netskope

Cyberworld 科明大同

Netskope One 安全服务边缘 (SSE)

解决方案

Netskope One Security Service Edge (SSE，安全服务边缘) 平台助力企业数字化转型。无论终端用户使用何种设备或身处何地，都能体验敏捷高效的办公模式。集成的自适应零信任控制，可降低数据与云端风险。依托融合的云原生解决方案，减少运营成本与复杂性，从而推动业务价值的实现。

概览

- 在Web、应用、用户、数据层面，提供最全面的可视化和上下文，以支持业务与风险洞察。
- 为 IaaS、PaaS、SaaS 提供安全的Web和云访问，强制执行企业安全策略、合规要求、最佳实践。
- 在 Web、SaaS 应用、云服务、私有应用中检测并缓解威胁。
- 在远程员工访问Web、云端、私有应用时，实现连接与安全保障。
- 在Web、云端、电子邮件、私有应用、设备中识别并保护敏感信息。

SSE技术以云为中心的方式来强制执行安全策略，让员工在任何时间、任何地点都能安全连接。[1]

[1] 信息来源：Gartner 发布的《4 Must-Have Technologies That Made the Gartner Hype Cycle for Cloud Security》

挑战

当下的企业环境正在经历“倒置效应(inversion effect)”：应用、用户、数据不再局限于企业内网，而是广泛分布在外部；配合现今的混合办公常态，必须重新审视 IT 安全及网络架构。目前，企业内的云应用流量已经盖过了传统 Web 流量，而那些旧有的、依赖本地安全设备访问数据中心的方案，在面对这种变化时显得力不从心，不仅产生了大量监控盲区，还增加了系统的复杂性。

这些挑战要求一种全新的云安全方法，能够在访问、安全与性能方面提供企业数字化转型所需的极简与敏捷，同时保护关键数据资产并践行零信任原则。它们还要求一种基于融合的云原生架构的智能解决方案，摒弃那些可能被宣传为“SSE”却在功能上存在局限的过时产品和传统方案。

Netskope One SSE

Netskope One SSE 快速且易于使用，在任何地点保护您的员工与数据。Netskope加速性能，降低风险，提升对云端、Web、私有应用活动的可视化，减少与网络安全相关的成本与复杂性。在您的 SASE 旅程中，借助“以云与数据安全为先”的 SSE，您将随时做好应对一切挑战的准备。

Netskope 化繁为简，提供强大的集成

Netskope One SSE 为客户提供对所有流量的深度可视化，包括Web、SaaS应用、云服务、私有应用。Netskope对80,000+个云应用进行实例感知（instance awareness）和画像（profiles），从而提供精细化的活动控制，助力客户保障远程办公安全，并确保云的成功采用。Netskope One SSE 把这些强大的访问控制、威胁防护、数据保护能力，以简洁直观的方式交付，便于客户轻松使用。客户可以针对 Web、私有应用、SaaS应用（无论企业已批准或未批准），灵活采用正向代理（forward proxy）或反向代理（reverse proxy）模式进行部署。所有功能均通过统一控制台进行管理，并由 Zero Trust Engine（零信任引擎）强制执行安全策略。

卓越的云安全能力

Netskope 卓越的安全能力在应用、用户、数据层面提供最深入的可视化与精细化上下文，并以 Netskope Zero Trust Engine 作为智能 SSE 服务的基础。在这一基础之上，独特的功能构建了有效 SSE 运作所必需的结构与属性。

- 由人工智能/机器学习（AI/ML）驱动的Web与云应用分类能力，以及对私有应用的识别能力，实现强大而精细的策略管控。
- 云应用实例感知，即 Netskope 专利技术 TrueInstance，实现了对应用实例的大规模动态检测。这对数据保护及预防云端威胁很重要。
- 通过 内联（inline）与 API 的应用覆盖，在个人实例与受管实例之间实现最大化的可视化与控制，适用于任何应用或云服务（例如：支持 AWS 中 250+ 项服务，细化到实例级别）。
- 基于ML的信任评分机制，针对云应用的 Netskope CCI（Cloud Confidence Index，云信任指数）、针对用户的 Netskope UCI（User Confidence Index，用户信任指数），能够捕捉异常与变化，进而触发自适应策略控制和自动化的调查工作流程。

凭借 Netskope Zero Trust Engine（零信任引擎）提供的丰富上下文，Netskope One SSE 在所有云端、Web、私有应用中，执行最具适应性的单次并行（Single-pass）策略管控，在简化运维的同时，实现更强大的风险管理。

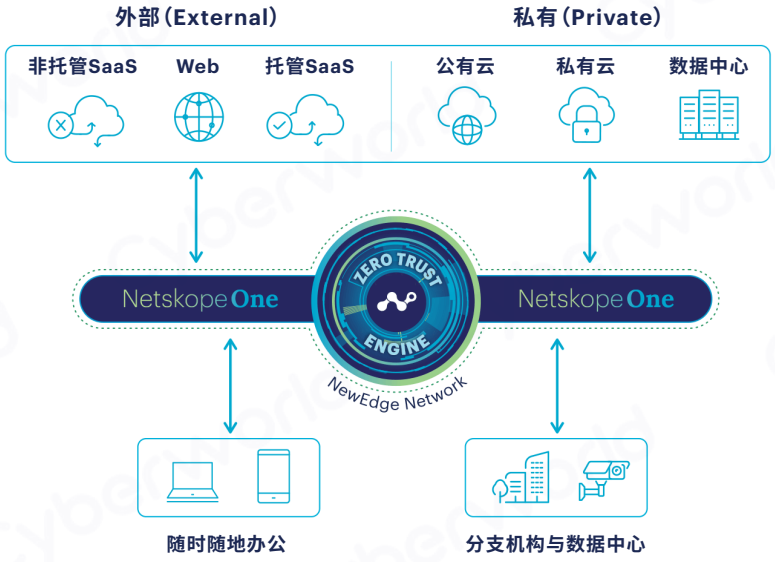
持续自适应控制，应用零信任原则

Netskope 持续自适应控制（Continuous Adaptive Controls）把零信任原则应用于 SASE、多云和混合架构，以实现访问控制、威胁防护、数据流动管理。对应用、应用实例、应用活动的明确权限定义、精细化访问控制，可有效减少针对主要威胁向量的攻击面，例如：高风险云应用、云钓鱼攻击、通过个人或经批准的企业应用实例（如 M365 或 Google Workspace）造成的数据泄露。在 Zero Trust Engine 的驱动下，Netskope One SSE 持续执行数据流动策略与威胁防护。针对由于无意或未经批准的访问、应用内部或应用间的数据流动，提供实时用户引导（inline user coaching）、额外的身份验证（step-up challenges）。

Netskope是最早意识到云原生威胁及数据窃取紧迫性的供应商之一，这些威胁往往利用受管应用（managed applications）的个人实例及公有云环境进行攻击。Netskope高级威胁防护（advanced threat protection）为 Web、SaaS、IaaS、所有端口和协议提供业界领先的防御能力，能有效缓解漏洞利用带来的风险，并通过实时策略响应选项，大幅减少内部用户或实体行为所带来的监控盲点。

实时用户引导（inline user coaching）有效减少因用户无意操作带来的风险，例如：把文件分享至个人应用实例、或上传至其他业务部门的应用实例（其中可能包含未获授权访问敏感数据的第三方用户）。先用精细化控制来缩小攻击面，再用实时引导（inline coaching）减少用户误操作带来的干扰，最后让环境更“干净”，以便有效实施高级数据泄露防护（Advanced DLP），从而保护企业最重要的资产：敏感及关键的业务数据。

Netskope One



领跑云数据安全防护

Netskope是云端数据保护领域公认的黄金标准。它开创了适用于多云和混合环境的现代数据保护技术，既简易又强大。与基于硬件设备的传统DLP所带来的僵化体验不同，Netskope为SASE架构创新了云数据保护方案，具备实现敏捷安全所需的大规模覆盖、精准识别、高精度管控。Netskope应用了AI/ML技术，在规模、效能、自动化方面发挥重要作用，帮助企业在云端发现应用、检测与分类数据，从而保护关键业务数据。

如今企业流量平均有20%是图像及图像中的文本，这进一步增加了数据安全的复杂性。Netskope基于 AI/ML 的图像分类技术采用深度学习模型，可识别护照、身份证、信用卡、社会保障卡等敏感图像。无需提取图像中全部文本，即可更快、更准确地检测图像。

Netskope还支持屏幕截图检测，这在远程办公环境下尤为重要，特别是当处理敏感数据的员工截屏时。借助这一功能，安全团队可大规模检测特定员工群体的截屏行为，同时降低图像匹配的误报率。

Netskope 还提供基于 AI/ML 的文档分类器，可识别源代码、专利、合同、简历、协议等。

兼顾业务生产力与敏捷性
打造流畅的用户数字化体验

Netskope 凭借其 NewEdge 网络和私有云基础设施，以极速的用户体验和优化的应用性能，提升了业务生产力与敏捷性。

通过与Web、云、SaaS供应商进行广泛的对等互联，结合快速、低延迟的流量接入，以及Netskope在全球59+个地区提供边缘计算能力，实现了实时、内联的安全流量处理，更贴近用户需求。Netskope以业界领先的服务级别协议（SLA）为其云安全服务提供保障。

通过 Netskope 灵活的部署选项（包括 Netskope One Client）以及与现有网络投资（如 SD-WAN）的集成，客户能在不牺牲性能的情况下，获得强大的数据中心安全保护，避免传统设备式方案或依赖公有云不稳定性能的竞争替代方案所带来的折衷。

客户反馈："通过NewEdge提升用户体验是Netskope使用过程中有较价值的部分之一。"通常可见应用性能提升 50%，在某些案例中，核心SaaS应用的性能提升了 6 倍。Netskope 还提供数字体验管理（DEM），用于监控、测量、调查 NewEdge 与数据中心安全服务的性能。

优势	说明
通过融合的云原生SSE解决方案，降低成本与复杂性	**Netskope One SSE 解决方案集成于单一平台：** • 云原生下一代安全Web网关 (NG SWG)、多模式云访问安全代理 (CASB)、零信任网络访问 (ZTNA)。 • 更多融合功能：数据泄漏防护 (DLP)、高级威胁防护 (ATP)、云防火墙即服务 (FWaaS)、远程浏览器隔离 (RBI)、用户与实体行为分析(UEBA)，所有功能均在单次并行处理架构（single-pass architecture）中实现，由统一平台交付、单一控制台管理、统一的零信任策略引擎驱动。 • 完整的威胁与数据保护，结合内联流量分析与云API交互，实现对敏感数据的感知、实时策略执行、静态数据检查。 • 基于云级扩展设计（Cloud-hyperscale）的云原生基础设施NewEdge，提供高弹性与高可用性，并以业界领先的SLA保障正常运行时间、可用性、低延迟。
提供混合办公用户体验，提升企业敏捷性	**混合办公（Hybrid Work）需要为所有用户和办公地点提供直接访问：** **随时随地办公模式：** • 直接访问云端、Web、私有应用。 • 在应用与服务之间开放协作。 • 以快速、全球化的用户体验，提升生产力。 **简化并转型分支机构网络与安全：** • 通过分支机构的直接访问，降低回传（Backhaul）成本。 • 无论用户身处何地，均在云端执行一致的安全控制。 • 采用多样化的流量引导方式（例如在分支机构部署SD-WAN），实现低成本的区域内连接。
重新定义风险管理与数据保护	**现代化风险管理，为所有用户和数据，提供高级数据保护与威胁防护：** **高级数据保护（Advanced data protection）：** • 基于 AI/ML 的检测，实现最精准、最全面的覆盖。 • 识别新型风险中的敏感数据，例如：识别图像与屏幕截图。 • 对数据流动进行精细化控制，包括个人与企业应用实例之间的数据传输。 • 态势管理，确保正确的访问与权限设置，减少因错误配置、配置偏离安全基线带来的威胁，并确保符合监管要求。 **SSE 架构下的威胁防护：** • 应对 Web 与云端传递的威胁。 • 自动化双向 IOC（入侵指标）共享，获取最新威胁情报。 • 在执行前进行分析，对文件进行解包与去混淆，并在沙箱中检测。 • 应用基于 ML 的分析，包括识别恶意 Office 文档。 • 使用远程浏览器隔离 (RBI)，防护高风险网站。 • 识别行为异常，评估风险与内部威胁。 • 在所有出口端口与协议上应用防火墙控制，覆盖用户与办公地点。
简化运维	**把安全功能整合并迁移到云端，简化运维：** **将 IT 整合至云端：** • 把 Web、云、私有应用的关键安全服务统一到云原生安全平台。 • 通过消除硬件设备、多重软件与支持许可、在云平台上整合安全服务所带来的资源效率，降低总拥有成本。 • 通过对云应用与 Web 的单次并行检测（single-pass inspection），提升安全效能，阻止威胁与数据泄漏。 **提升并简化运维：** • 采用 SSE 的单次并行策略方案，可实现高达 10 倍的策略简化。 • 利用实时用户引导（inline user coaching）与策略微调，优化安全运维流程。 • 提供动态可视化分析，实现实时深入调查与分析。

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