

BlinkOps Agentic IAM

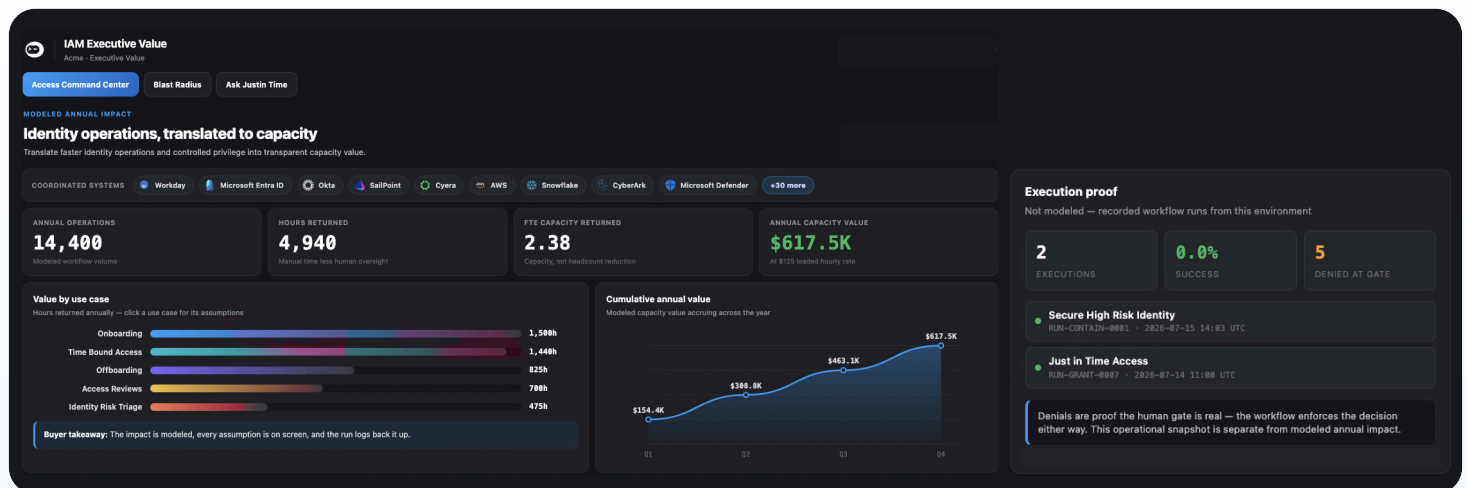
Agentic identity operations across access, lifecycle, risk, and governance

Current State

Identity tools generate access requests, lifecycle events, risk findings, and certification campaigns, but people still do the work between signal and resolution. Teams gather context across systems, interpret policy, coordinate approvals, provision or revoke access, and document every decision. As human and non-human identities multiply, requests wait in queues, deprovisioning misses long-tail applications, and periodic access reviews become costly rubber-stamp exercises.

Blink Solution

With BlinkOps, you can deploy agentic operators across the identity stack you already have. They evaluate access, run joiner-mover-leaver processes, investigate identity risk, and continuously review entitlements. Deterministic workflows handle policies, approvals, integrations, and authorized actions; AI reasoning is used only where context and judgment matter. Every decision and action is recorded, while your team controls when operators recommend, require approval, or act autonomously.



One operational view from identity event to governed access.

IAM Solutions that our customers run

Access Request Operator

Evaluates every request against role, peer access, policy, entitlement sensitivity, and current risk. It recommends whether to approve, deny, or escalate the request with a written justification, then routes the decision through your existing approval model.

Joiner-Mover-Leaver Operator

Provisions access for new hires, updates it when roles change, and revokes it when someone leaves. Deterministic workflows execute the approved change across the identity provider, SaaS, cloud IAM, PAM, data platforms, and long-tail applications.

Identity Risk Operator

Investigates impossible travel, MFA fatigue, privilege spikes, OAuth grant changes, token abuse, and other identity signals. It enriches the event across systems, validates whether the activity is expected, and escalates confirmed risk as a fully documented case.

Access Review Operator

Continuously evaluates entitlements and recommends keep, remove, or escalate. It surfaces toxic combinations, dormant access, and reviewers who are blanket-approving, so certifications become evidence-based decisions rather than periodic checkbox exercises.

Why Choose Blink

Work with top-tier security engineers

Blink's Forward Deployed Security Engineers have years of experience building and running security operations across complex enterprise environments. They bring proven solution designs, implementation expertise, and operational knowledge, not just a platform your team must figure out alone.

Agentify the entire security stack

With more than 30,000 integrations, Blink can gather the data required to make a decision across your existing stack and execute the approved action in the system where the work needs to happen. Your tools get operated, not replaced.

Get to value fast

Start with complete agentic solutions for common security processes, then adapt them to your organization. Use Workflow Studio for deterministic execution, Agent Studio for reasoning, Solution Studio for the end-to-end experience, and Case Management to track every decision and action through resolution.

Customer Proof



As the company grew, onboarding, offboarding, and access requests created manual handoffs across HR, IT, and engineering. Spectro Cloud connected BambooHR to BlinkOps to trigger onboarding, create Jira tasks, provision access, and activate Google Workspace accounts. Offboarding runs the process in reverse, with access revocation, assigned cleanup tasks, and visibility into who had access to what and when.

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.