Gartner

2026年十大战略技术趋势



驾驭智能互联世界

2026年对于科技领导者而言，将是至关重要的转折之年——颠覆、创新与风险以前所未有的速度加速并行。Gartner发布的《2026年十大战略科技趋势》不仅仅是技术上的变革，更是推动业务转型的催化力量，需要高层管理者作出积极响应。

今年的趋势反映出一个由AI驱动、万物互联的现实格局，单靠某一项能力已无法应对复杂挑战。Gartner将这些趋势归纳为三大主题，揭示领先企业在创新、竞争与价值守护方面的未来路径：

架构者（The Architect）

借助AI原生开发平台、AI超级计算和机密计算，构建安全、可扩展且自适应的数字基础。

整合者（The Synthesist）

整合多元技术——从多智能体系统、领域专用语言模型到物理AI，以开辟新的价值增长空间。

守卫者（The Vanguard）

以主动式网络安全、数字溯源、AI安全平台与“地缘回迁”（Geopatriation）等手段，提升信任、治理与安全水平。

在深入了解这些趋势的同时，请思考它们如何与企业的战略目标相匹配，以及如何将其纳入规划，助力可持续增长并建立竞争优势。



Gene Alvarez
Gartner业务与技术洞察杰出副总裁

《Gartner 2026年重要战略技术趋势》

这十大战略趋势的评选依据是其在智能互联世界中推动创新、增强韧性和提升信任的潜力。

这些趋势是技术领导者亟需深度思考，并积极采取行动的战略要务。



架构者

1. AI原生开发平台
2. AI超级计算平台
3. 机密计算

整合者

4. 多智能体系统
5. 特定领域语言模型
6. 物理AI

守卫者

7. 前置式主动网络安全
8. 数字溯源
9. AI安全平台
10. 地缘回迁



架构者

构建安全、可扩展且自适应的数字基础。

为了加速创新并增强韧性，科技领导者必须推动平台与基础设施的现代化建设。“架构者”类趋势聚焦于打造AI就绪的数字基础，以实现高速、安全与可扩展性——这些都是企业在智能互联世界中蓬勃发展的关键因素。

1

AI原生开发平台

核心概念

AI原生开发平台借助生成式AI，使得软件开发变得前所未有的快速和高效。这类平台形式多样，包括可通过单次提示生成完整软件的“一次性”生成工具，无需深厚技术知识也能进行软件开发的“氛围编码”工具，以及由多个AI智能体协同开发软件的系统。

趋势成因

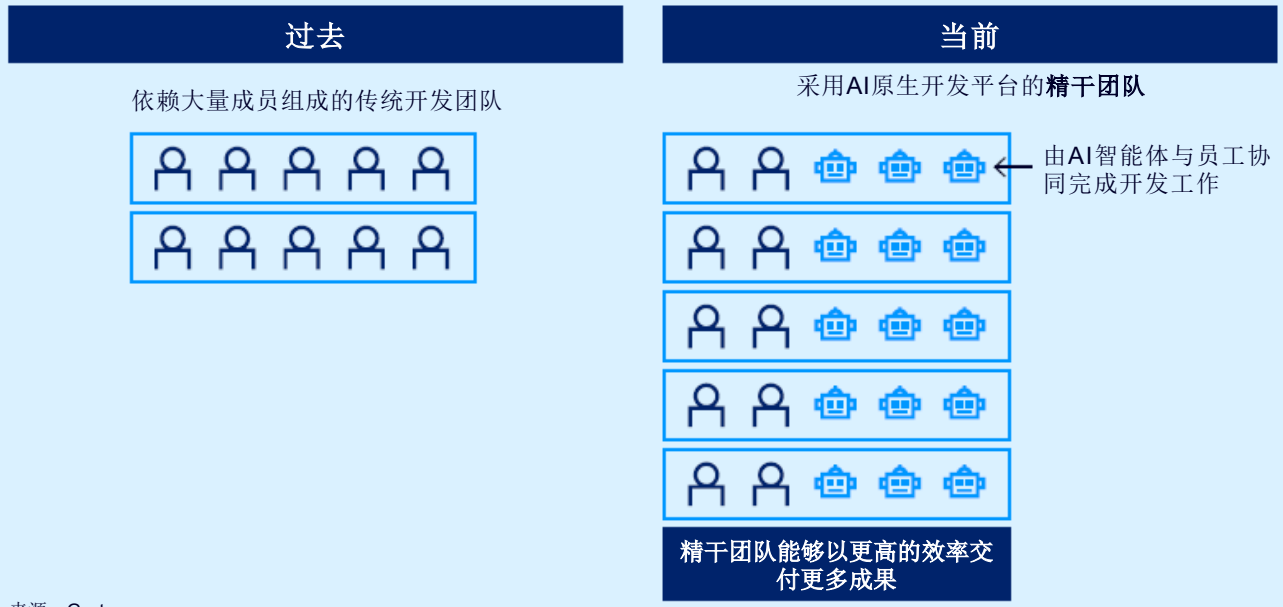
CIO（首席信息官）重视在交付速度与生产力方面的显著提升；CEO与CFO则聚焦成本节约。AI原生开发平台可赋能“精干团队”（Tiny Teams）以同等资源开发更多应用。例如，5个两人团队能够同时交付5个应用。这一趋势有助于CIO缓解开发积压问题，并使“自建”成为比“采购”更具吸引力的选项。

未来展望

80% 的企业将在2030年前将大型软件工程团队转变为AI增强型小团队。

40% 的企业应用组合将在2030年纳入使用AI原生平台构建的定制化应用（2025年这一比例仅为2%）。

精干团队



来源：Gartner

1



利用AI原生开发平台推动成果落地

提升速度、节约成本、激发创新的行动计划

步骤	1 建立平台团队	2 落实安全防护机制	3 试点AI原生开发	4 采用AI优先思维	5 提升团队能力
预期成果	集中监管确保标准一致和治理到位。	降低不安全或不合规代码的风险。	取得快速成果，验证价值并建立信心。	加速交付并提升创新能力。	推动广泛采用与高效协作。
行动	组建专门团队，负责管理AI原生平台，并筛选AI模型。	集成AI治理平台，用于代码审查与合规检查。	从低风险项目入手，检验生产力提升效果。	将AI原生工具优先应用于新开发项目。	对开发人员与业务伙伴进行提示词工程与治理相关培训。

确保成功落地的关键岗位

CIO

战略协作：制定AI优先战略与治理框架。

协同推进：协调平台能力与业务优先级对齐。

治理监管：确保AI原生开发的合规与安全。

IT合作伙伴

平台工程：管理AI原生工具、集成与性能。

安全管理：建立AI代码审查与风险管理治理框架。

采购支持：评估与筛选AI原生平台供应商及服务。

业务合作伙伴

产品负责人：提供领域专业知识并检验AI解决方案。

财务：调整资金配置模式以支持AI原生开发项目。

2

AI超级计算平台

核心概念
AI超级计算平台提供训练与运行先进AI模型所需的超大规模算力。此类系统集成了高性能计算（HPC）、专用处理器以及可扩展架构，用以处理数据密集型工作负载。

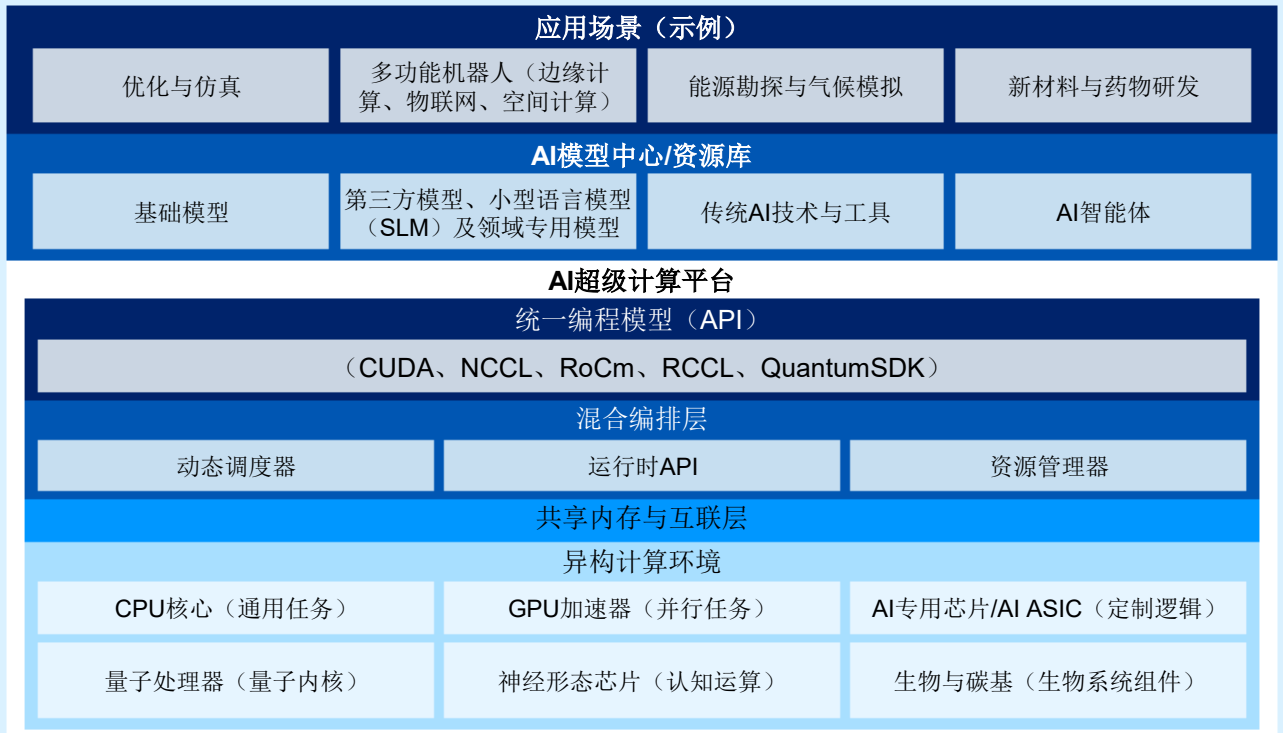
趋势成
随着AI模型开发的规模更大、复杂度更高，传统基础设施难已经难以满足需求，因此对AI超级计算的需求正在激增。

未来展望

40% 的企业将在2028年前采用混合计算架构（当前仅为8%）。

20+ 家供应商将在2028年前提供基于超级计算环境的统一开发平台。

AI超级计算平台



来源：Gartner

2

利用AI超级计算平台推动成果落地

释放海量处理能力的行动计划

步骤	1 识别高影响力工作负载	2 投资统一软件栈	3 制定分阶段集成策略	4 简化跨环境开发流程	5 制定治理与合规计划
预期成果	展示价值，构建内部专业能力。	简化整合流程，实现灵活的工作负载部署。	构建面向未来的基础设施与团队。	加速交付，减少摩擦。	降低风险，强化监管。
行动	通过混合编排策略开展试点项目。	采用适用于传统与新兴系统的开放标准。	分阶段引入新计算模式，并培训IT人员。	鼓励团队采用混合平台与可组合架构。	在系统层面设计安全与合规策略。

确保成功落地的关键岗位

CIO

制定与业务优先级匹配的混合编排战略。

保障工作负载部署、安全性与合规性治理。

与业务领导者**协作**，优先聚焦高影响力任务。

IT合作伙伴

基础设施与运维：将新兴加速器集成至遗留系统。

安全：实施多架构环境治理。

DevOps：采用统一的软件栈与编排工具。

业务合作伙伴

产品：识别混合计算的应用场景（如仿真、AI应用程序）。

财务：调整资金配置，支持分阶段集成与可持续目标。

运营：筹备在关键流程部署AI工作流。

3

机密计算

核心概念

机密计算通过基于硬件的可信执行环境（TEE），在数据处理过程中提供保护，防止未经授权的访问——包括云服务供应商。

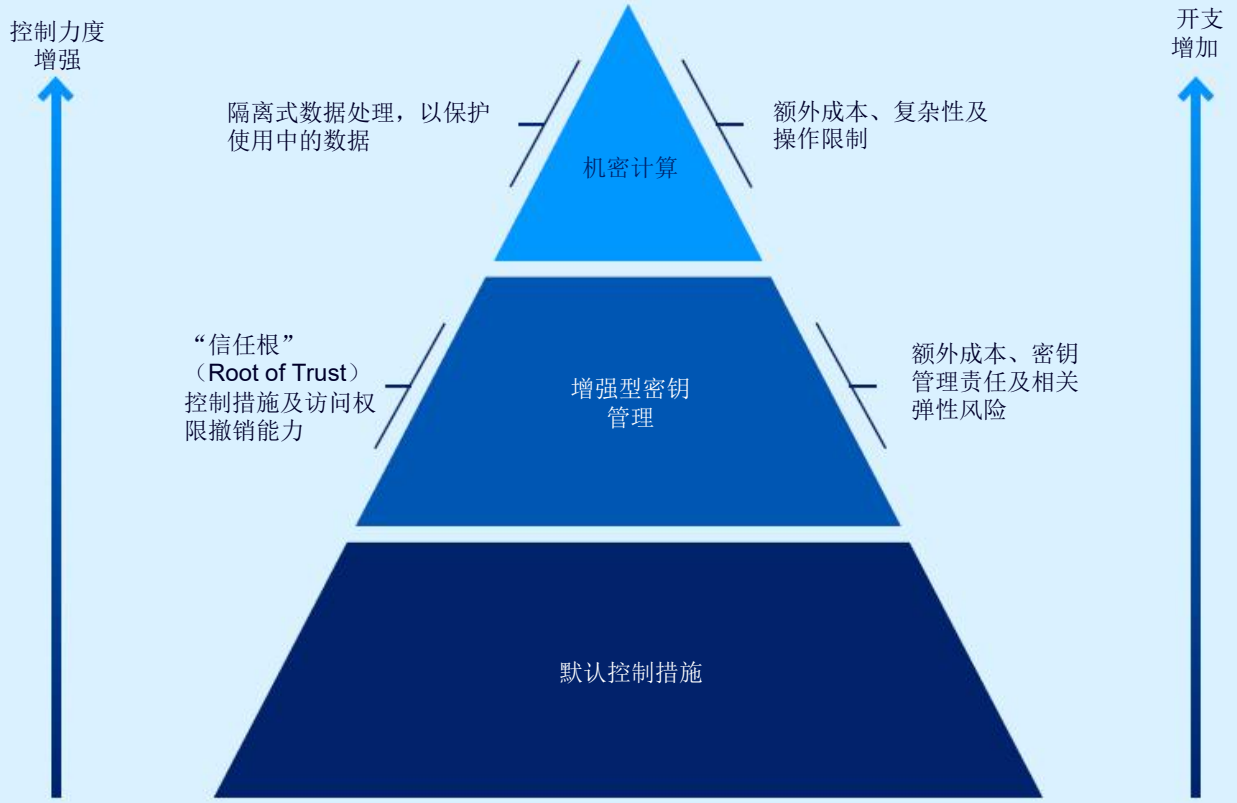
趋势成因

鉴于日益严格的隐私法规、数据本地化要求以及AI应用的普及，这使得企业对数据使用过程中的安全保障变得尤为关键。机密计算可为敏感工作负载提供安全的云端处理方式，并支持合规性管理。

未来展望

75% 在不受信任的基础设施上进行的数据处理将在2029年前通过机密计算加以保护。

云服务供应商（CSP）数据访问控制措施



来源：Gartner

3



利用机密计算推动成果落地

确保全场景安全合规数据处理的行动计划

步骤	1 审查敏感工作负载	2 在AI模型上测试TEE	3 开展安全协作	4 实施独立的密钥管理	5 准备好应对集成挑战
预期成果	明确需实施使用中数据保护的应用场景。	增强机密性与知识产权保护。	在不泄露原始数据的前提下实现数据洞见共享。	全面掌控数据访问权限。	实现跨环境无缝部署。
行动	梳理受隐私或数据本地化法规约束的工作负载。	在自有与开源AI模型上测试TEE。	在分析与商业智能（BI）项目中应用机密计算。	部署企业自有的加密密钥管理系统。	制定多芯片组、多供应商间的协同编排计划。

确保成功落地的关键岗位

CIO

制定符合隐私、合规及云战略目标的机密计算策略。

协同法务与合规团队，满足数据本地化与数据主权要求。

监督TEE治理，确保其与现有安全框架集成。

IT合作伙伴

基础设施与运维：在混合云及多云环境中部署TEE。

安全：实施认证流程与加密密钥管理。

DevOps与平台：调整工作负载以适配机密计算，并监测性能。

业务合作伙伴

合规：确认法规遵循情况并确保审计就绪。

财务：为机密计算部署与风险缓解配置资金。

数据负责人：识别需提供“使用中保护”的敏感工作负载并确定项目优先级。



整合者

统筹多元技术，创造新价值。

为开辟差异化优势，技术领导者必须整合专业化模型、多智能体系统与物理AI，打造领域专属解决方案。“整合者”类趋势着眼于编排多种技术，打造自适应、智能化的生态系统，从而推动跨工作流、产品与体验的创新。

4

多智能体系统

核心概念

多智能体系统（MAS）通过多个专业AI智能体的协同合作，完成复杂工作流。每个智能体各司其职，与单体式AI解决方案相比，MAS显著提升了效率与可扩展性。

趋势成因

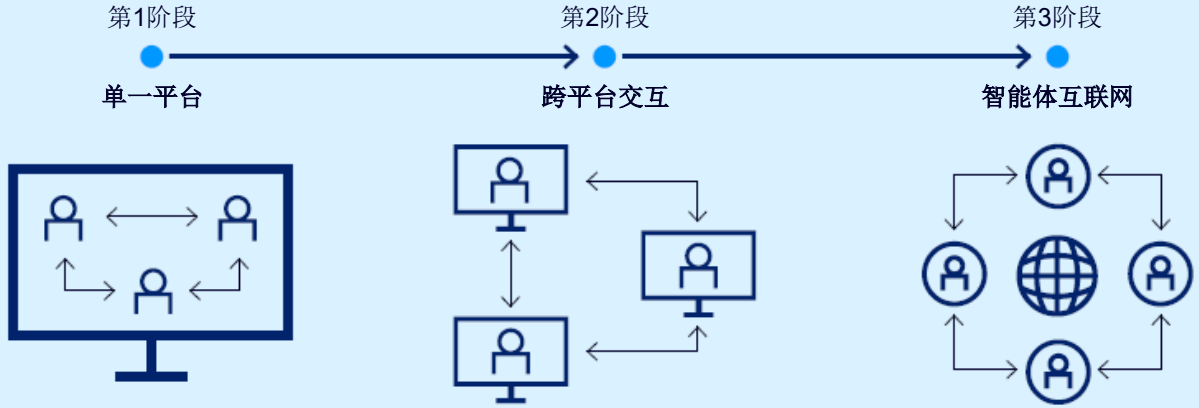
单智能体AI在多步骤任务中表现受限，而MAS提供了模块化自动化与跨平台集成的新路径。Gartner数据显示，从2024年第一季度到2025年第二季度，关于MAS的咨询量激增1445%，表明企业对此领域的兴趣正快速攀升。

未来展望

70% 的MAS将在2027年前采用高度专业化的智能体，在提升准确度的同时协调复杂性也将增加。

60% 的MAS将在2028年前支持多供应商互操作，推动创新并提升灵活性。

多智能体系统的演进历程



来源：Gartner

4



利用多智能体系统推动成果落地

驱动模块化自动化与无缝集成的行动计划

步骤	1 识别高价值应用场景	2 设计模块化智能体	3 落实治理与可观测性技术	4 采用互操作性标准	5 提升团队技能
预期成果	产生可量化的影响并加速推广应用。	提升可靠性与可扩展性。	降低风险并强化控制。	投资具备前瞻性的MAS项目。	实现高效部署与风险管控。
行动	从定义明确的工作流入手，开展MAS试点项目。	构建专业化智能体，而非单体式解决方案。	采用严格的API治理与监控工具。	利用新兴协议实现多供应商智能体协作。	对团队进行MAS框架与变革管理培训。

确保成功落地的关键岗位

CIO

制定针对高价值工作流的MAS战略，并与业务重点保持一致。

落实智能体互操作性、安全性与合规性治理。

传达变革管理计划，应对员工关切。

IT合作伙伴

平台与DevOps：设计模块化智能体并管理编排工具。

安全：实施API治理，并监控智能体交互。

集成团队：采用互操作性及可观测性标准。

业务合作伙伴

流程负责人：确定MAS试点工作流并检验成果。

财务：管理不可预测成本并为可观测性工具提供资金。

运营：支持人机协作与培训项目。

5

特定领域语言模型

核心概念

特定领域语言模型（DSLM）是基于特定行业或业务功能数据集训练的AI模型，相比通用大语言模型，能提供更高准确性与合规性。

趋势成因

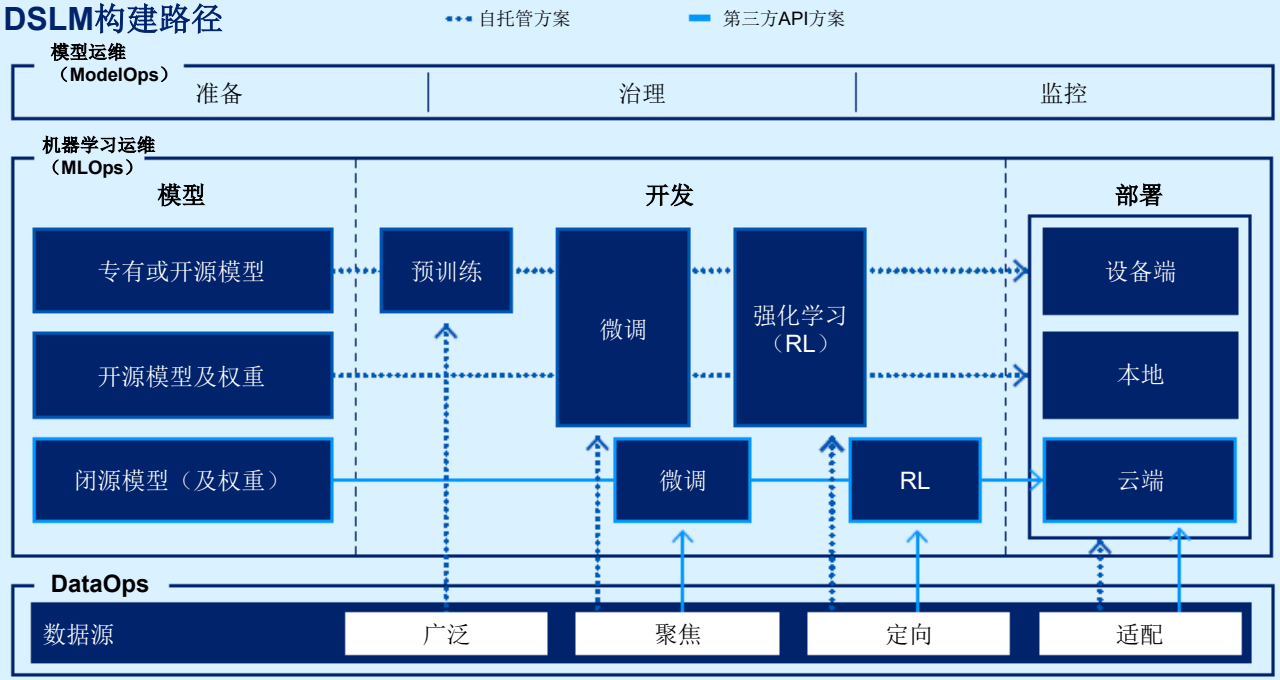
CIO追求可量化的AI商业价值。DSLM在金融、医疗、人力资源等关键工作流中能有效减少错误、加速部署并降低成本。

未来展望

+60% 的企业级生成式AI模型将在2028年前实现领域专用化。

30% 的生成式AI工作负载将在2028年前在本地或设备端运行DSLM。

DSLM构建路径



来源：Gartner

5

利用DSLM推动成果落地

实现专业领域精准合规的行动计划

步骤	1 识别高影响力应用场景	2 加强数据治理	3 开展关键领域DSLM试点	4 组建跨职能团队	5 监测优化
预期成果	加速投资回报（ROI）并提升准确性。	确保DSLM输出可靠合规。	展示能够量化的业务成果。	实现平滑集成与应用。	保持可持续性能与成本控制。
行动	锁定通用大语言模型（LLM）表现欠佳的工作流。	实施严格的隐私与质量控制。	从金融、医疗或人力资源流程入手。	吸纳IT、业务专家（SME）及合规人员参与DSLM项目。	应用可解释性与合规性框架。

确保成功落地的关键岗位

CIO

制定受监管及高价值领域的DSLM战略。

保障准确性、合规性与可解释性治理。

将DSLM应用与ROI及风险管理目标**对齐**。

IT合作伙伴

数据与分析：构建领域专用数据集并保障质量。

ModelOps：管理模型微调、监测与全生命周期治理。

安全：确保DSLM部署符合隐私与合规要求。

业务合作伙伴

领域专家：验证DSLM输出的准确性与相关性。

财务：规划DSLM实施预算并优化成本。

合规：确保符合监管标准。

6

物理AI

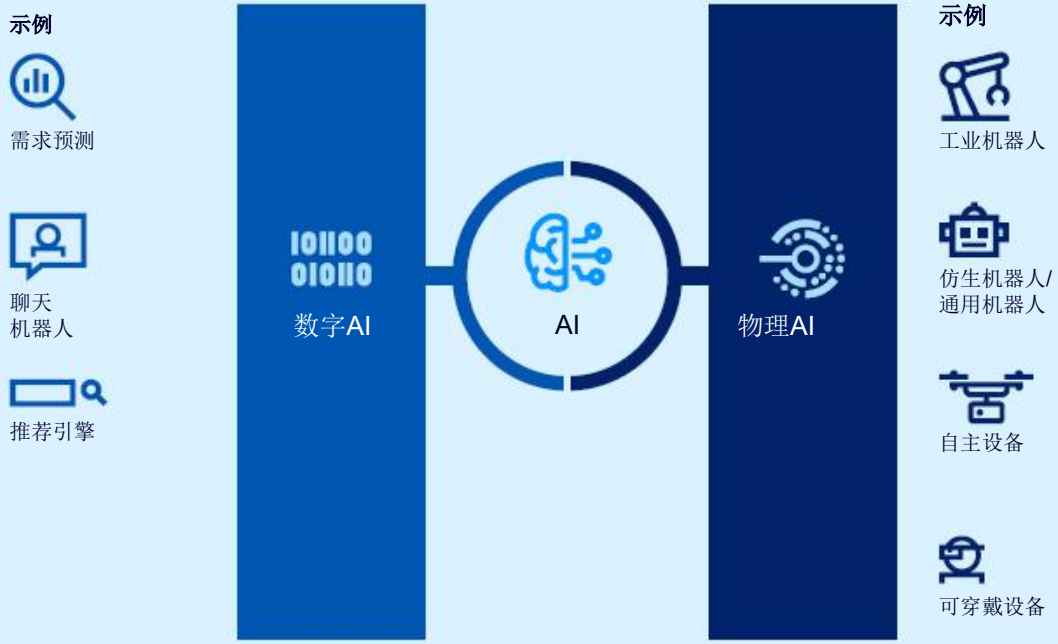
核心概念
物理AI通过具备感知、决策与行动能力的机器人、无人机、汽车及智能设备，将智能带入现实世界。这些集成了传感器、执行器与AI模型的系统，能够自动化执行物理任务。

趋势成因
各类企业正致力于将数字AI的生产力优势延伸至实体环境。预计到2028年，全球前十名AI供应商中将有五家推出物理AI产品。

未来展望

80% 的仓储设施将在2028年前采用机器人或自动化技术。

AI分类



来源：Gartner

利用物理AI推动成果落地

推动实体任务自动化与全场景效能提升的行动计划

步骤	1 评估业务运营场景	2 开展物理AI系统试点	3 组建跨职能团队	4 向利益相关方普及相关概念	5 规划多智能体协同
预期成果	明确可自动化领域与成本节约空间。	验证性能与ROI。	实现高效治理与融合。	避免概念混淆与投资错配。	开展前瞻性部署。
行动	聚焦物流、维护及安全工作流。	实地部署前采用仿真与数字孪生技术进行验证。	在规划阶段纳入IT、运营与工程团队。	厘清物理AI、嵌入式AI与边缘AI的界限。	探索设备集群编排平台。

确保成功落地的关键岗位

CIO

制定与运营目标契合的物理AI战略。

保障安全性、可靠性及可解释性治理。

协同运营与工程团队，推进集成与风险管理。

IT合作伙伴

基础设施与运维：将物理AI与物联网及遗留系统集成。

安全：构建自主系统安全防护体系。

数据与分析：支持仿真与数字孪生测试。

业务合作伙伴

运营：识别高价值应用场景并验证性能。

财务：为机器人及自动化投资项目规划预算。

合规：确保符合安全与监管标准。



守卫者

强化信任、治理与安全。

在风险攀升与监管趋严的时代，信任已成为不可妥协的底线。“守卫者”类趋势聚焦于主动安全、透明治理与数字诚信——助力企业在规模化应用AI和推进数字化转型的同时，保护声誉、确保合规并稳固利益相关方信心。

7

前置式主动网络安全

核心概念

前置式主动网络安全（PCS）采用先进的AI技术，在网络攻击发生前进行预测、干扰与化解，超越传统“检测—响应”的被动防御模式。

趋势成因

AI驱动的威胁正呈指数级增长，目标涵盖网络、应用及物联网系统。到2029年，缺乏主动式安全能力的技术产品将丧失市场竞争力，主动防御将成为行业的基本要求。

未来展望

50% 的安全软件支出将在2030年前流向主动式解决方案。

1M 到2030年，每年记录在案的网络漏洞预计将突破100万。

主动式网络安全的“三D”要素



来源：Gartner

7



利用前置式主动网络安全推动成果落地

实现预防性关键资产保护的行动计划

步骤	1 评估现有安全架构	2 在高风险领域试点PCS	3 制定供应商选择标准	4 推广PCS战略	5 将PCS与现有工具整合
预期成果	识别漏洞并确定PCS投资优先级。	展示可量化的风险降低成效。	确保PCS应用方案具备前瞻性。	获取高层与董事会支持。	最大化ROI并加速应用。
行动	开展风险分析与就绪度评估。	部署预测性威胁预防与诱骗技术。	要求提供详细的主动式防御能力路线图。	传达PCS的业务影响与ROI。	将PCS与当前安全合规流程相结合。

确保成功落地的关键岗位

CIO

主导从被动响应向主动防御的安全战略转型。

制定PCS能力采购标准并提升高层认知。

监督主动防御措施并确保其合规。

IT合作伙伴

安全：部署预测性威胁预防与诱骗技术。

基础设施与运维：将PCS与云端、运营技术及信息物理系统集成。

风险与合规：确保符合隐私及监管标准。

业务合作伙伴

财务：为PCS试点与长期部署项目分配预算。

运营：支持安全的数字化转型项目。

产品：将主动式安全能力嵌入产品，实现市场差异化。

8

数字溯源

核心概念

数字溯源技术通过材料清单（BOM表）、认证数据库和水印等工具，对软件、数据及媒体内容的来源与完整性进行验证，从而确保包含第三方组件或AI生成内容的系统具备透明性与可信度。

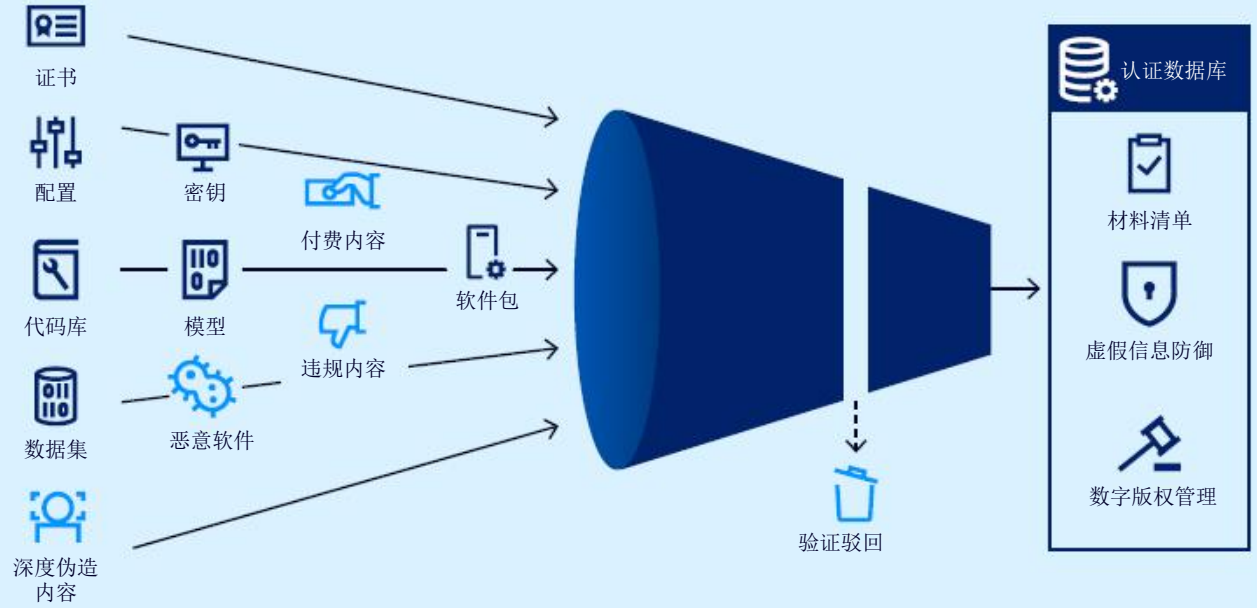
趋势成因

企业正面临各种各样的风险：代码篡改、遭到废弃的开源项目、以及由深度伪造技术引发的信息失真。

未来展望

随着监管要求（如欧盟《人工智能法案》）逐步落地，对AI生成内容进行水印标记与溯源将成为刚需。

数字溯源筛选流程



来源：Gartner

8

利用数字溯源推动成果落地

通过验证数据与内容真实性建立信任的行动计划

步骤	1 建立BOM表	2 建立认证数据库	3 采用虚假信息安全工具	4 应用数字水印技术	5 加强治理
预期成果	实现软件溯源与安全透明。	建立集中、可信的溯源记录。	防范身份伪造与欺诈行为。	满足AI内容监管要求。	降低法律与声誉风险。
行动	为软件项目建立软件材料清单（SBOM），为AI模型制定相应的机器学习材料清单（MLBOM）。	存储经加密签名的来源凭证。	将合成身份检测技术集成至身份威胁检测与响应计划。	以机器可读格式标注AI生成的媒体内容。	推动IT、合规与市场团队协同治理。

确保成功落地的关键岗位

CIO

制定满足合规与风险管理需求的数字溯源战略。

监督BOM表与认证数据库的落地实施。

与首席信息安全官（CISO）和首席市场官（CMO）**协作**，应对虚假信息并维护声誉。

IT合作伙伴

DevOps：将SBOM与MLBOM融入交付流程。

安全：部署虚假信息安全工具与数字版权管理（DRM）。

数据：记录AI模型训练数据谱系。

业务合作伙伴

合规：确保符合新兴监管要求。

法务：核实版权与许可合规性。

市场：管控深度伪造及合成内容引发的声誉风险。

9

AI安全平台

核心概念
AI安全平台（AISP）通过整合式管控机制，为第三方AI服务与自建AI应用提供安全保障，可应对提示词注入、智能体异常行为、数据泄露等AI原生风险。

趋势成因
随着AI应用的普及，传统安全工具已无法有效保护AI工作流程。

未来展望

+50% 的企业将在2028年前采用AISP。

80% 的未授权AI操作将源于内部政策违规，而非外部攻击。

AI安全平台能力图谱



来源：Gartner

9

利用AI安全平台推动成果落地

保障AI驱动业务稳健运营的行动计划

步骤	1 评估整体AI风险态势	2 开展AISP试点项目	3 优选统一平台	4 集成安全测试	5 关注厂商创新
预期成果	识别现有安全栈的漏洞。	验证方案成效与ROI。	简化管理并降低复杂度。	提高对提示词注入攻击的防御能力。	提前部署，应对新兴威胁。
行动	全面排查各流程的AI原生风险。	从高风险AI服务及自建应用入手。	选择同时支持AI使用管控与应用安全的AISP。	将自动化AI安全测试嵌入流程。	追踪初创企业及头部厂商的功能创新。

确保成功落地的关键岗位

CIO

制定涵盖第三方与自建AI应用的AI安全战略。

选择提供统一AI使用管控与应用安全功能的供应商。

向董事会**传达**AI风险态势与合规要求。

IT合作伙伴

安全：部署防护措施，防范提示词注入并检测智能体异常行为。

DevOps：将AI安全测试集成至开发流程。

基础设施与运维：确保平台兼容云端与本地环境。

业务合作伙伴

合规：确保AISP符合欧盟《人工智能法案》等监管框架。

财务：为平台部署与风险缓解规划预算。

产品：将安全功能嵌入AI驱动型产品。

10

地缘回迁

核心概念

“地缘回迁”（Geopatriation）是指将工作负载从全球超大规模云平台迁移至主权云或本地环境，以降低地缘政治风险。其策略包括将工作负载部署至主权云区域，或回迁至本地部署环境。

趋势成因

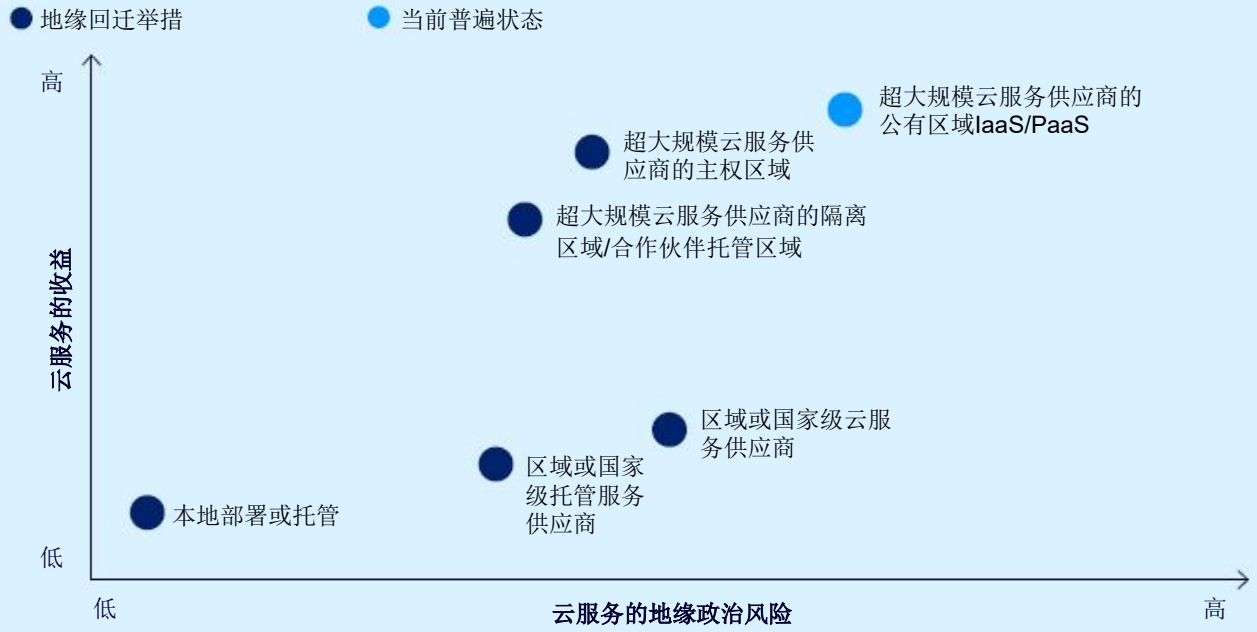
地缘政治动荡与监管要求正推动企业重新评估自身对云服务的依赖程度。

未来展望

75% 的企业将在2030年前开展工作负载的地缘回迁。

超大规模云服务供应商与本地供应商正迅速增加其主权云产品。

云服务的收益与地缘政治风险对比



来源：Gartner

10

利用地缘回迁推动成果落地

将关键数字工作负载本地化、以降低风险的行动计划

步骤	1 评估工作负载的重要性	2 评估主权云方案	3 制定混合部署战略	4 落实治理管控措施	5 跟踪地缘政治动态
预期成果	优先回迁高风险资产。	平衡敏捷性与主权要求。	维持韧性与性能。	降低合规与安全风险。	动态调整战略。
行动	根据敏感度与地缘风险暴露程度对工作负载进行评分。	比较超大规模云厂商的主权云方案与本地供应商方案。	结合主权云与本地部署/托管。	采用认证与主权治理框架。	根据风险环境变化，动态调整工作负载部署。

确保成功落地的关键岗位

CIO

制定平衡主权要求、敏捷性与韧性的地缘回迁战略。

评估本地供应商方案与全球超大规模云厂商主权云方案的优劣。

管理关键工作负载的风险评分工作，并确保其合规。

IT合作伙伴

基础设施与运维：规划迁移路径，并制定与遗留系统集成的方案。

安全：验证主权控制措施并确保合规性。

云架构师：优化工作负载布局以保障性能与韧性。

业务合作伙伴

合规：关注监管政策变化与主权要求。

财务：为迁移成本与风险缓解投资项目规划预算。

运营：保障工作负载迁移期间的业务连续性。

客观、可执行的洞察

探寻为IT领导者提供的其他免费资源和工具：



模板

《制定IT战略计划》

利用这份单页规划模板，将战略转化为实际行动。

获取模板



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

2025年Gartner Hype Cycle™技术成熟度曲线

《2025年人工智能技术成熟度曲线：突破生成式AI热潮》

立即阅读



研讨会

洞察AI重塑未来工作，激活人机协同组织进化

助您成功应对人工智能浪潮的挑战，构建以以人为本为核心的可持续新范式。

报名参会

您已经是Gartner客户？
通过Gartner客户服务平台获取更多资源。登录↗

联系我们

获取客观公正、切实可行的商业与技术洞见，驱动关键任务领域的智慧决策与卓越绩效。

成为客户

详细了解Gartner的CIO与IT高管服务

gartner.com/cn/chief-information-officer

©2025 Gartner, Inc.及/或其关联公司版权所有。保留所有权利。CM_GTS_4062400

Gartner