SOLUTION BRIEF

Cequence Security and AWS: Protecting APIs and Web Applications from Bot Attacks and API abuse

Runtime API discovery, risk assessment, and enhanced protection

Protect against bots and defend your APIs at the edge

Organizations have accelerated cloud adoption to improve engagement with their customers and suppliers and optimize operational efficiency. Although these digital transformation projects can improve customer satisfaction, the increased use of application programming interfaces (APIs) can also make way for new types of pervasive automated attacks, business logic abuse and bot traffic that target these APIs.

As a result, API security is a key initiative for organizations in multiple sectors, including retail, financial services, and travel and hospitality. Together, Amazon Web Services (AWS) and AWS Partner Cequence Security have partnered to deliver customers a robust solution that helps improve application performance and security. Amazon CloudFront provides customers a global content delivery network (CDN) that increases application availability, reduces latency, and integrates with AWS WAF and AWS Shield to improve security. This can be paired with Cequence Security's API Security Platform to help customers thwart attacks and further improve API and web application security.

Detecting fraud in a changing landscape

APIs have existed for years, typically behind a firewall or deep in the infrastructure, unexposed to the public. After moving to the cloud, organizations may not fully understand their API footprint, the associated risk of exposure, or what tools can help them mitigate risks.

As APIs become widely used and public facing, so has the rise of pervasive bot traffic and vulnerabilities to abuse them. These unwanted automated attacks are becoming more sophisticated and can appear to be legitimate transactions. This can make it difficult for security teams trying to protect their APIs at the edge and operations teams working to keep their sites running smoothly when being attacked. With this changing landscape, it is more important than ever before to know the answers to the following questions in order to protect and grow your business:

1. How many API endpoints do you have? Where are they?
2. Are bad actors targeting your APIs to disrupt your business?
3. Can you prevent abuse on your APIs natively, in real-time?

In collaboration with

CEQUENCE SECURITY

Key benefits of using CloudFront and Cequence API Security Platform

Improve productivity and site performance with ML-based automation that prevents attacks by redirecting and blocking unwanted activity in real time

Increase customer confidence and maintain brand integrity by protecting sensitive information leaking through APIs

Reduce infrastructure costs by avoiding volumetric attacks that require applications to be scaled up

Comprehensive API security

A comprehensive API security solution requires more than just visibility and management. It should also provide inventory tracking, risk analysis and remediation, and real-time threat mitigation without relying on third parties.

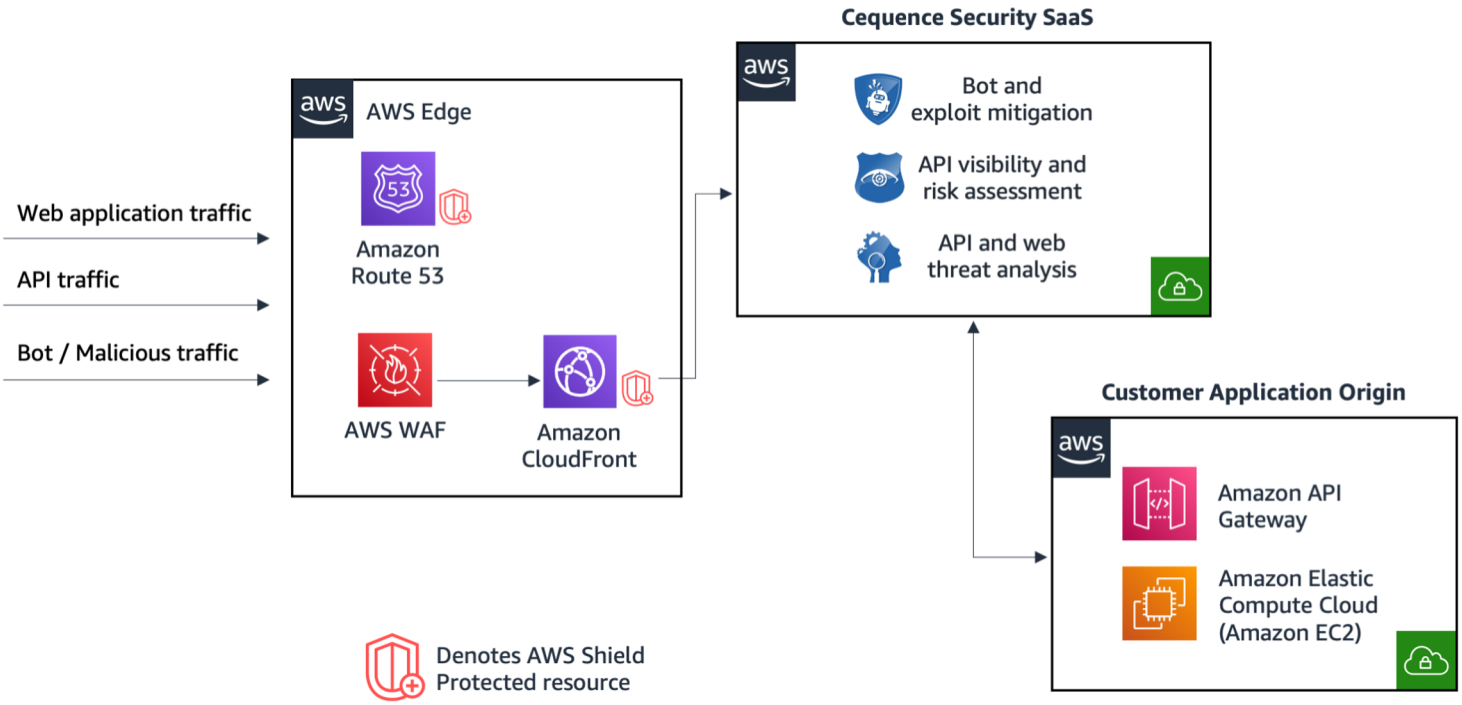
Using Amazon CloudFront as your CDN helps you accelerate static, dynamic, and API traffic with high-performance and built-in security functionality such as AWS Shield, Compliance Standards, and Identity and Access Management. Deployed with CloudFront, Cequence detects your public-facing applications 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 AWS Marketplace and redirect your traffic to a Cequence SaaS tenant via 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.

Resources to help you get started

- Get started with CloudFront
- Get started with AWS WAF
- Cequence CloudFront integration documentation
- API Sentinel on AWS

Onboard your applications and APIs in minutes with Amazon CloudFront and Cequence Security SaaS



Cequence and AWS: protecting businesses and their customers

For any organization with customer facing applications, preventing and defending your APIs from automated attacks and business logic abuse is critical. By running its security platform on AWS, Cequence can scale their solution to meet the growing automated API threat landscape. Here are three industry-specific examples to illustrate how Cequence Security and AWS work together to mitigate potential threats.

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 achieves this by doing continuous risk analysis on all of your API endpoints. From there, API Sentinel identifies all 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 account scraping. These issues can lead to inflated costs, site outages, skewed sales analytics, and a loss in sales revenue or poor branding optics from frustrated customers. By redirecting traffic to the Bot Defense SaaS instance, retailers can protect their apps quickly and avoid persistent problems. The patented ML-based analysis performed by Cequence Artificial Intelligence (CQAI) 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.

Travel and Hospitality

Travel and hospitality businesses are also at risk. When airlines and hotels run special discounts on room rates or ticket prices, bots can quickly buy or book these at the lower price and resell for a markup on competing or third-party websites. As a result, customers are not able to take advantage of these promotions or low fares because of the bots' unfair edge, and companies must scale applications up in order to handle the influx of fraudulent traffic, leading to further operational expenses. Cequence helps prevent these attacks with a similar approach described above. Bot traffic is blocked by the Bot Defense SaaS instance, leaving you with an accurate picture of online sales and/or bookings.

Better together: automated API Security with Cequence and AWS

While the use of APIs continues to grow, so does the risk of exposure, making the need for a comprehensive security posture more important than ever. Protect your applications and APIs by preventing fraud and data loss caused by API coding errors, unwanted automated attacks, and other vulnerabilities. Together, Cequence Security and AWS offer better performance, rapid deployment, and higher efficacy to protect your APIs at the edge.

Try Cequence Security Bot Defense SaaS free for 30 days. Visit **AWS Marketplace**.

Learn more about **Amazon CloudFront**, **AWS WAF**, or **AWS Shield**.

Learn about **Cequence Security** and get a FREE API Security Assessment.

About Cequence Security, Inc.

The Cequence API Security Platform unifies runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to consistently detect and protect against ever evolving online attacks without the development and deployment friction associated with alternative offerings.

aws Qualified Software