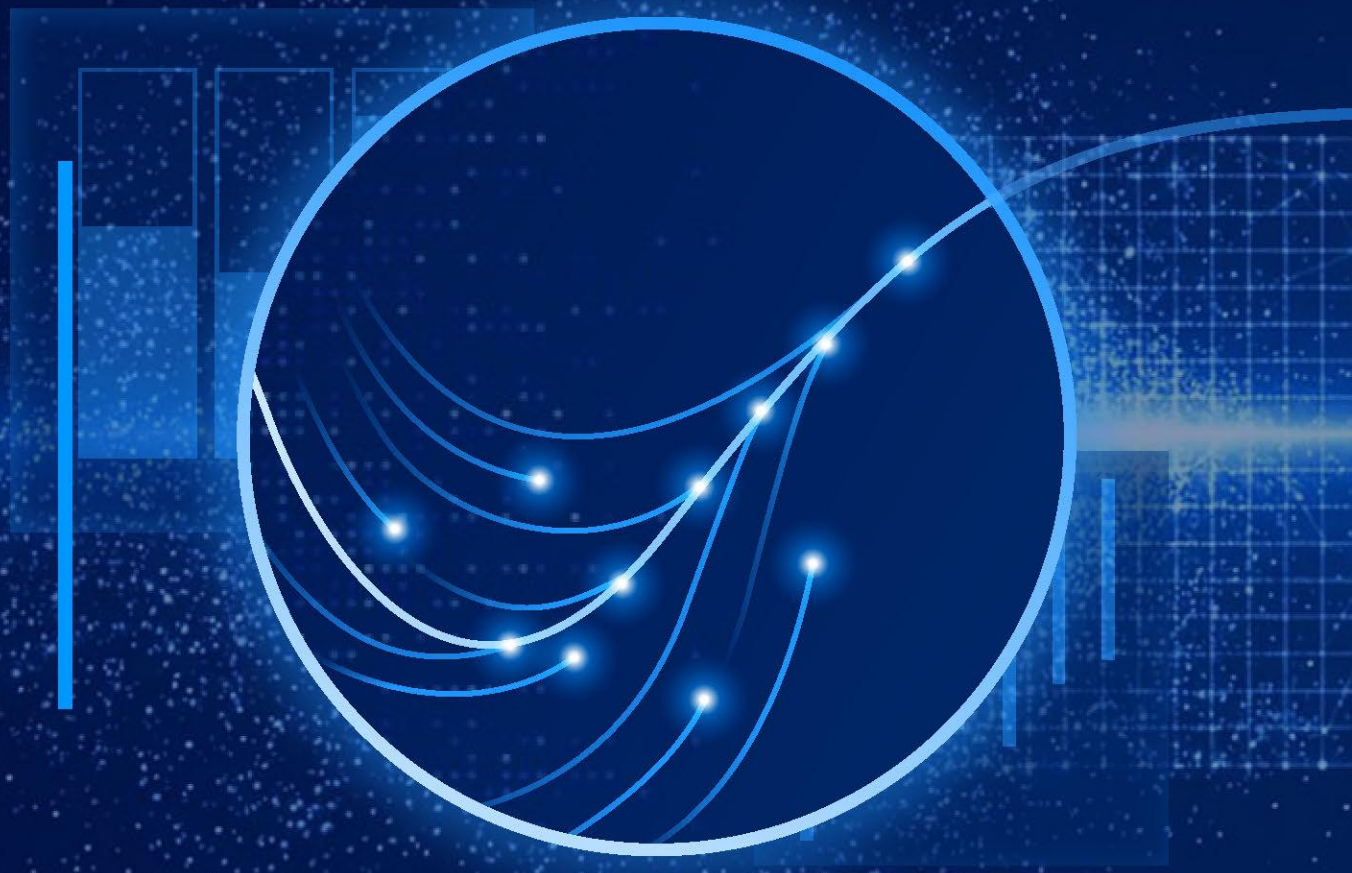
Gartner

2027年十大战略技术趋势



掌控机器行为的新边界

技术领导者必须安全地带领企业进入自主时代。传统 IT 受制于软件供给有限，而到 2027 年，软件生产能力将迎来爆发式增长。静态代码运行不再是主流，取而代之的是对自主机器员工、感知AI与主权边界的编排。要顺利实现这一转变，C级高管必须立即聚焦三大运营方向：

开拓非文本AI前沿

非文本AI指能够进行计算、聆听与模拟的模型。企业应提供基于数学、语音和物理的专用模型，以确定性精度和感知深度解决复杂问题。

治理自主智能体平台

依托系统级控制平面，实现可信自主运行。通过部署平台自有的AI上下文系统、AI编程管控框架、AI安全身份体系与自动化暴露面修复机制，有效管控机器行为并降低安全暴露风险。

构建持久的敏捷能力

逐步转向主权化、可弃置与有机环境。依托主权堆栈、便于彻底停用的可弃置应用和低功耗生物计算，保障技术的长期独立。

Gartner 2027年十大战略技术趋势，可帮助企业领导者建立必要边界，交付可信成果。在审视这些趋势时，企业应思考其与自身战略目标的契合点，并将其纳入规划，以支撑可持续增长与竞争优势。

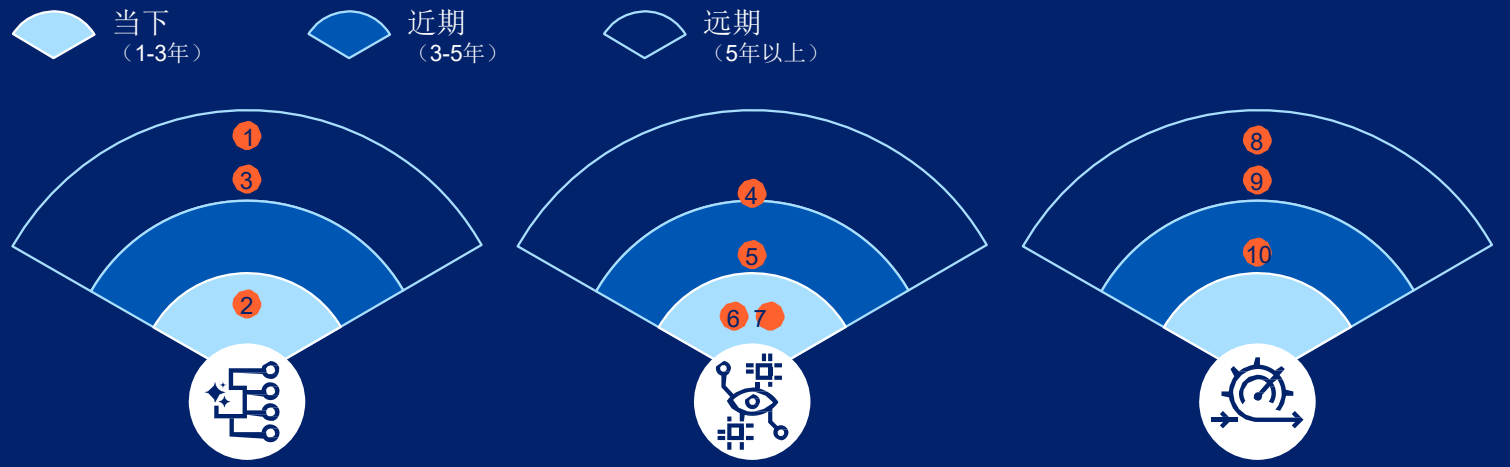
Gene Alvarez
Gartner商业与技术洞见杰出副总裁

Gartner 2027年十大战略技术趋势

技术决策需兼顾当下运营效率与长期业务生存能力。

这份中长期展望按照不同规划阶段对Gartner战略技术趋势进行梳理，帮助您判断各项能力的推进节奏：何时准备、何时试点、何时规模化。

按照这些规划阶段推进技术路线图，与企业整体目标同步，既能在波动中掌握主动，也能系统性升级核心能力。



开拓非文本AI前沿

1. 大型定量模型
2. 语音推理模型
3. 世界模型

治理自主智能体平台

4. AI上下文平台
5. AI编码智能体控制框架
6. AI智能体身份
7. 自主安全暴露修复

构建持久敏捷能力

8. 主权技术
9. 即弃型应用
10. 湿件即服务

开拓非文本AI前沿

AI的能力正在从文本向语音、数值和物理世界扩展。但语音原生的推理模型，其思考深度普遍不及文本模型。若企业将关键决策完全交由某个单一、无监督的语音模型处理，安全风险将被放大。因此，这一趋势的关键在于按复杂度分流：常规任务交给快速模型，复杂决策则交给深层推理模型，各司其职。

能计算、能聆听、能模拟，用于解决复杂问题的模型

趋势1

大型定量模型

是什么？

大型定量模型采用模块化混合神经网络架构，专门用于处理和分析定量数据。它依托确定性计算、既有数学公式、统计方法和数值算法，对复杂系统进行精确建模。

为什么值得关注？

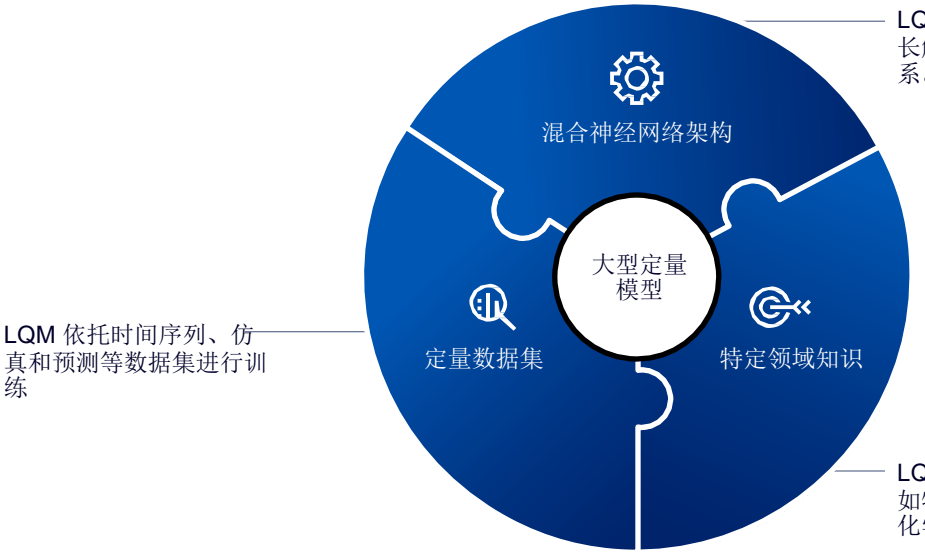
尽管生成式 AI 投资快速增长，但其仍无法满足所有业务场景的需求，尤其是在数值计算领域。大语言模型（LLM）本质是概率式猜测，难以胜任数学推理。大型定量模型（LQM）则专为数值推理设计，它们的资源消耗显著降低，内存、存储和算力需求均大幅减少。这种专用架构为快速预测提供了一条捷径，同时显著降低对高成本Token推理的依赖。

未来将如何发展？

25%

到2030年，企业主要职能部门的战略预测和运营建模任务中，大型定量模型将取代大语言模型，占比达25%。

大型定量模型的核心组成



来源：Gartner

趋势1 | 大型定量模型

通过LQM交付业务成果

行动方案：推动模块化自动化与无缝集成

关键步骤	1 部署混合AI架构	2 应用场景	3 建立严谨的数据验证机制	4 调整ModelOps策略
预期成果	快速预测的捷径	前所未有的业务敏捷性	自主预测的安全部署	省去模型重训，降低算力成本
具体做法	将大语言模型的对话能力与定量模型的确定性分析能力结合起来。	优先考虑金融风险建模、供应链物流、能源预测和农业土壤分析等场景。	确保数值输入准确无误，防止预测模型出现偏差。	持续监测模型部署情况，防止模型过拟合，并保持高效运营。

关键角色及职责

CIO

主导：制定定量AI战略，提升预测、规划与运营决策水平。

投入：优先支持能凭借数学精度和预测准确度形成竞争优势的高价值场景。

推动：将LQM融入更广泛的复合AI计划，加速AI价值释放。

IT协同方

数据与AI团队：搭建数据基础、治理机制和模型能力，支撑精准预测与仿真。

企业架构团队：构建可扩展平台，将LQM与现有AI、分析和业务应用打通。

ModelOps与治理团队：持续监控模型性能、数据质量和可解释性，维护信任与可靠性。

业务协同方

运营负责人：挖掘预测、规划与运营效率的改进空间。

财务与战略团队：将定量洞察应用于情景规划、风险管理和投资决策。

业务领域专家：验证模型假设、输入和结果，确保业务相关性，推动实际应用。

趋势2

语音推理模型

是什么？

语音推理模型是直接在音频上进行推理的语音AI系统，能够在对话中持续跟踪上下文与意图，并据此判断下一步行动。它无需先转录为文本，而是直接推理并执行多步任务，可自主完成多轮问题解决、话题切换和错误恢复。

为什么值得关注？

语音仍是企业最高频的交互渠道，但过去十年的客服自动化始终未能在准确率、响应速度和解决率上达到理想水平。语音推理模型能够大规模弥补这一差距，让复杂、依赖判断的对话也具备自动化条件。这是一种底层架构层面的变革，远不止语音能力的渐进式升级。其应用范围甚至延伸到物理AI领域，语音是机器人和人形机器人的主要交互界面。

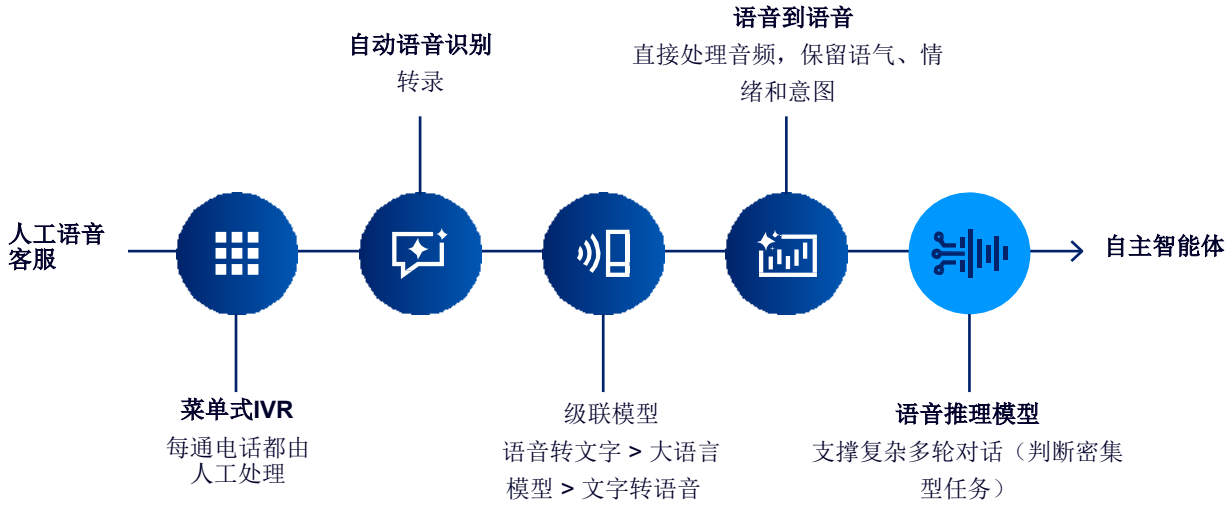
未来将如何发展？

70%

到2030年，超过70%的企业语音交互将由语音模型自主处理，2026年这一比例尚不足10%。

语音演进的阶段

从人工运营到智能体规模化接管



来源：Gartner

趋势2 | 语音推理模型

通过语音推理模型交付业务成果

行动方案：推动模块化自动化与无缝集成

关键步骤	1 制定严格的合规要求	2 按复杂度对需求分级	3 盘点高频交互
预期成果	完成合规就绪度评估	明确自建还是外购策略	建立清晰的标注规范
具体做法	制定严格的知情同意、隐私和审计日志要求，并明确各辖区的责任人。	按交互复杂度对语音场景分类，在低延迟模型与深层推理模型之间合理分流。	开展领域适配前，先对高频录音语音交互进行系统盘点。

关键角色及职责

CIO

主导：制定覆盖客户与员工体验的自主语音交互战略。

优先投入：投资对话式 AI 能力，在提高服务效率的同时，确保用户信任和回答准确性。

治理：明确语音数据的同意、隐私、合规及负责任使用策略。

IT协同方

客户体验与AI团队：设计并部署支持复杂多轮交互的语音推理解决方案。

数据与平台团队：管理语音数据、模型性能及领域专用训练资产。

安全与合规团队：为语音AI交互落实隐私管控、审计日志和治理机制。

业务协同方

市场与传播团队：参与定义语音人设、对话规范和客户信任标准。

客服负责人：发掘高价值应用场景，验证交互质量与问题解决成效。

法务与合规团队：确保各司法辖区均符合知情同意、隐私和监管要求。

趋势3

世界模型

是什么？

世界模型是基于多模态数据训练的计算系统，通过学习抽象表征来理解物理环境和虚拟环境。它能让自主智能体在行动前模拟可能的未来状态、预测结果，并预判自身行为的后果。

为什么值得关注？

语言模型天然缺乏对物理现实、因果关系和空间逻辑的理解能力。世界模型正在逐步突破这一瓶颈，建立以物理规律为先验的范式，让机器理解空间、时间和因果关系。资本正在大量涌入机器人、自动驾驶和空间计算领域，推动这一前沿方向加速发展。

虽然当前高昂的计算成本限制了其通用化部署，但模型训练成本预计将在三年内下降九成，届时企业级仿真应用将具备经济可行性。

未来将如何发展？

到2030年，40%的机器人应用将引入世界模型，支持在自适应环境中实现最优决策，2025年该比例尚不足1%。

世界模型：不同的世界，对应不同的模型

数据科学

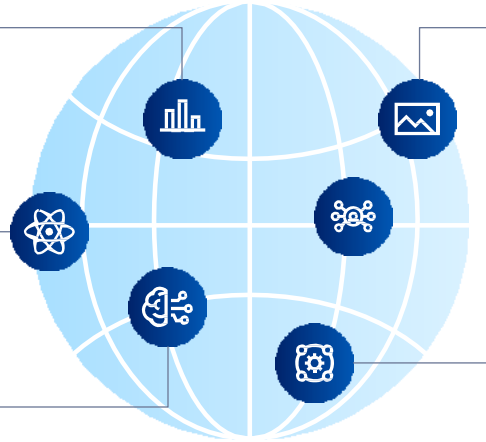
世界可被建模为概率分布。代表技术：MBRL、VAE、MAE、自回归模型、扩散模型

物理学

世界遵循物理规律运行。代表技术：物理仿真器、专家系统

神经科学

世界反映人类认知机制。代表技术：主动推理、认知架构



图形学

世界是一个三维空间。代表技术：空间AI、3DGS

控制论

世界可被建模为动态系统与控制回路。代表技术：MPC、JEPA

社会科学

世界由群体智能驱动。代表技术：复杂系统、多智能体系统

来源：Gartner

趋势3 | 世界模型

通过世界模型交付业务成果

行动方案：推动模块化自动化与无缝集成

关键步骤	1 制定五年路线图	2 验证可量化的商业价值	3 搭建部署落地基础
预期成果	实现智能工业化与预测前瞻能力	增强决策支持与流程优化	决策自动化空前提升
具体做法	系统性地投入资源，推动世界模型走向实际应用。	聚焦流程优化、生产效率和安全保障等高影响、快回报场景。	发挥多模态能力优势，将合成数据接入端到端管道。

关键角色及职责

CIO

主导：制定世界模型的长期战略，推动其在决策、规划与智能自动化中的应用。

投入：建设数据、技术与人才基础，支撑世界模型的大规模工程化部署。

推动：通过预测能力提升、风险降低和运营优化，验证其商业价值。

IT协同方

数据与AI团队：构建支持仿真、预测和自主决策辅助的多模态数据管道。

企业架构团队：搭建可扩展的基础架构，为未来世界模型的部署与集成预留空间。

平台与工程团队：建立健全测试、验证和监控机制，确保模型可靠可信。

业务协同方

业务负责人：发掘情景规划、预测和运营优化方面的高价值应用场景。

运营团队：结合真实业务流程和结果，对模型进行验证。

财务与战略团队：围绕提升韧性、生产力与长期竞争力的方向，提供资金支持。

治理自主智能体平台

依托系统级控制平面，实现可信自主运行

开发者正在部署数字员工，让它们实时生成代码、修复漏洞并执行交易。但机器生产软件的速度已远超团队审计能力，人工审查成为主要瓶颈。这类趋势的核心，是将治理能力下沉到平台层面：通过管控框架与语义上下文引擎，限定自主智能体所能看到、使用和生成的内容。

趋势4

AI上下文平台

是什么？

这项能力负责筛选、整合并提供动态背景知识，让AI智能体能够理解输入、做出决策，并按业务目标采取行动。它把零散的企业知识统一成机器可读的事实层，作为自主数字员工判断与行动的事实根基。

为什么值得关注？

自主数字员工的兴起，暴露出传统数据体系的局限。尽管42%的企业计划在2026年底前部署AI智能体，但目前仅有 22% 的企业通过生成式 AI 实现了可观的业务价值。差距的根源在于运营知识碎片化，由此导致模型频繁出现幻觉，计算成本也居高不下。要避免智能体部署陷入停滞，企业需要部署上下文平台，系统化地梳理业务知识并排定优先级。

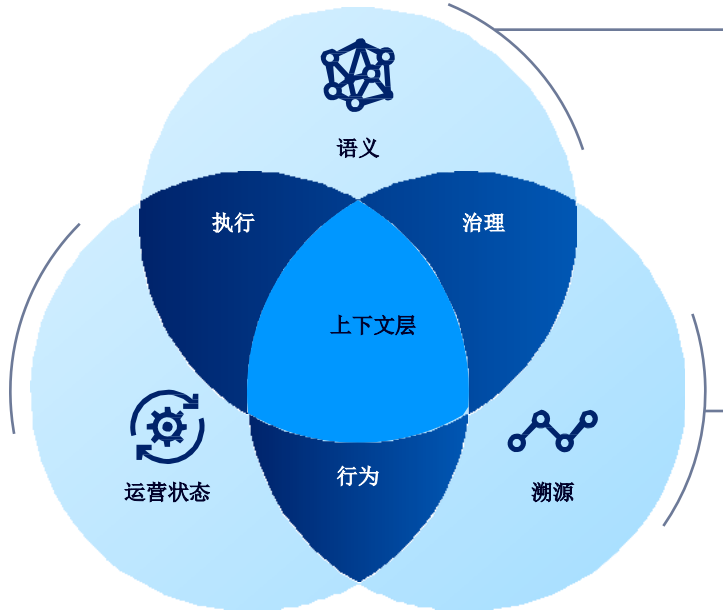
未来将如何发展？

80%　　60%

到2027年，优先做好AI就绪数据语义化的企业，代理型AI准确率最高可提升80%，成本最高可降低60%。

上下文层的三大组成部分

- 实体
- 环境条件
- 适时数据
- 组织知识（RAG）



- 本体/知识图谱
- 指标
- 规则
- 责任归属
- 政策

- 数据跟踪
- 流程
- 决策
- 行动
- 结果

来源：Gartner

趋势4 | AI上下文平台

通过AI上下文平台交付业务成果

行动方案：推动模块化自动化与无缝集成

关键步骤	1 制定分阶段成熟度路线图	2 建立双本体治理架构	3 建立持续双向的责任归属	4 引进知识工程人才
预期成果	从基础能力逐步迈向未来形态的语义与知识体系	AI准确率提升，成本下降	知识可解释、有组织、安全可控	面向AI智能体与人类共享的可信知识，可按需自助获取
具体做法	先把政策集中归拢、统一规范，再推进基于规则的语义自动化。	把被动触发的业务规则，与机器主动生成的决策轨迹分开管理。	IT负责维护基础设施，业务部门负责验证指导性政策。	落实RDF、OWL、SPARQL等关键语义标准。

关键角色及职责

CIO

主导：制定企业级上下文管理战略，支撑可信、可扩展的AI智能体。

投入：建设共享上下文平台，推动AI项目在全公司范围内规模化应用。

治理：明确业务知识、上下文及AI结果的所有权、责任与标准。

IT协同方

数据与AI团队：构建并管理上下文平台，包括语义模型、知识图谱和治理控制。

企业架构：建立AI项目通用的上下文标准，支持复用与跨项目迁移。

安全与治理团队：围绕数据质量、访问权限、数据血缘、审计与合规要求，建立管控机制。

业务协同方

业务领域负责人：制定、校验并持续更新AI智能体所遵循的政策、规则与知识。

运营负责人：发掘高价值的智能体应用场景，确保上下文真实反映当前业务流程与优先级。

风险与合规团队：确保上下文数据符合监管和治理要求。

趋势5

AI编码智能体控制框架

是什么？

该框架是一个贯穿软件开发生命周期的闭环系统，对自主编码智能体实施全流程管控。
它打通编码平台，接入企业上下文，设置模型路由与验证关卡，并建立反馈回路，确保软件交付符合安全与合规要求。

为什么值得关注？

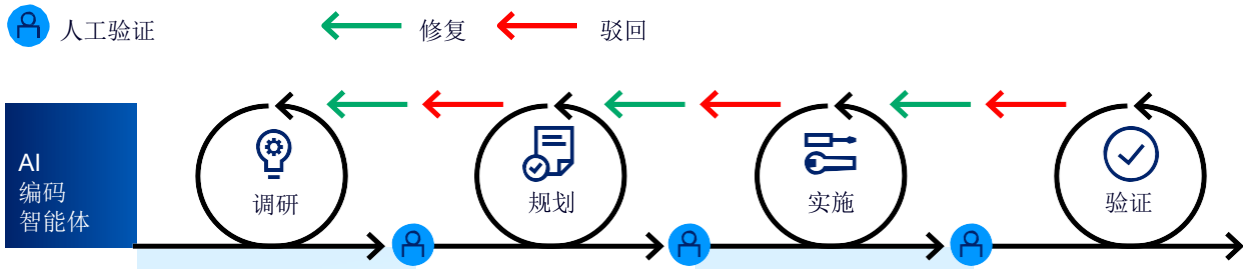
编码智能体正从被动辅助工具，转向独立承担软件生产任务的自主系统。如果只扩大代码生成规模，而验证能力没有同步跟上，真正的难点就不再是写代码，而是如何证明改动安全、正确且可维护。一旦代码生成失去管控，技术债务会快速堆积。部署管控框架，对软件生产体系实施全流程治理，才能持续保持生产力。

未来将如何发展？

20%

到2026年底，20%的公开代码提交将由自主编码智能体完成。
届时，闭环管控框架将成为必需品，否则关键软件交付的质量将无法保障。

AI编码智能体控制框架贯穿软件开发生命周期



	调研	规划	实施	验证
输入	转录文本、照片、录音	已审批的PRD	单一工作单元	可运行软件、PRD
上下文	外部上下文层	外部上下文层	外部上下文层	外部上下文层
输出	产品需求文档（PRD）	大型需求（Epic）、用户故事、任务	可运行软件	实证发现与证据
工具	模型上下文协议（MCP）/命令行界面（CLI）、技能、子智能体	MCP/CLI、技能、子智能体	MCP/CLI、技能、子智能体	MCP/CLI、技能、子智能体

来源：Gartner

趋势5 | AI编程智能体管控框架

通过AI编码智能体控制框架交付业务成果

行动方案：推动模块化自动化与无缝集成

关键步骤	1 明确平台团队为责任主体	2 架构标准与领域规则转成机器可读格式	3 实施自动交付背压机制
预期成果	企业软件交付标准化	每个智能体获得上下文指导	决策自动化空前提升
具体做法	统一设计编码智能体控制框架的配置方式、模型路由规则、允许使用的工具、可复用的流程和验证标准。	维护机器可读输入，形成清晰、结构化的知识文档。	任何代码进入人工审查前，先自动完成代码规范检查、测试、安全扫描和发布文档校验。

关键角色及职责

CIO

主导：将AI原生软件交付确立为企业战略平台能力。

投入：组建专职平台团队，负责控制框架配置、标准制定和日常治理。

治理：明确自主交付在风险、合规和问责方面的具体要求。

IT协同方

平台工程：负责控制框架配置、模型路由、可复用工作流建设，并保障开发者的使用体验。

架构团队：将技术标准、设计模式和内部积累的经验转化为机器可读的上下文资料。

安全与风险：在交付流程中嵌入验证关卡，同时防止管控框架本身被篡改或滥用。

业务协同方

产品负责人：为智能体生成的解决方案制定需求、领域规则和验收标准。

财务：支持平台的长期投入，跟踪评估实际价值回报。

法务与合规：确保自主交付符合监管、审计及政策要求。

趋势6

AI智能体身份

是什么？

AI智能体身份是组织中自主运行数字员工的唯一数字标识，借此统一管控这些数字员工。该框架将模型权重、提示词、凭据等计算复合要素与运行行为关联起来，建立持续信任与人工问责机制。

为什么值得关注？

传统系统缺乏按需授权机制，AI智能体的接入让这一安全短板暴露无遗。如果不尽快把这些自主数字员工纳入安全防护，零信任架构将难以落地，整体自动化投入也会受阻。

这一紧迫的安全危机正推动市场快速整合：大型网络安全厂商通过并购专业的创业公司，构建统一平台，将人与机器的行为纳入同一治理体系。

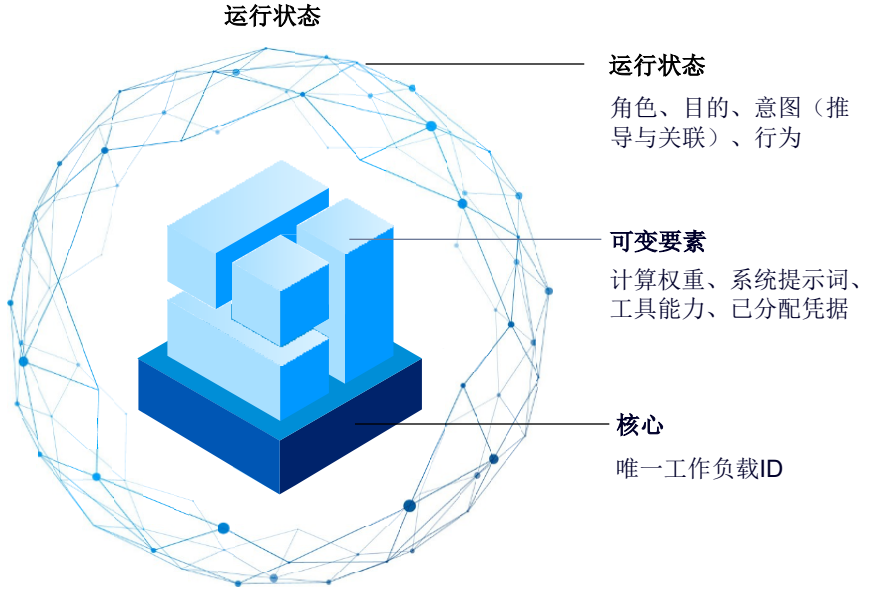
未来将如何发展？

25%

到2028年，因机器权限管理缺位和凭据管理方式陈旧，AI智能体滥用将占企业安全事件的25%。企业如果不能解决身份问题，超过半数的AI项目将全面停摆。

AI智能体身份：从以人为中心到复合身份

AI智能体的身份由可变的计算要素构成，因此需要一套身份模型，将智能体身份与实际运行状态持续关联起来。



来源：Gartner

趋势6 | AI智能体身份

通过AI智能体身份交付业务成果

行动方案：推动模块化自动化与无缝集成

关键步骤	1 盘点所有智能体身份	2 禁止复用人类凭据	3 转向复合身份	4 明确要求统一身份平台
预期成果	发现身份缺口	权责清晰、可审计	控制要求与分类体系明确	形成单一控制平面
具体做法	识别、梳理并管理环境中的受管智能体与影子智能体。	为每个智能体发放独立、专用的凭据。	执行动态、基于策略的访问控制，落实零信任。	与厂商对接，确保人和机器两类工作负载均纳入管理。

关键角色及职责

CIO

主导：制定企业级战略，把AI智能体当作数字员工来治理。

优先投入：投资能统一管理人类、机器和AI智能体身份的安全平台。

治理：明确所有智能体工作负载的问责机制、风险容忍度和所有权归属。

IT协同方

身份与安全：为智能体实施复合身份模型、最小权限访问和持续验证。

企业架构：制定智能体注册、凭据管理和基于策略的授权标准。

基础设施与运维：监控智能体活动，管理运行时控制，支持规模化安全部署。

业务协同方

风险与合规：确保智能体行为符合治理、审计与监管要求。

法务：为智能体的行为和决策权限设定问责框架。

业务负责人：在业务流程中验证智能体的角色、权限与使用边界。

趋势7

自主安全暴露修复

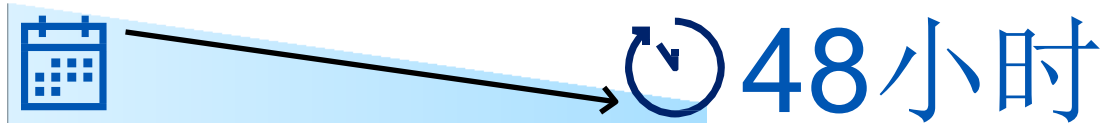
是什么？

这是一套综合能力，借助AI与自动化，发现企业数字环境中的安全漏洞、评估其优先级并执行修复。系统自动向生产环境推送补丁，并建立测试闭环，部署失败时可安全回滚。

为什么值得关注？

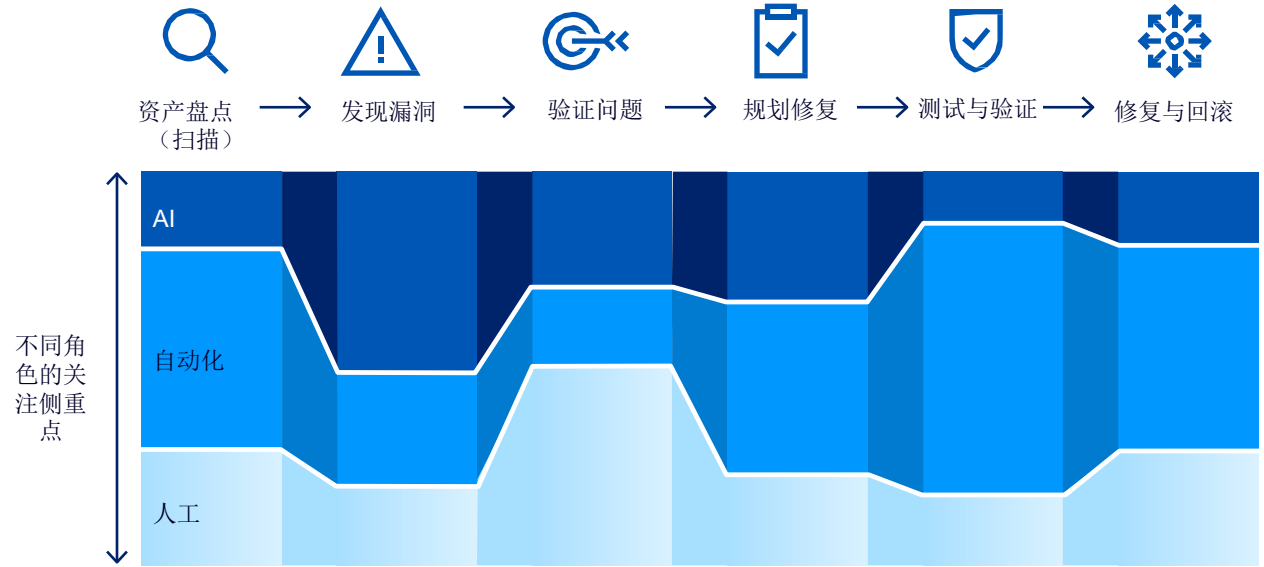
传统防御模式已经失效，漏洞平均要暴露50天才能修补，企业长期处于风险中。用机器速度的持续防御取代缓慢的人工验证，技术负责人便能将漏洞管理从被动处理变为主动防御。

未来将如何发展？



到2031年，采用自主安全暴露修复的企业，可将平均漏洞处置周期从数周压缩至48小时以内。

自主安全暴露修复阶段



来源：Gartner

趋势7 | 自主安全暴露修复

通过自主安全暴露修复交付业务成果

行动方案：推动模块化自动化与无缝集成

关键步骤	1 从小范围项目起步	2 整合漏洞检测能力	3 平衡自动化扫描强度	4 尽早并持续开展成本分析
预期成果	安全测试有保障，能力可长期扩展	漏洞发现量提升	性能与准确率提升	安全预算保持合理可控
具体做法	从非敏感的定制代码库入手，试点自动补丁生成与回滚，积累经验。	将实时修复建议直接嵌入正在运行的开发流程中。	扫描与分级排序协同推进，避免待办漏洞积压，让应用团队不堪重负。	分析计算成本与模型Token消耗，为成本波动较大的安全技术预留预算。

关键角色及职责

CIO

主导：制定自主安全暴露修复路线图，与网络安全和业务韧性目标对齐。

优先投入：投资自动化能力，缩短暴露窗口，提升修复速度。

治理：为自动化修复决策设定风险阈值、监督要求和问责机制。

IT协同方

网络安全：识别优先应用场景，部署AI增强的漏洞发现、验证与修复流程。

软件工程：将自动化测试、修复验证和修复操作嵌入开发流程。

基础设施与运维：提供安全自动化修复所需的部署、监控和回滚能力。

业务协同方

风险与合规：确保修复实践符合治理、监管和审计要求。

产品负责人：在修复优先级、交付目标和运营风险容忍度之间做出合理取舍。

财务：支持提升韧性的相关投入，降低可被利用的安全暴露对业务的影响。

构建可持续敏捷能力

逐步转向主权化、即弃型与有机环境

SaaS疲劳、供应商锁定和能源限制，让完全依赖云的做法成为企业发展的重大隐患。供应商随时可能限制、修改甚至收回其模型，把业务韧性建立在外方控制的模型之上，显然难以为继。当前趋势聚焦于主权架构：法律与技术独立，即弃型技术栈，以及生物计算的早期试点。

趋势8

主权技术

是什么？

主权技术，指在技术与法律层面经过专门架构设计的硬件、软件、数据库和AI模型，确保企业拥有切实可行的供应商退出方案。这类技术永久可用，既防止供应商锁定，又保障运营的连续性。

为什么值得关注？

地缘政治摩擦，以及美国《云法案》等域外法律，随时可能导致云服务被突然切断。DORA等法规在合同层面强制要求云退出方案必须经过验证，CADA也明确规定需采用严格的主权赋能架构。随着AI将大量专业工作自动化，向外国供应商支付的高额订阅费和API调用费，正在造成国内财富外流。

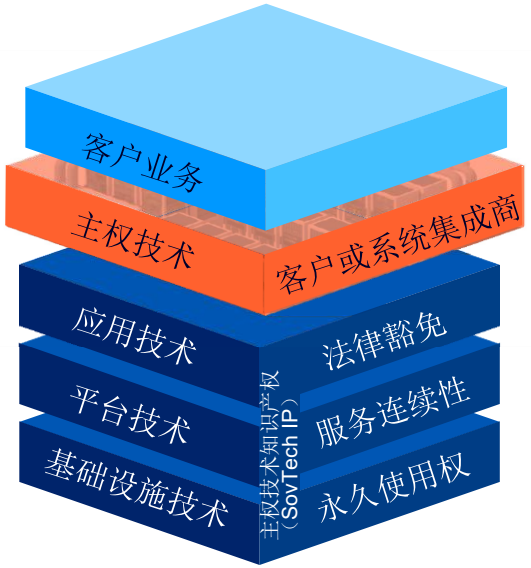
为保障长期业务的连续性，并防止专有数据永久融入外国模型权重，领导者必须从技术与法律两个层面实现独立。

未来将如何发展？

75%

到2030年，超过75%的非美国组织将采用数字主权战略，转移关键工作负载，以降低地缘政治与供应商锁定的风险。

技术主权的构成



主权技术（SovTech）确保：即使供应商撤回其知识产权，本地运营也不会瘫痪；AI创造的价值留在本地；面对危机时，你依然具备独立行动的能力。

是什么？

主权技术（SovTech）涵盖云平台、应用代码、服务器、芯片、数据库、智能体和AI模型等。这些技术在技术与法律层面均经过专门架构设计，一方面使企业具备切实可行的供应商退出路径，另一方面保证其永久可用，以支撑真正的自主与韧性。

来源：Gartner

趋势8 | 主权技术

通过主权技术交付业务成果

行动方案：推动模块化自动化与无缝集成

关键步骤	1 跟踪分布式主权交付模式	2 掌握精益创新策略	3 关注全球主权联盟动态	4 直接与技术供应商对接
预期成果	明确主权需求	多区域运营韧性	把握新兴标准动向	风险暴露最小化
具体做法	评估私有云、本地部署及生态驱动型方案，作为标准公有云的替代。	创造性地使用上一代技术，并与可信盟友共享能力、互通有无。	关注Trusted Tech Alliance (TTA)及欧盟技术主权一揽子计划（EU Tech Sovereignty Package）。	评估供应商是否愿意提供主权交付选项，并作出“无终止开关”承诺。

关键角色及职责

CIO

主导：制定数字主权战略，与业务连续性和运营韧性目标对齐。

优先投入：评估关键技术的依赖关系，制定切实可行的退出与替换策略。

治理：在选择云、AI及技术供应商时，平衡创新、风险与自主性。

IT协同方

企业架构：设计支持可移植、互操作和供应商灵活的系统。

基础设施与云：针对关键工作负载，评估主权、分布式及多伙伴交付模式。

安全与风险：定期测试业务连续性预案，持续跟踪并满足不断更新的主权与韧性合规要求。

业务协同方

采购：评估供应商时，除成本与功能外，还要考察韧性、退出选项及依赖风险。

法务与合规：持续跟踪数据、运营及技术主权相关法规要求。

财务：支持能增强长期韧性、降低单一供应商风险的投资。

趋势9

即弃型应用

是什么？

即弃型应用是为特定业务目的而构建的软件应用。业务目标一旦达成或不再适用，应用便按既定设计主动停用。这类应用按企业级标准运行，但在创建之初就设定了明确的生命周期，不是永久保留的常设系统。

为什么值得关注？

AI驱动的氛围编程大幅降低了软件开发门槛，业务人员和专业开发者都能快速生成定制应用，灵活满足短期运营需求。企业可以部署目的明确、生命周期清晰的临时方案，不再持续积累成本高昂的永久软件资产。

未来将如何发展？

80%

到2030年，SaaS疲劳以及 AI 推动软件供给大幅增长，将迫使领先企业确保80%的新应用皆为即弃型应用且易于替换。

即弃型应用将从根本上改变企业的软件采购、设计与预算方式。企业不再无限期维护遗留平台，应用组合将成为一个动态系统，随冗余资产逐一停用而持续自我更新。

即弃型应用生命周期

来源：Gartner

趋势9 | 即弃型应用

通过即弃型应用交付业务成果

行动方案：推动模块化自动化与无缝集成

关键步骤	1 盘点现有应用组合	2 组建专职平台团队	3 提前布局SaaS合同续约谈判
预期成果	形成应用现代化路线图	建立敏捷的软件生命周期流转机制	规避供应商锁定
具体做法	分类识别核心能力：哪些需要长期自建软件，哪些用临时按需方案即可满足。	统筹监督、治理和管理企业内临时应用资产的流转。	利用续约窗口压缩席位数量、争取开放API权限。

关键角色及职责

CIO

主导：制定即弃型应用战略，使应用生命周期与业务价值对齐。

投入：为支撑应用快速创建与停用的平台、自动化及治理机制提供资源。

治理：明确应用组合中的责任归属、所有权及生命周期标准。

IT协同方

平台工程：提供规模化构建与停用应用所需的工具、管控规则和自动化能力。

企业架构：制定标准，使治理要求与应用的风险水平、业务关键性及预期生命周期相匹配。

安全与运维：负责应用停用、数据生命周期管理及安全控制。

业务协同方

业务负责人：明确应用目标、预期生命周期及停用标准。

财务：调整资金投入方式，支撑应用的创建、续用与停用。

风险与合规：确保治理和控制措施在应用整个生命周期内始终适用。

趋势10

湿件即服务

是什么？

湿件即服务是一种新兴运营模式，通过云端远程接入活体或合成生物系统，将其用于计算任务。这些托管式生物处理器利用生化网络天然的可塑性，以极高能效运行复杂算法。

为什么值得关注？

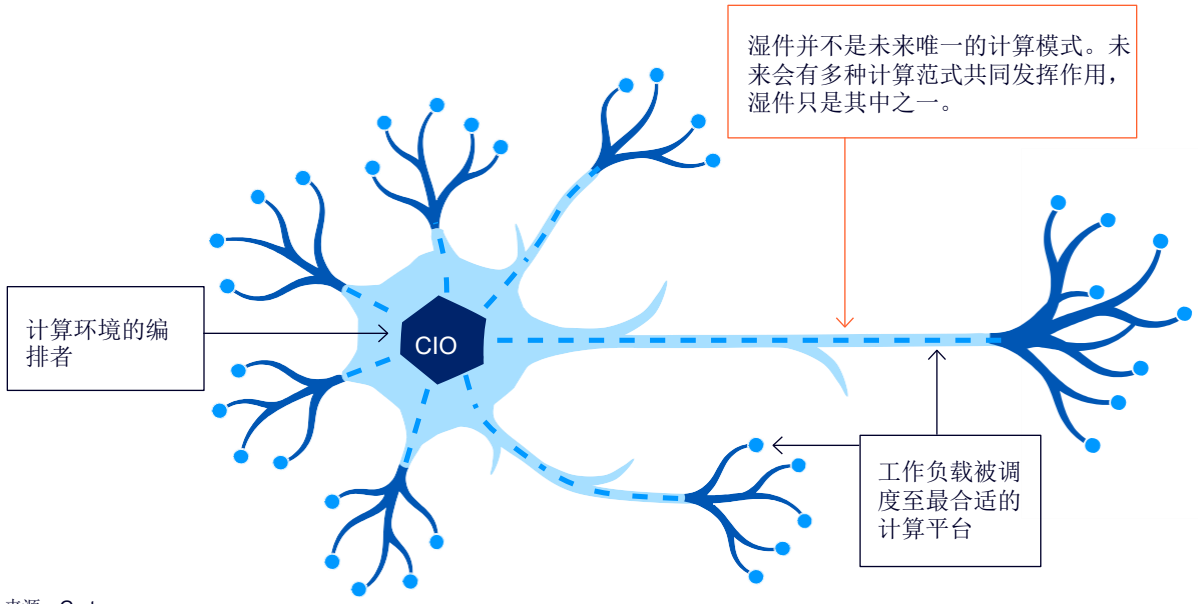
传统的硅基计算硬件无法支撑企业AI无限扩张，
能耗与环境压力都难以为继。实验室培养的生物神经元能以极高效率完成目标导向的计算，运行复杂模式识别算法只需传统服务器的一小部分功耗。初创公司将精密生物计算机托管在远程无菌实验室，填补了从科研到应用之间的空白。生物计算以云订阅服务形式对外提供，企业无需投入高成本的湿实验室或专门的神经运输基础设施，即可快速启动技术试点。

未来将如何发展？

25%

到2030年，25%优先发展专用低功耗AI的企业将部署生物计算，突破传统硅基芯片的算力瓶颈。

湿件即服务：计算编排的一环



来源：Gartner

趋势10 | 湿件即服务

通过湿件即服务交付业务成果

行动方案：推动模块化自动化与无缝集成

关键步骤	1 审计软件架构	2 搭建低风险云沙箱环境	3 组建跨学科工作组	4 制定数据复制与冗余策略
预期成果	识别高回报应用场景	低风险试点验证生物计算机的寿命波动性	弥合人才缺口	建立保护认知数据集与神经权利框架的保障机制
具体做法	筛选出高能耗的模式识别型任务，判断其是否适合转移到低功耗生物计算基底上运行。	利用远程订阅平台，让开发者尽早熟悉活体处理器的使用方式。	整合软件开发者、神经科学家和伦理学家的力量，推动计算机科学与神经科学的融合。	保护关键应用数据，规避细胞寿命波动和处理器突发失效风险。

关键角色及职责

CIO

主导：制定战略，将生物计算融入未来AI与基础设施路线图。

投入：建设编排能力，实现工作负载在多样化计算平台间动态调度。

治理：制定生物计算应用的风险、伦理与韧性框架。

IT协同方

企业架构：识别适合生物处理与混合计算模式的工作负载。

平台工程：构建编排层，统一管理硅基、量子、神经形态及生物处理器的负载路由。

安全与风险：为神经数据隐私、冗余及业务连续性制定防护控制措施。

业务协同方

研究与创新团队：评估生物计算在复杂的优化和探索发现领域的应用可能。

法务与合规：制定伦理使用、知识产权及新兴神经权利相关政策。

财务：支持新一代计算投资。

客观、可执行的洞见

探索IT领导者专属免费资源与工具库：

工具

AI成熟度模型与路线图工具包

评估企业AI成熟度，并获取相关资源以高效制定AI路线图。

了解更多

洞察

2026年生成式AI技术成熟度曲线：把握关键创新时机

在AI战略制定与落地执行中，甄别最值得优先投入的关键创新方向。

了解更多

电子书

《Gartner首席信息官报告》

基于12,000多位CIO同行的调研，了解当前CIO面临的核心挑战。

即刻下载

电子书

《构建 AI 优先的数据与分析体系》

强化数据、分析与AI能力，为组织迎接2030年智能化时代做好准备。

即刻下载

已是Gartner客户？登录客户门户网站，获取更多资源。登录 ↗

联系我们

获取Gartner客观、可执行的商业与技术洞见，助您针对关键优先事项做出更明智的决策，并提升业务绩效。

成为客户

详细了解Gartner的CIO与IT高管服务

gartner.com/cn/chief-information-officer

持续关注，掌握前沿洞察

© 2026 Gartner, Inc.及/或其关联公司版权所有。保留所有权利。GTS_542668

Gartner®