

AI 和机器学习 在您的组织中 组织权利

开始使用并获得收益。

从您的机器数据中获取答案

简介

- **AI 和机器学习将对您从机器数据中获得答案的能力发挥至关重要的作用。** 数字转换导致了复杂的环境，不断产生新的数据。不要因为缺乏正确的解决方案而错过可能的业务见解。
- **数据是 AI 和机器学习驱动的举措的动力。** 但拥有大量数据点还不够。确保您拥有获得最有价值业务成果所需的洞察力。
- **您可以通过智能的自动化解决方案改善检测和响应时间，** 让您在 IT 运营受到影响之前捕捉到代价高昂的问题。
- **使用主动监控和调查来领先一步，** 并减少昂贵的事件和停机时间。通过转向积极主动的方式，改进并取代资源密集型任务。

热点背后： AI 和机器学习

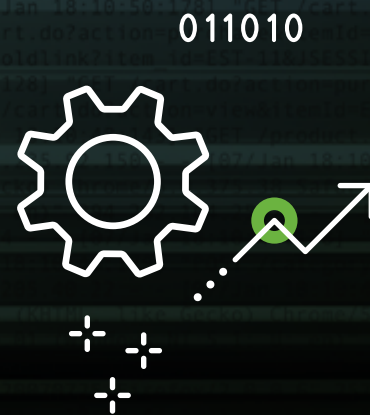
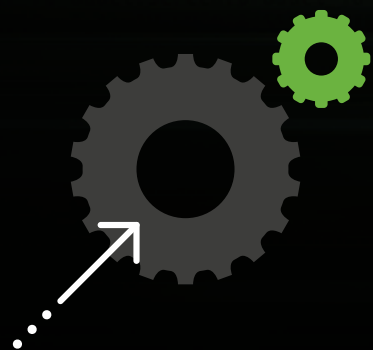
以最简单的形式，人工智能 (AI) 可以被定义为基于智能算法以近乎人类的方式执行任务的机器。在没有明确编程这样做的情况下，它拥有学习和采取行动的计算能力。机器和软件现在看起来可以模仿人类的认知功能，通常通过对丰富数据集进行训练并在引入新数据点时调整其响应。通过应用于大型数据集的预测建模，建立基于新数据点做出未来决策的模型，这是可能的。也被称为机器学习，这就是 Google Maps 知道您想在一天结束时回家的方式，Netflix 推荐您应该观看的下一部电影的方式以及自动驾驶汽车的操作方式。

简而言之，机器处理的信息越多，学习得越多。这不是人类的想法，但它不仅仅是花哨的自动化。

幸运的是（或不幸运），还没有出现具有感知力的机器人，但 AI 已经改变了我们工作、玩耍和交流的方式。随着越来越多的数据产生，各个组织认识到利用数据库进行数据驱动型决策的价值。但是，随着数据量的增加，人类将难以跟上。继而，组织利用机器学习支持的 AI 来处理他们的数据，并回答将他们提升到高于竞争对手的问题变得越来越重要。

AI 正在产生大量的行业热点，但获得 AI 优势的机会仍然没有得到组织的支持。现在是清除混乱的时候了，所以您可以利用 AI 的力量为您的组织带来效益。

机器数据： 助力 AI



以数据为中心的方法

数据是 AI 和机器学习工作的核心。为了预测未来的结果、检测异常并聚集重要事件，同时滤除噪声，机器学习依赖于历史和实时数据来检测模式。但是，这通常是组织无法克服的障碍。他们没有意识到 AI 的价值，因为他们要花费大量的时间和人力来精炼海量数据，这让他们望而却步。这包括必须移动、汇总和关联来自不同工具和系统的数据，导致浪费宝贵的时间、资源和机会。

但这不是一个可以跳过的步骤，因为如果将未经处理或未定义的数据用于 AI 和机器学习，将导致错误的结果。相反，有效的数据准备可以为 AI 和机器学习提供强大的动力，并提供重要的业务洞察，包括帮助确定问题出在哪里，优化客户体验并检测欺诈指纹。

为了有效地做到这一点，组织需要一个解决方案，既能准备分析数据，又可以将机器学习应用于所述数据。采用这种方法，您拥有的数据越多越好。有效的 AI 和机器学习意味着您不会被数据陷入困境；相反，您会因它而得到提升。更多的数据和复杂性创造了一个更大的背景来校准和提供您的模型，带来更丰富的见解。

其结果是为企业节省宝贵的时间和资源，同时最大限度地提高机器学习驱动的洞察力，从而了解如何实时预测和响应业务事件。

那么这是样子？我们来看看 AI 和机器学习如何影响 IT 和安全。



IT 运营 视角

IT 世界常常存在悖论。对最新和最好的应用程序提供支持的相同业务部门往往缺乏相同的技术。最终用户可以体验到精致的产品或平台，而实现这一目标的人仍然在处理传统解决方案、成千上万的警报，以及对复杂性持续增长的环境的可视性差。

但这终于开始改变。软件系统正在将大数据与 AI 和机器学习功能相结合，以改进和替代广泛的 IT 运营流程和任务 - 包括可用性和性能监控、事件关联和分析、IT 服务管理和自动化。结果是为企业赢得了时间和金钱。

IT 中大数据和机器学习的结合，也被称为 IT 操作的人工智能或 AIOps，使得更好地分配资源和执行任务变得比以往更容易。组织可以获得 IT 系统和服务性能过去、现在和未来模式的答案。更具体地说，组织可以通过预测分析以及自动事件响应和解决方案快速找到并解决问题。

- 避免代价高昂的停机时间并提高客户满意度
- 解决 IT 孤岛和不相关的响应
- 消除繁琐的手动任务
- 更好地与同行合作

简而言之，简化当前的监控和管理工作流程为 IT 专业人员提供了积极主动的机会。

安全性 视角

呼吁将 AI 和机器学习用于安全方面并不是首次出现，并且正显示出在所有安全环境中成为主流的前途。过渡的好处说明了一切。它可以帮助组织更好地分析和响应安全事件，更好地应对威胁并最大限度地降低总体风险，同时降低成本并减少对有限资源的压力。

特别是机器学习在安全方面取得了长足的进步，成为高级威胁检测和阻止内部威胁等用途的完美契合，这需要更细致的监控和响应系统。涉及网络内部横向移动的高级攻击、特权用户受到威胁以及不知情用户意外访问敏感信息，都可以通过机器学习驱动的自动化异常检测来解决。

在处理复杂的攻击时，组织经常需要比现有安全工具更多的工具。对于小型组织来说，这可能意味着部署更深入的网络防御或端点保护。对于大中型组织，它可能转化为部署工具和技术来收集、过滤、集成和链接各种类型的安全事件，以更全面地了解其安全状况。

机器学习通过一个“真相源”来满足这些需求，从而获得安全洞察力 - 分析师和 SOC 团队可以借助智能技术分析所有机器数据，包括来自应用程序、端点和网络设备的日志和事件数据。他们可以执行快速调查，找到有意义的见解，确定事件的根本原因，吸取历史趋势并共享研究结果，而不会因数千个警报和误报而陷入困境。

简而言之，组织可以提高检测速度，分析影响并快速响应任何安全事件。这有助于组织最大限度地降低威胁的负面影响，让他们更积极地管理安全状况 - 从持续监控到深度取证分析和自动响应。



越复杂 越好。

虽然 AI 的功能不会成熟到与人类的技能和能力媲美的程度，但使用机器学习的 AI 可以帮助企业根据大量数据做出决策。

金融服务机构可以应用 AI 和机器学习来识别异常行为，保护自己和客户免受欺诈。随着时间的推移，医疗保健和生物技术组织可以拥有更高保真度的实验室流程和改进的实验质量测量能力。制造商可以通过预测性维护和监控消除影响业务的故障。根据人口统计和购买历史等因素的公式，零售将提供更好的客户服务和针对性建议。可能的好处还会继续出现。

我们才刚刚开始。AI 和机器学习拥有光明的未来。很快，我们应该期望端到端的 AI，而不是一起工作来执行功能的零星模型。自我配置是很快会发生的事情，以减轻人类处理者的架构或验证。而预先经过培训的开源模型很快就可以作为可重用组件服务于各种使用案例。

您是否准备好使用 AI 和机器学习来潜入未来？

要了解更多关于 AI 和机器学习趋势以及如何最大限度获益的信息，请下载 ESG 报告：

利用 AI 和 ML 获得更大的影响力

→ 了解更多信息