Netskope One Agentic Broker

Data Sheet

Securing the agentic AI enterprise

As organizations transition to applications supporting the Model Context Protocol (MCP)—including AI code editors, chat interfaces, and developer tools—LLMs can now interact directly with data. Netskope One Agentic Broker secures these autonomous, non-human interactions, providing unified visibility and control of AI.

Why is Netskope the best choice?

Available independently, or as a connected capability to Netskope One Next Gen Secure Web Gateway, Netskope enables you to secure your AI ecosystem from user-to-LLM and MCP. Agentic Broker unifies visibility, inventory, and integrated policy to secure the MCP landscape. By embedding security insights into workflows, we prevent data loss and ensure unified, real-time protection across AI environments.

Solving security use cases for autonomous AI

- **Visibility into agentic AI and MCP communications**
  Receive session information including MCP server name, clients and tools, resource and prompt requests, and events including initializations and tool requests for oversight of non-human interactions.
- **Risk assessment for public and private MCP server inventories**
  Using the Netskope Cloud Confidence Index (CCI), evaluate public MCP servers, identifying risky attributes, authentication types, and protocol versions before deployment.
- **Access control and integrated DLP**
  Implement policies to block unauthorized communication to remote MCP servers, and prevent data leaks involving MCP servers through integration with Netskope One DLP.
- **Audit agentic tool interactions**
  Create comprehensive logs of MCP events, including initializations, tool requests, and responses, to provide the auditability essential for proper AI governance and retrospective investigations.

Key benefits and capabilities

Visibility of MCP traffic

Continuously discover remote MCP servers, clients, tools, resources and prompt requests in use within your organization.

Reduce supply chain risk

Evaluate third-party MCP servers and code repositories with comprehensive risk scores to identify the integrations that pose security and compliance risk.

Prevent sensitive data leaks

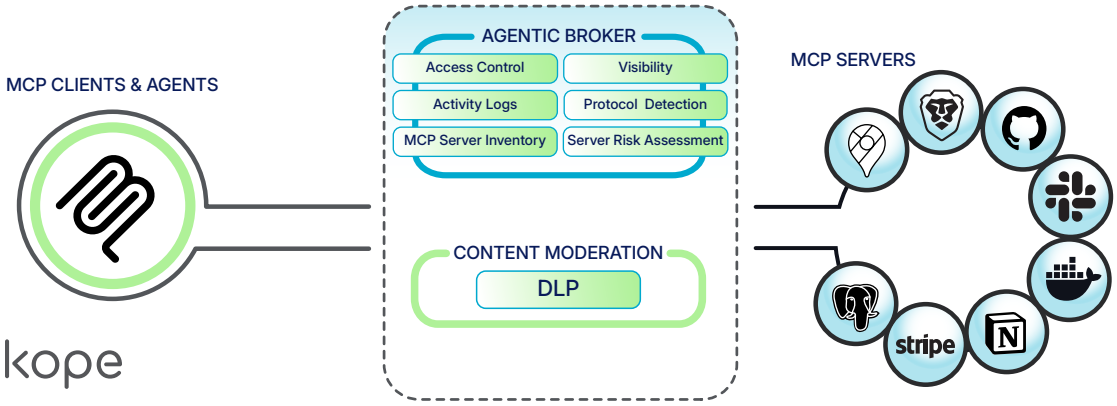
Protect intellectual property and passwords by applying Netskope DLP controls to MCP interactions.

Extend policy controls to agentic AI

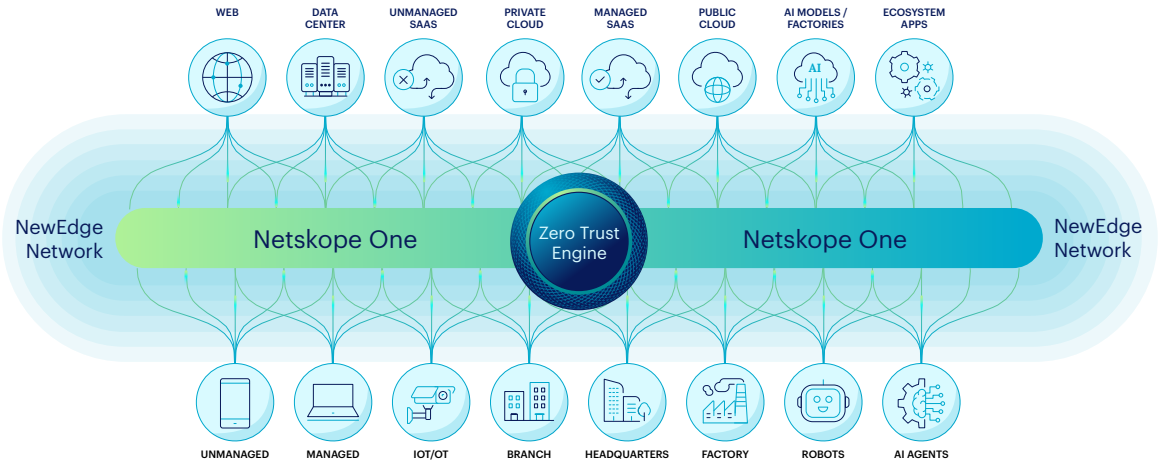
Impose granular policy controls to block cataloged public MCP servers, and MCP server events, with a default block option for all public MCP server use.

> "By 2028, 25% of enterprise breaches will be traced back to AI agent abuse, from both external and malicious internal actors"
>
> – Gartner, Top Strategic Predictions for 2025 and Beyond, 2025

Netskope One Agentic Broker



netskope



The Netskope difference

Netskope provides a unified platform where MCP and agentic AI are secured alongside human identities, addressing the growing complexity of communication between LLMs, tools, and data. The Netskope One Agentic Broker is available as a connected capability to Netskope One Next Gen Secure Web Gateway—adding public MCP security to user-to-LLM controls—or in addition to Netskope One AI Gateway to enable teams to secure agentic AI traffic flows for both public and private AI deployments, enabling you to secure the entire AI ecosystem.

We begin with comprehensive visibility, decoding MCP traffic to identify sessions, tool requests, and responses that bypass traditional security layers. We extend our proven Cloud Confidence Index (CCI) to the world of MCP servers, providing security teams with an inventory of public MCP servers, each analyzed for protocol version, encryption type, and authentication risks. This intelligence feeds directly into our real-time policy engine, allowing for granular control—such as blocking specific tool calls or preventing sensitive data from reaching an untrusted remote server. By integrating Nestkope One DLP and Threat Protection into the heart of the agentic workflow, Netskope ensures that AI agents can reason and act upon enterprise data without compromising the security posture. This integrated approach transforms security into an enabler, allowing the modern enterprise to innovate with agentic AI confidently and at scale while maintaining total control.

BENEFITS	DESCRIPTION
MCP traffic decoding	Netskope One Agentic Broker analyses all MCP-specific traffic passing through the proxy to identify active agents and remote servers.
Netskope CCI risk scoring	Evaluates public MCP servers based on risk profiles, authentication types, and protocol versions for safe adoption.
Real-time Access Control	Enforces granular policies to block or alert on specific MCP communication events and unauthorized tool requests.
DLP integration	Identifies and prevents the loss of sensitive data, such as passwords and intellectual property, during AI interactions.
Non-human traffic monitoring	Tracks autonomous communication between MCP servers, clients and tools. Including resource and prompt requests, and events including initializations and tool requests.
Integrated event logging	Captures detailed session info, initializations, and tool responses for comprehensive audit trails and forensic analysis.
MCP servers inventory	Provides a dedicated category in the Netskope One console App Catalog to help evaluate and approve public remote MCP servers.
GenAI client support	Ensures secure communication for popular generative AI clients, including ChatGPT, Cursor, and VS Code, using MCP.

netskope

Interested in learning more? Request a demo

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. 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.

©2026 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized "N" logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners.

02/26 DS-967-1