Apyguard

API SECURITY PLATFORM

- PRODUCT OVERVIEW 2026

Secure Every API. Ship with Confidence.

Apyguard gives security and engineering teams end-to-end visibility into their API attack surface. From automated discovery and AI-powered vulnerability scanning to full remediation management - in a single platform.

Complete API security visibility - from discovery to remediation.

01 APIScout

02 User-Driven Discovery

03 OpenAPI Blueprint

04 Behavior Profiling

05 AI Vuln Scanner

06 CI/CD Integration

07 Vuln Management

08 Traffic Analyzer SOON

8 modules
INTEGRATED CAPABILITIES

AI
POWERED SCANNER

0 blind spots
FULL API COVERAGE

- WHY API SECURITY IS CRITICAL TODAY

APIs Are the Largest Expanding Attack Surface

Modern applications expose hundreds of API endpoints. Most organizations lack visibility into what's running, what's vulnerable, and what data is being exposed. Attackers have learned to exploit this gap faster than security teams can respond.

Shadow & Zombie APIs

Undocumented and deprecated endpoints remain active and exposed - invisible to security teams but fully accessible to attackers who enumerate them.

Broken Authorization

BOLA and BFLA vulnerabilities account for the majority of API breaches. Traditional scanners routinely miss them because they lack application context.

Silent Data Exposure

APIs silently return PII, credentials, and internal data that was never meant to be exposed - without triggering any security alerts or monitoring.

The Apyguard Platform - Eight Integrated Capabilities

Apyguard addresses the full API security lifecycle in a single platform - eliminating the need to stitch together multiple point tools.

01 **APIScout - Source-Level Discovery in VS Code**

Reconstructs every route declared in the source, scores OpenAPI readiness, exports the spec that scopes every scan.

02 **User-Driven API Discovery via Chrome Extension**

Captures real browser traffic to build a complete live inventory - including undocumented, shadow, and zombie endpoints.

03 **OpenAPI Blueprint Static Analysis**

Analyzes API specifications before runtime, catching design flaws, missing auth schemes, and misconfigurations at the earliest stage.

04 **API Behavior Profiling & Drift Detection**

Builds behavioral baselines and detects deviations in real time - flagging new fields, sensitive data exposure, and abnormal patterns.

05 **AI-Powered Vulnerability Scanner**

Simulates real attacker behavior to detect OWASP API Top 10 vulnerabilities including authorization flaws and business logic issues.

06 **CI/CD Integration**

Runs security tests on every pull request and blocks regressions before they reach production.

07 **Vulnerability Management**

Tracks remediation from discovery through verified fix.

08 **Traffic Analyzer** COMING SOON

Ingests traffic logs from Cloudflare, API gateways, and other sources to automatically detect shadow APIs, sensitive data exposure, and real-time attack patterns - without agent installation.

- FEATURE 01 OF 8

APIScout · VS Code extension · free

Your OpenAPI file, your gateway config, and your traffic logs all describe the API second-hand. The source code defines it. APIScout reads the backend project open in the editor, reconstructs every route it declares, and exports an OpenAPI 3.x document built from the implementation rather than from documentation that has drifted away from it.

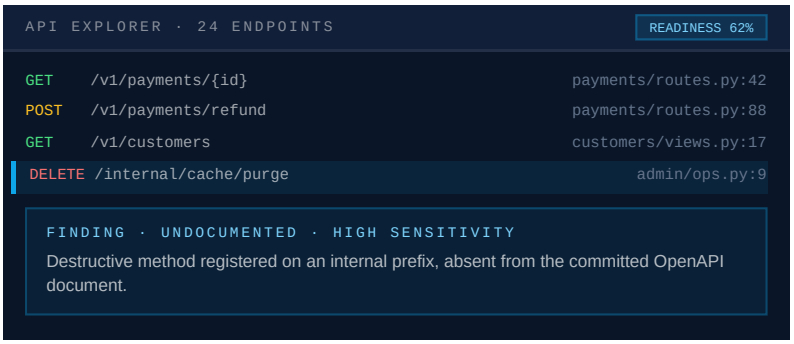
A · SOURCE-LEVEL DISCOVERY

01 · INSTALL
From the VS Code Marketplace. No agent, no config, no code changes, no running service.

02 · SCAN
Walks the workspace and reconstructs full paths, methods, handlers and groupings.

03 · REVIEW
Filter by method or path, inspect findings, jump straight to the handler that declares the route.

04 · EXPORT
OpenAPI 3.x as YAML or JSON - for docs, for review, or as the scope of an Apyguard scan.



Nothing leaves the machine
Scanning is local to the open workspace. The optional AI can run entirely against a local model.

Parsers, not pattern matching
Framework-specific parsing resolves mount prefixes and sub-applications that in-app schema generators never see.

Every route has a source
Method, path, handler, file and line - one click from the inventory to the code that declares it.

B · FROM INVENTORY TO A DOCUMENTED, REVIEWED API

An endpoint list is a starting point. APIScout scores how well that surface is documented, surfaces what needs attention, and tracks how the contract moves between scans.

OpenAPI Readiness score
A weighted measure across operation descriptions, parameters, request bodies, documented responses, security declarations and unique operation IDs - a number a team can be held to.

Priority findings, source-backed
Each finding carries confidence, evidence and a sensitivity level. Mark it reviewed, or suppress it with a recorded reason. Drafted descriptions can be inserted as TODO(APIScout) comments.

API change tracking
Every scan is diffed against the previous run or an accepted baseline. Added, removed and breaking contract changes export as Markdown, ready to paste into the pull request.

Swagger preview & request playground
A bundled, theme-aware Swagger UI renders the generated document with no external scripts. The playground sends real requests from the extension host - auth, headers, body, redirects, copy as cURL.

Optional AI enrichment
Off by default. Drafts endpoint descriptions and remediation notes through a hosted provider (OpenAI, Anthropic, Gemini, Azure AI, Together) or entirely on-device through a local adapter. Keys are held in the VS Code secret store.

SUPPORTED FRAMEWORKS
Django · Express · FastAPI · Flask · NestJS

REQUIREMENTS
VS Code 1.90+ · Python 3.9+

WHAT IT PROVES
The route exists in the code, what it accepts, and exactly where it is declared.

WHAT IT DOES NOT
Whether authorization is actually enforced. Structure is not behaviour.

WHERE APYGUARD TAKES OVER
The export becomes the scan scope for modules 02-07, where BOLA and BFLA are tested live.

WHY IT COMES FIRST

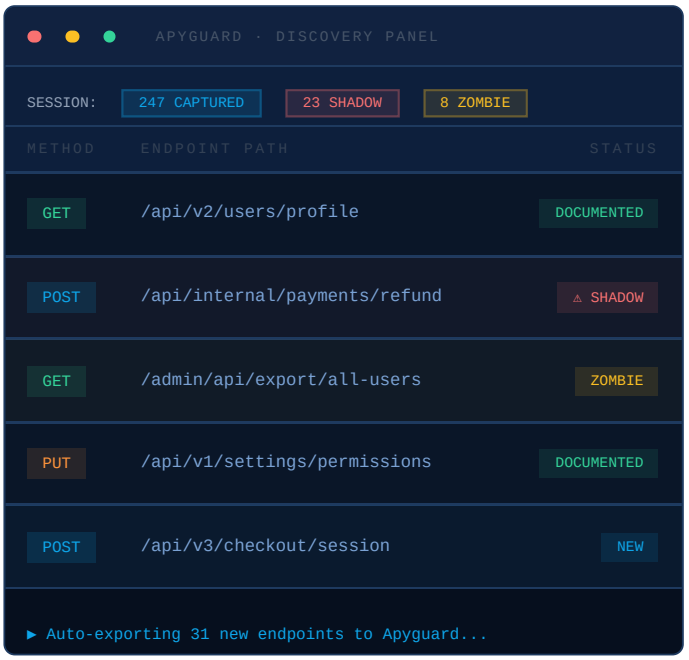
Every other module in this document is scoped by an inventory, and a scan is only as complete as the list it was given. APIScout builds that list from the one source that cannot drift - the code itself - before anything is deployed, documented or put behind a gateway.

FEATURE 02

User-Driven API Discovery via Chrome Extension

Most API security tools miss shadow APIs because they rely on documentation that's never complete. Apyguard's Chrome Extension captures real traffic as your team browses - automatically building a live, accurate API inventory with zero code changes required.

- Seamlessly captures **every** API request in real time during browser sessions, providing unparalleled visibility and control.
- Correlates discovered endpoints against existing OpenAPI specs to surface documentation gaps immediately
- Exports endpoints directly into the platform for immediate security testing - no manual steps required
- Just a few clicks to install, no code changes, no developer intervention - deploys in minutes



KEY INSIGHT

Organizations typically know about less than 60% of their active API endpoints. Every unknown endpoint is an unmonitored attack vector. Discovery closes the gap.

FEATURE 03

OpenAPI Blueprint Static Analysis

Apyguard analyzes your OpenAPI 3.x and Swagger 2.0 specifications before any request is made - catching security flaws, authentication gaps, and design vulnerabilities at the earliest possible stage.

- Detects missing or misconfigured security schemes per endpoint
- Flags overpermissive parameters and missing input validation
- Generates endpoint-level security score with remediation guidance

SHIFT LEFT BENEFIT

Security issues found at design time are 10× cheaper to fix than in production.

```
paths:
  /api/v2/orders:
    get:
      security: []  # ← no auth
      parameters:
        - name: user_id
          in: query  # no validation
```

✕ No security scheme on GET /api/v2/orders

⚠ user_id missing format/pattern validation

⚠ Rate-limit headers absent from response schema

FEATURE 04

Behavior Profiling & Drift Detection

Builds a behavioral baseline for every API endpoint and continuously monitors for deviations - catching silent changes before they become breaches.

- Daily baseline: response shape, latency, field presence, data classification
- Real-time drift detection - new fields, changed auth patterns flagged instantly
- PII, credentials, and financial data automatically detected in responses
- Slack and in-app notifications for instant team notification

RUNTIME INTELLIGENCE

Apyguard learns what "normal" looks like for each endpoint - and alerts the moment that changes.

DRIFT EVENTS (7D)
3
2 critical

SENSITIVE FIELDS
2
PII flagged

7-DAY BEHAVIOR CHART

FEATURE 05

AI-Powered API Vulnerability Scanner

Traditional scanners miss business logic and authorization vulnerabilities because they treat every API the same. Apyguard's AI engine understands your application's context - generating targeted test cases that simulate real attacker behavior to find what generic tools leave behind.

- **BOLA** - Tests object-level access control by manipulating IDs across requests
- **BFLA** - Verifies admin and privileged functions are properly restricted by role
- **Business Logic** - Price manipulation, workflow bypass, sequence tampering
- **Excessive Data Exposure** - Responses returning data clients don't render
- **Mass Assignment** - Privilege escalation via request body manipulation
- **OWASP API Top 10** - Full coverage: injection, auth bypass, rate limits, and more

AI ADVANTAGE

Context-aware test cases - not generic payloads. The result: significantly fewer false positives and more real, exploitable findings per scan.

SCAN RESULTS · e-commerce-api · 2025-01-14

CRITICAL	Broken Object Level Authorization	/orders/{id}
CRITICAL	Business Logic: Price Manipulation	/cart/apply
HIGH	Broken Function Level Authorization	/admin/users
HIGH	Excessive Data Exposure (PII)	/v2/profile
MEDIUM	Mass Assignment Vulnerability	/settings
MEDIUM	Authentication Bypass (JWT)	/auth/verify
LOW	Missing Rate Limiting	/auth/login

CRITICAL	HIGH	MEDIUM	LOW
2	2	2	1

FEATURE 06

CI/CD Pipeline Integration

Shift API security left. Apyguard integrates natively into your existing CI/CD pipelines, running automated security tests on every pull request and blocking vulnerable deployments before they reach production.

- Native plugins for GitHub Actions, GitLab CI, Jenkins, CircleCI, Azure DevOps
- Configurable security gates - automatically fail builds on Critical or High severity findings
- Diff-aware scanning - only tests changed endpoints, keeping pipeline runtimes fast
- Results posted in PR comments and synced to Jira tickets automatically

INTEGRATIONS

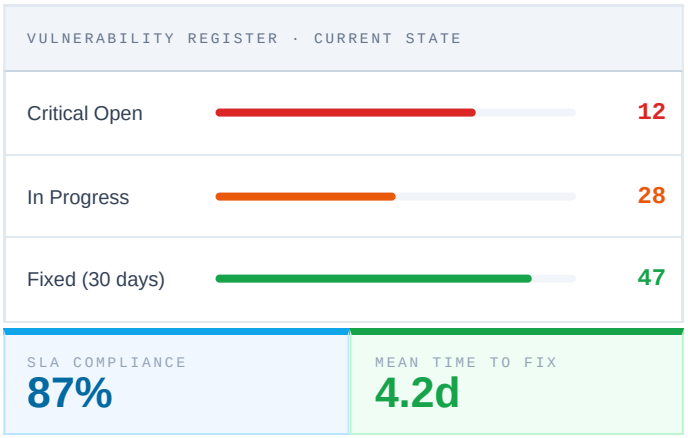
GitHub Actions | GitLab CI | Jenkins | CircleCI | Azure DevOps | Jira | Slack

FEATURE 07

Vulnerability Management

Finding vulnerabilities is half the battle. Apyguard turns scan results into tracked, owned, and time-bound remediation work - with full audit trails and compliance reporting built in.

- Centralized register with CVSS-aligned severity scoring and business impact context
- Assign to teams with SLA deadlines and automatic escalation on overdue items
- Open → In Progress → In Review → Verified Fixed lifecycle tracking
- Compliance-ready exports for ISO 27001, SOC 2, and PCI DSS audits



- THE COMPETITIVE DIFFERENCE

One Platform. Zero Blind Spots.

Most enterprise security teams stitch together 3–5 point tools to cover their API security needs - each with gaps, overlapping costs, and integration overhead. Apyguard replaces them all with a single, integrated platform covering the full API security lifecycle.

CAPABILITY	APYGUARD	POINT TOOLS
Shadow & zombie API discovery	✓	✗
OpenAPI spec-level static analysis	✓	Partial
Behavioral drift & anomaly detection	✓	✗
Business logic vulnerability testing	✓	✗
CI/CD native pipeline integration	✓	Partial
End-to-end vulnerability lifecycle	✓	✗

🎯

Context-Aware AI

Test cases generated for your specific API behavior - not generic payloads. Fewer false positives, more real findings.

⚡

No Agent Required

Deploy in minutes. No code changes, no proxy configuration, no SDK integration needed to get started.

🔄

Continuous Coverage

Security isn't a one-time scan. Apyguard monitors every commit, every deployment, every day - 24/7.

COMPLIANCE FRAMEWORKS SUPPORTED

ISO 27001 | SOC 2 Type II | PCI DSS | GDPR | OWASP API Security Top 10

✦ **COMING SOON** - This feature is currently in development and will be available in an upcoming release.

- FEATURE 08 OF 8

Traffic Analyzer

Apyguard Traffic Analyzer ingests log streams from your existing infrastructure - Cloudflare, API gateways, load balancers, and WAFs - and automatically surfaces security findings without requiring any agent installation or code changes. Every request is analyzed, correlated, and turned into actionable intelligence.

DETECTION CAPABILITIES

👻
Shadow API Detection
Identifies undocumented endpoints receiving real traffic - instantly cross-referenced against known API inventory.

🧟
Zombie API Detection
Flags deprecated or sunset endpoints still receiving traffic - hidden attack vectors that should have been decommissioned.

📋
OpenAPI Auto-Discovery
Reconstructs an OpenAPI spec from observed traffic patterns - generating living documentation directly from real request/response data.

🔐
Sensitive Data Disclosure
Detects PII, credentials, API keys, and financial data appearing in response bodies or headers - across every observed endpoint.

🚨
Attack Alarms
Real-time detection of brute force, credential stuffing, enumeration, and injection attempts - mapped to OWASP API Top 10 categories.

📈
Anomaly Detection
Behavioral baselines per endpoint, per consumer. Unusual spikes, new callers, and access pattern deviations trigger instant alerts.

SUPPORTED LOG SOURCES

Cloudflare	API Gateways	Load Balancers	SIEM / Log Pipelines	Custom Sources
Workers · Gateway · WAF logs	Kong · AWS · Azure · APIGEE	NGINX · HAProxy · AWS ALB	Splunk · Elastic · Datadog	Any JSON / CEF / W3C log format

LIVE ALARM FEED PREVIEW — COMING SOON

CRITICAL Shadow API Detected - /api/internal/billing/adjust receiving 142 req/hr Cloudflare · 2m ago

HIGH Sensitive Data Disclosure - email, phone in response body of GET /v2/users Kong GW · 5m ago

HIGH Attack Pattern - Credential stuffing on POST /auth/login, 3,200 attempts in 10 min AWS ALB · 12m ago

MEDIUM Zombie API Traffic - /api/v1/legacy/export still receiving requests (deprecated 6mo ago) NGINX · 18m ago

WHAT MAKES TRAFFIC ANALYZER DIFFERENT

No agents. No code changes. No blind spots. Traffic Analyzer works with your existing log infrastructure to deliver security intelligence across your entire API fleet - including APIs you didn't know existed.

Apyguard

API SECURITY PLATFORM

CONTACT US

WEBSITE

https://www.apyguard.com

EMAIL

info@apyguard.com

LINKEDIN

https://www.linkedin.com/company/apyguard

PLATFORM MODULES

01 · APIScout
02 · Discovery
03 · Blueprint Analysis
04 · Behavior Profiling
05 · AI Scanner
06 · CI/CD Integration
07 · Vuln Management
08 · Traffic Analyzer ✦

- NEXT STEPS

Your APIs are exposed. Let's fix that.

See how Apyguard discovers hidden endpoints, finds critical vulnerabilities, and integrates with your existing workflow - in under 30 minutes. No agents. No code changes. No friction.