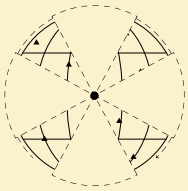
ESCAPE

OFFENSIVE SECURITY ENGINEERING PLATFORM

Offensive security for the teams that are 100x outnumbered

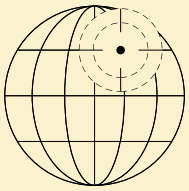
Replace legacy scanners and manual offensive security processes with AI agents that discover, test, and remediate directly in your engineering workflows.

Attack Surface Management



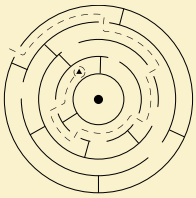
Discover and validate the exposure of modern applications, APIs, and infrastructure from code to cloud.

Business-logic-aware DAST



Replace legacy DAST with business-logic-aware testing that helps your team remediate real, exploitable vulnerabilities.

AI Pentesting



Replace manual pentest and bug bounty programs with a solution that scales.

30% MORE ASSETS DISCOVERED THAN LEGACY ASM SOLUTIONS

3900% CODE COVERAGE IMPROVEMENT OVER LEGACY DAST

393% ROI SEEN BY SECURITY TEAMS

80% TIME-TO-REMEDIATION REDUCTION VERSUS MANUAL OR SEMI-MANUAL PROCESSES

Trusted by 2000+ security teams worldwide

Trusted by the security teams all over the world

APPLIED · miro · HealthEquity · CATO NETWORKS · Hinge Health · ARKOSE LABS · SENSIA Rockwell Automation + SLB · PandaDoc

Stop playing whack-a-mole
Security isn't a checklist. It's a continuous program.

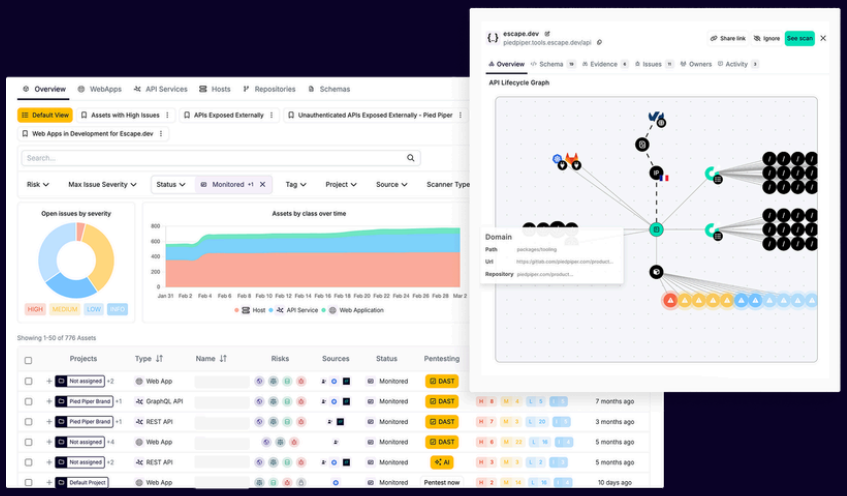
DISCOVER (ASM) | TEST (DAST) | VALIDATE (AI PENTESTING) | REMEDIATE | AUTOMATE | COMPLY

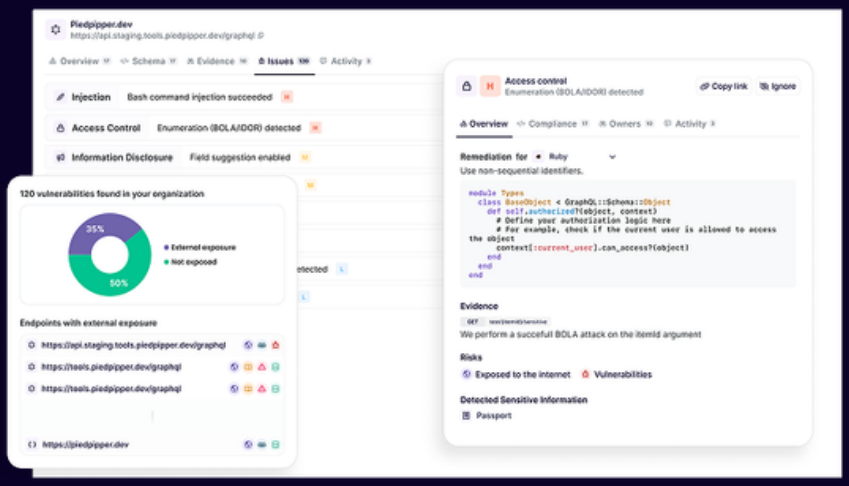
DISCOVER EVERY API, EVERY APP, IN REAL TIME

Assets flow directly to Wiz, so your risk platform gets better context

Findings route directly to the teams that own assets, with asset context already attached

We discover APIs and SPAs, not just DNS and ports, both internal and external





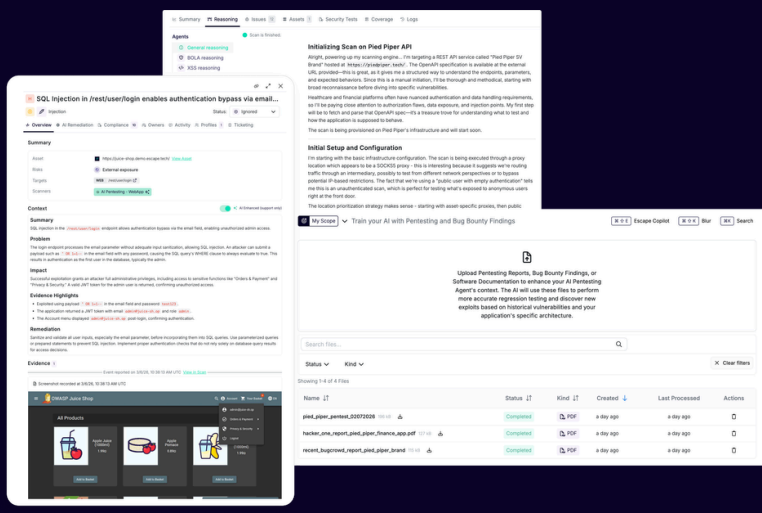
TEST EVERY RELEASE AT THE BUSINESS LOGIC LEVEL

Business logic testing: We test workflows, access control, and multi-step processes, not just payloads

Built for modern auth: OAuth, SSO, multi-tenant

Developer-friendly context: Screenshots, exploration graphs, and detailed, tailored remediation steps that ~~engineers trust~~

Integration with Wiz for unified risk view



PROVE EXPLOITABILITY AT SCALE

Agentic attack reasoning powered by Graph context : Finds complex multi-step attack chains

Proof of exploitability: Screenshots, execution logs, and attack path validation

Regression testing: Ingest bug bounty findings; AI reproduces them to prevent recurrence

AUTOMATE OFFENSIVE SECURITY END-TO-END

Fully programmable: Public API, CLI, and MCP Server. If the platform can do it, your scripts can too.

Event-based workflows to triage, route, and escalate findings. Define your policy once, the platform enforces it.

Trigger scans on every push. Security gates run in your CI/CD without your team in the loop.

Book a demo

ESCAPE

sales@escape.tech | escape.tech