

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

Modern Application and API Protection

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 protects application performance and security.



DISCOVER

Continuous discovery and inventory of internal, external, and third-party APIs, cloud hosting providers, API gateways, and infrastructure. Complete visibility into what APIs you have, where they are, and their accessibility.



COMPLY

Comprehensive view of your API attack surface and the risk it represents. Test APIs for conformance to specification. Ensure APIs comply with internal governance as well as external regulatory requirements such as PCI DSS, GDPR, and DORA.



PROTECT

Protects applications and APIs from business logic abuse and fraud by detecting automated threats and attacks and natively mitigating through blocking, rate limiting, header injection, or deceptive responses.

AWS and Cequence Unified API Protection

Cequence can be deployed on AWS and offers a managed WAAP solution as well as a SaaS deployment of the full Cequence bot management and API security platform:

Cequence Managed Web Application and API Protection

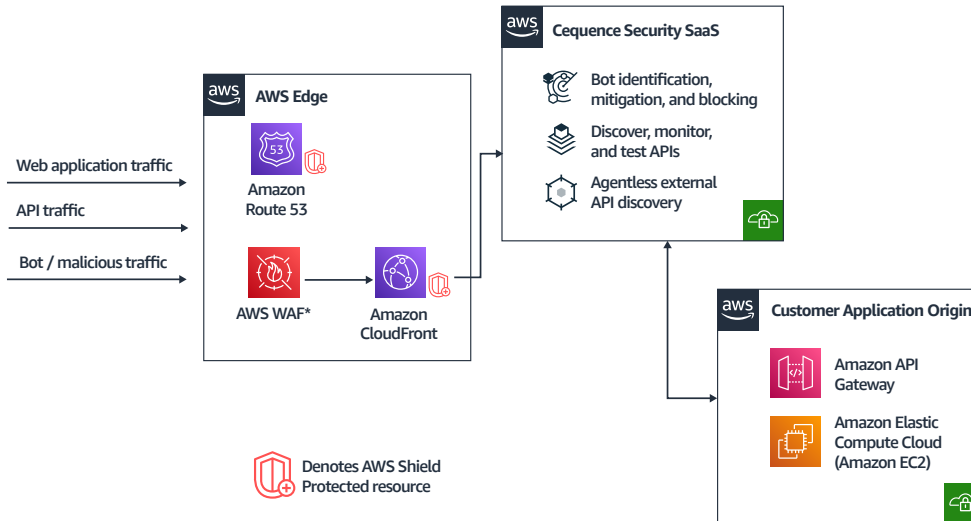
A managed Web Application and API Protection (WAAP) solution that combines the discovery, compliance posture management, bot management, and threat protection capabilities of Cequence with the WAF and DDoS protection capabilities of AWS WAF to protect against modern threats and bot attacks.

Cequence Unified API Protection platform

Offers superior API security and bot management to secure and defend your mission-critical applications and APIs. Discover all internal, external, and third-party APIs and flag risks for remediation. Ensure APIs comply with internal governance and external regulatory requirements. Detect sophisticated threats and natively mitigate in real time to prevent data loss, theft, and fraud.

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.

Onboard Your Applications and APIs in Minutes with Amazon CloudFront and Cequence Security SaaS



*AWS WAF can be deployed at the AWS Edge or in the Cequence SaaS tenant and can be centrally managed through the Cequence dashboard.

Expertise for Your Business

Cequence works with all business verticals; two example use cases follow.

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 a risk analysis on all API endpoints, identifies endpoints that are transmitting sensitive data, and finds data leaks that defy PCI, PHI, GDPR, or other PII compliance mandates. Cequence even alerts you when APIs pass credit card information, social security numbers, or other sensitive data patterns that you customize.

Retail

Online retailers are subject to a variety of shopping bots, inventory scraping and account takeover attacks. These issues can lead to inflated costs, site outages, skewed marketing and sales metrics, and revenue loss. Cequence's patented ML-based behavioral analysis eliminates the development, page load time, and forced mobile upgrade penalties introduced by JavaScript and mobile SDK integration efforts. This streamlined deployment enables swift deployment, broad app and API coverage, and a frictionless customer experience.

Frequently Handled Use Cases



Account takeover (ATO)



Flash sales & product scalping



API discovery & inventory



Sensitive data detection, masking, & exposure prevention



Content scraping



Business logic abuse



API risk identification and classification



Meet audit requirements

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 is a pioneer in API security and bot management, protecting the applications and APIs that organizations depend on from attacks, business logic abuse, and fraud. Our unique Unified API Protection platform unites discovery, compliance, and protection capabilities, providing unmatched real-time security in the face of sophisticated threats. 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 needs of the largest and most demanding private and public sector organizations, protecting more than 10 billion daily API interactions and 4 billion user accounts. To learn more, visit www.cequence.ai.



- AWS Security Competency
- AWS Retail Competency
- AWS WAF Ready
- AWS CloudFront Ready
- AWS Marketplace Seller