

[SOLUTION BRIEF]

Security at the speed of development.

AI agents that find and prove vulnerabilities across your web apps, APIs, cloud and dependencies. Continuously, not once a year.

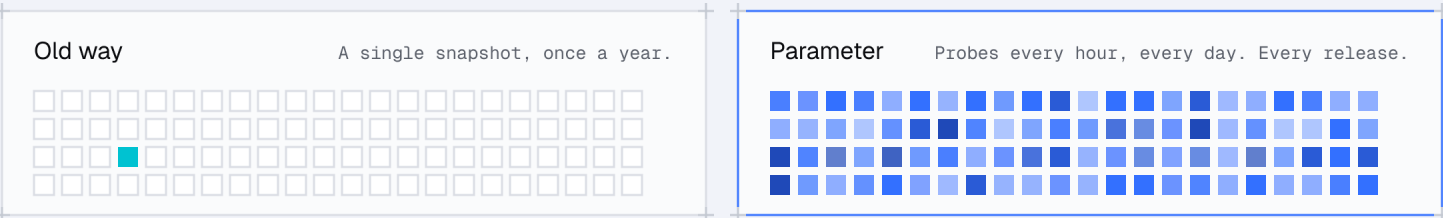
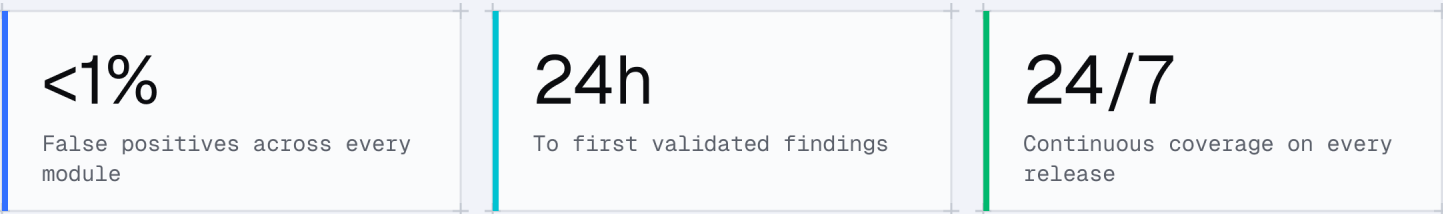
[THE PROBLEM]

Software ships every day. Security testing has not kept up. A traditional pentest is a person, booked weeks out, testing a single snapshot of your application. Scanners fill the gap with noise: pattern-matched findings that nobody has proven are exploitable, ranked by CVSS rather than by what an attacker can actually reach. The result is a queue that grows faster than it can be triaged, and coverage that lapses between engagements.

WHAT SECURITY TEAMS NEED

- 01 **Continuous coverage**
Testing that runs on every release and every deploy, not on an annual calendar.
- 02 **Proof, not probability**
A working exploit for every finding so engineers fix real risk, not theoretical risk.
- 03 **One queue, every layer**
Code, cloud, dependencies and secrets in a single place, routed to the tools teams already use.

[BY THE NUMBERS]



BUILT BY THE TEAM THAT SECURED

Apple · Google · Microsoft · U.S. Department of Defense · T-Mobile · Henkel · Epic Games · AT&T · Yahoo

BACKED BY Y COMBINATOR

[HOW IT WORKS]

One platform. Every layer of your security.

01

Connect

Point Parameter at your application, repositories and cloud accounts. No weeks of scoping, no agents to install. A URL and credentials, or a read-only role, is enough.

02

Test

Agents probe continuously across APIs, auth flows, business logic, infrastructure and dependencies, reasoning like a human red team rather than running down a checklist.

03

Report

Validated findings land with reproduction steps, a working proof-of-concept and remediation guidance, including fix pull requests ready to merge and re-test.

[SOLUTION ARCHITECTURE]

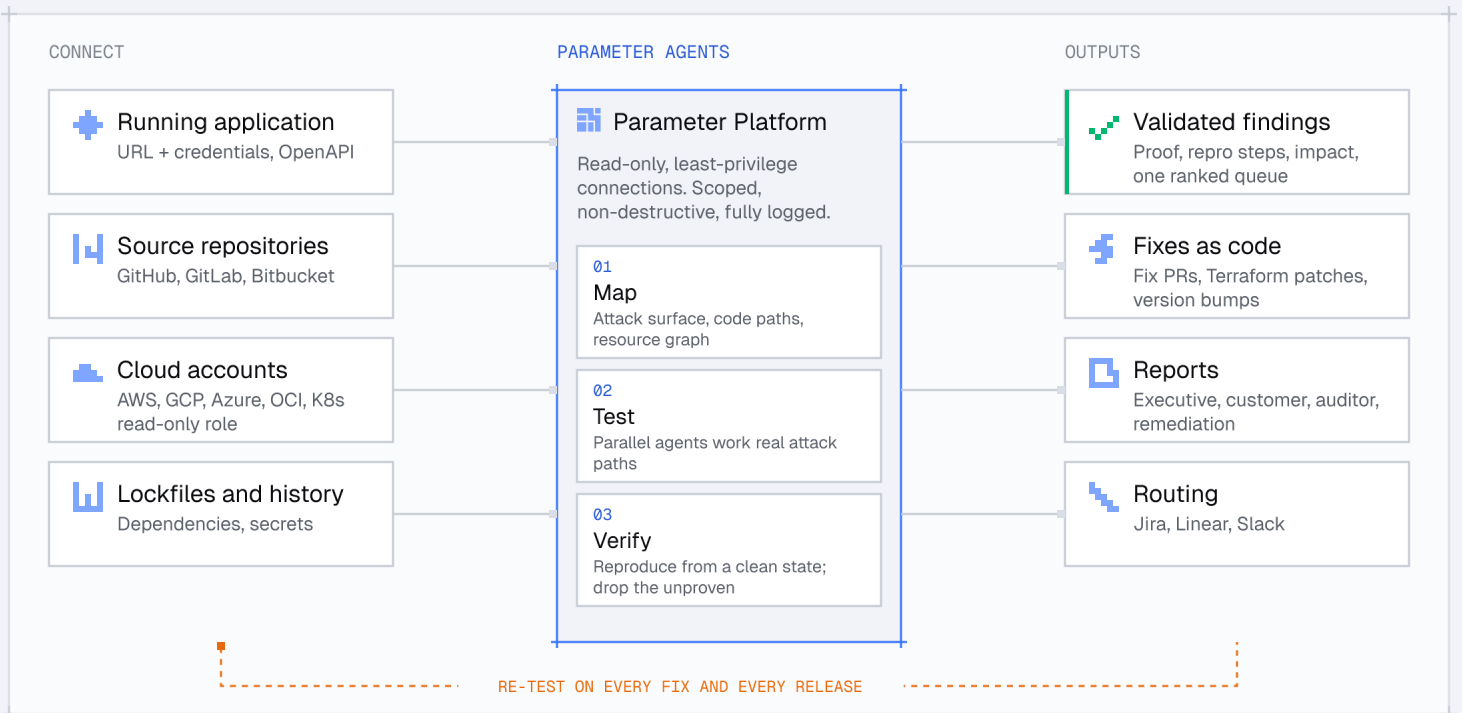


FIG. 01 Parameter Platform architecture. Read-only connections to code, cloud and running applications feed autonomous agents; only validated findings reach the shared queue, reports and integrations.

Aggressive testing, zero blast radius

Agents prove a vulnerability exists, then stop. No chaining or escalation without your go-ahead, no destructive actions, and a full audit trail of every step.

Signal over noise

Every finding is reproduced from a clean state before it is filed. Unproven findings are dropped, so the queue you see is real and short.

Finding to fix, automatically

High-confidence pull requests, Terraform patches and dependency bumps are generated with each finding, and re-tested the moment you ship.

[KEY CAPABILITIES]

Coverage across the stack, in one queue.



Pentesting Agent

Continuous, autonomous pentesting of web apps, APIs and auth flows with a working proof-of-concept for every finding.



Sentinel

An AI reviewer on every pull request that follows execution paths beyond the diff and comments inline.



Cloud Security

Attack-path reasoning across AWS, Google Cloud, Azure, Oracle Cloud and Kubernetes, with Terraform fixes opened as PRs.



Supply Chain

Full dependency graph with reachability analysis, malicious-package inspection and a signed SBOM.



Secrets Detection

Leaked keys, tokens and credentials found across repositories and git history.



Audit-ready reporting

Executive, customer-facing, auditor and remediation reports mapped to SOC 2 and ISO 27001 controls.

[PRODUCT]

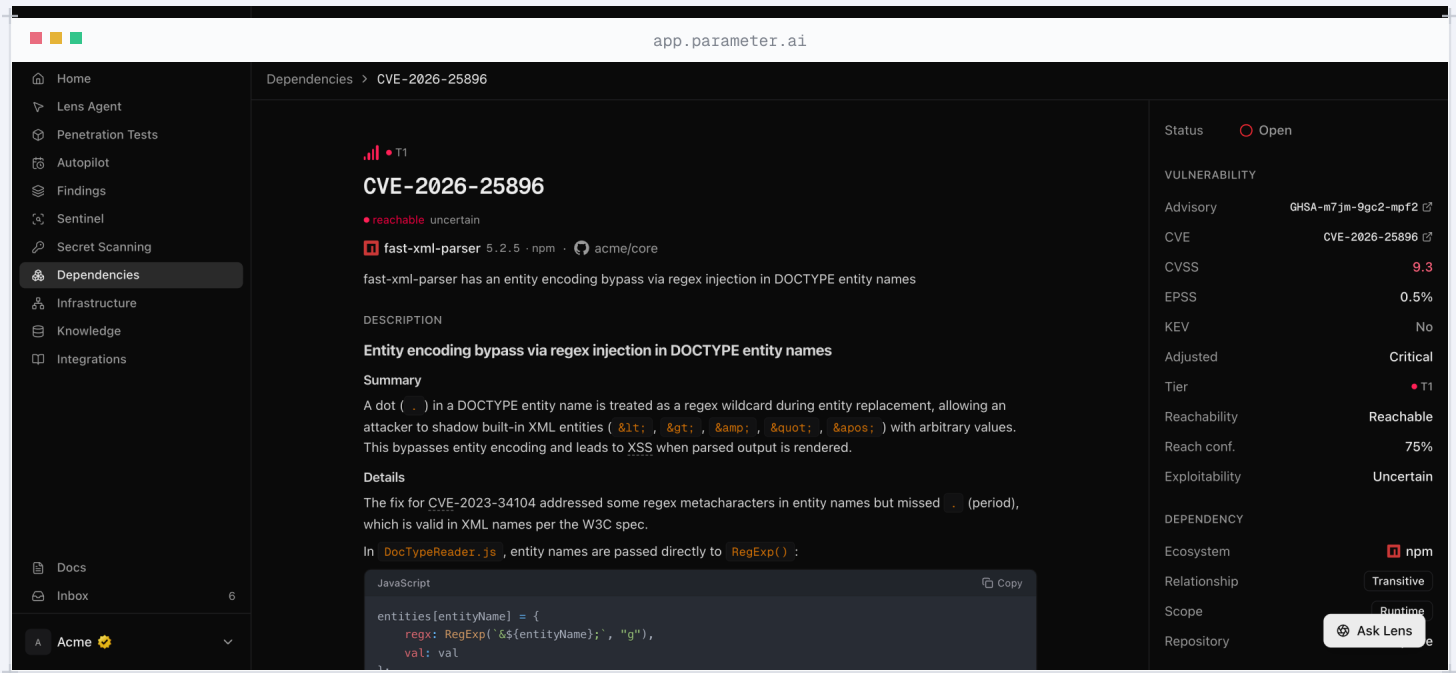


FIG. 02 The Parameter console. Findings from every module land in one ranked queue with proof, reproduction steps and remediation.

[TECHNICAL SPECIFICATIONS]

DEPLOYMENT	SaaS, agentless. Data processed in the US
CONNECTIONS	Read-only, least-privilege. URL + credentials, OpenAPI spec, or source
SOURCE CONTROL	GitHub, GitLab, Bitbucket Cloud
CLOUD PROVIDERS	AWS, Google Cloud, Azure, Oracle Cloud, Kubernetes
ROUTING	Jira, Linear, Slack; fix pull requests against your repositories
ENCRYPTION	In transit and at rest; role-based access control; audit logging
DATA USE	Customer personal data never used to train foundation models
REPORTS	Executive, customer-facing, auditor (SOC 2 / ISO 27001), remediation

SAFETY MODEL

- **Confirm and hold**
Agents prove a vulnerability exists, then stop. No chaining or escalation without your explicit go-ahead.
- **Scoped, never stray**
Agents stay inside the targets you authorize. No wandering into systems that are not in scope.
- **No destructive actions**
No dropped tables, no deleted data, no denial of service. Safe against production by design.
- **Full audit trail**
Every action an agent takes is logged and reviewable, so you can see exactly what happened.

[PACKAGING]

Single App

Fixed scope. One app and its APIs. Whitebox, greybox or blackbox. Same-day results, free re-testing, audit-ready report.

Rightsized

Everything in Single App. Scope set automatically from repos. Multi-service and multi-repo, built for complex platforms.

Continuous

Pentest on every deploy. Everything in Rightsized plus enterprise SLA and support and a dedicated success manager.

[WHY PARAMETER]

- ✔ **Proven, not predicted**

Every finding ships with a working proof-of-concept. Unproven findings are dropped before they reach you.
- ✔ **<1% false positives**

Validation from a clean state keeps the queue short and every entry real.
- ✔ **Top 3 in the US on HackerOne**

Offensive-security pedigree behind the agents, with independent third-party review.
- ✔ **Same-day results**

First findings within 24 hours; most runs finish the same day. No engagement to book.

[NEXT STEP]

See first findings in 24 hours. Connect one application, repository or cloud account and Parameter returns validated, proven findings the same day, with no engagement to book.

ABOUT PARAMETER

Parameter is an AI-powered security platform that continuously finds and validates vulnerabilities before attackers can exploit them. Autonomous agents pentest like a real adversary across your code, cloud and dependencies, with every finding proven. Formerly Hex Security, Parameter is backed by Y Combinator and built by a team that has secured Apple, Google, Microsoft, the U.S. Department of Defense, T-Mobile, Henkel, Epic Games, AT&T and Yahoo.

TRUST AND COMPLIANCE

SOC 2 Type I (Type II observation underway)
HIPAA BAA available
GDPR DPA with SCCs
Data processed in the US
parameter.ai · support@parameter.ai · app.parameter.ai