CLOUDFLARE

电子书

CISO 的 SASE 采用指南

如何针对高优先级用例评估 SASE 平台

实现网络安全韧性的使命

美国国家标准与技术研究院 (NIST) 对网络韧性的定义是：使用或由网络资源支持的系统对不利条件、压力、攻击或破坏进行预测、抵御、从中恢复和适应的能力。

然而，增强网络韧性在降低入侵缓解成本的同时，也带来了一些挑战：

- **网络犯罪分子的手段不断演进：**随着攻击者开发出更复杂的工具、技术和程序，组织防御各种威胁的难度进一步增加
- **IT 环境正变得越来越复杂：**由于跨多云架构连接的设备和应用数量庞大，保护这些环境是一个成本高昂且复杂的过程
- **内部团队负担过重：**随着预算收紧且内部团队负担过重，组织可能会遇到资源限制问题

为了应对这些挑战，许多首席信息安全官 (CISO) 正在转向安全访问服务边缘 (SASE) 框架。与过去的网络方法不同，SASE 架构将安全和网络整合到一个云平台上，以实现一致的可见性和控制。SASE 将网络控制放置在云边缘，而不是企业的数据中心，从而使企业能够为任何用户、应用、设备或网络提供简单、安全的访问，无论其位于何处。

本指南涵盖 SASE 的一些最常见用例，并概述启动 SASE 实施的关键步骤，以便您加强网络韧性并快速取得成果。

用例 #1：

采用 Zero Trust 网络访问 (ZTNA)

依赖基于边界的传统安全方法来保护混合办公、多云环境和未管控设备，给组织带来有限的可见性、互相冲突的配置和过度风险。Zero Trust 方法采用细粒度访问控制，确保没有任何实体默认受到信任，可帮助通过以下方式现代化企业的安全策略：

取代基于硬件的传统安全性

传统的网络边界控制，例如虚拟专用网络(VPN)，难以扩展，影响可见性，并导致安全团队难以发现和应对攻击。SASE 模型通过实施 Zero Trust 网络访问 (ZTNA) 提供安全的替代方案，同时在一个全球云网络中路由和处理网络流量，帮助减少最终用户摩擦和横向移动。

防止勒索软件攻击

勒索软件可以在整个网络中迅速传播——某些情况下，甚至可以跨多个网络和组织中传播。SASE 在检测到感染后立即撤销网络和应用访问权限，从而帮助防止勒索软件攻击的传播。在“最低权限访问控制”的 Zero Trust 原则支持下，这种方法使攻击者难以提升权限并在网络内横向移动。

管理设备访问

为第三方用户（如承包商、机构和供应商）提供访问权限时，如果组织意外地授予过多权限，或向未受管控的设备授予访问权限，就可能引入风险。SASE 允许组织设置无客户端 Zero Trust 策略，从而确保第三方用户只能访问他们需要的内容。

限制数据暴露

随着用户在经批准和未批准的应用中上传或分发敏感信息，数据暴露和泄露可对组织构成严重威胁。SASE Zero Trust 策略限制每个用户可以访问的应用，同时扫描流行的 SaaS 套件以查找敏感数据和错误配置，从而帮助防止数据暴露。

案例研究

采用 Zero Trust

一家财富 500 强电信公司利用 Cloudflare 的 SASE 平台，为 10 万多名员提供安全的混合办公环境——覆盖托管于 AWS、Azure 和其他云环境中的数百个应用。通过基于身份的 Zero Trust 网络架构、安全网关和统一访问控制，他们能够保护用户免受威胁，无需在多个策略管理界面、VPN 和互联网过滤服务之间来回切换。

用例 #2：

保护攻击面

数字转型和远程办公扩大了攻击面，更多分散的用户和未受管控的设备需要访问内部资源。但是，将本地防火墙延伸到云端，并通过 VPN 来扩展网络可能增加对外部和内部威胁的暴露，同时降低了可见性。采用 SASE 架构后，组织可以扩展可见性和控制，支持“无边界”模型，并通过以下方式实施持续一致的防护：

防范多渠道网络钓鱼

攻击者往往在用户容易对点击位置放松警惕的渠道发起钓鱼攻击，特别是那些通常不受电子邮件安全控制保护的工具。统一的 SASE 平台可以跨所有环境提供全面的保护，减少凭据盗窃、账户接管和数据外泄的风险。

保护远程员工

远程办公要求用户从多个地点和设备连接，而这些地点和设备通常超出其雇主组织的监管范围。SASE 架构允许组织保护员工和第三方对关键环境和数据的访问，帮助实现一种受保护、高效的随处办公方式。

改善用户体验

清洗办公室流量的传统方法通常需要将流量回传到集中式企业数据中心，这会增加延迟并损害生产力。然而，另一种选择——即让用户直接访问互联网——会带来安全风险，并造成不一致的用户体验。SASE 智能地管理和优化与任何云或互联网目的地的直接连接，并在尽可能接近最终用户的地方执行策略和保护。

保护广域网 (WAN)

一些广域网为分支机构之间的流量绕过云安全控制，因此有关安全服务和软件定义广域网之间的集成可能名不符实。SASE 过滤和检查办公室、数据中心、公共云以及更广泛的互联网内外的其他位置之间的流量，使组织能够简化和保护其通过 WAN 连接的方式。

案例研究

保护不断扩大的攻击面

Werner Enterprises 在其云迁移期间无缝部署了 SASE 服务，没有任何关键业务或客户服务发生中断。部署完成后，他们的恶意电子邮件数量减少了 50% 以上，同时每天减少了数小时的手动电子邮件分类工作，因而他们的安全团队可以专注于更具战略意义的业务目标。

用例 #3:

在任何地方保护数据

随着数据跨越更多环境，组织往往发现很难加以跟踪。未经批准使用生成式 AI 和影子 IT 可能暴露敏感数据，造成可能需要高昂成本才能补救的泄露。SASE 融合了 Web、SaaS 和私有应用程序环境中的数据可见性和控制帮助组织实现以下目标

简化数据隐私合规

随着大型语言模型 (LLM) 和其他 AI 工具的兴起，合规标准需要发展以保护用户数据。SASE 通过统一数据控制来保护数据的安全和隐私，使安全团队能够锁定受监管的数据类别，降低泄露风险，并确保持续遵守严格的数据要求。

安全地使用生成式 AI

随着更多组织采用 AI，暴露敏感数据的风险也在增加。通过安全 Web 网关和内联云访问安全代理，SASE 方法使安全团队能够检测和批准 AI 应用的使用，扫描存在数据泄漏风险的错误配置，或在隔离的 Web 浏览器中运行 AI 应用以限制数据输入和输出。

管理影子 IT

影子 IT 是未经批准的应用，不受使用它们的组织管理或保护，当敏感数据移入或通过它们传输时，就可能带来风险。SASE 代理流量通过内联云访问安全代理 (CASB)，后者记录每个连接和请求，以揭示未经批准应用的存在，然后允许组织控制这些应用的访问和使用方式，从而帮助最大程度地降低这种风险。

保护敏感数据

SASE 架构允许组织检测和控制敏感数据进出其 IT 环境及在其中移动的方式这包括扫描应用和检查流量，确认其中是否存在受监管的个人数据和知识产权，阻止钓鱼和勒索软件等互联网威胁，并实施额外的保护措施以防数据被盗和意外泄漏。

案例研究

在任何地方保护数据

Applied Systems 采用 SASE 服务来保护 2500 多名员工对自托管应用和基础设施的访问。这种新方法使他们的安全团队能够灵活应用严格的控制措施，以满足不同用户需求，同时控制他们的数据如何与 AI 工具共享。

选择 SASE 解决方案：

单一供应商整合 vs 多点解决方案

单一供应商 SASE 提供商将网络和安全功能融合到单一云交付服务中。这允许企业整合不同的单点产品，淘汰硬件设备，并确保持续一致的策略执行。虽然多供应商的 SASE 实施可能会达到与单一供应商方法类似的结果，但通常会增加复杂性和成本，同时降低内部可见性和灵活性。

将这些功能整合到一个统一的平台上，可以实现 SASE 的真正承诺：一个简化、高效的网络和安全基础设施，它降低总拥有成本，并轻松适应您不断发展的业务需求。

在评估潜在的 SASE 提供商时，请记住以下问题：

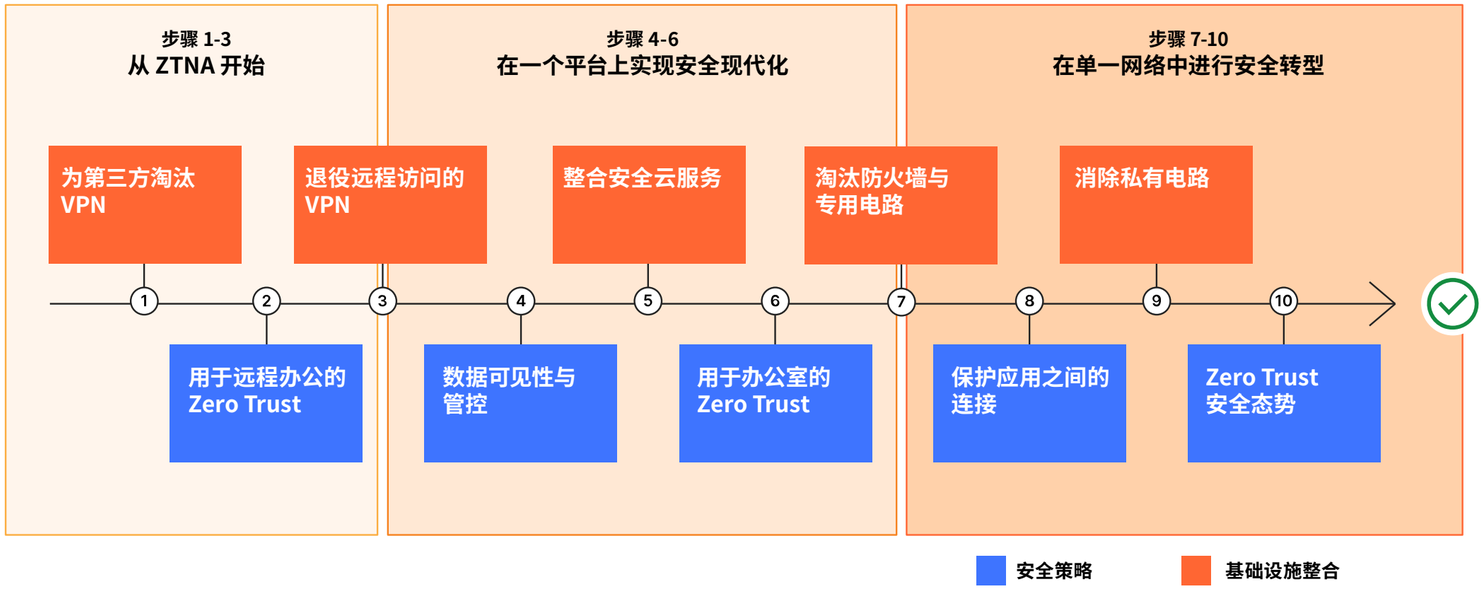
1. 应用的流量是否由威胁和敏感数据检测引擎一次性解密和检查？部署方面是否有任何限制？
2. 所有通过 SaaS 套件的数据流和通信在每个渠道（内联与带外 Web 和电子邮件活动）是否均受到保护？
3. 是否为每个用户和应用启用了远程浏览器隔离？这对生产力有何影响？是否产生额外费用？
4. 是否基于任何网络入口绕过任何安全功能？
5. 是否可能确保客户流量在多租户云架构中得到隔离和保持私密？
6. 有哪些数据本地化功能可用？启用数据本地化是否会给从本地化区域以外连接的远程用户增加延迟？
7. 您能否将威胁情报源集成到他们的架构中？该平台如何减少来自威胁情报源的误报？
8. 有哪些类型的用户/设备风险评分和分析可用？风险评分是否可以跨所有应用统一执行？

Cloudflare 如何交付 SASE

REV:BDES-6017.2024JUNE06

为了实施统一 SASE 平台，许多企业都信任 Cloudflare 。我们是唯一从 Zero Trust 网络架构开始的 SASE 提供商，整个平台一致地内置了基于身份和上下文的连接性。

您实现完整 SASE 架构的长期路线图可遵循类似如下示例的流程：



借助覆盖全球 310 多个城市的全球网络，Cloudflare 帮助 CISO 实现企业级安全、韧性和性能。我们的单一控制平面整合了跨多个安全领域的单点解决方案，以便企业和组织简化其安全运营，并确保针对不断演变的威胁提供持续一致的保护。

请访问我们的网站以进一步了解 Cloudflare 和 Cloudflare SASE 平台。

电话：010 8524 1783
电邮：enterprise@cloudflare.com
网站：cloudflare.com/zh-cn