AI SOC Solution Brief

End-to-end agentic investigation, from alert to resolution

Current State:

Security work arrives at machine speed. Human capacity doesn't scale. Every team is buying AI tools to close that gap, but most of what's on the market solves one stage of the job – triage.
Faster triage is not an outcome. A closed case is. Products that stop at a verdict move the bottleneck from investigation to response instead of removing it. And an agent that can't show how it decided won't be allowed to act on anything that matters.

Blink Solution:

BlinkOps is an AI SOC built to scale across every security workflow. BlinkOps runs the full incident lifecycle on one platform: ingest and triage, enrich and route, investigate to a verdict, execute the response, and close the case. Agents reason. Workflows execute. The harness enforces. Every decision is auditable, every action is one you granted, and autonomy is a dial you widen as trust is earned.

Blink analyzes and acts on any alert from your stack

blinkops

Key Features

30,000+ integrations

Deploy fast. Ingest alerts from any detection source. Pull context from any tool. Execute response back into all of them.

Hybrid architecture

Workflows run the deterministic steps. Agents run the judgment. Reasoning happens where needed, not on every step, which keeps cost bounded and behavior repeatable at scale.

End-to-end investigation

Enrich, route to a specialist agent, build the timeline, verdict with evidence, then act, through containment, remediation, ticketing, or notification – all from one platform.

Case management and Analyst Copilot

One queue, one timeline, one source of truth. History persists, so nobody starts from zero. Analysts ask questions in plain language and execute response from the same place they read the evidence.

Why Choose Blink:

Architecture built for trust

The bounds on our agents are platform controls, not prompt instructions. Agents never hold credentials, never spawn their own agents, and never grade their own verdicts. You set which actions run autonomously and which wait for approval, per action and per use case.

Deep security expertise

The agents, the alert-type logic, the enrichment steps, and the case configuration all ship out-of-the-box, built by people who ran SOCs. You connect your alert sources and the investigations start. Every step it takes is recorded, so when the audit comes you pull one record. You also get Blink Forward Deployed Engineers who extend your team.

Reach beyond the SOC

You already bought the tools. What you're short on is people to run them, which is why half your stack sits underused. Blink puts agentic operators on top of it: the identity workflow, the vuln workflow, the cloud finding, the compliance evidence pull. Same agents, same integrations, same controls as the SOC. The tools you own start doing the work you bought them for.

"This is what security teams have been waiting for. It's not a low-code platform trying to look like automation. It's real logic, built the way we actually work. We saved money on Sumo Logic, killed our Python workers, and started trimming costs on Wiz and Datadog, all because BlinkOps could take over those workflows directly. It paid for itself before we even got the PO in."
— David Grable. Sr. Director of Incident Response.

About Blink:

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.

See BlinkOps in Action

blinkops.com