



BlinkOps Agentic AppSec

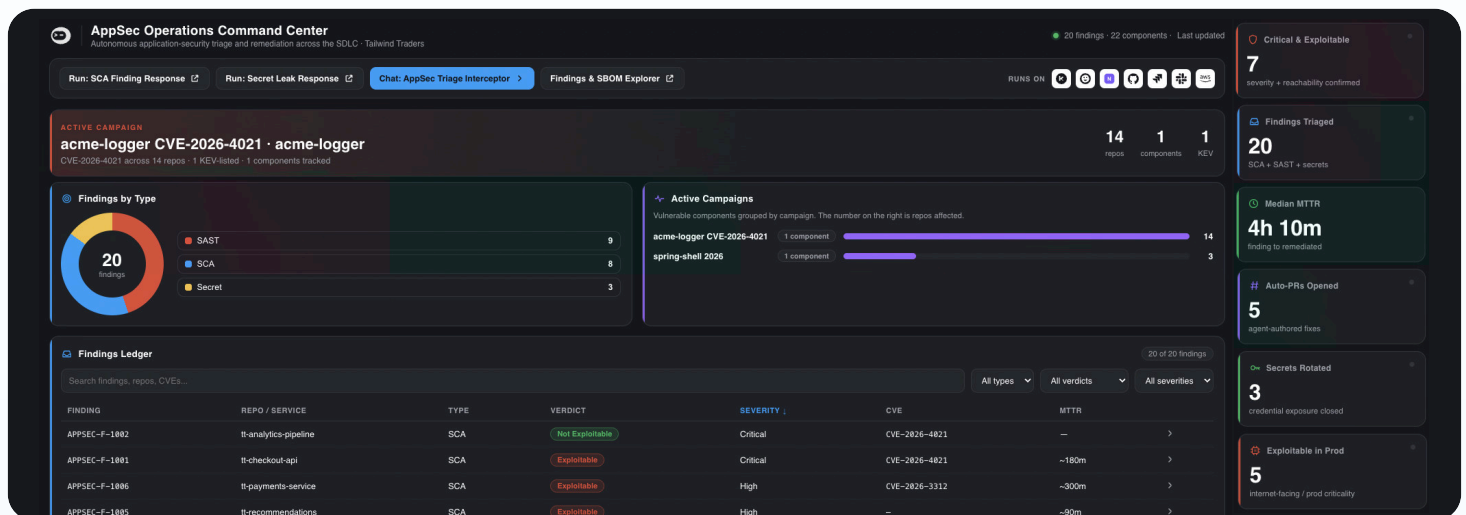
Agentic identity operations across access, lifecycle, risk, and governance

Current State

SAST, DAST, SCA, secret, and container scanners generate more findings than security and development teams can investigate. People must deduplicate results, reconcile severity, validate reachability, identify the owner, explain the risk, and wait for remediation. Developers lose trust in noisy output, critical issues sit beside false positives, and backlogs grow because AppSec tools find vulnerabilities but do not carry the work through to a verified fix.

Blink Solution

With BlinkOps, you can deploy agentic workflows that take findings from every AppSec tool through triage, validation, routing, remediation, and verified closure. Deterministic workflows handle integrations, ownership rules, approvals, repository actions, and pipeline checks; AI reasons over code context, reachability, exploitability, and the appropriate fix. Operators suppress noise, route validated issues to the correct developer, draft pull requests in your conventions, and confirm closure through rescanning.



One AppSec operational view from finding to verified fix.

AppSec Solutions that our customers run

Triage Operator

Takes findings from SAST, DAST, SCA, secret, and container scanners, deduplicates them across tools, suppresses false positives, and reconciles conflicting severity. One underlying issue becomes one governed case, not several disconnected tickets.

Reachability Operator

Examines code, dependencies, runtime context, and execution paths to determine whether the vulnerable code can actually run. Developers see the issues that matter, with the evidence behind the conclusion, before anyone is pulled into remediation.

Routing Operator

Maps each validated finding to the correct application, repository, service, and developer using code ownership, asset inventory, and team context. The issue lands where it can be fixed, already enriched with the information the owner needs.

Fix Operator

Drafts a pull request in your repository conventions, explains the attack path and proposed change, and routes it through existing developer and security approvals. After merge, deterministic workflows trigger rescanning and close the case only when the fix is verified.

Why Choose Blink

Work with top-tier security engineers

Blink's Forward Deployed Security Engineers have experience connecting security findings to the development processes where fixes happen. They help design solutions that work across security, engineering, repositories, and CI/CD —not another isolated AppSec queue.

Agentify work end to end

With more than 30,000 integrations, Blink can ingest findings from SAST, DAST, SCA, secret, container, and cloud security tools; enrich them with code and asset context; and take action in repositories, ticketing systems, developer channels, and CI/CD pipelines.

Customize it to fit your business

Start with pre-built solutions for cross-tool triage, reachability validation, ownership routing, fix generation, and verified closure. Adapt them using Workflow Studio, Agent Studio, Solution Studio, and Case Management to match your repositories, coding conventions, review requirements, and release controls.

Customer Proof

A global media & entertainment company automates AppSec vulnerability remediation with Blink

The company's AppSec team uses Blink to orchestrate its Snyk Code and Snyk Open Source workflows, closing the gap between vulnerability discovery and remediation across its application portfolio. This AppSec work sits alongside the company's broader security automation program with Blink, which has saved an estimated 4,000+ hours and run 600,000+ production workflow executions, all supported by a small team.

About BlinkOps

With BlinkOps, security teams gain an operating layer that spans their entire security stack. From AI SOC, to vulnerability management, GRC, and IAM, Blink automates workflows from triage to remediation. One Agentic Security Operations Platform, infinite possibilities.