The bridge to possible

2022 全球网络趋势报告

专题研究：SASE 最新动态和网络即服务 (NaaS) 的兴起

专题研究：SASE 最新动态

目录

采用安全访问服务边缘 (SASE) 战略

混合办公模式需要部署一个整体性的 SASE 战略，以便随时随地提供始终如一的卓越用户体验。

为了解决围绕安全访问服务边缘 (SASE) 引发的市场热情和疑问，我们展开了这项专题研究，作为《2022 全球网络趋势报告：网络即服务 (NaaS) 的兴起》的补充和完善。

在采用率激增的远程办公和混合云的推动下，SASE（发音为“sassy”）可以通过任何网络、从任何位置或设备为任何应用提供安全且无缝的连接。

SASE 将网络和安全功能整合为一个统一的云原生解决方案或服务。

与传统的安全解决方案相比，它的安全策略和实施过程更贴近分布日趋分散的终端用户和应用。它对零信任策略进行扩展，消除了不断向数据中心回传数据的需要，有效地减少了网络负载和瓶颈问题，提供了卓越的用户体验。

作为传统安全堆栈的替代方案，它提供了从边缘到边缘的安全接入，全面覆盖数据中心、远程办公室、漫游用户，乃至更广的范围。

本专题研究重点关注 SASE 的最新趋势和洞见，相关数据来自多项市场调查，相关观点源于知名行业分析师和专家。我们希望这些信息能帮助您更好地理解 SASE 的优势和作用，制定行之有效的网络、安全和云战略。

– Omri Guelfand，思科网络服务副总裁

> “关于什么是 SASE，市场尚无定论。然而，业界正在形成的共识与我们的一贯观点不谋而合，即 SASE 不是一项全新的技术，而是将现有的网络（如软件定义广域网 [SD-WAN] ）和安全技术（如安全 Web 网关 [SWG]）整合到一个基于云的安全连接解决方案。”
>
> – Dell’Oro Group[1]

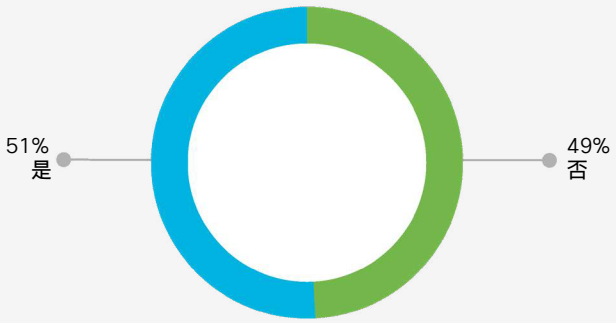
IT 面临的挑战：提供安全、云优先的混合办公体验

不可否认，IT 团队目前面临的两个最大趋势是继续向多云应用战略过渡和采用混合办公模式。随着用户和应用比以往任何时候都更加分散，连接和保护它们的复杂性也急剧增加。

由于混合办公导致员工和工作场所呈密集分布，应用跨多个私有云和公共云分布的情况更加明显。随着这种高度分散趋势的发展，试图保持高质量、包容性用户体验的挑战与曾经高度可控的企业内部环境形成了鲜明的对比。

在最近的调查中，76% 的 IT 团队表示，远程办公员工更难保持互联互通，[2]51% 的组织表示，在过去 18 个月中，他们在连接员工和公司资源方面遇到了问题。[3]

您/您的公司在过去 18 个月中，是否难以让员工保持互联互通？



以数据中心为中心的应用模式向以支持互联网的云为中心的模式的持续转型，迫使 IT 团队全盘重新思考他们的网络战略。同样，当用户和应用都进行非本地部署时，安全团队需要努力提供安全且无缝的用户体验，因为在这种部署下更容易受到意外暴露或蓄意攻击。

这有助于解释人们对云交付 SASE 模式高度感兴趣的原因，该模式将 SD-WAN 等网络解决方案与安全服务边缘 (SSE) 和零信任网络接入 (ZTNA) 等云安全解决方案结合在一起。

SASE 旨在连接和保护用户与应用，无论它们如何部署或托管，最终提供更出色、更一致、更安全的用户体验。它还有望降低 IT 成本和复杂性，提高网络灵活性和性能，并最终改善应用体验。

> “由于疫情的影响，截至 2020 年的最高点，与疫情前的基线相比，全职或兼职远程办公的美国员工数量增加了 450%。虽然比率已经开始下降，但我们预计长期远程办公的比率将稳定在比疫情前基线高 200% 的水平。”
>
> – Dell’Oro Group[4]

基本结论：

员工日趋分散和多样化的办公模式将继续存在。正确实施 SASE，可以连接并保护分散的用户和应用，调整网络和安全策略，并减少网络和安全管理负担及风险。

SD-WAN 和 SASE 之间的关系

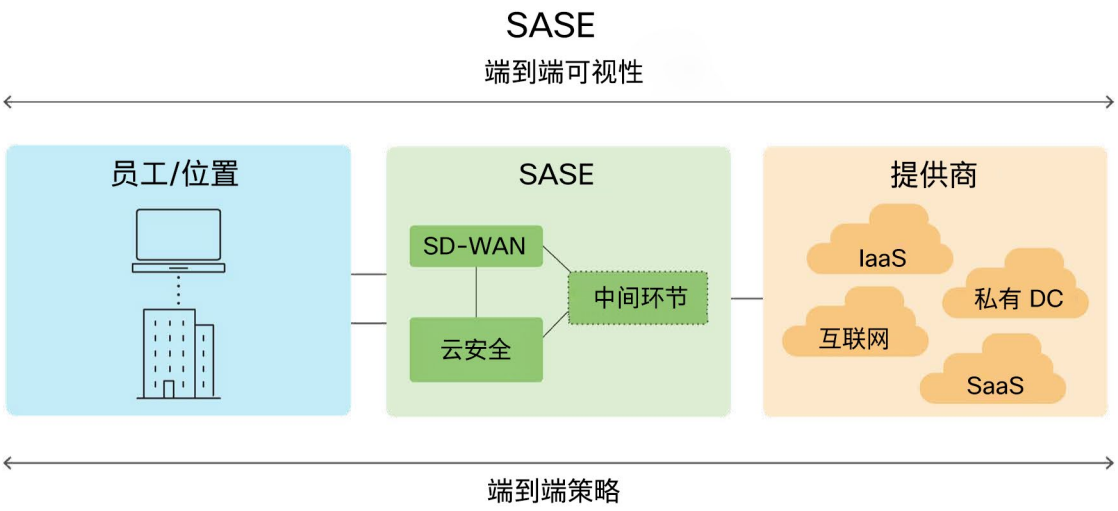
围绕 SASE 引发的市场疑问催生了一些现有 SD-WAN 解决方案相关的问题。SASE 是否取代了 SD-WAN？它们是否互为补充？还是说它们是针对不同需求提供完全不同的解决方案？

答案很简单：SD-WAN 是 SASE 的基础。

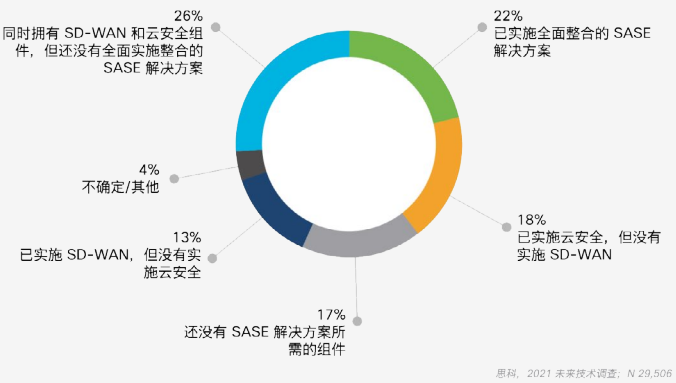
SASE 将 SD-WAN 本地安全功能与以云为中心的安全功能相结合，连接和保护用户与应用，无论它们如何部署或托管。作为一个重叠架构，如果没有 SD-WAN 提供的保障措施，SASE 无法提供无处不在的安全，包括：

- 启用网络地址转换 (NAT)
- 将网络分割成多个子网络
- 监测和阻止恶意软件与恶意流量
- 限制未经授权的用户
- 防止不需要的内容或应用
- 通过防火墙阻止不需要的入网和 VLAN 之间的流量
- 确保站点间/隧道内 VPN 的安全
- 基于位置访问控制的地理围栏

> “SASE 并没有使 SD-WAN 过时。相反，SD-WAN 是 SASE 的一个基础组成部分。SASE 产品融合了多种网络和安全即服务功能，如 SD-WAN、安全 Web 网关 (SWG)、云访问安全代理 (CASB)、下一代防火墙 (NGFW) 和零信任网络访问 (ZTNA)。”
>
> – 2021 Gartner®，快速回答：SASE 是否取代了 SD-WAN？[5]



您在 SASE 采用全程中处于什么阶段？



IT 组织应该从 SD-WAN 还是云安全入手？许多组织采取分阶段的方式来实施 SASE。大多数组织正处于 SASE 全程的中间阶段，即将 SD-WAN 与云安全组件相结合，尚未全面整合或实施。

18% 的公司有云安全但没有 SD-WAN，13% 的公司有 SD-WAN 但没有云安全。[6]

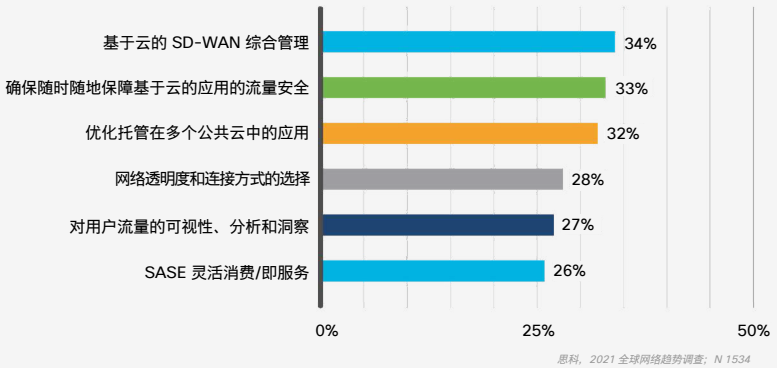
基本结论：

SD-WAN 是 SASE 的一个基础要素，它与以云为中心的安全解决方案或服务相辅相成，保护本地部署、云和边缘域的用户和数据。

SASE 功能需求

由于 SASE 代表了网络和安全功能的整合，34% 的组织正在优先考虑提供基于云的 SD-WAN 综合管理解决方案和服务。确保随时随地保障基于云的应用的流量安全 (33%)，优化托管在多个公共云中的应用 (32%)，以及提高网络透明度和灵活性 (28%) 也被列为优先考虑功能。

在您看来，SASE 的哪些功能将是您所在组织的优先考虑项？



为了连接远程员工：

43% 的组织计划使用 VPN 作为一种服务。

36% 希望采用零信任网络访问和多因素身份验证功能。

35% 对基于主机的统一客户端感兴趣。

35% 希望将其 SD-WAN 扩展到移动和家庭用户。

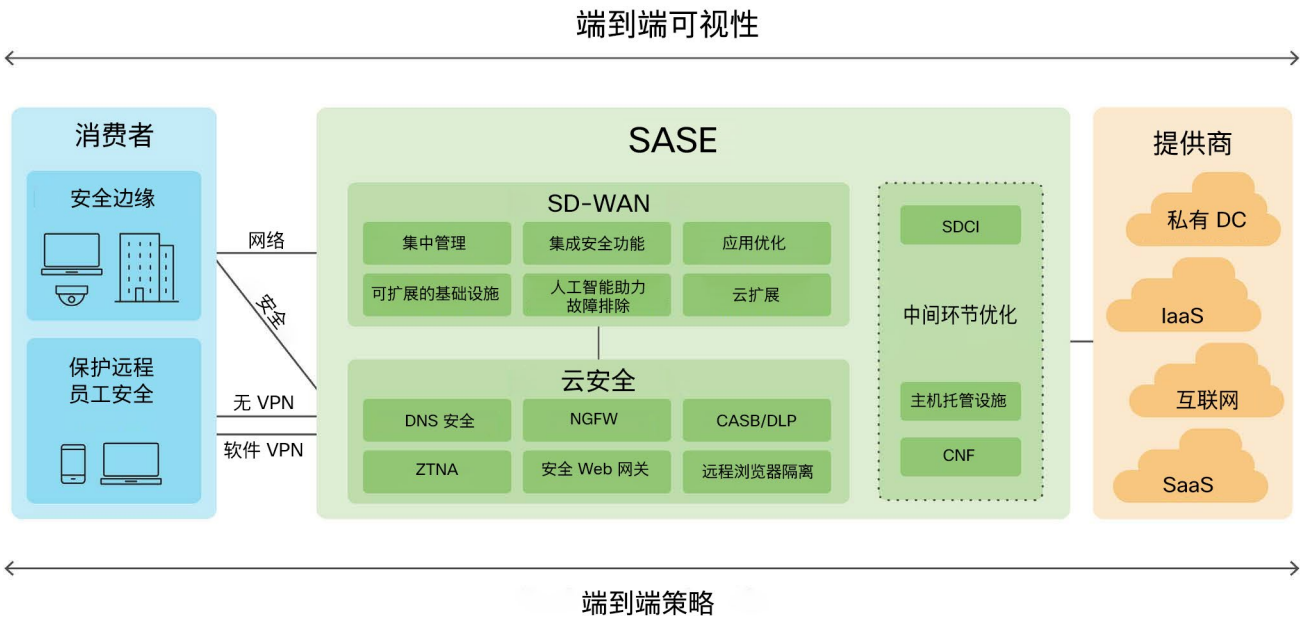
虽然 SASE 架构、解决方案和服务不断发展，但从根本上说，它们旨在汇集 SD-WAN 和云安全提供的部分或全部核心功能。

SD-WAN	云安全
集中管理 一个集中的、高度可视化的控制面板，便于设备配置、网络管理、监控和自动化。包括网络边缘的零接触配置。	**零信任网络访问 (ZTNA)** 一个可以减轻未经授权的访问，遏制漏洞，并减少攻击者在网络中的横向移动的安全框架。ZTNA 应与强大的身份和访问管理相结合，验证用户的身份，并在授予授权应用访问权之前建立设备信任。
云网络扩展和中间环节优化 广泛的云端集成，实现与任何站点到云端和站点到站点配置的无缝、自动连接。包括通过软件定义的云互连 (SDCI) 和主机托管集成优化中间环节的连接。	**安全 Web 网关 (SWG)** 一个记录和检查 Web 流量的网关，以提供全面的可视性、URL 过滤和应用控制，以及恶意软件防护。
应用体验 能够监测和验证 Web 应用的可用性和性能。详细的指标和瀑布图显示了 Web 组件的顺序获取和加载，以确定错误和瓶颈问题，了解对应用性能的影响。	**带有入侵防御系统 (IPS) 的云端防火墙** 基于软件的云部署服务，帮助管理和检查网络流量。
灵活且可扩展的基础设施 一个广泛的物理和虚拟平台，提供高可用性和吞吐量、多千兆端口选项、5G 蜂窝网链路和强大的加密功能。通过动态选择符合服务水平要求的最有效的 WAN 链路，优化 WAN 流量。	**云访问安全代理 (CASB)** 检测和报告整个网络中使用云应用的软件，发现影子 IT，并阻止有风险的 SaaS 应用和特定操作，如发布和上传。
人工智能助力故障排除 强大的 AI/ML，用于优化网络性能，自动化常规人工任务，并加速故障排除。提供智能警报、自我修复和预测性互联网改道能力。	**防数据丢失 (DLP)** 对数据进行在线分析的软件，以提供对推送或拉出组织网络或云之外的敏感数据的可视性与可控性。
集成安全功能 强大的安全功能，与云安全相辅相成，保护分支机构、家庭用户和基于云的应用免受渗透。	**远程浏览器隔离 (RBI)** 将 Web 流量流量与用户设备隔离的软件，以减轻浏览器传递威胁的风险。
基于身份的策略管理 跨多个地点和域的微分段和基于身份的策略。	**DNS 层安全** 作为抵御互联网上威胁的第一道防线的软件，在与一个 IP 地址建立连接之前就会阻止恶意的 DNS 请求。强大的 DNS 安全功能可以大幅减少安全团队每天必须处理的威胁数量。
高级洞察 通过全面的、逐跳的分析，增强对应用、互联网、云和 SaaS 环境的洞察。实现故障域的隔离，并提供切实可行的洞察，加速故障排除，并尽量减少或消除对用户的影响。	**全面、广泛的威胁情报** 威胁研究人员、工程师和数据科学家使用遥测和复杂的系统来创建准确、快速和切实可行的威胁情报，识别新兴威胁，发现新的漏洞，并在威胁扩散之前拦截它们，其规则集支持您安全堆栈中的工具。

除了整合 SD-WAN 和云安全功能外，SASE 模型还可以帮助打破运营孤岛，促进网络和安全团队之间的进一步协调。通过标准化策略、共享遥测数据以及所有安全和网络组件的协调警报，SASE 使 NetOps 和 SecOps 团队能够提高 IT 效率、可视性和保护。

考虑到这一点，企业必须制定一个全面的 SASE 战略，兼顾 NetOps 和 SecOps 的目标，增加操作的一致性，并能够在可预见的未来支持组织的需求。

SASE：详情



> “到 2024 年，30% 的企业将采用同一供应商提供的云安全 Web 网关 (SWG)、云访问安全代理 (SWG)、零信任网络访问 (ZTNA) 和分支机构防火墙即服务 (FWaaS) 功能，而 2020 年这一比例不到 5%。”
>
> – Gartner[7]

基本结论：

在评估 SASE 战略和产品时，组织正在寻求能够提供 SD-WAN 和云安全基本功能的解决方案*和*服务，满足其当前和不断发展的需求。

整合的重要性

现代企业依赖于一些网络环境（数据中心网络、局域网、广域网）和安全解决方案（防火墙、网关以及本地和基于云系统的访问控制）。通过技术和服务的整合，SASE 可以在所有这些方面提供可视性、策略协调和保护。

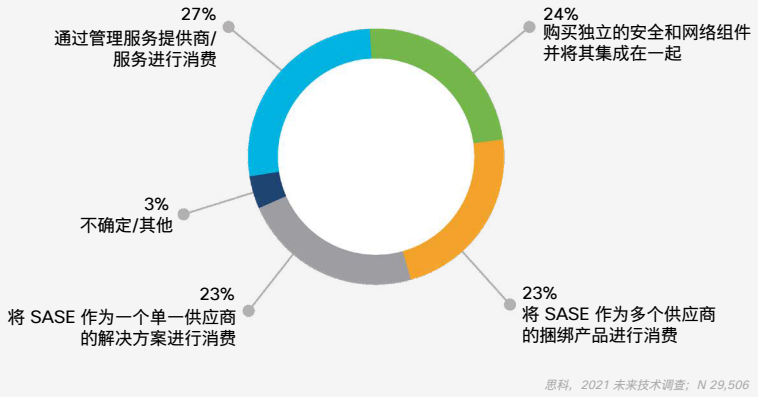
由于最终目标是安全地连接用户和应用，无论它们如何部署或托管，这类整合服务也有助于：

- 减少安全事件的数量。
- 加快故障排除和问题解决。
- 简化系统监控和管理。
- 改善策略的标准化和执行。
- 支持区域合规和数据要求。
- 降低资本和运营成本。

“市场上存在两种主要的 SASE 实施类型：统一型和分类型。统一实施型由单一供应商、紧密集成的 SASE 平台组成。分类实施型是一种多供应商或多产品的实施，与统一型相比，整合程度较低。”

– Dell’Oro Group[9]

您将如何部署和实施 SASE 解决方案？

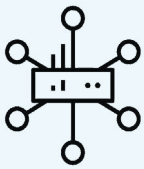


随着单一供应商和多供应商解决方案和服务的出现，以及有可能采用将点解决方案集成在一起的定制架构，组织在如何部署和运营 SASE 方面有很多选择。

因为制定和整合一个定制解决方案或运营一个多供应商 SASE 捆绑产品会带来不必要的复杂性、运营挑战和安全漏洞。故许多组织 (50%) 正在寻求单一供应商提供的统一和/或管理解决方案。

- 70% 的组织同意或强烈同意有效管理多供应商网络和安全堆栈已经变得越来越复杂。
- 26% 的组织同时拥有云安全和 SD-WAN 功能，但尚未完全实施并将它们集成到完整的 SASE 模型中。[10]

无论它是一个定制架构，一个多供应商的捆绑产品，一个单一供应商提供的全程管理服务，或其变体，每个 SASE 解决方案都应该在以下两方面之间提供更好的协调和整合：



SD-WAN 和云安全

- 在 SD-WAN 设备和云安全接入点 (PoP) 之间自动进行流量路由。
- 如果出现性能问题，自动将流量重新路由到另一个 PoP，获得弹性。
- 使用人工智能预测分析，在用户体验受到影响之前，自动将流量重新路由到备用 PoP。

NetOps 和 SecOps 团队

- 能够在 SD-WAN 和云安全实施之间持续共享安全策略（如访问授权和分段）。
- 允许 SD-WAN 和云安全管理平台之间进行数据交换，提供策略和事件的一致可视性。
- 将企业网络结构（如 VPN 和安全组标签）和策略扩展并传播到云安全平台。
- 在 SD-WAN 和云安全管理平台上使用单点登录 (SSO) 管理认证。

终端用户和应用

- 实现 SD-WAN、中间环节（如 SDCI）、多云和 SaaS 服务之间的直接连接。
- 通过对 SD-WAN、云安全 PoP 和 IaaS/SaaS 连接的全面可视性和分析，监测和优化用户体验。

“不整合安全，就不可能做好网络。我需要全面地看待安全问题，从终端到网络一直到应用。通过网络即服务，我需要供应商对网络和安全负责。如果他们只对网络负责，我需要必要的可视性与可控性，确保全面保护和快速缓解威胁。在理想状态下，供应商会把网络和安全都做得非常好。”

– 全球消费品公司 IT 基础设施总监

基本结论:

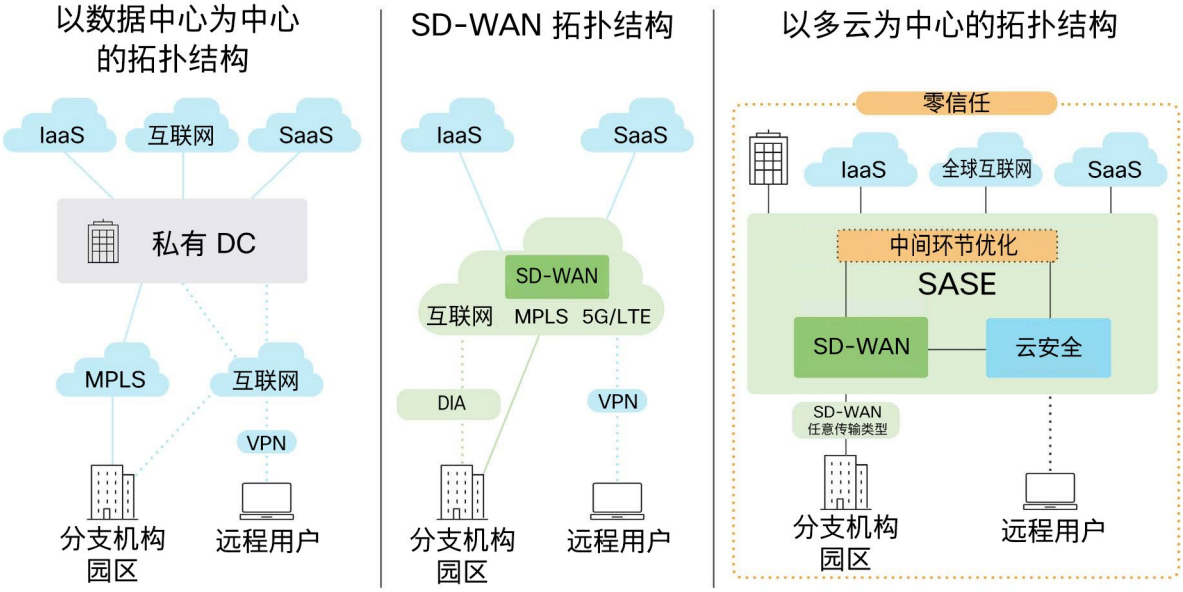
无论是定制架构还是由一个或多个供应商提供的产品，SASE 解决方案和服务都应该在 SD-WAN 和云安全系统之间提供紧密的整合，优化安全的用户体验并简化 NetOps 和 SecOps 的合作。

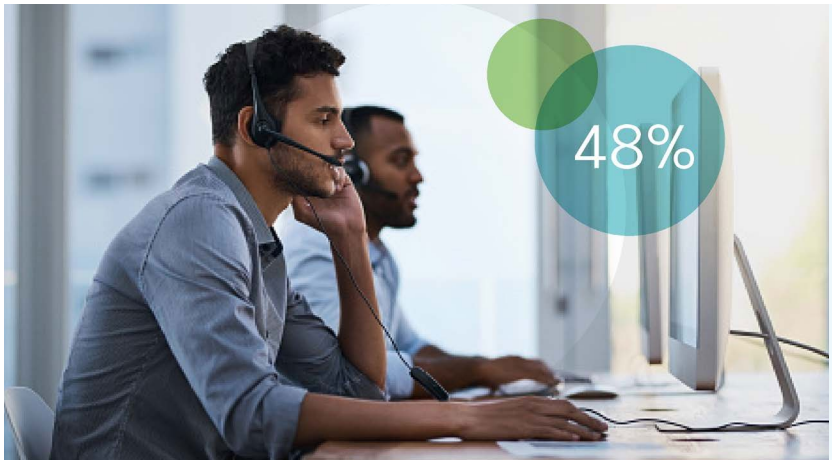
SASE 采用趋势

与任何技术决策一样，正确的 SASE 模式和部署方法对每个组织来说都是独一无二的。已经到位的网络和安全解决方案，以及总体运营战略和业务优先事项，应该是任何 SASE 决策的驱动因素。还应考虑关键举措、监管要求、兼并和收购、供应链运作以及业务弹性要求。

从以数据中心为中心的应用模式迁移到以云或多云为中心的模式的组织可能会从 SD-WAN 开始他们的 SASE 过程，例如，随后是中间环节的优化和云安全整合。

从以 DC 为中心到以多云为中心的拓扑结构

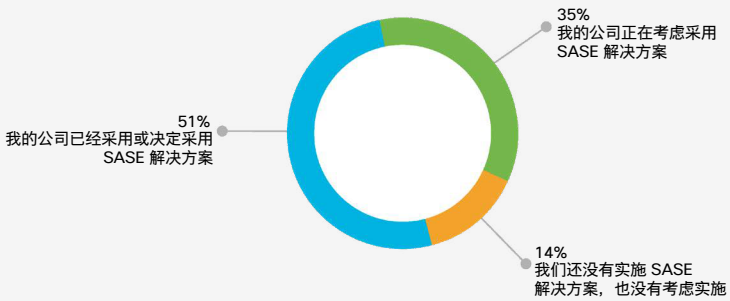




48% 对 SASE 感兴趣的公司将从安全开始，31% 将从网络开始，21% 计划同时解决安全和网络问题。[8]

无论采用何种特定的模式或部署方法，许多公司都表示他们在采用 SASE 的过程中进展顺利；86% 的组织正在考虑采用或已经采用 SASE。[11]

您的公司是否采用、决定采用或考虑采用 SASE 解决方案？



思科，2021 未来技术调查；N 34,351

“到 2025 年，至少 60% 的企业将制定明确的战略和时间表来采用 SASE，包括用户、分支机构和边缘接入，而 2020 年只有 10%。”

– Gartner[12]

基本结论：

SASE 部署方法受到现有基础设施生命周期、运营优先级和业务举措的影响。IT 团队应该采用一种战略规划方法，旨在逐步建立一个完整的 SASE 架构。

SASE 消费模式

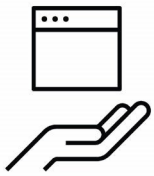
SASE 解决方案和服务有三种主要消费模式。虽然这些消费模式对内部团队和运营有不同的影响，但它们都打破了传统的网络和安全孤岛。因此，SASE 可以成为一种提高业务协调度和效率的强制功能。

即服务

对于那些希望快速部署、对运营和员工影响最小以及降低风险的组织来说，SASE 即服务，提供了一系列完全集成的、由云端交付的功能，具有单一的控制面板和全生命周期的支持。26% 的组织将 SASE 即服务作为其首选消费模式。

混合或共同管理

那些还没有准备好采用全面的即服务模式的组织，或者希望得到比这些服务更多的定制化服务的组织，可以采取混合方法。这涉及到将基于云的安全功能与现有 SD-WAN 解决方案整合，和/或与管理服务提供商分担网络和安全责任。这些混合方法提供了额外的安全和支持，并允许 IT 团队保持一定程度的可视性与可控性，同时减少整个生命周期的管理需求。



高度定制化或 DIY

希望完全定制和控制其网络和安全足迹的组织可以自行建立、整合和管理 SASE 功能。这种定制和控制水平通常是以牺牲速度和敏捷性为代价的；需要对硬件、软件和许可证进行额外的生命周期管理；并需要额外的安全和合规专家。对于那些有非常专业的需求，现有网络和工作人员可以满足 SASE 架构和运营要求的组织来说，这是一个很好的选择。

阅读这份思科安全访问服务边缘 (SASE) 部署案例研究，了解我们的经验总结。

基本结论：

有多种 SASE 消费模式，具有不同的运营影响。每个组织的正确模式取决于许多因素，包括内部 IT 团队的规模、技能和带宽，以及专门需求、速度、敏捷性、可视性与可控性的优先次序。

SASE 结论

SASE 架构、解决方案和服务在任何用户和任何应用之间提供安全的连接，无论它们如何部署或托管。但对每个组织来说，采用 SASE 全程服务将各具特色。正确的模式和方法将取决于现有的技术投资，以及 IT 和业务优先事项。

思科和我们的合作伙伴生态系统可以通过市场上最完整、最灵活和最有弹性的 SASE 解决方案帮助解决您独特的网络和安全需求。

您可以从我们广泛的 SASE 组合中选择，该组合结合了一流的网络、客户连接、安全和独特的互联网观察能力，提供您需要的结果。您还可以从一系列简单、灵活的 SASE 部署和消费模式中选择，满足各种情况和要求。

我们高度可用的全球云安全基础设施提供安全的访问，无论用户和应用在哪里。而我们市场领先的 SD-WAN 解决方案提供了为您的用户提供持续的高质量体验所需的敏捷性和功能。我们的云安全和 SD-WAN 解决方案一起提供了业界最完整和独特的集成 SASE 功能。

展望未来，思科正在通过不断的整合和持续的功能增强，加速围绕 SASE 进行创新。我们正在发展我们的产品，以便根据您的条件提供最灵活和最易于使用的 SASE 服务。

要了解更多信息，请访问 Cisco SASE 资源中心。

凭借执行能力和完整的愿景，思科被评为 Gartner Magic Quadrant™ WAN 边缘基础设施的领导者。[13]

其他资源和帮助

SASE 路线图链接 >

查找思科合作伙伴 >

联系思科销售人员 >

SASE 资源

1. 《高级研究报告：SASE 市场预测》第 2 卷第 1 期，Dell'Oro Group，2021 年 9 月。
2. 《2021 安全现状》，Splunk，2021 年 2 月。
3. 《科技的未来》，思科，2021 年 11 月。
4. 《高级研究报告：SASE 市场预测》第 2 卷第 1 期，Dell'Oro Group，2021 年 9 月。
5. Gartner 快速回答：SASE 是否取代了 SD-WAN？Andrew Lerner，Neil MacDonald，2021 年 12 月。
6. 《2022 思科全球网络趋势报告：网络即服务的兴起》，思科，2021 年 10 月。
7. 《2021 Gartner SASE 融合战略路线图》，2021 年 3 月。
8. 《SASE 趋势：计划凝聚但融合将分阶段进行》，ESG 研究报告，2021 年 12 月。
9. 《高级研究报告：SASE 市场预测》第 2 卷第 1 期，Dell'Oro Group，2021 年 9 月。
10. 《2022 思科全球网络趋势报告：网络即服务的兴起》，思科，2021 年 10 月。
11. 《科技的未来》，思科，2021 年 11 月。
12. 《2021 Gartner SASE 融合战略路线图》，2021 年 3 月。
13. “Gartner Magic Quadrant WAN 边缘基础设施”，2021 年 9 月。

网络即服务 (NaaS) 的兴起报告

目录

迎接 NaaS 时代的到来!

*《2022 全球网络趋势报告：网络即服务 (NaaS) 的兴起》*隆重发布!

无论是作为普通人还是网络专业人员，我们正在经历一个前所未有的时代。过去一年，IT 主管和网络专业人员肩负重任，他们不仅需要为远程员工提供支持、在更加分散的计算环境中保护数据，还要为用户、客户和合作伙伴提供新的服务。许多企业加快了全数字化转型进程以满足这些新需求，并利用云和软件即服务 (SaaS) 模式来提高组织的灵活性、敏捷性和速度。

在《2021 全球网络趋势报告》中，我们重点探讨了在各种环境中利用网络技术提高业务弹性的方法。

在今年的报告中，我们主要关注一个对未来有着深远影响的新趋势：网络即服务 (NaaS)。

随着 SaaS 和基础设施即服务 (IaaS) 等 “即服务” (aaS) 模式日渐盛行，NaaS 将不可避免地改变许多公司获取、交付和管理网络功能的方式。为深入了解这一趋势，我们采访了 20 位 IT 主管，并调查了 13 个国家/地区的 1534 位 IT 专业人士，了解他们如何看待 NaaS 及其优势和局限性，以及是否计划采用这一新兴的网络使用模式。

我们期待本报告中的数据、观点和指导信息能帮助您更好地理解 NaaS 的优势和影响，制定更有效的网络战略。

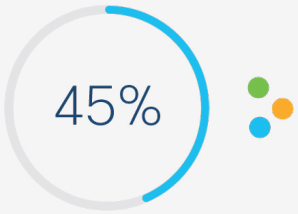
– James Mobley，思科网络服务高级副总裁

主要研究结果

要彻底改变网络的使用和运维方式，并非易事。只有具备充分的商业理由和技术理由，才能转向 “即服务” 模式。而且，为了确保您的组织正常运营，值得信赖的合作伙伴也必不可少。尽管如此，许多组织仍然非常积极地朝着这一方向转型。以下是 2022 年 NaaS 研究活动的主要研究结果。

主要研究结果 1：挑战

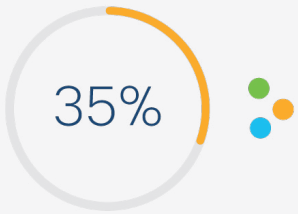
NaaS 可以帮助组织解决弹性和灵活性问题。



- 据我们调查，在 2021 年，组织面临的主要网络挑战是应对服务中断 (45%) 和满足新业务需求 (40%)。
- 与此同时，IT 团队认为 NaaS 的最大优势是将 IT 团队解放出来，使他们能够专注于实现创新和业务价值 (46%)。另有 40% 的受访者认为 NaaS 有助于提高对服务中断的响应能力，34% 的受访者认为 NaaS 帮助改善了网络灵活性。

主要研究结果 2：优势

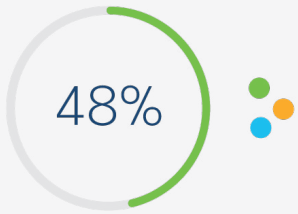
高预期：快速获取最新技术是重中之重。



- 如今，技术的发展速度总是快于企业采用技术的速度。35% 的受访者认为，对持续部署最新网络技术（例如 Wi-Fi 6、软件定义广域网 [SD-WAN]、安全访问服务边缘 [SASE]、5G、人工智能等）的需求是促使其采用 NaaS 的最大动力。

主要研究结果 3：运维

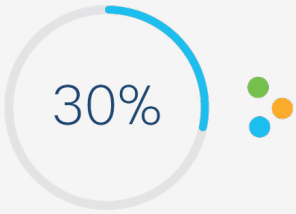
NaaS 固然优势突出，但前提是它必须能帮助网络团队满足服务级别协议 (SLA)。



- 受访者认为 NaaS 提供商需要提供的主要服务包括：网络生命周期管理 (48%)、网络弹性 (42%)，以及能满足 SLA 要求的监控和故障排除 (38%)。

主要研究结果 4：问题

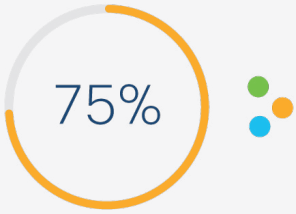
NaaS 之旅不会一帆风顺，有些受访者比较担心丧失控制力和成本方面的问题。



- 受访者担心的问题十分广泛，包括 NaaS 能否满足无法预期的新需求 (30%)、丧失安全控制力 (26%) 等。
- 转型所产生的成本和业务中断问题也深受关注 (28%)。

主要研究结果 5：角色

NaaS 开阔了 IT 专业人员的视野，但也对其技能水平提出了更高的要求。



- 超过 75% 的组织认为或强烈认为 NaaS 有助于提升 IT 团队的技能。
- 但如今，只有四分之一的组织可能相信，自己的 IT 人员能够将业务需求转化为技术策略，而不需要依靠系统集成商、托管服务提供商或 NaaS 提供商。

主要研究结果 6：采用

我们可以通过多种方式开启 NaaS 之旅，其中之一是 SASE。

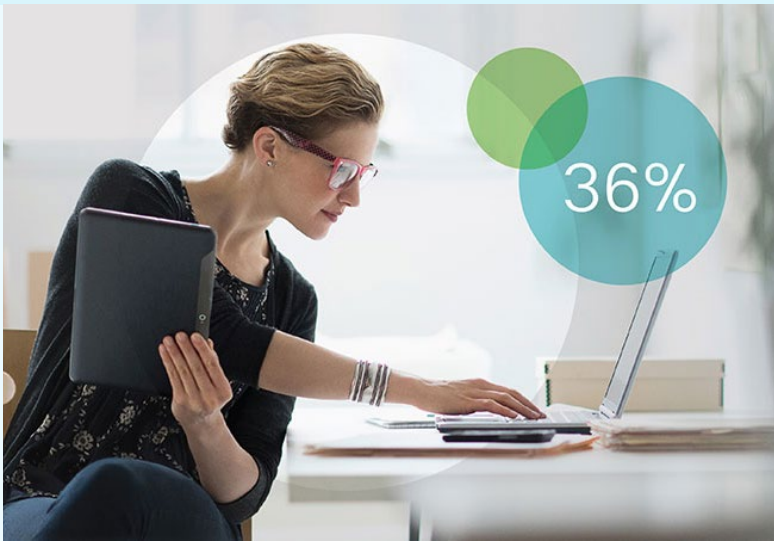
- 受访组织认为多云访问 (40%) 和安全性 (34%) 是 NaaS 的优势所在，因此，SASE 可能是 NaaS 的一个切入点。
- 49% 的组织计划在技术更新或升级周期中开始采用 NaaS，34% 的组织表示他们将先从调整现有站点着手。

前所未有的网络模式

在经历长达 18 个月的混乱和适应后，网络技术的作用从未像现在这样清晰，也从未像现在这样重要，因为它关乎企业的兴衰成败。网络早已成为远程办公的关键推动力，但现在它还要进一步支撑更安全的工作场所、混合办公模式和不断变化的业务运营活动。要满足这些要求，企业本地、多云和边缘环境中的网络必须能够无缝协作。无论用户的位置、设备或连接方式如何，网络都必须为用户提供安全且一致的体验。不仅如此，还需要支持由传统的和现代的微服务推动的应用。

由于资源和带宽往往有限，许多 IT 和网络主管正在研究将 NaaS 作为替代方案，解决这些挑战。但 NaaS 究竟是什么？

在向 IT 主管询问 NaaS 的定义时，我们很快就发现，NaaS 对于不同的受访者有着不同的含义。事实上，在我们的调查中，有 36% 的受访者声称他们已经拥有 NaaS，这令人惊讶。对于一项新兴技术来说，这样的比例似乎非常高。不过在采访中我们意识到，许多受访者认为，如果其公司网络的任何部分由第三方服务提供商管理，那么他们会认为自己的公司已经拥有 NaaS。我们认为这一定义过于宽泛，需要进行具体化。



NaaS 是一种可支持云、基于使用情况的使用模式，它允许用户无需拥有、构建或维护自己的基础设施就可以获得和协调使用网络功能。

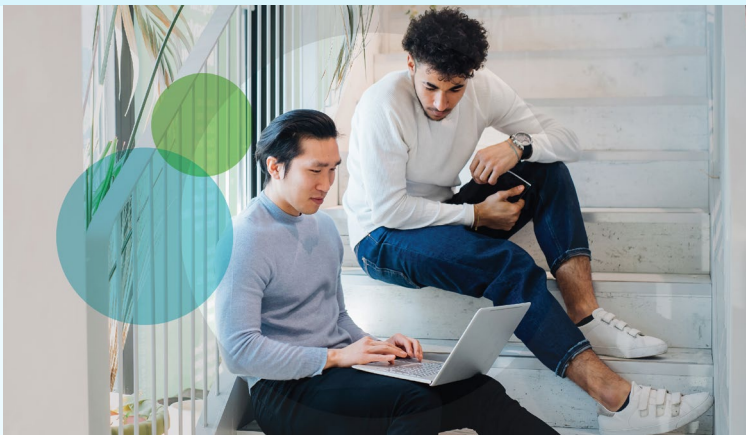
“各种组织正努力探索如何合理地搭配内部资源以及合作伙伴所提供的资源。许多组织选择在人员、分析程序、可观察性和自动化能力方面进行投资，同时努力思考如何利用战略性提供商资源来减轻基础设施管理和维护过程中的负担。”

– Mary Turner，IDC 研究副总裁

NaaS 可为广泛的网络元素（包括有线和无线局域网、广域网、VPN 以及分支机构、数据中心、边缘、多云和混合云环境）提供不同的使用模式。它可用于实现新的网络模式，例如 SASE。它可以帮助实现组织模式的转换，例如转向混合办公模式。作为一种按需服务，NaaS 可以让 IT 团队更轻松地扩大或缩小规模、快速部署新服务，以及优化资本支出和运营支出之间的平衡。

我们采访过的一些 IT 主管认为，NaaS 代表了他们急需的一种更优更新的网络形式。

他们意识到自己已经落后，失去了用户的信任。他们相信 NaaS 可以帮助其获得最新技术、满足不断增长的需求，并适应不断加快的业务节奏。



“由于网络的复杂性如此之高、企业对市场变化做出反应的速度要求如此之快、现代网络的覆盖面如此之广，很多人意识到：不能再这样下去了，我们需要得到帮助。”

– Mark Leary，IDC 网络分析研究总监

基本结论:

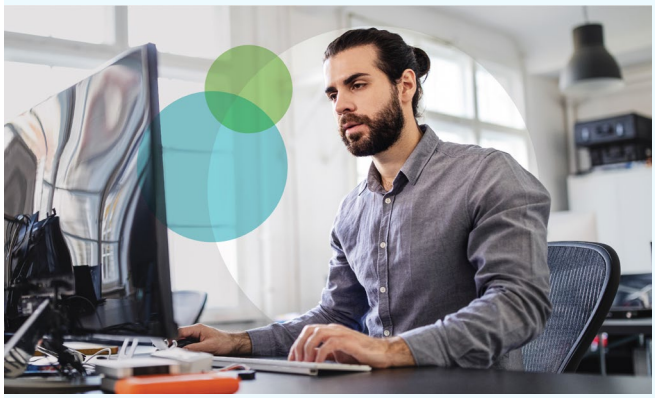
从 2021 年到 2027 年，预计 NaaS 采用率的年复合增长率将达 40.7%。[1]

应对挑战，创造效益

是否采用 NaaS 模式最终取决于它解决业务和技术挑战的能力，及其带来的好处。

对于我们所调查的组织来说，灵活性仍然是最重要的。当被问及其网络必须应对的最大业务挑战时，近 50% 的 IT 专业人士的回答是应对服务中断，40% 的回答是适应新业务应用和业务项目。超过三分之一的受访者认为，对网络灵活性的需求是促使其采用 NaaS 的主要原因；一半的受访者表示，他们预计 NaaS 将使其能够实现更多创新和商业价值。

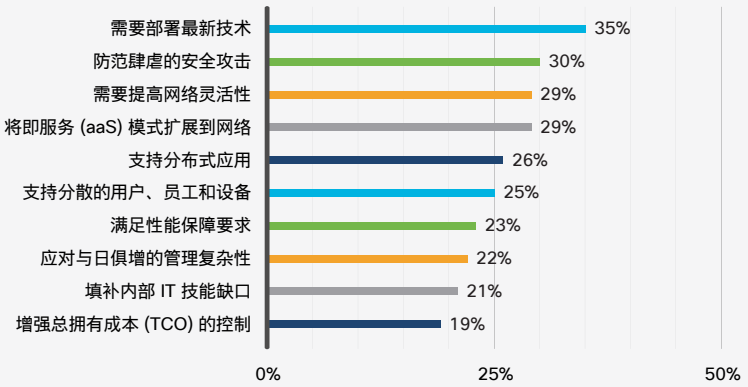
为了提高灵活性，许多 IT 组织正在将其应用和服务迁移到云，
而这可能会带来安全、治理及合规性方面的新挑战。



根据我们的调查，受访的 IT 专业人士表示，他们目前在管理网络方面面临的最大技术挑战是连接多个云 (36%)、保护网络、用户和应用 (34%)、确认问题根源和快速修复安全或性能问题 (31%)。

同时，有三分之一的受访者确认，不断部署最新网络技术（如 Wi-Fi 6、SD-WAN、SASE、5G、AI 等）的需要是导致采用 NaaS 的一个关键动机。

什么原因最可能促使您的组织改用 NaaS 模式？



> “我们的高管认为，把人力资源花在配置设备或运维基础设施上没有任何价值。他们希望 IT 能够想业务之所想，合理分配资源。通过使用外部服务来完成基本运维，让员工从事更能推进业务成果的工作。”
>
> – 某全球消费品公司 IT 基础设施总监

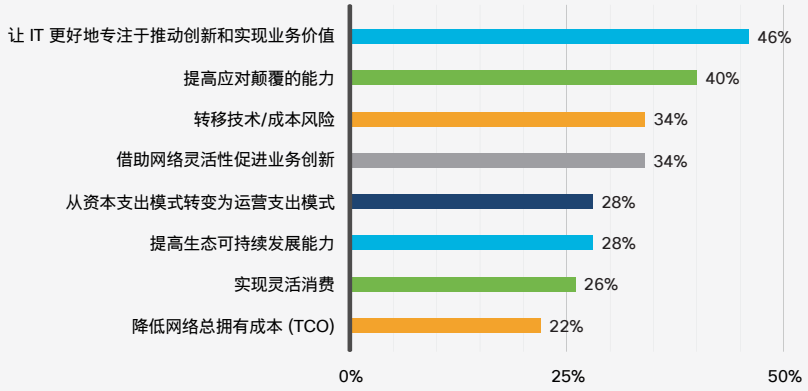
当我们问及 IT 专家期望 NaaS 带来的主要优势时，主要决策者提到了专注于创造业务价值而非日常基础设施管理的能力。

改善对网络和安全事件的响应是 NaaS 备受好评的另一个优势，45% 的网络从业者和 40% 的关键决策者提到了这一点。安全性提升被排在优先位置并不令人意外，我们更感兴趣的是，超过 25% 的网络从业者和 33% 的关键决策者认为，改善生态可持续性是 NaaS 的一大贡献。

更令人惊讶的是，受访者对 NaaS 所产生经济效益的评级很低。

通过采用灵活的使用模式和基于订用的定价，NaaS 使 IT 团队的支出从资本支出转向运营支出，从而避免对网络基础设施进行大规模和经常性投资。支出变得更加稳定且可预测，公司只需为他们使用的资源付费。然而，与 NaaS 倍受赞赏的灵活性、创新性和可托管方面的优势相比，IT 主管和网络专业人士对其经济效益的评价低得多。

在您看来，通过使用 NaaS 模式可获得的三大业务优势是什么？



基本结论:

对于 NaaS 而言，TCO 的优先级较低，这是因为公司更关心实现业务价值和快速响应服务中断。68% 的 IT 主管认为或强烈认为 NaaS 能将其团队从日常网络管理中解放出来，投入更多时间专注创新和提供业务价值。

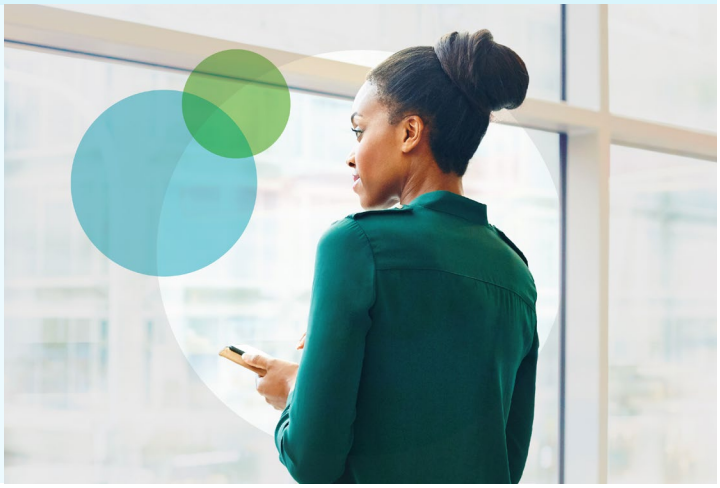
NaaS 如何改变网络运维 (NetOps)

我们了解到，对 NaaS 的一个普遍担忧是，它需要组织完全托管网络运维，也就是将所有责任移交给 NaaS 提供商，而不给组织内部的 NetOps 团队留下任何工作。但事实上，当涉及运维责任时，NaaS 并不是非此即彼的零和游戏。

在 NaaS 模式中，提供商对网络生命周期管理的所有方面负责。这包括部署、整合、控制、更新、监测和维修网络基础设施的所有元素（以及客户的任何本地设备），以根据合同交付成果。成果可能包括用户、站点、云提供商和应用的连接数量，以及双方商定的服务水平、带宽、应用性能、安全规定、合规性和其他要求。

那么还剩下什么让内部团队去管理？
NaaS 客户的 NetOps 团队能够将更多时间用于专注核心或增值活动。

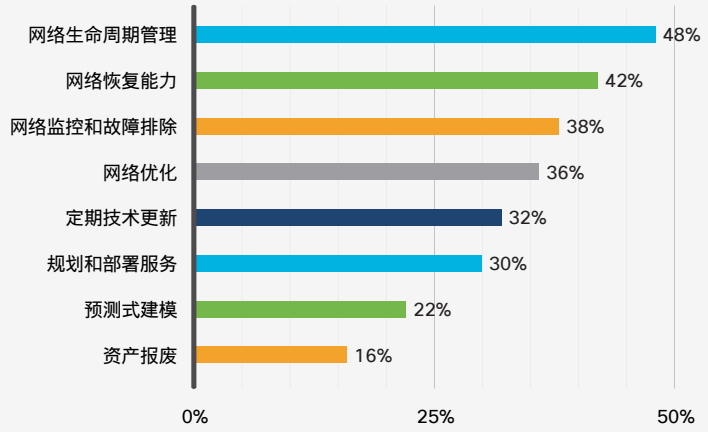
这可能包括定义和监测所需的网络成果，例如用户、应用访问策略和应用性能水平等。通过监测网络性能和获得洞察，客户的 NetOps 团队可以持续调整和优化跨领域的网络策略和行为。



客户的 NetOps 团队也可以通过 API 管理 NaaS 与其现有系统之间的整合，以简化 IT 工作流程和过程。他们可能希望与 NaaS 提供商密切合作，以确保满足 SLA 和服务级别目标 (SLO) 的要求。很明显，不管运维责任和交接如何，IT 专业人士都渴望减少基础设施管理的负担。

在我们调查的 IT 专业人士中，有 48% 的受访者表示，网络生命周期管理是 NaaS 模式包括的最重要服务。受访者将网络弹性 (42%) 和网络监控与故障排除 (38%) 视为最重要的三个服务中的另外两个服务。这强化了一种观念，即，管理日益分散及复杂的地点、用户、设备、应用和云资源组合给 IT 团队造成了沉重负担，使他们只能将很少的时间用于进行增值活动和创新。

您认为在 NaaS 模式中，以下哪些服务最重要？



“提供商将处理日常琐事。然后，内部团队可以全力以赴地通过网络增添更多价值，并满足即将出现的新需求。我们的工程师和技术人员不需要停下手头工作来解决问题。他们可以专注于新项目。”

– 某全球咨询公司高级网络工程师

基本结论:

在 NaaS 模式中，运维责任由提供商和内部 IT 团队共同分担。网络生命周期管理工作由提供商承担，使客户的 IT 团队能够更专注于可帮助提高商业价值的运维活动。

角色、责任和技能组合

在将基础设施维护和生命周期管理责任转移给提供商后，NaaS 将帮助网络运营团队节省大量时间。这使网络运营团队能够专注于实现所需的网络成果，而不是将宝贵资源花在维持基础设施的技术和运维方面。

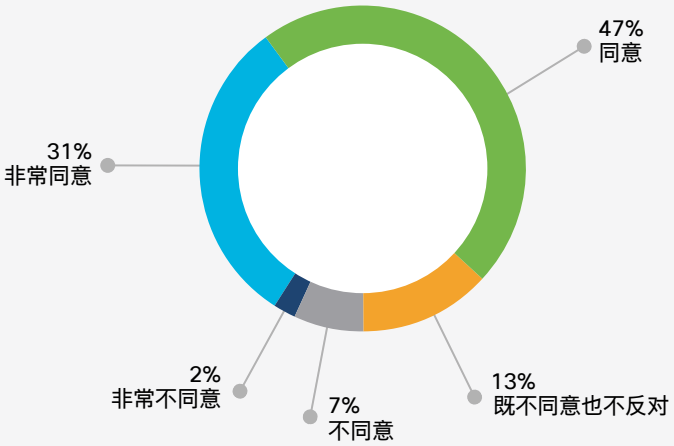
换句话说，网络工程师可以从具体的基础性工作中脱身，转而发出指令让别人去做基础性工作。但是，他们预计会如何大显身手？

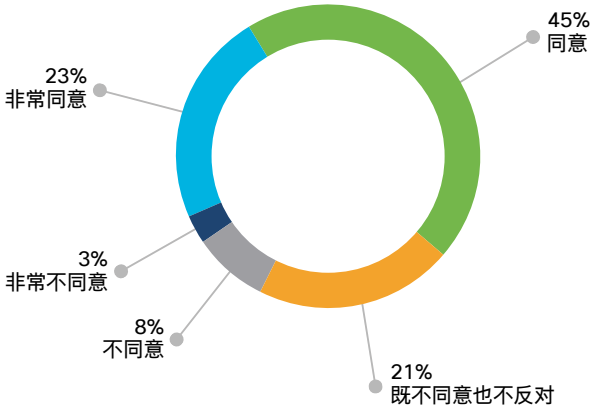
根据我们的访谈，27% 的受访者认为他们的 IT 人员会利用技术专长和 NaaS 控制面板，将业务需求转化为网络策略。令人惊讶的是，73% 的受访者表示，他们更愿意让第三方提供商承担此业务关键型角色，这可能说明他们认为内部技能组合短缺，或他们对内部团队缺乏信心。

“随着大部分日常工作转移到 NaaS 提供商，客户的网络运维团队可能会转向一般的网络运维和网络安全技能，以及将商业意图转化为高级网络概念的设计技能。他们必须与 NaaS 提供商密切合作，优化网络设计、策略、性能和 SLA。并且，需要具备强大的数据科学技能，以发现和协调这些变化。”

– Joe Clarke，思科杰出工程师

通过采用 NaaS 模式，我们的网络团队成员将获得提升技能的机会，并为组织创造更大价值。





NaaS 将为我的网络团队腾出时间，让他们专注于 IT 创新和商业增值任务，而不是日常的网络管理。

基本结论：

超过 75% 的组织认为或强烈认为 NaaS 模式将使他们的团队有机会提升技能组合，并创造更多价值。

关切和犹豫

NaaS 影响了 IT 组织的许多领域，它要求使用新的运维模式、与现有流程和技术进行新的整合、改变角色和技能组合，以及实现从资本支出到运营支出的财务转变。考虑到这些广泛的影响，我们采访的 IT 专业人士对 NaaS 有不同的反应。在 NaaS 的采用上，大多数人处于对立的两端，态度不是热就是冷。

IT 主管对 NaaS 的看法似乎反映了他们的总体网络理念。这些理念主要分为两个阵营：“控制 IT” 和 “精益 IT”。秉持 “控制 IT” 理念的人不仅拥有技能娴熟的员工，而且还坚信他们的团队应该拥有并完全控制网络系统。相反，秉持 “精益 IT” 理念的人正在寻求整合他们的 IT、重新评估常规任务与增值任务，并找到用于减轻基础设施维护负担的方法。毫不奇怪，具有 “精益 IT” 心态的组织已经将他们的一些 IT 资源迁移到云端，并对 NaaS 解决方案持非常开放的态度。

> “我们在 NaaS 上迟疑不决，因为我们觉得网络不会得到应有的照顾和处理优先权，而且 NaaS 无法完美地匹配我们的环境。”
>
> – 美国军事机构网络部 IT 主管

我们采访的一些 IT 主管表示，他们的网络和流程十分特殊，
因此他们不相信 NaaS 能够解决他们所特有的复杂性问题和挑战。

另一些人则表达了真正的关切，即 NaaS 会引起 IT 组织内部的剧变。

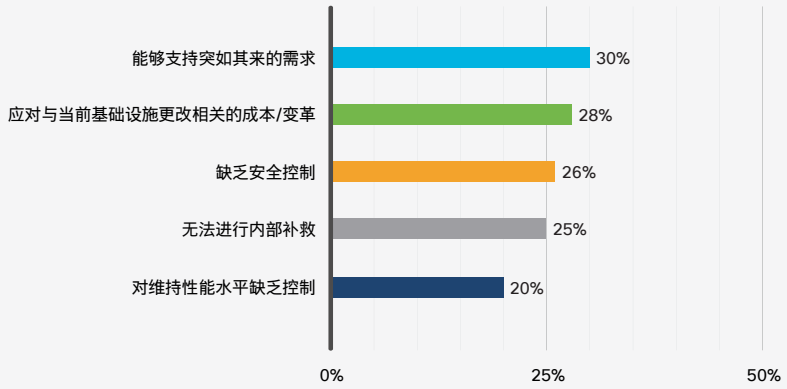
在 IT 主管的大量关切中，控制权丧失是主要的关切。30% 的受访者质疑，如果采用 NaaS，他们是否能够满足未来的需求？其他受访者担心失去对安全 (26%) 和性能 (20%) 的控制。实际上，NaaS 可以提供更强的按需扩展性和更快的最新技术支持速度。而安全、性能和其他重要控制决策仍然掌控在 IT 团队手中，而不是 NaaS 提供商。

“提供商必须遵从我们的安全准则，并接受我们的指令。这是 NaaS 与众不同的一个关键因素。”

– 某全球科技公司首席架构师

28% 的受访者表示，改变现有基础设施和运维所引发的成本及业务中断令他们望而却步。这可以理解，因为组织拥有众多的技术和投资，其中许多有着不同的折旧期限。另外一些组织采用传统技术和应用，这些技术和应用可能不适合 NaaS。还有一些企业根本不愿意将基础设施的日常管理工作假手他人。

您对部署 NaaS 模式的主要关切是什么？



为了应对这些关切和犹豫，组织可以从一个小领域开始测试 NaaS 模式。这有助于他们更好地了解 NaaS 的能力和控制点，而不需要大幅改变现有的网络基础设施或运维。他们将能够体验和优化提供商和其内部团队之间的责任分工，并学习如何加强合作，以获得最佳结果。一旦他们完全了解和适应了角色、职责和控制点，就可以随着时间的推移扩展到其他领域，并充分利用在此过程中收获的洞察和最佳实践。

基本结论:

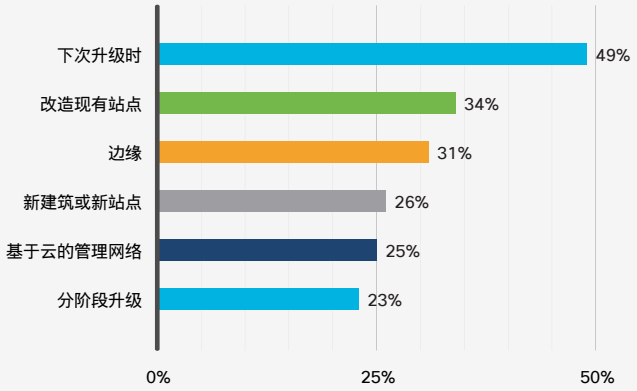
转型总是伴随着风险和担忧。IT 主管可以从小处着手评估与 NaaS 相关的风险和回报，看看它是否适合其组织。

采用趋势

由于 NaaS 对网络运维的影响及其利用方式的多种多样，每个组织采用 NaaS 的方式都是不同的。NaaS 就绪性评估和部署计划可以帮助组织最大限度地减少潜在问题，并最大程度地取得成功。

根据我们的访谈，49% 的 IT 主管和 57% 的网络从业者认为，网络基础设施升级或更新期间是采用 NaaS 的最佳时机和环境，因为他们会在此期间努力部署新技术（自动化、百兆以太网、Wi-Fi 6、5G、SD-WAN、SASE 等）。34% 的受访者表示，对已部署网络技术的现有站点（棕地）进行改造是采用 NaaS 的理想场景。有趣的是，只有 26% 的受访者认为绿地场景最适合采用 NaaS。同时只有 23% 的受访者认为，对他们的组织来说，分阶段使用 NaaS 逐个升级域的方法是最好的方案。

您认为 NaaS 在以下哪种场景中最适合您的组织？



基本结论:

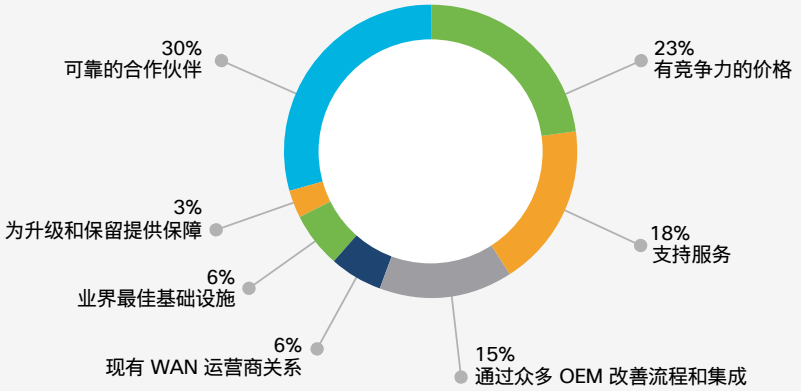
关于如何部署、何时部署以及为何部署 NaaS 的问题，每个组织都有不同的答案。

选择 NaaS 提供商

由于网络是提高员工生产力、客户参与度和业务运营绩效的关键因素，选择合适的 NaaS 提供商至关重要。我们采访的一些 IT 主管确实担心失去对网络的控制。然而，他们愿意让渡一定程度的控制权，前提是控制权会移交给一个足可信赖的合作伙伴。无论合作伙伴是系统集成商、托管服务提供商或增值经销商，IT 主管对那些已经深入了解他们的网络环境、业务目标和支持需求的成熟合作伙伴最具信心。

在我们的调查中，对于 NaaS 部署，近三分之一的 IT 专业人士认为系统集成商比网络提供商更值得信赖，而且价格更具竞争力。他们还告诉我们：“可信赖的专业水准”比“一流的基础设施”重要得多。

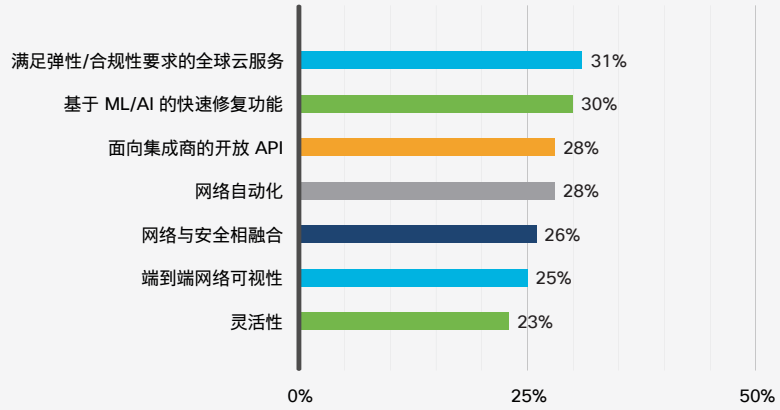
在部署 NaaS 时，您更愿意与合作伙伴合作而非直接与网络提供商合作的主要原因是什么？



当涉及到将业务需求转化为技术策略时，IT 专业人士对系统集成商或其内部 IT 人员的信任度，比对 NaaS 提供商的信任度高 2 至 3 倍。这凸显了一个事实：当涉及到 NaaS 时，企业不仅仅是在寻找一个解决方案，而且还在寻求熟悉他们情况的可靠顾问的指导和帮助。

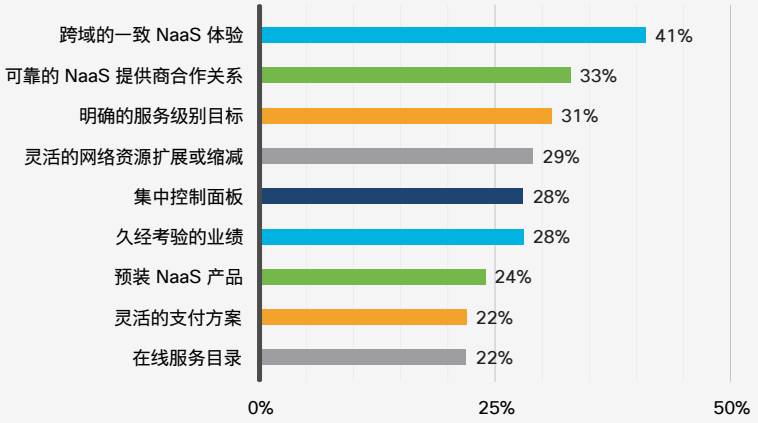
当考虑到 NaaS 提供商和解决方案的技术特性时，受访者优先考虑全球云覆盖带来的可靠性、绩效和区域合规性 (31%)，以及能够持续优化 NaaS 服务的机器学习 (ML) 和人工智能功能 (30%)。API、自动化、集成安全、网络可视性和网络灵活性也得到了高度重视。

您认为 NaaS 产品的两个最重要技术属性是什么？



41% 的受访者表示，NaaS 提供商提供跨网络域（接入、广域网、数据中心和云等）的一致 NaaS 平台很重要。由于许多 IT 团队正在努力管理多种环境、工具集和运维模式，NaaS 提供了一个整合网络资源、策略和运维的机会。

当您考虑选择 NaaS 提供商的产品时，以下哪项是最重要的因素？



“我真正需要的是能够处理我们的整个网络和系统中的日常管理活动（如固件更新、配置和更改）的人。这样，我的团队就可以专注于改进、构建和战略实施等任务。而且我们需要一定的灵活性。也许这个月我们自己完成了一些相当繁重的工作，然后在接下来几个月内得到帮助，以扩展服务的使用并协助我们的工作。”

– 美国某资产上亿的非营利组织的技术和安全副总裁

基本结论：

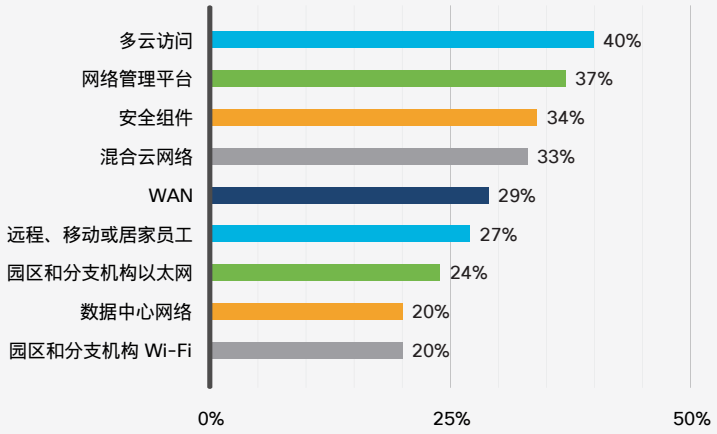
人们认为系统集成商比 NaaS 提供商更值得信赖、价格更有竞争力、服务更优质。无论选择哪个提供商，客户都希望获得跨越所有网络域的服务和运维的一致体验。

SASE 与 NaaS 的不同风格

NaaS 产品层出不穷，包括有线和无线局域网、VPN、广域网、网络安全、远程或在家办公访问、数据中心网络和云网络。根据我们的研究，可支持多云访问和安全功能的 NaaS 模式最受青睐。这意味着，可以从任何地方提供安全多云访问的 SASE 将成为许多 IT 组织渴求的 “即服务” 产品。

考虑到连接多个不同云时面临的挑战，多云访问被受访者视为 NaaS 的首要优先级 (40%) 就不足为奇了。通过提供 SD-WAN 服务，NaaS 提供商可以利用一致和优化的方式来连接各种云应用（IaaS 和 SaaS）。

您的网络设备和管理程序的哪些特性很适合 NaaS？

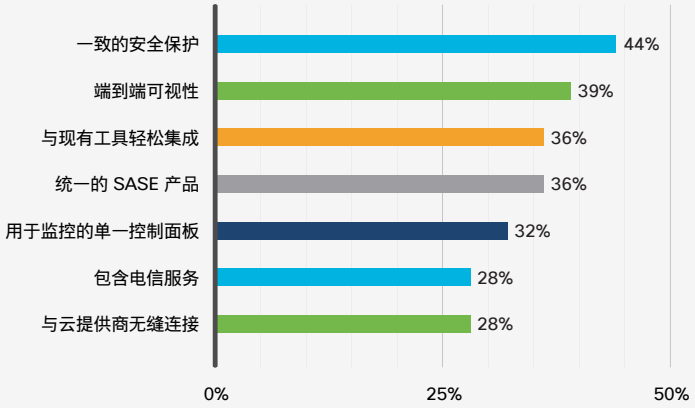


34% 的受访者优先考虑以安全为重点的 NaaS 解决方案，包括 VPN、安全信息和事件管理 (SIEM)、安全 Web 网关、防火墙以及入侵防御和检测服务 (IPS/IDS）。这些功能可以帮助客户在多个云和计算环境中持续保护用户、设备和应用。

能在边缘同时提供多云访问和安全功能的 NaaS 提供商可以很好地满足客户对 SASE 解决方案不断增长的需求。

近一半 (44%) 的受访者将 “为所有用户和设备提供一致的安全，包括威胁检测和修复” 视为 SASE 的一项重要功能，而不管他们从哪里访问。随着人们越来越依赖互联网以访问基于云的应用，超过三分之一 (39%) 的受访者希望获得 “对互联网和云基础设施的网络流量的可视性和洞察”。36% 的人正在寻找能够与其当前使用的工具轻松整合的 SASE 解决方案。

如果您的组织选择将 SASE 作为一项服务部署，以下哪些是最重要的功能？



基本结论:

多云访问和安全是 NaaS 的首要优先事项。提供商在 NaaS 产品组合中纳入 SASE 选项以满足日益增长的需求，确保企业本地资源和云资源的稳定性及安全性。

结论

无数的 IT 组织正在竭力管理网络复杂性，应对中断和干扰，保护用户和数据，并努力跟上不断加快的业务步伐。为了应对这些挑战，许多人正在研究新的网络模式，例如 NaaS。

NaaS 通过按需或基于订用的模式提供对最新网络技术的持续访问。它将日常网络管理的负担转移给第三方提供商。这样做的结果是，IT 团队能专注于增值活动，为组织实现更高的灵活性、弹性和创新性。

与任何转型模式一样，围绕 NaaS 也存在着一些顾虑和犹豫。但这并不是一个非此即彼的零和选择。IT 团队可以联手值得信赖的合作伙伴，小规模地试用 NaaS，评估风险和回报，以决定 NaaS 是否契合他们的总体业务和技术战略。

其他资源和帮助

网络即服务 (NaaS) 简介 >

思科解决方案 >

查找思科合作伙伴 >

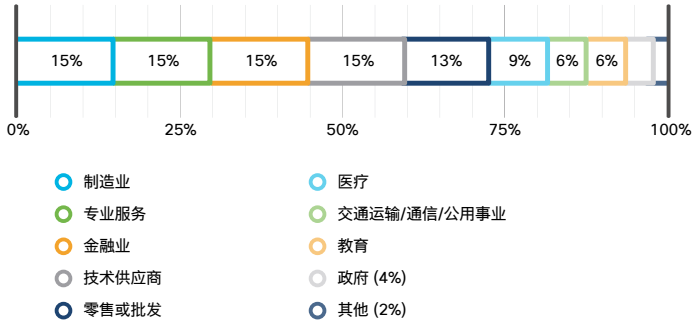
联系思科销售人员 >

关于本报告

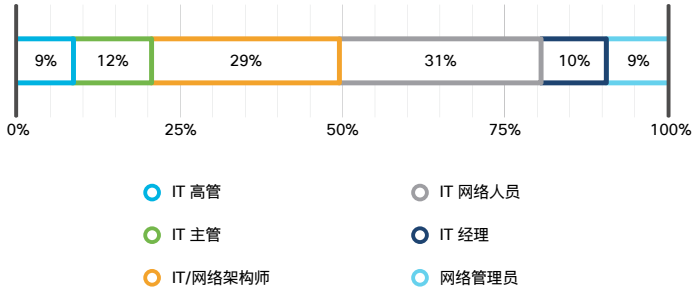
《全球网络趋势报告》于 2019 年首次发布，重点关注企业网络和云计算行业内的最新战略和技术。该报告利用行业研究，提供观点、见解和指导，帮助 IT 组织了解当前的技术趋势，发展他们的网络模式，并支持满足动态业务需求。

为了编制 2022 年的报告，我们对 20 位 IT 主管进行了访谈，并收到了来自 13 个国家/地区的 1534 位 IT 专业人士对 NaaS 的看法，以及他们如何看待 NaaS 在未来两年内与他们的网络战略保持一致或增强其网络战略的意见。对于每个问题，受访者最多可以选择 3 项答案。

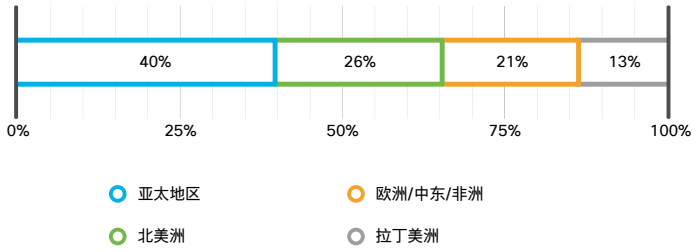
受访者所在行业



受访者角色



受访者所在位置



本报告的使用许可

思科欢迎并鼓励新闻机构、分析师、运营商和其他对本报告感兴趣的机构使用本报告中提供的信息。我们要求以印刷或电子形式发布或分享的任何及所有思科《2022 全球网络趋势报告》数据（无论是私人的还是公开的）都要适当地注明出处（即 “来源：思科《2022 全球网络趋势报告》”）。参考我们公开发布的白皮书、报告或 Web 工具无需另行经过我们签字和同意。

我们会随时关注报告内容的使用环境，如果使用这些内容的相关方愿意分享其引用思科《2022 全球网络趋势报告》的完整作品，我们将非常感谢。您可以将引用了思科《2022 全球网络趋势报告》内容的文档转发至 networkingtrends-inquiries@cisco.com。

《2022 全球网络趋势报告》来源

1. 《全球网络即服务 (NaaS) 市场行业动态、市场规模和机会预测（至 2027 年）》，Report Ocean，2021 年 3 月。