TRACEABLE_

PARTNER SOLUTION BRIEF

Traceable AI + Amazon CloudFront and Lambda@Edge Services

Easily Scale Security and Performance Across Modern Application Architectures with Amazon CloudFront and Traceable AI

In today's API-driven digital economy, ensuring secure delivery of web applications and APIs (Application Programming Interfaces) is more critical than ever. Cloud technologies and APIs are foundational to modern application development, but have increasingly been targeted by cyberattacks. To protect these vital components, robust security measures are essential. This overview explores how AWS services—CloudFront and Lambda@Edge—work in conjunction with Traceable AI to deliver comprehensive protection against threats targeting APIs and web applications.

Amazon CloudFront - Defense for Cloud Applications

Amazon CloudFront is Amazon's globally distributed content delivery network (CDN) service, designed to deliver applications, APIs, and content with low latency and high transfer speeds. It caches content at edge locations around the world, allowing end-users to access data quickly, regardless of their location. CloudFront is integral to modern web application performance, accelerating everything from static website delivery to real-time streaming, and integrating seamlessly with other Amazon Web Services (AWS).

Key Security Use Cases

Amazon CloudFront

- Global Scalability
- Performance Optimization
- Edge Security Protection

Traceable API Security Platform

- API Discovery
- Threat Detection
- Attack Protection
- Fraud and Bot Prevention
- API Security Testing
- Gen AI API Security

AWS Lambda@Edge Services

Lambda@Edge, a feature of Amazon CloudFront, allows developers to run serverless functions at AWS edge locations. It enables real-time execution of code in response to CloudFront events, improving application performance and reducing latency. Developers can manipulate content, apply custom security rules, or perform real-time analytics directly at the edge—without managing infrastructure or provisioning servers.

Traceable API Security Platform - Comprehensive API Security From Code to Cloud

Traceable's, API security platform specializing in API security, focuses on protecting APIs and microservices across complex environments. Traceable uses distributed tracing and machine learning to monitor APIs, detect malicious traffic, and prevent breaches by analyzing how data flows through APIs. It offers deep visibility into API behavior, helping businesses secure their applications against sophisticated threats like OWASP API Top 10, API abuse, data leaks, and zero-day attacks.

How Traceable and Amazon CloudFront Protect Enterprise Web Applications and APIs

Cybercriminals are increasingly targeting APIs, exploiting their interconnections to access sensitive data or execute sophisticated attacks. According to the 2023 State of API Security Report, 61% of organizations expect API-related risks to increase. By integrating Amazon CloudFront, Lambda@Edge, and Traceable AI, businesses gain a robust multi-layered security solution.

Advanced API Security and Threat Detection: CloudFront serves as the first defense, managing incoming traffic through its distributed architecture. Lambda@Edge intercepts requests, applying security rules and filtering malicious traffic before it reaches the origin. Traceable AI adds a layer of protection by continuously monitoring API traffic for anomalies, adapting to evolving threats. This combined approach mitigates risks from API-based attacks like DDoS, account takeovers, and credential stuffing.

Gartner Peer Insights.

"

Traceable has the comprehensive solution for protecting all API endpoints in all deployment models - very customizable and easy to operate.

Pathik Patel,
Head of Cloud Sercurity,
Informatica

Gartner Peer Insights.

"

It's a single control center allowing superior monitoring and tracking of all API traffic.

Sr. Security Engineer,
Large Financial Organization

CloudFront's caching capabilities reduce the load on APIs, ensuring only necessary requests reach the backend. Lambda@Edge can authenticate requests or apply rate-limiting rules at the edge, while Traceable provides continuous learning and threat prevention by monitoring API traffic patterns.

Custom Content Filtering and Authorization: CloudFront and Lambda@Edge enable the enforcement of custom security rules. For instance, streaming services can restrict access based on geographical locations using Lambda@Edge to assess and block or redirect requests dynamically. Traceable AI adds visibility into user interactions with APIs, detecting unauthorized access attempts and blocking suspicious activity based on real-time analysis.

For sensitive applications like banking or healthcare, Lambda@Edge can perform user authentication at the edge, while Traceable ensures that API endpoints are protected from unauthorized access and data breaches, securing sensitive information.

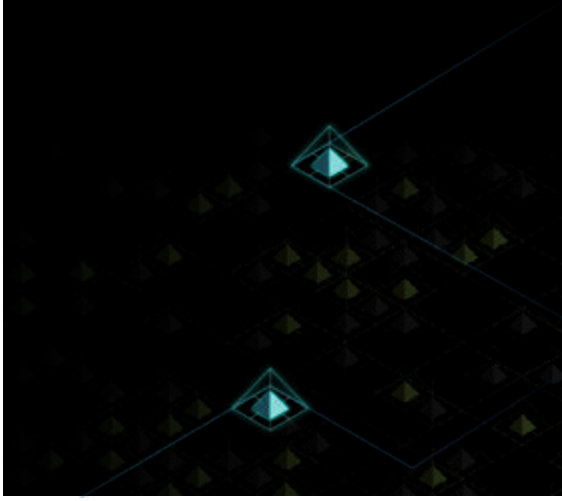
DDoS Protection and Bot Mitigation: DDoS and bot attacks threaten application availability. AWS CloudFront, with AWS Shield, provides built-in DDoS protection by absorbing malicious traffic at the edge. Lambda@Edge further enhances protection by blocking suspicious IP addresses and throttling traffic. Traceable AI adds AI-driven behavioral analysis, identifying and mitigating slow, sophisticated DDoS attacks targeting APIs.

While CloudFront and Lambda@Edge handle infrastructure security, Traceable focuses on traffic patterns, detecting automated attacks that might evade traditional DDoS protection mechanisms. This layered approach ensures comprehensive defense against both volumetric and slow-drip DDoS attacks.

Amazon CloudFront, Lambda@Edge, and Traceable AI offer a multi-layered defense for web applications and APIs. CloudFront accelerates content delivery while Lambda@Edge enables real-time security at the edge. Traceable AI provides deep, continuous insights into API traffic, protecting against evolving threats. This integrated approach allows businesses to innovate with confidence, knowing their applications are secure and performant.

Traceable API Security Platform is Built for Enterprise Scale

- Over 500 billion API calls protected per month
- More than 50,000 critical vulnerabilities found each week
- Over 200,000 API attacks detected and blocked each month



Learn More or Request a Demo

For more information on Traceable AI, visit www.traceable.ai or visit us on the AWS marketplace.

TRACEABLE

About Traceable

Traceable is the industry's leading API security company helping organizations achieve API protection in a cloud-first, API-driven world. Traceable is the only contextually-informed solution that powers complete API security – API discovery and posture management, API security testing, attack detection and threat hunting, and attack protection anywhere your APIs live. Traceable enables organizations to minimize risk and maximize the value that APIs bring to their customers. To learn more about how API security can help your business, visit https://www.traceable.ai/.

www.traceable.ai