SCA, SAST AND FIX PULL REQUESTS · DATASHEET

Safeguard

One queue for what you import, what you write, and the fix.

Dependency risk and code risk in one findings queue, with policy-gated fix pull requests for your team to review.

THE PROBLEM

Dependency scanners and code scanners usually report into separate queues. The same issue appears twice, ranked differently, and every report ends as a ticket that someone must turn into a change. The backlog grows faster than the team can work it.

WHAT IT DOES

SCA with reachability

Resolves direct and transitive dependencies, matches vulnerabilities with EPSS and CISA KEV, and checks whether the vulnerable code path is called.

SAST with a trace

Follows untrusted input from source to sink across files, so each finding shows the path and not only a line number.

One findings queue

SCA, SAST and DAST share one model. AutoTriage de-duplicates across scanners, and the queue puts reachable issues first.

Policy-gated fix PRs

Griffin, Safeguard's security model, opens fix pull requests, one repository or in bulk. Your CI runs your tests.

HOW IT WORKS

1. **Scan** — Dependencies, containers and source
2. **Match and trace** — Vulnerabilities, reachability and dataflow
3. **Prioritize** — One queue, reachable issues first
4. **Fix pull request** — Policy-gated, single or bulk
5. **Review** — Your reviewers and your CI decide

YOU DECIDE WHAT RUNS ON ITS OWN

Autonomous fixing ships switched off, with every category on Manual. Each fix arrives as a pull request, so your normal review and CI apply.

CAPABILITIES IN DETAIL

SCA inventory	Direct and transitive components for npm, PyPI, Maven and Gradle, Go, Cargo, NuGet, Composer and Bundler, plus container layers.
SBOMs	SPDX and CycloneDX. Generate, compare and export.
Reachability	Static reachability from a call graph. Classes are reachable, conditionally reachable, unreachable and unknown.
SAST	JavaScript and TypeScript, Python and Java. Sources include request parameters, command-line arguments and file reads. Sinks include SQL queries, command execution and file paths.
Findings	Rule, CWE and OWASP mapping, severity, location and, for SAST, a dataflow trace.
Fix pull requests	Dependency upgrades with lock file updates, configuration fixes and some code patches. One fix, a bulk selection, or one plan to approve.
Categories	Dependencies, licenses, security posture, findings, attestation, provenance, compliance and code quality, each with its own mode.

INPUTS

- Repositories on GitHub, GitLab, Bitbucket and Azure DevOps
- Container images and local directories
- Uploaded SBOMs
- Your policies and the scope you pre-approve

OUTPUTS

- Findings with reachability and dataflow traces
- SBOMs in SPDX and CycloneDX
- Fix pull requests with lock file updates
- Tickets and chat alerts
- An audit trail of what ran and why

INTEGRATIONS AND SURFACES

GitHub · GitLab · Bitbucket · Azure DevOps · Jira · Linear · Asana · Notion · Microsoft Planner · Slack · Teams · Google Chat · Discord · CLI · IDE extensions · CI/CD actions · Webhooks

DEPLOYMENT AND DATA HANDLING

Local runner

The CLI scans on your machine and sends only encrypted results. No open inbound connections; it polls.

Regions and hosting

SaaS in US, EU (Frankfurt) and Gov regions. Private VPC, on-prem and fully air-gapped deployments are available.

Model choice

Zero AI mode runs the platform deterministically with no LLM. Or bring your own model (Claude, OpenAI and others), or run Safeguard models inside your environment.

Access control

SSO (SAML 2.0, OpenID, Google, Microsoft, GitHub), roles and 2FA.

See auto-fix in action

`safeguard.sh/use-cases/auto-fix-vulnerabilities`

Scan the code or type the address. Questions: hi@safeguard.sh

Safeguard

SOC 2 Type I and Type II audited; reports available on request (safeguard.sh/trust). Designed for FedRAMP High.