netskope

Cyberworld 科明大同

Netskope One 平台

解决方案

Netskope One 是一个专门为云环境而设计的平台，提供融合的安全与网络服务，助力企业实现 SASE（安全访问服务边缘）及零信任转型。Netskope One 依托其获得专利的 Zero Trust Engine（零信任引擎）、Netskope One SSE（安全服务边缘）、NewEdge 网络，在为企业筑起坚实安全防线、守护核心资产，更带来了极致的用户体验。

概览

- 通过简化您的 IT 安全与网络架构，最高可降低一半的成本与复杂度。只需使用一个的 Zero Trust Engine、一个客户端、一个网关、一个网络。
- 依托 Netskope 专利 AI 创新技术以及 Zero Trust Engine 无可比拟的精准度，对云端、SaaS、Web用户活动进行解密和解码，从而降低安全风险。
- 依托业界最快、最可靠的网络与安全云基础设施，全面加速混合办公模式落地。我们不仅是监控，更是主动管理从用户到应用及其间所有环节的交互体验。
- 这是一个融合的 SASE 平台，它集成了 SSE 与 SD-WAN 的核心功能，帮助企业构建起有效的零信任架构。

“使用单一供应商的融合SASE平台来应对安全与网络应用场景，实现真正统一的端到端战略。这不仅能降低风险、提升敏捷性、缩减成本、简化运维，还能提供极致的终端用户体验。”

挑战

传统的IT安全与网络架构已无法应对由混合办公普及、云应用、数据无处不在、威胁环境不断扩大所带来的冲击，这些因素会导致策略脱节、为了维持性能而绕过安全防御机制、用户体验不佳，从而增加了企业风险。

网络性能对于顺畅交付精准的安全控制至关重要。传统的IT安全架构把所有流量绕回数据中心的安全栈，这会严重拖慢性能。虽然孤立的云安全堆栈提供了另一种选择，但它们通常存在延迟和服务中断的问题。此外，零散的安全解决方案会导致过多的冗余安全策略，进一步降低员工的访问速度和生产力。

云交付的 SASE 方案是把 IT 安全与网络服务扩展到企业边界之外（从边缘到用户所在地）的最佳选择。然而，由互不关联、独立的 IT 安全与网络服务构成的碎片化 SASE 生态，会增加 IT 团队的运维复杂度，使企业背负更高的成本。

Netskope One 平台

Netskope One 平台通过整合与企业业务需求、优先级、运维时间表相匹配的工具与功能，真正兑现了 SASE 的承诺。这种方法不仅规避了因系统全面大修或购买非必要产品而带来的风险与成本，还赋予了 IT 团队前所未有的可视化，使其能够洞察 SaaS、AI、Web 、私有应用的流量。此外，它提供持续的自适应控制，应用零信任原则来阻断威胁、规范数据访问。

一体化的力量

Netskope One 平台的主要组件：

Netskope Zero Trust Engine (零信任引擎)：
作为平台的核心，该引擎持续收集风险遥测数据，针对所有用户、设备、应用、数据生成广泛的上下文感知。与其他会绕过某些流量或服务的 SSE 产品不同，该引擎能对 Web、SaaS 应用、云服务、私有应用的流量进行解密和解码，从而在最广泛和最深入的层面上实现可视化与防护。

Netskope NewEdge 网络：
Netskope 独一无二的网络专为提供完整的计算型 SSE 和 SD-WAN 而打造。它在全球 75+ 个地区设有超高速数据中心，为各个国家提供本地化体验。它还具备高度灵活性，易于扩展，旨在直接向用户和办公室所在地交付云安全与网络服务，无需在性能上做任何妥协。

Netskope One Client (客户端)：
Netskope 的 端点代理（Endpoint Agent）把远程用户对 Web、云端、私有应用的访问统一起来，同时在端侧融合了数据保护、语音和视频优化功能。它把 SWG、CASB、ZTNA、FWaaS、DLP、SD-WAN 整合在一起，易于使用、轻量化，并具备高吞吐性能。为SASE和零信任场景提供了单一代理（Single Agent）模式，大大简化了桌面管理，提升了用户体验。

Netskope One Gateway (网关)：
提供硬件和虚拟两种形态，支持极其广泛的部署选项，包括：蜂窝网关、从微型到大型分支机构、数据中心、多云环境。它把分散的设备整合为统一的SASE网关，提供多项服务，例如：路由、WiFi、SD-WAN、应用防火墙（App FW）、入侵防御系统（IPS）、物联网设备智能识别（IoT Device Intelligence）、数字体验管理（DEM）、边缘计算，并可无缝接入 Netskope One SSE。

Netskope One Orchestrator (编排器)：
作为 Netskope One 平台所有组件的统一策略管理中心。该 100% 云端控制台把分支机构、远程站点、多云环境及远程用户的 SSE 和 SD-WAN 的统一管理进行整合，并内置 SD-WAN 控制器，实现控制面与数据面的分离。

具备上下文感知的持续自适应信任可降低风险

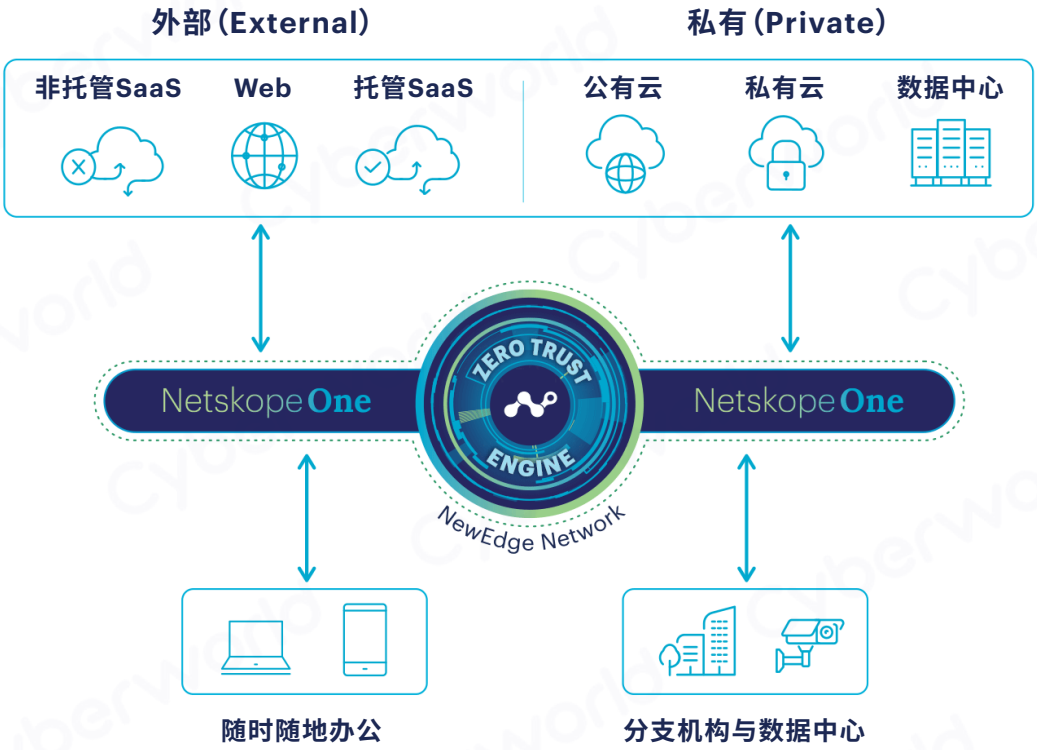
传统的网络与安全架构依赖于典型的“城堡加护城河”式防御，默认信任已授权用户，允许其在企业网络内自由活动并访问数据。零信任安全模型摒弃了这种传统的方法，强调任何用户、设备或应用在未经验证之前都不应被默认信任。 Netskope Zero Trust Engine 在此基础上进一步发展，引入持续自适应信任（continuous adaptive trust）机制，利用上下文，实时判断在用户、应用、数据、其他多种因素不断变化的情况下，应当授予的访问级别。

实现这一能力的关键在于 Netskope Zero Trust Engine。它通过采集用户交互全链路的实时风险数据，利用这些上下文信息，对所有云端、Web、私有应用实施最具适应性的单次并行（Single-pass）策略控制。让 IT 管理员能够实时对每一项交互做出风险管理决策。

这对 IT 管理员来说是一个重大变化，他们过去习惯了传统的“允许或阻止（allow or block）”二元访问选择。通过更先进、更精细的零信任执行方式，IT管理员可以使用多种措施来降低风险，包括：允许流量、阻断交互、在用户操作过程中实时给予引导（Coaching）、要求用户进行身份验证、要求用户为某些操作提供理由、将该访问与其他操作隔离。

持续自适应信任标志着策略控制告别了简单粗暴的“允许或拒绝”二元法，转而提供一种更先进、更精细的零信任执行方式。

Netskope One



以闪电般的速度与可靠的弹性，提升业务敏捷性

Netskope One 通过 Zero Trust Engine 极速的单次并行（Single-pass）检测架构，结合 NewEdge 网络可靠的弹性与高性能，提升了业务敏捷性和生产力。

Netskope 的单次并行架构旨在把端到端延迟降至最低，平均扫描时间低于 15 毫秒。这一机制通过仅对流量进行一次解密，而不是由各个安全服务多次解密来实现。此外，单次并行架构还让 Netskope One SSE 产生的安全事件在一个统一的控制台中呈现。

NewEdge 网络旨在以极低延迟，把全球各地的数百万用户、办公室、分支机构连接到 Netskope 全套 SASE 服务。客户在每个数据中心都能享受“全算力”支持，并通过Netskope One Client和Netskope One Gateway等灵活的部署方式，把流量引导至 NewEdge。Netskope One 还叠加了数字体验管理（DEM）服务，用于监控、测量、分析从客户端到应用的用户体验与性能，包括逐跳（hop-by-hop）可视化及平台处理延迟。

Netskope One 平台通过行业领先的服务级别协议（SLA），为其云安全服务提供保障，确保客户获益于强大的“以数据为中心”的安全防护，无需忍受传统硬件设备常见的性能折损，也不会面临公有云或虚拟入网点（PoP）那种不可预测的性能表现及额外延迟。

使用人工智能/机器学习（AI/ML）创新技术，实现高级数据与威胁检测

网络犯罪分子对 AI 的使用呈指数级增长，令大多数企业的网络防御措手不及。因此，当下的数据安全与威胁防护方法，也需借助 AI/ML 来应对新兴的网络安全挑战。Netskope作为网络、云端、数据安全转型的领导者，负责任地运用 AI/ML 技术来保护数据、抵御威胁。

Netskope 在 SASE 架构中率先实现了简洁而强大的云数据保护。不同于传统的数据安全解决方案依赖正则表达式、关键词和字典来识别敏感数据，Netskope One 平台自动应用 3,000+ 种先进的 AI/ML 数据分类器，以及 42 项获得专利的 AI/ML 检测技术，对存储在云端的业务文档进行高精度的恶意软件、钓鱼攻击、敏感数据的检测与分类。此外，Netskope 的图像检测 AI/ML 模型运用深度学习算法，识别和分类嵌入在图像文件及图像密集型文档中的敏感数据。

除此之外，自公司成立之初就已存在的 Netskope SkopeAI 创新技术，释放了 AI/ML 的强大力量，以高可靠性和高速率检测并保护新的非结构化数据。它通过普及现代数据与威胁检测技术，以符合 AI 时代所需的速度运行。

核心能力包括：

- SkopeAI 的用户与实体行为分析 (UEBA) 采用 65+ 个训练模型和 130+ 个检测器，通过内联与 API 检查，区分正常的行为模式（基于内部基线）与来自恶意内部人员或外部威胁向量的异常行为。

- SkopeAI 的威胁防护功能能够拦截各种具有规避性的未知威胁，包括：AI 生成的威胁、多样化攻击、多态恶意软件、新型网络钓鱼域名、零日漏洞威胁、恶意网页内容。

- SkopeAI 在保障生成式人工智能（GenAI）方面展现了最前沿的进展，助力企业安全地启用相关应用；通过 ML 辅助的发现与风险分类技术，对运行中的 GenAI 应用提供业界最广泛的分类与可视化。

- SkopeAI 还提供了多种强制执行选项，以阻止敏感数据上传或发布到 ChatGPT 等 GenAI 应用中；同时，它还能提供实时引导（Coaching）警报，告知用户相关安全策略，从而最大限度地减少重复性的风险行为。

优势	说明
降低安全风险	根据 Netskope 客户的反馈，得益于 Netskope One 平台能够快速定位并管控云服务及网站上的各类活动，从而保护敏感数据、阻断威胁，他们发现由外部攻击导致的严重数据泄露风险降低了 80% 。
更严密的整体安全防护	除了降低风险，使用 Netskope One 的安全管理员还反馈了多项能够强化整体安全性的益处，包括：瞬间识别数千个影子 IT SaaS 应用、跨越地理位置限制管理所有终端、显著减少安全策略数量、实现租户级别的策略对齐。
提升业务敏捷性	使用 Netskope One 的客户报告称，由于用户体验显著改善、应用性能大幅提升、对 IT 的整体满意度增加，远程用户连接服务所需的时间缩短了 50% 。
高投资回报率	通过淘汰低效的传统工具并采用 Netskope One，安全管理员在三年内实现了 104% 的投资回报率。这主要得益于硬件成本的降低、运维效率的提升、安全风险的减少。
降低复杂度	安全管理员表示，对多云环境进行持续审计变得异常简单，并且能够自动修复那些因疏忽导致敏感数据暴露的安全误配置。
更快的价值实现速度	客户表示，Netskope One 在保护与速度之间提供了恰到好处的平衡，把实现安全的平均时间从数月甚至数年缩短至数天，大大加快了安全数字化转型的价值实现进程。
加速网络转型	在网络层面，Netskope One 的客户报告称，他们的网络转型显著加快，因为能够消除与传统 MPLS WAN 以及关键 SaaS 或云服务提供商的专用连接相关的费用，并通过引入诸如 Netskope One SD-WAN 等网络创新来实现。
重新分配人力资源	Netskope One 的客户表示，他们能够在更少的人力支持下、更快地部署更多席位，超出了预期，从而使 IT 团队能够将精力重新集中在其他战略性举措上。

公司网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

关注公众号

Netskope 作为全球 SASE（安全访问服务边缘）领域的领导者，运用零信任原则与人工智能/机器学习（AI/ML）创新技术，在保护数据安全并抵御网络威胁的同时，实现了安全与性能的极致平衡，无需任何妥协。成千上万的客户信赖 Netskope One 平台及其强大的 NewEdge 网络，以降低风险并获得对云端、Web、私有应用程序活动的卓越可视化。