TRACEABLE_

SOLUTIONS BRIEF

API Abuse Protection:

An Overview of Traceable's Approach to Today's Most Common Attack Vector

APIs serve as vital conduits for the flow of data between software applications, enabling the digital services we rely on daily. Yet, with the pervasive use of APIs, there is an escalating risk of API abuse, posing significant cybersecurity threats.

According to Gartner:

- By 2022, API abuses will move from an infrequent to the most frequent attack vector, resulting in data breaches for enterprise web applications.
- By 2024, API abuses and related data breaches will nearly double.

This solutions brief provides a comprehensive overview of the API abuse problem and discusses Traceable's approach that addresses these challenges.

The Problem of API Abuse

The methods of API abuse can range from simple yet destructive brute force attacks, where an attacker repeatedly attempts to guess valid credentials, to more sophisticated injection attacks and man-in-the-middle strategies. Data breaches frequently occur when attackers exploit weaknesses in API security, often leading to unauthorized access to confidential data. On the other hand, Denial of Service (DoS) attacks are designed to overwhelm an API with requests, causing it to become slow or unresponsive.

The complexity of APIs and the rapid pace of digital innovation makes safeguarding APIs from abuse a challenging task. As organizations continually develop and deploy new APIs to support new services, the task of ensuring their security becomes increasingly complex.

Each new API represents a potential point of vulnerability that must be identified and protected. To make matters more difficult, traditional security measures often fall short, unable to effectively deal with the dynamic nature of API threats.

The nature of these challenges makes it clear that protecting APIs from abuse requires an evolved, intelligent, and behavioral approach.

SOLUTION HIGHLIGHTS

- **Built-in BOT Classification** based on API access behavior and threat intel.
- **BOT, TOR, Proxy Correlation in all Protection Modules**: Require API keys, OAuth, or other secure methods for access control.
- **Protection Against API Entry Point Attacks:** Credential Stuffing, Account Takeover, Fake Account Creation, and more.
- **Auto Detections Complemented with Custom Policies**: Rate Limiting, Data Access Policies, Enumeration, and more.
- **Server Side Protection:** No need for JavaScript, browser extensions or SDK integrations.
- **Block Users Inline or with Out-of-Band Integrations:** Block based on IP, custom signatures, tokens; block inline or out of band with WAF, NGFW, API Integrations.

Traceable's Approach

API abuse poses a covert, serious threat. Traceable protects against these risks with 360-degree context gathering and machine learning-powered behavioral analytics. Our solution detects even the most nuanced, low and slow attacks.

Augmented by strict rate limiting and granular blocking capabilities, we provide a robust barrier against API abuse, offering an impenetrable defense for your digital ecosystem.

Bot Detection and Bot Protection

As API usage continues to grow, so does the prevalence of bots—both legitimate and malicious. From web scraping and content aggregation to fraudulent activities and DDoS attacks, bots can drastically impact a company's digital presence and security posture. This task is inherently complex due to the evolving sophistication of bot strategies. Advanced bots can mimic human behavior, rotate IP addresses, and utilize headless browsers to bypass traditional detection methods.

Traceable's Bot detection distinguishes bots from human users, in real-time. It extends beyond rate limiting and IP blocking, offering deep analysis of traffic patterns, detects anomalies, and differentiates between harmful bots and legitimate users.

The platform takes it further by incorporating behavior-based machine learning, fingerprinting, and challenge-response mechanisms, to enhance the resilience of APIs against malicious bot activities.

Dynamic Data Access Policies

With Traceable, you can detect and classify the data that APIs are handling, to apply proper access control policies. These policies define which users and roles can access different data types, at what times, from what geolocations and from what client types. This includes sources like bots, residential proxies, and anonymous VPNs. With dynamic data access policies, you can quickly and easily create policies with out-of-the-box templates or customize policies based on organization needs.

Identify "Interesting APIs"

APIs which are critical to the business function and can severely impact continuity when overwhelmed need to be identified upfront. In few cases, the business is aware of such APIs and their capacity – this is the easy but rare scenario.

In majority of the cases, businesses struggle to capture the "interest" metric in their APIs.

Traceable offers security analytics functionality by providing all the API endpoint traffic and merging that with information of sensitive data, authentication, source of the traffic (BOTs, Residential proxy, TOR, Anonymous VPN's etc).

"Suspicious" Users

Traceable helps in identifying such users or user groups as well as their intended target API's and sensitive data (PCI, PII, HIPAA, GDPR etc) or materially significant data they access (payment info, referral amounts, gift card numbers, etc) that are specific to the business.

Apply Policies for Rate Limiting

Traceable allows security teams to apply policies to rate limit APIs and/or users by defining known candidates or broader options in their absence, defining crucial conditions to identify the targets where rate limiting is essential for the business applications to function smoothly.

Along the same lines, Traceable allows options to define rate limits manually or with GraphQL APIs which is useful when the intended volume of the endpoints is known. Traceable also provides options to dynamically calculate the rates based on usual traffic and use that to rate-limit endpoints and/or users.

Businesses can apply these policies to detect overuse of endpoints or to even block such abusing users, source types like Bots, Residential proxies, user agents, domains etc from accessing the application.

Traceable's Approach Cont...

Credential Stuffing Protection

APIs, by design, are vulnerable to credential stuffing attacks due to their automation-friendly, stateless nature, which lacks traditional web interface protections like CAPTCHAs.

This, along with the challenges in implementing effective rate limiting due to the breadth of clients APIs serve, and their lack of a graphical user interface, makes them ripe for exploitation by cybercriminals.

Their exposed endpoints, especially for authentication, can be direct targets, bypassing standard security measures. This underscores the critical need for robust protective measures against credential stuffing in API security.

Traceable's API security platform delivers the essential contextual data that enables incident response teams to swiftly and efficiently counteract credential stuffing attacks. Our solution provides comprehensive timelines of attacker behavior, offering valuable insight into the attacker's actions and the application's response.

With Traceable, teams can bypass the manual task of correlating attack information, as our platform seamlessly automates this process, enhancing the efficiency and effectiveness of response measures.

Stop API Fraud

API fraud, a rapidly escalating cyber threat, poses a significant challenge to modern digital enterprises. Despite the critical role APIs play in enabling inter-application communication and facilitating digital innovation, they also present an attractive attack surface for cybercriminals. The inherent traits of APIs – their automation-friendly nature, stateless operation, lack of user interface, and exposed endpoints – make them susceptible to various fraud activities.

Additionally, the increasing complexity and scale of API deployments make detecting fraudulent activities and implementing effective security measures a daunting task, leading to potential data breaches, financial losses, and damage to brand reputation.

Traceable offers a comprehensive and proactive approach to API fraud protection. Through advanced Graph Machine Learning technologies, we uncover hidden threat correlations across various dimensions, providing a holistic view of potential 'fraud rings' and enhancing early threat detection and response.

Our unique user profiling technique leverages both temporal and spatial patterns from each user's API call sequences, creating a distinct 'fingerprint' for improved threat detection accuracy.

This, in conjunction with proactive anomaly detection, empowers organizations to swiftly mitigate potential threats. Traceable's API Fraud Ring Detection establishes an additional layer of data protection, identifying sudden changes in access patterns and enhancing data security.

ADDITIONAL FEATURES

- **IP Reputation Scoring:** Block or limit request patterns or usage spikes.
- **Machine Learning:** Use AI algorithms to detect and block potential abuse patterns.
- **Customizable Rules:** Allow configuration of specific rules to suit business requirements.
- **Logging and Monitoring:** Capture detailed usage logs for analysis and real-time monitoring.
- **Reporting and Alerting:** Provides comprehensive reporting and timely alerts for potential abuse incidents.

TRACEABLE

Traceable is the industry's leading API Security company that helps organizations achieve API protection in a cloud-first, API-driven world. With an API Data Lake at the core of the platform, Traceable is the only intelligent and context-aware solution that powers complete API security – security posture management, threat protection and threat management across the entire Software Development Lifecycle – enabling 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, book a demo with a security expert.

www.traceable.ai/request-a-demo