

Netskope One AI Gateway (网关)

保护 由 AI 驱动的应用程序

随着企业开始构建 由 AI 驱动的应用程序，主要的数据流风险正从“人工输入的提示词 (human prompts)” 转向自主的“应用到大语言模型 (app-to-LLM)” API调用，这些调用往往绕过传统的安全边界。Netskope One AI Gateway (网关) 旨在保护这一现代化生态系统，为您 AI 创新提供安全动力。

为什么 Netskope 是最佳选择？

Netskope One AI Gateway (网关) 保护 私有的 由 AI 驱动的应用程序 与其通信的 LLM 之间的 关键 API 流量，无论模型是私有部署还是公有的。在您的环境中部署 AI Gateway (网关) 作为软件层，它能集中进行身份验证、流量管理、内容检查，保护自主数据流，这些自主数据流正是推动 由 AI 驱动的应用程序 正常运行和创新的核心动力。

集中进行身份验证、流量管理、内容检查

- **构建由AI驱动的应用程序**: 建立“应用到大语言模型 (app-to-LLM)” 流量的安全检查点，加速AI计划的落地。该检查点可针对访问敏感数据和调用工具的API及Agent (智能体)，实现统一的身份验证与权限管理。
- **保障Agent身份验证与日志记录的安全**: 只有经过身份验证的Agent (智能体)，才能凭唯一的 网关令牌 (Gateway Token) 与 LLM 进行通信。同时，维护可搜索的 API 日志，确保所有交互无法绕过安全控制。
- **优化可靠性与性能**: 把 AI 消耗量作为 API 请求进行追踪，对请求的总次数与频率实施 Rate Limiting (速率限制)，从而防止资源滥用，并高效管理流量。
- **集成全方位的内容检查**: 通过 SkopeAI 集成 Netskope One AI Guardrails (防护栏)、DLP (数据泄露防护)、Threat Protection (威胁防护)，实现统一的内容检查。在单一视图中提供连贯的上下文信息，支持集中化的策略检测，提升调查效率。

优势与功能

统一多模型 (Multi-LLM) 环境

使用单一网关，集中控制部署在私有和公有基础设施中的 OpenAI、Gemini、Claude 等 AI 模型。该网关可强制执行统一的身份验证和一致的流量管理。

提升安全运营 (SecOps) 效率

把集成的内容审查检测结果映射至 MITRE ATLAS 和 OWASP Top 10 for LLM 框架。这统一视图可以缩短调查时间，让安全团队的防御策略“跟上”黑客最新的招数。

集中化的流量管理与审计可视化

实施Rate Limiting (速率限制) 来维持应用程序的稳定性，并记录所有API调用的可搜索审计日志，以满足合规性监管、使用情况监控的需求。

灵活的私有化部署

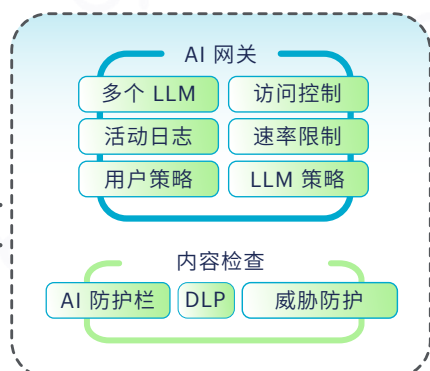
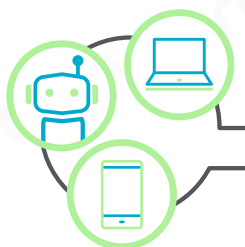
在您私有托管环境中，从AWS到VMware ESXi，直接部署轻量级、高性能的虚拟设备，确保在任何地方都能执行统一的安全策略。

“到 2028 年，25% 的企业数据泄露事件将被追溯到 AI Agent 的滥用，来源既包括外部攻击者，也包括恶意的内部人员。”

来源: Gartner 发布的《Top Strategic Predictions for 2025 and Beyond》

Netskope One AI Gateway (网关)

AI AGENTS & APPS
(AI 智能体与应用程序)



LLM 提供商





Netskope 的与众不同之处

Netskope One AI Gateway (网关) 提供 现代化、具备自主行动能力的 AI 所需的 可视化与控制,助力企业加速发展。传统 Proxy (代理) 主要针对“用户到应用(user-to-app)” 的流量设计,而智能体交互通常在内部系统与 LLM 之间自主发生,会绕过标准安全机制。Netskope 的灵活部署架构填补了这一空白:一个轻量级虚拟机 (VM) 可直接部署到模型所在位置。这种架构优势让安全团队能够在私有环境中采取实时行动,为 AI 创新提供快速通道。

Netskope把安全机制直接嵌入流量路径,让您能够部署分层的复杂策略,包括:精细化访问控制、提示词速率限制 (rate limiting of prompts), 并可整合 Netskope One AI Guardrails (防护栏)、DLP (数据泄露防护)、Threat Protection (威胁防护),形成统一的 AI 安全解决方案。这些工具确保了自主智能体在调用工具和访问数据时,不会面临泄露敏感知识产权的风险,也不会沦为 提示词注入 (prompt injection) 攻击 的受害者。此外,该网关通过集中管理包括 OpenAI、Google Gemini、Anthropic Claude 在内的多个提供商,优化了 AI 的商业价值。这种整合简化了身份验证与流量管理,从而提升可靠性。Netskope 确保在 AI 采用加速的同时,您的生态系统能像企业其他数据和网络安全环境一样,保持安全、受控、可管理。

优势	说明
灵活部署	Netskope One AI Gateway (网关) 可作为 轻量级虚拟设备 使用,部署在公有云 (AWS) 或私有云 (VMware ESXi) 环境中。
集成软件层	作为软件定义的网关运行,拦截并治理 内部应用程序、自主智能体 (Autonomous Agent) 与 私有部署 LLM 之间的 API 流量。
统一 API 控制	提供统一的 API 入口,用于管理跨多个提供商的交互,包括 OpenAI、Google Gemini、Anthropic Claude 以及 遵循这些模型 API 架构的自定义模型。
Agent 身份验证	对 每次请求 强制要求 提供由 AI Gateway (网关) 生成的有效令牌 (Token), 只有经过身份验证的 Agent (智能体) 才能与 LLM 进行通信。
监控与可搜索的日志	维护 API 调用和交互内容的可搜索日志,以满足合规性要求,并监控内部使用情况。

Cyberworld
科明大同

中国区
代理商

公司网站 www.cyberworld.com.cn
业务联系 info@cyberworldchina.com
售后支持 support@cyberworldchina.com



关注公众号



Netskope作为安全与网络领域的领导者,可满足安全团队和网络团队的需求,提供更优的访问体验及基于实时上下文的安全防护,覆盖人员、设备、数据的任意使用场景。数以千计的客户 (其中包括 30+ 家《财富》100 强企业) 信赖 Netskope One 平台、其 Zero Trust Engine (零信任引擎) 及强大的 NewEdge 网络,以降低风险并实现对 云、AI、SaaS、Web、私有应用程序 的全面可视化与控制。既保障安全,又加速性能,两者兼得。

©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-965-1