API Protection Datasheet

Automatically detect and stop known and unknown API attacks, business logic abuse attacks, as well as API abuse, fraud, and sensitive data exfiltration.

APIs pose a direct threat to systems, data, and privacy

APIs are now the largest attack vector for abuse, data loss and fraud across nearly every industry. In addition, organizations are using outdated, unreliable approaches to API security, and aren't yet including the protection of the API layer in those plans. These approaches are proving insufficient, especially given the average cost of data loss, and the number of recent API data breaches.

Consider the statistics...

- According to Gartner, API abuse is the top attack vector for 2022.
- APIs now transmit the majority of sensitive data.
- Current solutions, such as legacy WAFs and Gateways, were not built to address the unique nature of API security incidents.

Why APIs are difficult to protect

APIs are difficult to protect because API malicious traffic often looks normal to security tools like a web application firewall (WAF). The Venmo and Coinbase API attacks are good examples of this. For Venmo, one of their public endpoint unsecured APIs allowed a student to scrape 200 million users' financial transactions. This looked like normal traffic to their security solution. At Coinbase, an improper API validation allowed an attacker to make unlimited cryptocurrency trades between different currency accounts. Again, this looked like perfectly normal traffic to their security solution.

With access to APIs, malicious users can:

- Obtain unauthorized access to accounts.
- Manipulate inventory availability or purchase prices.
- Exfiltrate sensitive data such as PII, PHI, social security numbers or banking information.

If API attacks are successful, these security incidents create massive financial loss, brand value erosion, as well as failures in company operations and compliance.

API Protection Highlights

- Detect and stop data exfiltration, fraudulent activities
- API bot mitigation
- Runtime exploit prevention
- Defend against attacks - OWASP web top 10, OWASP API top 10, and many others
- Business Logic Abuse Protection
- Create and track incidents

> With Traceable, we are able to detect and respond to breaches in the shortest possible time. For us, it was also important to have continuous visibility into the APIs, identify root cause, and remediate those issues.

Pathik Patel
Head of Cloud Security,
Informatica

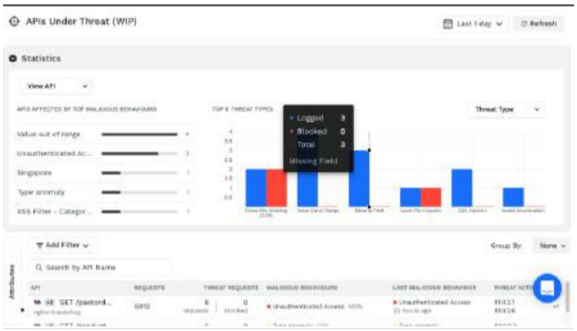
How Traceable Helps

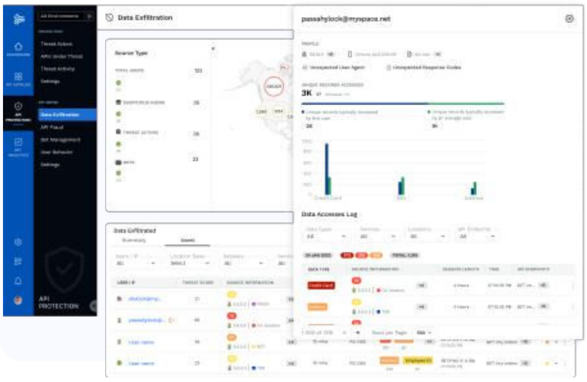
Traceable’s API Protection automatically detects and stops known and unknown API attacks, business logic abuse attacks, as well as API abuse, fraud, and sensitive data exfiltration.

01

Detect and Block API Attacks

Automatically detect and block both known and unknown API attacks and vulnerabilities, including the OWASP web and API top 10, business logic abuse attacks, and zero days.





02

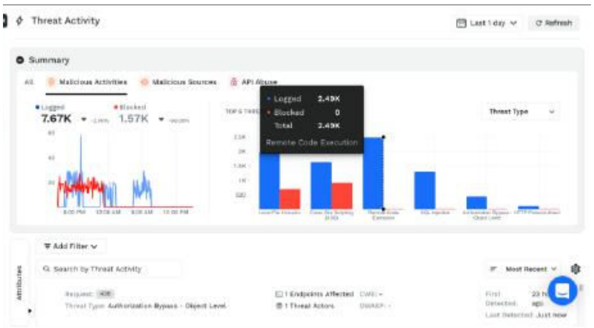
Stop Sensitive Data Exfiltration

Immediately detect where hackers gain access to sensitive data by exploiting software bugs or CVEs. Understand the flow of transactions through your application, from edge to data store and back, to quickly respond and shut down the attempted theft.

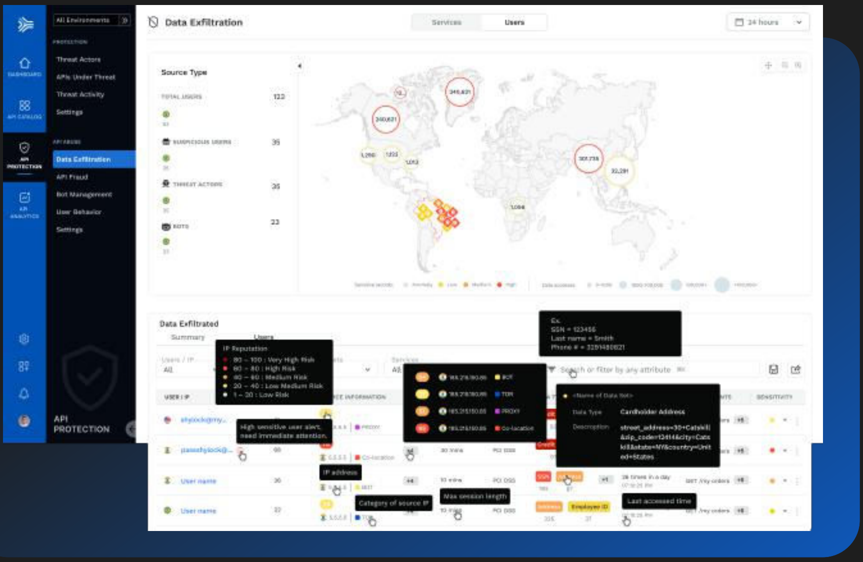
03

Eliminate API Abuse and Fraud

Traceable provides real-time detection and protection against API abuse such as gaining unsanctioned access, account takeover, and malicious bots.



Robust Capabilities for Runtime API Threat Protection



01 Sophisticated Anomaly Detection

By monitoring how your API endpoints are communicating and how your application services are behaving, we can quickly identify any abnormal behavior that could indicate a security threat and generate a security alert in real-time – whether its highly anomalous behavior or an anomalous flood of incoming API calls from a foreign API address.

.

02 Industry-Leading Machine Learning Models

With a series of sophisticated algorithms, Traceable establishes a baseline of normal API behavior, app services, and data. With high accuracy, if there is an event or behavior that is sufficiently anomalous, based on our ML models – Traceable generates a security alert in real-time giving your security team and the SOC the ability to take action on any threat event happening at runtime.

03 Run Policy-Based Detection and Blocking

Since Traceable is deployed at your API edge – i.e. within an API Gateway, a proxy, or service mesh – we give you the ability to detect and block a variety of API and web-based attacks. For instance, you can implement a rule to detect all remote code execution attacks, DDoS attempts, or any API object authorization bypass.

04 Capabilities Beyond Detection

More than just detecting, you can run Traceable in blocking mode that will prohibit any of these attacks or events across your environment. You can block threats based on threat actor, IP range, geolocation, or attack type like cross-site scripting, parameter anomalies, or recent CVEs like Log4js or Log4shell.

Traceable protects the APIs of enterprise organisations like yours

Canon Informatica ETHOS

Jobvite DigitalOcean Zolve Bullish

harness FALCONX MARQETA DRATA

block.one BlueVolt Outreach NextRoll

360Learning ATHEER leaflink Houwzer

Meet with a security expert

Our crack security research team is happy to meet with you to talk about your API security challenges.

Schedule Meeting

About us

Traceable is the industry's leading API security platform that identifies APIs, evaluates API risk posture, stops API attacks, and provides deep analytics for threat hunting and forensic research.

With visual depictions of API paths at the core of its technology, its platform applies the power of distributed tracing and machine learning models for API security across the entire development lifecycle. Visual depictions provide insight into user and API behaviors to understand anomalies and block API attacks, enabling organizations to be more secure and resilient.

www.traceable.ai

TRACEABLE