从 ITOM 到 AIOps：IT 运维管理向智能运维的进化

当前互联网和移动互联网发展迅猛，从事各个行业的企业为了应对日趋激烈的市场竞争，纷纷进行了数字化转型，利用移动互联网技术、云计算及大数据等新兴信息技术发展企业的数字服务，从而吸引客户，帮助销售和推广产品，提升客户体验。

然而，随之而来的是规模不断扩大的 IT 系统、日益复杂的系统架构，以及海量的 IT 运维数据，同时公司业务对 IT 系统的连续性要求也进一步提高。

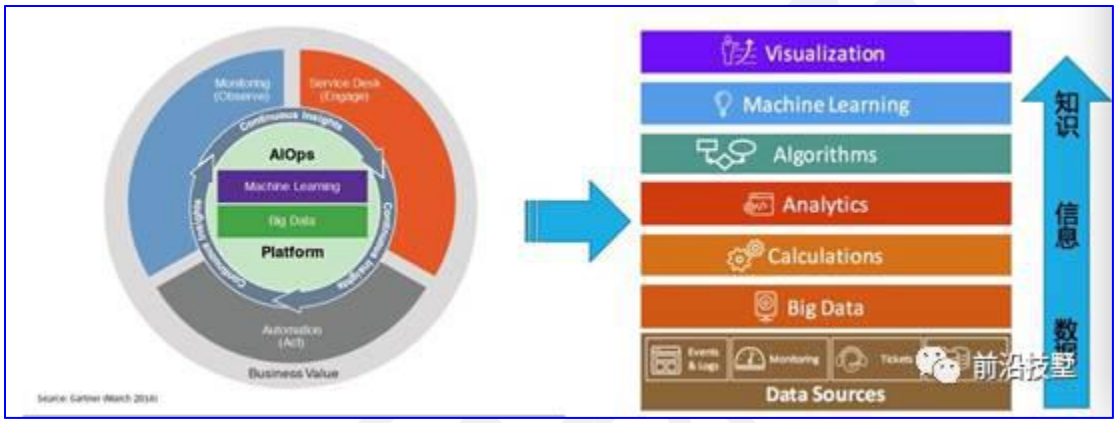
面对这些新形势下的挑战，IT 运维管理（ITOM）需要从原有的人工加被动响应，转变为更高效、更智能化的运维体系，为新形势下的 IT 系统保驾护航。

当前传统的 ITOM 工具往往缺乏分析能力，虽然也能采集到运维数据，但无法对这些数据所包含的信息进行洞察，更加无法将数据进行知识化的本质提升。研究机构 Forrester 曾在之前的一份报告中指出：“这些工具为我们提供了大量的原始数据，但能洞察出埋在这些数据中的有价值信息的能力还是非常稀缺的。”（来源：Turn Big Data Inward With ITAnalytics）

令 IT 运维团队感到欣慰的是，智能运维（AIOps）踏着人工智能的时代浪潮应运而生。

Gartner 在 2016 年发布的报告中首先提出了基于大数据及算法（Algorithmic IT Operations）的 IT 运维概念。随着人工智能的快速兴起，Gartner 将 AIOps 的概念从原本的基于大数据及算法，扩充为基于人工智能（Artificial Intelligence for IT Operations，AIOps），期望通过大数据、现代机器学习及更多高级分析技术，提供具备主动性、人性化及动态可视化的能力，直接或间接地提升目前传统 IT 运维（监控、自动化、服务台）的能力。

AIOps 为 IT 运维提供了全新的管理思路。AIOps 的定义涵盖的两个阶段，可概括为两个层次的提升：数据到信息分析层次的提升；信息到知识提取层次的提升。



从数据到信息的分析，更多的是采用数据统计方法，帮助运维相关人员更好地从众多运维数据中了解系统的运行状态，分析并定位故障，实时获取统计数据。而信息到知识的提升更多的是希望借助人工智能算法，在信息分析的基础上通过机器学习的方式实现异常状况检测、故障/趋势分析、故障关联和精准告警。

根据权威机构 Gartner 的预测，比起现今 5%这样的数据比例，到 2019 年，全球 25%的公司都将系统性部署实施 AIOps 平台支持两个及以上的主要 IT 运维功能。到 2022 年，40% 的大型企业会通过大数据和机器学习的能力来帮助甚至逐渐取代传统运维中的监控、服务台及自动化流程。

AIOps 重新定义了 IT 运维的管理方式，为 IT 运维团队适时提供适当信息，以便实现以下几点。

●通过采集当前环境中的运维数据，集成现有 IT 运维管理工具，利用聚合数据分析的技术，对 IT 系统中各个环节的问题进行快速定位、故障排除和预测。

●对来自业务环节中各个分布系统的数据进行整体分析，合理优化 IT 服务，挖掘关键业务 KPI 指标，反哺业务端，帮助其做出明智决策。

●通过大数据和人工智能技术分析用户的行为日志和运维数据，发掘潜在的系统安全和合规问题，为企业的信息安全保驾护航。

那么 AIOps 究竟在 IT 运维中有哪有典型的应用场景呢？常见的场景大致如下。

◎ 全局日志检索

以一个典型金融行业为例，他们有上百个业务系统，面对每天产生的大量日志数据（几 TB），日常运维过程中，当运维人员需要排错或日志巡检时，需要逐台登录服务器，无法集中查看和管理日志数据；另外，日志查询方式比较原始，比如 Windows 服务器，手动查看 Event Log，Linux 服务器则只能通过 less、grep 和 awk 等常见的 Linux 指令，无法从时间段、关键字、字段值统计等方面进行多维度查询。

AIOps 平台通过收集各类数据源（包括操作系统、系统软件、数据库、应用日志等），统一进行管理。不同于以往每次仅可查看数量有限的几种日志，运维人员可通过智能运维平台所提供的关键字、统计函数、单条件、多条件、模糊查找等功能，在多个系统中快速定位故障信息，帮助运维人员从全局视角查看系统的运维数据信息。

◎ 复杂多维报表，应用深度监控

AIOps 将各系统的运维数据进行统计分析并生成各类实时报表，对各类运维数据（如应用日志、交易日志、系统日志）进行多维度、多角度深入分析及可视化展现，以业务视角实时展示各种业务指标，具体如下。

◎ 快速发现故障，精准告警

实时采集各类运维数据（日志、监控系统告警、性能数据等），通过对历史数据的挖掘和分析，AIOps 可以找出哪些告警和事件是频繁一起出现的，并将其认看作同一类故障的告警，从而把多个告警和指标合并，推送给运维人员，做到精细化告警，避免传统监控工具因一故障而导致的告警风暴，生产告警噪音。

◎ 缩短故障解决时间

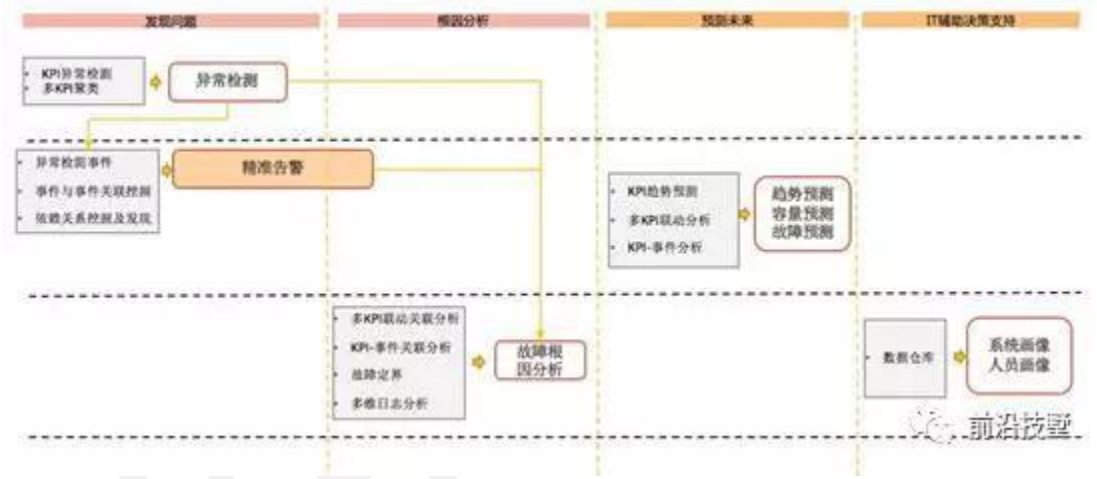
通过运维数据可视化（复杂多维报表，热力图）及精细化告警信息，结合以前发现问题的经验知识库和模型，从而将运维信息从平面变为立体，立体展现故障树分析，通过推导路径使运维人员对于问题的定位更加快速、直观，使得问题的解决更加容易。

◎ 预测未来

进行数据挖掘，生成分析类报表，进行趋势/容量/故障预测。例如，某些故障之间有时间上的先后关系，交换页不足、内存不足会逐渐导致系统故障或应用故障，该系统建立关联模型，发现前者故障，提醒用户可能后继可能发生系统故障或应用故障。在故障产生真正业务影响前，告知运维人员事先解决问题。

◎ IT 辅助决策支持

通过采集海量多维度数据，构建多元结构化底层数据仓库，以搭积木的方式适配各类运维场景，并在场景里刻画系统和人员画像，通过画像形式来辅助企业进行 IT 决策。

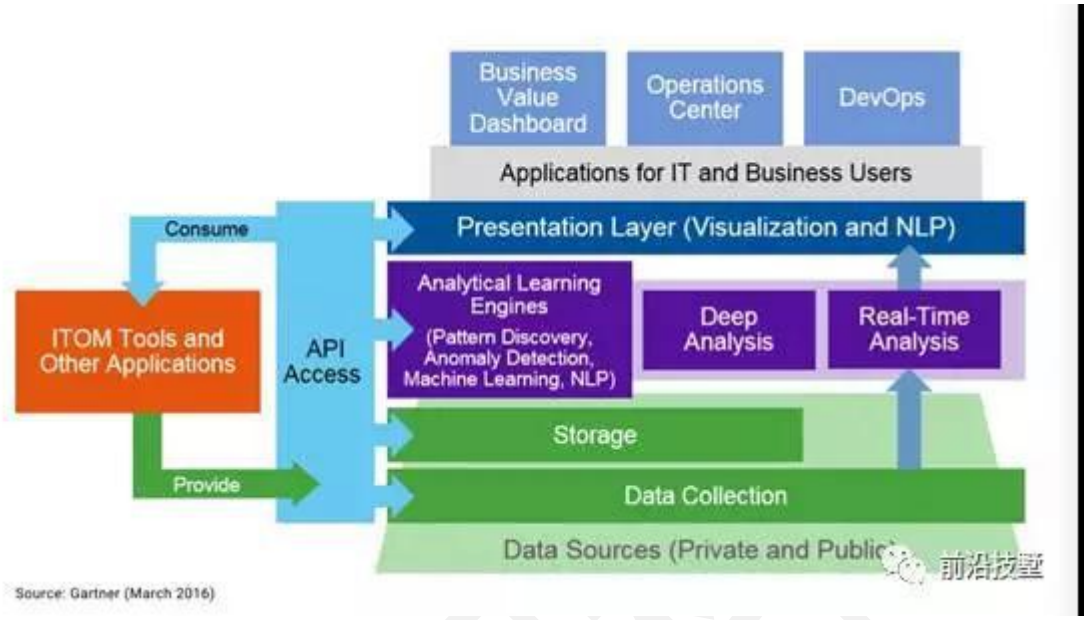


AIOps 与现有 ITOM 平台的关系具体如何呢？传统 IT 运维管理平台，即 ITOM 平台，往往是为完成单一管理任务而设计的，更偏向于管理某一细分专业领域。

- 监控系统：负责 IT 系统的健康及可用性管理
- IT 服务管理平台：负责配置管理，资产管理，事件/问题/变更等服务流程管理
- SOC 平台：专注于信息安全管理
- APM 平台：应用逻辑拓扑管理，应用故障诊断等

而 AIOps 平台则构建在传统 ITOM 平台的上层，把 ITOM 作为分析的源头，通过接口集成将各个 ITOM 平台组件中的孤立运维数据进行汇总，使其突破数据孤岛的壁垒，其次借助自身的关联分析、机器学习、

数据建模、全局搜索能力，帮助企业从 IT 系统的行为、状态、配置、故障和事件中等多个维度，产生趋势预判、快速故障定位和商业洞察等价值。



在信息架构与应用系统日渐庞大的今天，如果再通过人工分析定位的运维方式，很难适应目前日益快速增长的业务需求。规模不断扩大的 IT 系统、日益复杂的系统架构，以及海量的 IT 运维数据对使用传统 ITOM 的运维人员而言都如芒在背。因此，我们有理由相信 AIOps 能够帮助企业及各类运维人员在大数据中找到合适的发展模式。现在是时候用一些类似人工智能的思维方式来为 IT 产业服务，使大数据的分析方向转到 IT 运维上了。