HyperFRAME RESEARCH

研究简报

Cisco AgenticOps:

依托自主网络和跨域智能，重塑全球业务韧性

2026 年 3 月

作者:
Ron Westefall
基础设施与网络副总裁兼业务负责人

执行摘要

网络运维 (NetOps) 不断演变，其重心已跳出单一的设备管理范畴，全面转向对分布式 AI 能力的管理。现有的运维框架专为应对静态环境与线性增长而打造，如今已难以为继。当下，NetOps 的复杂程度呈指数级增长：运维已然延伸至数百万个瞬态云实体和数十亿台 OT/IT 边缘设备，这些设备所生成的遥测数据规模庞大，远超人类认知和处理能力极限。仅靠一群工程师手动翻阅日志，不仅排障与修复效率低下，而且无法有效防范服务中断。现如今，必须借助机器级速度的逻辑运算，方能保障网络稳定、优化流量路由并缓解安全威胁。要在这场变革中立于不败之地，企业和组织必须摒弃被动监控，转而采用掌握全局情景信息的系统，在还没来得及进行人工干预之前便自动完成纠偏。Cisco AgenticOps 正是此类系统的理想之选。

Cisco AgenticOps 是一套完备的框架，可帮助企业有效管理自主程度各异的 AI 智能体，并按需对智能体集群进行弹性扩展。该框架确立了一套严谨的运维规范，可确保在 IT 环境中对自主 AI 智能体进行合规部署、管理、监控和监管。借助该框架，智能体可自主观测基础设施、深入推理分析问题并采取纠正措施，最大限度减少对人工干预的需求。AgenticOps 覆盖智能体的全生命周期，并通过统一基础设施保障智能体安全可靠且具备清晰的责任可追溯性。同时，它还提供监管机制、可视性和可控性，确保运维团队能够有效监督智能体的自主决策与执行过程。

Cisco AgenticOps 是 IT 运维 (AIOps) 的最新发展方向，它将以智能体为核心、专门构建的自主执行能力与人工监督相结合，让人类与智能体能够在同一环境中高效协作。与 AIOps 相比，AgenticOps 实现了多方面的重要突破：

- AIOps 应用生成式 AI 和机器学习来检测异常并对相关事件进行关联分析。整个过程离不开人工干预，需由运维人员解读建议、编写自动化脚本，并手动批准或执行修复操作。
- AgenticOps 则更进一步，赋能企业安全可靠地部署 AI 智能体。这些智能体能够对问题进行独立推理分析，并以机器级速度在不同软硬件平台上完成复杂的多步任务。AgenticOps 让 IT 运维真正迈向自主化，它不仅能极大提升人员能力和技能，还能通过融合逻辑推理、场景模拟与闭环执行，成功推动网络从 “被动救火” 的传统模式，蜕变为主动防御、自我优化的智能系统。

落实到日常运维中，这意味着团队将彻底告别紧盯海量控制面板、手动流转工单的困境。借助 AgenticOps，智能体可持续感知并推理分析各种依赖关系，在工程师收到网络瓶颈告警之前，就已提前发现并定位问题。无论是本地设备还是云端环境，智能体都能即时检测问题并执行修复操作。AgenticOps 有助于打破不同运维域间的孤岛，最大限度提升整体服务体验。

更重要的是，AgenticOps 框架必须与企业和组织现有的工作流程紧密结合。向自主运维的跨越绝非一蹴而就，更不应盲目求快。在 AgenticOps 框架下，智能体会提供具体的补救方案，由人工审批，并在统一协作环境中与团队共同推进处理流程。通过这种方式，团队可逐步增进对系统的信任，并循序渐进地授予智能体更多自主权限，从而推动 IT 生命周期管理从频繁人工干预向高度互信自动化监督的转变。

本研究简报提出了三个核心观点：

1. 首先，AgenticOps 势在必行。现代数字基础设施的复杂程度已达临界点，唯有依靠机器级速度的自主执行能力，方能弥合实时遥测与有效补救之间的鸿沟。
2. 其次，借助 Cisco AgenticOps 框架，企业和组织得以配备一支专注于排障、优化与验证的智能体数字员工团队。这些智能体能够充分利用跨域遥测数据与思科 40 年来沉淀的专业知识，与 IT 团队协同工作，打破运维孤岛，提升网络运维的自主化水平。
3. 最后，本文深入剖析了思科缘何能成为 NetOps 领域领先的 AgenticOps 提供商。凭借独树一帜、深度集成的多层 AI 架构，思科能够通过全面的跨域部署来简化运维操作，加速实现业务价值。在简报结尾，我们提供了一份切实可行的行动路线图，旨在帮助决策者将战略蓝图转化为分阶段执行的具体举措。

战略必然之选：AgenticOps 为何势在必行

AgenticOps：传统 AIOps 已无法满足需求

传统 AIOps 解决方案的能力存在明显上限。纵观其演进历程：最初引入的是机器学习技术，能够发现异常并生成告警；随后生成式 AI 震撼登场，已经具备解释问题并给出修复建议的能力；再后来，各大 AIOps 平台相继涌现，可用于收集遥测数据、对事件进行关联分析，并优化告警机制，但这些能力通常仍局限于网络、安全防护等独立的职能领域。虽然 AIOps 有助于减少告警干扰，却无法从根本上改变运维模式。运维人员依然是解决问题的核心主体，他们需要手动打通各个孤立的域，整合零散的数据洞察。

现实情况是，现代基础设施的网络中断和性能下降很少只发生在单一层面，而是由网络、云环境、安全协议以及应用栈之间的复杂交互共同引发。由于传统 AIOps 很大程度上仍处于孤立运行与被动监测的状态，一旦遭遇跨域故障，运维团队只能被迫组建紧急“作战室”，手动进行关联分析。AIOps 只能检测系统中的异常，但具体原因分析仍需人工完成。这种高度依赖人工的排障模式，不仅极易引发告警疲劳，更会严重拉长平均修复时间 (MTTR)。

举例来说，AIOps 只能被动响应结构化数据和阈值告警，例如面对流量激增，仅抛出“CPU 占用率过高”这类通用告警。而 AgenticOps 则能够凭借基于大语言模型 (LLM) 的工具增强型规划能力，以媲美人类的推理能力，对整个运维栈进行梳理。面对异常，自主智能体不再只是向工程师发送告警，而是会主动调查根本原因，例如查询营销工作流程可视化数据以确认是否有正在进行的促销活动，从内部文档库中检索专门针对促销场景的扩容操作手册，执行必要的资源扩展脚本，最终在团队沟通渠道中汇总整个处理过程。得益于这一转变，系统不再只是历史数据模式的“被动观测者”，而是成为具备跨平台排查与端到端任务执行能力的“主动参与者”。简而言之，面对当今数字化 NetOps 的庞大需求，传统 AIOps 模式难以有效扩展，早已力不从心。

AIOps 与 AgenticOps：对运维影响的关键差异

NetOps 活动	传统 AIOps	AgenticOps
监控和监督	工程师人工监控控制面板并处理告警。	智能体持续监控系统，人类则担任监督角色。
变更管理	系统变更需由人工执行，同时需要人工值守监看。	智能体可在预设安全边界内自主规划、模拟并执行变更。
故障排除	由人工主导调查：工程师需逐条排查海量日志，以找出根本原因。	由智能体主导诊断流程：智能体可自动识别问题、推理出解决方案并采取相应操作，至于是否需要人工验证，则可根据实际场景灵活配置。

来源：HyperFRAME Research

AgenticOps 注重“智能执行”，具有超越传统模式的鲜明优势。它让“网络自修复”不再停留在概念阶段，而是真正落地执行：依托智能体 AI 预测故障，及时触发纠正措施，防止性能下降或更严重的问题在网络中蔓延。实现从被动监控到机器级速度自动执行的跨越后，企业和组织不仅有余力优先清理基础设施技术负债，还能打破人工“作战室”无力应对数字化故障频发的困局，从而大幅减少乃至杜绝由此引发的运维停机。

为实现 AgenticOps 的全面安全落地，企业和组织必须首先做到以下几点：

1. 确立监管框架：明确自主智能体的权责边界与审计机制，为其设置“人机协同”防护措施。
2. 重点打造基于数据的模块化架构：采用“先爬、后走、再跑”这种循序渐进的策略，确保搭建高质量的数据架构，并在与现有工作流程和系统集成时保持低延迟。
3. 采用端到端 AgenticOps 框架：将域专属智能功能、统一跨域遥测数据、“人机协同”监管机制相结合，为全面落地做好准备，弥补技能缺口，并降低采用难度。

从辅助工具到得力伙伴：思科智能体数字员工的崛起

AgenticOps 让 AI 蜕变为一支具备高度自主能力的数字员工队伍。思科将专门打造的 CCIE 级逻辑嵌入平台，赋予其始终在线的能力，助其突破基础自动化的局限，迈向主动协作。其智能体依托深度运维智能，可以主动管理网络，并具备不同程度的自主性，既可以执行由人工触发的调查，也可以持续对环境进行深入评估。这一转变具有颠覆意义：AI 不再是工具，而是与运维人员共同管理网络的协作伙伴。AI 与人类专家的经验融为一体，以一种全新的智能体协作模式共同协调网络。

思科最近推出了新一代 AgenticOps 框架，主打简化运维和基于 AI 的解决方案，致力于帮助企业和组织打破运维孤岛，迈向自主网络运维模式。此次升级的亮点在于，全面扩展了排障、优化与验证等智能体能力，旨在尽量减少人工干预，实现网络环境的高效管理。这些智能体能力以及新增 AI 增强型功能已集成至 IT 人员常用的平台/应用，包括 Cisco AI Assistant、Agentic Workflows、Cisco Cloud Control、AI Canvas（即将推出），以及各类第三方应用。

智能体数字员工的第一项能力是 “Autonomous Troubleshooting”（自主排障），即主要负责从事件检测到解决的整个处理过程。得益于这一能力，智能体可实时对网络、安全和互联网层的遥测数据进行关联分析，实现跨域问题调查、推理和解决。它们不是依赖各种假设，而是大规模分析海量信号来确定问题根本原因，并推荐或直接执行补救措施。AI Packet Capture 等新工具进一步增强了这一能力，使智能体能够同时处理数千条信号，并在数分钟内提供可信的证据和清晰的解释说明。

思科智能体数字员工：智能体能力

智能体能力	主要职责	核心功能	高级工具
自主排障	全程主导事件处置（从检测到解决）	基于遥测数据推理分析问题根本原因，同时验证多项假设，并以 CCIE 级精度执行确定性补救措施。	AI Packet Capture（实时对数千个信号进行关联分析）
持续优化	持续提升（性能与效率）	通过实时感知端到端网络状态，自主优化射频 (RF)、服务质量 (QoS)、流量路径和控制平面，持续保障用户体验。	AI 配置建议（主动优化配置，提升网络可预测性）
可信验证	变更安全（从意图到结果的全程把控）	基于风险感知的智能体评估，依据实时拓扑、配置与遥测数据对网络变更进行验证，包括识别其影响与波及范围。	影响建模（推理分析变更在系统中的传播路径）

来源：HyperFRAME Research

负责保障网络健康运行的是“Continuous Optimization”（持续优化）这一智能体能力，这些数字化运维助手专注于持续提升网络性能和效率。得益于这一能力，智能体能够检测无线、交换和 WAN 环境中的配置偏移并预测性能下降趋势，在用户受到影响之前主动采取行动。它们无需等待工单，而是能够主动识别潜在风险模式，并在既定防护措施下对环境进行优化调整。智能体能力持续扩展，其中包括“AI Configuration Recommendations”（AI 配置建议），旨在确保网络性能稳定可预测。

智能体数字员工的另一项核心能力是“Trusted Validation”（可信验证），即负责提升网络变更的安全性和可预测性。得益于这一能力，智能体能够在变更实施前，模拟其潜在影响和波及范围，并识别隐藏依赖关系和后续风险。变更实施后，智能体会自动验证结果，并从中持续学习，以优化后续行动。智能体通过推理分析变更在系统中的传播路径，可确保每一次更新都能让网络向预期状态更进一步，同时避免产生意外后果。

思科智能体具备灵活能力，可根据所需自主程度以不同模式运行：

1. 按需模式由人工触发，专注于完成特定目标，例如解决具体的客户端问题。
2. 环境智能体模式始终在线，可持续执行 Wi-Fi 优化或策略偏移纠正等任务。
3. 深度推理模式适用于全网环境验证、大规模规划等长期且复杂的任务。

展望未来，思科生态系统中的各项智能体预计都将涵盖这三种模式，为 IT 团队提供更加全面且灵活的支持体系。

从遥测数据到可信决策：Cisco AgenticOps 的基础架构

思科智能体框架由四大战略架构支柱构成，其中首要基础支柱便是跨域遥测数据。我们发现，思科智能体技术采用业界最广泛的遥测数据，涵盖园区、分支机构、WAN 和数据中心环境，以及安全层和应用路径。借助全面的端到端观测点，智能体能够在整个系统范围内开展推理并执行相关操作，确保所有判断均基于完整网络环境，而非孤立的数据点。

第二大支柱聚焦集成模型和思科积淀的专业知识，可使通用 AI 具备面向运维场景的专业智能。思科将前沿模型、基础模型和深度网络模型等专用模型相结合，并融入思科认证互联网络专家 (CCIE) 知识库和人工精心编撰的操作手册，以此增强智能体能力。通过协同运用多种模型，系统能够根据不同任务（无论是快速响应、精细排障，还是解决复杂架构难题），选择最合适的能力。

第三大支柱从设计层面融合了工具、防护措施和可信机制，旨在确保各项操作安全执行。思科智能体绝非盲目行动，而是通过 MCP 和 API 收集数据，始终遵循明确的防护措施和客户定义的审批模式。为保持透明的可追溯性，系统会针对每一次行动提供清晰的推理过程、相关证据和完整的审计记录。在思科看来，可信能力并非可有可无的附加功能，而是系统的根本属性，可确保 IT 团队始终掌握自动化执行的控制权。

思科智能体架构的最后一项支柱能力是多模态交互，充分考虑了 IT 团队需要灵活使用 AI 的实际需求。思科没有拘泥于单一界面，而是通过多种接触点开放其智能体能力，包括现已正式发布的控制面板与 AI Assistant，以及 AI Canvas 等新兴平台、消息系统和 ServiceNow 等第三方工具。通过与事件驱动型告警机制和第三方平台/应用集成，系统能够灵活适配现代 IT 企业和组织的既有工作流程，为团队提供所需支持，而无需强迫他们改变现有工作方式。

面向 NetOps 的思科智能体框架：四大战略支柱

支柱	核心目标	关键能力	重要价值
跨域遥测	可视性与上下文感知	涵盖园区、分支机构、WAN、数据中心、安全防护和应用路径。	让智能体能够在整个系统范围内进行推理分析，打破传统运维孤岛。
集成模型和专业知识	运维智能	融合前沿模型、专门构建的深度网络模型和 CCIE 知识库。	突破通用 AI 的局限，实现专业化、专家级的故障排查逻辑。
工具、防护措施和可信性	安全执行	通过 MCP 和 API 在明确的防护措施范围内执行操作，并提供完整推理依据与审计记录。	确保 AI 不会“盲目行动”，且始终由运维人员掌控。
多模态交互	工作流程集成	支持通过控制面板、 AI Assistant、AI Canvas 和消息系统进行访问。	灵活适配 IT 团队的工作方式，无需强制切换至统一交互入口。

来源：HyperFRAME Research

思科独特优势：通过 AgenticOps 为自主网络的未来保驾护航

Cisco AgenticOps 框架的独特之处在于能够针对不同客户需求提供相应的智能能力，具体包括:

1. **深度网络模型：**专门构建的大语言模型 (LLM)，基于思科 40 余年的知识产权成果训练而成，能够理解网络运行背后的逻辑，并结合实时遥测数据提供即时洞察。
2. **跨域范围：**实现对思科网络、安全与协作各类工作负载的统一可视性。
3. **数据底座：**庞大的数据湖，由 Splunk 的安全与日志能力、ThousandEyes 的互联网与 SaaS 可视能力，以及 Meraki 的云网络能力共同支撑。
4. **智能体互联协同：**集成并协调思科各类平台和解决方案中的网络、安全和协作技术，确保智能体能够与各类工具实时顺畅共享信息并协同工作。

思科的深度网络模型可赋予智能体更广泛的运维智能，使其能够执行复杂任务。竞争对手的智能体能力往往局限于无线诊断或数据中心自动化等单一领域，而思科的智能体能力则依托基于 Splunk、ThousandEyes 与 Meraki 构建的庞大数据湖。因此，AgenticOps 框架不再局限于简单的模式识别，而是通过 CCIE 级逻辑，在企业全栈范围（从用户设备延伸至云应用）内执行复杂的自主操作。思科还通过 3,000 多条推理路径进一步优化此模型。这些路径源于专家经验，确保 AI 能够模拟专业人员的诊断步骤，而非依赖统计层面的概率猜测。

Splunk 平台所形成的数据护城河，使 Cisco AgenticOps 框架有别于 HPE Juniper 和 Arista 等竞争对手的方案。思科智能体具备跨域上下文感知能力，覆盖数据包整个生命周期。思科将 Meraki 和 ThousandEyes 的实时遥测数据以及 Splunk 庞大的安全与日志数据架构整合至 AI Canvas，为智能体提供全面可视性，使其能够端到端（从家庭 Wi-Fi 出发，穿越公共互联网，直至云原生应用后端）追踪用户体验。

依托这些遥测数据，思科得以突破行业普遍存在的单域孤立诊断方式。在思科环境中，自主智能体可对应用性能下降进行分析，判断其是源于特定的安全更新还是区域性 ISP 中断，从而查明根本原因，而只专注内部网络的供应商往往无法做到这一点。得益于这种全面的数据底座，思科智能体在采取行动（例如重新路由流量或调整安全策略）时能全面了解对业务的影响，从而展现出竞争对手 Arista 和 HPE Juniper 难以企及的全栈运维智能能力。

最后，在思科跨域智能体互联协同功能的加持下，智能体能够在网络、安全以及 Webex 等协作工具之间协同工作，无需人工交接即可解决问题。这种集成水平是 HPE Juniper 或 Arista 等产品组合相对单一的竞争对手所无法比拟的。这种横向集成可确保在最终用户感知到中断之前，及时缓解不同部门和技术栈出现的性能问题。例如，网络智能体识别出延迟后，可自动与 Webex 智能体协同改善通话质量，或触发安全智能体隔离受感染的设备，全程无需人工干预，也无需在不同 IT 团队/系统之间来回交接。

思科始终将 AI 安全性与可信性置于首位，依托强大的可解释性与内置防护机制予以保障。为确保可靠性，系统会针对智能体的每项操作提供透明的推理说明，从而实现以下能力:

- **AI 幻觉缓解：**每项自主操作均附带推理链路，用于说明得出结论所依据的数据与逻辑。
- **自动回滚：**保护网络，使其免受意外后果的影响。该框架内置自动回滚机制，即如果 AI 发起的变更导致性能下降，系统会立即恢复相应配置，确保即便在自动化优化过程中也能保持高可用性。

由此可见，思科独具优势，是目前唯一能够打破网络、安全与应用平台之间壁垒的供应商。

思科与竞争对手的对比

功能	Cisco AgenticOps	HPE Juniper/Arista
智能引擎	**深度网络模型：** 基于思科 40 多年积淀的知识产权成果和 CCIE 逻辑训练而成。	通用模型或局限于单一领域的 AIOps 模式匹配能力。
数据范围	**跨域整合：** 打通网络、安全与协作 (Webex) 三大领域。	主要局限于内部网络或无线网络等单一领域。
数据底座	**Splunk + Meraki + ThousandEyes：** 构筑起覆盖自有网络和非自有网络的庞大 “数据护城河”。	主要依赖专有硬件遥测数据或特定云工具。
智能体间协同同步	**横向集成：** 不同域的智能体可相互联动，协作解决问题，整个过程无需人工交接。	不同 IT 部门各自为政，问题解决需依赖人工交接。

来源：HyperFRAME Research

思科产品组合优势：以 AgenticOps 引领企业迈向自主化新时代

我们认为，思科的主要优势在于其具有变革意义的 AgenticOps 框架，可使得网络管理从依赖人工操作的模式，转向自动化的统一数字系统。此次升级由一支 AI 智能体数字员工团队推动，它们专注于排障、优化和验证，具备类似 CCIE 专家的运维能力，全面管理从事件处理到变更安全的完整流程。这套端到端架构由 Cisco AgenticOps 的四大核心支柱共同支撑:

1. 庞大的跨域遥测数据
2. 融合专家智慧的集成模型体系
3. 严格的可信防护措施
4. 灵活的多模态交互界面，如 Cisco AI Assistant 与 AI Canvas

我们认为，思科是企业和组织成功实施 AgenticOps 战略不可或缺的可靠合作伙伴。思科将可确保诊断准确性的深度网络模型、Splunk 庞大的数据架构以及 Meraki 和 ThousandEyes 的遥测数据相结合，提供统一的网络视图，几乎没有竞争对手能够与之匹敌。思科智能体具备灵活能力，可根据不同运维需求与自主程度，在按需模式、环境模式或深度推理模式之间自由切换。

68% 的企业计划每年更换基础模型[1]。在此背景下，Cisco AgenticOps 相比竞争对手具备显著优势，可在不影响核心业务逻辑且不积累技术负债的情况下，实现 AI 引擎的无缝切换。此外，针对 90% 受访者所表达的对 AI 幻觉与安全性的担忧[1]，Cisco AgenticOps 提供了可追踪、可由智能体调用的 API 以及安全防护措施，确保智能体的自主操作始终处于受监管的可靠状态。

综上，建议企业和组织循序渐进，逐步迈向自主化网络运维。我们预计，大多数企业将采取 “先爬、后走、再跑” 这种循序渐进的策略来引入 AgenticOps：从智能体辅助诊断、人工审批补救措施起步，随后将机制明确、风险较低且具备明确回滚路径的操作扩展为闭环执行，并随着系统可信度的不断提升，最终迈向由智能体主导的自主化程度更高的运维模式。从长远来看，AgenticOps 在监管控制、可审计性与影响范围控制方面的能力，将与 AI 技术本身同等重要。

1（HyperFRAME Research：2026 年第 1 季度）

AgenticOps 采用和评估建议

- **借助 AgenticOps 推进战略转型：**CTO、CIO、基础设施/运维副总裁、网络运维 (NetOps) 副总裁、安全运维 (SecOps) 副总裁、云/IT 战略总监和首席架构师等关键决策者，应将评估 Cisco AgenticOps 框架列为优先事项。该框架将 AI 从基础效率工具升级为由专用智能体组成的数字员工，能够在复杂环境中大规模自主完成排障、优化与验证等任务。该框架依托思科 40 年来积淀的网络专业知识，并融合 NetOps、SecOps 与云等不同领域的统一遥测数据，不仅可大幅降低运维风险、缩短问题解决时间，还能通过透明、可信的防护措施确保人工监督机制始终发挥作用。
- **以全面自主的 NetOps 为目标：**企业和组织应考虑采用 Cisco AgenticOps 框架，该框架可提供一支全面的智能体数字员工队伍，能够在复杂网络环境中自主排查故障、主动优化性能并基于风险感知验证变更，从而直接提升团队能力。智能体可在多种执行模式（比如按需辅助、深度推理规划）下运行，利用实时遥测数据，在用户受到影响之前完成事件处置并预防问题发生。
- **优先采用以信任为中心的智能体框架：**企业和组织可将思科视为值得信赖的 AgenticOps 顾问，其框架基于 40 年来积淀的专业知识和跨域遥测数据，可确保智能体的每项自主操作均遵循人工精心打磨的专业化运维智能的指引。Cisco AgenticOps 框架同样强调透明性与可控性，通过清晰的防护措施与多模态交互界面，确保智能体的每项操作均可审计，并与既有 IT 工作流程保持一致。

HYPERFRAME RESEARCH 简介:

HyperFRAME Research 致力于为全球科技领域提供深度研究与洞察，研究范围涵盖从超大规模公有云到大型机，以及两者之间的各类技术形态。我们提供战略咨询服务、定制研究报告、个性化咨询服务、线上活动策划、市场推广规划、信息传播测试以及潜在客户开发计划。

我们的行业分析师擅长运用严谨的定性与定量研究方法，对各行业的技术解决方案、业务挑战、市场趋势和最终用户需求进行评估。HyperFRAME Research 与企业分析师关系团队、产品团队和营销团队紧密协作，打造思想领导力并放大其影响力，凸显企业专业实力，从而提升品牌与产品认知度。借助能够同时打动读者、观众与听众的优质内容，我们确保企业声音能够在各个渠道中广泛传播、引发共鸣。

联系 HYPERFRAME RESEARCH:

Steven Dickens
首席执行官兼首席分析师 | HyperFRAME Research
电子邮箱:
steven.dickens@hyperframeresearch.com
电话号码:
+1 845 505 1678
X: @StevenDickens3
LinkedIn: Steven Dickens
BlueSky: Steven Dickens

撰稿人

Ron Westefall
基础设施与网络
副总裁兼业务负责人

业务咨询

如果希望探讨本报告内容，请与 HyperFRAME Research 联系，我们将及时回复。

引用声明

许可

披露声明

HyperFRAME Research 为众多高科技企业提供研究、分析、建议和咨询服务，其中也包括本报告中提及的相关企业。本公司员工未持有本文档所提及任何企业的股权。


HyperFRAME
RESEARCH