研究报告



智能体 AI 对网络运营的影响

思科与 Omdia 2026 年联合研究报告

© 2026 思科和/或其附属公司。版权所有。

目录

01 执行摘要

02 增员已无法解决 IT 困境

03 网络盲区比想象中更为普遍

04 自主化运营已成共识

05 确保智能体 AI 值得信赖的必要条件

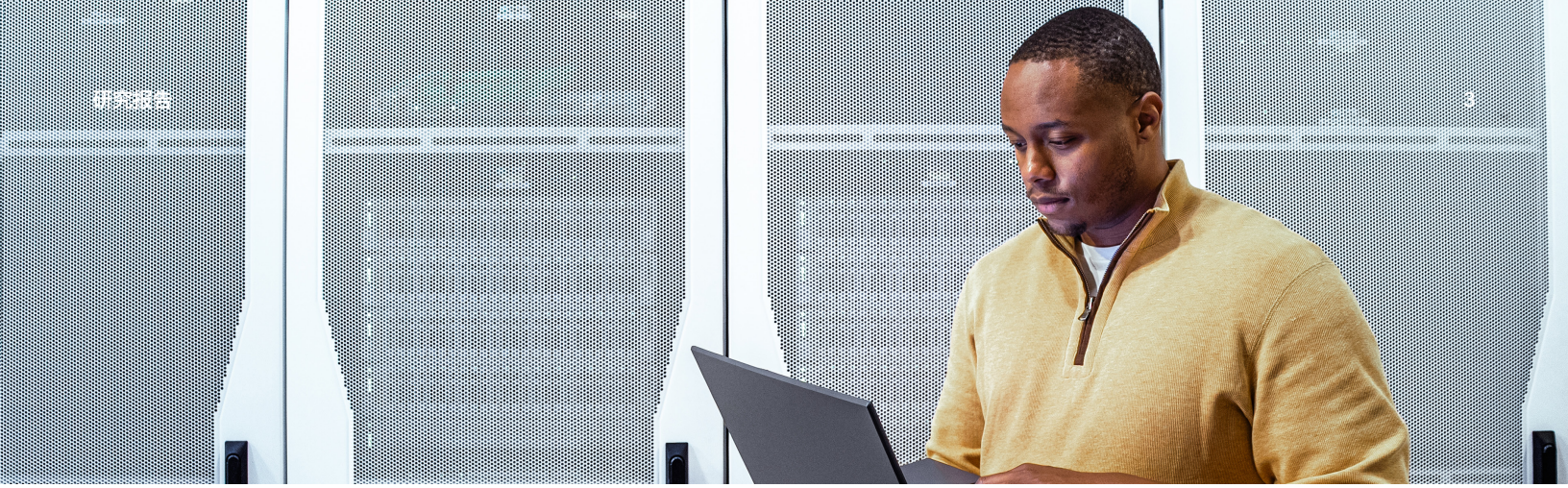
06 企业内部的认知差距可能拖慢转型进程

07 初步成效已得到验证

08 未来 12 个月将成为决定成败的关键时期

09 关于本研究

© 2026 思科和/或其附属公司。版权所有。



01 执行摘要

关于是否应借助 AI 来管理网络的争论如今基本有了定论。

谈及智能体 AI 在网络运营中的应用，讨论几乎总会回到相同的问题：智能体 AI 是否值得信赖？企业是否真的愿意交出控制权？Omdia 开展的独立研究以及思科牵头开展的汇总网络遥测数据分析表明，如今再提这些问题，或许已经不合时宜。

本研究对 1,000 名 IT 和网络运营负责人展开调查，结果显示，企业正在有条不紊地在网络运营中应用 AI。四分之三的企业已将 AI 应用于网络运营。半数企业目前已在生产环境中运行既能提供建议又能自主执行操作的智能体 AI 系统。84% 的企业预计将于未来 12 个月内实现 AI 主导的运营模式，推动网络运营从传统 AIOps 转向智能体驱动的运营，即 AgenticOps。

在已使用 AI 的企业中

75%
已将 AI 应用于网络运营

51%
目前已在生产环境中运行既能提供建议又能自主执行操作的智能体 AI

84%
预计将于未来 12 个月内实现 AI 主导的运营模式

来源： Omdia

© 2026 思科和/或其附属公司。版权所有。

这并非企业一味追逐愿景、脱离实际的表现，而是应对网络运营结构性难题的理性选择。现代网络的规模和复杂性不断提升，已超出人类运营能力的极限。告警数量持续增加，变更频率不断加快，跨域协同愈发复杂，这些挑战已无法单靠增员来解决。企业经过权衡后逐渐认识到，自主化运营并非需要设法管控的风险，而是需通过技术手段加以实现的必然之举。

本研究的主要发现：

- **增员已无法解决 IT 困境。**网络需求空前高涨，但 95% 的受访者表示，以 AIOps 为代表的现有非智能体工具至少在某一方面已难以满足实际需求。对于尚未采用 AgenticOps 的企业而言，仅靠人工清理积压的网络告警，需要约 100 名专业人员。
- **网络盲区比想象中更为普遍。**92% 的受访者表示，网络问题通常涉及多个领域，而各团队往往需要借助十种或更多不同工具才能掌握网络状况。工具各自为政、信息彼此割裂，已成为制约网络运营的结构性障碍。
- **自主化运营已成共识。**面对增员也难以应对的工作量，以及无法单靠人工完成关联分析的碎片化信息，51% 的企业已在生产环境中运行智能体 AI，84% 的企业则预计将于未来 12 个月内实现完全由 AI 主导的运营模式。
- **确保智能体 AI 值得信赖的必要条件十分明确。**企业并未降低对自动化的期待，而是希望确保智能体驱动的自动化值得信赖。透明度是不可妥协的要求，69% 的受访者要求能够详细追溯智能体 AI 各项操作的原因及其依据。86% 的受访者认为，与其再添单点工具，不如采用统一集成平台，这才是最有效的解决之道。
- **最大的障碍可能不在技术，而在于企业的准备程度。**意识到向 AgenticOps 转变这一趋势的网络运营 (NetOps) 一线人员比例几乎是业务部门高管的两倍。这种上下之间的认知差距可能会拖慢 AI 的采用进程，延缓运营转型的步伐。
- **AI 应用领先者的优势正在显现。**与 NetOps 领域 AI 采用成熟度较低的企业相比，AI 采用成熟度最高的企业人均工作效率高出近 30%，实现端到端全面可视性的比例更是前者的 3.2 倍。这表明，AI 采用成熟度不仅仅是提升运营效率的手段，还正逐渐成为企业的竞争优势。

© 2026 思科和/或其附属公司。版权所有。



02 运营承载能力

增员已无法解决 IT 困境

20 年来，面对日益复杂的运营工作，企业的应对之道无外乎增添人员、增加工具、增设流程。然而，基于 AIOps 的运营已无法满足需求，这一模式也走到了尽头。

仅靠人工处理告警已不再现实。

如今，企业平均每天产生约 4,100 条监控告警和事件，其中略过半数 (51%) 与网络相关。一名普通一线人员每天只能完成约 21 条网络告警的审核、调查和处理。要手动清理每日积压的网络告警，需要约 100 名专业人员。然而，绝大多数网络运营团队的人员规模都远低于这一数字。

告警处理的现实挑战

4,100 条	51%	21 条	约 100 名
企业平均每天产生的告警和事件数量	**与网络相关（每天约 2,100 条）**	**一名一线人员每天可处理的告警数量**	**手动清理积压的网络告警所需的专业人员数量**

来源： Omdia

© 2026 思科和/或其附属公司。版权所有。

由此产生的后果不难预料，而且会持续造成损耗：

46% 的网络告警未经调查就被关闭，或因人手不足、反复出现的无效告警或误报而被搁置。

45% 的调查时间都耗费在排查误报上，这些工作既无法解决问题，也不产生任何价值。

65% 的负责人表示，“告警疲劳”是员工不满的重要原因；另有 67% 表示，大量告警使团队无暇处理其他重要工作。

来源：Omdia

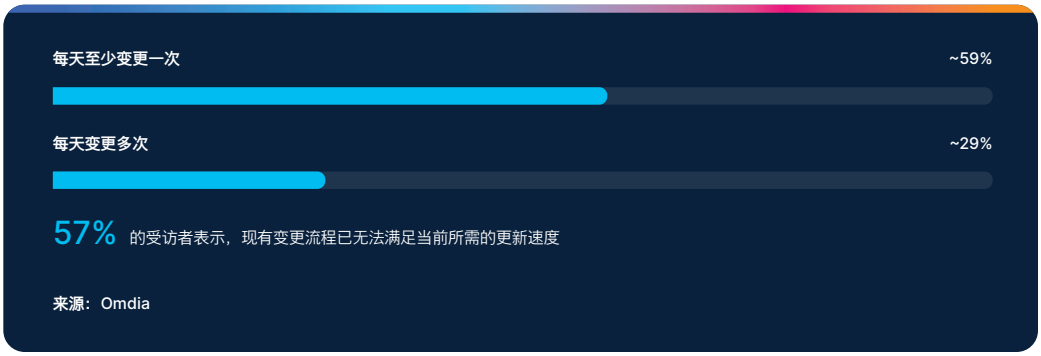
这已不再是单靠加强招聘就能解决的人手问题，而是一种结构性失衡：各类环境产生的信息量远超人类的处理能力。

变更已成常态

目前，近五分之三的企业每天至少会对生产网络环境进行一次变更。其中，约一半的企业每天会进行多次变更，相当一部分甚至每小时就要变更多次。57% 的受访者表示，现有变更流程已无法满足当前所需的更新速度。网络已不再是偶尔调整一次的稳定系统，而是始终处于动态变化之中。运营模式也必须适应这种持续变化的节奏。

生产网络的变更频率

网络变更已不再是偶发事件。对大多数团队而言，变更每天都会发生，甚至每小时都会发生。



© 2026 思科和/或其附属公司。版权所有。

AI 本身也在进一步加剧运营压力。

本研究揭示了一个颇具讽刺意味的现象：原本旨在减轻运营负担的技术，如今却在增加负担。三分之二 (67%) 的受访者表示，生成式 AI 的快速发展显著增加了网络复杂性；另有 70% 的受访者表示，采用 AI 后，NetOps 的工作量不减反增。值得注意的是，95% 的企业表示，以 AIOps 为代表的现有非智能体工具仍存在明显不足，主要体现在过度依赖人工解读和无法提供跨域可视性。

AI 所引发的变化远不止工具和工作量的变化。更重要的是，AI 正在从根本上改变网络流量的使用模式以及各项工作的开展方式。思科对直接流向 AI 的网络流量进行分析后发现，AI 流量的日均规模预计每六个月就会翻一番。这一预测并非凭空推测。同一项分析的数据显示，每个客户端直接流向 AI 的流量增长了 54%。AI 流量之所以加速增长，可能是因为 AI 任务日趋复杂，所需的数据交换量远超简单查询。

更重要的是，现有数据并未完整呈现 AI 流量的真实规模。具体而言，Copilot、Search 等平台内置 AI 产生的流量并未纳入统计。此外，智能体产生的持续性机器间通信流量势必大幅增长，而这部分流量同样未纳入统计。事实上，思科研究发现，AI 智能体堪称网络的“重度用户”，其运行速度取决于软件执行速度，而非人类的操作速度。实测表明，智能体执行任务时，每项任务产生的总流量最多可增加 450%。

AI 流量占网络总流量的比例

每 6 个月

AI 流量翻一番，并持续倍增



来源：思科

至少在现阶段，AI 之所以具有颠覆性，并不在于其规模，而在于其影响不断累积，而且其行为模式与现有网络和运营体系的设计初衷截然不同。

综合来看，传统 AIOps 运营模式正面临多方面的压力：告警数量不断增加；网络变更日益频繁；AI 流量也即将迎来大幅增长。

© 2026 思科和/或其附属公司。版权所有。



03 碎片化

网络盲区比想象中更为普遍

如果说工作量过大是第一个结构性难题，那么碎片化就是第二个。

现代网络故障往往涉及企业不同部门。92% 的企业表示，性能问题通常涉及多个领域，包括云、安全、应用和终端。问题最初出现的位置往往并非根源所在。用户反映的延迟问题，根源可能是云网络配置错误，表现为应用运行缓慢，同时被安全工具标记为异常。

然而，用于诊断此类问题的工具依然各自为政。为了实现对整个网络的端到端可视性，企业平均要使用近十种不同的工具。每种工具都只能反映局部情况，无法单独呈现全貌。因此，相关团队往往难以全面掌握问题情况，只能手动对日志和事件进行关联分析，并将故障转交给其他职能团队处理。

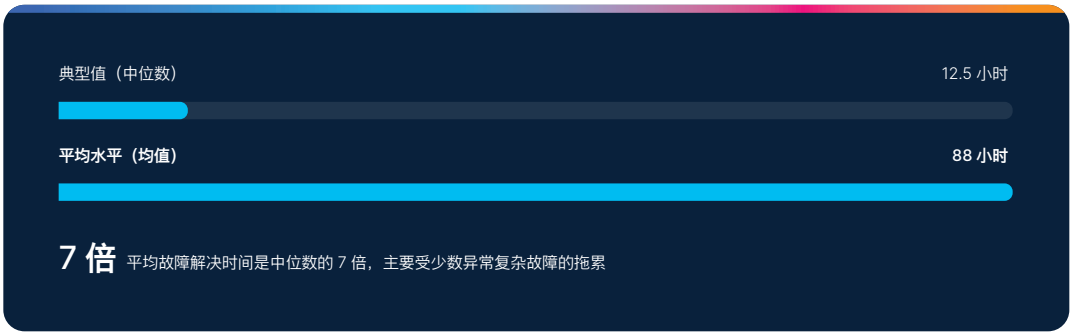
可视性不足与工具碎片化



来源： Omdia

© 2026 思科和/或其附属公司。版权所有。

故障解决时间



46%

的企业表示，故障通常需要一天以上才能解决

十分之一

的企业表示，故障通常需要一周以上才能解决

来源： Omdia

这种碎片化造成的影响在故障解决时间上体现得最为明显。网络故障的平均解决时间为 88 小时，是 12.5 小时中位数的 7 倍。这一差距表明，尽管许多企业能够较为顺利地处理故障，但仍有相当一部分企业经常受困于复杂故障，处理起来动辄耗时数天，甚至数周。近半数受访者 (46%) 表示，故障通常需要一天以上才能解决；十分之一的受访者表示，故障解决时间超过一周。少数异常复杂的故障正成为企业运营工作的主要掣肘。这类影响严重、难以解决的故障如同沉重的锚，一旦发生，就会拖慢运营团队的故障处理速度，致使 NetOps 无法满足业务对速度的要求。

© 2026 思科和/或其附属公司。版权所有。



04 自主化运营

自主化运营已成共识

面对增员也难以应对的工作量，以及无法单靠人工完成关联分析的碎片化信息，企业已形成明确共识：解决之道不在于增加人手或控制面板，而在于采用由智能体驱动的自主化运营模式。

支撑这一结论的证据十分明确：

75% 的企业已将 AI 技术（包括 AIOps、AgenticOps）应用于网络运营。

51% 的企业已在生产环境中运行能够自主执行操作的智能体 AI 系统。

80% 的企业愿意让 AI 承担高度自主乃至完全自主的角色；其中，56% 的企业要求人工审批，24% 的企业则完全不需要人工监督。

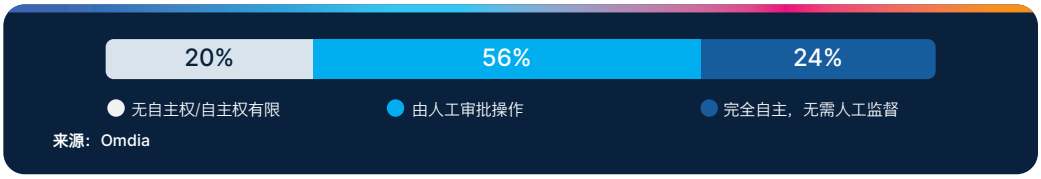
82% 的企业愿意允许 AI 在无需事先获得人工许可的情况下变更生产网络，至少适用于某些类型的操作。

来源：Omdia

© 2026 思科和/或其附属公司。版权所有。

自主化程度的不同层级

深入剖析这 80% 愿意赋予 AI 高度自主乃至完全自主角色的企业：

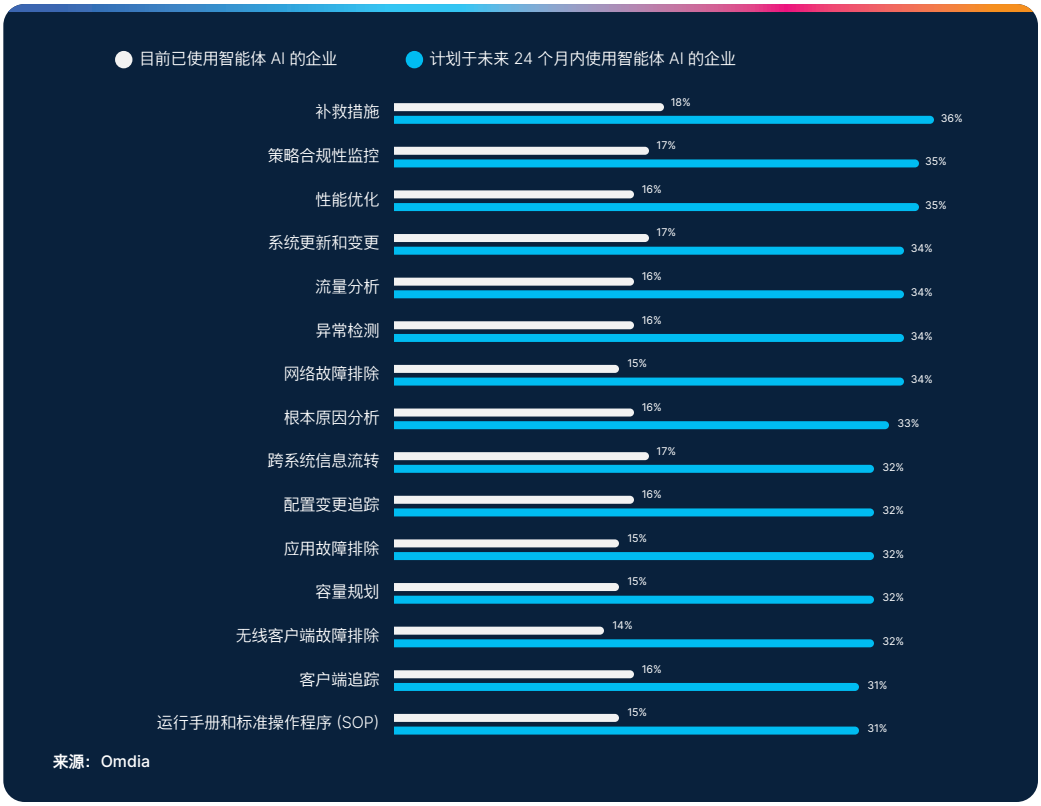


大多数企业 (85%) 认为，未来五年内，大部分运营任务将由 AI 智能体自主管理。事实上，如今已有 80% 的企业愿意让 AI 在 NetOps 中承担高度自主乃至完全自主的角色。82% 的企业愿意允许 AI 在无需事先获得人工许可的情况下变更生产网络，至少适用于某些类型的操作，包括重新路由流量、调整无线网络参数、隔离可疑终端，以及端到端地解决故障。

企业采用智能体 AI 不再是纸上谈兵，而是大势所趋。84% 的企业预计将于未来 12 个月内实现完全由 AI 主导的运营模式，与此同时，智能体在 NetOps 各具体流程中的采用率有望翻一番。

智能体在各 NetOps 流程中的应用趋势

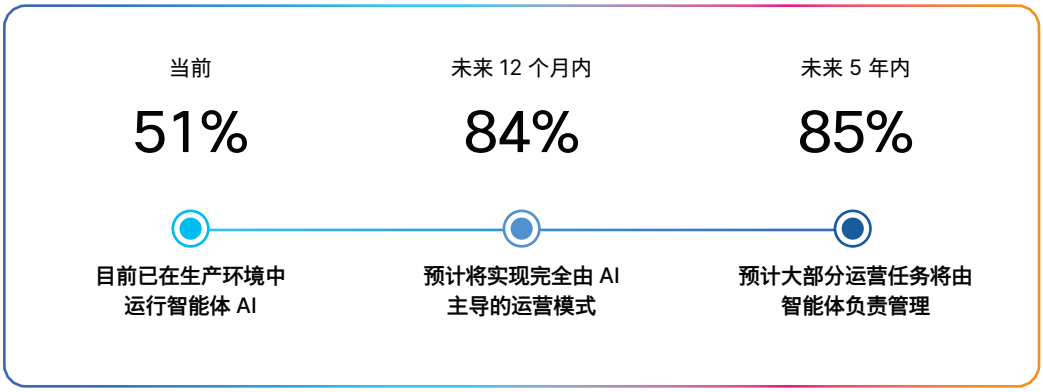
未来 24 个月智能体在各 NetOps 流程中的计划采用情况（各流程的采用率预计都将较目前翻一番）



© 2026 思科和/或其附属公司。版权所有。

采用趋势

本研究分别从三个不同的问题入手，得到的结果却一致指向同一个方向。

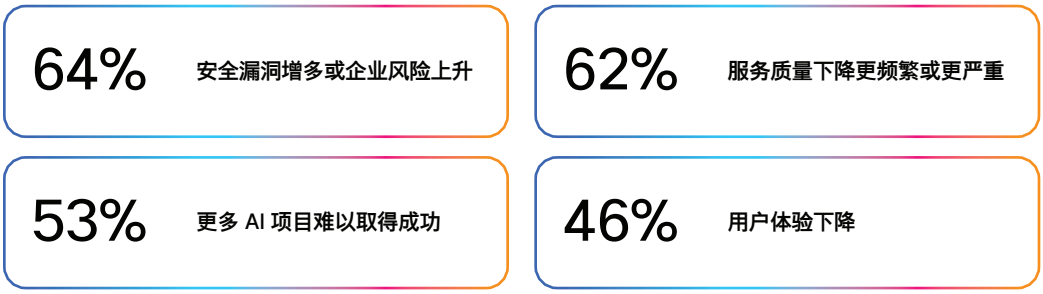


来源： Omdia

企业采用智能体 AI，出发点是解决实际问题，而非追逐某种理念。企业在 NetOps 中采用智能体 AI 的主要驱动因素包括加强安全防护与威胁检测、降低网络复杂性，以及改善最终用户体验。企业采用 AgenticOps，并非出于跟风，而是因为不推进自动化所带来的后果难以接受：64% 的企业担心安全漏洞增多或企业风险上升，62% 预计服务质量下降会更频繁或更严重，53% 预计会有更多 AI 项目无法成功，46% 预计用户体验会下降。

不推进自动化的代价

在负责人看来，维持现状绝非稳妥之策。大多数负责人预计，不推进自动化将在多个方面带来损失。



来源： Omdia

业界已不再争论是否应借助 AI 来管理网络，而是开始探讨如何实现。

© 2026 思科和/或其附属公司。版权所有。



05 信任

确保智能体 AI 值得信赖的必要条件

企业不会盲目地交出控制权。即使是积极采用 AgenticOps 的负责人也清楚地表明，只有满足特定条件，才会赋予 AI 自主权，而各家企业提出的条件惊人地一致。

透明度是不可妥协的要求。

虽然企业对 AgenticOps 的需求十分强烈，但只有清楚了解 AI 的推理过程，并确保这一过程透明可见，才会真正信任它。对于智能体的自主操作，69% 的企业要求其操作过程和决策依据清晰可解释。在受访企业中，选择全面可观测性作为最低要求的比例最高，占 36%。这意味着，企业至少需要能够详细追踪操作全过程、了解决策依据，并在操作完成后进行审计。

这清晰表明，只有让 AI 的操作过程和决策依据足够透明，才能赢得企业的信任。

集成式架构是企业的首选。

缺乏全面了解，信任就无从谈起。由于各类工具彼此割裂，企业难以全面掌握系统的运行情况，也无法消除不同工具之间的信息盲区，进而难以建立对 AI 的信任。企业对此心知肚明。86% 的企业表示，解决之道在于采用涵盖计算、安全、应用和网络的统一集成平台，而不是在现有工具基础之上再添单点工具。

未来方向

86% **的企业表示，最有效的解决之道在于采用涵盖计算、存储、应用和网络的统一集成平台。**

来源： Omdia

© 2026 思科和/或其附属公司。版权所有。

安全护栏需要配套落实，而非择一而用。

在被问及不可或缺的安全护栏时，受访者平均从六项中选出三项，而且各项的选择比例相差不大：

不可或缺的安全护栏

99%

的企业表示，如果缺少这些安全护栏，就不会放心让 AI 自主执行操作。仅有 1% 的企业表示，即使不设置任何安全护栏，也愿意继续采用 AI。

来源： Omdia

六项安全护栏都必须落实，不能有所取舍：

- 要求 AI 清楚说明操作依据
- 操作须经人工审批
- 根据策略限制操作范围
- 支持在紧急情况下强制接管
- 按照角色分配访问权限
- 确保审计记录不可篡改

在企业看来，这些安全护栏不是可供选择的不同方案，而是都必须满足的基本要求。

综合来看，这些研究结果表明，企业关注的已不只是是否信任 AI，更在于如何确保 AI 值得信任。企业并未降低对自动化的期待，而是希望确保自动化值得信赖。企业希望通过统一的界面就能清楚了解并追踪 AI 的运行情况，而不必在十几种工具之间来回切换、拼凑信息。企业希望在赋予智能体自主权的同时，确保其操作有据可查、关键操作经过审批、行为符合既定策略，并且在紧急情况下能够接管、事后能够审计。

© 2026 思科和/或其附属公司。版权所有。



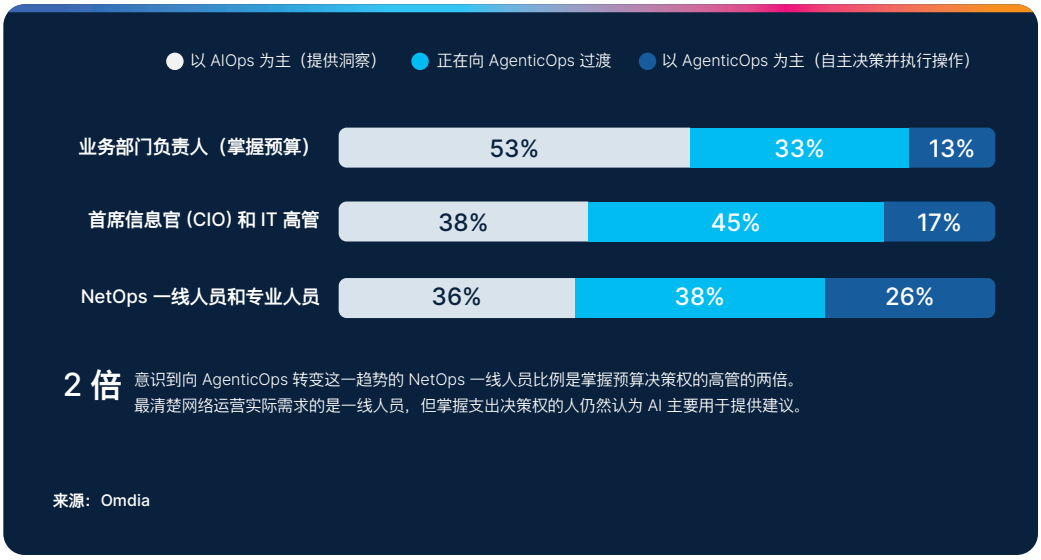
06 准备程度

企业内部的认知差距可能拖慢转型进程

阻碍 AgenticOps 落地的最大难题，可能不在技术，而在企业内部。研究显示，负责日常运营的一线人员与掌握预算的管理者对 AgenticOps 的理解存在明显差距。意识到向 AgenticOps 转变这一趋势的 NetOps 一线人员比例几乎是业务部门高管的两倍。一线人员每天都在承受实际的运营压力，因此更能清楚地认识到这一转变。相比之下，能够影响预算决策的业务部门负责人更倾向于认为 AI 在运营中主要发挥提供洞察和建议的作用（即传统的 AIOps 模式），而没有充分认识到智能体还能够自主执行操作。

不同群体对 AI 在 IT 运营中所扮演角色的看法

越是直接参与日常运营的人越容易认识到，AI 不再只是提供建议，还能自主执行操作。



© 2026 思科和/或其附属公司。版权所有。

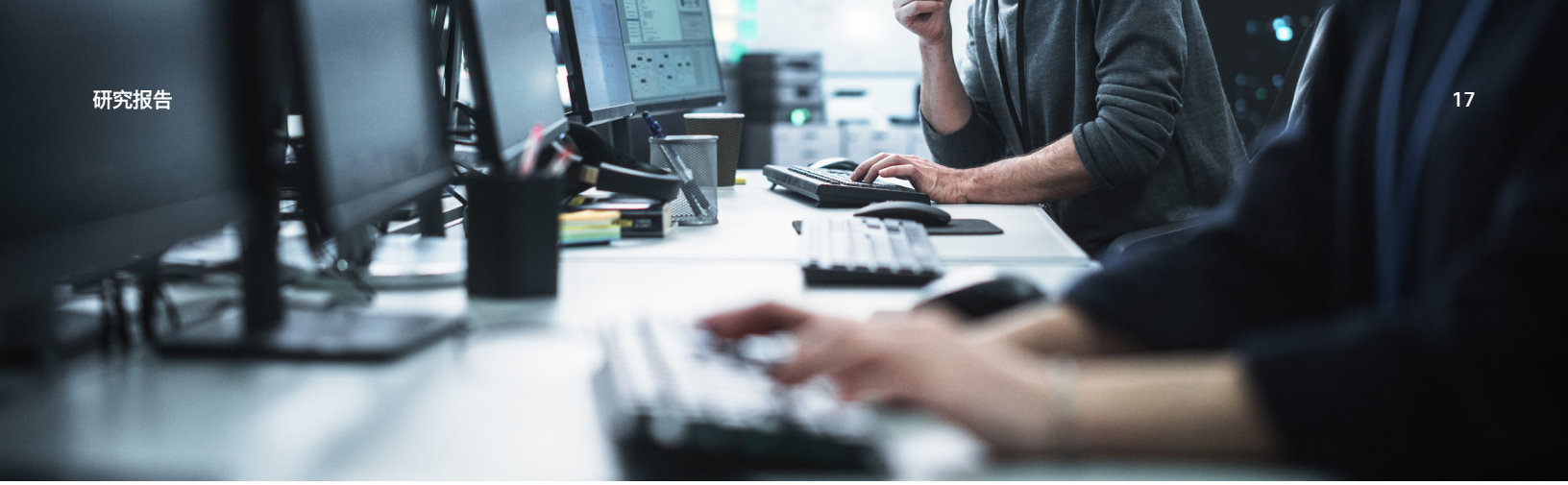
这一认知差距不容忽视，因为最了解实际需求的人未必拥有投资决策权。因此，技术负责人需要向财务和业务部门的同事说明，AgenticOps 带来的并非渐进式改进，而是运营方式的根本性转变。

除认知差距外，其他障碍确实存在，但其影响并没有预想中那么突出。企业最主要的顾虑包括数据安全与隐私 (38%)、AI 的实施与集成难度 (34%)，以及风险与合规 (30%)。值得注意的是，很少有受访者将 “目标不明确” 或 “缺乏领导层支持” 视为主要障碍。这说明，企业并非没有明确目标，也并非缺少推动变革的意愿。真正的障碍在于如何落地实施和建立信任，而不是企业是否愿意推进。

阻碍 AI 在 NetOps 中应用的主要因素



© 2026 思科和/或其附属公司。版权所有。



07 成效

初步成效已得到验证

投入是否已见回报？目前的初步结果令人鼓舞。

在网络运营中更深入地采用 AI（包括部署 AgenticOps）的企业，在几项关键指标上的表现明显优于 AI 采用成熟度较低的企业：

NetOps 领域 AI 采用成熟度带来的回报

约 30%

人均工作效率提升约 30%。在 AI 采用最成熟的企业中，人均每日处理的告警数量更多。

3.2 倍

在全面洞察边缘基础设施瓶颈情况方面，AI 采用成熟度最高的企业比例是 AI 采用成熟度最低企业的 3.2 倍。

来源： Omdia

© 2026 思科和/或其附属公司。版权所有。

工作效率

提高个人工作效率。在采用 AgenticOps 且 AI 采用成熟度最高的企业中，其一线人员的工作效率比 AI 采用成熟度最低企业的一线人员高出近 30%，人均每天调查和处理的告警也明显更多。在其他条件相同的情况下，工作效率提升后，处理同等数量的积压告警所需的专业人员可以减少数十名，稀缺人才也能将更多精力投入到更具价值的工作中。

可视性

提升可视性。在智能体采用最成熟的企业中，全面洞察边缘基础设施瓶颈情况的比例是其他成熟度较低企业的 3.2 倍。这些企业也更容易发现性能问题涉及多个领域这一特点，而这正是解决此类问题的前提。

运营承载能力

增强信心，提升运营承载能力。AI 采用较为成熟的企业更有可能表示，团队能够从容应对工作量，而非疲于应付或不堪重负。

© 2026 思科和/或其附属公司。版权所有。



08 展望未来

未来 12 个月将成为决定成败的关键时期

本报告的研究结果表明，行业已经迎来重要转折点。面对网络规模庞大、变化迅速且彼此割裂的局面，传统的人工运营已难以应对。企业因此认识到，要解决这一结构性难题，需要借助智能体实现自主化运营。企业已开始在生产环境中部署这一模式，明确了建立信任所需满足的条件，并预计在一年内实现由 AI 主导的运营模式。

当前需要解决的已不再是方向问题，关键在于如何落实：企业能否落实各项安全护栏，确保智能体驱动的自主化运营值得信赖？企业能否整合彼此割裂的工具，打造其认为必不可少的一体化平台？技术负责人能否成功争取业务部门的理解与支持，共同推进转型？

未来 12 个月的关键已不再是企业是否会采用 AgenticOps 来管理网络，本研究所涉及的企业早已对此作出选择。未来 12 个月将检验企业的落地成效，也将决定哪些企业能够率先建立起面向未来十年的网络运营模式。

告别混乱，实现自主高效运营。

要摆脱当前运营混乱的局面，迈向以 AgenticOps 为代表、优先采用智能体实现高效运营的未来，企业领导层必须果断采取具有战略意义的行动：

© 2026 思科和/或其附属公司。版权所有。

01

从 “增加人手” 转向 “构建自主化运营体系”

不要再试图单靠增加人手来解决规模性难题。每天积压 4,100 条告警，企业不可能一味扩招来应对。即便能够做到，这种业务模式也难以持续。调整工作重点和预算分配，不再一味增加人手，而是着力打造更完善的自主化运营体系。对团队进行再培训，让成员不再只是手动追查误报、处理工单，而是转为负责管理智能体的 “协调人员”。这样做的目的是将优秀人才从应对海量告警、处理系统频繁变更等日常事务中解放出来，让他们投入更具价值的网络战略设计工作。

02

弥合高管和一线人员之间的认知差距

负责网络运营的人与掌握资金投入决策权的人之间存在着不容忽视的认知脱节。NetOps 团队已经意识到，现有的人工运营模式难以为继；但业务部门高管可能仍认为，采用智能体实现自动化只是锦上添花，而不是生存之策。您需要让高管认识到，每天 4,100 条告警和迟迟无法解决的问题，不只是技术层面的挑战，更会带来业务风险；采用 AgenticOps 不只是升级 IT 系统，更是降低业务风险、避免服务中断和安全漏洞的重要举措。

03

建立 “信任优先” 的监管框架

不要等到危机发生后，才着手制定 AI 和智能体安全护栏。只有建立起充分的信任，企业才能真正发挥智能体自主操作和决策的价值。在扩大应用规模之前，应先部署能够保障智能体安全、确保运行过程透明且可审计并支持人工监督的解决方案。除了工具本身，还需要完善相应的监管机制，明确规定 AI 的操作权限，并确保每项决策都有据可查、能够说明原因。唯有如此，才能消除对未知风险的担忧。无论引入哪家供应商或哪种系统，都必须确保 AI 的决策依据清晰可查、能够得到合理解释。

© 2026 思科和/或其附属公司。版权所有。

09 附录

关于本研究

随着 AI 在网络运营中的应用日趋成熟，业界正逐步形成一套共同的术语体系。以下定义反映了业界在 IT 运营和 NetOps 场景中区分各类 AI 时日益通行的方式。

人工智能 (AI) 是指机器执行通常需要人类智能才能胜任的任务的能力，例如理解语言、识别模式、解决问题，以及根据新信息不断学习。这是一个总称，涵盖下文所列的各类 AI。

生成式 AI 能够根据提示词生成新内容，例如文本、代码、图像或摘要。生成式 AI 不仅能够进行分类或预测，还能产出原创内容，为聊天助手和编程助手等工具提供支持。

AIOps 起源于机器学习和数据分析，如今又借助生成式 AI 得到进一步扩展。AIOps 能够检测问题、关联分析不同系统中的事件，并提出解决建议，但通常仍需由人工解读结果并执行相应操作。

智能体 AI 则更进一步，能够在明确的安全护栏下自主执行操作。智能体 AI 能够根据既定目标自主决策、执行操作，并根据情况变化灵活调整。人类则负责为智能体指明方向、设定目标，无需亲自执行每个步骤。人类负责确定目标和方向，具体执行工作则交由智能体完成。

AgenticOps（智能体运营）是在智能体 AI 的基础上发展起来的一种运营模式，即由人类指导智能体跨领域感知环境、推理分析问题并执行操作。运营人员负责确定方向并制定安全护栏，原本需要人工完成的任务则由智能体执行。

本报告中的所有信息均基于 Omdia 于 2026 年开展的一项独立研究。该研究面向北美、西欧和亚太地区员工人数不少于 500 人的企业，共有 1,000 名 IT 和网络运营负责人参与。本报告还引用了思科的一项分析结果。该分析基于汇总遥测数据，追踪了 2025 年 10 月至 2026 年 4 月期间直接流向 AI 的网络流量。

© 2026 思科和/或其附属公司。版权所有。