实施 AI 技术的 4 个关键注意事项

想要开始使用人工智能（AI）技术或扩展该技术用例的企业领导者有一些共同的问题和顾虑，包括如何使用 AI 来提升运营效率并拓展业务，同时保持稳定性并降低风险。无论您的公司处于 AI 实施之旅的哪个阶段，都需要考虑下文列出的 4 个注意事项。

1 选择灵活的平台

无论您是刚开始接触 AI，还是想要扩展现有用例并更广泛地实施 AI，都应选择可扩展的灵活平台来支持您的 AI 部署发展成熟，这一点很关键。

如果您正处于 AI 采用的初始阶段，您需要实施稳定而又灵活开放的基础架构，以便您的团队建构并运行小型工作负载。随着公司 AI 用例的增加和工作负载的增长，所使用的平台应支持大规模的模型训练 。

借助稳定的平台，数据科学家和开发人员可以构建能为您的客户提供真正价值的模型，让客户放心地使用可靠且注重安全性的平台。

如果您的企业在使用更高级的 AI 功能，则需要采用支持性技术，让企业能够发挥 AI 的全部潜能。要实现这一点，可能需要大量投资图形处理单元（GPU）和其他硬件加速器。

稳定、开放的平台可以：

- 为您的公司奠定良好的基础，从而花更少的时间来构建 AI 驱动的应用并实现这些应用的现代化。
- 让您能够加速部署 AI 驱动的应用。
- 帮助您在瞬息万变的 AI 形势中实现竞争优势。

借助合适的基础架构，无论未来出现什么样的 AI 创新，您的企业都能做好准备拥抱新技术。

2 针对混合 AI 做好准备

生成式人工智能（gen AI）对计算资源的需求不断增加，并将处理任务推向了网络边缘。混合使用云资源和本地资源有助于实施生成式 AI 用例，但一些工作负载（尤其是受合规问题或数据引力支配的工作负载）应该只在本地运行。借助混合 AI，您的团队可以在任何最合适的地方运行工作负载，包括靠近数据生成位置的地方。

混合 AI 提供诸多益处，包括：

- **灵活性。**在最合适的环境中运行实验性工作负载和生产工作负载可以节约成本。
- **加快交付。**边缘处的小型工作负载推理运算可加快向用户交付信息的速度。
- **降低风险。**在边缘运行 AI 应用可以减少将大量信息传输到核心的需求，从而更好地保护数据。

通过使用混合 AI，您的 IT 团队可以在核心数据中心或公共云中训练模型，然后将其分发到端点，让模型在端点处更快地进行推理运算并提供有用的智能。这样一来，可以将任务繁重的工作负载分散到中心云和边缘，从而平衡对处理能力的需求以及对快速准确的建议的需求。

3　不断扩展，不局限于第一个模型

您的 IT 团队可能只需付出少许努力就能将一个 AI 模型投入生产，但成功往往取决于能否不断扩展。要最大限度地增加业务价值，团队必须能够部署该模型的多个版本，可能需要每天部署数百次。

实施机器学习运维（MLOps）流程 可以帮助您的团队轻松扩展部署。与 DevOps 类似，MLOps 可将开发人员、运维经理和数据科学家汇集起来展开协作，以加速基于 AI 的应用的开发与成功部署。通过 MLOps，企业可以更轻松地扩展应用开发，从而在更短的时间内为客户提供更多服务。

MLOps 可成为一种经济高效的开发方式。通过在通用平台上协同工作，团队可以提高效率，这有助于节省时间和成本，可能会直接对企业的净利润产生积极影响。

4　注重安全防护

面对修复成本高昂的网络攻击，企业高管们越来越希望找到方法来保护敏感数据并降低风险。生成式 AI 进一步加剧了这种紧迫性，因为使用该技术可能会增加机密数据的泄露风险。

保持强健的安全态势至关重要，有助于避免各种威胁，例如：

- **数据中毒。**该攻击会将错误或恶意数据注入 AI 模型，导致模型生成不准确的信息或欺诈性建议。
- **窃取模型。**该攻击会对机器学习模型进行反向工程，并使用副本提取数据。
- **后门攻击。**该攻击会在 AI 模型中隐藏恶意代码，从而使攻击者能够窃取信息。

这些攻击方式以及其他手段可能会对您的业务构成重大威胁，导致企业面临财务和法律风险。不妨让值得信赖的应用平台供应商为您提供帮助，最大限度地减少与 AI 相关的漏洞。该供应商应具备良好的口碑，并拥有处理安全补丁和发布的成熟流程。

了解更多

加快实施您的 AI 战略。了解红帽的 AI 解决方案。

关于红帽

红帽帮助客户跨环境实现标准化，支持他们开发云原生应用，并利用红帽一流的支持、培训和咨询服务，实现复杂环境的集成、自动化、安全防护和管理。

红帽官方微博

红帽官方微信

销售及技术支持

800 810 2100
400 890 2100

红帽北京办公地址

北京市朝阳区东大桥路 9 号侨福芳草地大厦 A 座 8 层　邮编: 100020
8610 6533 9300

cn.redhat.com