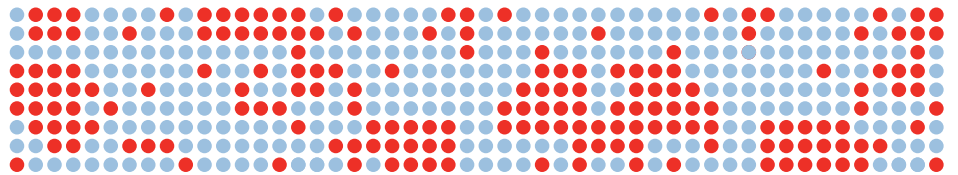


The API you don't know about is the one that **breaches** you.

Modern enterprises run on APIs — thousands of them, scattered across clouds, gateways, and dev environments.

40%
are undocumented



Many are forgotten. Some were never supposed to exist.

The Threat Landscape

40%

of enterprise APIs
are undocumented
or unknown

\$4M

average cost of a
single API data breach

68%

of breaches start at
web apps & APIs
(Verizon DBIR)

The Visibility Gap

Inventory lives in spreadsheets, ticket queues, and tribal memory.

~~api_v1_legacy.xlsx~~

~~TKT-3492~~

~~??? endpoints~~

postman.json

~~m&a_inheritance~~

readme.md

prod-east-gw

~~tribal knowledge~~

specs/

~~-shadow.svc.local-~~

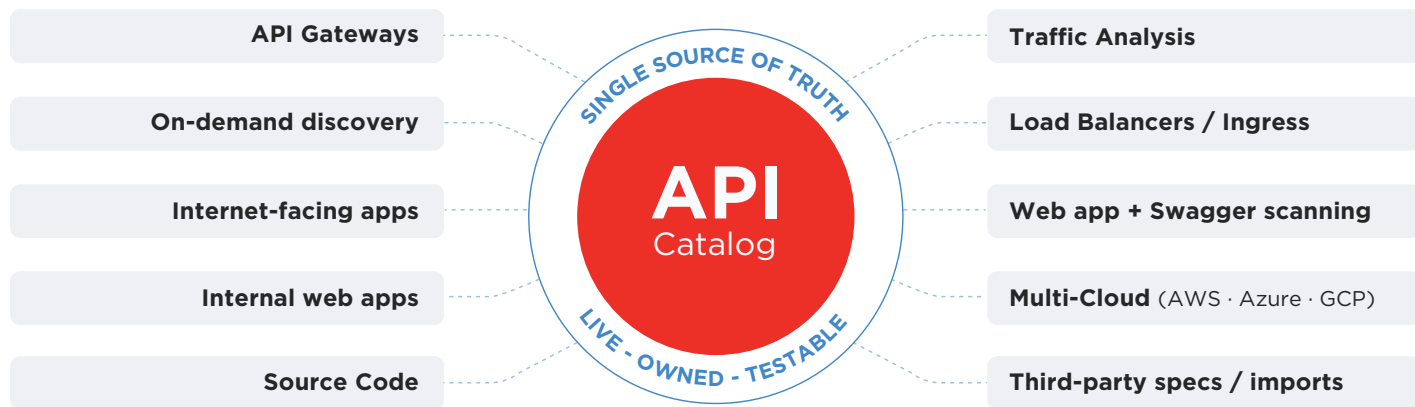
openapi.yml

~~-/internal/debug-~~



Security only covers 'known apps,' not what the load balancer actually exposes. Attackers don't care about your spreadsheet. They probe every shadow, every forgotten endpoint, every undocumented path. They find the gaps. And they walk right through.

Mapping The Path To Complete API Visibility



Each Source Plays A Different Role

API Gateways

Documented APIs, plus the forgotten endpoints living inside gateways that AppSec never onboarded.

Web App Scan to API Discovery

Shadow APIs surfaced from the running app. Swagger artifacts and endpoints observed mid-scan.

Spec & Collection Imports

Known APIs from imported specs, plus drift checks for "should-exist" endpoints that aren't actually live.

Source Code Discovery

Endpoints defined in code but never registered with a gateway or spec caught before release.

Internet-Exposed

Internet-facing apps and APIs surfaced through DNS, certs, subdomains, and other external signals.

Load Balancers & Ingress

Side-door APIs exposed through L7 routing rules that never appear in any application inventory.

Multi-Cloud Discovery

Web apps and APIs across accounts & subscriptions where ownership has blurred like M&A, drift, sandbox-to-prod.

Traffic Analysis

Shadow APIs actually used in production, partner and internal calls that never made it into a spec.

Internal Blind Spots

Internal web apps and APIs, legacy systems and "quiet critical" services that AppSec never onboarded.

On-Demand Discovery

A rapid baseline of what exists when no clean inventory is available, exportable snapshot for scoping.

Qualys TotalAppSec

AI - Powered Application Risk Management



See everything

Continuous auto-discovery across on-prem, multi-cloud, API gateways, containers, and microservices. Integrates with EASM, CSAM, Postman, and MuleSoft.



Know what hurts

AI-powered DAST + OWASP API Top 10 coverage. Detects BOLA, PII exposures, auth flaws, injection attacks, OpenAPI drift, and zero-day malware via deep learning models.



Fix what matters

TruRisk™ prioritizes by exploitability, data sensitivity, and business impact - not just CVSS. QFlow™ automation + native Jira, ServiceNow, GitHub Actions, Jenkins integrations.

From "we think we know" to "here's the list."

One catalog that drives testing scope, audit answers, M&A diligence, and the coverage number you report up - all from sources you can re-run on demand.



Qualys.

©2026 Qualys, Inc. All rights reserved.

Request a Demo