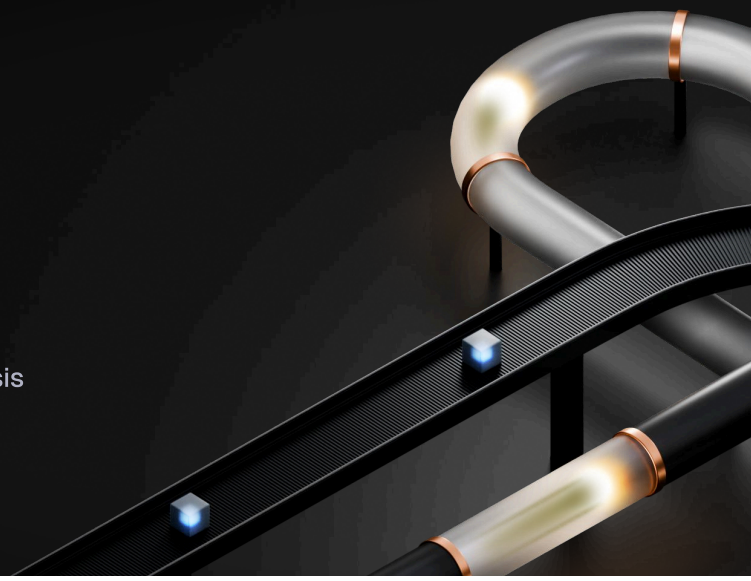
TRACEABLE by harness

Traceable Bot Protection

Adaptive detection engine that uses user behavioral analysis across sessions to proactively stop malicious automation targeting your key business flows.



Why It Matters?

In today's digital economy, distinguishing between a bot and a human is no longer enough to protect your business or your revenue. The landscape has evolved beyond simple, malicious bots; we are entering an era of beneficial automation where customers will use personal AI assistants to interact and transact online. Legacy bot protection systems that reflexively block all automation will soon start turning away your best customers, mistaking their helpful AI agents for threats.

These traditional defenses fail because they cannot discern the critical difference between malicious intent, like inventory hoarding or credential stuffing, and desirable automation, like an AI assistant making a legitimate purchase. Modern protection must therefore analyze the intent behind the traffic. By doing so, you can seamlessly welcome advantageous automation that drives business while definitively stopping the sophisticated threats that target your revenue and data.

What Traceable Delivers

Traceable Bot Protection provides real-time bot detection powered by behavioral intent analysis, and automated mitigation in a single platform. It understands the intent behind your traffic—distinguishing human users from malicious and even beneficial bots. This helps security teams stop business logic abuse, prevent account takeover, and safeguard the digital user experience.

Highlights

Intent detection to accurately differentiate between bad bots, humans, and helpful AI agents.

AI-powered attacker fingerprinting combined with automated actioning for continuous protection against bots.

A spectrum of automated responses, from advanced invisible challenges and CAPTCHAs to foundational controls like rate limiting and blocking.

Simple setup and integrates smoothly with your existing security tools, CI/CD pipelines, and operational workflows.

TRACEABLE by harness

Key Capabilities

Behavior-Driven Bot Detection
By mapping user journeys through your APIs, we analyze collective behavior to discern the intent behind every action—differentiating legitimate users from malicious bots and helpful AI agents.

Attacker Fingerprinting
We fingerprint attackers using API telemetry and HTTP payloads, creating a persistent identity that tracks them even when they alter their JavaScript signatures to evade detection.

Low & Slow Abuse Detection
Our patent-pending API Sequence analysis detects sophisticated, low-and-slow abuse, identifying malicious traffic that would otherwise fly under the radar.

Automated Mitigation
By leveraging attacker fingerprints, our automated mitigations—from invisible challenges to outright blocking—provide continuous protection for your platform.

Rich Analytics
Our rich dashboards help you analyze attacks, identify persistent threats, and connect attackers to their methods and compromised accounts. Take immediate action with one click in the dashboard or stream alerts in real-time to your preferred security tools.

DevSecOps Integration
Connects with CI/CD pipelines and infrastructure-as-code tools to embed bot protection into development workflows.

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

Key Use Cases

AI Crawling Protection
Protects against excessive crawling of known AI bots, thereby saving compute resources.

Payment Fraud Prevention
Protects against bots that test stolen credit card numbers and exploit payment systems.

Account Takeover Prevention
Prevents bots from using stolen credentials to compromise user accounts and commit fraud.

Content and Price Scraping Defense
Stops bots from stealing proprietary content, pricing data, and other intellectual property.

Inventory Hoarding Mitigation
Prevents bots from making products and services unavailable to legitimate customers by holding them in carts.

OWASP Automated Threat Protection
Protects against the full range of automated threats to web applications, including credential stuffing and carding.

Business Benefits

Preserve Customer Trust
Safeguard your customers from account takeover and fraud to maintain their confidence in your brand.

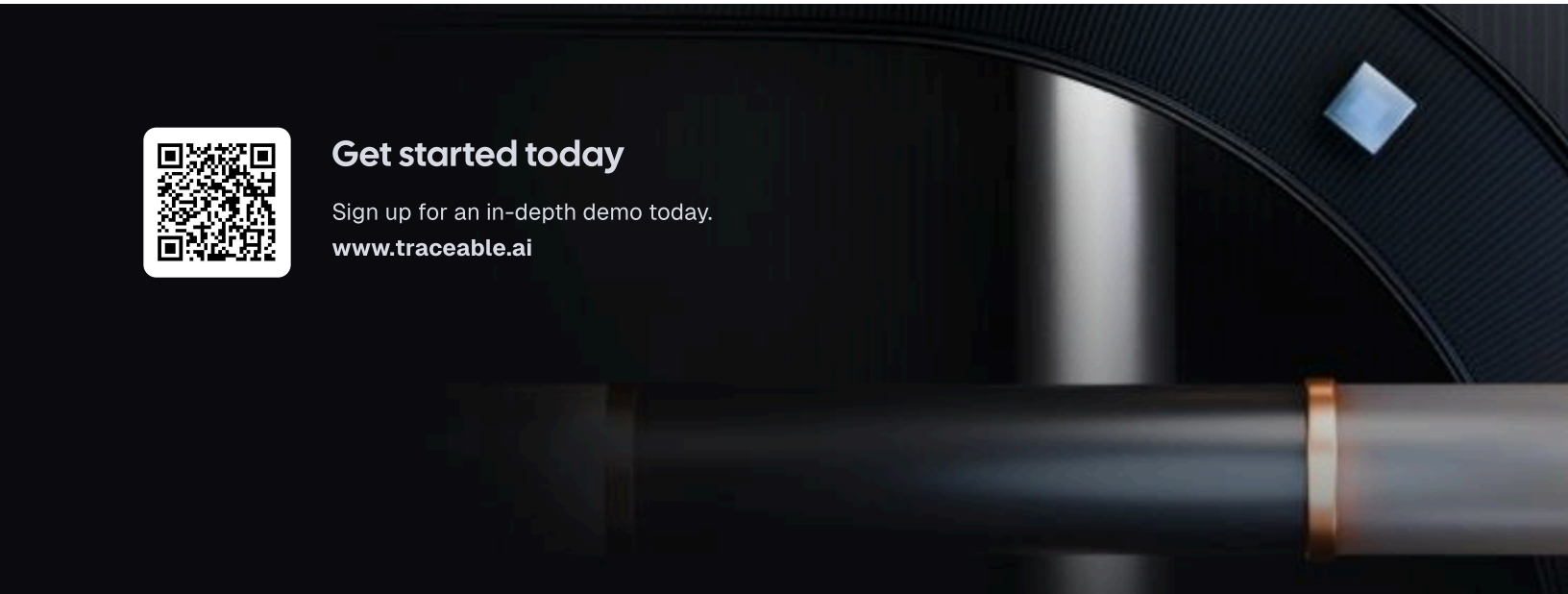
Optimize User Experience
Accurately mitigate malicious bot traffic at the edge without subjecting legitimate users to intrusive and frustrating challenges.

Lower Operational Overhead
Reduce infrastructure costs by blocking unwanted bot traffic that consumes bandwidth and server resources.

Improve Business Analytics
Ensure your marketing and business data is accurate by preventing bots from skewing user behavior analytics.

Protect Digital Assets
Prevent content scraping to protect your brand's unique intellectual property.

Outsmart Evolving Threats
Stay ahead of attackers with continuously updated threat intelligence and adaptive AI that learns from new attack patterns.



Get started today

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