Netskope One AI Gateway

Data Sheet

Secure your AI-powered applications

As organizations build AI-powered applications, the primary data flow risk shifts from human prompts to autonomous, app-to-LLM API calls that are often bypassed by traditional security perimeters. The Netskope One AI Gateway is here to secure this modern ecosystem fueling your AI innovation.

Why is Netskope the best choice?

Netskope One AI Gateway secures the critical API traffic between your private AI-powered applications and the LLMs they communicate with, whether they are privately hosted or public. By deploying AI Gateway as a software layer within your environment, it centralizes authentication and traffic management while providing content inspection to protect the autonomous data flows fueling your AI-powered applications.

Centralize authentication, traffic management, and content inspection

- **Build AI-powered apps with confidence**
  Accelerate AI initiatives with a secure inspection point for app-to-LLM traffic controlling authentication and management for APIs and agents accessing sensitive data and tools.
- **Secure agent authentication and logging**
  Ensure only authenticated agents communicate with LLMs via unique gateway tokens. Maintain searchable API logs to ensure no interaction bypasses security controls.
- **Optimize reliability and performance**
  Track AI consumption as API requests and rate limit the volume and frequency of requests to prevent abuse and manage traffic.
- **Integrate full content inspection**
  Unify content inspection by integrating Netskope One AI Guardrails, DLP, and Threat Protection through SkopeAI for centralized policy detections, providing cohesive context and accelerated investigations within a single, unified view.

Key benefits and capabilities

Unify multi-LLM environments

Centralize control of AI models from OpenAI, Gemini, and Claude deployed in private and public infrastructure through a single gateway that enforces uniform authentication and consistent traffic management.

Enhanced SecOps efficiency

Map integrated content inspection detections to MITRE ATLAS and OWASP Top 10 for LLMs. This unified view reduces investigation time and aligns teams with the latest TTPs.

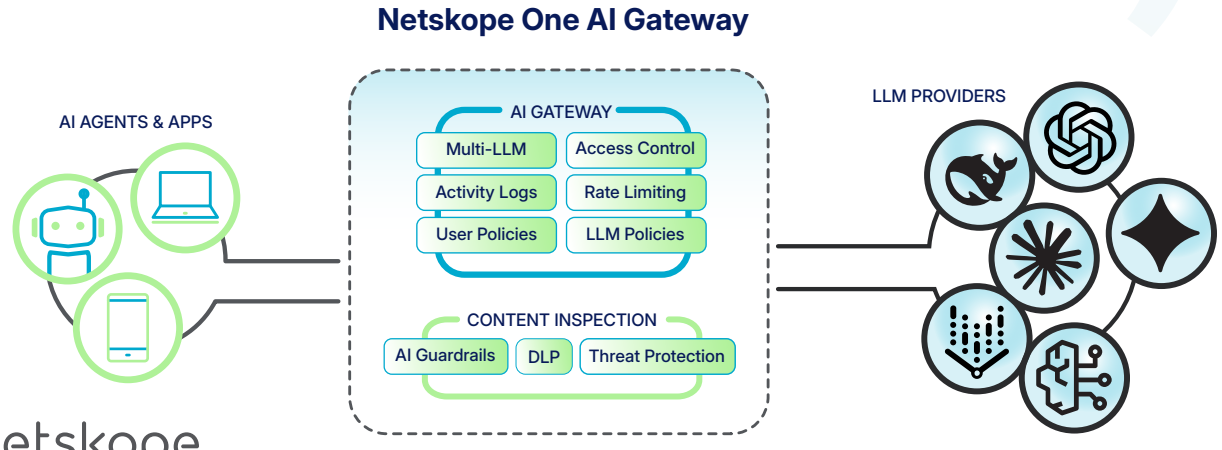
Centralized traffic management and audit visibility

Maintain application stability with rate limiting while capturing searchable audit logs of all API calls to satisfy regulatory compliance and usage monitoring requirements.

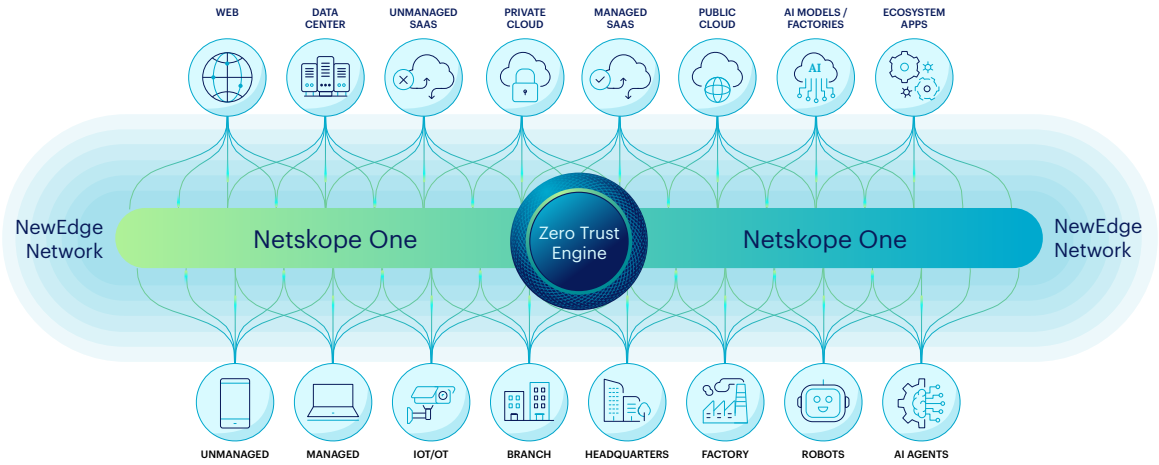
Flexible private deployment

Deploy a lightweight, high-performance virtual appliance directly in your privately-hosted environments, from AWS to VMware ESXi, to enforce consistent security policies everywhere.

> "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



The Netskope difference

Netskope One AI Gateway enables organizations to move faster by providing the visibility and control necessary for modern, agentic AI workloads. While traditional proxies are designed for user-to-app traffic, agentic interactions often occur autonomously between internal systems and LLMs, bypassing standard security. Netskope bridges this gap with a flexible deployment construct—a lightweight VM that sits exactly where your models reside. This architectural advantage allows security teams to take real-time action in private environments, providing a fast lane for AI innovation.

By embedding security directly into the traffic path, Netskope allows you to layer sophisticated policies including granular access control, rate limiting of prompts, with integrations available for Netskope One AI Guardrails, DLP, and Threat Protection for a unified AI security solution. These tools ensure that autonomous agents can invoke tools and access data without risking the exposure of sensitive intellectual property or falling victim to prompt injections. Furthermore, the gateway optimizes the business value of AI by centralizing governance across multiple providers including OpenAI, Google Gemini, and Anthropic Claude. This consolidation simplifies authentication and traffic management to optimize reliability. Netskope ensures that as AI adoption accelerates, your ecosystem stays as secure, governed, and managed as the rest of your enterprise data and network security environment.

BENEFITS	DESCRIPTION
Flexible deployment	Netskope One AI Gateway is available as a lightweight virtual appliance for public cloud deployments in AWS, or private cloud deployments with VMware ESXi.
Integrated software layer	Operates as a software-defined gateway to intercept and govern API traffic between internal applications, autonomous agents, and privately hosted LLMs.
Unified API control	Provides a unified API entry point to manage interactions across multiple providers, including OpenAI, Google Gemini, Anthropic Claude, and custom models following the API schema for these models.
Agent authentication	Ensure only authenticated agents can communicate with LLMs by requiring a valid, AI Gateway-generated token for every request.
Monitoring and searchable logs	Maintains searchable logs of API calls and interaction content to satisfy regulatory requirements and monitor internal usage patterns.

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.

02/26 DS-965-1