

# Netskope One AgentSkope

Netskope One AgentSkope is an intelligent layer of the Netskope One platform that enables agentic operations, supporting security and networking operations teams via Netskope AI agents. It acts as an autonomous force multiplier, automating onerous operational processes and freeing up skilled staff to focus on strategic initiatives.

## Quick Glance

- Unlock faster administration and policy management, reduced incident resolution times, and lower manual reporting overhead.
- Reduce mean time to resolution for both network and security operations tasks.
- Reduce alert fatigue by automating triage and clustering related signals into high-priority

Security operations centers (SOCs) and network operations centers (NOCs) face unprecedented challenges: 40% of alerts go un-investigated due to a lack of capacity.

[Software Analyst Cyber Research \(SACR\) 2025](#)

## The challenge

Security and networking teams face significant operational complexity and friction, compounded by understaffing and heavy reliance on repetitive, manual effort across numerous disparate tools. Highly skilled analysts are prevented from focusing on strategic initiatives as a result.

The impact is evident across operations:

- **Security operations centers (SOCs)** are overwhelmed by the sheer volume of alerts, requiring manual correlation and resulting in long incident resolution times.
- **Network operations centers (NOCs)** struggle to troubleshoot increasingly virtualized networks and provide adequate support for a distributed, often highly mobile, workforce.
- **Security policy operations teams** are burdened by complex rule sets and the constant need for manual investigation and analysis to refine them.

## Netskope One AgentSkope

Netskope One AgentSkope, with its Netskope AI agents, acts as an autonomous force multiplier that reduces operational complexity by automating repetitive tasks, correlating data, and shortening administration time.

The foundational AgentSkope infrastructure allows Netskope to build and release agents quickly and efficiently. It creates a common set of security, privacy, and GRC controls to protect customers uniformly across the platform, provides a consistent experience, and tracks and monitors Agent utilization.

## AgentSkope Foundation

Key capabilities include:

- Every agent runs on a unified security and compliance substrate: built in, not bolted on. Each agent utilizes standardized controls enforced across the entire agent lifecycle: GRC, corporate policy, regulatory compliance, AI governance, data privacy, audit, and lineage.
- No variation in security posture between agents; the platform enforces it uniformly. Customers do not need to evaluate compliance per agent; the platform handles it automatically. This simplifies audit readiness, and reduces risk for organizations deploying AI at scale.
- Standardized workflows, a single pane of glass, and predictable agent behavior. One architecture to understand, operate, and govern, reducing complexity.
- Includes secure runtime, thousands of pre-integrated model context protocol (MCP) tools, domain-specific knowledge bases, playbooks, and a full AgentOps pipeline (build, evaluate, deploy, monitor).

---

Netskope AgentSkope reduces the burden on your operations teams, reducing routine tasks and investigations from hours to minutes.

---

## AI Security Operations

Modern SOCs are trapped in an exhausting cycle of manual triage. As thousands of users move data across a huge number of applications, analysts are buried under a mountain of alerts. Everything from data loss prevention (DLP), insider threat, user and entity behavior analytics

(UEBA), and AI risks generates alerts. Because most of these notifications stem from low-risk, routine activities, genuine threats often remain hidden from sight. The volume of these alerts makes it impossible for teams to maintain the pace required by modern business demands.

The AI SecOps agents solve this challenge by mimicking a dedicated analyst, streamlining end-to-end workflows.

**Key capabilities include:**

- **Intelligent triage:** Drastically reduces alert fatigue by deduplicating and clustering related signals into high-priority cases.
- **Autonomous investigation:** Automatically gathers deep forensic context from sources like Entra ID and the Netskope cloud confidence index (CCI), eliminating manual data collection.
- **Rapid differentiation:** Analyzes user identity and device posture to distinguish between accidental errors and malicious intent in minutes, not hours.
- **Unified remediation:** Allows analysts to execute response actions directly from a single interface, removing the need for tool-switching.
- **Continuous learning:** Recognizes harmless patterns to recommend rule refinements, progressively lowering incident volume.
- **Operational efficiency:** Enables leaner security teams to achieve robust protection through automated, high-fidelity security outcomes.

---

The Netskope DLP AI SecOps Agent is a first-of-its-kind solution that automates data protection workflows, by mimicking the actions of a security operations analyst.

---

## AI Network Operations

Network operations teams are frequently paralyzed by the massive volume of telemetry produced by distributed networks. When performance drops, administrators are forced into a manual, time-consuming process of correlating disparate data points to find a root cause. This reliance on manual discovery leads to slow resolution times and a widening skills gap; complex issues can only be solved by senior engineers, leaving the help desk overwhelmed.

Netskope AI network operations agents bridge this gap by acting as an automated troubleshooting partner, transforming raw metrics into actionable intelligence through natural language interfaces and intelligent dashboard and workflows.

### Key Benefits & Capabilities:

- **Automated data discovery:** Leverages large language models (LLMs) to synthesize granular telemetry into clear, conversational insights.
- **Cross-signal correlation:** Connects data across users, devices, and applications to uncover hidden patterns and surface the true source of performance hits.
- **Rapid root cause analysis:** Uses machine learning to instantly determine if a problem stems from the user's device, the local network, or the application provider.
- **Guarded remediation:** Provides logical inferences and contextual advice, offering technicians a clear path to resolution rather than just raw data.
- **Help desk empowerment:** Enables junior staff to resolve sophisticated cases accurately without escalating to senior engineering.
- **Proactive optimization:** Minimizes end-user downtime and maintains peak performance for critical business services through faster, more consistent triage.

## Policy Orchestration

Policy administrators face a daunting reality: Implementing true least-privilege access is often manual, error-prone, and slow. To avoid user disruption, many teams resort to broad IP subnets or wildcards, fundamentally breaking the zero trust model. Over time, this leads to configuration sprawl, cluttering environments with dormant policies and unused segments that are nearly impossible to audit manually.

The Netskope policy orchestration agents streamline this process by automating the discovery, audit, and optimization of Netskope One policy management.

### Key Benefits & Capabilities:

- **Automated zero trust:** Analyzes network traffic to automatically generate granular application segments and policy rules, replacing manual definitions with precision.
- **Configuration housekeeping:** Audits existing environments and rules to identify and remove inactive rules, effectively eliminating technical debt and sprawl.
- **Natural language risk queries:** Allows administrators to query complex risk data across thousands of apps using conversational English.
- **Instant risk assessment:** Provides immediate summaries of application attributes, drastically shortening the time needed to understand security postures.
- **Optimized policy alignment:** Ensures real-time protection policies stay perfectly synchronized with internal risk assessments as the business evolves.
- **Operational efficiency:** Reduces the friction of policy creation, allowing for robust security without the traditional administrative overhead.

BENEFITS	DESCRIPTION
<b>Hassle Free Agentic Operations</b>	Netskope's AgentSkope infrastructure provides a unified architectural foundation, simplifying agentic operations via a shared runtime and integration bus. By centralizing operations, it ensures all agents follow consistent security guardrails, visual design, and share data context. This removes complexity and prevents information silos, replacing disparate tools with a streamlined, cohesive ecosystem.
<b>Centralized Agent Library</b>	The AgentSkope Library is a central, user-friendly hub for Netskope's specialized, AI-driven agents, perfectly matched to operational requirements. Every agent is listed with a detailed description of its unique functions and a brief demonstration video, making it simple for organizations to appraise agent capabilities against their needs.
<b>Automated Incident Triage</b>	Drastically reduce alert fatigue and manual noise, de-duplicating and clustering signals into high-priority cases, by filtering out routine, low-risk notifications. This allows security teams to focus exclusively on genuine threats, transforming an overwhelming stream of data into a manageable, actionable workload.
<b>Rapid Root Cause Identification</b>	Pinpoint performance issues across complex distributed networks by instantly correlating telemetry across devices, networks, and applications. This replaces manual data sifting, so administrators can quickly determine whether a connection issue stems from a local hardware fault, a network bottleneck, or application failure.
<b>Streamlined Configuration Lifecycle</b>	Eliminate technical debt and policy configuration sprawl, continuously auditing to identify dormant policies and unused segments that clutter mature environments. By automating many housekeeping tasks, the system ensures that security rules remain lean, optimized, and easy to audit, preventing the accumulation of error-prone manual configurations.
<b>Workforce Multiplier Effect</b>	Empower junior staff to resolve complex cases by providing guided remediation and autonomous data gathering. Helpdesk technicians can handle sophisticated troubleshooting typically reserved for senior engineers. This bridges the skills gap, improves ticket closure rates, and allows senior staff to focus on high-level strategic initiatives.



Interested in learning more?

Request a demo

Netskope (NASDAQ: NTSK), a leader in modern security and networking for the cloud and AI era, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for the AI ecosystem inclusive of agents, applications, tools, LLMs, people, devices, and data. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications – providing security and accelerating performance without trade-offs. Learn more at [netskope.com](https://netskope.com), [Netskope.ai](https://Netskope.ai), on [LinkedIn](#), and [Instagram](#).