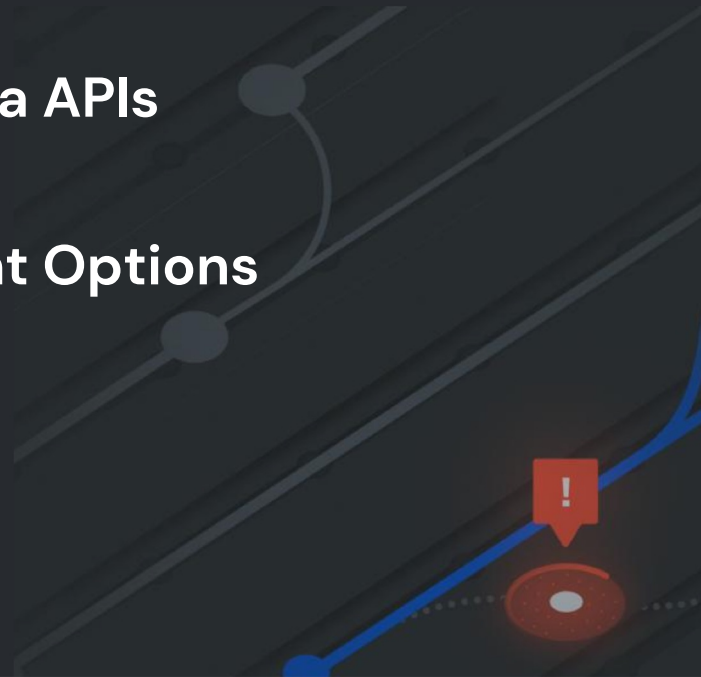
TRACEABLE

API Security Platform

Key Differentiators

What are TRACEABLE_'s key differentiators?

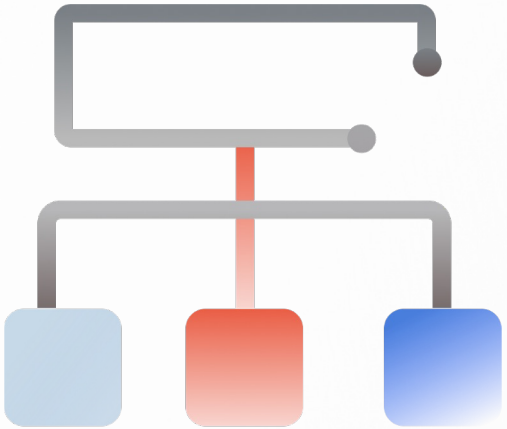
1. Breadth of Platform Capabilities
2. Protection Against Data Exfiltration via APIs
3. Deep Security Analytics
4. Flexible Data Collection & Deployment Options
5. Built for Massive Scale



#1 Breadth of Platform Capabilities

The majority of API security vendors focus on only one element of the API security challenge: API endpoint discovery and security posture. Traceable doesn't believe full API security and runtime protection can be accomplished through a point solution. Traceable provides 3 platform capabilities:

(1) **API Discovery & Security Posture**: providing you with visibility, inventory, and risk-ranking of all your known or unknown API endpoints
(2) **Runtime API Protection**: capable of detecting & blocking both known API vulnerabilities and unknown threats and zero-days,
(3) **Security Analytics:** designed to give you a rich set of security and application flow data for threat hunting, red team / blue team activities, and security optimization.

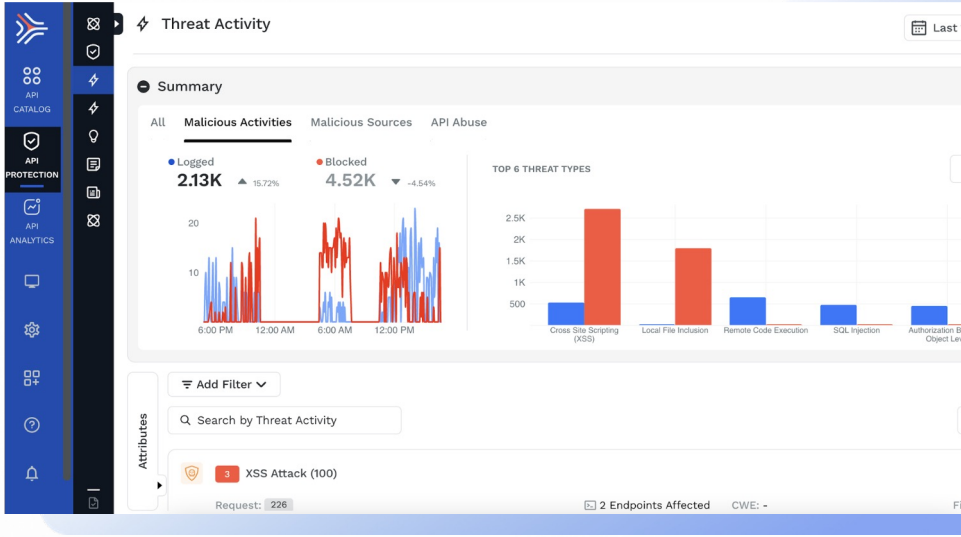


Collecting and analyzing network logs only out-of-band can't provide in-line security blocking. These products rely on other WAF, RASP, or API gateway tools for any in-line blocking. They cannot detect zero-day attacks which require deep knowledge of applications, microservices, & users.

#2 Protection Against Data Exfiltration via APIs

Traceable can be instrumented inside your API gateway or in-line your application architecture to provide real-time detection and protection against sensitive data theft. You can immediately detect when and where a bad actor gains access to confidential information by exploiting software bugs, CVEs, or zero-days.

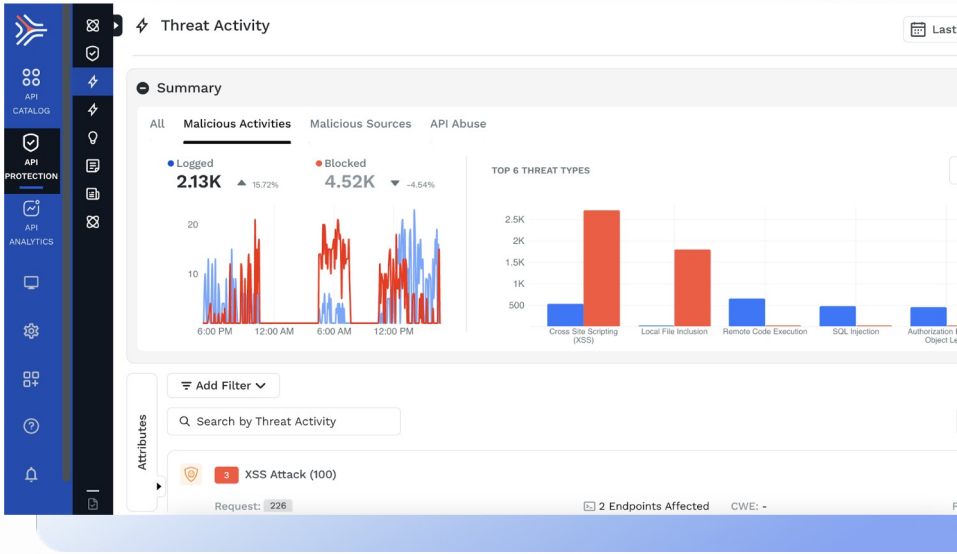
More valuably, you can track the flow of transactions through your application from edge to data store and back to quickly respond and shut down the attempted theft. It's nearly impossible to do this via out-of-band solutions provided by other API security vendors.



#3 Deep Security Analytics

Traceable provides a rich set of security and application flow analytics in a data lake which can be used by your SOC team or security analysts. Your team can hunt for hidden IOCs and breaches, track and trace activities of suspicious users, run postmortem analysis of security incidents, spot malicious users, speed incident response, and lower MTTR.

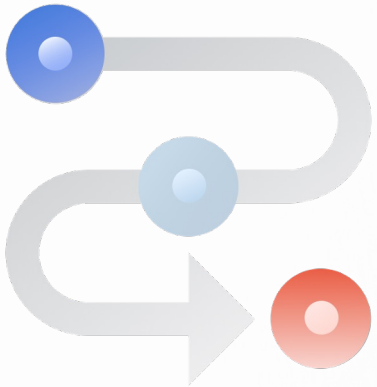
This capability cannot be provided by other API security solutions that collect and analyze data in a purely out-of-band manner.



#4 Flexible Deployment Options

Traceable can collect data through a variety of methods: including

(1) Fully out-of-band collection via traffic stream analysis of AWS, GCP, and Azure clouds,
(2) Collection by instrumentation within your API gateway, proxies, or service mesh, and
(3) In-app data collection through instrumentation by language-specific agents or via socket filtering.

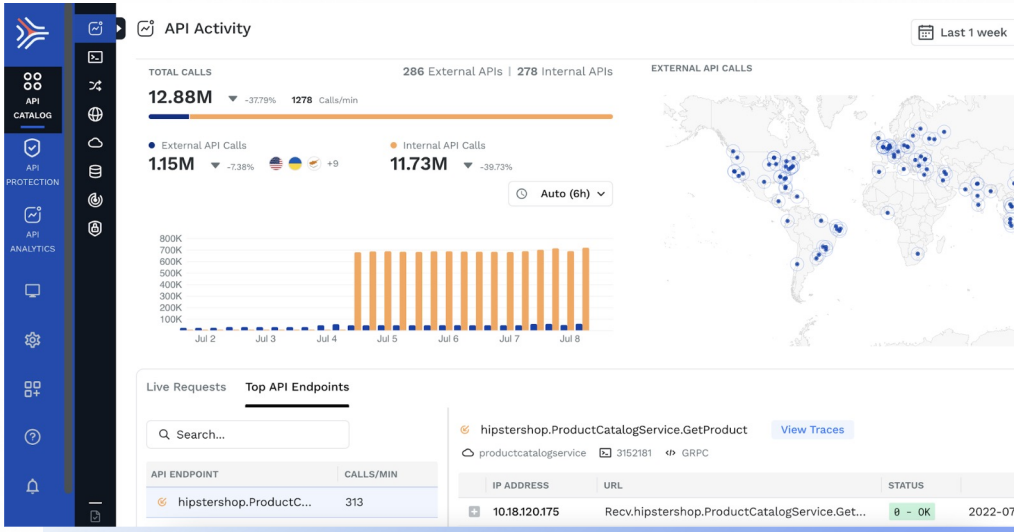


Equally important, the entire Traceable platform can be deployed 100% on-premises in a fully air-gapped model or can be delivered by SaaS or hosted in your own AWS, GCP, and Azure cloud.

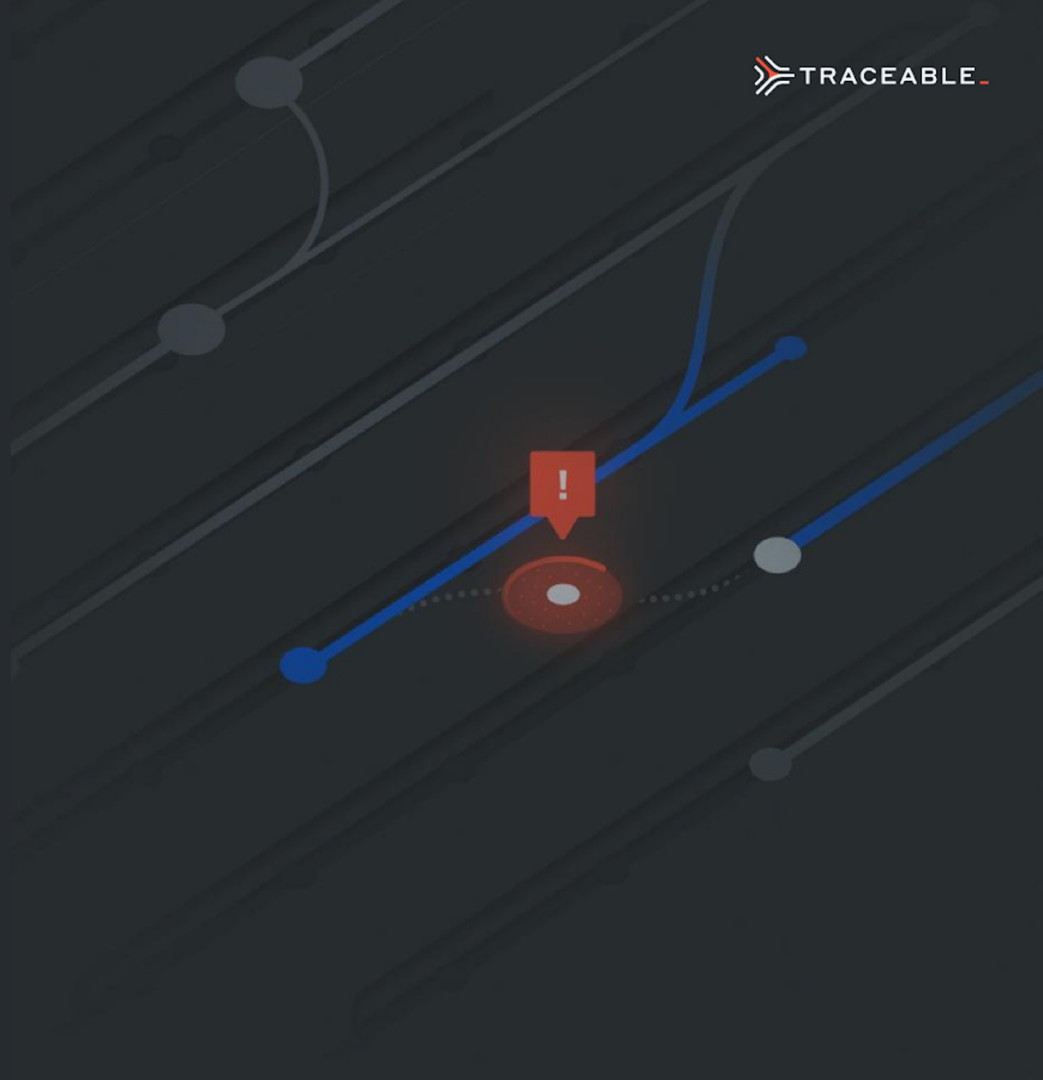
#5 Built for Massive Scale

Traceable was designed to process and analyze APIs, application communication, & user behavior data at cloud-scale.

It is designed to support very large customer deployments consisting of thousands of API endpoints and billions of API calls.



TRACEABLE



Thank you.