CLOUDFLARE

白皮书

SASE 用例采购及部署指南

如何确定优先事项并为您的部署计划选择正确的平台

目录

如何使用本指南

对象

尽管对网络和安全进行现代化以实现安全访问服务边缘 (SASE) 最终将使组织中的每个人受益，**但《SASE 用例采购及部署指南》**主要是为如下人群编写的：

CIO

负责组织的整体数字现代化战略和优化 IT 成本

网络负责人

负责交付高性能、有韧性和安全的现代网络，支持公司目标

CISO

专注于提高网络威胁韧性，加强整体安全态势，降低泄露成本

无论组织的 SASE 部署计划最初以安全为主导，网络为主导，还是覆盖安全、传统网络和现代 DevOps 团队的理想化全面协作和跨职能 IT 努力，您选择的技术平台都需要服务每一个团队。真正的 SASE 架构应该具备足够的灵活性和可组合性，以便完成每个团队的短期和长期路线图上的优先用例；在您确定用例并遴选供应商时，本指南将帮助您引导那些计划沟通。

如何使用本指南

用途

如今，许多组织都意识到采用 SASE 架构的优势，然而，实现这一目标不存在“一刀切”的路线图。在每个组织独特的 SASE 部署过程中，存在着各种各样的安全和网络现代化挑战，因此每个 SASE 的实施方式也各不相同。

要为自己独特的 SASE 部署计划找到切入点，请使用**《SASE 用例采购及部署指南》**：

- **确定 SASE 的起始用例**并确保“快准狠”，以及长期但敏捷的项目路线图。反思内部优先事项，促进有助于对其进行排序的跨职能讨论。
- **计划与供应商的沟通策略**，基于超越简单模仿和商品化功能的示例问题。深入了解供应商的技术架构，包括前端界面和后端网络、计算和存储，以及长期商业战略。
- **评估 SASE 方案**，基于按照核心服务组件组织的示例考虑问题。了解供应商平台的独特要素，以超越基本和预期之中的组件。

本指南假设您熟悉 SASE 架构的主要原则和组件，但附录包括一份扩展的“SASE 入门指南”以提供清晰的说明。

找到您的部署切入点：优先用例

Gartner®, Inc. 识别了三个单一供应商 SASE 用例[1]以帮助区分组织的首要优先事项：

1. **基本 SASE** — 这种用例涵盖易于操作的产品，通常涉及寻求为公共和私有应用程序的用户提供保护的中小企业。
2. **网络驱动的 SASE** — 这种用例中，企业寻求部署具有高级网络功能的 SASE。
3. **具备高级安全性的 SASE** — 适用于要求最佳安全性而易用性优先级较低的组织。

Cloudflare 还注意到一些客户主要专注于改善最终用户体验，因而通过一种有时被称为**“咖啡店网络”**的方式简化基础设施。

虽然这种模式通常情况下有用，但许多组织倾向于讨论更狭窄的用例，类似于一个有限范围、可实现的项目，以便简化其部署过程，并更好地区分短期和长期目标。从小处着手也有助于证明有效性，激发内部动力，增加来自利益相关者的支持，提高未来推进大型项目的可能性。

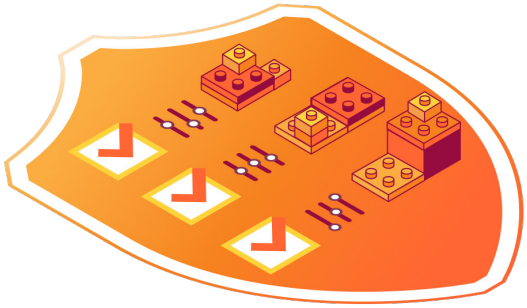
如何选择切入点并没有完美的答案，但经常被提及的内部决策因素包括：

- **改变的灵活性和开放性** — 例如，如果试点项目的范围限制更严格并利用现有基础设施开展，安全团队可能是初始 SASE 用例的最佳首批客户
- **实施速度** — 承包商的远程访问需求尤其有限，通常可以在不安装最终用户软件的情况下满足，这可以简化项目实施并为加强安全性提供“快准狠”的成果
- **面临更大攻击风险的用户/角色** — 具备有价值知识产权访问权限的开发人员、安全/风险专业人员或高管可能是主要目标
- **面临更大攻击风险的应用程序** — 例如，存放客户或财务数据的敏感内部应用程序
- **员工体验反馈** — 考虑终端用户的投诉，以确定哪些内部工作流程最受益于提高业务生产力的努力
- **现有合同时间/组织** — 现有单点解决方案即将进行合同续订可能促使您将注意力转向一个要处理的相关用例，并帮助为传统解决方案的增强或替换制定目标时间表

请查看下面的用例。这些用例按照更大的公司倡议分类，以反映在长期项目路线图的背景下，哪些用例可能对您的组织目标产生最直接的影响。尽管您的内部优先事项和现有 IT 堆栈最终将引导您选择最佳路径，但大多数组织选择从结合以上多个优先事项的用例开始，例如增强他们的 VPN，保护承包商的访问，防止多渠道网络钓鱼，保护远程办公人员和分布式办公室，或简化分支机构的连接。

话虽如此，对可编程、可组合的 SASE 架构而言，最大优点之一是没有完美的操作顺序。无论是业务优先事项的变化，还是新的技术集成，随着时间推移均可予以满足。建议制定长期路线图，但您应该保持敏捷。

关键是不要过度规划，以免延迟开始的时间过长。**SASE 架构解决的数十个用例可以被视为累积的：**为一个或两个用例付出的努力仍能增强组织的安全态势，而且由于 SASE 平台上跨服务的相互作用，实施一个用例可能降低未来实施另一个用例的难度。



倡议：采用 Zero Trust

现代办公模式（例如混合办公、多云泛滥、未受管设备等）带来了新的安全挑战。依赖基于边界的传统安全模式导致组织可见性有限，并带来互相冲突的配置和额外风险。

因此，组织正转向 Zero Trust 安全最佳实践，作为其更大的 SASE 部署过程的核心原则，这些最佳实践基于维持细粒度访问控制以进行验证的原则，且默认情况下不信任任何人或任何事物（即使在网络边界内）。

用例：增强或取代 VPN

基于网络边界的控制，例如虚拟专用网 (VPN)，可能会增加您的攻击面，限制可见性，并使终端用户感到沮丧。VPN 日益成为攻击目标，并越来越容易遭到入侵；它们还会造成中央本地设备收发所有流量的“长号”效应，导致访问内部工具和数据时出现延迟。

因此，迁移到 SASE 架构的一个常见动机是改善资源访问和连接。利用全球云网络上在尽可能靠近用户的地方路由和处理网络流量，即利用 Zero Trust 网络访问，而非通过 VPN，可减少最终用户的摩擦，同时消除横向移动的风险。

用例：保护承包商/非受管设备访问

为第三方用户（承包商、机构、供应商、合作伙伴等）设置安全访问可能会引入额外的风险和行政开销。这些协作者通常只需要在有限的时间内访问一组有限的资源，然而传统的访问控制方法可能会意外地过度配置权限。向每个人配发企业设备通常也不是一个可行的方案，而不受管理的设备缺乏企业配发设备的保护和可见性，从而增加了风险。特别是考虑到由于混合办公的普及，合同工作和临时工作比以往任何时候都更加流行，许多团队在其 SASE 部署过程初期选择保障承包商的访问安全。

设定 Zero Trust 策略可确保承包商只能在需要的时间访问他们需要的内容。尤其是无客户端的 ZTNA 能快速部署，有助于承包商快速入职，因为无需安装任何最终用户软件。承包商可以通过社交登录选项“携带自己的”身份，ZTNA 作为所有身份的聚合层。还可以轻松添加其他数据保护措施以增强态势。

用例：缓解勒索软件攻击

由于 Zero Trust 持续监控并定期重新验证用户和设备，一旦发现勒索软件感染，可以立即通过撤销网络和应用程序访问权限来阻止攻击的进一步传播。Zero Trust 还遵循访问控制的“最低特权”原则，使勒索软件难以提升其权限以获得对网络的控制权。

用例：查看和减少数据暴露

通过 Zero Trust 策略限制谁可以访问哪些应用程序，可以帮助防止数据外泄，但您可以采取进一步的措施来减轻数据泄漏风险，采用帮助检测潜在暴露并改善安全姿势的数据保护策略。这可以包括扫描 Google Workspace、GitHub 或 Salesforce 之类的流行 SaaS 套件，以查找敏感数据和存在泄漏风险的错误配置，然后根据规范指导采取阻止或其他管理操作来进行纠正。

案例研究：采用 Zero Trust

某《财富》500 强电信服务提供商通过 Cloudflare 保护超过 10 万名混合办公人员

- 全球领先的信息、通信和技术 (ICT) 解决方案提供商
- 5G 网络基础设施的主要供应商之一
- 在欧洲、印度和美国雇佣超过 10 万人

挑战：

在各部门和地区扩展访问控制

经过几十年的技术创新和增长，一家《财富》500 强电信服务提供商开发了一个复杂的 IT 和安全架构，包含涵盖数百个传统应用程序。

维护本地基础设施变得难以为继。IT 复杂性减缓了公司加强安全性和实施 Zero Trust 最佳实践的能力。而且依赖思科 Umbrella 存在沉重负担 — 难以根据特定用户群定制政策；基本网络访问需要广泛的行政监督；它提供的威胁保护在公司架构中留下了漏洞。

公司开始寻找方法以迁移到更敏捷的云环境。其中包括：

- 选择安全合作伙伴以支持将应用程序从本地环境迁移到 AWS、Azure 和其他云环境
- 用更简单、更具成本效益的 DNS 过滤替换思科 Umbrella

关键结果

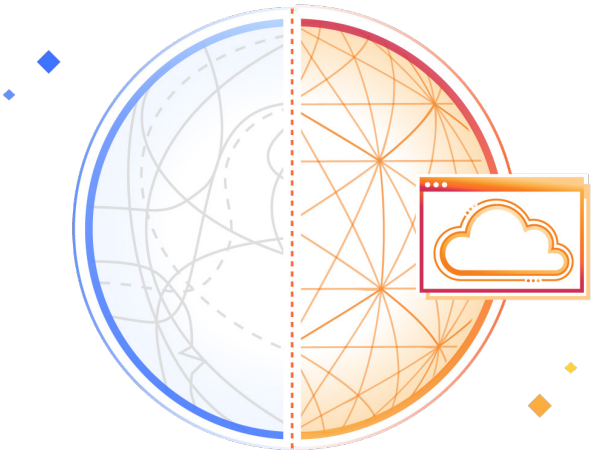
使用 Cloudflare 的 ZTNA 和 SWG 服务：

该公司意识到，支持其混合办公人员和数字转型雄心需要将安全性整合到单个云平台上。

部署 Cloudflare 的 ZTNA 和完全 Web 网关 (SWG) 服务（分别是 Cloudflare Access 和 Cloudflare Gateway）后，该公司：

- **保护混合办公**，为超过 10 万员工提供针对应用程序和互联网访问的统一控制
- **将思科 Umbrella 替换成** Cloudflare 以防范恶意软件、网络钓鱼和其他威胁
- **实施基于身份的 Zero Trust 策略**，覆盖位于 AWS、Azure 和其他云环境的数百个应用程序
- **不再需要来回切换多个策略构建界面**以管理不同的 VPN 和互联网过滤服务
- **集中日志记录，**简化 SOC 事件响应和任何合规审计

倡议：现代化您的网络



在当今的分布式环境中，与其尽可能长时间地维护传统的企业网络，组织可以利用分布式、动态的云原生 SASE 服务实现网络现代化。

整合网络和安全服务可降低复杂性和风险，从而帮助企业变得更加敏捷和更具竞争力。

用例：简化分支机构连接/从 MPLS 或传统 SD-WAN 过渡

高效连接分支机构是一个挑战。多协议标记交换 (MPLS) 配置和调整单点解决方案需要太多时间；通过安全设备的拼凑组合回传流量带来糟糕且不安全的体验；而且存在一些迅速倍增的低效率问题。与此同时，如果绕过云安全来处理分支机构之间的流量，传统 SD-WAN 实施可能增加风险。

使用 SASE 架构，您可以增强或替换 MPLS 电路和传统网络设备的拼凑组合，从而更轻松地在分支机构之间路由流量，并促进跨地点的站点到站点连接。在物理场所部署最低要求的硬件，并利用低成本的互联网连接到达最近的“服务边缘”位置。

用例：减少/消除 DMZ

组织使用 DMZ 在企业防火墙分隔出的网段中托管公共或私有应用程序，旨在防止企业网络的其余部分暴露给外部。然而，作为一种网络结构，DMZ 的重要性正在降低，因为有其他的方式在无需暴露的情况下构建和托管应用程序。

除了采取措施利用现代应用程序和网络服务将 DMZ 安全性转移到云端，组织还可以开始减少或完全消除对 DMZ（和 VPN）的需求。通过采用 Zero Trust 方法，组织无需允许入站流量即可提供简单、安全的访问。这显著减少了攻击面，并改善了有关谁有权访问什么的可见性，而无需审计防火墙或网络。

设定 Zero Trust 策略可确保承包商只能在需要的时间访问他们需要的内容。尤其是无客户端的 ZTNA 能快速部署，有助于承包商快速入职，因为无需安装任何最终用户软件。承包商可以通过社交登录选项“携带自己的”身份，ZTNA 作为所有身份的聚合层。还可以轻松添加其他数据保护措施以增强态势。

用例：缓解勒索软件攻击

由于 Zero Trust 持续监控并定期重新验证用户和设备，一旦发现勒索软件感染，可以立即通过撤销网络和应用程序访问权限来阻止攻击的进一步传播。Zero Trust 还遵循访问控制的“最低权限”原则，使勒索软件难以提升其权限以获得对网络的控制权。

用例：查看和减少数据暴露

通过 Zero Trust 策略限制谁可以访问哪些应用程序，可以帮助防止数据外泄，但您可以采取进一步的措施来减轻数据泄漏风险，采用帮助检测潜在暴露并改善安全姿势的数据保护策略。这可以包括扫描 Google Workspace、GitHub 或 Salesforce 之类的流行 SaaS 套件，以查找敏感数据和存在泄漏风险的错误配置，然后根据规范指导采取阻止或其他管理操作来进行纠正。

案例研究：现代化您的网络

网络即服务助力鞋类零售商 DTLR 逐步迈向 Zero Trust

- 成立于 1982 年
- 总部位于美国的鞋类和街头服饰零售商，拥有近 250 家门店
- 雇佣了超过 3000 名店铺员工

挑战：

加强网络边缘的安全性

时尚零售商 DTLR 正在大力推动数字转型。店铺经理们寻求更好的数据分析，公司希望客户能够在两小时内从实体店提货。

然而，他们的 IT 基础设施难以跟上步伐。例如，他们的安全框架包括将店铺连接到一个中央位置的 IPSec VPN。“从 IT 的角度来看，这种方式是完全缺乏控制的。”

DTLR 还面临独特的安全挑战（例如安全地向所有店铺广播 DTLR Radio 内容）。

正如其 IT、总监 Nigel Williams-Lucas 向 Network World 所指出的那样，“……我们需要单一视图，以便我们的团队能够执行对所有店铺生效的变化，而不必逐一处理。我们希望能够审计以确保它们正确。对于网络安全，我需要能够看到进出的流量。”

DTLR®

关键结果

使用 Cloudflare 的 Zero Trust 和网络服务：

DTLR 需要逐步有条不紊地向云端迁移，同时维持可预测的成本。

该公司（已经在使用 Cloudflare 的 DNS 服务）选择 Cloudflare 的网络即服务 (NaaS) 来开始采用 Zero Trust 的分阶段过程。

通过 Cloudflare，DTLR：

- **使用 Cloudflare Tunnel 以 Zero Trust 模式部署应用程序**，无需更换防火墙
- **提升网络性能，** 现在每家店铺都连接到最近的 Cloudflare 入网点 (PoP)
- **获得对端点流量传输的可见性**，并关闭不再使用的遗留端点
- **改善整体安全态势**：“我们现在了解什么在我们的网络中流动，因此应该能够为明天构建更好、更强大的安全态势。”

倡议：保护您的攻击面

随着企业创新、扩展和多样化其数字足迹 — 从云迁移到增加基于 API 的功能 — 他们无意中创造了更多可供对手利用的入口点和途径。

SASE 方式可保护随着组织采用分布式/混合办公、加速云迁移和投资数字转型而不断扩大的攻击面。

用例：防止多渠道网络钓鱼和企业电子邮件破坏

攻击者越来越多地将钓鱼诱饵投放到用户对点击不那么谨慎的渠道中。在“多渠道”网络钓鱼中，攻击来源可能不限于电子邮件 — 还包括短信/文本消息、即时通讯、社交媒体、云协作/生产力服务以及其他通常不受电子邮件安全控制保护的工具。SASE 能够从单一平台提供覆盖所有这些环境的全面保护 — 减少高级钓鱼手段造成的凭据窃取、账户劫持或数据外泄风险。

用例：保护远程办公人员

远程办公扩大了攻击面，因为更多分散的用户和未受管理的设备都需要访问内部资源。采用 SASE 架构扩展了可见性和控制，以支持“无边界”模型，使您能够通过一个统一平台对网络内外的威胁执行一致的保护。扩大安全边界以适应“随时随地工作”的方式，还可以确保用户体验更加高效，并有助于留住来自任何地点的最佳人才。

用例：保护分布式办公室

传统的办公流量清洗方法涉及将流量回传到集中式公司数据中心，这可能会增加延迟并影响生产力。同时，允许员工直接访问互联网会导致针对每个地点的保护措施不一致、低效和无效。相比之下，SASE 方法可以在办公室之间实现一致且高效的安全性，以支持混合办公，同时减少管理具体场所防火墙或其他本地设备的开销。

用例：保护 WAN

SASE 使组织能够简化连接和保护办公室、数据中心和云的方式。这意味着通过在广域网 (WAN) 上叠加基于防火墙和代理的 SWG 控制，为那些地点（分支机构、数据中心等）之间以及进出更广泛互联网的流量应用过滤和检查。一些 WAN 解决方案中，分支机构之间的流量绕过云安全，因此安全服务与 SD-WAN 之间的集成声明可能并非最初看起来那样（具体因供应商而异）。

案例研究：保护您的攻击面

Werner Enterprises 与 Cloudflare 合作整合电子邮件、应用程序和网络安全解决方案

- 创立于 1956 年
- 北美最大的卡车运输公司之一
- 利用一流技术为客户提供优化的货运管理服务和道路资源

挑战：

阻止钓鱼和 BEC 攻击，并保护本地/云混合基础设施

由于其员工的规模和地理多样性，且广泛使用电子邮件进行通信，Werner Enterprises 对网络钓鱼和企业电子邮件破坏 (BEC) 攻击存在担忧。随着电子邮件威胁增加，该公司之前的电子邮件安全系统已经不堪使用。

此外，Werner 正在系统地将其传统的本地应用程序迁移到云端，以便其北美资源能够摆脱传统 VPN 的限制。

在过渡期间维持这些核心系统的可用性至关重要，同样重要的是保护其客户的商业历史和员工的个人身份信息 (PII)。

该公司还希望最小化工具泛滥，并减少管理多家供应商的安全解决方案的复杂性。

关键结果

使用 Cloudflare 的电子邮件安全和网络安全服务：

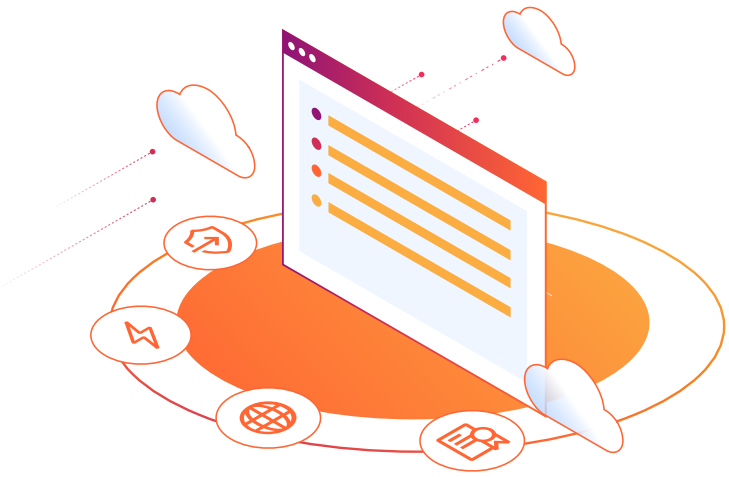
Werner 希望拥有一套统一工具，使他们能够迁移到云以减轻威胁并提高性能，并为他们的客户和用户提供与实际身处建筑物中时同等的安全性。通过 Cloudflare 的电子邮件安全和网络安全服务，该公司：

- **将用户收件箱中的恶意电子邮件减少**超过 50%
- **将人工电子邮件分类**时间减少数小时/日，允许各团队将其精力重新投入到其他战略业务目标中
- **将核心传统服务迁移**到云，而不会导致关键业务或客户服务中断

通过整合为单一供应商、单一界面的解决方案，Werner 减少了系统复杂性，促进了自动化，并改善了数据可见性。

WERNER ENTERPRISES

倡议：现代化您的应用程序



如今一切都可以通过一个应用程序完成，从订购早餐到处理工资单。然而，传统应用程序（无论是面向消费者还是用于后台功能）需要现代化以便更多由数据驱动或利用人工智能。

应用程序还需要为最终用户提供安全、韧性和高性能，具有处理数据增长的可扩展性，同时仍满足数据治理要求。SASE 架构可帮助为开发人员及其关键合作伙伴简化应用程序现代化过程的几个阶段，同时保持安全性。

用例：保护应用程序访问和云迁移

开发人员应该能够专注于以他们希望提供的业务价值为导向构建全新的应用程序，无需考虑从头开始创建定制的安全访问机制。ZTNA 作为组织所有资源的访问聚合层，集成所有现代身份协议，按照企业内部一致的方式简化对全新应用程序的安全访问。

对于现代化传统本地应用程序并将其迁移到云的团队，现代化的访问解决方案还可以通过相同的 ZTNA 解决方案连接本地和云实例，从而简化过渡并确保最终用户访问体验在整个切换过程中的连续性。

用例：保护特权（开发人员/IT）访问

开发人员需要对关键基础设施拥有访问特权，使他们成为诱人的攻击目标。他们需要访问许多不同类型的资源（SaaS、自托管、SSH/VNC/RDP 等），但不能因为过于严格的安全措施而感到受限。Zero Trust 方法有助于特权用户保持高效率，提供流畅、低延迟的用户体验，同时维持最低权限访问。会话日志记录可以进一步提供对特权用户会话的可见性，加强对更高风险工作流程的可见性。

用例：防止开发人员代码泄露和盗窃

代码数据正迅速增加。开发人员的代码推动数字业务发展，但这些高价值的源代码可能会在许多开发工具中被暴露或成为盗窃目标。保护在 SaaS 数据存储库（如GitHub）或 AI 工具（如 GitHub Copilot）中存储和共享的代码，并通过 SASE 查看暴露的代码并控制其去向。

用例：保护 DevOps 工作流程

DevOps 团队需要通过更简单的方式建立安全的 Zero Trust 连接，以加快测试。一些 SASE 解决方案将其覆盖范围扩展到超出用户到应用程序用例以外，以涵盖网状和点对点安全网络，并支持服务到服务的工作流程和双向流量。以真正的任意对任意连接为目标进行现代化可以帮助简化持续集成和持续交付 (CI/CD) 管道及其相关流量传输。

案例研究：现代化您的应用程序

Cloudflare Zero Trust 保护 5000 多名 Creditas 员工的居家办公访问

- 巴西最大的贷款金融科技平台
- 47 亿美元估值
- 在拉丁美洲、欧洲和墨西哥提供房屋产权贷款、汽车贷款、抵押贷款和其他服务。

挑战：

一夜之间为 5000 名员工提供对内部工具和应用程序的安全访问

当 COVID-19 在巴西爆发时，巴西政府指示 Creditas 让所有人回家。Creditas 只有 48 小时的时间将其整个办公模式从 100% 的现场转变为几乎完全远程。

在准备满足这一要求时，工程团队面临着多重挑战，包括：

- 维护一个传统 VPN，其要求复杂的配置以便在不同操作系统上运行，并且只能支持有限的一部分员工
- 在 Creditas 团队与第三方供应商之间进行耗时的协作，修改新的 VPN 工具，确保其安全可用
- 坚持安全和数据保护标准以及合规要求

关键结果

使用 Cloudflare 的 ZTNA 服务：

Creditas（最初是 Cloudflare 核心应用安全套件的客户）转向简化员工连接和保护对内部资源的访问，以满足紧迫的政府截止日期，确保远程办公安全。

Creditas 迅速部署了 Cloudflare 的 ZTNA服务（Cloudflare Access），在其全体员工中实施针对每个应用程序的身份认证。

关键结果包括：

- **提高了 DevOps 的生产力**，将应用程序调试和实施所需的时间从 2-4 周减少到两天
- **简化员工连接**并保护 45 个易受攻击的应用程序和内部资源
- **100% 员工增长**而工程支持人员增长不到 30%

creditas

倡议：在任何地方保护您的数据

数据涉及的环境超过大多组织所能跟踪的范围；例如，敏感数据可能因为未经授权使用生成式 AI (GenAI)和影子 IT 而暴露。这些泛滥的云和 SaaS 环境会造成更多风险。

SASE 将网络、SaaS 和私有应用程序环境中的数据可见性和控制汇聚到一个架构中，因此它有助于简化组织跟上监管要求并领先于现代数据风险的方式。

用例：简化数据隐私监管合规性

数据隐私从未像现在这样重要；例如，在 2023 年，立法者对 GDPR 违规行为开出破纪录的 12 亿欧元罚单。企业可以继续预期保护用户数据的法规将更加严格，尤其是在大语言模型和其他 AI 工具的使用增加的情况下。

SASE 帮助组织保护数据安全和隐私的努力：统一跨各种环境的控制和可见性，从而更易锁定受监管的数据类别，通过日志维护详细的审计跟踪，并改善您的安全态势以降低数据泄露的风险。

用例：管理影子 IT

SASE 帮助组织重新掌控并减轻影子 IT 带来的风险。通过内联云访问安全代理 (CASB) 代理流量，记录每个连接和请求，以揭示未经批准的 SaaS 应用程序，以及用户在其中进行的操作。然后，管理员可以审查这些应用程序，予以批准/阻止，并相应应用基于身份和设备的策略。

用例：安全地使用生成式 AI

SASE 服务帮助组织安全高效地使用生成式人工智能，对于流量来源的任何地方（无论是来自您的员工还是自动化服务），以及流向的任何地方（例如，类似 ChatGPT 的公共应用程序或私有 AI 应用程序），都可以应用控制和获得可见性。

例如，使用 SASE 平台的安全 Web 网关 (SWG)/内联 CASB 服务，安全团队可以检测和批准 AI 应用程序的使用，通过 API 驱动的 CASB 扫描可能致数据泄漏的配置错误，或在隔离的网络浏览器中运行 AI 应用程序以限制数据的输入和输出。

用例：保护您的敏感数据

SASE 服务使组织能够检测和控制敏感数据如何进入其 IT 环境、在其中移动和离开。这包括扫描应用程序和检查流量中的敏感数据，包括受监管信息（例如个人身份信息、健康、财务信息）和高价值信息（例如开发人员代码或知识产权）。额外的 SASE 保护措施可防止数据被盗或意外泄露，包括使用 Zero Trust 最佳实践保护数据访问，并阻止诸如网络钓鱼和勒索软件之类的互联网威胁。

案例研究：在任何地方保护数据

Applied Systems 整合跨员工、应用程序和网络的安全性，以加速数字化转型。

- 成立于 1983
- 构建适用于保险行业的 SaaS 解决方案
- 在美国、英国、加拿大、西欧和印度雇佣超过 2500 名员工。

挑战：

加速数字转型

安全对 Applied Systems 至关重要，必须为其保险客户保护大量财务数据、付款记录、个人身份信息 (PII) 以及其他受监管和敏感信息类别。

随着新的执行团队就职，Applied Systems 寻求变得更灵活、高效和安全的机会。他们使用着来自不同供应商的组件，但存在抱怨；例如，他们的开发人员抱怨 Zscaler 阻止了对工作至关重要的网站，影响了生产力。

Applied Systems 专注于整合大量的安全和网络功能，包括：

- 公共网站和应用安全保护和性能提升
- 网络基础设施安全、可扩展的连接能力
- 员工和内部资源的 Zero Trust 安全态势

关键结果

使用 Cloudflare 的应用服务和 Zero Trust 组合：

Applied Systems 希望与一个云原生且了解云原生客户期望的供应商进行合作。为了提高技术效率并支持业务增长和雄心，Applied Systems 部署了 Cloudflare 的一系列应用程序服务、Zero Trust 和网络连接服务。

关键结果包括：

- **保护** 2500 + 员工对自托管应用和基础设施的访问，取代了 Zscaler 和 Cisco
- **灵活性**，可应用更严格或更宽松的控制以满足不同用户需求
- **保护** ChatGPT 和 Bard 等新兴 AI 工具中的数据

Applied Systems 的 CISO 指出：“当客户问及监管合规性时，我们可以直接告诉对方的 CISO 我们是 Cloudflare 的客户，并解释我们正在使用的产品。”

APPLIED

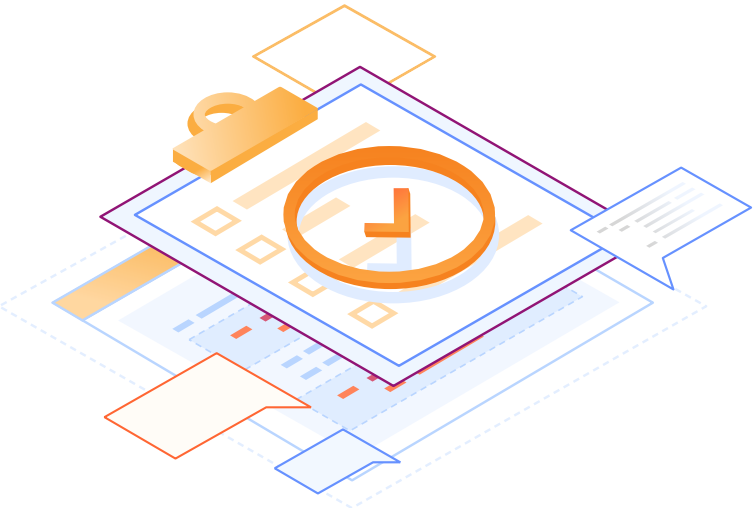
进行供应商评估

在全面了解组织的需求之后，**无论处于 SASE 过程中的任何阶段，您寻找的供应商都应该能够满足您的需求，**并与您现有的网络入口、身份管理、终端安全、日志存储以及其他网络安全工具集成。

许多供应商都宣称自己是一体化平台，但实际上却要求组织集成几个不同的单点产品。

基于角色的沟通开场白

尽管传统供应商的“并排”比较仍然有价值，但往往会偏向功能清单，在市场本身发展如此迅速的情况下，难以客观进行比较。任何供应商的解决方案中第二天都可能出现新的小部件，但深层次的基础架构优势（或缺陷）持续时间将长得多。



一些 SASE 供应商也是在十多年前从一个或两个核心服务开始的，此后匆忙通过增加或收购以在视觉上完善他们的 SASE 组合。这些供应商的观点或所声称的清单可能固有地偏向于他们的长期优势。如果您首先深入了解内部优先事项，确定要求的 SASE 用例最需要哪些能力，那么在选择供应商时将更加游刃有余。把您实际将使用每个供应商的最主要差异化因素进行的工作写下来；归根到底，即使是世界上最先进的小部件，如果闲置不用，也是毫无意义的。

根据您的主要利益相关者，考虑以下将与供应商讨论的比较性主题。SASE 供应商的功能正在快速迭代（甚至可能每个月都有显著变化），因此找到更深入的标准和讨论要点将帮助您在这个充斥着类似声称的市场中选择最佳的长期合作伙伴。

CIO 办公室

请注意，这些问题中有很多也直接适用于其他团队。

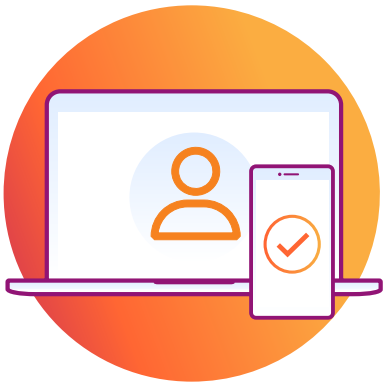
关键优先事项

- 提高团队生产力
- 改善用户体验
- 加速数字现代化
- 降低总体拥有成本

向供应商提出的问题

团队生产力

- 对于所有 SASE 功能是否有一个集中的用户界面（即一次登录）还是多个？
- 对于所有 SASE 功能是否有一个集中的 API（即一个 API 密钥），还是多个？
- 安全（例如 ZTNA、SWG、CASB）和网络（例如 WANaaS、SD-WAN、FWaaS）功能是否默认原生集成，还是需要您或我们进行手动操作？
- 我们是否一次或多次将我们的身份提供者（例如 Microsoft、Okta、Ping）集成到 SASE 平台，以便为每个应用程序（Web、SaaS 和私有）启用基于身份的访问策略？
- 您的用户设备代理能够以可组合的方式连接到任何其他网络入口（例如WAN 连接器、应用连接器以及其他设备代理的网状/P2P 连接）吗？
- 我们的安全和 DevOps 团队能否在用户、应用程序和/或服务工作流之间实现双向的任意对任意连接，而无需要求我的网络团队部署设备或更改网络路由？
- 您提供到多大程度的自动化（除拥有 API 外）？您的基础设施即代码（例如 Terraform）提供商有多完善？
- 我可以多快开始免费试用您的完整平台，包括所有安全和网络服务以及可用的入口？我能在今天立即开始运行吗？



用户体验

- 您的全球网络地图上的每个数据中心是否都对每位客户可用，还是有些数据中心仅供您的电信合作伙伴的客户专享？
- 您的全球网络地图上的每个数据中心是否都提供每个 SASE 功能，还是有些功能（例如 RBI）仅在有限的数据中心运行？
- 每个 SASE 网络入口（例如设备代理、WAN 连接器、应用程序连接器）是否都能连接到您的全球网络地图上的每个数据中心，而无需支付额外费用或带宽附加费？
- 在您的 POP 和其他网络之间存在多少互连，以最小化中间传输提供商的跳数和延迟？

数字现代化

- 每种连接方法是否都能在每一个位置与 SASE 服务进行互操作？我在哪里可以阅读关于底层架构的更多信息？
- 您的平台拥有哪些认证？（ISO27701，SOC2，FedRAMP 等）
- 它是否能够与任何现有的云端或本地系统进行互操作？L2-7 连接是否完全可通过 API 编程？
- 如果在不同云之间切换，我们的 SASE 服务/成本会发生什么变化？
- 您将如何服务我的组织在未来 5 年、10 年后的发展目标？
- 您目前的生态系统（包括技术合作伙伴）能如何支持我的现有投资？

总拥有成本

- 您的 Zero Trust 解决方案如何定价？我是否需要为部署应用程序连接器或使用带宽付费？
- 是否有任何数据中心在公共云提供商 (Azure、AWS、GCP、Oracle) 上运行？
- 您是否对产品的任何级别设置了流量使用上限？
- 是否有每个位置需要激活、管理或扩展的硬件或虚拟设备？
- 用于保护分支机构的任何网络安全功能是在本地运行还是完全云原生的？
- 在云之间移动数据的出口费用是多少？

网络负责人

请注意，CIO 办公室的许多问题也直接适用于网络团队。

关键优先事项

- 降低网络安全风险和攻击面
- 改善安全态势
- 支持效率并缩短响应时间

向供应商提出的问题

网络现代化

- SASE 网络覆盖所有流量传输（入站、出站、广域网、公共云网络），还是仅部分？整个流量传输过程中的后端架构是否相同？
- 您在多少个不同的国家/地区和城市维护自有的数据中心基础设施？您的全球网络地图上是否显示了任何默认情况下无法路由到的地点？
- 将我们的网络连接到您的网络的所有不同选项是什么？在您的全球网络地图上，是否每个连接选项在每个数据中心基础设均可用，而无需支付额外费用或带宽附加费？
- 如果我们需要更多容量或更低延迟，您能在每个数据中心位置即时配置每一项 SASE 服务吗？

业务敏捷性

- 您提供哪些高级网络功能（例如，专用主干传输、缓存、协议和应用程序优化、高级路由、SaaS 优化、专用主干、应用程序优化/加速）？
- 您提供哪些网络监控、可见性和观察功能？
- 您如何处理流量引导、整形和故障转移，以确保我们的数据包始终采用最佳可用路径？

性能和韧性

您的 SLA 是什么？当任何 SASE 服务（例如，解密流量接受所有威胁和数据保护功能的检查）处于活动状态时，您是否提供正常运行时间和/或最终用户延迟保证？

- 延迟保证是衡量从流量来源到 SASE 网络的时间，流量通过 SASE 网络的时间，还是完整往返时间（流量来源到目的地）？
- 您在网络路由中使用 Unicast 还是 Anycast？如使用 Anycast，您是否维护自有的网络硬件？您如何确保流量不会在多个位置之间“震荡”？
- 如果一个或多个数据中心由于计划外故障（例如，断电，DDoS 攻击）或计划维护而完全关闭，您如何确保网络韧性？由您还是我们管理次要/备用流量路由？
- 如果在我们的网络位置和您的数据中心位置之间的公共互联网上某个地方发生故障，您将如何确保业务连续性？

CISO 办公室

请注意，CIO 办公室的许多问题也直接适用于安全团队。

关键优先事项

- 进行网络现代化以满足未来需求
- 提高业务敏捷性
- 韧性和维持 100% 正常运行时间

向供应商提出的问题

减少网络风险/攻击面

- 您的威胁和敏感数据检测引擎（例如 AV，DLP）是否会对所有应用程序（Web，SaaS，私有）流量进行一次性解密和检查，无需任何特殊配置？
- 所有通过 SaaS 套件（例如Microsoft 365、Google Workspace）的数据流和通信是否在每个通道上都受到保护 — 包括内联网络活动、内联电子邮件活动以及带外 Web 或电子邮件活动？
- 是否能够为每个用户和每个基于浏览器的应用程序（Web，SaaS，私有）启用 RBI，而不影响用户的生产力或产生额外费用？

一致的安全态势

- 是否有任何安全功能基于所用网络入口被绕过？
- 您如何确保客户流量在您的多租户云架构中是隔离和私密的？
- 您如何提供数据本地化功能？启用这些功能会导致本地化区域之外连接的远程用户增加延迟吗？

效率并缩短响应时间

- 将我们的数据湖和分析（即 SIEM、XDR、云存储桶）集成到您的 SASE 平台，以实现对每个应用程序（Web、SaaS 和私有）的访问日志可见性，一次性完成还是需要多次？
- 如何将我们的威胁情报源集成到您的 SASE 架构中？
- 您或通过技术合作伙伴集成提供哪些针对动态设备和用户风评分的分析？当用户访问任何应用程序（Web、SaaS 和私有）时，这些评分可以统一应用吗？
- 您如何减少威胁情报源中的误报？

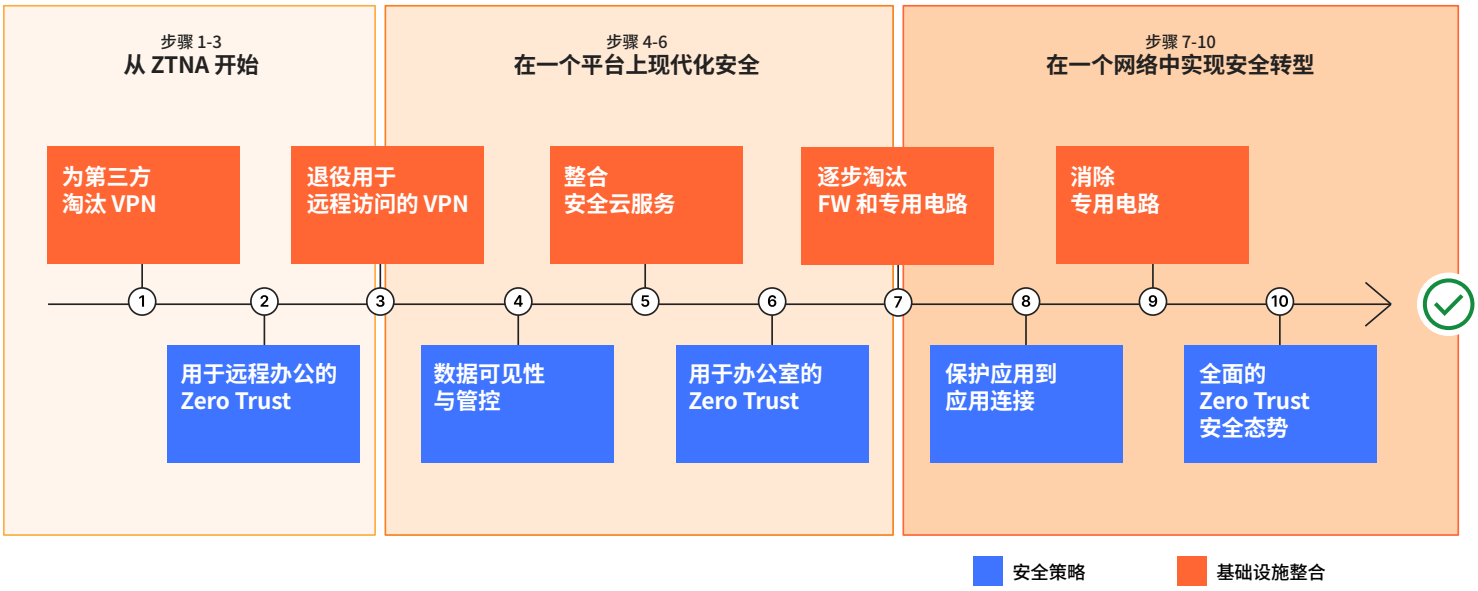
选择单一供应商 SASE 整合的理由

大部分大型企业预计将逐步转变到 SASE 架构，而不是一次性全部完成。在这个过程中，企业可能选择使用来自多个供应商的 SASE 服务（特别是因为许多市场上销售完整 SASE 解决方案的供应商实际上是将单独的产品拼凑在一起，导致非融合体验，类似于您管理多个独立供应商时所看到的情况）。

然而，通过单一供应商部署和管理 SASE 的所有组件 — 相比将不同的网络和安全解决方案拼凑起来 — 显著简化部署和管理，减少复杂性、安全漏洞以及潜在的集成或连接挑战。

整合在单一供应商的 SASE 平台上，使组织能够实现 SASE 的真正承诺：**获得一个简化、高效和高度安全的网络和安全基础设施，从而降低您的总拥有成本，并适应现代数字环境中不断变化的需求。**

虽然没有完美的操作顺序，而且每个组织都应评估其独特的优先事项，但单一供应商的 SASE 架构的长期路线图可能类似于下面的示例流程

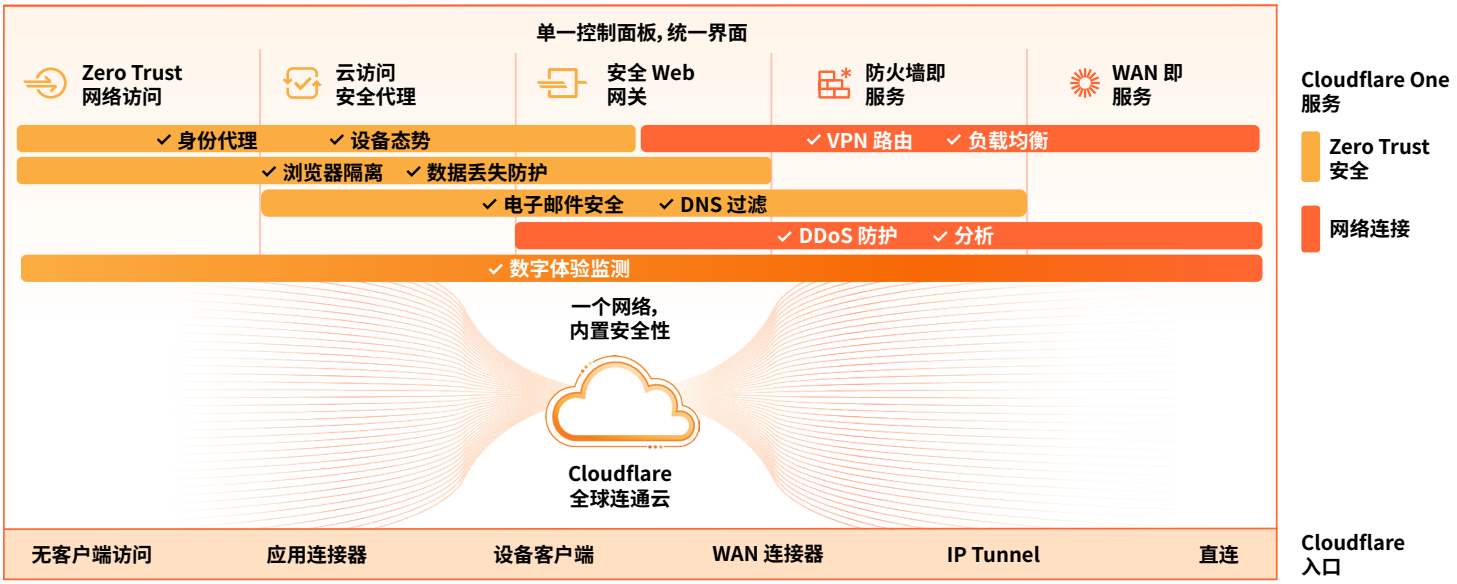


为什么选择 Cloudflare One?

Cloudflare 的单一供应商 SASE 平台 Cloudflare One 是在我们的全球连通云中构建的，后者是公共云的下一场变革，提供一个统一的智能平台，包含可编程、可组合的服务，在所有网络（企业和互联网）、云、应用和用户之间实现任意对任意连接。

其他 SASE 供应商通常会在云中单独构建南北向互联网网关，独立于通过本地设备支持的东西向流量，这会导致在没有 MPLS 电路备份以确保性能和韧性的情况下，对东西向流量路径的控制微乎其微。Cloudflare 的中间传输全球骨干网络原生聚合南北向互联网网关和东西向私有流量传输，以确保企业级的韧性和性能，而且全部通过低成本的互联网连接传输。

一些 SASE 供应商也是在公共云上构建的，并将高昂的费用转嫁给客户；它们被设计为数据的最终目的地，而 Cloudflare 则被设计为将数据传输到任何目的地，而不会牺牲企业的敏捷性、韧性或控制。由于我们构建全球网络和世界级应用安全的方式，代理、防火墙、解密、流量扫描、数据处理、管理等功能都可在未来的服务中重复使用。**利用以上基础，我们成为唯一一家从 ZTNA 开始的 SASE 提供商，身份和基于上下文的连接始终内置在我们的整个平台中。**



Cloudflare 帮助组织实现真正的网络现代化，以简化 SASE 实施，无论由哪个团队领导倡议。我们的平台使 SASE 网络对安全团队更灵活和更易用，对传统网络团队更高效，并在更大的 SASE 连接相关讨论中将覆盖延伸至支持不足的技术团队：DevOps。我们的全球连通云提供一流的灵活性，使得任意对任意连接对实施 SASE 架构的组织来说更加可行，支持规范指导以及部署偏好。

如今，我们的整合安全平台和连接纽带使 Cloudflare 与其他超大规模厂商并驾齐驱，傲视其他 SASE 领域参与者。例如，Cloudflare 的全球连通云提供其他改善应用程序性能和安全的服务，包括 API 网关、WAF、内容分发网络 (CDN) 和 DDoS 缓解 — 这些服务都可以补充组织的 SASE 架构。

Cloudflare 提供的广度和深度有助于组织通过单一供应商 SASE 及其他方式重新获得 IT 控制，所有这些都使用路由约 20% 网站的相同 Cloudflare 代理。随着数字化倡议和安全风险不断加速演变，我们的网络最为敏捷，长期为组织提供连接和保护服务。

FORRESTER®

Cloudflare 被“2023年第三季度 Forrester Wave™：Zero Trust 平台”报告评为“表现卓越者”

阅读报告 >

IDC

Cloudflare 被 2023 年 IDC MarketScape 的 Zero Trust 网络访问 (ZTNA) 报告评为“领导者”

阅读报告 >

kuppingercole ANALYSTS

Cloudflare 被 2023 年 KuppingerCole SASE “领导力指南针”报告评为“领导者”

阅读报告 >

了解更多

Cloudflare One 简化您采用 Zero Trust、实现网络现代化、保护攻击面、实现应用现代化以及随时随地保护数据的过程，无论切入点是什么。

如需了解更多信息，请阅读我们的参考架构《使用 Cloudflare 进化到 SASE 架构》，或者联系 Cloudflare One 专家。

附录：SASE 入门指南

Gartner®, Inc. 表示，“未来五年内，安全访问服务边缘 (SASE) 市场将以 29% 的复合年增长率增长，到 2027 年达到 250 亿美元以上[2]。”**为什么需求如此巨大？**

今天的 IT 和安全领导者有望帮助实现快速数字现代化优先事项，以满足在任何地方连接、保护和构建一切的当务之急，拥有网络安全和基础设施以支持：

- **分布式、动态的云服务**，以获得更多保护、更多计算能力和更多容量
- **保护混合办公**连接用户、应用程序和数据，无论位于何处，且符合监管要求
- 通过 Zero Trust 安全**降低网络风险**，同时确保快速、可靠的连接
- **降低总拥有成本**，减少资本支出/运营支出成本，并整合单点解决方案
- **敏捷性和灵活性**，以快速适应新技术、功能和可扩展性要求

然而，基于“城堡+护城河”方式的传统物理和虚拟化网络系统无法有效解决以上所有需求。尽管这些系统在过去的时代具有意义，但如今它们建设成本过高，维护复杂，并且没有为云或远程办公而优化。

换句话说：急需通过 SASE 对网络进行现代化。

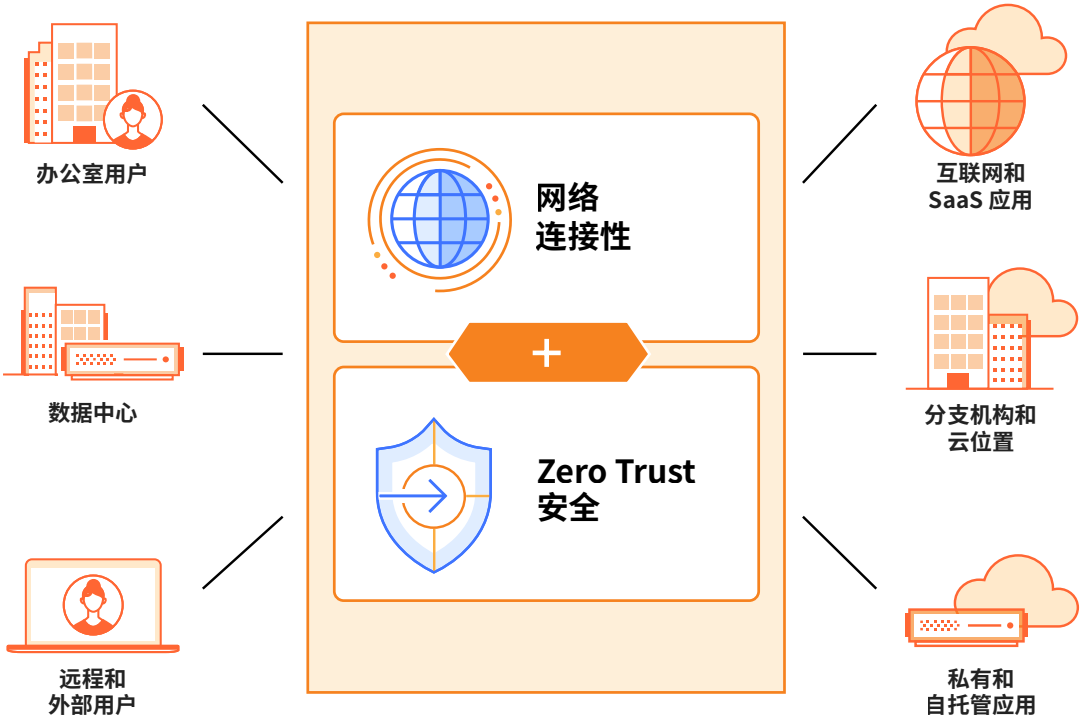
尽管 IT 环境变化的完整“前后对比”可能令人不知所措，但大多数组织正在启动为期数年的 SASE 路线图，以便维持实施的可行性，并随着时间的推移逐步增加更多用例。在完全替换之前，传统设备可以逐步通过 SASE 平台进行部分增强，为业务带来新的价值。这里不可避免地要进行 IT 现代化，同样要将跨职能的利益相关者汇聚在一起进行内部协作，以成功实施 SASE。

什么是 SASE?

在传统的企业网络（不同于 SASE）中，数据和应用程序位于核心数据中心内。要访问这些资源，用户、分支机构和应用程序从本地专用网络或次要网络（一般通过安全的租用线路或 VPN 连接到主要网络）连接到数据中心。

然而，基于边界的模型难以应对远程/混合办公、SaaS 和云迁移以及多手段、多通道网络威胁的增加。

与过去的网络方法不同，SASE（发音为“sassy”）架构将安全和网络统一到一个云平台上，提供一致的可见性和控制。SASE 将网络控制放在云边缘，而不是企业数据中心。**这使企业能够为任何用户、应用程序、设备或网络提供简单、安全的访问，无论其位于何处。**



具体而言，SASE 平台将网络连接功能与多个从单一界面管理、从单一控制平面交付的安全功能融合在一起。通过将这些服务合并到统一、可组合的架构中，SASE 简化了网络连接和网络安全基础设施，使企业能够在其优先事项随时间推移而变化的同时保持敏捷。

下面更详细地解释核心 SASE 服务和组件。**然而，在深入了解各个 SASE 架构组件和功能之前，首先澄清您要解决的最重要挑战。**

创建 SASE 的商业案例

因为 SASE 架构涉及将许多传统上不同的服务融合在一起，着手开始您 SASE 部署过程最初看起来可能让人不知所措。在技术方面开始之前，您应该首先让业务、IT、安全和网络利益相关者就通过 SASE 实现的所有业务结果达成一致意见，同时确定哪些对您的具体目标最为重要。

在启动漫长的 RFP 过程和遴选供应商之前，针对 SASE 转型准备您的业务和 IT 用例，并决定哪些变化需要尽早进行。

定义商业和 IT 驱动因素

安全和网络现代化将帮助您的组织实现什么目标？

根据 Cloudflare 委托 Forrester Consulting 进行的一项全球调查，过去三年内，全球 IT 和安全决策者的责任显著增加了。如果您正在考虑 SASE，那么您的组织很可能面临着类似的挑战：

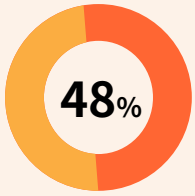
过去五年来 IT 和安全团队的责任增加

（显示“我们在五年前不负责这项工作”）

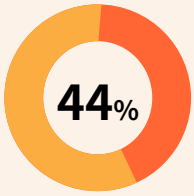
基数：449 名全球决策者，具有总监级别、更高影响力或指导组织的企业解决方案选择
注：显示您的回应
来源：Cloudflare 委托 Forrester Consulting 进行的研究，2023 年 8 月

贵组织的 IT 和安全团队目前面临的主要挑战是什么?

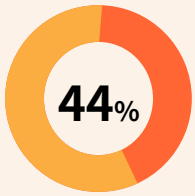
排名前五位



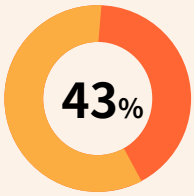
要支持不断发展的用户类型和不断增长的用户数量（例如人类、机器、本地、混合和第三方）



攻击面扩大



难以维护或提高 IT 和安全团队生产力



合规要求的复杂性增加

基数: 449 名全球决策者，具有总监级别、更高影响力或指导组织的企业解决方案选择
注: 显示排名前五的回应
来源: Cloudflare 委托 Forrester Consulting 进行的研究，2023 年 8 月

如果要解释 SASE 的业务和 IT 用例，请从考虑以下问题的答案开始:

- *您当前的架构是否能够有效地连接和保护所有用户、设备、应用程序和数据?*
- *接下来的 12 个月内，对您当前系统（通常来自多个不同的供应商，难以维护）进行维护/升级的成本是多少? 接下来的 3-5 年呢? 下一个 10 年呢?*
- *您需要哪些 IT 预算和资源来满足组织不断增长的数字需求? 对于技术投资的 ROI，高管的期望是否发生了变化?*
- *过去是否曾经因为网络宕机和其他网络漏洞而对客户体验、员工生产力或创新能力产生了重大影响?*
- *您的组织最近是否因为可预防的供应链入侵和/或由于安全或网络供应商的漏洞而导致数据丢失?*

在制定采用 SASE 架构的路线图之前，企业通常从总体大局开始，例如改善业务敏捷性，降低 IT/安全复杂性，减少网络风险，提高整体技术效率 — 所有这些综合起来，都会改善总拥有成本。

下面的图表可以帮助您评估哪些最优先挑战可以通过将网络和安全整合到 SASE 架构中来解决。

列出并排序：您面临的最大挑战是什么？

挑战：提高业务敏捷性	
如果您的现代化目标如右方所示，则这是一个**核心业务驱动因素**	→ 简化并加快任何用户在任何设备上的安全连接，无论位于何处 → 提高网络可靠性，减少用户在任何设备上的延迟，无论身在何处 → 增加网络容量/功能时，减少或消除停机时间和服务中断 → 减少 IT 管理和故障排除所用时间
然而，您需要一个全新的解决方案，因为**您的当前基础设施……**	⊘ **不能跟随您的业务增长而扩展。**过去，组织只需要网络以支持办公室的工作人员，但现在应用程序涉及每个工作职能。因此，如果您的架构基于“城堡+护城河”方法，增加连接要求意味着在您运营的每个地方添加更多数据中心设备。但是，随着您的员工规模增长，配置更多防火墙、路由器、负载平衡器和其他设备会带来新的风险、停机时间和潜在的服务中断。 ⊘ **导致欠佳的用户体验。**过去组织通过部署 VPN 设备将用户连接到托管应用程序的公司网络。然而，随着远程访问的需求出现，许多应用程序现在位于云基础设施即服务 (IaaS) 平台上，传统的 VPN 解决方案难以配置。这经常导致终端用户的应用程序和连接性能不佳。 ⊘ **效率低下。**传统网络将出口集中通过边界/数据中心防火墙。例如，无论分支流量是前往数据中心还是云端/互联网，都要经过总部路由。这对于访问互联网特别低效，因为需要将流量回传到针对出口的安全服务。

	⊘ **缺乏灵活性。**管理多个云服务提供商可能会对每个提供商的安全方法产生依赖。应对每个提供商特定的配置和要求可能变得极为复杂，并导致安全漏洞。
挑战：降低复杂性	
如果您的现代化目标如右方所示，则这是一个**核心业务驱动因素**	→ 淘汰传统数据平台，整合供应商，并优化云服务支出 → 减少维护网络安全设备的硬件和运营（包括带宽）成本 → 释放 IT 和安全资源以用于更长期战略项目和新技术
然而，您需要一个全新的解决方案，因为**您的当前基础设施……**	⊘ **不断推高成本。**由于多种原因，企业网络是庞大的成本中心。网络必须过度配置以支持预期容量；设备（例如 VPN、硬件防火墙和 MPLS 连接）必须成对购买以便故障转移，并且每隔几年进行更新；更多用户和设备需要更多的连接；更多应用意味着更多带宽成本；等等。 ⊘ **本质上是复杂的。**例如，您可能在两台本地服务器之间的网络层连接（通过防火墙执行安全控制），多个用户通过 NAC WiFi 或 VPN 进行连接（各有自己的访问策略），以及来自受管设备、非受管设备、企业管理的浏览器、自带设备 (BYOD) 应用程序等的大量用户。随着更多技术的加入，复杂性也在增加—反过来，您的网络设计也会变得更加脆弱和难以改变。 ⊘ **带来复杂、反应迟钝、不可扩展的流程。**您的 IT/安全团队花费太多时间管理孤立的部署、多个仪表板、复杂的用户界面和冗余的功能。

挑战：降低网络风险，保护不断增长的攻击面	
如果您的现代化目标如右方所示，则这是一个**核心业务驱动因素**	→ 减少数据泄露、多渠道网络钓鱼、勒索软件、企业电子邮件破坏、API 滥用和 DDoS 攻击的风险 → 确保您的组织可以安全地使用生成式 AI，而不会将知识产权和客户数据置于风险之中 → 监控和保护受监管的数据（例如财务数据、健康数据、个人身份信息、精确数据匹配） → 减少在事件响应上花费的总时间
然而，您需要一个全新的解决方案，因为**您的当前基础设施……**	⊘ **缺乏 Zero Trust 方法。**基于边界的网络设计原则侧重于信任内部用户和应用程序，并阻止外部威胁。但它并非设计用于连接和保护任何地方的用户（内部或外部）、任何地方的应用程序（本地、数据中心或云）和任何地方的威胁。换句话说：您当前的系统缺乏细粒度、一致的安全策略，无法覆盖所有用户、设备和环境。 ⊘ **缺乏完全的可见性和执行。**由于用户和应用程序连接方式数量不确定，存在不一致的安全和网络控制，影响到您了解风险的能力。 ⊘ **越来越脆弱。**传统基础设施（如数据中心和广域网）和传统安全单点解决方案（例如防火墙和 VPN）本身就是横向移动的入口点。迅速增长的远程办公对您的 VPN 造成了压力，而脆弱的 VPN 让攻击者在您的网络中几乎可以到达任何地方。 ⊘ **缺乏内置的隐私和数据保护。**随着您继续将更多应用程序和数据迁移到云端，一些传统供应商难以遵守不断变化的数据隐私和数据保护要求。

附录 B: 定义 SASE 的范围

SASE 已成为应对上述 IT 和业务挑战的理想架构。

在真正的 SASE 方法中，网络连接和安全服务融合于单一云平台上，并从一个控制平面交付，从而降低复杂性。

因此，您的候选供应商应该提供一个可编程、可组合的网络架构，以最低延迟提供您需要的所有服务：

- ☑ **网络服务**将来自各种网络的 L2-7 层流量转发到一个全球企业网络。这些服务提供防火墙、路由和负载平衡等功能。
- ☑ **安全服务**检查网络上传输的流量，对第 3 层 (IP)、第 4 层 (TCP、UDP、ICMP) 和第 7 层 (DNS、HTTP、SSH) 流量执行基于防火墙代理的过滤，通过默认拒绝控制谁可以访问什么。
- ☑ **运营服务**提供平台范围的功能，例如日志记录、API 访问和通过 Terraform 之类的供应商提供的全面基础设施即代码支持。
- ☑ **跨所有服务的集成**允许管理员一次定义策略，并在所有连接的服务中上下文中重复使用。

SASE 架构的核心组件

Zero Trust 网络访问 (ZTNA)

这是什么?

Zero Trust 安全模型假定威胁同时存在于网络内外; 因此，个人、应用程序或设备每次尝试访问企业网络上的资源时，都需要进行严格的上下文验证。

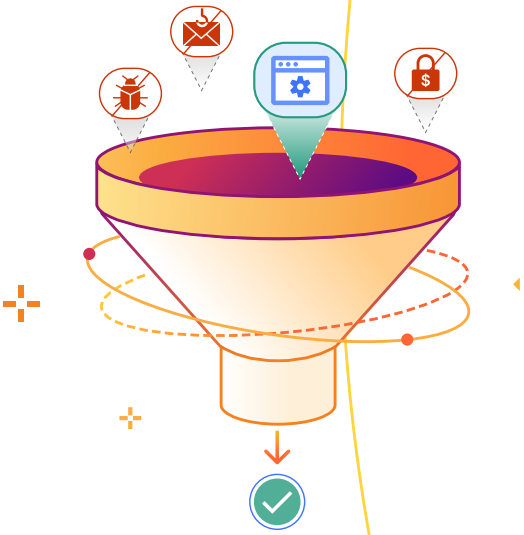
与过度授权的传统网络访问工具 (例如 VPN) 相比，Zero Trust 网络访问 (ZTNA) — 这是使 Zero Trust 方法成为可能的一种主要技术 — 在用户和他们所需资源之间建立一对一连接，并要求定期重新验证和重建这些连接。

考虑因素:

- 验证 SASE 供应商提供的 ZTNA 解决方案类型是否能够满足您的短期和长期架构需求。例如:
- **基于客户端的 ZTNA** 需要在所有端点上安装一个名为 “客户端” 或 “代理” 的软件应用程序。如果组织对专用网络访问、日益增多的受管和未管设备或设备姿态感到担忧，那么基于客户端的 ZTNA 可能是一个有效的选择。
- **无客户端 ZTNA** 无需端点软件即可执行 Zero Trust 访问策略。如果一个组织主要专注于保护某些基于 Web 的应用程序，或者为承包商/未受管设备提供简单、安全的访问，那么无客户端模式可以迅速实施。

其他重要的 ZTNA 考虑因素包括:

- **努力程度**: 应用连接器的工作流程可能因供应商架构而异，例如，基于虚拟机还是安装在客户基础设施上的轻量级后台程序，以及它们的相关吞吐量限制 (如果有)。
- **对传统应用程序的支持:** 一些组织仍然拥有对业务至关重要的本地传统应用程序。大多数 ZTNA 解决方案可以轻松支持云和 Web 应用程序，但对于业务需要支持的长尾资源 (例如专用网络中的资源或涉及双向流量的资源)，实施细节可能有所不同。
- **身份提供商 (IdP) 集成:** 许多组织已有一个 IdP。一些 ZTNA 解决方案在同时支持多个 IdP 或甚至同一 IdP 的多个实例方面比其他解决方案更灵活，这对于容易发生并购或剥离的组织尤其有用。



安全 Web 网关 (SWG)

这是什么?

安全 Web 网关 (SWG) 过滤掉无用的 Web 流量内容和阻止危险或未经授权的用户在线行为，以防止网络威胁和保护数据。SWG 可以部署在任何地方，因此非常适合用于保护混合办公。

与许多安全产品一样，SWG 是一个单点产品，通常与其他网络连接和网络安全功能分开管理。然而，在建立 SASE 框架后，企业可以在一个基于云的供应商处整合和维护其网络与网络安全。

考虑因素:

SWG 需要速度快，因为组织所有前往互联网流量都要通过这里。如果 SWG 运行缓慢，那么用户任何前往互联网的流量将变慢。如果前往互联网的流量缓慢，用户可能发现网页加载缓慢，视频通话卡顿或丢包，或者无法完成工作。

为了减少延迟并确保良好的用户体验:

- **尽可能接近最终用户**: 所选 SASE 平台的 SWG 服务应该缩短请求在公共互联网花费的时间。
- **网络互联合作伙伴关系**: 如果您的 SASE 提供商与全球许多 ISP 或托管提供商有牢固的对等互连关系，这些提供商将把直接流量发送到网络，而不是第三方。这样可以跳过传输提供商之间拥挤的路径，让用户快速访问他们所需的服务。

此外，SWG 通过与内联云访问安全代理 (CASB) 功能协同工作以控制数据移动并保护数据。下一节将介绍 CASB。

云访问安全代理 (CASB)

这是什么?

使用云和 SaaS 应用程序导致使数据保持私密和安全变得更加困难。团队可能在未经 IT/安全团队许可的情况下使用某些 SaaS 应用程序（例如，影子 IT），这可能导致潜在数据丢失和数据泄露。

为了保护云中的数据，组织通常也使用基于云的安全服务。CASB 与数据丢失预防 (DLP) 功能紧密结合，以更有效地保护 SaaS 应用程序，但许多组织仍在使用传统的本地 DLP 设备，这些设备完全不是为保护云而设计的。这加剧了“单点解决方案”问题，并带来挑战：必须单独谈判数份合同，多次配置安全策略，实施和管理多个平台会增加 IT 复杂性。

现代化的云访问安全代理 (CASB)，其中包括 SaaS 安全姿势管理 (SSPM) 作为一种原生功能而非附加产品提供，是应对这些挑战的一种解决方案：CASB 提供数据安全控制，以及对组织云托管服务和应用程序的可见性。

考虑因素：

- **可扩展性**：CASB 必须管理大量数据和多个云平台以及应用程序。您的 SASE 供应商的 CASB 功能应该能够随着您的组织增长而扩展。
- **易于集成**：确保 CASB 能够与您的首要应用程序（例如 Google Workspace，Microsoft 365，Salesforce）进行快速、基于 API 的集成。如果与您的首要应用程序之间缺乏强健的集成，CASB 将无法获得对未授权 IT 和潜在安全威胁的充分可见性。
- **数据隐私**：CASB 服务是否会保持数据私密，抑或只是接触到敏感数据的另一个外部方？如果 CASB 解决方案将客户数据转移到云端，那么数据有多安全和私密？这些问题对于按照严格数据隐私法规运营的组织来说是特别重要。
- **缓解**：并非所有 CASB 都提供在识别到安全威胁后立即予以阻止的能力。一些 SASE 解决方案超越监测，提供“找到和修复”工作流程，帮助管理员更有效地针对安全发现采取纠正措施。
- **集成 DLP**：集成数据丢失防护 (DLP) 的 CASB 服务更容易扩展可见性，并统一跨所有应用程序、用户和服务的数据保护。

远程浏览器隔离 (RBI)

这是什么?

RBI 将 Zero Trust 原则应用于 Web 浏览，假设任何网站代码（例如 HTML、CSS、JavaScript）默认情况下均不予信任并运行。RBI 在云端加载网页并执行任何相关代码，远离用户的本地设备。这种分离有助于防止恶意软件下载，最小化零日浏览器漏洞的风险，并防御其他基于浏览器的威胁。

广泛的数据保护控制还可以防止在隔离浏览器中发生危险的用户操作，例如限制下载、上传、复制粘贴、键盘输入和打印功能。一些组织使用无客户端方式部署的 RBI 来帮助保护数据免受未受管设备的影响。

考虑因素:

- **兼容性**: 第一代技术，例如文档对象模型 (DOM) 操纵和像素推送，扰乱了用户与现代 SaaS 和基于 HTML5 的应用程序的交互。基于 SKIA 的网络供应商渲染 (NVR) 推送 HTML5 绘制命令而非像素，以无缝支持任何用户在任何浏览器中与任何应用程序进行交互。
- **可扩展性**: 如果远程浏览器在距离本地设备太远的地方运行，仅靠 NVR 技术不足以在日常浏览对所有用户透明。RBI 服务必须通过一个全球网络交付，其数据中心与所有互联网用户之间的延迟在数十毫秒内。每个数据中心的每台服务器都必须拥有大量计算资源，以真正将 RBI 服务扩展到每一个地方。
- **部署:** 由于混合办公流行，加上现在劳动力团队中包括大量承包商，需要同时提供基于客户端和无客户端的部署选项来覆盖所有用户。无客户端选项应支持已接入 SASE 网络的办公室用户（例如，通过 WAN 连接器）以及使用未受管设备的远程用户。
- **可组合性**: 无论是基于客户端还是无客户端的部署，所有 SWG、ZTNA 和 DLP 功能都应在远程浏览器中可用，提供相同的策略控制和可见性。与无客户端 ZTNA 的原生集成可保护承包商和未受管设备上的使用中数据。与云电子邮件安全的原生集成支持隔离可疑电子邮件链接，以防范多渠道钓鱼攻击。

软件定义广域网 (SD-WAN) 或 WANaaS

这是什么?

在 SASE 架构中，组织可以选择采用软件定义广域网 (SD-WAN) 或 WANaaS，有时也称为网络即服务 (NaaS)，以便跨越远距离连接和扩展运营（例如办公室、零售店、数据中心）。

- **SD-WAN**: 大型组织通常使用广域网 (WAN) 将各分支办公室和位置（局域网，缩写 LAN）连接到企业中央网络。软件定义广域网 (SD-WAN) 是一种更灵活的 WAN 架构，通过控制软件进行路由来连接 LAN，可与各种网络硬件平台和连接选项配合使用。
- **WANaaS** 是一种云服务模型，其中客户使用云提供商的网络连接服务。它遵循“轻分支，重云端”方法，主要通过软件运行网络功能，从而允许公司现代化其网络，而无需对其自身的网络基础设施进行大规模更改 — 它们仅需要互联网连接。WANaaS 可以替代 VPN、多协议标记交换 (MPLS) 连接或其他传统网络配置。它也可以取代传统的本地网络硬件，例如防火墙设备和负载平衡器。

考虑因素:

- 例如，如果对分支之间的流量不予检查，许多 SD-WAN 实施将可能增加风险。因此，对于希望最大程度减少性能和安全折衷的组织来说，提供原生网络连接和 Zero Trust 安全的 SASE 解决方案通常更具吸引力。
- 对于 WANaaS，网络服务是从云服务提供商采购的，而不是组织完全配置自己的网络。对于 WANaaS，您的组织仅需互联网连接即可配置和使用内部网络。根据服务的配置方式，这可能比 SD-WAN 提供更大的灵活性并节省更多成本，就像其他云服务模型（例如 SaaS 和 Iaas）相对于传统的本地计算一样。

企业网络防火墙或 FWaaS

这是什么?

企业使用防火墙来保护他们的网络，控制流量，并执行针对互联网交互的策略。随着时间的推移，防火墙的使用和其提供的服务已经得到发展，具有各种功能和形式。

- **企业网络防火墙:** 大多数组织在其网络边缘使用企业防火墙设备，用于隔离组织的内部网络与互联网。组织也可以使用硬件和虚拟化防火墙的组合来将流量隔离到其内部私有云。
- **防火墙即服务 (FWaaS)**: 企业网络防火墙在地理位置上受到限制，因为它们仅部署到有限的地点。这在支持混合办公团队和云应用程序方面就会造成问题。为了支持这样的用例，FWaaS 提供防火墙策略执行，而无需管理和部署设备。通过从云端使用防火墙服务，而非管理防火墙设备，这有助于组织解决扩展和架构挑战。

考虑因素:

- 与其让硬件防火墙执行它本身设计不具备的功能，不如考虑哪些功能最适合从云服务交付。
- 作为基准，组织可以使用 FWaaS 提供深度防御，从而为到达组织网络的流量提供上游保护。
- FWaaS 作为安全 Web 网关的补充，通过 Web 和云检查流量并阻止规避技术的使用，帮助组织提高安全性。
- 如果采用 “轻边缘”（即最小化硬件和最小化管理）理念来连接和保护远程站点（例如门店和分支办公室），可考虑使用 FWaaS。

基于全球连通云构建的平台的额外组件

SASE 将用户的安全访问作为网络架构的一部分。*(值得注意的是，行业分析公司 Forrester 将 SASE 模型归类为“Zero Trust 边缘”，缩写为 ZTE)*。然而，并非所有组织都针对 IT、网络安全和网络团队采用统一的方法。因此，它们可能优先考虑安全服务边缘 (SSE) — SASE 功能的一个子集，主要专注于保护对 Web、云服务和私有应用程序的访问。

虽然大多数 SASE 平台包含前面提到的核心功能，但在**全球连通云上构建的单一供应商 SASE 平台将捆绑额外的 SSE 功能**（下文将进一步说明）。全球连通云是一个统一的云原生服务平台，简化了跨 IT 环境的安全“任意对任意”连接。

基于全球连通云构建的 SASE 平台的额外功能	
云电子邮件安全 (CES)	电子邮件是的首选通讯方式，研究表明超过90%的网络攻击都始于钓鱼邮件。钓鱼攻击利用用户的信任进入系统，无需依赖网络入侵、恶意软件传播或命令和控制回调。多渠道钓鱼攻击活动（如前所述）则更进一步，通过各种应用程序接触用户。 为了应对这种不断增长的风险，云电子邮件安全补充云电子邮件提供商的内置安全能力，并与其他 SASE 服务集成，能够全面保护超越电子邮件的多渠道威胁。
数据丢失防护 (DLP)	为了防止数据在未经许可的情况下被窃取或破坏，DLP 技术可以检测传输、使用和静态数据，并覆盖 Web、SaaS 和私有应用程序，尤其是作为更广泛的 SASE 平台的一部分时。例如，与 SWG 结合使用，DLP 解决方案可以控制传输中的数据；与 CASB 结合使用，DLP 解决方案可以检测静态数据。
Digital Experience Monitoring (DEX)	DEX 是一种工具，用于监控用户行为以及在网站流量和应用程序性能方面的体验。它帮助组织捕获关于网络问题、性能下降和应用程序中断的实时数据。这有助于准确定位网络问题并识别连接异常的根本原因。

递归式 DNS 过滤	DNS 过滤阻止或覆盖域名的 IP 地址解析，从而使恶意、有风险或不可接受的网站和应用程序无法通过任何端口和协议在任何设备上访问。当作为递归 DNS 解析服务的一部分提供时，它可以快速、透明地保护连接到大量网络位置的任何东西，例如分布式办公室，而无需设备代理、网络连接器或路由更改。它可以作为 SWG 的一部分，与其他技术一起保障内部用户和设备的安全。
权威 DNS 安全	DNS 安全保护DNS 基础设施免受网络攻击，确保其运行快速可靠。有效的 DNS 安全策略包括多重防御，包括建立冗余 DNS 服务器，应用 DNSSEC 之类的安全协议，并要求进行严格的 DNS 日志记录。 通过扩展单一供应商 SASE 平台提供的权威 DNS 安全可以为通过无客户端 ZTNA 保护的公共主机名进一步加强安全性。
内容交付网络 (CDN)	CDN 为网站和互联网服务提供快速、高效、安全的内容传递。如果配置得当，CDN 还可以帮助保护网站防范 DDoS 攻击等威胁。 通过扩展单一供应商 SASE 方法提供 CDN 时，可以进一步提高面向公众资源的性能，在流量通过其他单次通过安全步骤（例如 CASB 或 SWG）时最大限度减少跳数。
Web 应用程序和 API 保护 (WAAP)	WAAP 是一个大类，涉及旨在保护 Web 应用程序和 API 的安全解决方案。其中包括 Web 应用程序防火墙 (WAF)、机器人管理、DDoS 缓解 和 API 保护 服务（例如速率限制、模式验证、API 身份验证）。 这些能力巩固针对第 7 层资源（例如内部 ZTNA 保护的应用程序）的核心 SASE 服务，加强对内部威胁和横向移动的防护。WAAP 和核心 SASE 服务可以在全球连通云融合，即使将额外的安全服务引入到 Web 流量中，也能保持强大的性能。
专用骨干网	尽管 SASE 提供商承诺提供云交付的网络，但事实上许多供应商构建的网络仅支持前往互联网的流量，而他们的数据中心之间不存在互连。因此，远距离 WAN 网络连接的性能变得不可预测。 要提供企业级网络体验，请确保您的 SASE 供应商拥有适当的专用骨干网来支持您的 WAN 流量。专用骨干网是一个专用网络，作为不同地区数据中心之间的快速通道。这可以避免公共网络的拥塞和不可预测的性能，从而消除了导致延迟的主要因素。

尽管每个企业IT环境都包含高度特定的工具、流程和架构配置，但全球连通云可以适应组织的独特需求，同时提供一致的用户体验。这为技术领导者提供了一个可定制的控制平面，用于他们的整个 SASE 平台。

如需进一步了解如何演进到全球连通云上构建的单一供应商 SASE 架构，请阅读 Cloudflare 的 SASE 参考架构。

引用

[1] Gartner，《单一供应商 SASE 的关键能力》，Jonathan Forest、Nat Smith、John Watts。2023 年 8 月 21 日。

[2] Gartner，《预测分析：全球安全访问服务边缘》，Nat Smith、Neil MacDonald、Christian Canales、Andrew Lerner、Jonathan Forest、John Watts、Shailendra Upadhyay、Charlie Winckless。2023 年 10 月 10 日。

CLOUDFLARE

010 8524 1783 | enterprise@cloudflare.com | cloudflare.com/zh-cn

REV:BDES-5482.2024FEB07