TRACEABLE

API Security for Cloud-Native Apps

Traceable enables security and engineering to keep up with the continuous pace of change and complexity, and to protect applications from traditional & advanced application and API threats

Traceable AI applies the power of distributed tracing and unsupervised machine learning to enable you to:

Know where you are exposed

- API Discovery - auto inventory of all your APIs
- API DNA - auto generated detailed API specs
- API Insights - runtime API and user behavior
- API Risk Monitoring - continuous scoring
- User Attributed Activity Tracking

Detect & Stop API and Web Attacks

- API & Web Application Protection
- Sensitive Data Tracking
- ATO and Brute-force Attack Protection
- API Vulnerability Detection
- Multi-session Threat Detection
- OPA policy enforcement / blocking
- Drop-in Security Enhancement
- Satisfies PCI-DSS 6.6 WAF requirement

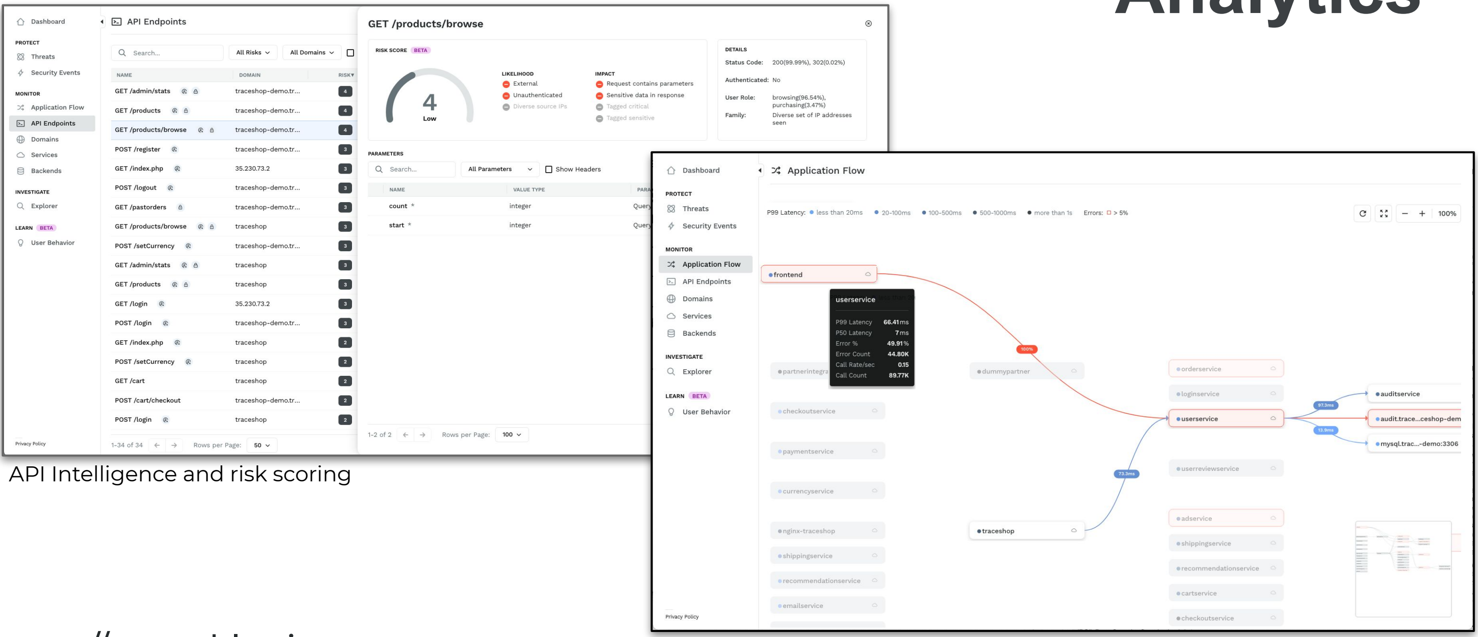
Use Insights to Improve

- Trace Explorer - searchable transaction data lake
- Threat Hunting - explore for signs of threats
- Forensics - review full requests and responses
- Audit and Compliance - track API and data changes
- API Performance Metrics - errors, latency, calls, etc

Visibility

Protection

Analytics



NAME	DOMAIN	RISK▾
GET /admin/stats	traceshop-demo.tr...	4
GET /products	traceshop-demo.tr...	4
GET /products/browse	traceshop-demo.tr...	4
POST /register	traceshop-demo.tr...	3
GET /index.php	35.230.73.2	3
POST /logout	traceshop-demo.tr...	3
GET /pastorders	traceshop-demo.tr...	3
GET /products/browse	traceshop	3
POST /setCurrency	traceshop-demo.tr...	3
GET /admin/stats	traceshop	3
GET /products	traceshop	3
GET /login	35.230.73.2	3
POST /login	traceshop-demo.tr...	3
GET /index.php	traceshop	2
POST /setCurrency	traceshop	2
GET /cart	traceshop	2
POST /cart/checkout	traceshop-demo.tr...	2
POST /login	traceshop	2

1-34 of 34 ← → Rows per Page: 50

GET /products/browse

RISK SCORE BETA

4 Low

LIKELIHOOD
- External
- Unauthenticated
- Diverse source IPs

IMPACT
- Request contains parameters
- Sensitive data in response
- Tagged critical
- Tagged sensitive

DETAILS

Status Code: 200(99.99%), 302(0.02%)

Authenticated: No

User Role: browsing(96.54%), purchasing(3.47%)

Family: Diverse set of IP addresses seen

PARAMETERS

NAME	VALUE TYPE	PARA
count *	integer	Query
start *	integer	Query

1-2 of 2 ← → Rows per Page: 100

API Intelligence and risk scoring

userservice

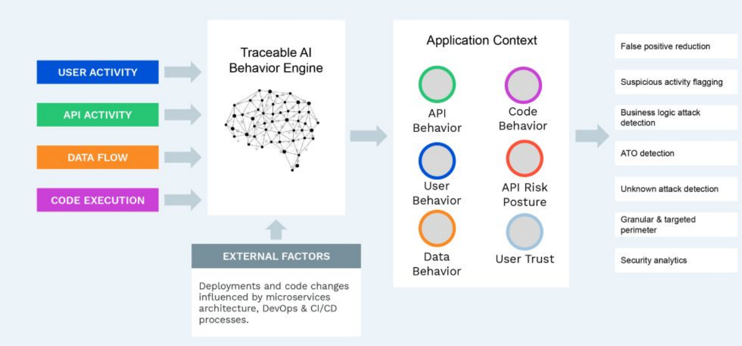
P99 Latency	66.41ms
P50 Latency	7ms
Error %	49.91%
Error Count	44.80K
Call Rate/sec	0.15
Call Count	89.77K

Interactive visual data & API flow

https://traceable.ai

Doc ver: 2021-08-12-01

TRACEABLE

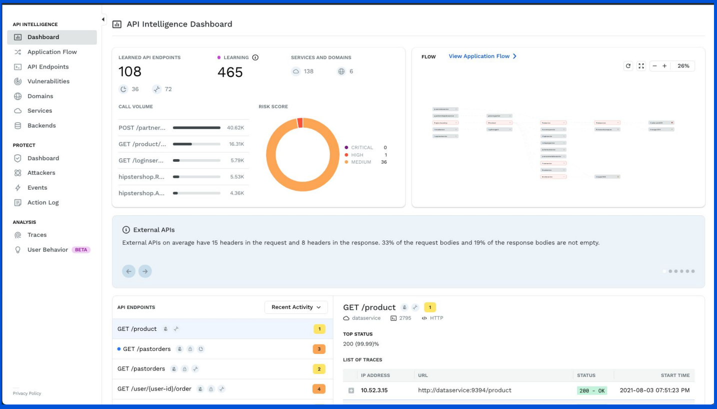


Traceable deploys in 10 mins in Kubernetes environments and supports DevOps-friendly deployment tools.

Supported in non-cloud, cloud, and hybrid cloud architectures including private cloud, AWS EC2, GCP, NGINX load balancer, Istio and many other deployment environments.

Distributed tracing agents based on OpenTelemetry standards provide native protection for Java, Golang, Node.js and Python, REST, GraphQL and gRPC API observability and protection to support a variety of application architectures.

Security posture dashboard



API Intelligence Dashboard

LEARNED API ENDPOINTS 108 · 36 · 72

LEARNING 465

SERVICES AND DOMAINS 138 · 6

CALL VOLUME

POST /partner...	40.62K
GET /product/...	16.31K
GET /loginser...	5.79K
hipstershop.R...	5.53K
hipstershop.A...	4.36K

RISK SCORE

CRITICAL	0
HIGH	1
MEDIUM	36

External APIs

External APIs on average have 15 headers in the request and 8 headers in the response. 33% of the request bodies and 19% of the response bodies are not empty.

API ENDPOINTS

GET /product	1
GET /pastorders	3
GET /pastorders	2
GET /user/{user-id}/order	4

GET /product 1

dataservice · 2795 · HTTP

TOP STATUS

200 (99.99)%

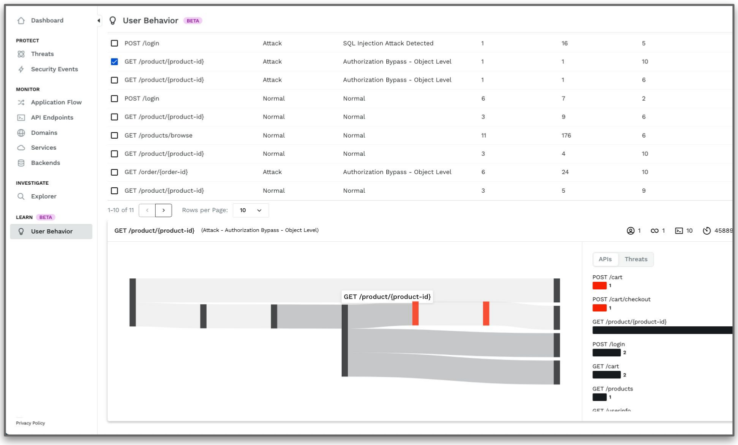
LIST OF TRACES

IP ADDRESS	URL	STATUS	START TIME
10.52.3.15	http://dataservice:9394/product	200 - OK	2021-08-03 07:51:23 PM

Detects & Protects

- OWASP Top 10 (WAF)
- OWASP API Top 10
- Business logic attacks
- Anomalous user and API behavior
- Other attacks such as SSRF, local file inclusion, remote code execution, and more

User behavior analysis



User Behavior BETA

□	POST /login	Attack	SQL Injection Attack Detected	1	16	5
☑	GET /product/{product-id}	Attack	Authorization Bypass - Object Level	1	1	10
□	GET /product/{product-id}	Attack	Authorization Bypass - Object Level	1	1	6
□	POST /login	Normal	Normal	6	7	2
□	GET /product/{product-id}	Normal	Normal	3	9	6
□	GET /products/browse	Normal	Normal	11	176	6
□	GET /product/{product-id}	Normal	Normal	3	4	10
□	GET /order/{order-id}	Attack	Authorization Bypass - Object Level	6	24	10
□	GET /product/{product-id}	Normal	Normal	3	5	9

1-10 of 11 · Rows per Page: 10

GET /product/{product-id} (Attack - Authorization Bypass - Object Level) 1 · 1 · 10 · 45889

GET /product/{product-id}

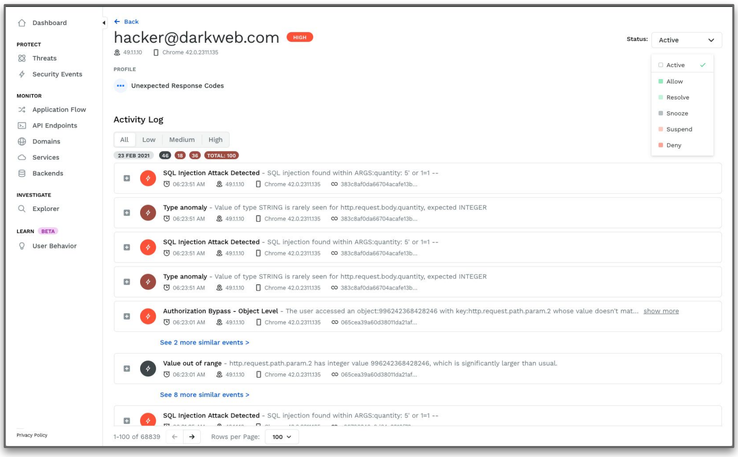
Infrastructure

- AWS EKS
- AWS ECS
- GCP GKE
- Azure AKS
- Docker
- Kubernetes
- Helm
- Ambassador
- Istio
- NGINX ingress
- NGINX load balancer
- Kong API gateway

Languages

- Java
- Golang
- Python
- NodeJS*
- Zipkin agent support
- Jaeger agent support
- OpenTelemetry agent support

Threat actor storyboards (user attribution based)



hacker@darkweb.com HIGH

49.1.1.10 · Chrome 42.0.2311.135

PROFILE

Unexpected Response Codes

Activity Log

23 FEB 2021 · 46 · 18 · 36 · TOTAL: 100

SQL Injection Attack Detected - SQL injection found within ARGS:quantity: 5' or 1=1 --
06:23:51 AM · 49.1.1.10 · Chrome 42.0.2311.135 · 383c8af0da66704acafe13b...

Type anomaly - Value of type STRING is rarely seen for http.request.body.quantity, expected INTEGER
06:23:51 AM · 49.1.1.10 · Chrome 42.0.2311.135 · 383c8af0da66704acafe13b...

SQL Injection Attack Detected - SQL injection found within ARGS:quantity: 5' or 1=1 --
06:23:51 AM · 49.1.1.10 · Chrome 42.0.2311.135 · 383c8af0da66704acafe13b...

Type anomaly - Value of type STRING is rarely seen for http.request.body.quantity, expected INTEGER
06:23:51 AM · 49.1.1.10 · Chrome 42.0.2311.135 · 383c8af0da66704acafe13b...

Authorization Bypass - Object Level - The user accessed an object:996242368428246 with key:http.request.path.param.2 whose value doesn't mat... show more
06:23:01 AM · 49.1.1.10 · Chrome 42.0.2311.135 · 065cea39a60d38011da21af...

See 2 more similar events >

Value out of range - http.request.path.param.2 has integer value 996242368428246, which is significantly larger than usual.
06:23:01 AM · 49.1.1.10 · Chrome 42.0.2311.135 · 065cea39a60d38011da21af...

See 8 more similar events >

SQL Injection Attack Detected - SQL injection found within ARGS:quantity: 5' or 1=1 --

1-100 of 68839 · Rows per Page: 100

https://traceable.ai

*roadmap

Doc Ver: 2021-02-24-01