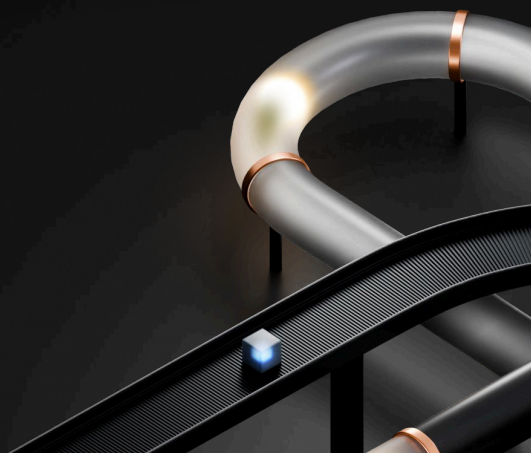
TRACEABLE by harness

Traceable API Protection

Purpose-built security to detect and stop API threats, business logic abuse, and sensitive data exposure



Why It Matters?

Signature-based detection is ineffective against today's API threats. Attacks like business logic abuse do not involve obvious exploits. They use valid requests to perform unauthorized actions by manipulating how the API is intended to work.

Take Broken Object Level Authorization (BOLA), for example. An authenticated user changes an object ID in an API call to access another user's data. There is no malicious payload, just misuse of expected behavior. Traditional tools cannot tell the difference.

Protecting against these threats requires a deep understanding of API behavior in real time.
Traceable API Protection analyzes live traffic, learns typical usage patterns, and detects deviations that signal abuse. It enables precise enforcement against OWASP API Top 10 threats like BOLA, excessive data exposure, and function-level access flaws.

What Traceable Delivers

Traceable provides real-time API threat detection, behavioral analytics, and risk-based enforcement in a single platform. It understands how APIs behave in context, helping security teams stop abuse, enforce governance, and reduce operational noise.

Highlights

Detects advanced API threats, including business logic abuse and access misuse.

Profiles all API traffic to understand normal behavior and surface anomalies

Identifies sensitive data exposure and maps data flows across services

Supports CI/CD and DevSecOps workflows for continuous security coverage

Scores API risk contextually and enforces policy based on real-time conditions

TRACEABLE by harness

Key Capabilities

Runtime Threat Detection
Continuously monitors API traffic to detect advanced threats like business logic abuse, excessive data exposure, and access misuse using behavioral and contextual analysis.

Sensitive Data Protection
Tracks how sensitive data such as PII or payment info moves through APIs. Highlights potential exposure and helps enforce data protection policies.

DevSecOps Integration
Connects with CI/CD pipelines and infrastructure-as-code tools to embed API security into development workflows without slowing releases.

Behavioral Baselines and Anomaly Detection
Learns typical API behavior across users, services, and endpoints. Flags deviations that indicate abuse or misuse, even when requests appear valid.

User Attribution and API Flow Sequencing
Connects API activity to individual users and sessions, enabling deeper investigation and detection of misuse. Tracks API call sequences to identify abnormal patterns and business logic attacks that unfold over multiple steps.

Contextual Risk Scoring and Enforcement
Evaluates APIs based on usage, sensitivity, and access patterns. Applies real-time enforcement aligned to risk levels, including blocking and alerting.

Deployment Options

Edge Deployment
Configure DNS or CDN based traffic steering to route requests through Traceable's fully managed cloud platform. This deployment requires no installation of agents and delivers immediate protection at the edge.

Inline Agents
Deploy lightweight agents within your infrastructure, at the web server, API gateway, or application level (for example, NGINX, Apigee, or language-based instrumentation). Provides real-time threat detection and policy enforcement at the source.

Out-of-Band
Mirror traffic from gateways, load balancers, or eBPF to passively collect API and application traffic. Detection is handled asynchronously, with enforcement actions triggered through out of the box integrations with third party WAFs, SIEMs, or SOAR platforms.

TRACEABLE by harness

Use Cases / Threats Addressed

Traceable API Protection solves key API security challenges:

Authentication and Authorization Attacks
Detects and blocks abuse of authentication or access control logic, including unauthorized access to objects, functions, or workflows.

Excessive Data Exposure
Prevents extraction of sensitive data via legitimate API calls, pagination abuse, or overly permissive responses.

Business Logic Abuse
Identifies misuse of expected API behavior, such as bypassing rate limits, manipulating workflows, or triggering unintended outcomes.

Server-Side Request Forgery (SSRF)
Flags attempts to exploit APIs as proxies to access internal services or restricted systems.

Injection and API Misconfiguration
Protects against injection flaws and exposed endpoints caused by weak configurations or insufficient validation.

Business Benefits

Traceable API Protection helps security teams stay ahead of evolving API threats while preserving developer speed and maintaining governance. It delivers accurate detection, clear visibility, and protection that fits naturally into modern software delivery.

Key benefits

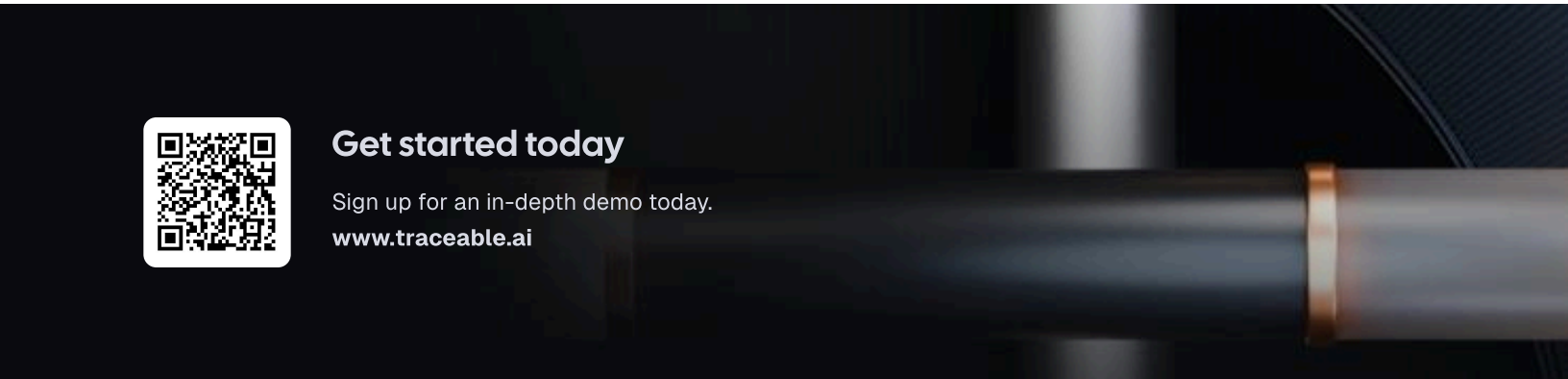
Real-Time Protection Against API Threats
Detects and blocks business logic abuse, access misuse, and data exposure as it happens.

Context-Aware Detection with Low False Positives
Uses behavioral analysis and traffic baselines to reduce alert noise and improve accuracy.

Operational Visibility and Risk Insights
Maps sensitive data flows, highlights high-risk APIs, and tracks activity across environments.

Built for Developer Workflows
Integrates with CI/CD and infrastructure-as-code tools to support DevSecOps without slowing teams down.

Support for Compliance and Governance
Helps meet PCI DSS, HIPAA, and GDPR requirements through policy enforcement and data tracking.



Get started today

Sign up for an in-depth demo today.
www.traceable.ai