



BlinkOps Agentic Vulnerability Management

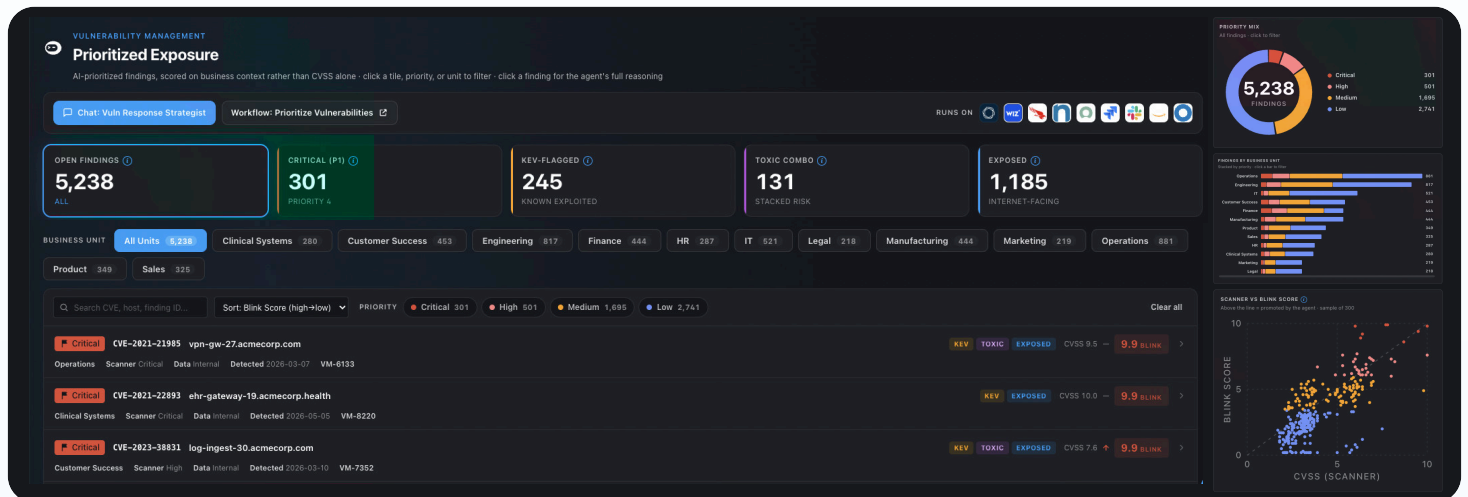
Prioritize real exposure, harden quickly, and verify the outcome

Current State

VM, CSPM, ASM, cloud, and application security tools continuously generate vulnerability findings, but people must determine which exposures matter, identify the owner, select a remediation, coordinate approvals, and verify closure. Critical issues compete with thousands of low-impact findings, patching depends on maintenance windows, and teams often lack a safe way to reduce exposure while they wait. The tools identify risk; the operational work remains manual.

Blink Solution

With BlinkOps, you can deploy agentic operators that carry vulnerability findings through prioritization, routing, hardening, remediation, and verification. Deterministic workflows enforce risk policies, approvals, change controls, repository actions, and rescans; AI reasons over asset criticality, exposure, exploitability, attack paths, and compensating controls. Operators identify the findings that require action, draft patches or hardening changes in your conventions, route them to the right owner, and verify that the exposure is actually closed.



One operational Vulnerability Management view from exposure to verified remediation.

Vulnerability Management Solutions that our customers run

Risk Operator

Identifies affected assets, classifies exposure, and correlates business criticality, exploitability, attack paths, and controls. It narrows thousands of scanner findings to the small number that require action now, with an explanation of why.

Routing Operator

Maps each prioritized exposure to the correct application, infrastructure, cloud, or service owner using asset inventory, environment tags, and ownership records. The finding reaches the right team with remediation context and the applicable SLA.

Hardening Operator

When a patch is slow or unavailable, drafts the appropriate mitigation: infrastructure-as-code guardrails, dependency updates, egress controls, WAF rules, or configuration changes. Every proposal follows your conventions and moves through your approval and change controls.

Verification Operator

Triggers rescans after the change lands, confirms closure across every platform that reported the issue, and reopens the case if the exposure remains reachable. Closure is based on verified risk reduction, not a manually updated ticket.

Why Choose Blink

Work with top-tier security engineers

Blink's Forward Deployed Security Engineers have experience building vulnerability processes across security, infrastructure, cloud, and application teams. They help convert your risk model, ownership structure, and change controls into solutions that move findings through remediation and verified closure.

Agentify the entire security stack

With more than 30,000 integrations, Blink can gather findings and context from VM, CSPM, ASM, cloud, AppSec, asset, and threat-intelligence tools—then take action through ticketing, endpoint management, cloud controls, repositories, CI/CD pipelines, WAFs, and infrastructure platforms.

Get to value fast

Start with pre-built solutions for exposure prioritization, ownership routing, patching, compensating controls, hardening, and verification. Adapt them using Workflow Studio, Agent Studio, Solution Studio, and Case Management to match your risk policies, SLAs, maintenance windows, approval paths, and remediation conventions.

Customer Proof

A global consumer intelligence company replaces its vulnerability management platform with Blink

Blink Deployed Engineers built a custom solution that unified vulnerability findings, asset and exposure context, prioritization, remediation, and verification. The solution allowed the company to retire its standalone Vulnerability Management and Attack Exposure Management platforms and consolidate both functions on BlinkOps. This reduced technology costs, removed operational duplication, and avoided the additional headcount required to manage multiple platforms, generating significant savings while giving the company a solution it can continue to customize.

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.