

Gartner®

2024年重要战略 技术趋势

10

Gartner 2024年十大战略 技术趋势

1. 与AI合作：AI信任、风险和安全管理（AI TRiSM）
2. 保障安全：持续威胁暴露面管理（CTEM）
3. 守护未来：可持续技术
4. 开发人员驱动的自助服务：平台工程
5. 加速创造：AI增强开发
6. 定制化解决方案的进一步定制化：行业云平台
7. 优化决策：智能应用
8. 权力与责任：生成式AI全民化
9. 助力先行者：增强型互联员工队伍
10. 字节组成的买家：机器客户

Gartner重要战略 技术趋势研究，助力 企业在AI时代优化 技术投资

在这个人工智能（AI）技术飞速发展的时代，Gartner重要战略技术趋势收录的创新技术可以帮助企业机构在创造价值的同时，构建强大能力并保障自身安全。

这些创新技术部分由AI驱动，其他则旨在帮助企业机构实现高效、安全的运营和增长，适应AI的发展给客户期望和业务模式带来的新变化。

无论是否已领先一步对这些技术有所涉猎，企业机构都可以利用其构建符合自身及员工需求的基础设施、治理机制和工具，以提高自身的韧性和自主性。如使用得当，这些技术将为企业机构带来以下优势：

- 建立信任和信心，安全地使用AI
- 提高在所处生态系统中运营活动的可持续性
- 选择适合的技术，满足具体任务、行业和功能的需求
- 提高效率和生产力，同时减少所需投资或工作量
- 为内外部利益相关方创造更多价值

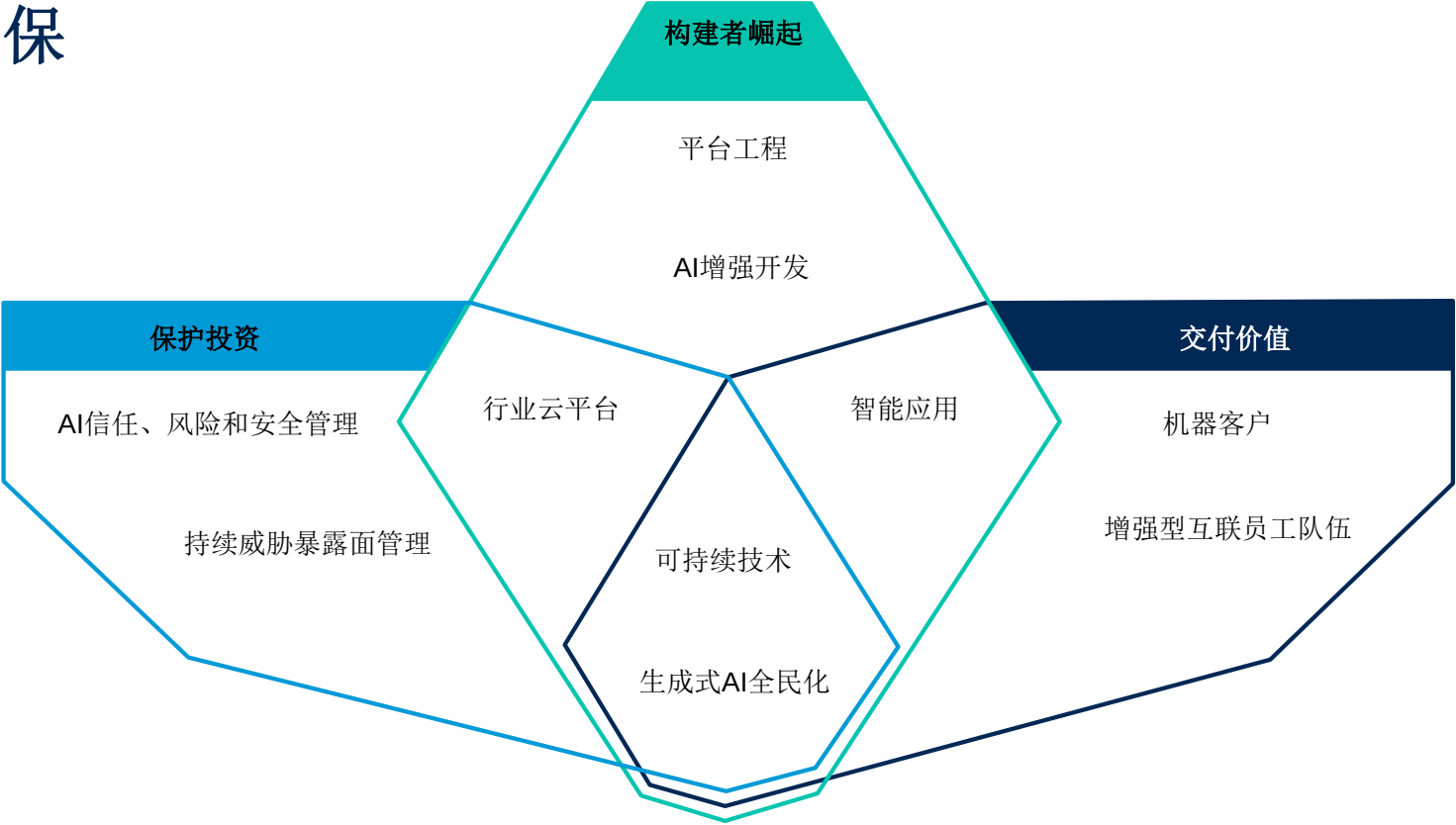
是否以及何时采用这些技术，取决于企业机构的业务目标和当前的发展水平。只有实现业务目标，才能真正创造价值。



Bart Willemsen
Gartner研究副总裁

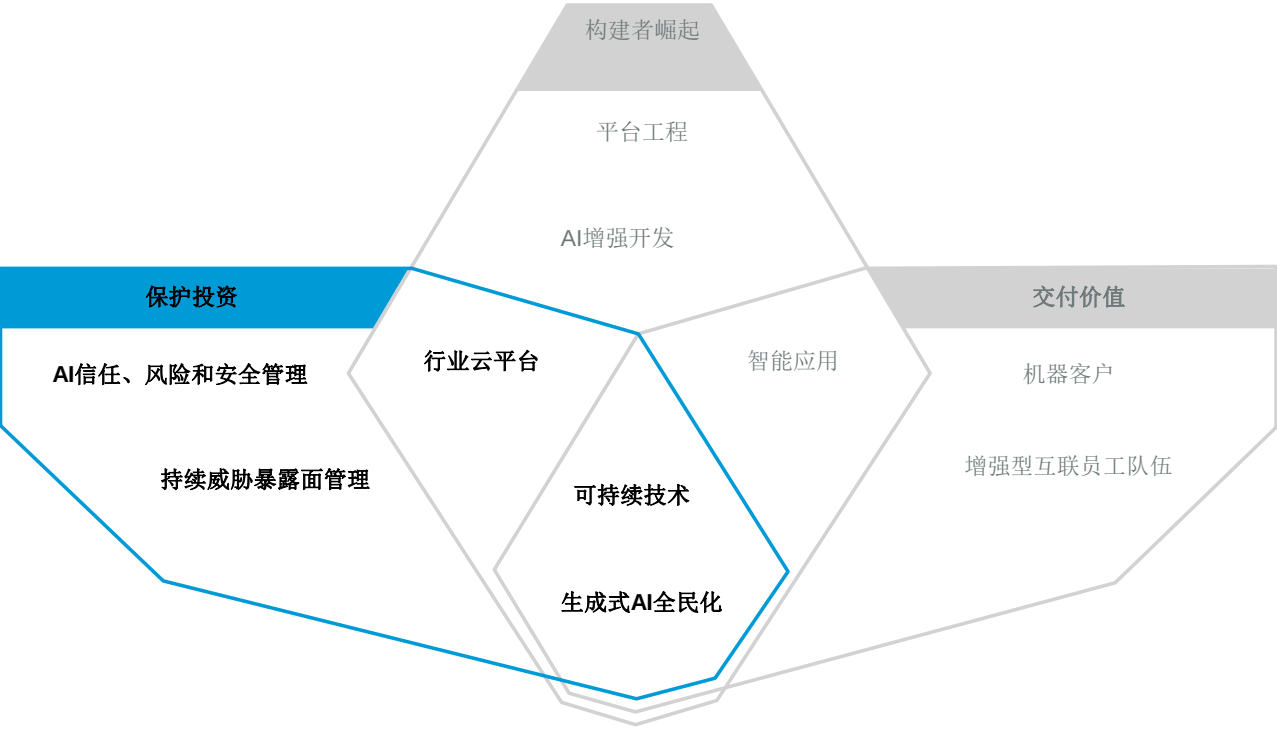
创造价值，构建强大能力并保障自身安全

Gartne预计，未来36个月内，这十项技术趋势（每项趋势可能属于一个或多个类别）将被众多业务和技术决策纳入考量。是否以及何时采用这些技术，取决于企业机构的业务目标。



保护投资

保护企业的投资，确保企业能从过去和未来的战略技术决策中持续获益。



行动建议

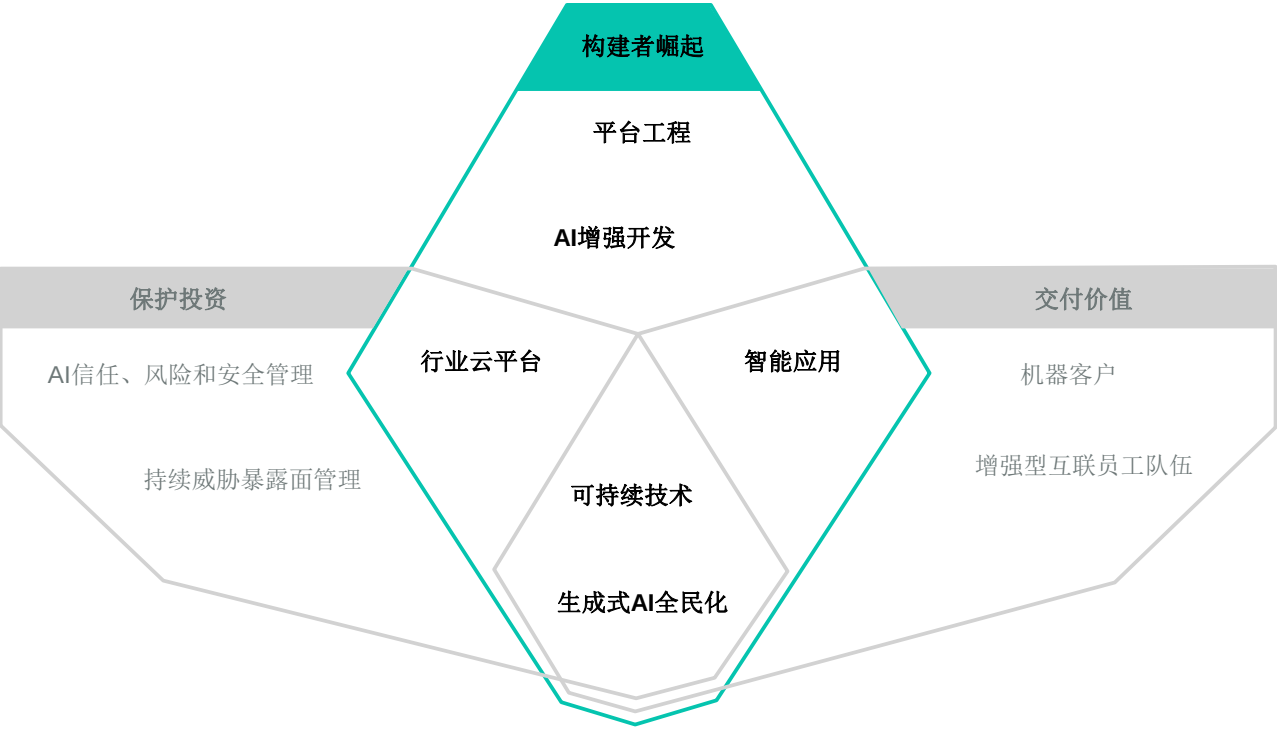
- 保持谨慎——肆无忌惮、漫无目的地进行投资的时代已经过去。
- 计算投资回报率（ROI）时，将用于保护性措施的投资考虑在内。
- 在确保自身权利的同时，以分布式开发为导向，调整开发方式。

实践案例：AI TRiSM

富达投资使用模型运营框架部署了数百个AI模型。该框架遵循详细的控制步骤持续监控部署中可能发生的问题（如漂移），以便在事态升级前及时处理这些问题。最终，富达投资将AI模型投入生产的速度提高了100%，并将发现和解决问题所需的时间缩短了80%（从数周缩短为数个小时）。

构建者崛起

赋能员工和开发人员，使其能够利用适合的技术实现适合的功能，进而构建适合的解决方案。



行动建议

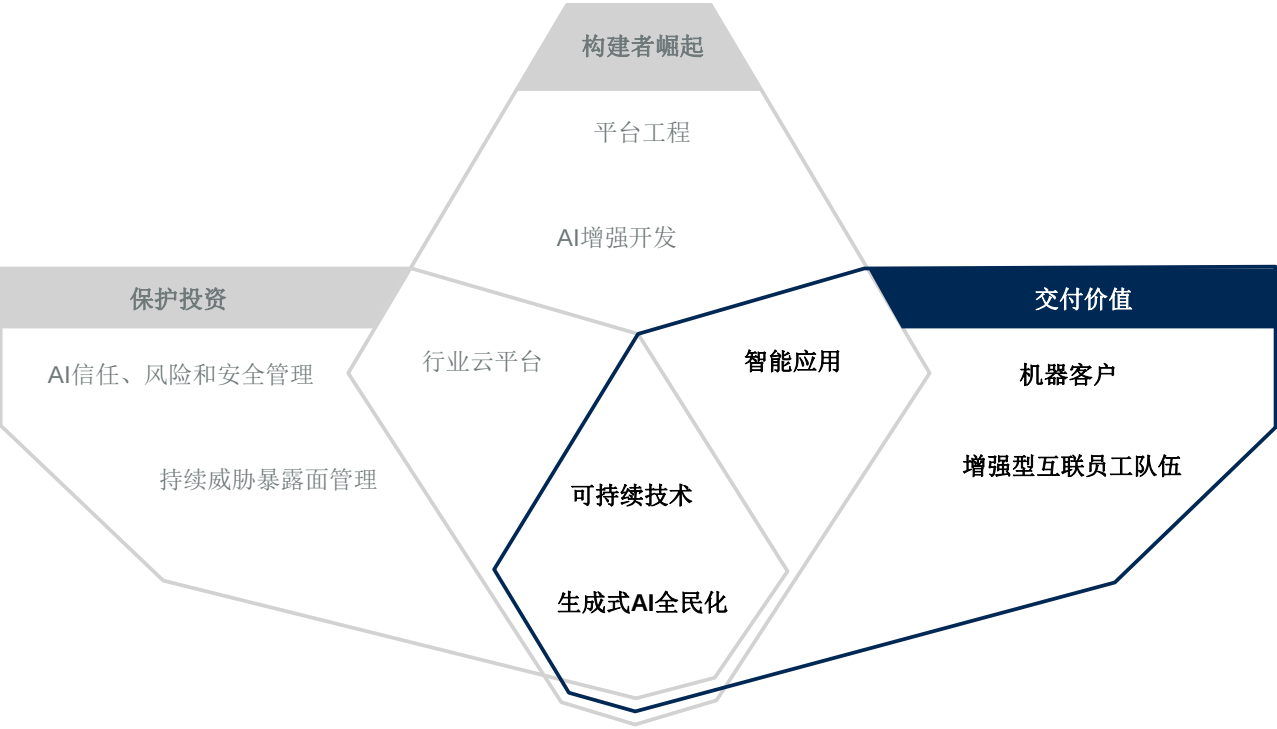
- ✔ 使用对**自身企业机构**（及内部专业人员）有所助益的技术。
- ✔ 制定技术路线图，发掘**非专业人员**的创造力。
- ✔ 与业务利益相关者密切的合作，**确定范围和能力**。

实践案例：平台工程

英国石油公司针对不同用户的能力和**需求**，开发了丰富的数字平台组合，并通过这些平台实现了安全测试、组件扫描与授权以及发布的自动化。借助这些平台，员工可以在IT部门有限参与的情况下，自行创建解决方案。

交付价值

保持卓越运营的同时，持续完善和加速价值优化。



行动建议

- ① 持续调整以满足内外部客户的需求，建立良性循环。
- ② 同时覆盖基于算法的客户和内部员工。
- ③ 对快速演变的数字工具部署访问控制。

实践案例：增强型互联员工队伍

为充分利用员工的时间，默克公司推出了专门的扩展现实项目。该项目由IT部门联合人力资源以及学习与发展合作伙伴、业务部门领导者和运营部门共同开发，员工可以在知识转移、测试和培训过程中支持相关应用场景。项目为每个生产基地提供了模板，用于指导部署和变更管理。最终，默克公司将其主题专家70%的时间从非增值性工作中释放出来，并将员工培训和胜任工作所需时间平均缩短了两周。

Gartner 2024年十大重要战略技术趋势要点

深入了解每项趋势以及启动相应举措的方法。

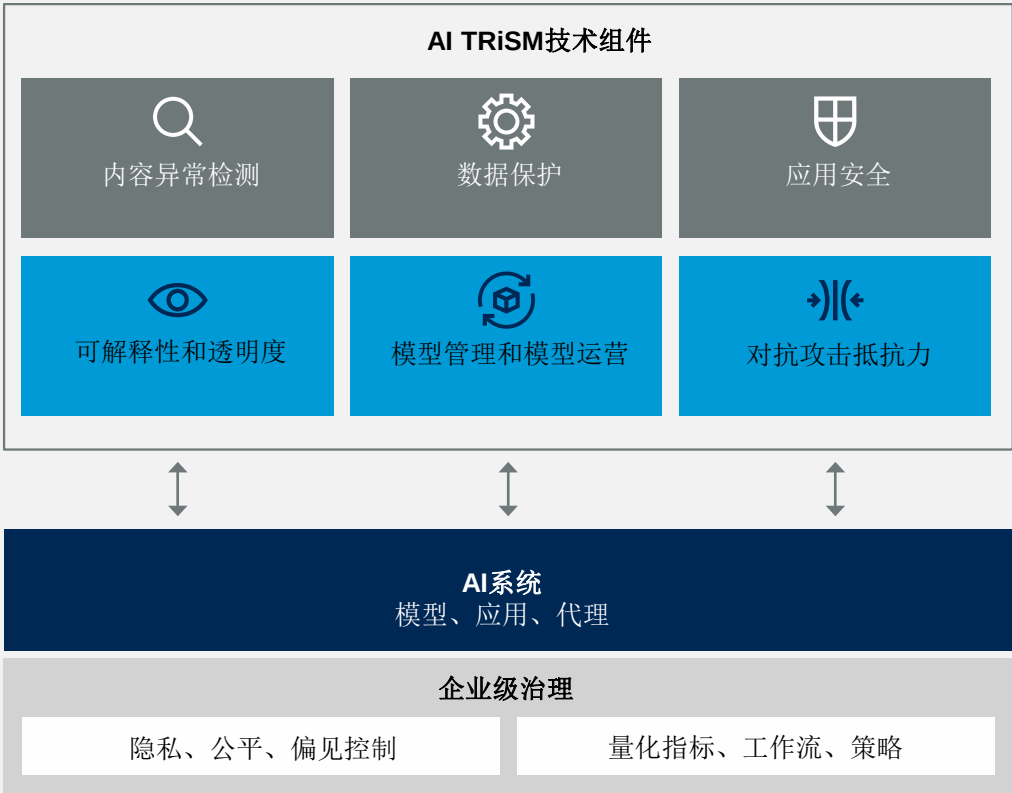
1

AI信任、风险和安全管理 (AI TRiSM)

支持AI模型治理，改善模型的可信度、公平性、可靠性、稳健性、透明性和数据保护。



AI TRiSM技术



AI系统用户需要获取这项技术，以填补构建者/所有者解决方案的空白

构建者/所有者的专属职责

来源：Gartner

1 AI TRiSM

Gartner预测

到2026年，对AI应用部署信任、风险和安全管理控制措施的企业，将能过滤掉80%的错误和非法信息，从而提高决策的准确性。

来源：Gartner

入选原因

- 与不使用AI TRiSM技术的企业机构相比，积极运用AI TRiSM技术的企业机构，其AI项目投入生产的比例更高，创造的业务价值更多，模型的准确性和一致性也更高。
- 对AI模型实施信任、风险和安全管理的企业机构，可以提高AI应用的公平性，同时更好地控制决策偏差。
- 通过监控AI模型不断对模型的可解释性进行测试至关重要，因其能够确保模型原有的解释以及可解释性在其投入生产后仍然适用。

启动方法

- 设立专门的工作小组或部门，管理与AI TRiSM相关的工作。
- 创建全面的AI TRiSM项目，与企业机构各部门通力合作，有效管理最优工具集。
- 制定可接受的使用政策，并创建必要的系统，有序记录和批准对于AI模型的访问以及实际使用证明。

2

持续威胁暴露面管理

(CTEM)

一种实用的系统性方法，旨在持续调整网络安全优化优先事项。



持续威胁暴露面管理



来源：Gartner

2

持续威胁暴露面管理

Gartner预测

到2026年，通过持续威胁暴露面管理项目确定安全投资优先级的企业机构，将使违规事件减少三分之二。

来源：Gartner

入选原因

- 该方法能够根据具体业务项目的特点或关键的威胁向量确定安全暴露面的评估周期。
- 可同时覆盖可修补（漏洞）和不可修补的暴露面。
- 引入攻击方视角并测试安全控制的有效性，从而对企业风险暴露面和修复工作的优先级进行验证。
- 提高整个团队的动员效率，调整成果预期，从策略和技术响应转变为基于证据的安全优化。

启动方法

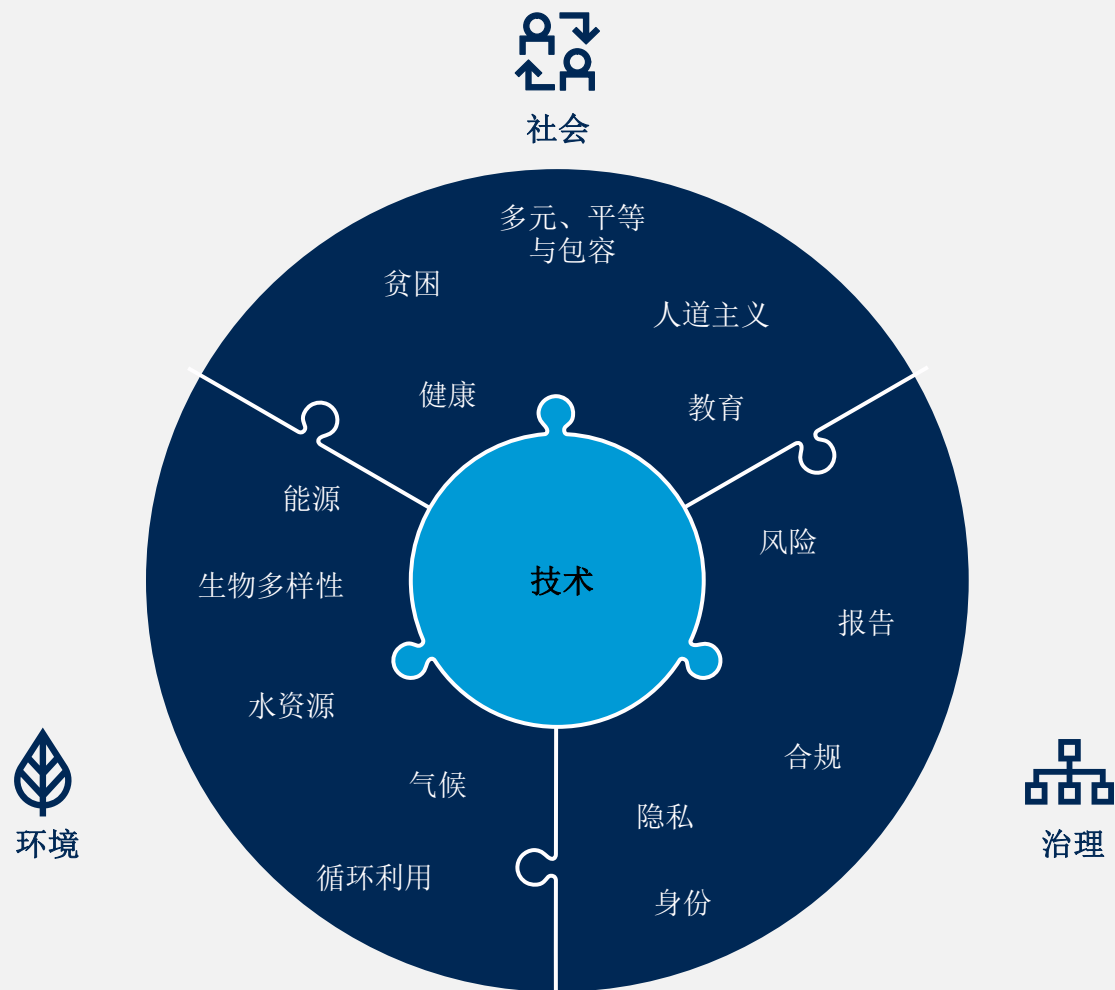
- 持续将CTEM与风险意识和管理项目进行整合，以业务重点为导向，根据业务价值确定风险缓解措施的优先级。
- 在扩展漏洞管理项目时，利用验证技术对所发现的暴露面进行验证，进而优化其优先级，通常可以取得快速的运营成功，从而为项目的扩展提供动力。
- 采用网络安全验证技术，完善现有优先级制定 workflow，提高网络安全就绪程度。

3 可持续技术

数字解决方案框架，旨在推动环境、社会和治理（ESG）成果，支持人权和长期生态平衡。



可持续技术框架



来源：Gartner

3

可持续技术

Gartner预测

到2027年，25%的CIO的薪酬将与其在可持续技术方面的贡献挂钩。

来源：Gartner

入选原因

- 环保技术可以预防、减轻和适应自然界中的风险。
- 社会技术可以改善人权成果、提升人类福祉、促进社会繁荣。
- 治理技术可以加强业务规范、监督和能力建设。
- 可持续技术可以为提高IT的整体绩效提供必要的洞察。

启动方法

- 选择有助于所在行业实现可持续发展、且为企业机构和主要利益相关者优先考虑的技术，如云服务和AI等。
- 邀请伦理委员会参与制定结构化的决策路线图。对于任何有利于企业机构整体可持续发展的价值，都应尽力优化，而不是寻求折衷办法。
- 参阅Gartner 2023年可持续技术成熟度曲线，立足企业的可持续发展目标，在成熟技术与前沿技术之取得适当的平衡。

4 平台工程

关于构建和运行内部自助服务平台的学科，每个平台是一个层，由专门的产品团队创建和维护，通过对接不同的工具和流程支持用户的具体需求。



平台工程图解

□ 团队

■ 要素

▲ 使用方向



产品与服务团队

即服务

开发人员门户



可复用组件



工具



平台服务



知识

数字平台



平台团队

基础设施平台



基础设施复杂度

来源：Gartner

4 平台工程

Gartner预测

到2026年，80%的软件工程部门将设立平台团队，在企业内部提供可复用的服务、组件和工具，支持应用交付。

来源：Gartner

入选原因

- 平台工程实践可以优化开发人员体验，加快业务价值交付。
- 通过改善开发人员体验和提高开发人员生产力，减轻认知负荷。
- 提高开发人员独立运行、管理和开发应用的能力，同时确保应用的可靠性与安全性。
- 提高重点人才的留任率。

部署方法

- 利用可复用、可组装、可配置的平台组件、知识和服务，设计和构建内部平台。
- 将平台视为产品。与最终用户合作，确定并优先提供对用户最有价值的技术能力、工具和流程，并据此搭建平台。
- 培育产品管理文化，在平台工程师与其服务的最终用户之间建立常规合作机制，使双方可以在安全、高效的环境中为彼此提供反馈。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/637043000106006044>