TRACEABLE

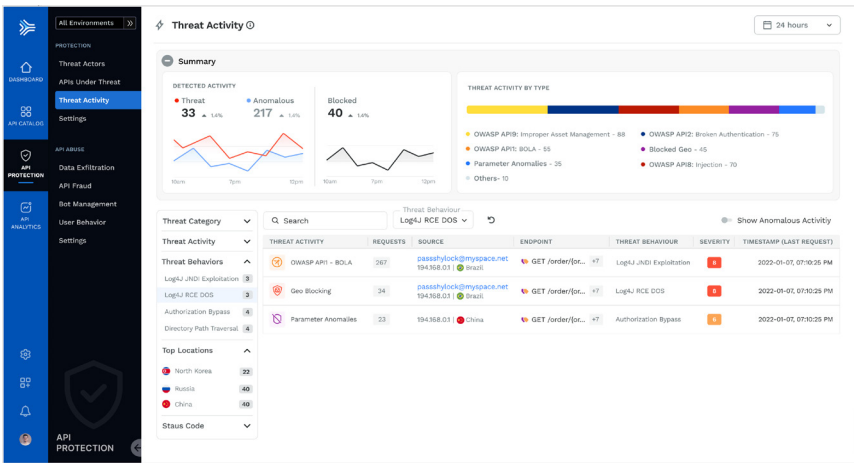
API Security Risk Assessment from Traceable

Instantly discover your APIs and where you are vulnerable, evaluate risk, obtain actionable intelligence, and build an enterprise-grade API security strategy.

Are you prepared to defend against the biggest security risk to your organization?

APIs are now the top attack vector for organizations across multiple industries. Organizations are contending with API security breaches including fraud, abuse, and sensitive data exfiltration - all of which result in financial losses, brand value erosion and operational downtime.

- **API Sprawl:** No visibility into the number of APIs, where those APIs reside, and what they are doing.
- **Shadow APIs:** Undocumented APIs create massive security and governance risks for the organization.
- **Distributed Applications:** Microservices architectures make applications massive distributed, creating more unknowns, and therefore, unknown risk.
- **API Abuse**: Unsanctioned access to APIs, modifying keys and servers, financial fraud, and more.
- **API Fraud:** APIs used for fraudulent activities such as changing the price of products in stores, to unauthorized access and use of accounts and financial information.
- **Malicious API Bots:** Automated API attacks to exploit unknown weaknesses in APIs.
- **Sensitive Data Exfiltration:** Using APIs to gain unsanctioned access to sensitive data, and exfiltrating it outside the organization.



What's included in the assessment?

Instantly discover your APIs and risk exposure

Instantly know where you are exposed. Tackle API sprawl, head on. See first hand how automatic and continuous API discovery gives you comprehensive visibility into all API, sensitive data flows, and risk posture – even as your environment changes.

Determine if your API security has been compromised

The assessment evaluates if you've already been compromised. We also identify all known and unknown API attacks, including internal and external API attacks, cover the OWASP API and web top 10, business logic attacks, API abuse, API fraud, malicious bots, and sensitive data exfiltration.

See through the eyes of API attackers

Determine how well your current security controls are working to secure your APIs. Immediately discover the signs of reconnaissance and be able to take action before attacks are successful.

TRACEABLE

Understand your API security posture in <48 hours

Instantly discover your APIs and risk exposure

Instantly know where you are exposed. Tackle API sprawl, head on. See first hand how automatic and continuous API discovery gives you comprehensive visibility into all APIs, sensitive data flows, and risk posture -- even as you environment changes.

Determine if your API security has been compromised

The assessment identifies all known and unknown API attacks, including internal and external API attacks, the OWASP web and API top 10, business logic attacks, API abuse, API fraud, malicious bots, and sensitive data exfiltration.

See through the eyes of attackers

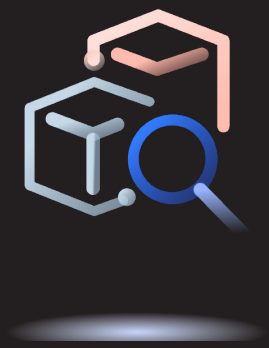
Determine how well your existing security controls are working to secure your APIs. Immediately discovery the signs of reconnaissance and be able to take action before attacks are successful.

TRACEABLE

What's Included in the API Security Assessment?

API Security Summary of Findings

Detailed discovery and catalog of all APIs, including known and unknown, shadow APIs, API endpoints, sensitive data, parameters and risk scores, so you instantly know where you are at risk, and what to do about it.



Shift Left Security Evaluation

API security is especially valuable when it's applied across the entire software development lifecycle (SDLC). We'll show you how to implement API security across build, deploy and runtime, how to actively test your APIs in pre-prod, and how to provide developers with remediation insights to further harden your APIs.

API security best practices and recommendations

Learn how API security can become an integrated part of your data security strategy, as well as your API planning, design and development process.

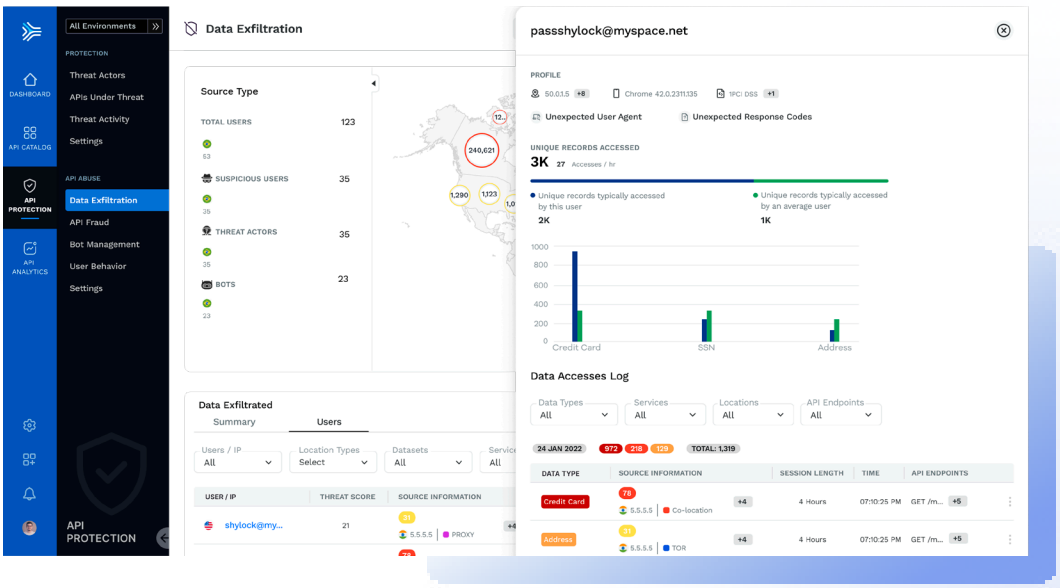
> With Traceable, we are able to detect and respond to breaches in the shortest possible time. For us, it was also important to have continuous visibility into the APIs, identify root cause, and remediate those issues.

Pathik Patel
Head of Cloud Security, Informatica

TRACEABLE

Traceable's API Security Risk Assessment Covers your Top Use Cases

- API Discovery
- Sensitive Data Exfiltration
- Account Takeover
- Bot Mitigation
- Shift Left Security
- Incident Response
- Data Privacy
- Developer Remediation
- API Security Testing



About Traceable

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.

Learn more at traceable.ai.

TRACEABLE_

Intelligent API Security at Enterprise Scale