TRACEABLE

DATASHEET

Traceable Bot Defense

Unwanted Bad bots are bad news, but separating bad bots from good bots and real users is HARD. Traceable takes a unique approach combining traditional detection techniques and advanced behavioral analysis to deliver fast, accurate, and appropriate bot defense.

The internet is rife with bots – and while some are welcome, most represent anything from an annoyance to a real threat. Bots are used to scrape information, manipulate application behavior, or drive services off-line. Bots are the foot soldiers of fraudsters and hackers, so managing bot traffic is important for your security posture.

Wide Context for Advanced Detection

A holistic view of app and API activity combined with critical indicators from client evaluation delivers massive context, enabling Traceable's patented detection system to more accurately detect bots . Traceable's OmniTrace Engine keeps session data your applications and APIs longer, helping spot anomalies and tracking behavior to account level.

Spot Bots with Bad Intent Post-Login using Full Session Tracing

Give yourself another weapon in the arms-race of bots pretending to be humans. Where client-side detection might not reveal the full truth, spotting anomalous behavior can give you the edge in blocking fraud or misuse attempts. Traceable captures every request and response – including API traffic to build a comprehensive model of normal behavior.

Solution Benefits

Accurate Bot Identification

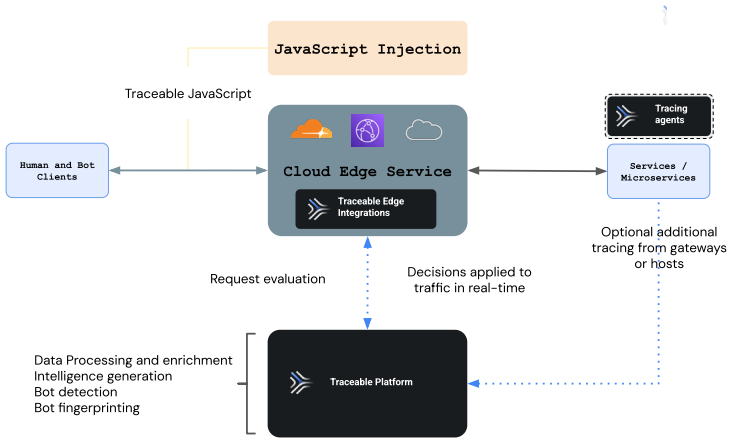
Advanced behavioral analysis deep combined with powerful client-side detection gives Traceable 's machine learning engine a wide context – powering accurate categorization

Identify Compromised Accounts

Use Traceable to track bot-created or compromised accounts. Traceable correlates attack and victim data to remove or remediate problem accounts

The Traceable Solution

Traceable bot defense integrates with popular cloud edge services and tag management solutions to gain a comprehensive picture of client status and session behavior. This data is fed into the powerful data lake at the heart of the traceable platform where it is enriched and analyzed by machine learning algorithms that are continuously learning from existing traffic. Activity can be correlated down to the account level to spot anomalous behavior that might indicate a compromised account, and when malicious activity, a custom fingerprint is created, enabling further bot instances to be identified and managed quickly.



Solution Benefits

Automatic Fingerprinting for Zero-Day defense

Once the Traceable platform has identified malicious bot activity, a bot fingerprint is automatically generated, enabling rapid response and control of new-bot instances .

Flexible Response Options

When a bot is identified, choose to block, allow, insert a Captcha, rate limit, or add custom headers for further correlation.

Flexible Detection and Response

In conjunction with automated bot detection, customers can define specific activity flows requiring custom policies tailored to their business needs. Policies can be chained together into workflows to provide more fine grained risk scoring.

Traceable Bot Defense offers flexible responses to detected bot activity, including blocking traffic, rate-limiting, challenge insertion, or header injection for upstream management.

TRACEABLE

Features at a Glance

Comprehensive Bot Defense	**Automated Bot Detection:** Detect volumetric attacks, browser or device anomalies, mouse replays, API access anomalies and more. **Custom Policies:** build business-specific detection rules and actions. **Workflow Builder:** Chain multiple policies and actions into a comprehensive detection and response configuration **Selectable Actions:** choose the correct response for the attack, rate-limit, block, challenge, or header insertion options for maximum flexibility.
Account Journey Tracking	**Track accounts involved in attacks:** including business-specific risk indicators, identify compromised accounts and bot-created accounts. **Custom Entity Attribution:** Define the entities that describe account IDs or other important attributes to use in detection rules or analysis. Use specific values to indicate higher risk activities such as financial transaction amounts.
Business Impact Analysis	**Define KPIs that matter:** track them against attacks to evaluate the business impact of bot activity.
Rich Reporting and Deep Insights	**Comprehensive dashboards and reports:** fast indications of attacks and responses, victim identification combined with flexible alerts via email, slack, web hooks, and multiple integrations with SEIM/SOAR solutions. **Traceable data lake:** Attack data is stored in a data lake and accessible by a flexible query engine with powerful visualization capabilities.

Find out More

Visit the Traceable website discover Traceable's API Security and Bot protection platform.

www.traceable.ai/bot-defense

About Traceable

Traceable is the industry's leading API Security company helping organizations achieve API visibility and attack protection in a cloud-first, API-driven world. Traceable is the only intelligent and context-aware solution that powers complete API security – API discovery and posture management, API security testing, attack detection and protection, anywhere your APIs live. Traceable enables organizations to minimize risk and maximize the value that APIs bring their customers.

Learn more at www.traceabe.ai