

2025 年

全球云安全报告

云环境保护关键见解和重要战略



FORTINET®

引言

凭借无与伦比的可扩展性和灵活性，云部署为 IT 基础架构和安全环境带来了持续变革。但多云战略是一把双刃剑，进一步增强现有优势的同时，也带来了独特的安全挑战，推动组织积极部署创新解决方案，有效保护关键资产。

《2025 年全球云安全报告》基于全球 873 名网络安全专业人士的深刻见解，深入剖析当前不断变化的云安全态势，重点介绍了组织面对日益复杂的网络环境应关注的关键趋势、安全挑战和优先事项。本报告旨在为寻求加强混合云和多云安全态势，同时持续创新的 IT 和安全专业人员提供宝贵指南。

本报告主要发现包括：

- **混合云和多云战略日渐兴起：**超 78% 的受访者拥有两个或多个云提供商，凸显了多云解决方案在增强网络弹性和利用专业功能方面日益增长的重要性。54% 的受访组织已部署混合云模型，并集成本地和公有云环境，持续优化灵活性和控制能力。
- **安全和合规性问题跃升首要关注事项：**61% 的受访组织表示，安全与合规性问题成为当前开展云部署的首要阻碍，此类组织致力于满足监管合规要求和保护敏感数据。
- **云安全专业知识和技能差距：**76% 的受访组织表示云安全专业知识匮乏，凸显了当前组织对自动化技术、定向技能提升和资源优化的迫切需求。
- **对实时威胁检测能力信心不足：**调查数据显示，64% 的受访者对组织实时处理威胁检测的能力信心不足。
- **统一云安全平台：**调查显示，97% 的受访者更青睐配备集中式仪表板的统一云安全平台，以简化策略配置、确保一致性，并提升组织云足迹的可视化。
- **加速部署云安全态势管理（CSPM）和云原生应用程序保护平台（CNAPP）：**为有效应对配置错误和合规性差距，67% 的受访者计划采用 CSPM 工具，而 62% 的受访者则打算部署 CNAPP 方案解决方案来保护云环境。



本报告着重强调了统一云安全解决方案的重要性。这些解决方案可帮助组织简化策略执行、自动检测威胁，并确保能够跨混合云与多云环境提供一致的安全防护。借助这些深入洞察和最佳实践，组织可成功构建弹性云安全态势，从容应对不断变化的威胁环境和业务发展需求。

我们衷心感谢云安全领域的全球领导者 [Fortinet](#) 为本次研究做出的宝贵贡献。Fortinet 在混合云和多云环境保护方面的专业知识和深入见解，为本报告的关键发现和建议举措提供了有力支撑。

在云计算迅猛发展的当下，本报告旨在为 IT 和网络安全专业人士提供不可或缺的宝贵资料，助力组织构筑坚实的安全防线。

感谢您的关注和支持！

Holger Schulze

Cybersecurity Insiders 创始人

云部署策略转变

云部署战略的选择，直接影响组织的安全需求、运营成果和对基础设施的要求。选择适当的云部署战略，已跃升为组织高效应对当今多元化 IT 环境的关键决策。

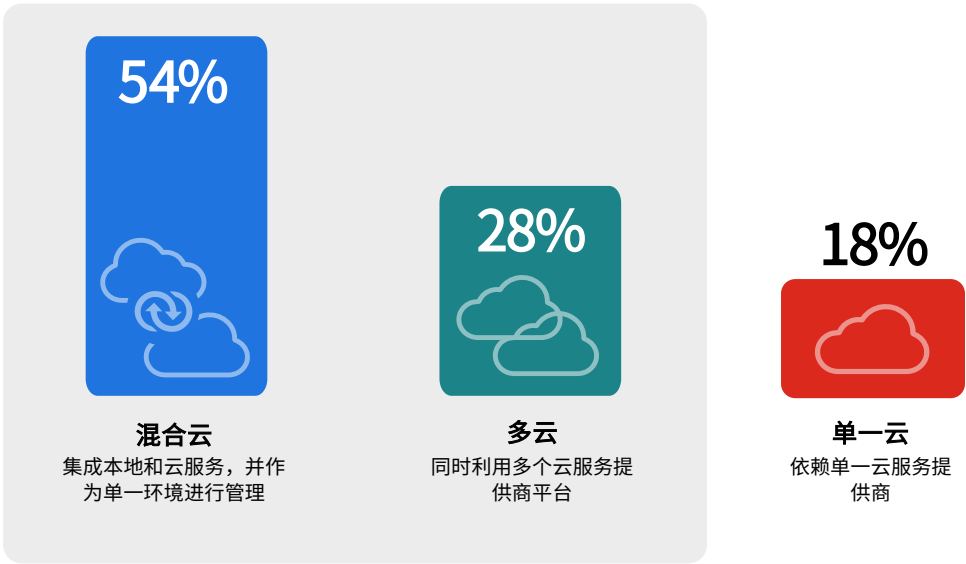
调查结果显示，混合云已成为当下企业首选主流云战略。本次调查中，54% 的受访者选择了混合云部署方案，较去年的 43% 有了显著提升。这一增长趋势有力印证，企业正从传统单一云模式向深度整合多云服务与本地系统，以打造统一高效运营环境的战略转变。例如，零售企业可能利用公有云托管面向客户的应用程序，同时，为了满足 PCI DSS 等严格的监管合规要求，选择将敏感的支付数据保留在本地私有系统。这种混合部署战略，不仅能让企业充分享受公有云带来的可扩展优势，还能确保对关键数据的绝对掌控权。

多云部署战略紧随其后，占比 28%。该战略便于组织在多个供应商间分配工作负载，避免供应商锁定或优享某些特定功能。例如，一家科技公司可能在 Amazon Web Services (AWS) 上托管计算密集型应用程序，同时使用 Google Cloud 的高级 AI 服务进行数据分析，帮助企业优化性能，同时减少对单一供应商的依赖。

单一云部署趋势正逐渐减弱，仅有 18% 的受访者表示仍依赖单一云服务提供商（占比略低于 2024 年的 22%）。这一选择虽然有利于简化管理，但也可能因此牺牲灵活性。这种部署模式可能更受小型企业的青睐，比如专注于利用 Microsoft Azure 进行文档存储和工作流管理的律师事务所，此类组织可能更倾向于选择易于管理的方案，而非追求多样化的云服务。

► 您的组织主要采用哪种云部署策略？

82% 的组织正使用多云或混合云环境

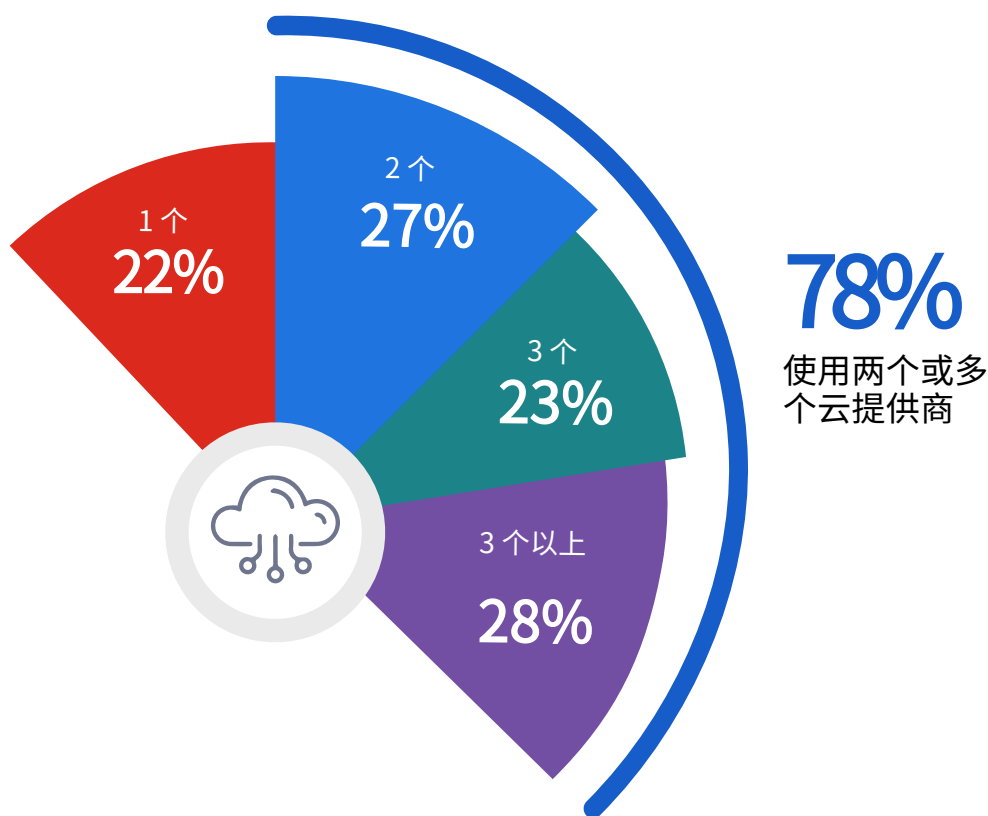


多云部署率持续攀升

当前，组织的云提供商合作数量呈现持续增加趋势。这一现状表明，越来越多的用户开始选择混合云和多云部署战略，与此同时，运营复杂性也随之攀升。

调查结果显示，78% 的受访组织拥有两个或多个云提供商。这一比例较去年的 71% 上升 7 个百分点，表明越来越多的组织开始转向多云部署战略。例如，一家跨国公司可能将 AWS 用作全球内容交付网络，同时在数据驻留法规和要求严格的区域依赖 Microsoft Azure 的合规性就绪产品。战略性地使用多个提供商，企业得以灵活利用诸如 Google Cloud 的 AI 服务或 Oracle Cloud 数据库中的专业知识和功能，同时借助服务和功能的冗余确保运营弹性。

► 目前，您的组织使用多少个云提供商？



主流云提供商占据市场主导地位

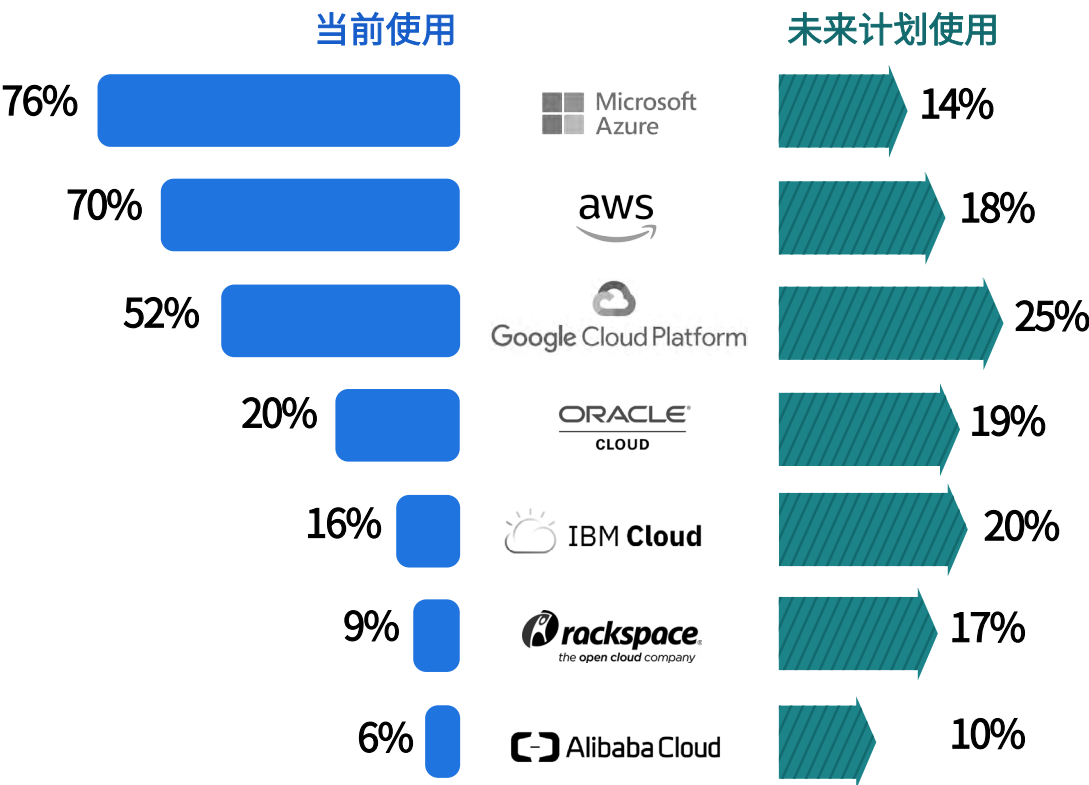
了解组织当前使用或计划采用的云服务提供商，有助于清晰洞察市场偏好，并揭示企业如何根据不断演进的工作负载和专业功能需求，调整自身云战略。

调查结果证实，Microsoft Azure 和 AWS 是企业当前青睐的主流云提供商，分别有 76% 和 70% 的受访者正在使用这两款云平台。

当前受访者中，52% 的受访者正在使用 Google 云平台，25% 的受访者未来计划使用 Google 云平台。

与此同时，尽管 Oracle Cloud 和 IBM Cloud 目前所占市场份相对额较小，但均展现出了令人瞩目的增长潜力。这一趋势很可能得益于它们在集成企业遗留系统方面的深厚专业知识与差异化优势。

► 您的组织当前使用或未来计划使用哪些云基础设施即服务（IaaS）提供商？
(选择所有适用项)



破除云部署绊脚石

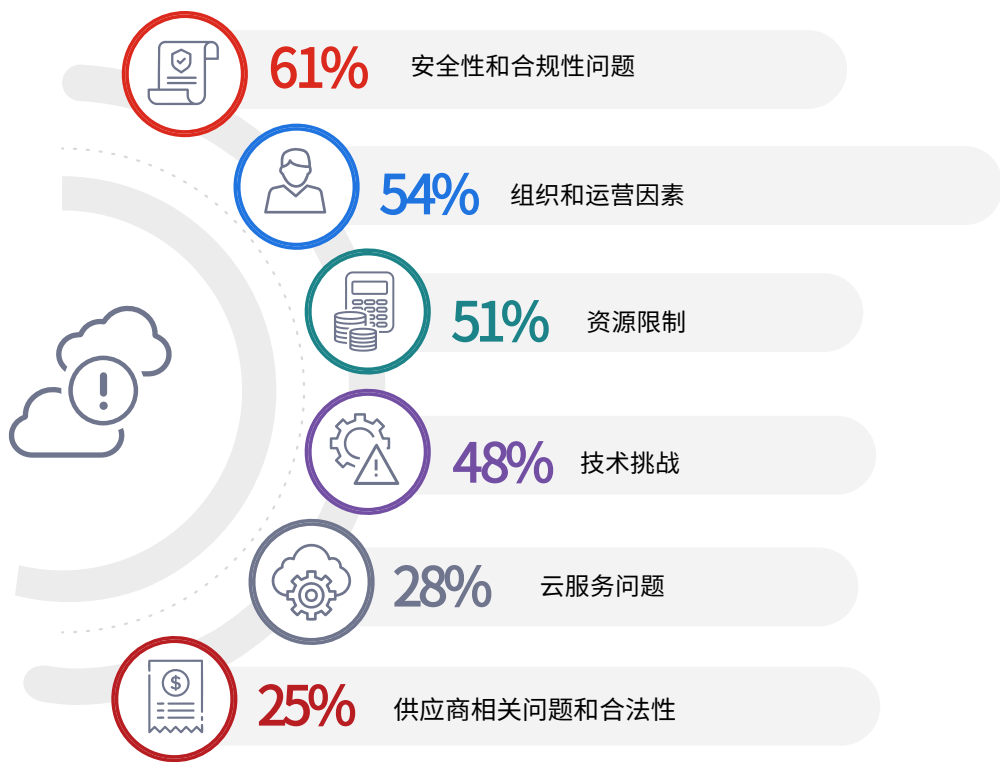
本次调查揭示了组织在部署云服务时面临的主要阻碍，深入剖析了 IT 和安全团队必须解决的关键挑战，助力组织充分利用和挖掘云环境的优势和潜力。

安全性和合规性问题仍是组织面临的最大挑战，61%的受访者提及该问题（比例高于去年的59%）。这一数据反映了企业日益关注数据泄露以及满足合规性要求的复杂性等问题。例如，由于医疗保健组织对《健康保险便携与责任法案》（HIPAA）或其他地区数据保护法律遵循情况存在不确定性，可能因此推迟将敏感的患者资料迁移至云端。

紧随其后的制约因素是组织和运营，占比近 54%（较去年的 49% 上升 2 个百分点），突显了企业对变革的抵制、供应商锁定问题和文化壁垒等挑战。例如，制造公司将遗留系统迁移至云端时，可能因担心失去对专有流程的控制而面临内部阻力。

此外，51%（高于 2024 年的 49%）的组织还提及资源限制问题，包括员工专业知识欠缺以及预算紧张。这一高比例数据凸显了，众多组织在管理和保护云功能方面面临的严峻挑战。与此同时，今年技术层面的挑战稍显缓和，占比48%，但仍然是不可忽视的重大阻碍，特别是在集成复杂的混合云环境时，技术难题的制约性尤为突出。

► 您的组织部署云服务时面临哪些主要阻碍？
(选择所有适用项)



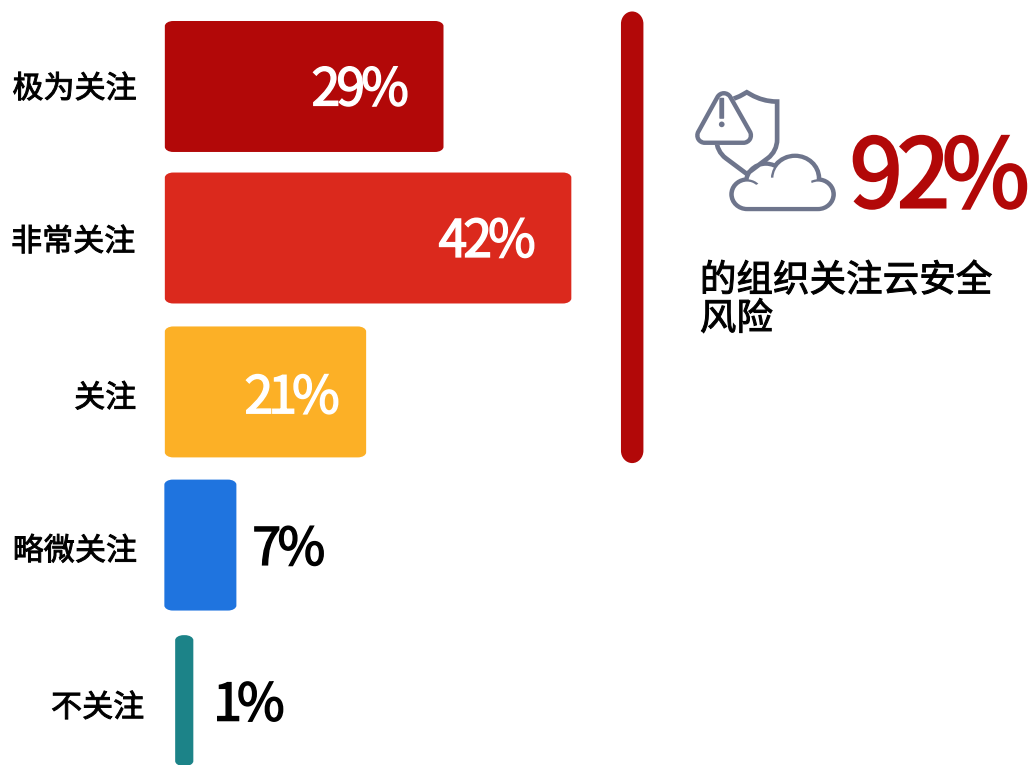
公有云安全挑战

对公有云安全性的持续担忧，凸显了企业在追求可扩展性和敏捷性等优势与构建强大防护机制之间，寻求平衡所面临的持续挑战。

高达 92% 的受访者对公有云的安全性表示担忧，充分体现了公有云在 IT 和网络安全专业人士关注的关键领域中占据重要地位。

这种担忧与本次调查结果一致，其中 61% 的受访者认为安全性和合规性是云部署的最大障碍。例如，金融服务公司将客户交易数据迁移上云时可能犹豫不决，因为担心无法满足监管合规要求或可能通过错误配置泄露敏感信息。这种担忧还延伸到部分特定风险，包括数据泄露、责任共担混淆和对云提供商活动的有限可见性，进一步导致部署决策复杂化。

► 您对公有云安全性的关注度如何？



云安全运营挑战

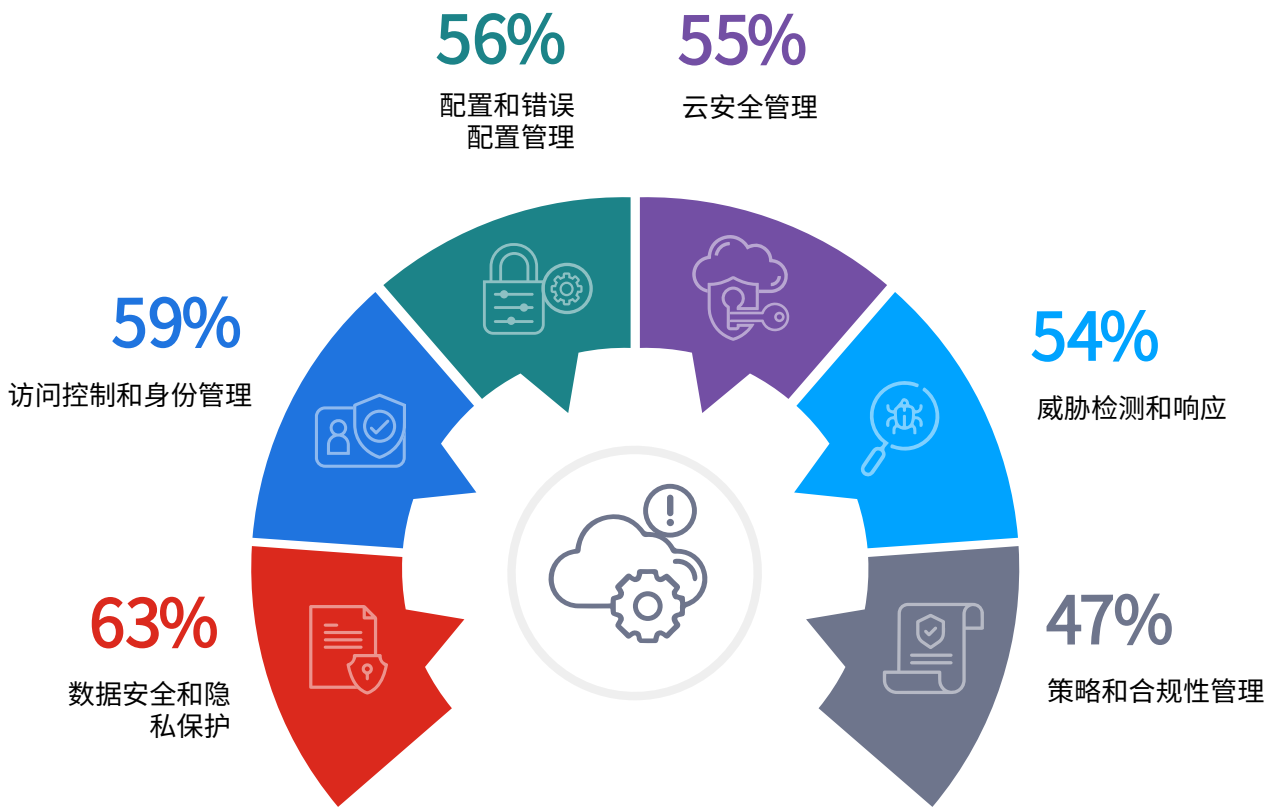
当前云安全日常运营管理现状，揭示了组织在网络环境保护方面面临着复杂且不断变化的阻碍。

63% 的受访者将数据安全和隐私保护视为首要挑战，充分体现了组织高度关注敏感信息保护和数据泄露防护。访问控制和身份管理紧随其后，占比 59%，进一步凸显了在分布式云环境中构筑强健可靠的身份验证和权限管理机制的必要性。以混合云部署为例，跨本地系统和云平台同步用户访问策略时，组织可能面临类似挑战。

配置和错误配置管理挑战位列第三，占比 56%，这一数据凸显了云的正确配置依然存在难度。例如监控云存储桶，以防止其被无意公开暴露，因为此类配置不当已引发了多起备受关注的泄露事件。

云安全管理（55%）、威胁检测和响应（54%）以及策略和合规性管理（47%），这些数据体现了组织亟需一种既支持一致策略执行又可灵活扩展的解决方案，以有效管理多云环境。

► 在日常云安全运营管理方面，您面临的主要挑战是什么？
(选择所有适用项)



其他挑战包括：
影子 IT 和未经授权的应用程序使用 46% | 云集成和自动化 43% | 终端安全性 40% | 资源分配 38%
DevSecOps 实践 31% | 运营敏捷性和复杂性 25%

多云环境保护

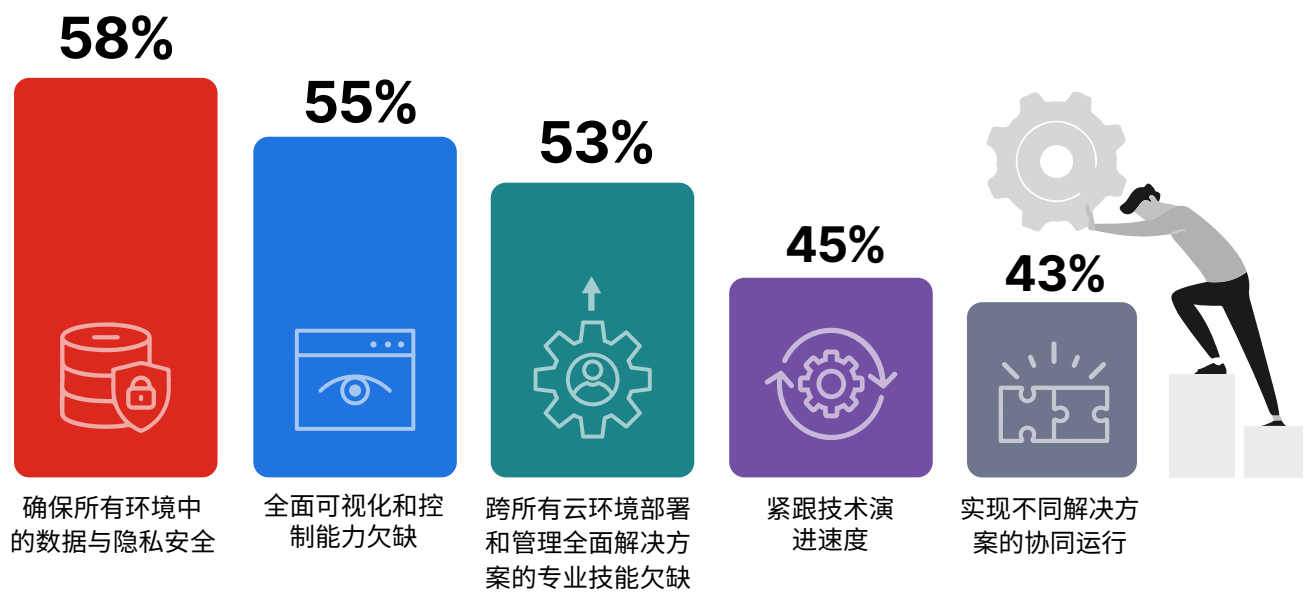
保护混合云环境面临诸多独特挑战，主要源于其内在的复杂性、标准化程度不足，以及技术的飞速发展。这些因素直接影响组织保护敏感数据、维持高效运营以及管理多元化生态系统等方面的能力。

58% 的受访者认为，确保所有环境中的数据和隐私安全仍是企业面临的主要挑战，这一比例高于 2024 年的 55%，与我们早期的调查结果相吻合。在云安全运营挑战调查中，数据和隐私安全被视为首要运营挑战（63%），这一数据充分强调了企业亟需在分散化云基础架构中采取一致的防护措施。

全面可视化和控制能力欠缺（55%），凸显了组织在多云环境中保持全面监管的挑战性。这一担忧在云安全运营挑战调查中也有所体现，55% 的受访者将云安全管理视为一项日常挑战。

53%的受访者表示，缺乏部署和管理全面多云解决方案的专业技能。另外，45%的受访者将紧跟技术演进速度视为关键挑战，而43%的受访者则表示正面临不同解决方案如何实现协同运行的难题。这些挑战普遍反映了，面对快速演进的云技术现状，企业在运营和战略层面面临多样化挑战。

► 在多云环境保护方面，您面临的最大挑战是什么？
(选择所有适用项)



其他挑战包括：
不同解决方案的管理成本 41% | 了解服务集成选项 40% | 基于用户凭证为用户提供无缝访问 37% | 筛选适当的服务集 30% | 其他 1%

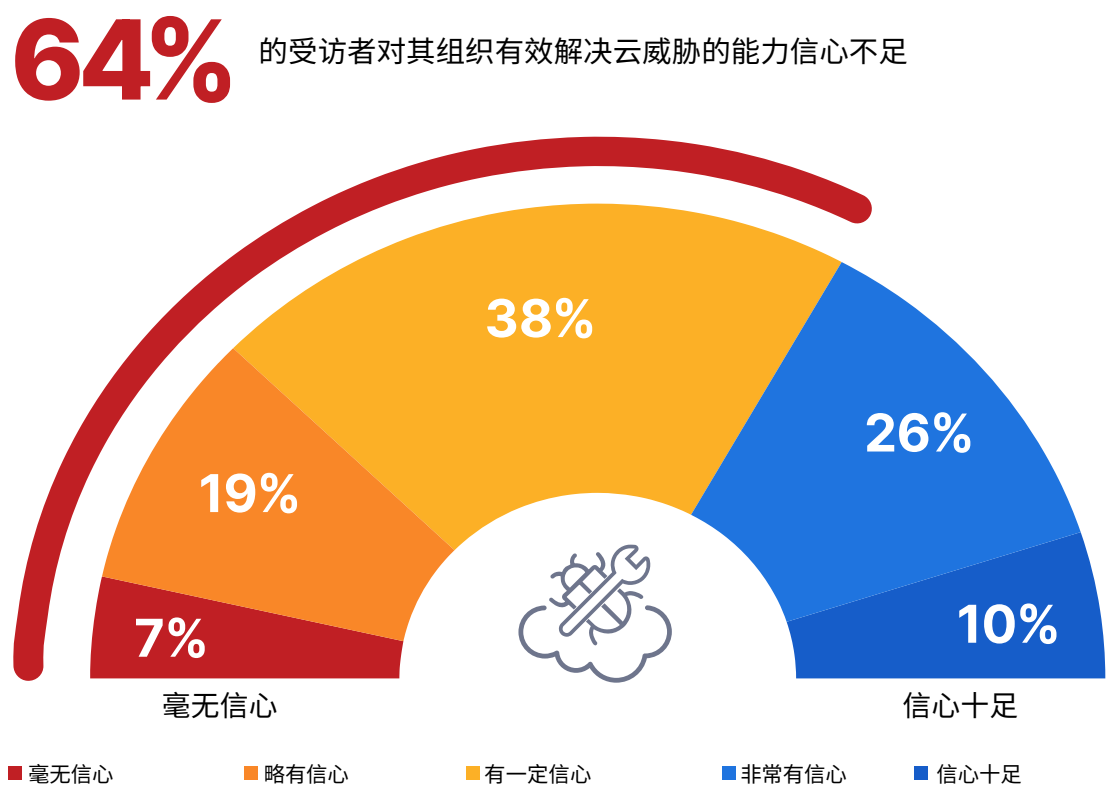
对实时威胁检测能力信心不足

随着多云和混合云战略部署的日益复杂化，具备跨多个云环境实时检测和响应威胁的能力，对于组织而言至关重要。这些架构在跨不同平台实现无缝可视化和快速响应的同时，也为企业带来了独特的安全挑战。

调查数据表明，不同组织之间存在巨大的信心差距：64% 的受访者坦言，对组织处理实时威胁检测的能力缺乏信心。例如，有效关联和综合分析一系列孤立的恶意行为时，组织可能力不从心，导致识别和响应潜在入侵行为时出现严重滞后。这一趋势清晰表明，尽管许多组织已经部署基本的安全防护措施，但面对日益复杂的云威胁态势以及管理多元环境时存在重重挑战，企业依然易遭受高级攻击，或因错误配置而引发安全风险。前文讨论的调查结果与此一致，表明全面可视化和控制能力缺乏（55%）以及威胁检测和响应能力（54%）方面的挑战，是当前企业实现云安全运营面临的主要阻碍。

仅有 10% 的受访者表示信心十足，另有 26% 的受访者表示非常有信心，其他受访者信心不足或毫无信心，超 40% 的受访者已为管理现代云威胁的需求做好了充分准备。

► 您对组织跨所有云环境实时检测和响应威胁的能力有多大信心？



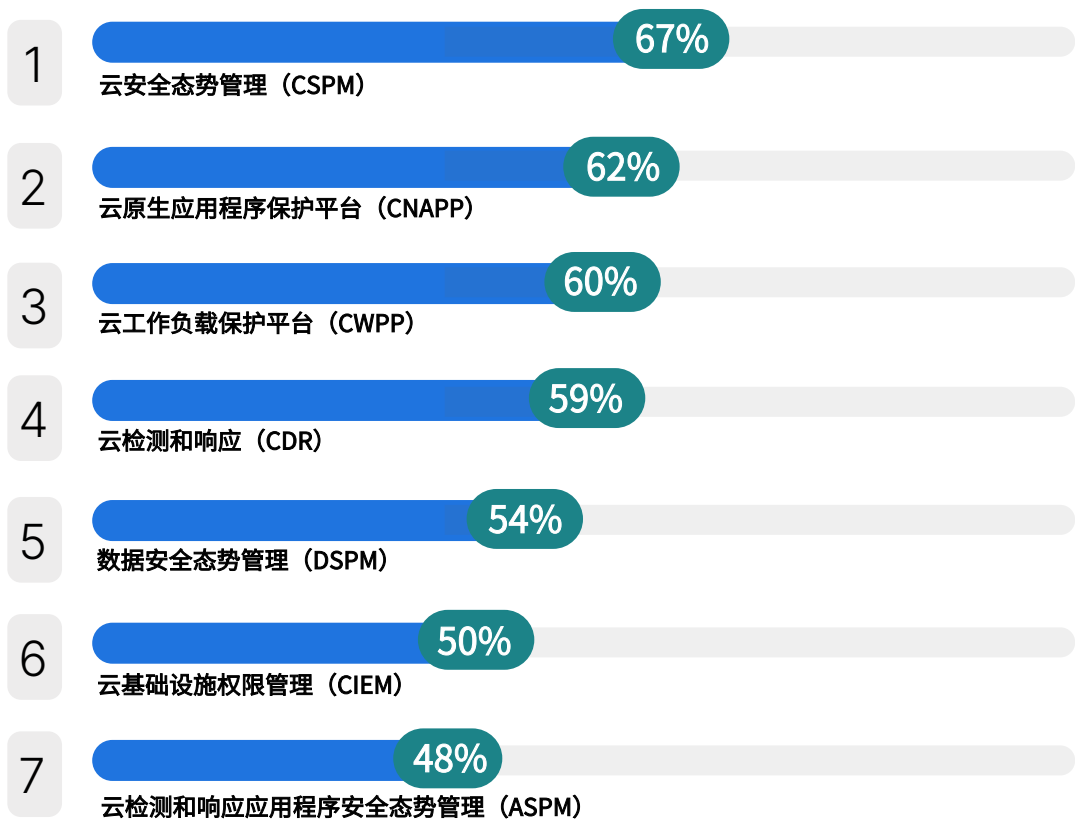
云安全优先事项

随着组织云足迹的持续扩展，部署恰当的安全工具组合变得至关重要，这一举措不仅能够支持组织在面对层出不穷的威胁时，持续确保网络弹性，还能有效维护合规性并提升运营效率。

当问及未来 12 个月内关键云安全工具的部署优先级时，云安全态势管理（CSPM）以 67% 的占比稳居首位，突显了该工具在识别和修复云环境错误配置方面的关键作用。例如，CSPM 工具能够及时向零售商发送告警，警示其 AWS 云中存在公开暴露的存储桶，从而有效防范代价高昂的数据泄露事件。

此外，云原生应用程序保护平台（CNAPP）占比达 62%，表明企业对保护端到端应用程序生命周期安全性的需求日益迫切。CNAPP 能够主动标记 Kubernetes 中运行的容器化工作负载中的安全漏洞，识别恶意运行时活动，并有效检测存在潜在系统入侵风险的事件链。紧随其后的是云工作负载保护平台（CWPP）（60%）和云检测和响应（CDR）（59%）工具，体现了企业对工作负载安全和威胁缓解的日益关注，尤其在多云设置方面，关注度有所提高。此外，云基础设施权限管理（CIEM）占比达50%，进一步表明企业亟需跨不同云平台实施强大的安全访问和权限控制，并深入推行最低访问权限或删除未使用凭证的举措。

► 您正在使用或未来 12 个月内计划使用以下哪些工具？
(选择所有适用项)



弥合网络安全技能差距

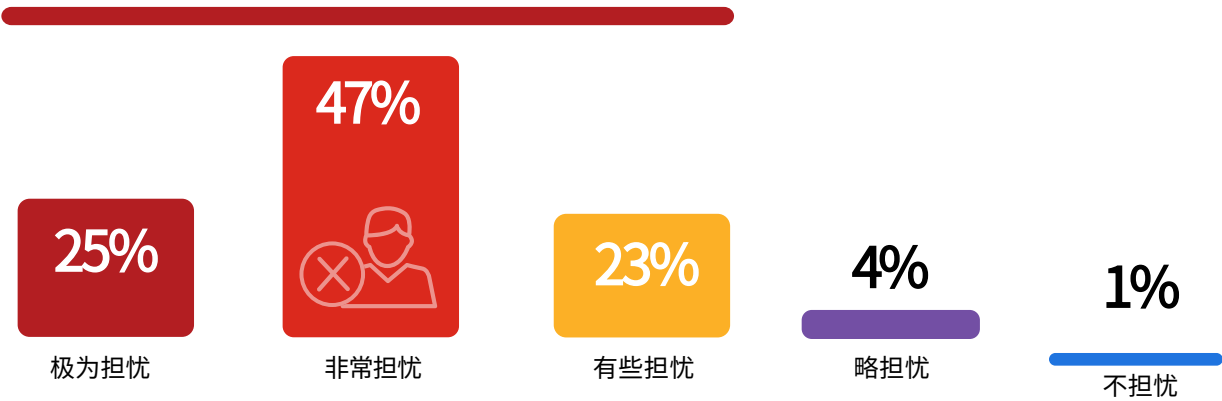
网安行业专业技能人才短缺仍是企业面临的关键问题，直接影响企业保护资产以及有效应对持续演进威胁的能力。

调查结果显示，95% 的受访者对网络安全技能人才持续短缺表示很担忧和极为担忧，凸显了组织为有效应对日益复杂的网络安全挑战，在招募和留住所需人才方面所承受的巨大压力。例如，由于配置管理或云基础设施权限管理（CIEM）等特定云技能专业人才短缺，希望实施多云安全控制的医疗保健提供商可能迟迟无法开展此类工作。

► 您对网安行业专业技能人才短缺的担忧程度如何？

95%

的组织对业界普遍存在的网安专业人才短缺问题表示很担忧和极为担忧。



调查数据显示，高达 76% 的组织正深陷人才短缺的困境，这一数据充分印证了当前人才担忧的现状。

► 您的组织是否存在网络安全人才短缺问题？



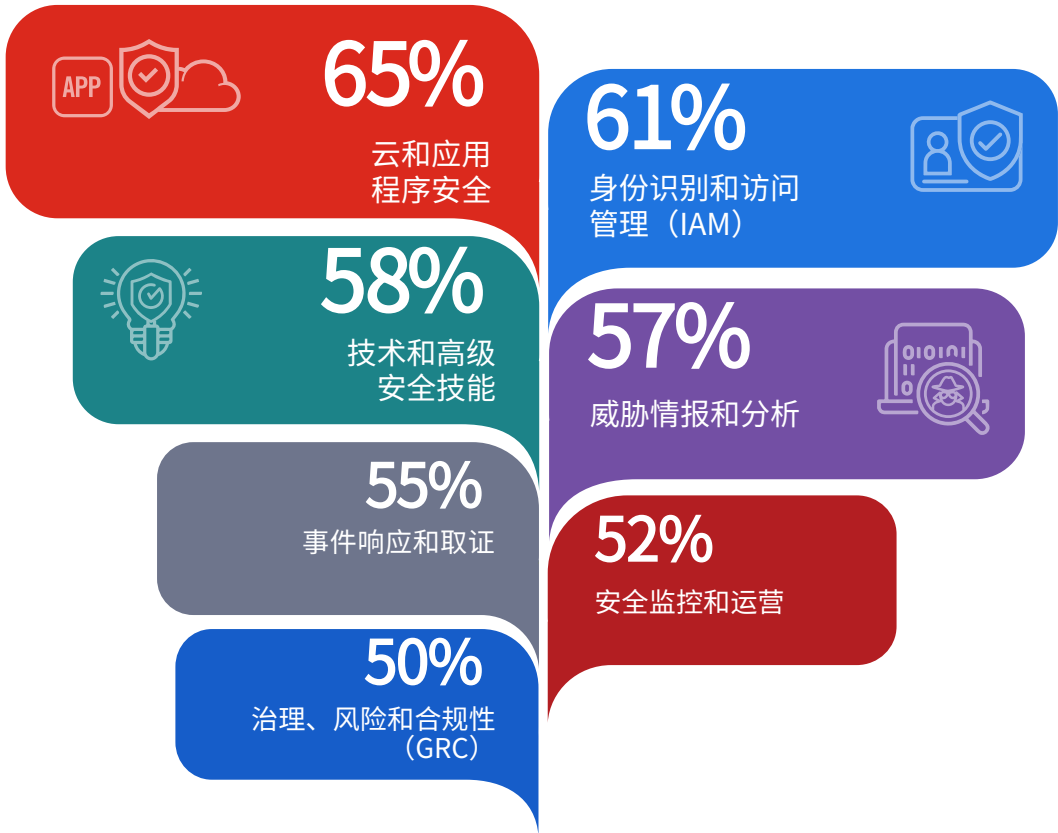
应对当今威胁的关键安全技能

有关“最重要安全技能”的调查结果，揭示了组织应对日益复杂的云安全挑战时，需具备不断提升的多样化专业知识。

在所有调查选项中，云和应用程序安全技能以 65% 的占比位列榜首，反映了组织对保护云平台 and 应用程序的高度重视。例如，云平台的安全性领域是一个高度专业化的范畴，涵盖了构建自动化 Guardrails（防护栏）和可扩展的、安全可靠的 DMZ 区等复杂任务。这些高级功能往往通过精密的代码实现自动化部署，从而确保云环境的稳健与安全。

身份识别和访问管理紧随其后，占比 61%，体现了企业对严格访问控制功能的迫切需求，尤其在混合云和多云环境中，统一用户权限管理至关重要。此外，技术和高级安全技能占比 58%、威胁情报和分析占比 57%，均反映了组织对专业技能人才需求的不断增长，这些特定领域的专业人士能够充分运用 AI 技术并深谙复杂的攻击战术，从而精准识别和缓解恶意活动，快速处理被盗用的云管理员帐户。事件响应和取证技能占比 55%，该技能对于减少入侵行为和降低入侵事件影响仍至关重要，而安全监控和运营占比达52%，表明企业亟需具备检测异常事件和加速威胁缓解的专业知识和技能。

► 您的组织希望具备哪些重要安全技能？
(选择所有适用项)



其他安全技能包括：
安全意识和培训 45% | 通信与策略 39% | 不确定 3%

云安全投资趋势

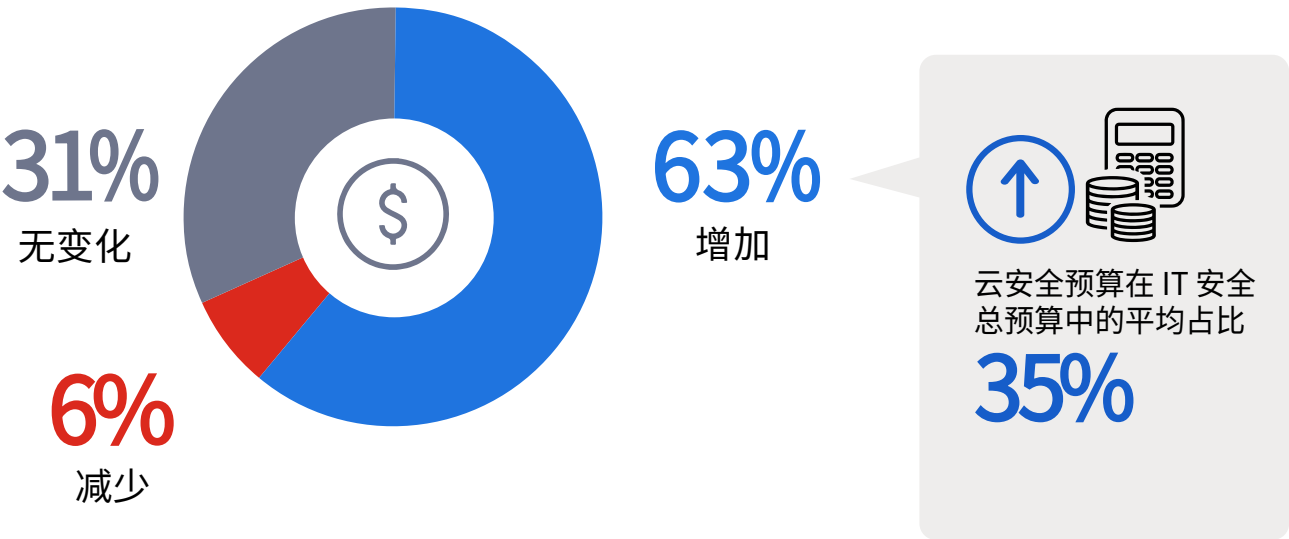
本次调查结果揭示了一项全新见解，即组织如何优先分配财务资源以有效应对云安全挑战。高达 63% 的受访者表示，计划在未来 12 个月内增加云安全预算（略高于去年的 61%）。这一增长趋势表明，企业已强烈意识到加强混合云和多云环境防御的紧迫性和必要性。

同时，31% 的受访者表示未来 12 个月内云安全预算保持不变（略低于 2024 年的 32%）。该调查结果可能源自已投入大量资金或存在持续运营管理需求的组织。仅有 6% 的受访者坦言未来 12 个月内将减少云安全预算。在云威胁不断升级和监管要求日益严格的当下，该趋势较为罕见。

调查显示，云安全预算在IT 安全总预算中的平均占比为 35%。这表明云保护支出在企业整体安全支出中的比重正逐渐攀升，尤其在组织加速云部署加速的当下，该项支出占比有望持续增加。

对云安全投资的日益重视，表明企业正普遍采取积极主动的战略，以弥合本报告提及的可视化、访问控制和威胁检测等关键能力差距。建议计划增加云安全预算的组织，专注于有效集成多种关键功能的解决方案（如CNAPP），最大限度提高投资效益。

► 未来 12 个月内，您的云安全预算有何变化？



统一云安全平台的价值与优势

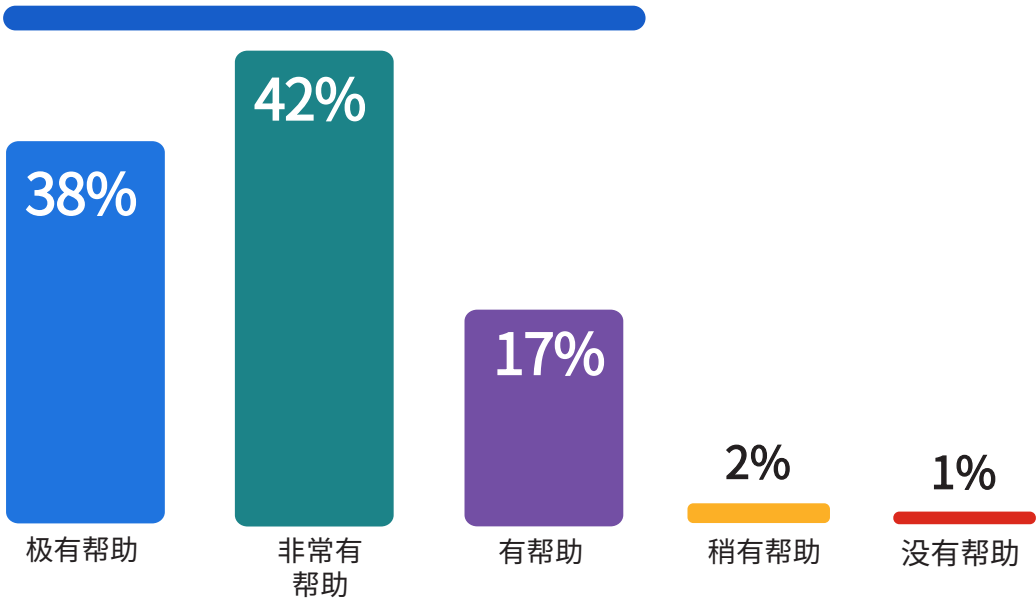
配备集中式仪表板的统一云安全平台的价值与优势在于，助力组织跨整个云环境简化策略配置、确保一致性并增强可视化能力。

本次调查结果显示，组织对统一云安全平台概念展现出了浓厚的兴趣。高达 97% 的受访者坚信，统一平台能为组织提供中等乃至极高的帮助。例如，单一仪表板支持金融服务组织跨 AWS、Azure 和 Google Cloud 等多个云平台实施统一的访问控制策略，有效降低配置错误风险。该结果与上述调查结果相互印证，上述调查结果显示，55% 的受访者认为在多云和混合云环境中，全面可视化和控制能力欠缺是企业面临的主要挑战，并强调需部署集中式工具来缩小此类差距。

► 如果您部署了一款配备单一仪表板的统一云安全平台，支持您轻松配置所有所需策略，并能跨整个云环境实现更为一致和全面的数据保护，这将对您的工作带来多大帮助？



的组织认为，配备单一云安全仪表板的统一平台能够提供中等乃至极大的帮助



增强混合云和多云安全性的最佳实践

随着云计算的快速发展，采用多云与混合云架构已成为企业在现代商业环境中保持竞争力的有效策略。然而，组织在管理多样化的云提供商及确保强大安全性方面所面临的挑战也愈发严峻。为有效应对这些挑战，组织必须紧跟行业洞察，实施战略性的最佳实践，并采纳符合自身需求的高级安全解决方案。

以下建议提供了可操作的步骤，助您增强多云安全态势。

1

自动检测和修复云风险

错误配置仍是云安全的常见漏洞，67% 的受访者坦言正使用或计划采用自动化工具解决此类难题。持续监控和实时修复解决方案可帮助组织主动识别风险，例如存储配置错误或过高权限，并有效地纠正这些风险。这些工具还可帮助组织简化合规性流程，满足行业法规的监管要求。

2

保护跨云环境的数据流

当数据跨云环境移动时，确保其安全性与完整性至关重要。58% 的受访者强调数据与隐私安全是其关注的首要问题，充分利用数据流全面可视化工具，可帮助组织在数据传输过程中有效保护敏感信息外泄。这些工具能够实时监控潜在风险，有效防止未经授权的非法访问，同时助力组织严格遵守 GDPR、CCPA 等监管框架要求，全面强化企业整体的数据防护体系。

3

实施统一的威胁检测机制

超半数受访者（54%）强调，在多云环境中检测和响应威胁困难重重。统一威胁检测解决方案集成了可视化功能，赋能安全团队快速识别和响应异常情况。这些工具能够关联不同云环境中的海量数据，大幅减少检测时间并提高响应准确性。

4

投资安全团队的云安全专项培训

技能短缺影响了 76% 的组织，限制了他们有效部署和管理云原生解决方案的能力。积极投资云安全专项培训，提升员工在 DevSecOps 和容器安全等领域的专业技能，赋能团队从容应对各类新兴威胁和安全挑战。

5

利用策略即代码实现一致的安全策略实施

43% 的受访者坦言，在实现不同解决方案的集成和协同工作方面存在挑战，利用策略即代码方法可确保跨多个云平台实施一致的安全策略。策略即代码解决方案简化了审计流程并实现了自动化配置管理，确保安全控制功能与组织需求高度契合。

6

将安全投资与对应用程序工作负载的实际需求精准对接

应用程序级安全性已成为一项备受关注的优先事项，62% 的受访者计划部署全面的保护平台。从开发到运行时，应用程序的端到端安全性可确保为工作负载提供量身定制的安全保护，同时支持跨多种环境实施一致的安全策略。能够与容器化环境和运行时防护措施集成的解决方案，可有效满足这一需求。

7

跨云平台实现标准化访问控制

访问控制和身份管理仍是 59% 的受访组织所面临的主要挑战，特别是在进行分布式云设置时，这一问题尤为突出。集中式访问控制解决方案可有效简化用户权限管理，并能够帮助组织在混合云和多云环境中实施一致的安全策略。部署统一身份验证平台，可确保安全策略的无缝实施，并大幅降低因未经授权访问引发的安全风险。

8

部署可扩展的云端安全工具

54% 的受访者将混合云视为其主要部署模型，因此部署可扩展的云端安全工具至关重要。这些解决方案能够跨本地系统和公有云环境实现一致的安全防护，确保组织实现高效运营同时，按需安全扩展云足迹。

结论

本报告着重强调，各规模企业应基于自身的环境和挑战，积极投资于量身定制的统一工具、专业培训及流程，从容应对不断演变的混合云和多云安全需求。通过有效应对配置错误、技能差距和可见性缺乏等关键挑战，帮助企业构筑强健的安全防御体系。

遵循本报告中推荐的最佳实践，企业将能够在纷繁复杂的云环境中蓬勃发展，有力守护关键资产，同时在迅猛推进的数字化转型浪潮中，持续保持高度的敏捷性与合规性。

云安全术语表

本术语表简要概述了本报告中讨论的关键云安全技术，重点介绍了这些技术的作用、可解决的安全挑战，以及它们在保护当今复杂的云环境方面的重要性。

应用程序安全态势管理 (ASPM) —— ASPM 提供对整个软件开发生命周期中应用程序漏洞和配置问题的全面可见性，支持安全的编码实践，并将安全性无缝集成至 DevSecOps 工作流。ASPM 对于确保应用程序从开发、部署到运行时，持续保持安全性至关重要。

云检测和响应 (CDR) —— CDR 是一种识别和缓解云环境中威胁的专用技术，可提供对云活动的实时可见性，帮助用户快速检测异常和响应事件。CDR 在分布式云环境的设置中，对于构建针对复杂威胁的强大防御体系至关重要。

云基础设施权限管理 (CIEM) —— CIEM 专注于管理云环境中的权限和访问控制，可帮助组织全面了解其云身份和权限，确保剔除多余的特权，强制实施最低访问权限原则，有效降低权限滥用风险。CIEM 对于在多云架构中维护安全合规性访问策略非常重要。

云原生应用程序保护平台 (CNAPP) —— CNAPP 集成了多种安全功能，可在云原生应用程序的整个生命周期内提供全面的安全保护。该解决方案结合了工作负载保护、配置管理和运行时防护，全面保护容器、无服务器功能和其他云原生工作负载。CNAPP 非常适用于采用 DevOps 和微服务等现代开发实践的组织。

云安全态势管理 (CSPM) —— CSPM 是一款能够自动检测云环境中错误配置的解决方案，可帮助组织持续监控云基础设施的安全风险，例如暴露的存储桶或过于宽松的访问控制策略，确保符合监管框架要求。CSPM 可帮助用户解决多云和混合云环境中的安全漏洞，并提供全面的可见性。

云工作负载保护平台 (CWPP) —— CWPP 可保护云环境中的工作负载，包括虚拟机、容器和无服务器架构，可提供对漏洞的全面可视化，确保一致的安全策略实施，并保护工作负载免受各类高级威胁。CWPP 是组织管理各种动态云工作负载的关键工具。

数据安全态势管理 (DSPM) —— DSPM 是一种以数据为中心的解决方案，用于识别、分类和保护云环境中的敏感信息。该工具可确保数据得到适当保护，并符合 GDPR 和 CCPA 等隐私法规的监管要求。DSPM 在解决复杂的云生态系统中保护敏感信息的挑战方面，发挥着至关重要的作用。

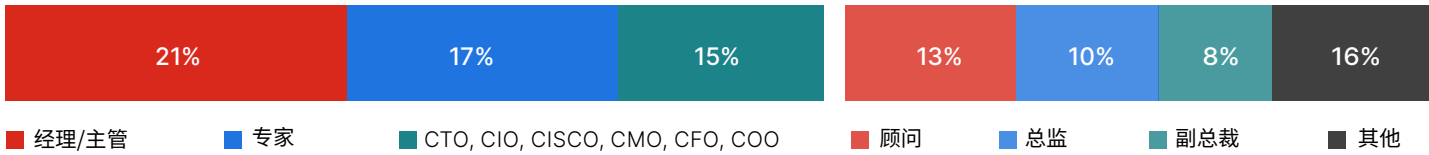
问卷方法和人口统计

《2025 年全球云安全报告》是依托 2024 年底开展的一项综合性调查，广泛汇集了来自全球多个国家/地区并跨技术、金融服务、医疗、政府机构等多个行业的 873 名 IT 与网安领域专业人士的深刻见解。受访者覆盖了从小型企业至大型企业的各类规模组织，同时囊括了从专家到 CXO 高管的各层级专业人士。

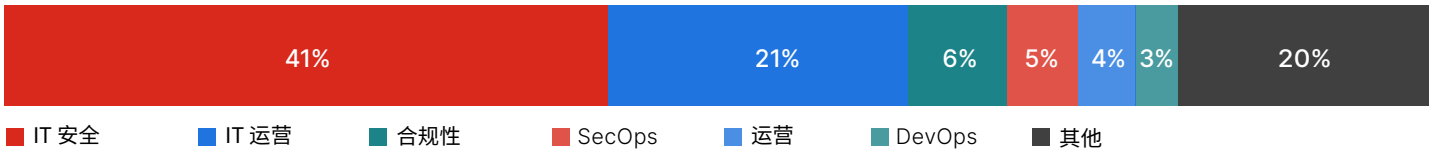
这项调查通过在线进行，探讨了当前云安全的主要趋势、挑战和优先事项。这些发现为组织提供了全面的视图，帮助组织了解如何驾驭复杂的云环境，并采用适当的安全技术从容应对各类新兴威胁。

对于允许受访者选择多个答案的问题，其百分比总和可能超过 100%，因为受访者可选择多个选项。

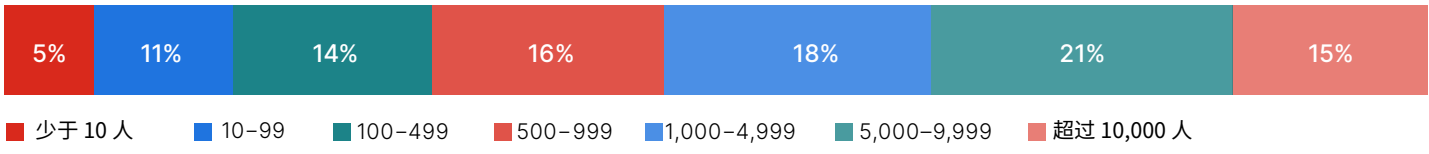
职位



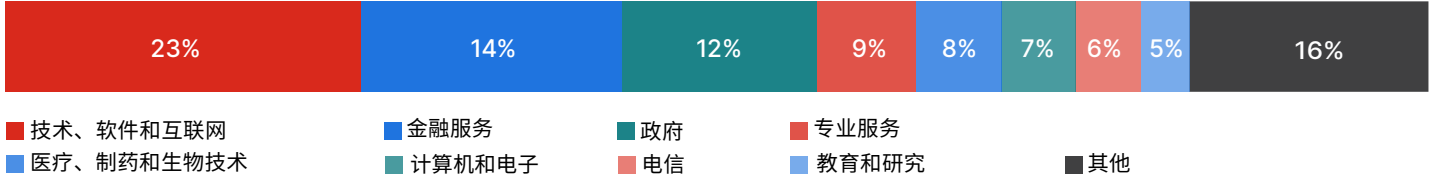
部门



企业规模



行业



内容重用

我们鼓励根据 [Creative Commons Attribution 4.0 International License](#) 的条款重复使用或引用本报告中发布的数据、图表和文本。您可以在遵守许可条款的前提下，自由分享本作品并将其用于商业用途，但需按规定对报告进行署名。例如：“Cybersecurity Insiders 和 Fortinet 2025 年全球云安全报告”。



Fortinet (NASDAQ: FTNT) 致力于为全球大型企业、服务提供商和政府机构提供安全保护服务，赋能组织跨多种环境轻松实现整个攻击面的全面可视化，全方位掌控各类威胁挑战，持续满足企业当今和未来不断扩展的性能需求。

无论是在网络、应用程序、多云还是边缘环境中，Fortinet Security Fabric 安全平台均能够提供卓越的安全防护，帮助企业组织克服关键的安全挑战。Fortinet 在全球安全设备出货量中排名首位，超 80 万名用户选择 Fortinet 解决方案和服务保护其业务。

www.fortinet.com

Cybersecurity

I N S I D E R S

Cybersecurity Insiders 汇聚了 600,000 余名 IT 安全专业人士及世界级的技术供应商，旨在助力智能解决问题，携手应对当下紧迫的网络安全挑战。

我们专注于打造并精选独特内容，为网络安全专业人士提供最新网络安全趋势、解决方案及最佳实践的教育与资讯。从全面的研究报告、公正的产品评测，到实用的电子指南、引人入胜的网络研讨会及教育性文章，我们致力于提供广泛且宝贵的资源，为当今复杂的网络安全挑战提供基于证据的答案。

立即联系我们，了解 Cybersecurity Insiders 如何助您在竞争激烈的市场中脱颖而出，提升需求、品牌知名度和思想领导力地位。

发送电子邮件至 info@cybersecurity-insiders.com 或访问 cybersecurity-insiders.com