netskope

Cyberworld 科明大同

Netskope One Data Security

解决方案

在 AI 时代，数据安全比以往任何时候都更加至关重要。Netskope One 提供一体化数据安全解决方案，无论数据存储在何处、如何流动，都能为其提供保护。Netskope One Data Security 整合了 数据安全态势管理 (DSPM) 与具备上下文感知能力的 数据泄露防护 (DLP) 技术，旨在降低数据风险、确保合规、实现数据隐私保护，同时降低成本与复杂性。

概览

- 在发现并保护各处数据的同时，最大限度地降低数据外泄风险。
- 通过防止敏感数据泄露及管理流经生成式人工智能 （GenAI） 基础设施的数据，确保 GenAI 的安全使用。
- 通过数据发现、分类、访问控制和使用风险分析，全面管理数据安全态势。
- 通过内置的合规框架和自动化策略执行，满足 GDPR、HIPAA、CCPA 等法规要求。
- 通过一体化数据安全平台，实现资源整合。Netskope提供“一个引擎、一个客户端、一个网关、一个网络”的极简架构。

“网络安全是我们的竞争差异化优势，它帮助我们吸引新客户，尤其是那些高度重视强大数据保护的行业客户。”

CISO, Global Services Industry

挑战

云计算和分布式办公模式在提升生产力的同时，也带来了严峻的数据安全挑战。传统的、基于边界的安全模型 (perimeter-based security model) 已不再奏效，企业迫切需要一种全新的方法，来保护散落在各种地点和设备上的敏感数据。

GenAI 的兴起进一步增加了复杂性，因为这类工具极易导致无意间的数据泄露。为了应对这些不断演变的威胁，企业必须采取多维度的数据安全策略，在最大程度降低风险的同时，确保护敏感信息的安全。

解决方案：Netskope One Data Security

Netskope的一体化数据安全解决方案可保护云端应用、端点、协作工具中的敏感数据，其保护范围远超传统的安全边界。

Netskope One Data Security 在单一平台中融合了 DSPM 与 DLP 技术，在提升可视化与控制能力的同时，降低了成本与架构复杂性。

这一全面的防护可帮助企业预防数据泄露、未经授权的访问、数据丢失，确保合规、维系客户、保护知识产权。

全方位发现并保护各处数据

随着数据在企业环境中激增，“数据究竟在哪里?”要回答这一问题变得愈发困难。Netskope One 通过对所有数据提供深度洞察，帮助企业实现全面的数据保护与控制。无论数据位于何处，该方案能让企业对敏感数据在内的所有信息拥有完整可视化与控制。这一全面的解决方案涵盖了对结构化数据、非结构化数据在静态存储、传输中、使用状态下的安全防护。防护范围覆盖所有通道，包括：Web流量、电子邮件、云应用(SaaS)、端点、私有应用、IaaS基础架构，确保整个数字化生态系统获得一致的安全保障。核心能力包括：

- 使用基于 API 的管控技术，自动发现 Microsoft 365 和 AWS 等受管云服务中静态存储的敏感数据。
- 持续扫描 IaaS 存储服务（例如 AWS），监测数据流动或意外暴露。
- 使用内联控制 (Inline Controls) 技术，检测并监控数千个云应用、服务及实例之间传输中的动态数据。
- 在云应用和实例之间查看、控制数据传播，并结合云应用风险、用户风险进行分析，无需依赖租户限制。
- 无论用户位于办公区内，还是远程办公，也无论其使用浏览器、同步客户端，还是移动App，皆可实现行为透明化。
- 通过检查元数据、隐藏字段、注释信息，超越传统的内容分析。

无论数据存储在何处、如何流动
Netskope 始终保驾护航

您可以回答这 4 个问题吗?

- 您的数据在哪里?
- 您拥有哪些类型的数据?
- 谁可以访问这些数据?
- 数据交互的风险有多大?

确保 GenAI 的安全使用

随着企业越来越多地使用GenAI来实现业务目标，安全负责人正努力保障企业数据安全。这一趋势毫无放缓迹象，我们必须正视这一新现状带来的安全隐患。如今，企业可以在不牺牲防护或性能的情况下推动创新。Netskope One 为各类 AI 赋能的SaaS应用提供无与伦比的可视化与精细化控制，助力安全团队监控访问行为、执行数据保护策略，并严防敏感信息外泄。核心能力包括：

- 通过实施控制、强制执行安全 API 连接、SaaS 防护，实现 GenAI 应用的安全部署。
- 在GenAI工作流程中，通过监控敏感数据的使用情况，并使用数据分类与数据脱敏技术，实现数据防泄漏。
- 使用AI威胁防护进行威胁检测与响应，主动解决漏洞，揭示内部威胁。
- 通过自动化、实时的指导及强制执行数据使用策略，实现策略管控与用户引导。
- 让GenAI的使用符合行业特定法规，维护审计追踪，整合安全能力，从而实现合规与风险缓解。

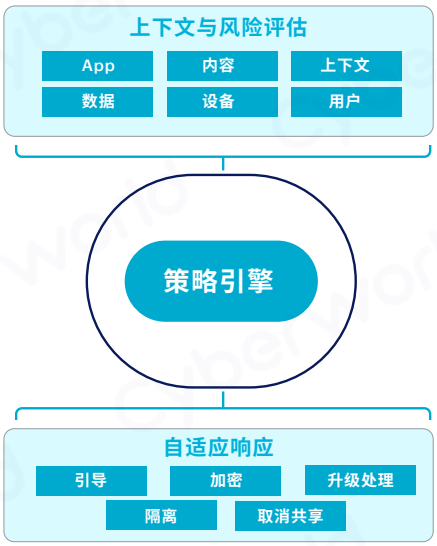
一体化数据安全

平台化数据安全方法，兼具全面性、有效性、高效性。

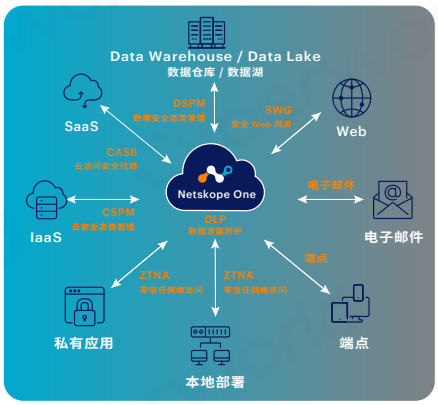
一次分类 (Classify Once) 技术

- 3,000+ 种用于标识和处理不同语言数据的标识符
- 40+ 种法规与合规模板
- 30+ 个 人工智能/机器学习（AI/ML）模型
- 基于内存的高速实时处理架构

实时访问与策略控制



保护您的数据
无论它存储在何处、如何流动



一体化数据安全策略
适用于静态与传输中的结构化数据
及非结构化数据

管理数据安全态势

随着数据环境日益复杂、网络威胁不断演变，在云端与本地系统之间构建一体化数据安全体系的需求愈发迫切。您的数据在哪里?您拥有哪些类型的数据?谁可以访问这些数据?数据交互的风险有多大?Netskope One 凭借其强大的 DSPM 能力，提供对数据安全态势的持续、实时可视化。DSPM评分和风险指标能够突出数据存储、用户访问、交互中的严重风险，同时持续扫描风险行为、敏感数据违规、潜在的有害查询。核心能力包括：

- 获取可视化：在所有环境中发现并分类数据，包括影子数据存储，确保符合数据主权法律要求。
- 控制访问权限：管理权限、监控访问行为，执行严格管控，确保敏感数据仅限授权用户访问。
- 监控使用行为：通过设置告警、强制执行治理标准，并确保端到端加密，为每一次数据交互提供安全保障。

支持隐私保护与合规

通过 DLP、精细化访问控制、审计、报告、对敏感数据的强加密，维护数据隐私并满足 GDPR、CCPA、HIPAA、GLBA、PCI DSS 等监管合规要求。核心能力包括：

- 针对所有云端和Web用户活动，提供精细化审计，涵盖所使用的云服务、访问的网站、执行的操作、相关数据、位置、所用设备等全维度信息。
- 实时文件加密且不影响用户生产力。
- 针对全球数据保护法规，提供 40+ 种合规模板。
- 定期提供服务使用情况的合规报告，为云安全策略的制定与调整提供参考。
- 基于用户、应用、设备、位置、活动、内容等上下文细节，对云服务和网站的使用进行管控，以满足合规与风险标准。

降低数据外泄风险，防范恶意与疏忽导致的数据暴露

面对攻击者的狡诈手段以及员工无意识的操作行为，企业正持续遭受着数据泄露的威胁。仅仅一次点击或回应就可能导致未经授权的访问，使内部威胁和疏忽的用户行为成为重大隐患。Netskope的一体化数据安全方案通过监控和缓解数据暴露、过度共享、个人应用和影子 IT 的使用，为企业提供了强有力的解决方案。安全团队可以使用统一的策略控制、基于UEBA（用户与实体行为分析）的数据防护技术，把电子邮件、USB 及批量下载带来的风险降至最低。核心能力包括：

- 限制个人应用和影子 IT 的使用。
- 防止过度共享、大批量数据传输或邮件外泄。
- 抵御 C2（命令与控制）及其他定向攻击。
- 主动识别恶意外部人员。

优势	说明
降低数据安全风险	在数据的各个状态下保护您的重要数据：无论是存储中（静态）、传输中（动态）、正在处理（使用中），还是跨越任何潜在风险点（所有关键向量）。这种全面的方法确保您的数据始终安全受保护，降低潜在威胁和漏洞。
通过上下文与高级分析增强安全性	共享的上下文把用户行为与数据和应用使用相关联，提升分析与安全性。这让主动威胁检测、异常检测、定制化安全策略成为可能，从而提高防护效果，减少中断。
降低成本与复杂性	企业可从分散的传统安全工具，转向 Netskope One 平台，实现高达 50% 的成本节约。这种整合简化了运营，消除了维护多个不同系统所带来的额外开销。
满足合规要求	通过内置的合规框架和自动化策略执行，简化对数据保护法规的遵循，帮助企业满足 GDPR、HIPAA、CCPA 在内的多种数据保护法规要求。这包括识别和分类敏感数据、监控数据访问与使用，以及执行策略以防止未经授权的访问或泄露。

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。