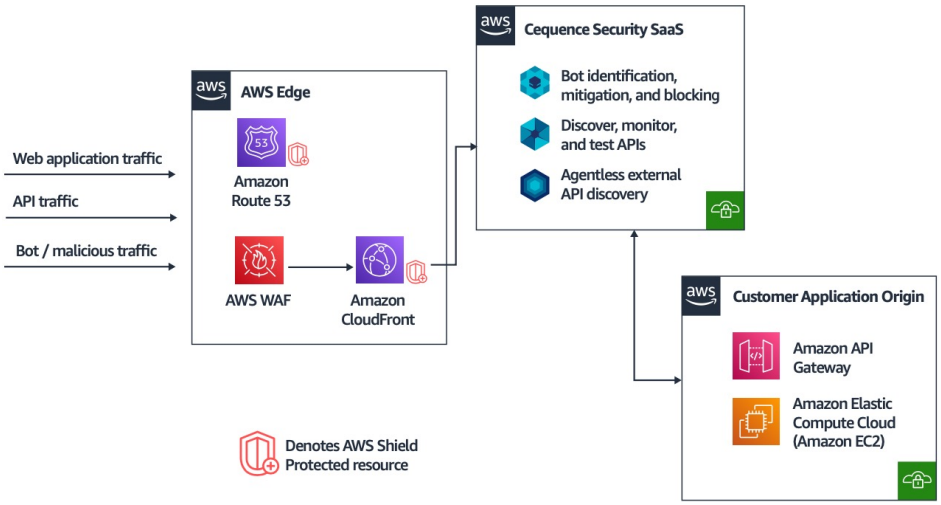
AWS and Cequence Unified API Protection

Using Amazon CloudFront as your CDN helps you accelerate static, dynamic, and API traffic with high-performance and built-in security functionality such as AWS Shield, Compliance Standards, and Identity and Access Management. Deployed with CloudFront, Cequence detects your public-facing applications and APIs, then analyzes each transaction using machine-learning based automation to uncover and block unwanted activity in real time. For additional protection against common application-layer vulnerabilities, you can deploy AWS WAF on CloudFront to enhance your security posture.

Implementation is simple. Deploy Cequence as a SaaS solution directly from the AWS Marketplace and redirect your traffic to a Cequence SaaS tenant through a simple DNS change via Amazon Route 53 to CloudFront. In as little as 30 minutes, you can begin preventing attacks via traffic redirect from CloudFront to the Cequence SaaS.

API Edge Protection

Cequence API Edge Protection is a managed services offering that augments your Cequence deployment with web application firewall (WAF) configuration and optimization, distributed denial of service (DDoS) protection, and transport layer security (TLS) certificate provisioning. Cequence Managed Services extend your team with additional API security expertise, enabling them to scale to meet the security challenges faced on a daily basis.



Use Cases

Cequence works with any business vertical. Here are some examples of real-world scenarios.

Financial Services

With strict compliance and governance laws surrounding the financial services industry, it's imperative for organizations to protect customer data, and find and quickly remediate data exposure errors before they cause violations. Cequence Security performs continuous risk analysis on all of your API endpoints, identifies endpoints that are transmitting sensitive data, and finds data leaks that defy PCI, PHI, GDPR, or other PII compliance mandates. API Sentinel even alerts you when APIs pass credit card information, social security numbers, or data patterns that you customize.

Retail

Online retailers are subject to a variety of shopping bots and business logic abuses including scraping and account takeover. These issues can lead to inflated costs, site outages, and a loss in sales revenue. By implementing Cequence, retailers can protect their apps and avoid persistent problems. Cequence's patented ML-based analysis eliminates the development, page load time, and forced mobile upgrade penalties introduced by JavaScript and mobile SDK integration efforts. This streamlined deployment makes it easy on security teams with limited resources or potential knowledge gaps.

Case Study: Ulta Beauty

Challenges

Ulta Beauty suffered from high-volume API scraping attacks that could inform criminal activity via mapping out desirable inventory at physical stores for in-person burglary. Massive quantities of malicious third-party API transactions – spiking at 700 times normal volumes – generated real cloud and bandwidth costs for Ulta. The attacks were executed over a third-party local-inventory search API, and high-quality, residential proxy IP addresses were used to make IP blocking at the edge difficult.

Solution

Ulta Beauty partnered with Cequence to identify the attack vector and put policies in place to block the malicious requests. The Cequence platform provided visibility into the API traffic and supports both out-of-the-box policies as well as customized policies such as those needed in this situation. The policies enabled the Cequence platform to block malicious API requests while allowing legitimate traffic without disrupting business.

Results

The Cequence Unified API Protection platform enabled Ulta Beauty to block tens of millions of malicious requests that resulted in savings of over $80,000 in infrastructure costs and loss prevention during the period. Additionally, the mitigation solved the problem for the local-inventory search partner. The rapid and complete resolution was made possible by the Cequence platform's highly accurate attack detection and built-in mitigation and blocking capabilities.

"Through the Cequence UAP solution and managed services, our security team was able to achieve an application security defense-in-depth approach that provided comprehensive security to defend our entire application portfolio."

Diane Brown

VP, IT Risk Management, CISO, Ulta Beauty

About Cequence Security

Cequence Security specializes in API security and bot management, delivering Unified API Protection (UAP) uniting discovery, compliance, and protection across all internal and external APIs to defend against attacks, targeted abuse, and fraud. Cequence solutions scale to handle the most demanding Fortune and Global 2000 organizations, securing more than 8 billion daily API calls and protecting more than 3 billion user accounts.