



Code to Cloud: API Threat Correlation

Accelerate threat response with complete visibility from API to cloud layers.

Prioritize threats across API and Cloud layers

Infosec teams need visibility from code to the cloud stack to identify threats. With code to cloud correlation of threats via the Wiz and Traceable integration, IT and security teams will have correlated and prioritized threats across architectural layers.

Complete Threat Correlation

Complete Threat correlation with cloud context in Kubernetes and VM deployments across cloud services

Prevent Data Loss via APIs

API Data loss mapping with data stores protects sensitive data

Scale easily and securely

Automatic mapping of APIs to cloud deployments automatically by Traceable

Traceable API Platform

- API Risk Posture Management
- API Threat Protection
- Data Protection at API Layer
- API Security Testing
- API Security Analytics



Secure your API applications with visibility from code to cloud

Traceable API Security Platform

Traceable's context-aware solution powers complete API security including: API security posture management, threat protection and threat management across the entire Software Development Lifecycle (SDLC). Powered by analytics across our API Data Lake, API behavior analytics can identify run-time threats including OWASP API top 10 and business logic attacks. The correlation of threats between Wiz and Traceable builds a strong layer of defense and accelerates remediation.

TRACEABLE_

WIZ Cloud Security Platform

Wiz swiftly identifies and mitigates critical risks in cloud environments. It offers full-stack visibility, accurate risk prioritization, and enhanced business agility. Wiz connects quickly, scans without agents, and performs a comprehensive assessment to uncover real risks. Security and cloud teams proactively remove risks and strengthen cloud environments. For more information, visit www.wiz.io.

- Cloud Security Posture Platform
- Container and Kubernetes Security
- IAC Scanning
- Data Security Posture Management
- Cloud Infrastructure Entitlement
 Management

Complete Visibility to APIs Under Threat in Traceable

Traceable integrates with Wiz to dynamically capture security findings from Wiz regarding the mapping of Kubernetes instances, services, and VM's. This ensures that you do not have to manually track the resources where these APIs are running to understand any threats. In addition your security posture is continuously maintained even as newer versions of APIs are released and cloud instances are auto scaled.

You can easily view all Wiz services and associated issues in Traceable by navigating to: **Protection** \rightarrow **APIs Under Threat.**

All Environments	APIs Under Threat		🗇 Las	t 1 day 🗸 C Refresh	
PROTECTION	• Statistics				WIZ
APIs Under Threat Events	View API 🗸				
Threat Activity	APIS AFFECTED BY TOP MALICIOUS BEHAVIORS	TOP 6 THREAT TYPES		Threat Type 🗸 🗸	
API ABUSE	Unrecognized field	7 7			
🛛 Data Protection	Broken Function Level Au	- 6 5 -			Certified Wiz
🖶 API Fraud	Unexpected response con	- 5 3			Integration
Q User Behavior	Value out of range				integration
SETTINGS	Server Side Request Forg	3 Unicognized Ride Contest Type Assamely. Bolion Pur Autorease	rdion Level Server Side Request Forgary Cross Site Borgary on (DFLA) (SSRIP) Signatures	X85) Value Out of Range	
1 Threat Scoring	(TT) - see			Group By	
Custom Policy	₹ Add Filter ∨			Service Name 🗸	
	Q. Search by API Name				
	SERVICE		TOTAL APIS	INTEGRATIONS	
	nginx-traceshop		18	wiz	
	S shashankOCIService		3	wiz	
	stashankOCIService		,	wiz'	
	D frontend		1	wiz'	
	Cartservice		1	wiz'	
	O orderservice		1	WIZ	
PROTECTION	API REQU	UESTS THREAT REQUESTS MALICIOUS BEHAVIORS	LAST MALICIOUS BEHAVIOR	THREAT ACTORS	
	an over 2 1 17 1 10	ana a			

