报告思科公开信息

The bridge to possible

2023 年全球网络趋势报告

为分布式员工提供简便安全的多云连接

2023 年全球网络趋势报告

为分布式员工提供简便安全的多云连接

目录

引言

思科年度《全球网络趋势报告》重点关注企业网络和云领域的最新战略和技术。该报告将基础研究和行业研究的结果与企业高管的观点和见解相结合，确定最新技术趋势并提供指导，帮助 IT 组织改进网络模式，支持不断变化的业务需求。

在 2023 年报告中，我们探讨了组织如何部署和改进网络，帮助满足分布式应用、人员、场所和事物的安全连接需求。我们对北美、拉丁美洲、亚太地区和西欧 13 个国家/地区的 2,500 多名 IT 主管进行了调查。

主要研究结果：多云连接的网络现状

混合办公模式仍在不断带来安全连接方面的挑战。

混合办公时代的到来催生了新的需求：企业希望通过新的方法让远程员工能安全访问多云环境中的企业数据和资产。

- 虽然企业鼓励员工恢复现场办公，但超过 40% 的员工选择继续远程办公（全时远程或每周几天远程）。
- 如今，应用部署于多个云中，员工高度分布式办公，这种转变导致传统的安全模式难以奏效，给 IT 专业人员带来了难题。超过半数 (51%) 的受访者认为云安全存在风险，39% 的受访者认为远程员工的增加是主要挑战。

向云和多云转变的步伐正在加快。

在面临业务敏捷性问题时，许多企业继续将云技术视为解决之道。

- 很多组织继续采用云平台，78% 的调查受访者表示，他们的组织计划在 2025 年前将 40% 以上的工作负载托管于云端，而目前做到这一点的组织只有 63%。
- 多云的采用也日益普遍，42% 的云和网络专业人员表示，能够提高应用开发的敏捷性和可扩展性是采用多云的重要动力。

在 2023 年的网络挑战清单上，保护用户安全访问云应用位居榜首。

保持对整个数字化服务交付链的端到端可视性（例如用户和云之间）以确保一致的应用体验也是企业 IT 专业人员关心的主要问题。

- 41% 的网络专业人员认为，确保安全访问分布于多个云中的应用是最大的挑战。
- 37% 的受访者认为，随着企业网络边界之外发起或终止的流量越来越多，获得对网络性能和安全性的端到端可视性已成为第二大挑战。

基本指导：确保安全访问云应用的成功网络策略

寻求网络与安全融合

增进 IT 团队之间的协作，简化从接入网络到云的整体运维流程。

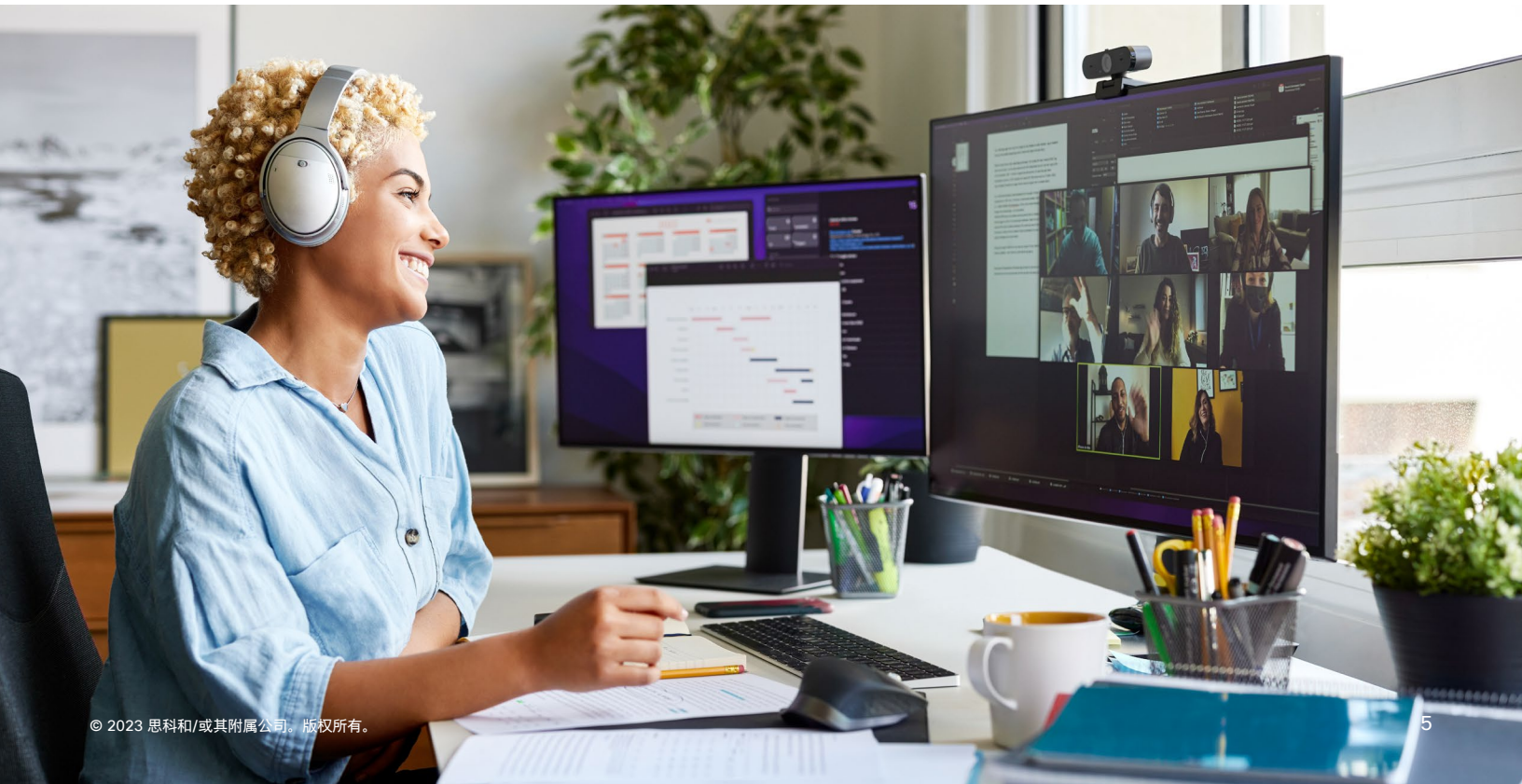
组织各自为政的运维方式和传统的连接模式已无法满足分布式应用、人员、场所和事物不断变化的安全需求。

- 与技术孤岛运维环境相比，跨安全、网络和云运维提供标准化策略、共享遥测数据和简化工作流程能够以更快的速度实现更出色的 IT 和业务成果。
- 40% 的受访者表示，确保从分布式位置安全访问多云应用时，孤立的运维是一项主要挑战。
- 云领域专业人员认为网络运维需要更好地与云运维保持一致，38% 的受访者希望与网络团队更密切地配合，34% 的受访者将运维一致性视为关键目标。

利用 SASE 架构，转向融合的网络与安全模式。

安全访问服务边缘 (SASE) 可以实现运维简化并提供一致的安全性和性能，满足多云访问和混合办公所需。

- 组织将软件定义广域网 (SD-WAN) 和云安全功能融合，提供 SASE 架构。
- 47% 的受访者希望在两年内将 SD-WAN 环境扩展至完整的 SASE 架构，连接分支机构和远程客户端。



采用云优先的网络和安全

跨多个云一致地扩展 SD-WAN 连接，简化 IT 管理并提升应用体验。

在所有云环境中一致地应用策略，以自动执行与云无关的连接、优化应用体验并保障其安全。

- 跨云、SaaS 和中间一英里提供商扩展可视性、可控性和零信任访问，帮助 IT 组织提供更出色、更安全的用户体验。
- 一半以上的受访者 (53%) 表示，他们未来两年的首要任务是与云服务提供商集成，以提升从所有位置访问云应用的能力。

转向以云为中心的安全，实现一致的运维和策略。

将安全功能整合到云平台中，使企业能够更轻松、更广泛且更有效地实现可视性、策略管理和可控性。

- 59% 的受访者表示，他们未来两年在云接入网络方面的首要任务是将安全功能集中到云端，并承认对所有位置的用户和设备实施一致的策略是一项主要要求。

向主动式运维模式转变

在日益复杂的数字化服务交付链中，寻求通过端到端网络可视性实现一致的用户体验。

如果不能将可视性扩展到自有网络以外的互联网和云环境，IT 团队就无法确保基于云的应用和服务提供一致的出色用户体验。

- 51% 的受访者将使用端到端网络遥测和可视性来主动检测问题并实施补救视为首要任务。
- 当大多数用户和设备事务在企业边界之外进行时，对互联网和云流量的可视性变得尤为重要。

转变运维模式，化被动反应为主动前瞻，提高正常运行时间和性能水平。

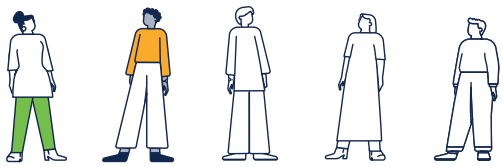
作为 IT 智能运维 (AIOps) 工具包的重要组成部分，预测性分析可以实现更简便、更快速且更有效的整体 IT 运维，因此正逐渐获得认可。

- 47% 的受访者决心主动防止网络性能下降而不是被动补救网络中断事件，他们将采用预测性网络分析作为未来两年内的首要任务。

简介：多云访问发展趋势

“有朝一日，计算能力可能会变成一种公共资源，就像电话系统是一种公用设施一样，每个用户只需要为实际使用的容量付费。”[1] 这些富于先见之明的话是 John McCarthy 教授 1961 年在麻省理工学院进行演讲时对观众们预言的。

六十多年后，McCarthy 教授对于计算能力作为共享公共资源按需使用的设想不仅已经实现，而且还成为如今推动全球数字化变革的主要因素之一。



五分之二的人至少每周有部分时间远程办公。

继续向多云环境迁移

如今，大多数组织已采用多个云。思科 2023 年全球网络趋势研究发现，三分之二的组织已将 40% 以上的工作负载部署于多个云环境中。此外，大多数组织使用的云提供商不止两家，绝大多数组织使用的 SaaS 提供商多达五个以上（请参阅图 1）。

混合办公已成常态

如今，不仅应用变成了高度分布式应用，混合办公的日益普及还意味着分布式人员和事物也更甚以往。

根据近期进行的一项研究，尽管 59% 的人已恢复全时现场办公，但仍有很大一部分人继续远程办公，其中 28% 的人采用混合办公安排，其余 (13%) 的人则完全远程办公。[2] 当然，行业和职位不同，这些数据也会有很大差异。

另一方面，原本每天需要管理和保护的连接数量也在不断增长，数据流高达数万亿，而物联网技术和边缘计算的快速普及还在持续推高流量。

员工分布式办公以及物联网和边缘计算的激增推动了组织的需求，组织希望提供可扩展的安全连接并确保用户能够访问任何网络中的多云应用和全球托管服务（图 2）。网络专业人员认为这是 2023 年他们面临的主要挑战。

1 https://www.technologyreview.com/2011/10/03/190237/the-cloud-imperative

2 https://wfhresearch.com/wp-content/uploads/2023/02/WFHResearch_updates_February2023.pdf

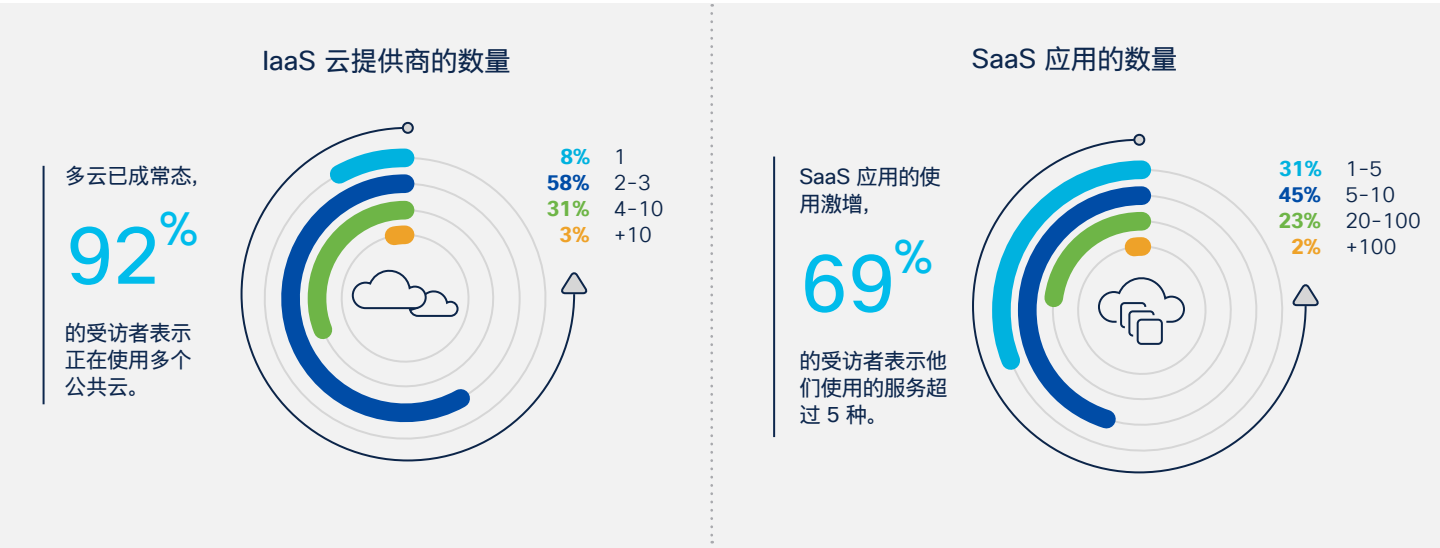


图 1. 使用多个云和 SaaS 提供商已成为常态。

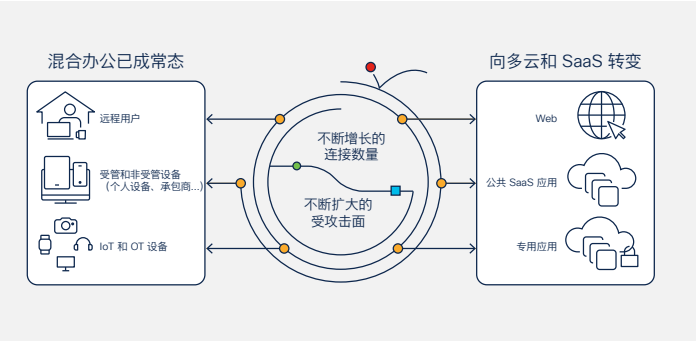


图 2. 混合办公的盛行以及向云和 SaaS 的转变意味着组织面临网络安全挑战时力有不逮。

互联网连接使这一挑战变得更加复杂，因为互联网基础设施超出了网络和安全专业人员的可视性与可控性范围。尽管如此，他们仍要为员工、客户和合作伙伴的数字化体验和安全保护负责。

速度和敏捷性的重要性与日俱增

敏捷性已成为当今大多数组织必须达到的基本要求。调查结果显示，迁移到多云的最大动力并非 McCarthy 最初预测的成本，而是对业务敏捷性和创新的需求，以及快速部署新的优质应用和服务的需要。在经历了造成破坏性后果的疫情、地缘政治和经济动荡以及供应链挑战之后，快速应变并把握市场趋势的能力已成为重中之重。

组织认识到，在当今的环境中，孤立的技术和运维模式局限性太大，已无法再为他们提供良好的服务，他们亟需新的工具和流程。连接和安全方面的挑战要求他们采用一种着眼于全局的方法，提供更简单、更安全、更灵活的网络基础设施和运维模式。

本报告的下一部分将探讨这些挑战，并就如何实现灵活而安全的连接提供最佳实践指导。此外，下一部分还将概述网络和安全团队为什么必须合作以及如何合作，为所有位置的员工、合作伙伴和客户提供可靠、安全、稳定的云交付体验。

“人们不想等待数周或数月才能满足重点业务的需要。因此，现在业务部门提出任何计划，都希望比以往更快地得到满足。”

- 零售业 IT 总监

1 https://www.technologyreview.com/2011/10/03/190237/the-cloud-imperative

2 https://wfhresearch.com/wp-content/uploads/2023/02/WFHResearch_updates_February2023.pdf

基本指导：确保安全多云访问的六项最佳实践

基本指导 1：增进 IT 团队之间的协作，简化从接入到云的整体 IT 运维流程。

组织各自为政的运维方式和传统的连接模式已无法满足分布式应用、人员、场所和事物不断变化的安全需求。

面对日益增加的复杂性和不断扩大的受威胁面，IT 主管需要加强团队之间的协作，让他们能够更迅速、更高效、更安全地响应快速变化的业务需求。

在确保用户能从分布式位置访问多云应用（例如，基础设施即服务 [IaaS] 和软件即服务 [SaaS]）方面，前五项挑战中有四项与安全相关。40% 的受访者表示，确保从分布式位置安全访问多云应用时，孤立的云、网络和安全运维是主要挑战。

许多 IT 组织的网络和安全团队在制定计划和运维方面各自为政，而 IT 主管只能通过消除技术和运维孤岛以及减少单点集成系统的数量来应对当今的安全挑战。

想要通过团队、工具和流程的协调一致来简化运维，需要提高运维模式的一致性。思科进行的研究表明，86% 的首席信息官和 IT 主管认识到，需要开发一种更一致的运维模式，全面涵盖本地、私有云、公共云和 SaaS 系统。[3] 人们普遍认为，事实已证明，云运维模式的原则能够成功帮助开发运维和云运维团队简化运维并实现敏捷性。IT 团队也可以采用云运维模式的原则来获得类似的优势。调查数据也支持这一观点，38% 的云领域专业人员表示，他们面临的最大运维挑战是与网络团队更密切地配合，另有 34% 的受访者表示，他们面临的最大挑战是保持云和网络之间的运维一致性。

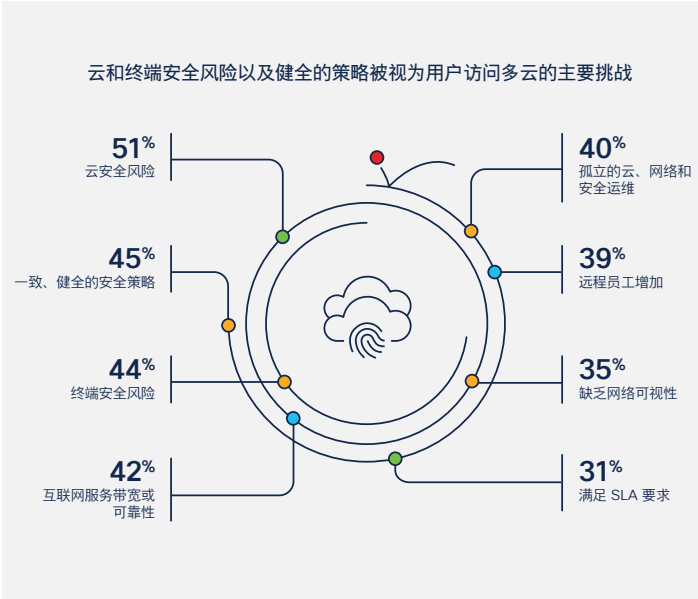


图 3. 确保从远程位置安全访问多云应用时所面临的挑战。

通过将云运维模式原则引入网络以及整个云/网络 IT 堆栈，IT 团队就可以加速创新，提高安全性，并消除云运维风险。他们可以减少复杂性和碎片化，避免其阻碍网络、安全和云运维之间的协作，最终为组织不断变化的需求提供支持。

The bridge to possible

38% 的云领域专业人员认为与网络团队更密切地配合是运维方面的一大挑战。

基本结论

基于以云为中心的模式融合网络和安全策略、技术、工具和运维工作流程，组织就能使用一组通用工具开展工作，在提高效率和降低风险的同时，促进始终如一的安全连接。

3 https://ebooks.cisco.com/story/accelerating-digital-agility-2021/page/7/1

专家观点

团队保持高度协调一致可提高安全性、简便性和性能。

“在遥远的过去，运维团队了解每一层每个系统，从布线到应用无一遗漏，并将其作为一个整体进行管理。我们需要回到那种模式。

即便云环境中的网络与本地网络不同，而且组织也无法再控制生态系统中的所有设备和软件，但是安全需求却并未改变。重要的是，无论用户身在何处或当前使用什么设备，保护用户安全访问云应用都需要一组一致的策略；在组合设计、运维和架构时，这一主旨可以为我们指明方向。

未来，在安全性和简便性原则的推动下而不仅仅是受到运维性能的驱使（因为它们都指向同一个目标），更多网络和安全团队将在端到端基础设施上开展协作。”

Wendy Nather
首席信息安全官咨询主管
思科

基本指导 2：利用 SASE 架构，转向融合的网络与安全模式。

SASE 可以实现运维简化并提供一致的安全性和性能，满足多云访问和混合办公所需。

为了做到这一点，它将网络功能与安全性集于一体来提供急需的框架，让用户能够在复杂的高度分布式环境中安全顺畅地访问应用。

SASE 正在迅速成为安全多云访问的融合架构之选。47% 的受访者希望在两年内做到主要使用 SASE 模式连接分支机构和远程客户端。

不过，许多组织目前尚难以发挥 SASE 的全部潜力，因为他们的解决方案缺乏某些功能或无法提供完全融合的网络和安全解决方案。

SASE 融合不仅需要坚实的 SD-WAN 基础，还需要丰富的云安全或安全服务边缘 (SSE) 解决方案（图 4）。只有当这些架构完全融合时，IT 组织才能实现 SASE 的全部优势。这些优势包括简化的运维模式，能够尽可能实现简单、一致的可视性、管理与随时随地安全连接用户的可控性。

统一的 SASE 解决方案提供标准化策略、共享遥测数据以及所有安全和网络组件的协调警报，能够帮助网络运维和安全运维团队提高 IT 效率、改善性能和加强保护。在网络运维和安全运维团队间采用更高效、更一致的运维模式和工作流程，一定会带来更出色的用户体验。

“安全访问服务边缘 (SASE) 提供融合的网络和安全即服务功能，包括 SD-WAN、SWG、CASB、NGFW 和零信任网络访问 (ZTNA)。SASE 支持分支机构、远程员工和本地安全访问使用案例。SASE 主要以服务的形式提供，基于设备或实体的身份并结合实时情景信息以及安全与合规策略来实现零信任访问。”

– Gartner IT 术语表，安全访问服务边缘 (SASE)，截至 2023 年 5 月 2 日。

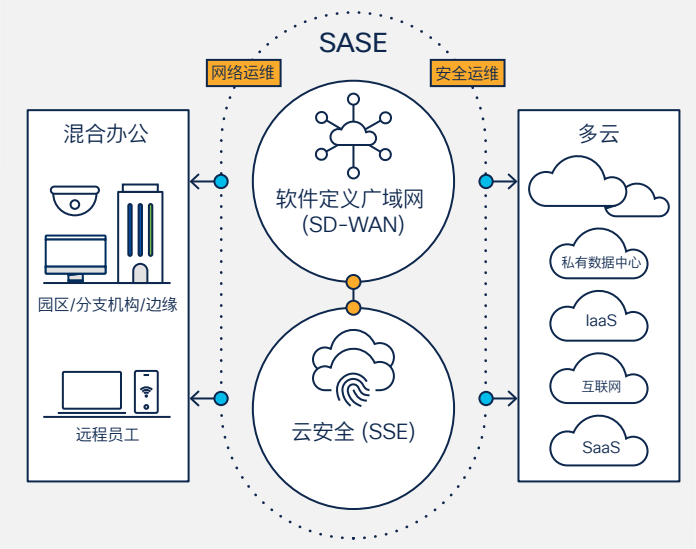


图 4. 网络和安全方面的技术与运维融合，提供了一种全新的安全连接模式 – 安全访问服务边缘。

The bridge to possible

Gartner® 预测，到 2025 年，50% 的 SD-WAN 采购将包含在单一供应商 SASE 服务中，而 2021 年这一比例还不到 10%。[4]

功能齐全的 SASE 实施可以提高运维效率、改善用户体验并加强安全保护。以下几个例子体现了这些优势:

- 思科内部 IT 团队表示，使用 SASE 后，运营支出减少了 40%
- 由独立测试公司进行的严格性能评估表明，实施了安全策略的 Umbrella（Cisco SASE 的核心组件）性能不逊色于（往往还优于）在没有安全保护措施的情况下通过互联网访问 SaaS 应用
- TechValidate 客户研究表明，85% 的思科客户在部署 SASE 架构后能够将恶意软件感染减少一半

有两种基本方法可以实现这些预期成果。

第一种是由单独的网络和安全/SSE 产品组成，这些产品通常由一个或两个供应商提供，并可集成到完整的 SASE 解决方案中。此方法适用于已经部署 SSE 或 SD-WAN 的组织，并且可能需要提高定制化程度和灵活性。

第二种是统一方法，将所有网络和安全组件作为一项统包式云服务提供，并采用统一的管理。精心设计的统一 SASE 解决方案可提高速度，简化运维，并更快实现价值。

4 Gartner，2022 Strategic Roadmap for SASE Convergence（《2022 年 SASE 融合战略路线图》），Neil MacDonald、Andrew Lerner、John Watts，2022 年 6 月。GARTNER 是 Gartner, Inc. 和/或其附属公司在美国及世界其他国家/地区的注册商标和服务标志，此处使用已获得许可。版权所有。

专家观点

在什么情况下，SASE 解决方案做不到名实相符？

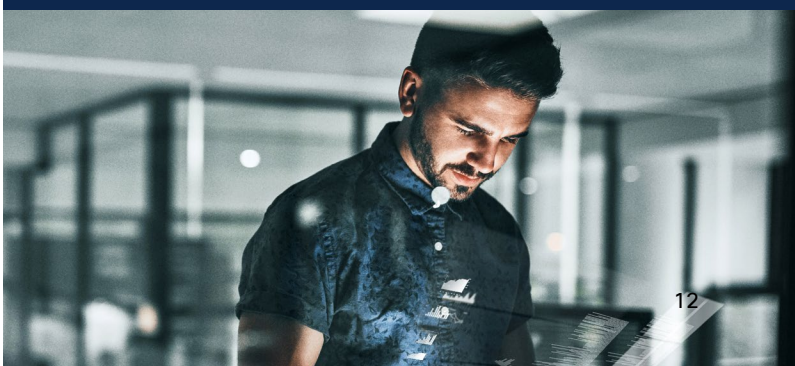
“每个组织都有已经安装的技术基础，因此，他们可能会忍不住想要直接将缺少的 SASE 功能添加到现有的不管什么基础之上。但必须注意的是，SASE 是一项长期战略选择，直接部署 SASE 模式的所有组成部分而缺乏深度集成，并不能形成功能完备的 SASE 解决方案，也无法实现预期成果。

网络和安全主管应当根据优先事项，选择已经充分集成的 SASE 解决方案或统包式统一服务。

选择统一的统包式云服务，网络运维和安全运维团队可以受益于集中管理以及智能化分布式实施，还有跨终端、企业边缘和云边缘的可控性与可视性，从而提供更安全的端到端解决方案，进一步提升最终用户体验。

无论您选择什么技术和架构来更好地满足您的需求，重要的是要确保供应商始终承诺将所有组件整合到一个充分集成的或统一的系统中。”

Omri Guelfand
NaaS/SASE 产品管理副总裁
Cisco Meraki



The bridge to possible

基本结论

与传统的安全解决方案相比，SASE 采用以云为中心的统一架构，其集中管理的安全策略和实施过程更贴近最终用户和应用，可提供灵活、顺畅、安全的连接。

深入了解 SASE

基本指导 3：跨多个云一致地扩展 SD-WAN 连接，简化 IT 体验并提升应用体验。

在所有云环境中一致地应用策略，以自动执行与云无关的连接、优化应用体验并保障其安全。

云俨然已经成为企业网络的延伸。对许多人而言，SD-WAN 也已成为实施完整 SASE 的跳板。通过各大 IaaS、SaaS 和中间一英里提供商以自动化方式扩展 SD-WAN 交换矩阵，IT 组织就能获得更大的运维控制权，从而改善用户体验。

加强对用户体验的掌控显然是网络团队最关心的问题，53% 的受访者表示，他们的首要任务是与云服务提供商集成，以提升从分布式位置访问云应用的能力。网络团队正在采取行动，49% 的受访者表示，他们将优先考虑 SD-WAN 和多云集成，将其作为未来 24 个月的首要计划。

进行 SD-WAN 多云集成后，网络和云团队就能通过互联网、互连或主机托管和云提供商网络，加速并自动完成从企业站点到各个云提供商和其他企业站点的扩展（图 5）。借助这些集成，管理员可以优化应用体验，并在所有云和本地位置实现更一致的运维体验。此外，IT 组织还可以通过与 Equinix 和 Megaport 等全球网络互连提供商的集成，对云应用和入网点提供安全且可扩展的访问。利用这些集成，IT 组织可在几分钟内以经过简化的全自动化方式构建一个全球网络。

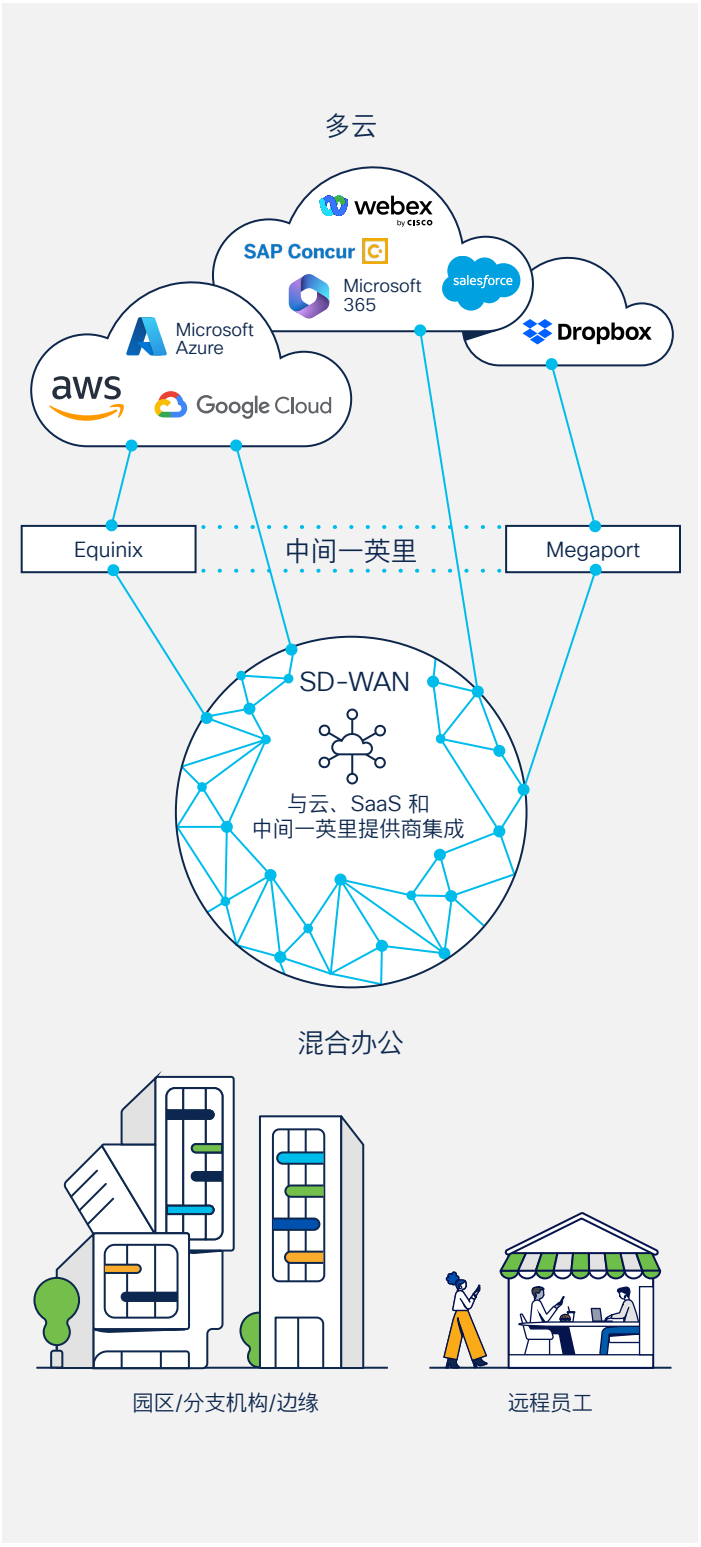


图 5. 与 IaaS、SaaS 和中间一英里提供商建立的 SD-WAN 集成对于改善 IT 和用户体验至关重要。

The bridge to possible

基本结论

对任何 IT 团队而言，如果他们需要加速和简化从企业内部到一个或多个云的扩展、优化用户应用体验，以及通过零信任访问更好地确保云应用的安全，SD-WAN 多云集成都至关重要。

详细了解 SD-WAN

专家观点

我们不能忽视多云连接的复杂性和风险。

“在当今以云为中心的时代，提供的 SD-WAN 解决方案若不与领先的云、SaaS 和中间一英里提供商紧密集成，委实难以想像。通过自动扩展客户全球站点与云工作负载之间的 SD-WAN 交换矩阵，客户可以加快向云迁移的步伐，并从简化的网络运维、端到端加密保障和灵活快速的业务创新中受益。

此外，由于与使用分布式云和 SaaS 应用相关的威胁日益增加且威胁形势不断发展变化，网络必须采用“零信任”方法并遵循其核心原则：“绝不信任、始终验证并实施最低权限”。将 SD-WAN 与零信任方法集成，组织就可以实现以下安全状况：控制哪些用户可以访问哪些云服务，为获准流量提供自动安全控制，确保持续实施，并支持立即适应安全状况的变化。”

JL Valente
企业路由、SD-WAN 和云网络产品管理副总裁
思科

基本指导 4：转向以云为中心的安全，实现一致的运维和策略。

将安全功能整合到云平台中，使企业能够更轻松、更广泛且更有效地实现可视性、策略管理和可控性。

如今，混合办公大行其道，员工不仅同时使用公司设备和个人设备，而且还会在企业网络内部和外部的受管和非受管网络中使用越来越多的应用。基于边界的传统安全保护已无法满足需求。因此，IT 组织将确保所有终端、应用和数据的安全作为重中之重。

以往，针对远程员工使用的安全策略一直与针对本地员工使用的安全策略不同。远程安全策略具有不同的信任级别并以单独的安全工具进行管理。支持不同的策略会增加 IT 开销，并有可能给最终用户带来不良体验。在研究中，当被问及安全策略时，45% 的受访者认为一致、健全的安全策略是从分布式位置提供安全多云访问的主要挑战。

除了处理层出不穷的网络威胁之外，安全团队还需要定期更新安全策略。需要在所有分布式员工中一致更新应用安全策略是集中安全功能的强大动力。59% 的受访者提到了这一点，他们表示在未来 24 个月的云接入网络计划中，他们首先要实现的是将安全功能集中到云端（图 6）。

仅凭传统的边界防御将不再有效。在集中式云安全解决方案中，需要采取一种更智能的方式来保护大规模访问应用和工作负载的安全。SSE 作为 SASE 的核心支柱，这正是它的用武之地。

图 6. 未来 24 个月的首要云接入网络计划。

The bridge to possible

基本结论

曾经定义明确的安全边界因为随时随地办公、自带设备 (BYOD) 和云服务激增而变得不合时宜。由于许多日常使用的应用都驻留在云端，组织有必要设计一种全面的 SSE 策略，整合多种安全功能并从云端有效交付。

专家观点

云安全融合是集中式集成模式的关键。

“多年来，组织一直通过增加单点安全产品来应对不断增加的威胁。这种做法确实能提高安全性，但是近来运维复杂性的急剧增加却使其得不偿失。迁移到 SSE 解决方案可以提供一组融合的可扩展云原生安全功能（安全 Web 网关、云访问安全代理、零信任网络访问和防火墙即服务），从而提高最终用户体验，改善安全成果并减轻 IT 团队的负担。

选择此类集成的集中式方法，您可以确保简化管理任务，轻松扩展性能，获得深入可视性，并在整个组织中实现强大的安全保护。融合 SSE 解决方案对于完整的 SASE 架构不可或缺。”

Jeff Scheaffer
安全/SSE 产品管理副总裁
思科

基本指导 5：在日益复杂的数字化服务交付链中，寻求通过端到端网络可视性实现一致的用户体验。

如果不能将可视性扩展到自有网络以外的互联网和云环境，IT 团队就无法确保基于云的应用和服务提供一致的出色用户体验。

改善用户体验是 IT 部门的一个重要目标。为了提供出色的体验，网络团队将目光放到传统工具之外，采用新型解决方案来增强可视性，实时掌握自身网络内外发生的情况。通过将这些扩展指标与应用性能相关联，IT 组织可以使用由此产生的洞察力来优化所有员工和客户的数字化体验。

由于组织加速采用 SaaS 和云解决方案并加大对互联网等公共网络的使用以提供对这些应用的访问，而这些多跳网络又变得越来越复杂，投资高级可视性解决方案势在必行。超过半数受访者 (51%) 将此视为首要任务，以端到端网络遥测和可视性为主要网络计划。

任何应用事务都可能经过多个网络、多个网段和多项服务（图 7）。因此，跟踪任何特定应用的性能和可用性都很困难。近半 (48%) 受访者认识到，想要改善连接，需要优先考虑互联网可视性和洞察力。这进一步凸显了 IT 组织需要采用合适的工具帮助他们洞察并可视化完整的事务路径，包括不在他们拥有或控制范围内的外部网络和环境。

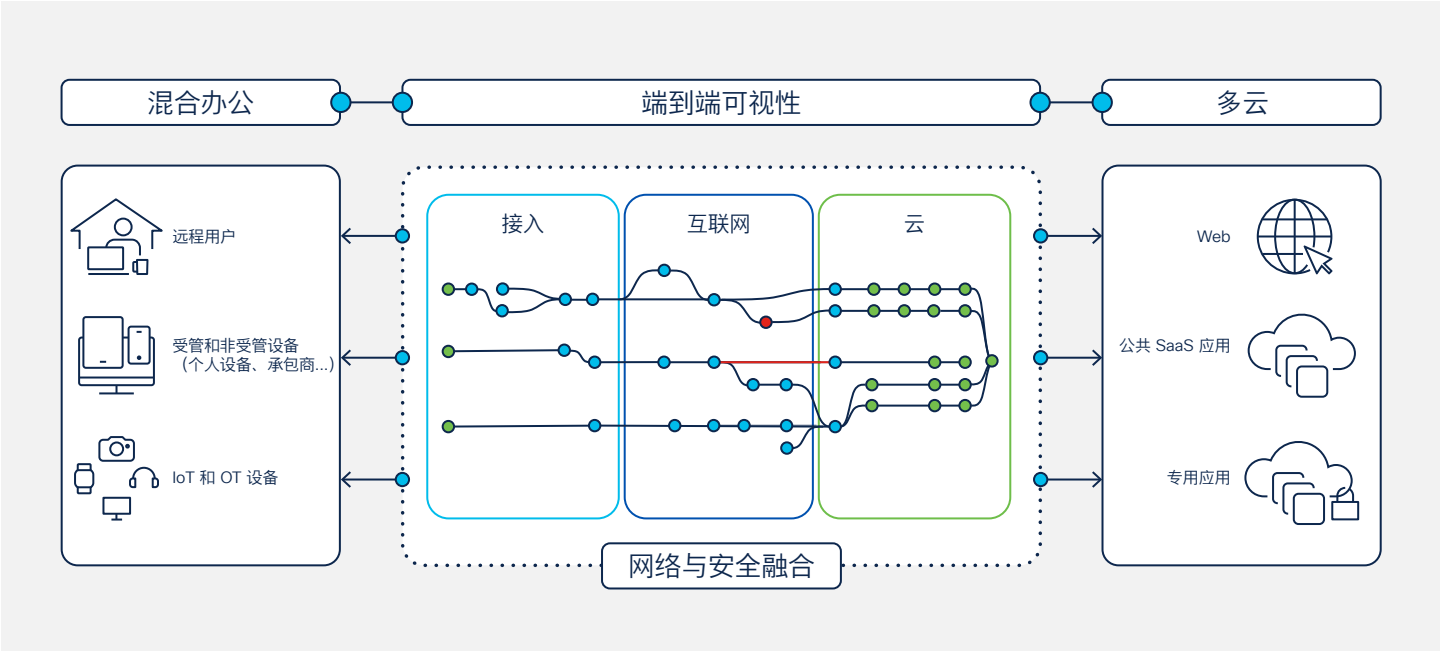


图 7. 通过互联网连接分布式环境的复杂性不断攀升，要求组织提高端到端可视性。

The bridge to possible

基本结论

云已成为新的数据中心，互联网成为新的网络，而云产品/云服务则成为主流应用。通过查看**全球互联网运行状况**和主要 SaaS 应用的性能，IT 团队可以主动检测影响到他们的重大意外网络或应用问题，并在这些问题发生后立即实施补救。

专家观点

考虑将互联网作为新的基础设施主干。

“数字化体验供应链已从单一领域转变为多方协作的系统和网络。用户可能位于任何位置。应用基于 API 和分布式微服务，旨在提高敏捷性。组织必须在可控性不如以往的许多应用、服务、云和网络之间实现顺畅无碍的体验。

因此，现代化数字体验需要采用不同的方法来实现可视性和网络状态感知；这种方法应该赋能团队快速检测和诊断网络中断并将之与基础设施和网络问题联系起来，不管出现问题的地点是家中、办公室、云端还是互联网。这要求我们能够在恰当的时间访问正确的数据，并能跨应用、网络和基础设施运维，通过互联生态系统中的第三方提供商，轻松地在内部收集和关联这些数据。”

Joe Vaccaro
ThousandEyes 产品管理副总裁
思科

基本指南 6：转变运维模式，化被动反应为主动前瞻，提高正常运行时间和性能水平。

作为 IT 智能运维 (AIOps) 工具包的重要组成部分，预测性分析可以实现更简便、更快速且更有效的整体 IT 运维，因此正逐渐获得认可。

由于扩展网络对组织开展业务的好坏具有至关重要的意义，因此任何服务质量下降或网络中断都令人难以忍受。IT 主管希望在问题发生并影响用户体验之前主动发现问题并实施补救。

随着基于云的管理平台问世，相比以往，企业可以从更多来源获得实时和历史遥测数据。使用人工智能和机器学习 (AI/ML) 技术的预测性分析模型已取得新的技术进展，可以根据所有这些历史数据和实时数据获得切实可行的智能建议。这有助于组织了解与数据相关的模式，并准确地预测问题和实施补救，以免问题影响到网络。这些模型通过一个持续的反馈循环从收到的数据中进行学习，久而久之，就会变得越来越智能。

47% 的受访者表示，他们未来两年内的首要任务是采用预测性网络分析来改善云连接。

要为访问分布式云应用的分布式用户提供一致的高性能服务，主动式 IT 运维正变得尤为重要。调查受访者认为这是一个重要的未来发展方向，47% 的受访者表示，他们未来两年内的首要任务是采用预测性网络分析来改善云连接。

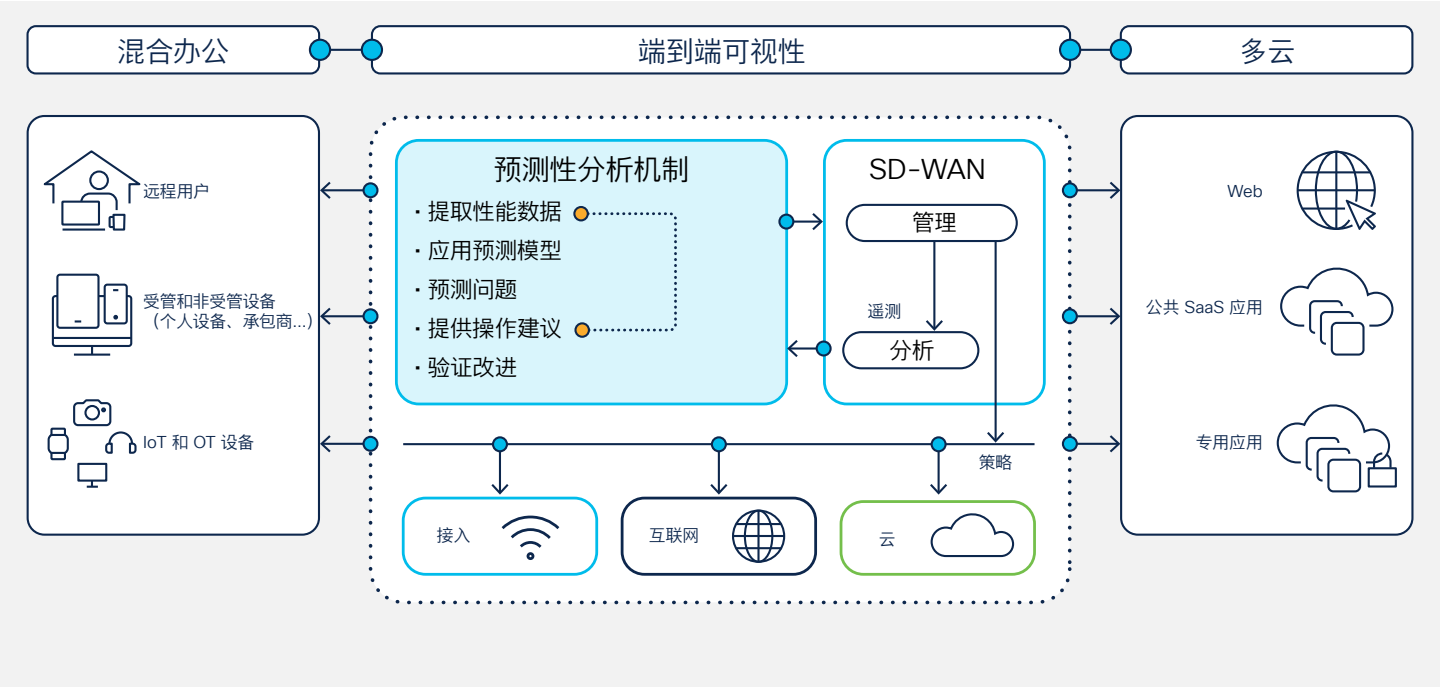


图 8. 将预测性分析与 SD-WAN 管理整合，识别并预防网络性能下降，以免影响用户体验。

The bridge to possible

基本结论

随着互联网不断变化和发展，数字化体验的速度、成本和质量都难以预料。组织需要采用预测模式和主动式运维工作流程，通过持续的数据反馈循环不断进行优化，从而确保提高基础设施的弹性和恢复能力。

专家观点

在当今技术能够支持其诞生的前提之下，预测性分析应 IT 团队的需求而生。

“传统的被动反应式运维模式会将流量重新路由到备用路径，但只有在检测到问题（通常由连接问题或服务质量下降引起）之后才会这样做。而预测性分析令人振奋的前景就在于，它能使用遥测数据、统计数据和基于 AI/ML 的计算模型预测潜在问题，从而防患于未然。以云为中心的环境在本质上是不可预测的。自动给出操作建议或主动重定向流量的能力将是优化性能和降低系统停机风险的关键。这可以改善用户体验并使 IT 部门能够专注于战略计划而非被动鉴别问题类别，从而使组织受益。”

Murtaza 博士
ThousandEyes 工程副总裁
思科

The bridge to possible

结论

远程办公和混合办公将长久持续下去。多云的采用正在加速。但是，由于威胁形势不断扩大，网络、云和安全团队使用的工具和技术十分复杂，想要为高度分布式员工、设备和应用提供安全、一致的连接，仍是一个不小的挑战。

这些团队如果各自为政，就无法解决这些连接和安全挑战，也无法提供组织参与竞争所需的数字化体验和敏捷性。大多数 IT 主管对此心知肚明。为了满足这些不断变化的需求，他们积极地结合网络、云和安全技术并试验创新的运维模式。

一个明确的方法是迁移到 SASE，近半数调查受访者计划在两年内部署充分集成的 SASE 架构，用于连接其分支机构和远程客户端。SASE 展现出了简化 IT 体验和提高安全性的前景，这要归功于它采用更轻松、更灵活的方式，能够让分布式员工和客户大规模地安全访问云应用。支持基于云的自动化和网络洞察的网络和安全平台相结合，可以提高工作流程的集成程度并促进网络运维和安全运维团队之间的协作。

以云为中心的 SASE 模式利用数据的力量提供端到端可视性和预测性分析等功能，而这些功能对于确保一致的用户体验至关重要。

您可以根据自己的业务和技术优先事项，通过多种方式开启 SASE 之旅。

详细了解 SASE 以及思科如何帮助您开启 SASE 之旅。

关于本报告

《全球网络趋势报告》于 2023 年 2 月编制，基于在北美、拉丁美洲、亚太地区和西欧 13 个国家/地区进行的调查。

今年的报告包括向网络运维专业人员收集的调查数据，这些调查对象来自使用云服务的组织。本报告使用调查数据来深入了解多云环境对网络技术以及运维方面的优先要务、偏好和选择有何影响。

本报告引用的调查数据受思科委托，由隶属于 S&P Global Market Intelligence 的 451 Research 收集，并由思科进行分析。该调查是对全球 2,500 多名 IT 决策者和担任云计算、开发运维和企业网络相关职务的专业人员进行的一项独立网络调查，本报告引用了其中的部分数据。

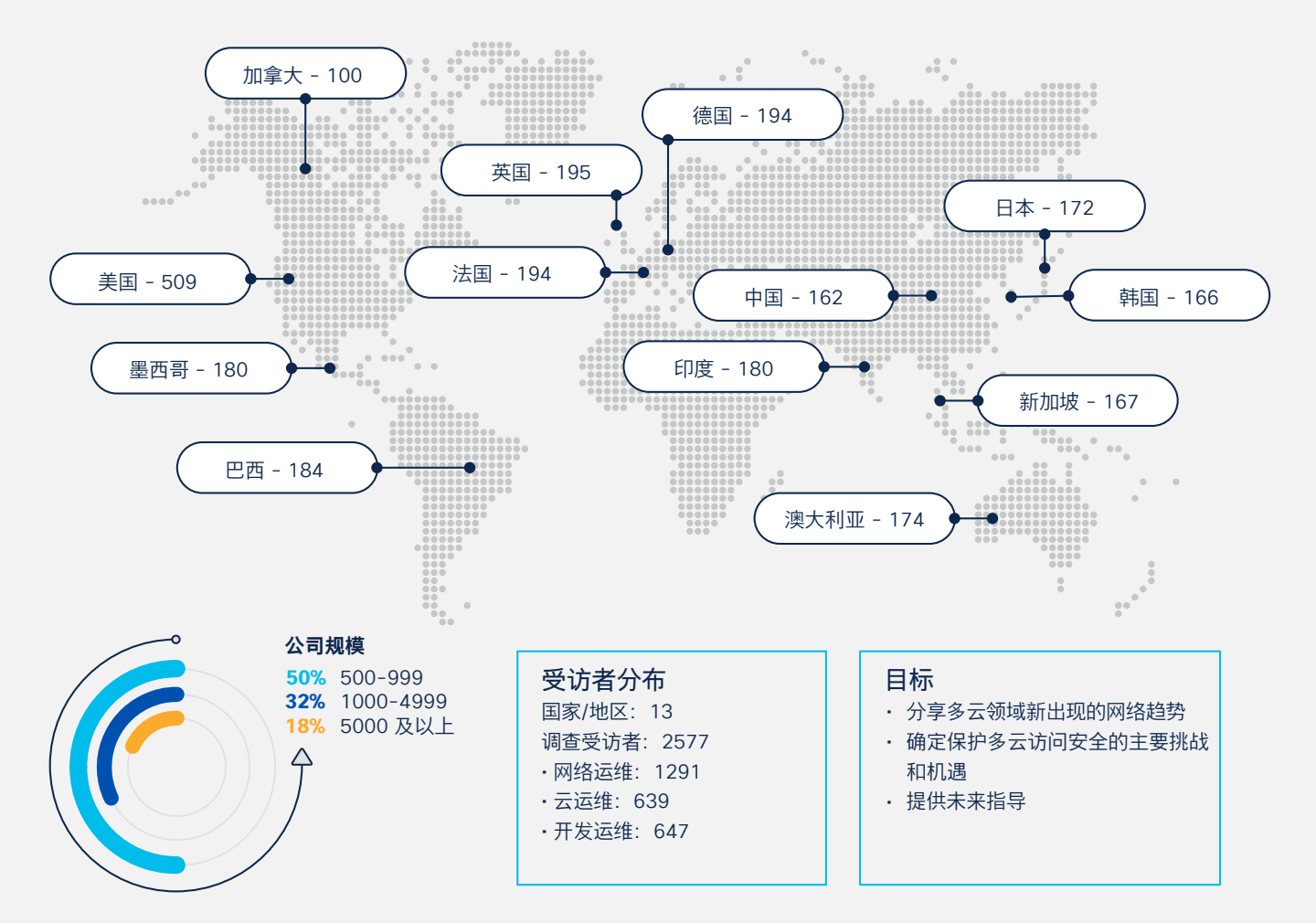


图 9. 思科 2023 年全球网络趋势调查研究方法和目标。