cloud security alliance®

tenable

Survey Report

The State of Cloud and AI Security 2025

致谢

主要作者

希拉里·巴伦

贡献者

马丽娜·布格库 乔什·布克 尔 Ryan·吉福德 亚历克斯·卡卢扎 约翰·Yeoh

图形设计

克莱尔·莱纳特 斯蒂芬·伦佩

关于赞助商

目录

执行摘要

混合云和多云架构已成为大多数企业的标准，82%的企业正在运营混合环境，63%的企业使用多个云服务提供商。与此同时，人工智能的采用正在加速，超过一半的企业为业务需求部署人工智能——而其中34%已经有AI工作负载遭遇安全漏洞。然而，安全策略并未与时俱进，导致团队反应迟缓且职责分散。

这项调查揭示了六点关键见解：

1. 混合云和多云主导：
灵活的基础设施需要统一的网络安全可见性和策略执行——这对于大多数情况仍然缺失。

2. 身份风险领先但仍管理不足：

身份现在是首要风险和违规原因，但许多组织依赖基本控制和指标，忽略了更深层次的治理差距。

3. 专业知识差距阻碍进展：
有限的云安全专业知识会削弱领导层的一致性、战略和投资。

4. 测量漏洞，而非预防：
KPIs仍然是被动的，专注于事件而非风险降低和恢复能力。

5. 人工智能采用速度快于安全准备情况：

组织优先考虑合规性和新型人工智能风险，而非成熟的云和身份控制。

—
过时的假设和投入不足，使安全团队缺乏成熟的结构性支持。

为解决这些差距，组织应：

• 跨越混合云和多云基础设施构建一体化可视性和控制能力 • 人类与非人类身份的成熟身份治理 • 将KPI聚焦于预防和韧性 • 提升领导层对真实运营需求的认知 • 将合规视为AI安全的基准，而非终点

安全成熟度取决于战略协同和风险驱动规划。超越点解决方案和被动式运营的组织将更能保障不断发展的云和人工智能环境。

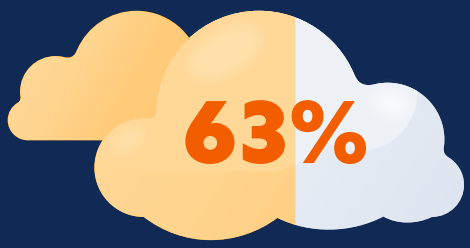
关键发现

云和人工智能不再是新兴趋势——它们已融入组织的运营方式中，混合云和多云架构提供了灵活性，人工智能正迅速从试点项目转向业务关键型工作负载。然而尽管采用率飙升，安全战略却难以跟上步伐。调查结果揭示了一个明显的认知与执行差距：尽管大多数组织都认识到风险所在，但许多组织仍处于被动响应、支离破碎且目标不一致的状态。

混合云和多云主导

混合云和多云架构并非新兴趋势——它们已是大多数组织的标准配置，并将长期存在。与其将一切迁移到单一供应商或放弃

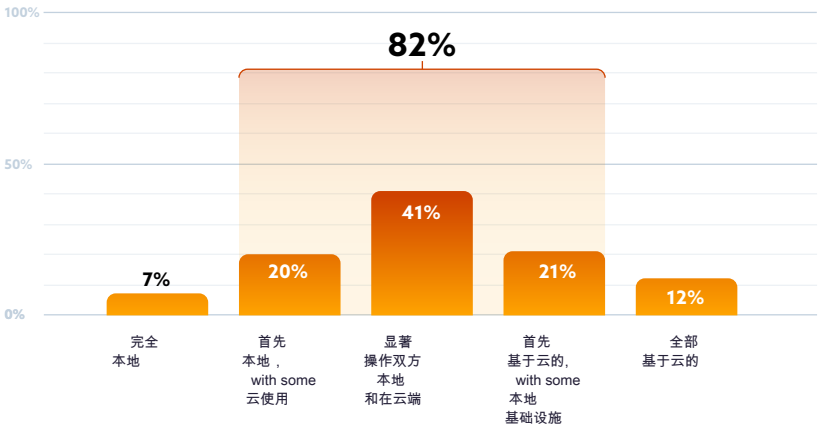
63% 有组织报告使用超过一个云服务提供商，多云用户平均操作2到3个云环境



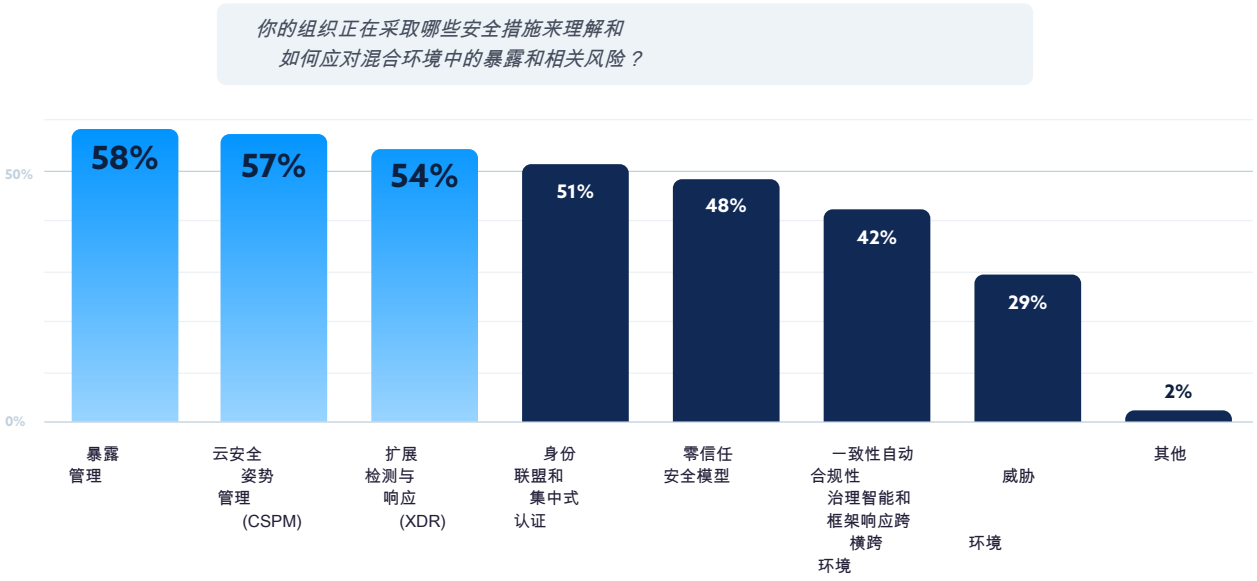
完全在本地，组织有目的地选择环境的混合，以满足其运营、财务和监管需求。这些模式提供了运行的灵活性工作负载在它们最有意义的地方——无论是云中、跨多个提供商，或仍然在本地。

63%的机构报告使用多个云服务提供商，多云用户平均运营2到3（2.7）个云环境。同时，**82%的机构维持某种混合基础设施**，或者平均分配给本地和云端，或者更侧重于一种环境。

哪项最能描述贵组织的IT/云基础设施？



为保障这一碎片化的基础设施，组织正转向使用专为跨越云和本地环境而设计的工具。 **统一安全监控和风险优先级（58%）**， **云安全态势管理（CSPM）（57%）** ，和 **扩展检测与响应 (XDR) (54%)** 在混合环境中，它们是最常用的控制方式。这表明正在从独立的或供应商原生工具向更广泛的可见性和控制机制转变，这些机制能够与混合基础设施的复杂性保持同步。



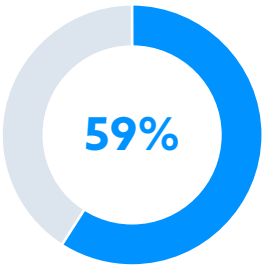
转向混合云和多云很可能是由成本优化、监管要求和性能需求相结合驱动的。在某些情况下，组织甚至将工作负载迁回本地以更好地 管理费用或获得更多直接控制 ，如一文中所述 之前的云安全联盟（CSA）调查报告 不论动机如何，该模型都要求具备安全策略，能够在非同质的场景中提供一致的策略执行、身份管理和风险监控能力。

关键发现2：

身份已成为云最薄弱（以及组织最关注的）链接

与身份相关的问题现已成为云安全问题之首——在感知、安全漏洞影响和战略关注方面，其风险已超过长期存在的配置错误、内部威胁和工作负载漏洞。尽管这标志着意识的显著进步，但在将身份视为关键威胁的理解与为有效保护它所采取的措施之间，仍存在一个关键差距。治理、衡量和运营协调均落后于报告的意图。

组织云基础设施的首要安全风险

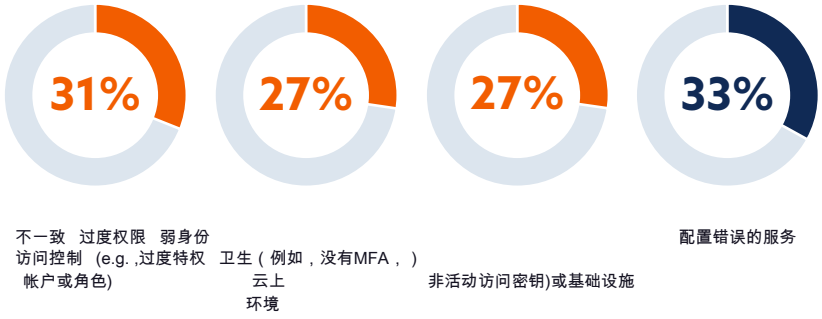


不安全的身份标识和风险权限

五十九%的组织识别出不安全的身份和有风险的权限 作为其云基础设施的首要安全风险。这一担忧在违规数据中得到了证实。在经历云相关违规事件的人中，前四名原因中有三个是

与身份相关： **过度权限（31%）**，**不一致的访问控制 (27%)** ，和 **身份疏于管理（27%）** .

您认为以下哪些因素对您组织的泄露贡献最大？



不一致访问控制

过度权限 (e.g. ,过度特权帐户或角色)

弱身份卫生（例如，没有MFA，）非活动访问密钥)或基础设施

云上环境

配置错误的服务

这些问题相互关联但各不相同。过度的权限—例如拥有管理员访问权限或广泛的角色分配—可能会将轻微的泄露升级为重大安全事件。不同环境之间不一致的访问控制

制造不均匀的保护和攻击者可以利用的盲点。薄弱的身份卫生——定义为识别和修复风险行为（如未轮换的密钥、未使用的凭证或遗弃账户）的流程不佳——会导致长期存在的漏洞，这些漏洞通常在事件发生后才会被发现。

这些模式共同指向了一个分层的系统性问题：不仅仅是几个配置错误的帐户，而是跨团队和系统在身份治理方面存在根本性断裂。这不是单纯的技术失误，而是源于云和身份访问管理（IAM）功能在共享所有权、监督和问责制方面的缺失所带来的运营挑战。

即使组织报告称他们认识到这些风险并将优先考虑零信任，安全成熟度仍然滞后。当被问及主要挑战时， **28%的受访者指出云和IAM团队之间存在脱节** ，和 **21%的人报告在执行最小权限时存在困难** 这表明许多组织知道问题在哪里，但仍然缺乏规模化的结构或工作流程来解决它。

组织云基础设施安全的主要挑战

28%
云安全与IAM团队之间缺乏一致性

21%
强制最小权限的难度

为缩小差距，组织正在优先考虑零信任架构和 **实现**

身份的最小权限是未来12个月最受欢迎的云安全优先事项（44%） 然而测量实践仍处于早期阶段。 **百分之四十二的组织跟踪多因素认证（MFA）或单点登录（SSO）的采用率** —the最常见的iam kpi—but这仅仅显示控制措施是否到位，而不是它们是否有效。很少有组织监控身份风险的更深层次指标，如权限滥用、访问异常或非人类身份滥用。

44%
若组织将身份实施最小权限视为首要任务

42%
哪些组织跟踪多因素认证（MFA）或单点登录（SSO）的采用率

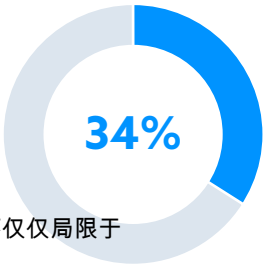
数据描绘了身份认证这一既被广泛认知为威胁，又是一个仍在成熟中的安全管理学科的图景。各组织正朝着正确的方向发展，但具有实质性的进展需要超越政策声明。他们需要重新构建IAM计划及身份提供者等支撑系统，改进与云团队的协调，并从二元采用指标转向更动态的身份风险与韧性指标。

关键发现3：

专长差距导致了领导力协同挑战

缺乏云安全专业知识不仅仅是人员配备或实际实施方面的问题，它是一个战略障碍，影响着组织在各个层面上规划、预算和优先考虑安全的方式。随着安全团队在专业知识有限的情况下努力将云保护投入运营，这个差距开始塑造影响领导层协同、资源分配和组织风险态势的决策。

保障组织云基础设施所面临的主要挑战

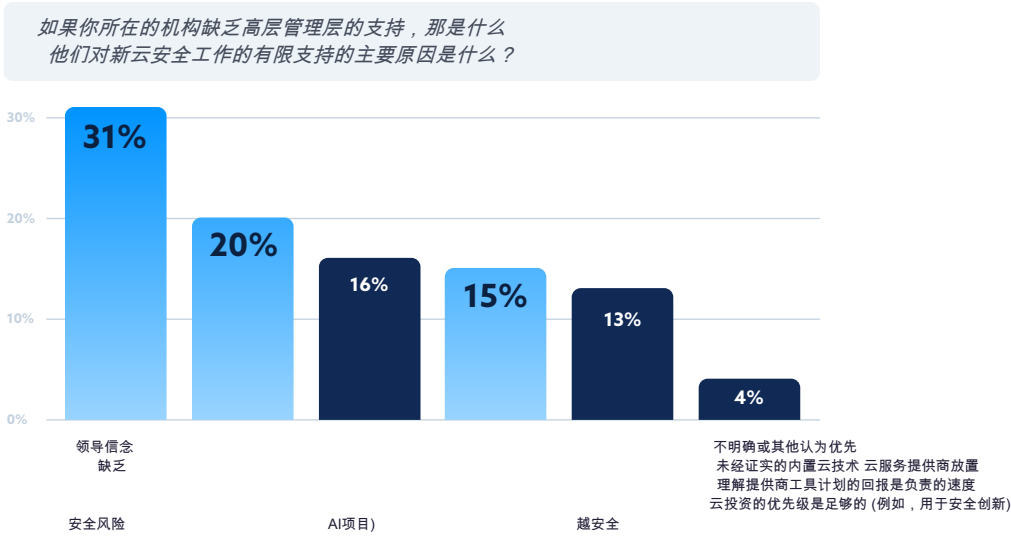


百分之三十四的受访者认为缺乏专业知识
作为保障云基础设施的首要挑战—比任何其他问题都更加严重。但这个差距的影响并不仅仅局限于缺乏专业知识
实际操作层面。它产生一种连锁反应，破坏规划和执行。当被问及实施新的云安全功能所面临的障碍时，受访者指出 **不明确的策略 (39%)**， **预算不足（35%）** ，和 **资源被转移至其他优先事项（31%）** —领导力在设定方向、评估权衡或全面把握所涉风险方面都存在问题的所有症状。

贵组织实施新的云安全功能的前三大障碍是什么？

39% 策略或计划不明确用于云安全	**29%** 与遗留系统集成系统	**17%** 供应商锁定或内部对供应商的忠诚度
35% 预算不足	**26%** 缺乏流程或文档	**16%** 可用的工具和解决方案不满足组织的需求
31% 资源被转移至其他优先事项	**23%** 缺乏支持高级管理层	**11%** 与运维团队的摩擦
30% 专业限制	**20%** 时间限制	**1%** 其他

这种脱节现象进一步体现在领导如何看待云安全上。几乎 **三分之一受访者（31%）表示，他们的高管层对云安全风险的认识不足** 。其他人指出领导认为 **内置云服务提供商工具是“足够好”(20%)** ，或者假设 **云服务提供商主要负责保障环境（15%）** —对…的明显误解



共同责任模型。这些认知表明，许多高管团队仍然在传统安全假设下运作，这使得安全团队难以获得支持，以获取用于保护当今复杂的混合云和多云环境所需的工具、人员配置或时间。

与其将专业知识仅视为招聘或培训问题，组织可以将问题重新定义为一个更广泛的运营挑战——通过内部赋能、外部合作以及减少认知负荷的平台选择来应对这一挑战。同时，也存在一个明确的机遇，即利用这些平台和工具不仅来提升安全态势，而且在这个过程中帮助教育领导层。通过使高管的理解与安全现实保持一致，组织可以摆脱被动、点解决方案的思维模式，转向更具战略性、更整合的安全项目。

与其预防火灾，不如灭火——测量漏洞，而非预防

云安全仍然陷入被动循环。虽然安全漏洞仍然是一个持续且重大的挑战，但组织却根据已经发生的问题来衡量绩效，而不是根据风险被有效降低或预防的程度来衡量。其结果是，形成了一种以危机应对为中心的指标文化，这反而强化了短期的危机反应，而不是长期的韧性。

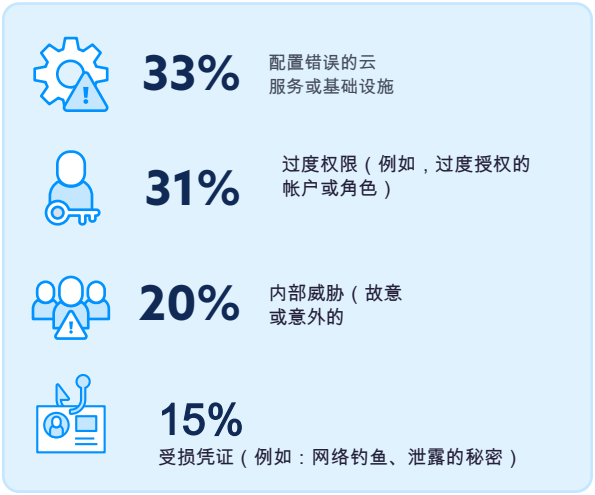
最常见的追踪的云安全kpi是 **安全事件发生频率和严重程度（43%）**，一个只有在事故发生后才相关的指标。在IAM中，最关键的指标是 **mfa/sso采用率（42%）**，它追踪的是基本控制措施是否到位，而不是它们是否有效或被滥用。这些数据共同表明，组织仍然专注于表面层次的指标，而不是更战略性的、具有前瞻性的绩效衡量标准。

这种后视镜心态也体现在违规数据中。过去18个月，各组织报告平均发生了2.17起与云相关的违规事件，然而 **只有8%将其归类为"严重"**。虽然一些事件确实可能是低影响的

平均而言，评价您组织所经历的与云相关的事故的严重程度级别。

差异表明许多人被认为严重程度较低——可能因为他们没有触发强制报告门槛、重大媒体报道或明显的运营影响。

您认为以下哪些因素对您组织的泄露贡献最大？



数据显示，违规频率与事件内部评估之间存在脱节，这增加了衡量和沟通真实安全绩效的难度。当考虑到这些违规事件的根本原因时，这种脱节就更加令人担忧，因为其中许多是可以预防的。 **33%的人引用了配置错误的云服务**，而 **31%的人指出权限过度**， **20%到内部威胁**，和 **15%到已受损的凭证**——可以通过更强的配置管理、访问治理和主动检测来减轻的问题。

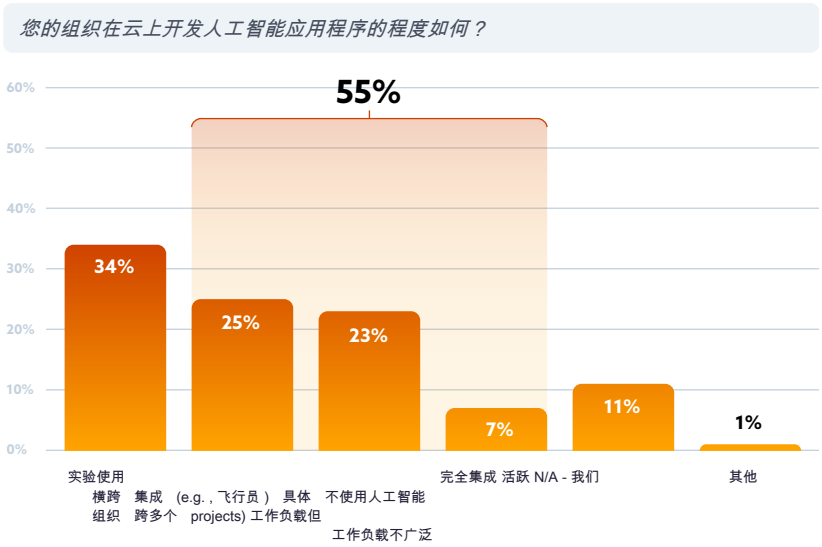
所有这一切都指向一个危险的测量盲点。突破率仍然很高，但很少事件被归类为严重，而且大多数组织追踪的kpi仍然根植于反应而非预防。测量仍然与事后响应而非前瞻性风险降低相关联。

这种方法在两个关键方面都失败了：它没有向领导层展示主动投资的价值，并且通过假设事件总是可见、可报告且被正确分类，它掩盖了风险的全貌。在检测能力有限的环境下——或者是在绩效由“严重”事件的缺失来评判的环境下——关键事件可能会被忽略或最小化。打破这种循环需要的不只是新的衡量标准或工具，它需要重新定义成功，这种定义应以风险降低为中心，而非以损害控制为中心。

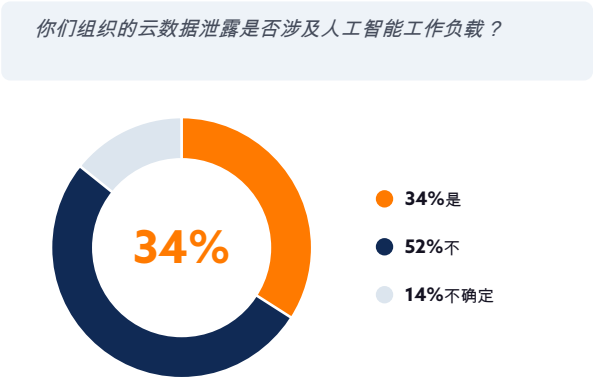
关键发现5：

人工智能应用加速，但安全目标针对错误风险

人工智能的采用速度超过了许多安全团队的准备情况。尽管34%的组织将他们的AI使用描述为“实验性”，但更多的人已经超越了那个阶段。 **55%的人正在使用AI满足主动业务需求** —25%针对特定工作负荷，23%正在跨多个系统积极集成，7%在整个组织中完全集成。这些不是理论试点；它们代表实际操作

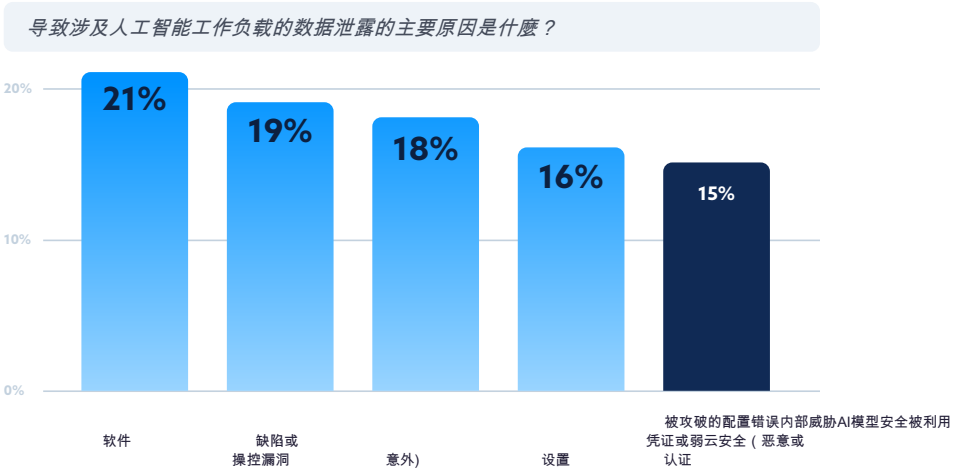


具有实际业务影响力的部署。然而，随着人工智能进入生产阶段，安全工作并非总能同步跟进。其结果： **超过三分之一的拥有人工智能工作负载的组织（34%）已经经历过与人工智能相关的安全漏洞** 引发关于人工智能安全准备和风险管理方面的紧迫问题。

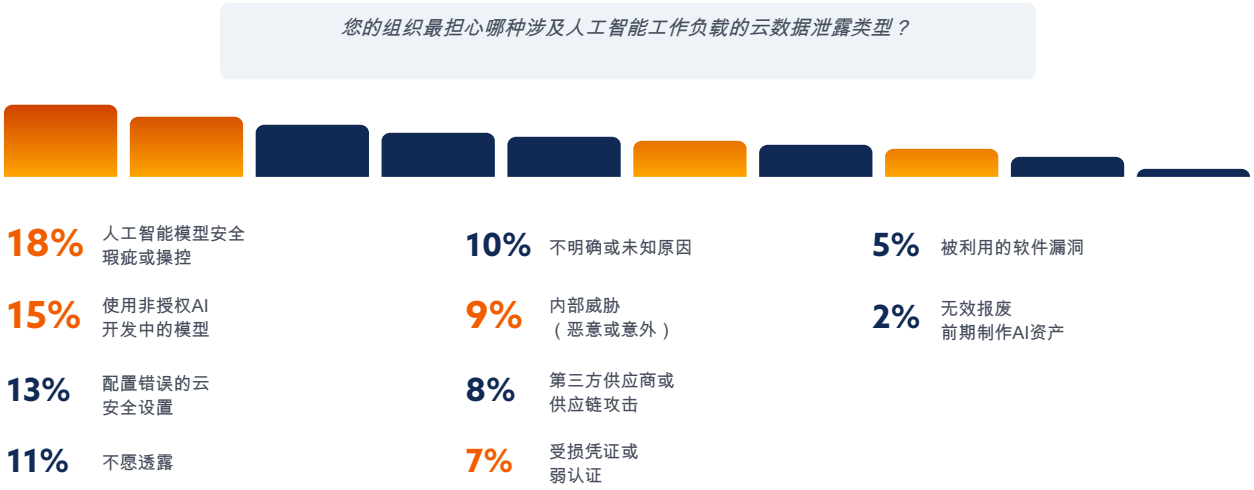


人工智能相关安全事件的频发表明存在一个更深层次的问题：尽管人工智能正在被投入使用，但安全实践尚未完全跟上。

组织正迅速部署人工智能，但他们对风险所在以及如何减轻风险的理解仍显得不成熟。当比较实际导致漏洞的原因与安全团队最关心的问题时，这种脱节就更加明显。与人工智能相关的漏洞最常见的原因包括熟悉的威胁： **被利用软件**

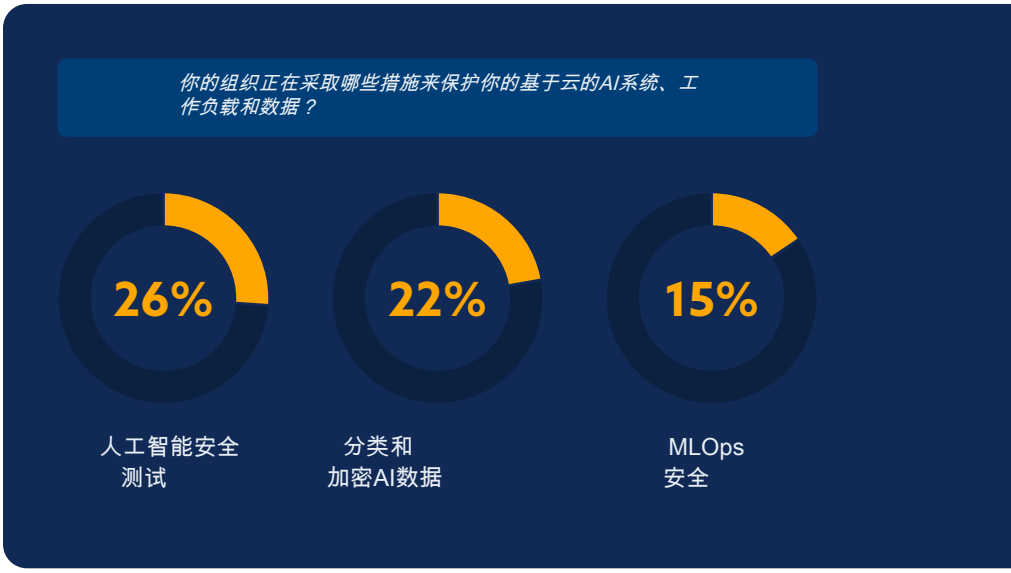


漏洞 (21%)， **人工智能模型缺陷（19%）**， **内部威胁（18%）**，和 **配置错误的云设置（16%）** 然而，当被问及他们最担心哪些漏洞类型时，组织们倾向于不熟悉或“人工智能原生”的风险——例如 **模型操作（18%）** 和 **未经授权使用人工智能模型（15%）** —而 **对内部威胁的担忧（9%）** 而受损凭证（7%）则排名很低。这种失调表明，许多安全程序仍然将人工智能视为根本上是新颖的，而不是将这些新系统应用成熟的云和身份安全原则。



安全控制进一步说明了这种不平衡。超过 **一半的组织（51%）依赖合规框架** 像 NIST AI RMF 或欧盟 AI 法那样，以指导其人工智能安全工作。监管协调至关重要，并提供了必要的基石，但仅靠框架无法保持与人工智能应用的速度和复杂性的同步。

一个强大的安全计划应当主动应对组织的特定风险概况。然而，核心技术防护措施的低采用率表明许多组织止步于合规。只 **26% 进行人工智能专项安全测试** 例如红队演练，只是 **22% 对AI数据进行分类和加密** ，和仅 **15%已实施MLOps安全实践** 这种合规性重但技术上浅薄的态度可能会使人工智能工作负载暴露。



缺乏更深层次的技术投入和风险导向策略，组织有可能会忽视其他领域已经存在的根本性安全实践，例如身份治理、工作负载硬化以及数据保护。而这也仅仅涵盖了合法使用的情况。
随着影子人工智能的兴起 ，未经监管的AI领域部分可能带来更大的风险。

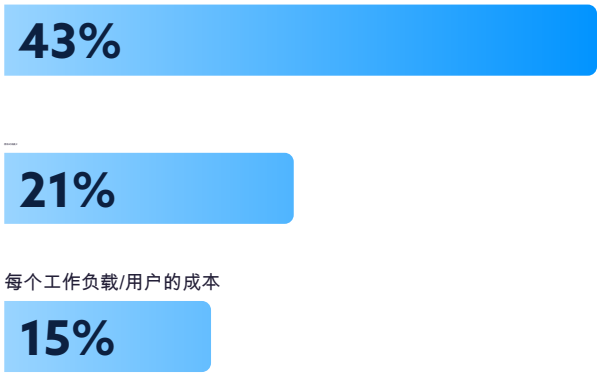
关键发现6：

重置安全策略时间

许多安全团队都知道该做什么，但他们的领导层仍在根据过时的假设运营。随着云和人工智能部署在混合和多云环境中扩展，安全复杂性正在增加。然而，在高管层面，关于责任和风险的误解正在阻碍进展，并阻止组织有效扩展其安全策略。

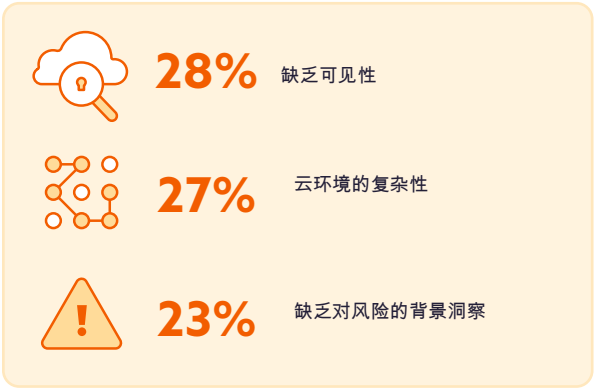
如前所述，许多高管仍然高估了云服务提供商或内置工具提供的安全覆盖范围，这种误解塑造了成功衡量的方式。尽管云服务提供商持续增强其原生安全产品，但这些通常仅限于其自身平台，并未延伸至多云或混合场景，导致可见性和控制方面的空白。大多数组织仍然依赖如 **事件发生频率和严重程度 (43%)** ，而很少关注更主动的指标，如
停机时间减少（21%） 或 **每个工作负载的安全成本（15%）**。加剧这一挑战的是，仍然相对较少的解决方案能够跨领域整合可视性和风险评估

如何展示您在云安全技术投资上的KPI？



混合环境，这使得团队更难全面衡量和管理风险。结果是一个持续的战略性盲点。在没有清晰的理解或有意义的绩效指标的情况下，安全团队缺乏优先考虑长期成熟的方向和资源。

组织云基础设施安全的主要挑战



影响是显著的。组织拥有复杂的环境——82%的组织采用混合环境，63%拥有多云环境——并且它们在应对这些环境时面临挑战。前面讨论过的一些主要挑战之外，还包括 **缺乏可见性（28%）**，**云环境的复杂度（27%）**，和 **缺乏对风险的背景洞察 (23%)** 所有这些都需要用来理解和确定风险的优先级。但是，他们并没有投资于基础工作，比如统一可见性或简化他们的工具环境，只有20%的人优先考虑统一风险评估，只有13%的人专注于工具整合。

这使得负责零散解决方案的安全团队缺乏结构性支持，无法全面降低风险或有效扩展其工作力度。

要打破这种循环，组织需要的不仅仅是技术修复，而是战略重置。领导层必须超越认为安全是“内置”的假设，转而投资于能够提供集成可见性、降低复杂性和实现前瞻性风险管理平台和流程。随着人工智能的采用加速，引入新的风险，这需要基础安全成熟度以及应对新兴威胁的敏捷性，这种转变尤为重要。在重置发生之前，即使是最能干的安全团队也将仍然陷入被动操作，缺乏扩展、适应和成熟所需的战略一致性。

结论

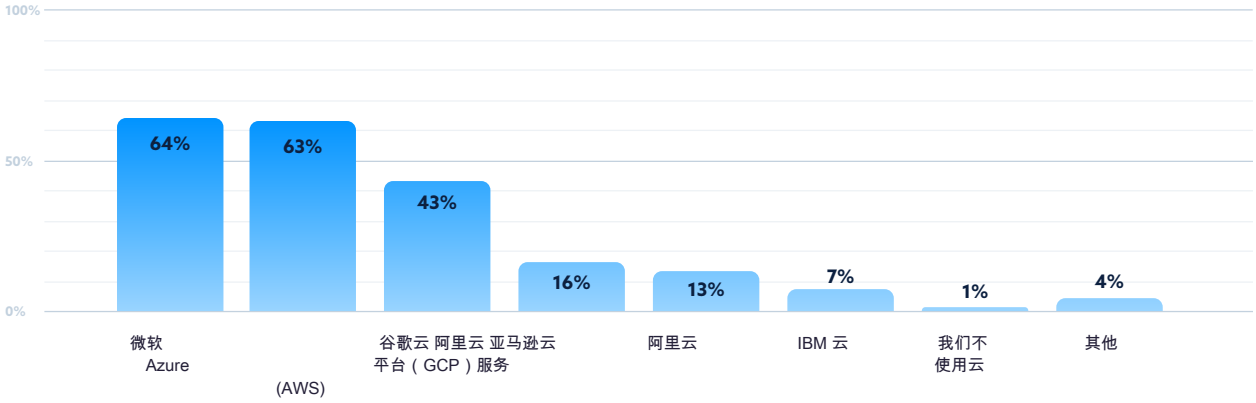
大多数组织已经运行在混合和多云环境中，超过一半的组织正在使用人工智能处理业务关键型工作负载。虽然基础设施和创新正在快速发展，但安全战略并未与时俱进。总体而言，组织正面临着安全工具碎片化、身份治理不成熟以及衡量实践被动而非主动等问题。为了强化云和人工智能安全项目，组织必须从被动应对转向主动的、基于风险评估的策略。这意味着：

• 优先确保混合云和多云环境下的统一可视性和一致策略执行 • 投资于身份治理，包括最低权限和非人类身份的管控 • 扩展KPI以反映预防和韧性，而不仅仅是事件响应 • 使领导层理解与运营现实相符，以支持更智能的规划和资源分配 • 超越AI安全合规性的上限，将其作为更深层技术保障的起点

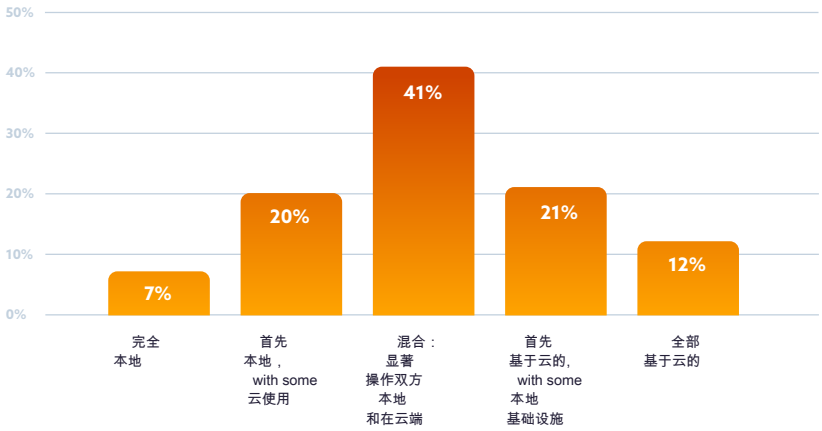
安全成熟度不能仅靠工具实现——它需要跨团队、领导力和战略的协调努力。成功的企业将是那些在事件发生前建立结构来理解、优先处理和降低风险的组织。

完整调查结果
云基础设施

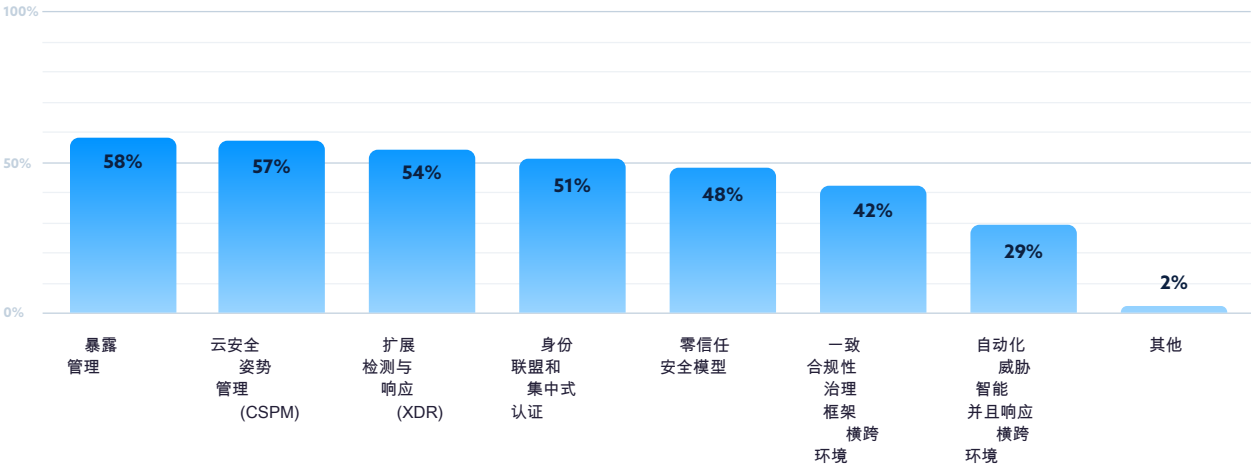
以下哪个云服务提供商您的组织使用？



哪项最能描述贵组织的IT/云基础设施？



你的组织正在采取哪些安全措施来理解和
如何应对混合环境中的暴露和相关风险？



你的组织正在使用哪些安全措施来理解
并且在您的云环境中对暴露和相关风险采取行动吗？

63% API安全

59% 合规与治理云环境框架

58% 云安全态势管理（CPSM）

57% 零信任安全模型

53% 身份联邦和集中式认证

42% 扩展检测and 响应 (XDR)

41% 基础设施即代码 (IaC)安全扫描

34% 自动化威胁情报和回复

27% 统一云风险监控和优先级

19% 云基础设施授权管理（CIEM）

6% 其他

风险、挑战和障碍

您认为3个最大的安全风险是什么
你们组织的云基础设施吗？

59%	不安全的人类/服务身份和风险权限	22%	公开暴露云资源	15%	网络配置错误
47%	云配置错误	21%	工作负载漏洞或运行时威胁	11%	不符合标准
31%	第三方风险/供应链攻击	20%	不安全的 API 或其他接口	11%	文档缺失或流程
31%	人为错误	19%	勒索软件攻击	1%	其他

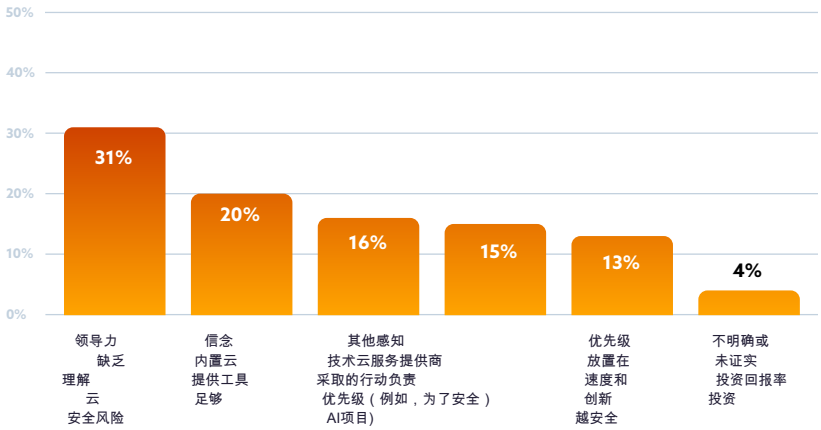
securing
贵组织的云基础设施？

34%	缺乏专业知识	23%	时间限制	16%	与 DevOps 的摩擦
28%	云之间缺乏一致性安全和IAM团队	22%	文档缺失和进程	12%	缺少粒度控制
28%	缺乏可见性	21%	执行困难最小权限	7%	缺少临时访问权限(准时制)控制
27%	云环境的复杂性	19%	自动化不足或合适的工具	2%	其他
23%	缺乏对风险的背景洞察	17%	身份认同困难生命周期管理		

实施新事物的前3个障碍是什么
您的组织云计算安全能力？

39%	不明确的策略或计划云安全	29%	与遗留系统集成系统	17%	供应商锁定或内部对供应商的忠诚度
35%	预算不足	26%	缺乏流程或文档	16%	可用的工具和解决方案不满足组织的需求
31%	资源被转移至其他优先事项	23%	缺乏支持高级管理层	11%	与运维团队的摩擦
30%	专业限制	20%	时间限制	1%	其他

如果你所在的机构缺乏高层管理层的支持，那是什么
他们对新云安全工作的有限支持的主要原因是什么？



优先级和KPI

你最重要的3种云基础设施是什么
未来12个月的安保优先事项？

44% 实施零信任和最小权限身份

36% 检测和修复云配置错误

26% 保持合规（例如，NIST、SOC2、ISO、PCI-DSS、CIS）

24% 实现临时提升权限jit用于devops和其他（即取消站立特权）

21% 评估并缓解攻击面云基础设施

20% 统一风险评估混合环境即云、本地、OT

20% 实现云检测和响应 (CDR)

17% 预算优化

17% 管理工作负载漏洞

15% 提高韧性并灾难恢复

15% 数据分析与人工智能安全集成

15% 实现基础设施-as-Code（IaC）扫描

13% 工具整合

2% 应对量子威胁

你如何展示你的KPI
云安全技术投资？

43% 安全事件频率和严重程度

36% 修复平均时间 (MTTR)

33% 合规与审计得分

32% 检测平均时间 (MTTD)

25% 识别平均时间 (MTTI)

21% 停机时间减少

18% 误报率

17% 平均遏制时间 (MTTC)

17% 恢复平均时间正态性 (MTTRN)

15% 单位安全成本workload\\user

14% 变现周期 (TTV)

14% 关于该技术的性能

6% 我们不测量我们的性能技术投资

1% 其他

你如何展示你的KPI
IAM安全技术投资？

42% 多因素身份验证 (MFA)/单点登录（SSO）采用率

28% 安全事件频率和严重程度

24% 合规与审计得分

22% 检测平均时间 (MTTD)

22% 识别平均时间 (MTTI)

21% 平均修复时间修复（MTTR）

21% 访问异常频率

16% 特权的频率访问滥用

16% 每个工作负载/用户的成本安全

14% 误报率

13% 平均遏制时间 (MTTC)

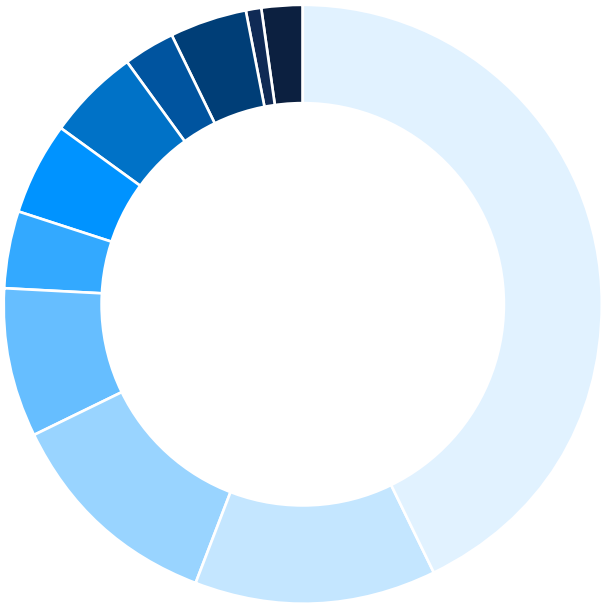
13% 变现周期 (TTV)

12% 恢复平均时间正态性 (MTTRN)

9% 关于轶事报道的该技术的性能

9% 我们不以我们技术的性能投资

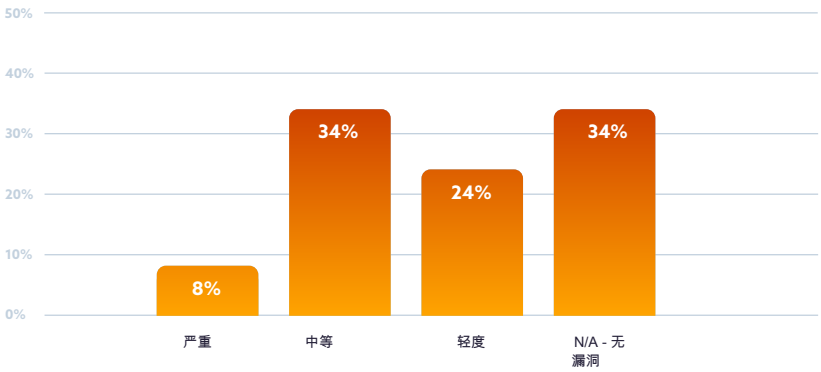
云渗透



您有多少与云相关的泄露事件过去18个月组织有哪些经验？

42%	0	5%	6
13%	1	3%	7
12%	2	4%	8
8%	3	1%	9
4%	4	2%	10
5%	5		

平均而言，评价您组织所经历的与云相关的事故的严重程度级别。

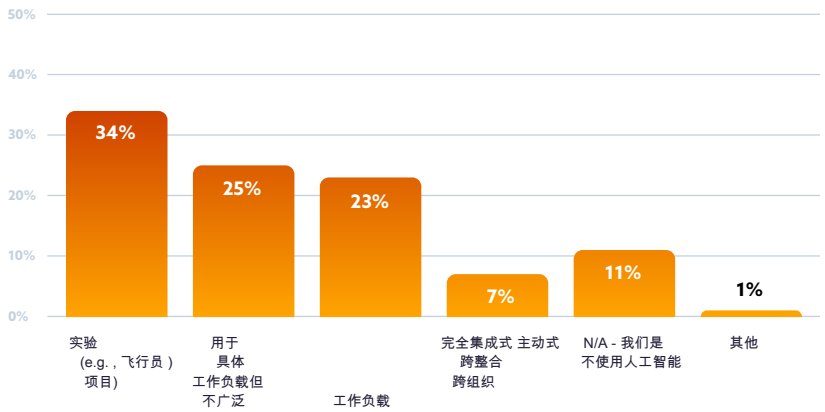


你认为以下哪些因素 contributes
对您组织最大的漏洞是什么？

33%	配置错误的云服务 或基础设施	**20%**	内部威胁 （故意或意外）	**15%**	受损凭证 （例如，网络钓鱼，泄露的秘密）
31%	过度权限（例如，过度授权的帐户或角色 ）	**20%**	不安全的API或 其他接口	**15%**	专业知识不足或 人员不足
27%	跨区域访问控制不一致 云端环境	**18%**	第三方/供应商妥协	**9%**	被利用的漏洞
27%	身份管理薄弱（例如，未启用MFA） 非活动访问密钥)	**17%**	意外公开 (例如打开 S3 存储桶，) 配置错误的数据库)	**25%**	N/A - 无违规

AI安全

您的组织在云上开发人工智能应用程序的程度如何？

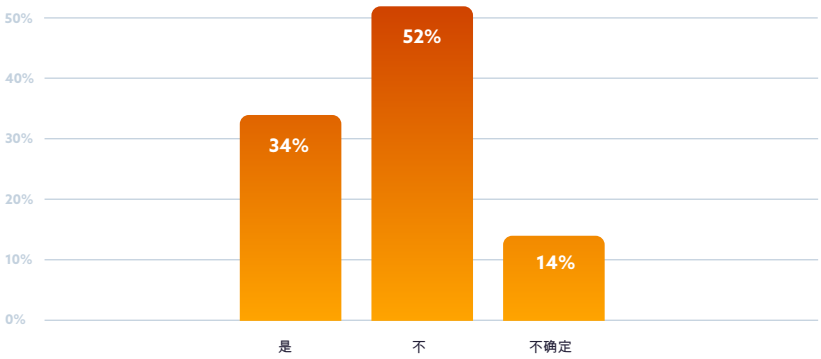


你的组织正在采取什么措施来保护
您的基于云的 AI 系统、工作负载和数据？

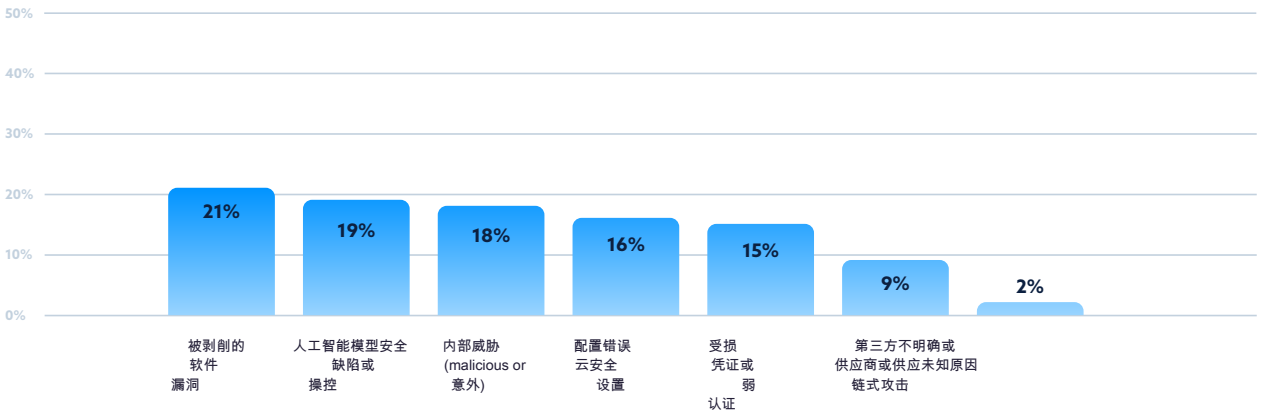
51%	执行 AI/云合规性 安全框架	**30%**	零信任与网络 AI工作负载分割	**22%**	分类和加密 AI数据
46%	采用行业最佳实践	**30%**	威胁检测和事件 人工智能相关活动的响应	**15%**	MLOps安全
35%	定期对AI模型进行安全审计 集成保护	**26%**	人工智能安全测试	**5%**	以上都不适用
34%	人工智能特有身份和访问控制	**23%**	人工智能供应链安全	**1%**	其他

人工智能入侵

是否有云数据泄露你的
该组织经历过涉及人工智能工作负载吗？



导致涉及人工智能工作负载的数据泄露的主要原因是什麼？



涉及人工智能工作负载的云数据泄露类型
你的组织最关心的是什么？

18% 人工智能模型安全瑕疵或操控

15% 使用非授权AI开发中的模型

13% 配置错误的云安全设置

11% 不愿透露

10% 不明确或未知原因

9% 内部威胁（恶意或意外）

8% 第三方供应商或供应链攻击

7% 受损凭证或弱认证

5% 被利用的软件漏洞

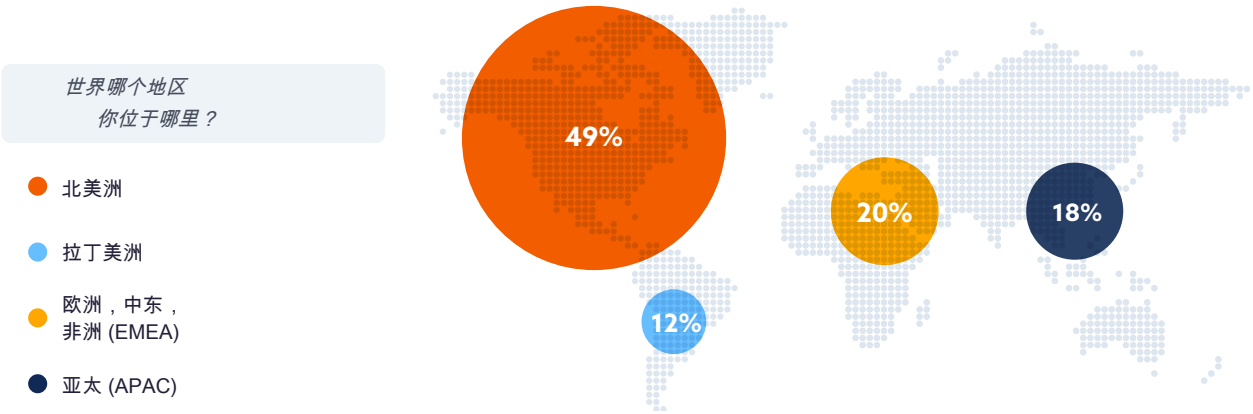
2% 无效报废前期制作AI资产

3% 其他

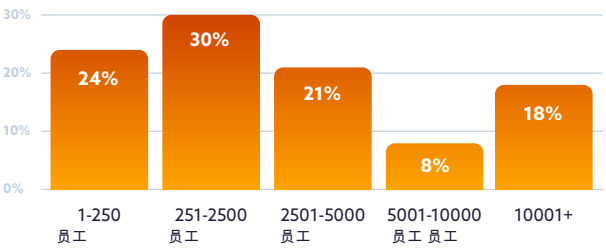
人口统计

这项全球调查从不同组织、行业、规模和地理区域的1025名IT和安全专业人员中收集了见解。人口统计细分提供了理解调查结果的重要背景，突出了不同部门和运营规模的组织所面临的多样化和挑战。

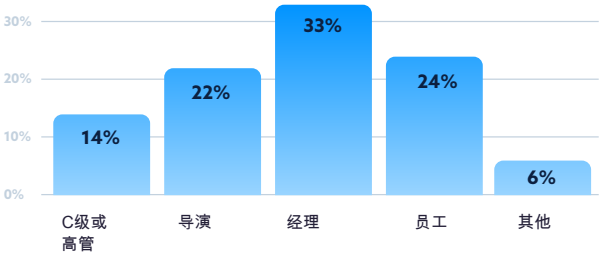
世界哪个地区
你位于哪里？



组织规模



哪个最好地描述了你的工作级别？



以下哪项最能描述您组织的主要产业？

23% 电信，科技，互联网 & 电子
17% 金融与金融服务
7% 教育
6% 政府
5% 商务支持与物流
5% 制造
4% 医疗保健与制药
3% 建筑，机械，和家
3% 保险
3% 汽车
2% 航空公司与航天航空（包括国防）
2% 公用事业、能源和开采
2% 广告与营销
2% 娱乐与休闲
2% 食品和饮料
2% 非营利
2% 零售与非耐用品
2% 运输与配送
1% 农业
1% 健康与健身
1% 房地产
4% 不愿回答

调查方法学及创建

云安全联盟 (CSA) 是一个非营利性组织，其使命是广泛推广最佳实践，并确保云计算和IT技术中的网络安全。CSA 还教育这些行业内的各种利益相关者关于所有其他形式计算中的安全问题。CSA 的成员包括来自行业实践者、企业和专业协会的广泛联盟。CSA 的一个主要目标是进行评估信息安全趋势的调查。这些调查提供有关组织当前成熟度、意见、兴趣和关于信息安全与技术的意图的信息。

Tenable委托CSA开发一项调查和报告，以便更好地了解该行业对云和AI安全趋势的知识、态度和观点。Tenable资助了该项目，并与CSA研究分析师共同开发了问卷。该调查由CSA于2025年5月在网络上进行，收到了来自不同规模和地点的组织的信息技术和安全专业人士的1025份回应。CSA研究分析师对该报告的数据分析和解释进行了处理。

研究目的

这项调查旨在更好地了解安全团队如何应对这种复杂性——涵盖从身份和基础设施保护到领导层协同以及人工智能在云工作负载中日益显现的作用等各个方面。其目标是揭示组织如何在快速变化的威胁环境中调整其战略、确定风险优先级以及衡量进展。

核心目标：

• 了解组织如何应对云、多云和混合环境中的不断演变的网络安全挑战 • 探索基础设施、工作负载、身份和数据在云原生和混合设置中的安全情况 • 识别塑造现代云安全战略的前十大风险、障碍和优先事项 • 检查组织如何跟踪并向业务领导层传达与云相关的安全KPI • 评估云中AI的采用情况以及AI系统、工作负载和数据的安全情况