2026年无线网络发展现状

解锁乘数效应: 战略性无线网络投资
如何在AI时代推动企业增长

中国市场洞察

摘要

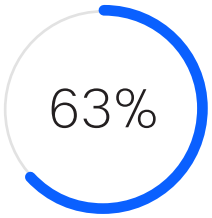
到2026年，Wi-Fi已从一种便利工具跃升为推动企业发展的战略增长引擎。在全球范围内，全面投资无线网络的企业在运营效率提升和收入增长方面获得高投资回报 (ROI) 和可量化业务收益的可能性，是其他组织的四倍。这种独特的“乘数效应”使无线网络投资区别于其他IT投资，能够在整个企业范围内产生复合回报。

然而，98%的企业98%都面临着相同的困境：运营复杂性日益加剧、安全威胁不断增加，而能够应对这些挑战的专业人才却愈发稀缺。与此同时，企业还必须适应日益多样化的连接需求，支持不断扩展的用户与设备——从员工、外部承包商，到自主机器人、智能传感器和各类AI应用等。

全球范围内，在AI、自动化、现代安全体系与获得专业认证的技术人才方面进行整体性投资的组织，相比未投资者具有显著优势：

+4x

获得高投资回报的概率增至4倍



无线网络平均投资回报率高63%

本报告首次提出“无线 AI 悖论”这一概念： AI 既是提升无线网络投资回报率的核心动力，也是风险急剧上升的主要原因。尽管 AI驱动的运营每年可为每位IT专业人员节省数百小时，但同时也带来更高的基础设施需求、更复杂的安全威胁以及更严重的人才短缺等挑战。本报告以Wi-Fi作为企业连接的核心基础层，同时从更广泛的无线网络生态系统视角展开分析，涵盖其所支撑的各类应用场景，包括AI驱动的应用、IoT与OT环境，以及新兴的企业级用例。

我们的研究指出，除了传统基础设施的限制外，还有三大相互关联的障碍正在限制企业释放无线网络投资回报的潜力：运营复杂性持续攀升、安全威胁不断加剧、人才缺口日益扩大。这些挑战会相互强化，形成复合风险。

能够全面解决运营、安全与人才三大挑战的企业，其投资回报比未能解决者高出63%。这表明，战略性无线网络投资能够在多个维度带来可量化的复合回报，也解释了为何在AI应用加速扩展与技术创新不断推进的背景下，无线网络投资依然持续增强的原因。

研究充分显示，当中国企业将无线网络视为战略重点时，能够在多个维度获得可量化的回报。84%的企业报告运营效率提升，80%报告客户参与度提升，74%报告收入实现增长，73%报告员工生产力提高。这充分证明，现代无线网络能够直接转化为业务增长动力。

打造竞争优势的窗口期已经开启。通过简化运营流程、推动无线安全现代化、打造经专业认证的技术人才团队，那些在2026年果断采取行动的中国企业将能够把Wi-Fi打造成未来十年的战略增长引擎。

多重挑战下的无线网络战略
应对AI悖论，打破投资回报率的受限瓶颈

“无线AI悖论”是什么，及其为什么重要

“无线AI悖论”既是2026年中国企业领导者所面临的核心战略挑战，也是先行者能够把握的重大机遇。在无线网络领域，AI 既是推动投资回报率增长的主要驱动力，也是带来最大挑战的源头。在全球范围内，已经部署 AI 的组织更有可能将无线网络视为战略关键，并且在将无线网络优化纳入AI 部署战略时获得更高的回报。同时， AI 也带来了前所未有的运营复杂性，催生新的安全威胁，并加剧人才竞争。

无线AI悖论
AI既是解决方案，也是挑战

解决方案

- AI驱动的运营能够简化无线网络复杂性
- 自动化使IT团队专注于战略工作
- 简化工单处理，加速工作流程

挑战

- AI生成的网络攻击成为首要安全威胁
- 无线网络的AI领域高级人才短缺
- IT人才从无线技术领域转向AI领域

AI既是推动无线网络投资回报增长的主要驱动力，
也是最大的风险来源

AI给无线技术团队带来的多重挑战

安全威胁的主要因素

#1 远程和混合办公模式扩大受攻击面，增加未受管控的终端

#2 AI生成或自动执行的网络攻击与自动化入侵工具

#3 IoT与各类联网设备快速增长

吸引无线 IT人才转型的主要方向

#1 AI 与机器学习

#2 软件工程与应用开发

#3 云基础设施与DevOps

招聘无线网络人才的主要障碍

#1 高级无线技术或AI融合技能人才短缺

#2 地域限制或远程办公带来的挑战

#3 对无线技术领域缺乏兴趣

在中国，已经部署AI的企业，对无线网络重要性的认知明显不同于其他企业。研究显示，在这类企业中，56%的全球无线网络领导者认为无线网络具有战略关键性；而在未部署AI的企业中，这一比例仅为46%。

无线网络战略地位提升的原因显而易见：AI对无线网络的性能与韧性提出了更高要求。将无线网络优化纳入AI 部署战略的企业，获得的回报明显更高。在中国，超过70%的企业报告称，无线网络投资在运营效率、客户参与度、员工生产力和收入增长等方面都带来了积极影响。

AI发展所产生的机遇、挑战与风险之间，究竟如何相互关联？

尽管AI被视为简化无线网络运营、解决系统复杂性的关键路径，但由AI生成或自动执行的网络攻击，正成为无线网络安全威胁加剧的重要因素之一。同时，AI 也是最有可能吸引中国无线技术人才转型的方向。

障碍一： 运营复杂性超出现有能力承载范围

企业在应对“AI悖论”时面临的首要障碍，是不断加剧的运营复杂性。中国98%的无线网络领导者反映，无线网络运营正变得愈发复杂，导致团队长期处于被动应对状态。这种复杂性不仅限制了资源的有效利用、挤压了战略性工作的空间，还直接拖慢了本应有助于降低复杂性的AIOps与自动化项目的推进，由此形成了一个不断加剧的恶性循环：复杂性迫使团队进行被动响应；被动响应限制了现代化进程；现代化进程受阻又进一步加剧复杂性。

中国企业指出，推动运营复杂性持续上升的主要因素有三项。一是关键IT任务、IoT和OT工作负载不断增加 (48%) ，其中包括越来越多的AI应用；二是客户端行为的不可预测性 (43%)；三是新应用场景带来的带宽需求不断攀升 (40%)。

这种复杂性已转化为实实在在的运营压力。56%的企业表示，其团队每周至少需要处理50个无线技术支持工单，这意味着IT团队每月可能要花费数百小时处理无线技术工单。

更令人担忧的是，这种复杂性导致团队陷入了被动应对的工作模式。57%的受访者表示，他们将大部分时间都花在被动式故障排除和事件管理上。这意味着战略性项目、培训、资质认证、网络优化等主动性工作往往被迫让位，优先级不断下降。

这种被动的运营模式正在直接拖慢企业的现代化进程。当团队大量时间被故障排查占用时，资源与注意力就不得不从其他关键任务上转移，例如无线网络的战略规划、人才培训、资质认证以及自动化能力的部署。

加剧这一运营挑战的一个关键因素是可视性不足。94%的企业表示存在可视性缺口，影响了其有效排查Wi-Fi问题的能力。最常见的挑战包括客户端可视性不足、数据包可视性不足，以及应用与云可视性不足。

缺少端到端的全面可视性，团队便无法快速隔离问题根源。这带来了一个特别危险的后果：无线网络往往成为其他系统问题的“替罪羊”。64%的受访者表示，超过10%的IT事件被错误地归因于无线网络。

在AI赋能企业数字化转型的大背景下，无线网络负责人普遍认为AI是应对这些日益复杂挑战的最具潜力的解决方案。AI带来的收益是实实在在且可量化的，包括显著节省时间、简化网络运营流程，以及大幅缩短工单处理时间等。

然而，在中国推广无线AI能力的实践中，理想与现实之间存在着显著差距。

仅运营复杂性这一个因素，就已成为破解“无线 AI悖论”、提升无线网络投资回报的首要挑战。当这一挑战与不断升级的安全威胁（第二大障碍）叠加时，其对组织韧性和财务表现的冲击将进一步放大。

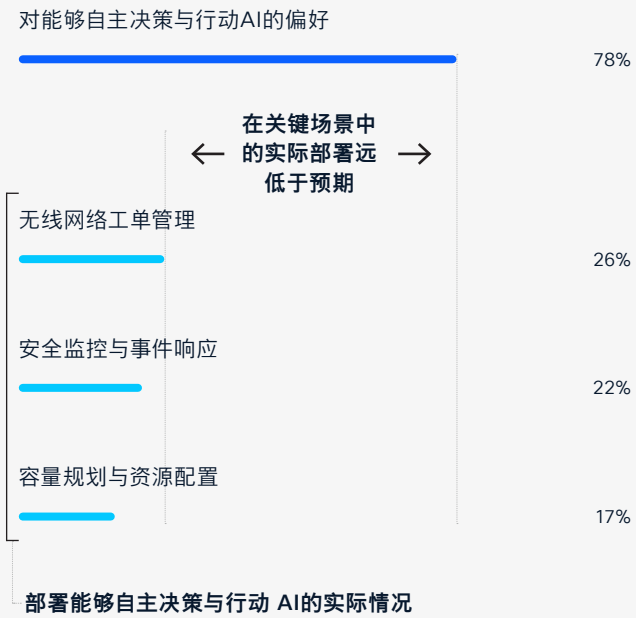
94%企业报告存在可视性缺口，包括

客户端可视性不足 58%

数据包可视性不足 52%

应用与云可视性不足 49%

AI应用差距：期望与现实之间的鸿沟



障碍二：无线网络安全面临严峻考验——IoT 设备激增叠加 AI 生成的安全威胁

无线网络安全已成为阻碍中国企业破解“无线AI悖论”、实现高无线网络投资回报的第二个关键障碍。在安全威胁不断升级、财务损失持续攀升的背景下，企业难以放心地将 Wi-Fi 作为承载关键业务工作负载的平台。

在过去一年中，中国有 94% 的企业至少经历过一次无线网络安全事件。36% 的企业反映，过去两年无线网络威胁持续升级，具体表现为攻击频率更高、破坏性更强，更难被检测和修复。

AI生成或自动执行的网络攻击频繁被列为导致无线网络安全威胁增加的前三大因素之一。这类攻击能够自动识别网络漏洞、根据防御系统响应动态调整攻击策略，并以远超人工攻击的规模与速度实施攻击。更严重的是，AI大幅降低了攻击 Wi Fi 的技术门槛，使得AI生成或自动化攻击工具无需大量资源即可发起高复杂度、高频次的攻击。

中国企业面临的攻击面仍在快速扩大。在遭受安全事件影响的企业中，35%表示受到了被攻破的IoT或OT设备的干扰。由于Wi-Fi是IoT设备最常用的连接方式，这一趋势对Wi-Fi构成了重大威胁。IoT设备数量激增，尤其是未受管控的设备，会导致安全漏洞不断累积。单个设备的漏洞不断累积，最终汇集成整个网络层面的安全隐患。

这些无线网络安全事件造成的损失不容忽视。54%的中国企业曾因无线网络安全事件遭受财务损失，其中更有55%的企业过去一年的损失超过100万美元，足以证明加强 Wi Fi安全投入的必要性。

中国企业因无线网络安全事件遭受的损失不仅限于资金层面。42%的企业因此失去了客户信任，32%的企业面临监管处罚或合规方面的不利后果。这些数据表明，安全事件的影响远超处理事件的直接成本。

然而，大多数企业仍对其无线网络安全保持信心。87%的企业认为自身已采取足够措施保护无线网络。但与此同时，又有57%的企业预计未来两年无线网络安全事故将会增加。

受访企业指出，阻碍无线网络安全提升的核心因素包括：实施复杂度高、传统基础设施带来的限制和性能顾虑。这些障碍并非孤立存在，而是与更广泛存在的无线网络挑战相互关联，如人才短缺、可视性不足和不断上升的运营压力等，共同限制了企业推进安全现代化的能力。

无线网络威胁水平上升的主要因素

远程与混合办公扩大受攻击面，增加未受管控终端的暴露风险	37%
AI生成或自动执行的网络攻击与自动化入侵工具	35%
IoT与联网设备使用量激增（设备数量快速增长）	35%
预算或资源受限，导致安全能力难以有效改进	28%
缺乏专业人员或运维能力来监控并应对威胁	27%

其结果是不断扩大的漏洞差距。在风险持续升级的同时，企业却受制于过时系统、复杂性和性能顾虑，导致安全转型放缓，组织韧性被持续侵蚀。

研究显示，采用基于证书或配置文件的现代身份验证方式的企业，不仅在安全表现上更为出色，在业务绩效方面也明显优于未采用现代认证的企业。此外，这类企业因无线网络安全事件造成的财务损失也显著更低。

然而，实施现代化安全协议需要专业技能，而这种技能正变得愈发稀缺。这也引出了第三个障碍：无线网络领域面临的人才竞争。

障碍三: 无线网络在AI人才争夺战中处于劣势

人才短缺是第三个关键障碍。它与运营复杂性和日益严峻的安全威胁叠加，正成为阻碍企业扩大无线网络投资回报的重要因素。

人才不足不仅放缓技术现代化进程，还直接加剧运营压力、放大安全风险，并使AIOps的实施变得更加困难。由此形成恶性循环:　缺乏人才的企业技术现代化进程更为缓慢；运营复杂性和安全风险持续升级；运营成本不断攀升；而最优秀的人才因此流向更现代的企业。

在中国，75%的企业反映招聘无线网络人才面临困难，因为IT人才更倾向于进入AI和网络安全等更受关注的技术领域。这种人才流失进一步扩大技能缺口，并带来一系列实际损失，包括: 运营成本上升 (41%) 、创新能力下降 (38%) 、团队士气低落 (31%) 。

在中国，人才短缺会十分明确地导致负面后果。那些在招聘无线网络人才方面遭遇极大困难的企业，在被动性事务上投入的时间要更多。人才短缺的影响不仅体现在运营层面。与招聘顺利的企业相比，这类企业每年因安全事件承担的成本也明显更高。

那些既难以招聘，又缺乏经专业认证的技术人才的企业，将遭遇多重不利因素: 更高的运营成本、更大的安全风险、更低的自动化水平，以及更弱的技术现代化能力。相反，那些及早投入人才培养与资质认证的企业，在复杂度不断上升、专业技能对运营成效的影响愈发关键、人才竞争日益白热化的背景下，将获得显著竞争优势。

人才危机清晰地展示了“无线AI悖论”中各要素相互关联的特性。如果不将AI融入无线网络运营核心，企业将会持续流失人才；缺乏人才，安全现代化等战略项目就难以推进；没有现代化的安全防护，安全事件的处理成本就会上升；成本上升使得对人才与技术的投入更加困难。

这种层层相扣的关系解释了为何企业必须同时解决这三大障碍，才能真正摆脱“无线 AI悖论”。

AI导致的人才流失与技能短缺

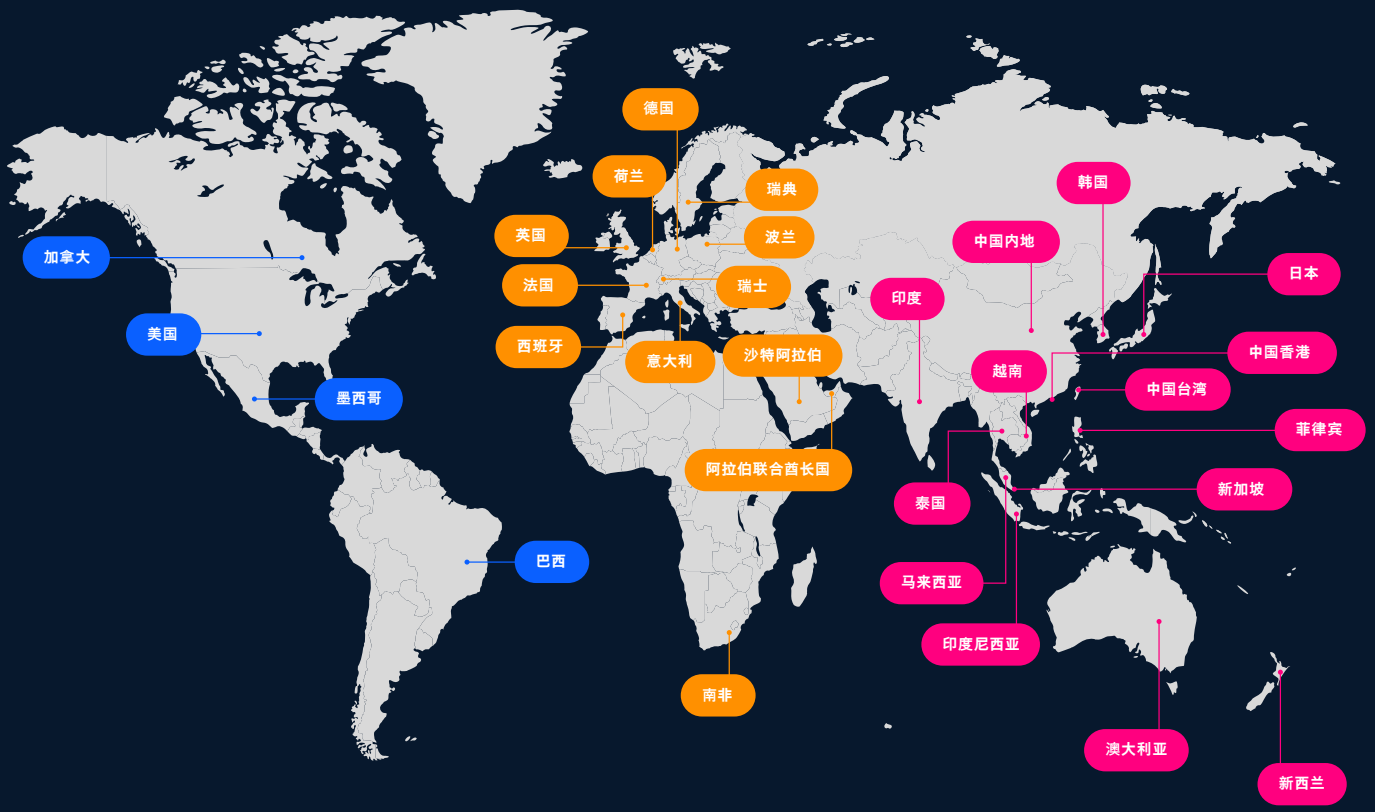
吸引无线技术人才转型的前三大领域

AI 与机器学习	49%
软件工程与应用开发	41%
云基础设施与 DevOps	41%

招聘无线网络人才困难的主要原因

高级无线技术或 AI 融合技能的人才短缺	49%
地域限制或远程办公模式带来的挑战	41%
对无线技术领域缺乏兴趣	39%

方法论



本研究由Sandpiper Research and Insights于2025年11月开展，共采访了30个市场的6,098家企业，包括中国内地的513家企业。

研究范围

受访者概括： 本次调研共采访了 6,098 名来自拥有至少 250 名员工的企业的无线网络决策者和技术专家。其中，61% 的受访者所在企业的年营业额至少为 1 亿美元。

美洲 22%

欧洲、中东、非洲 28%

亚太 50%

本研究覆盖30个市场，包括： 澳大利亚、巴西、加拿大、中国内地、法国、德国、中国香港、印度、印度尼西亚、意大利、日本、马来西亚、墨西哥、荷兰、新西兰、菲律宾、波兰、沙特阿拉伯、新加坡、南非、韩国、瑞典、瑞士、中国台湾、泰国、阿联酋、英国、美国、越南。

本报告受访者来自各个行业，确保研究结果具有广泛的适用性。 涵盖的行业包括：商业服务，建筑，教育，工程、设计与建筑，金融服务，政府和公共服务，医疗保健，制造业，媒体和通信，自然资源，房地产，餐饮服务，零售，技术服务，运输，旅游服务，批发。

调研时间： 2025年11月。

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**