

预测性 IT:

领先组织机构如何使用人工智能提供卓越的客户体验

1100110100111 - - - - -
100111001101001110 - - - - -
110100110100 - - - - -

×



splunk>

被动性 IT 已然成为过去式

各个行业和各个地区的 IT 运营团队都面临着复杂的问题。事件泛滥、复杂的连接服务、组织孤岛和高要求 SLA 都只是造成 IT 运营管理难题的一小部分原因。此外，整个组织机构只能依靠 IT 团队来防止运行中断，尤其是可能对客户体验产生负面影响的运行中断情况。

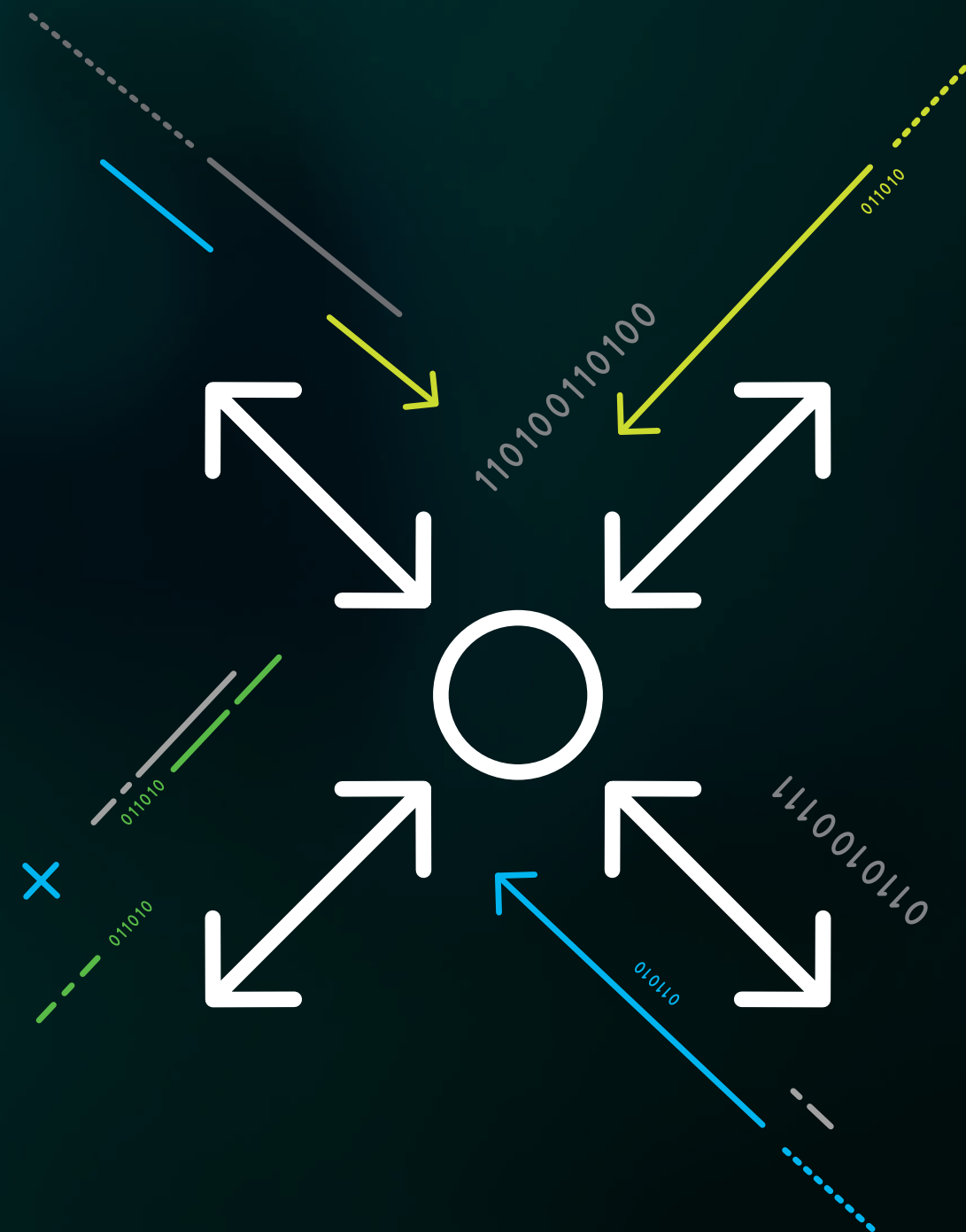
最具前瞻性的 IT 组织突出混乱之重围，找出问题的根源并快速解决问题。

但这只是第一步。这些团队还利用机器学习来预测异常行为，并使用 Splunk IT 服务智能 (ITSI) 避免运行中断。

了解组织机构如何使用 Splunk ITSI 预测、预防和解决难度最大的 IT 挑战。了解以下企业案例：

→ Leidos
→ ENGIE
→ 美光科技

→ Econocom
→ 世纪互联
→ 环联



更好的事件管理：
SPLUNK ITSI 造福 LEIDOS

事件杂讯 减少 97%

「我从事 IT 管理已有 20 多年，我从没见过具有这种功能的产品。Splunk 拥有所有数据并允许我以相同的方式搜索这些数据，它让我第一次能够真正对我的 IT 环境进行彻底的异构堆栈监控。」

- Leidos 绩效管理总监 **Don Mahler**

作为《财富》世界 500 强企业和全球技术解决方案领导者，Leidos 致力于解决国防、情报、健康等市场面临的全球性挑战 - 其自身在确保为客户提供服务方面也面临挑战。

挑战

Leidos 绩效管理总监 Don Mahler 称，他们需要既可以将子部门、IT 和功能孤岛汇总在一起，也可对大量事件进行分类的解决方案 - 以下挑战使事件覆盖了 120 多项 IT 服务：

- 全天候客户访问需要更大的监控和响应力度
- 独立的孤岛创建了一个 Balkanized IT 部门
- 需要减少成千上万的警报和事件

业务影响

除了基本要求，例如整合来自异构 IT 环境的事件，检测和隐藏重复警报，清除已解决的警报并将其提取细化到可操作事件，该公司还需要拥有其他功能，例如在一段时间后自动升级警报或当设备目的性脱机时抑制警报。Leidos 通过 Splunk ITSI 实现了这一切。Mahler 称：「总有些日子会遇到大量事件；不过，Splunk ITSI 会对这些事件进行优先排序，您不仅可以深入了解故障，还可以通过查看警报屏幕了解受事件影响的项目。」

Mahler 说 Splunk 平台还有一大好处，即 Splunk 平台能够破除数据孤岛，允许团队查看服务堆栈中的数据。今天，Leidos 使用的 Splunk ITSI 涵盖大约 20 个管理系统（从微软系统中心配置管理器 (SCCM) 到 SolarWinds 网络管理工具），4500 多个配置项 (CI) 覆盖全球 120 项 IT 服务和 240 个地点，帮助公司每天将 3500 到 5000 个警报归结为近 50 个可以操作的网络和数据中心运营故障单。将 CMDB 信息传递到 Splunk ITSI 可以为不同的员工提供不同的警报显示。重要的是：更容易访问更多相关数据，工作人员可以腾出时间专注于最重要的问题。

SPLUNK 保障 ENGIE 全球市场 核心交易应用程序 的性能



更快地解决 影响业务的问题

「通过 Splunk ITSI 的机器学习，我们不必手动创建阈值来衡量每台服务器的性能。我们可以动态调整阈值，将预期的性能差异考虑在内。这样不仅免掉频繁配置和调整的成本，而且使我们的团队能够在实际事件影响最终用户体验之前集中精力对事件进行分类。」

- ENGIE 全球市场基础设施负责人

ENGIE 全球市场 (EGM) 是天然气、电力和能源服务全球供应商 ENGIE 的核心能源交易平台。ENGIE 全球市场需要实时集中查看其关键交易应用程序的健康状况，以加快故障排除并保障性能。

挑战

应用程序的健康状况至关重要，因此 EGM 团队需要实时集中查看应用程序的健康状况，并且具备快速简明地向企业利益相关者提供系统性能信息的能力。而搭载应用程序的网格系统具有分布式特性，让这一切倍具挑战性。此外，EGM 还面临如下其他挑战：

- 需要确保核心交易应用程序的性能和可用性
- 需要实时集中查看系统健康状况
- 分布式网格系统意味着自行开发的解决方案很复杂并且会影响性能

业务影响

在部署 Splunk 平台之前，开发和基础设施团队使用自己的孤立监控工具，这需要反反复复地解决问题。使用 Splunk 软件之后，团队之间的协作得以改善，事件解决时间也缩短了。

部署 Splunk ITSI 之后，EGM 更容易关联 IT 堆栈中的数据，从而改善事件管理和解决。「出现问题时，Splunk ITSI 会为我们显示查看项目，指引我们解决问题，」ENGIE 全球市场基础设施负责人称：「通过 Splunk ITSI 的机器学习，我们不必手动创建阈值来衡量每台服务器的性能。我们可以动态调整阈值，将预期的性能差异考虑在内。这样不仅免掉频繁配置和调整的成本，而且使我们的团队能够在实际事件影响最终用户体验之前集中精力对事件进行分类。」

分析驱动方法改变 美光科技 IT 运营

影响业务的 IT
事件减少

50%
以上

重大 IT 事件的
平均解决时间缩短

32%

重大 IT 事件的
数量减少

23%

「如果我们碰巧遇到重大事件，Splunk ITSI 是我们的第一个求助对象。我们总是问自己一个问题，『是 ITSI 帮助我们找出了问题所在吗？』答案始终都是『是的』。这告诉我们，我们已经制定了正确的 KPI，并定义了正确的服务和依赖关系。」

- 美光科技 IT 总监 **Brian Best**,

先进半导体系统全球领导者美光科技公司，开发了大量的存储器解决方案组合，致力于提供卓越的服务质量，这对于确保良好的客户体验和保持竞争力至关重要。

挑战

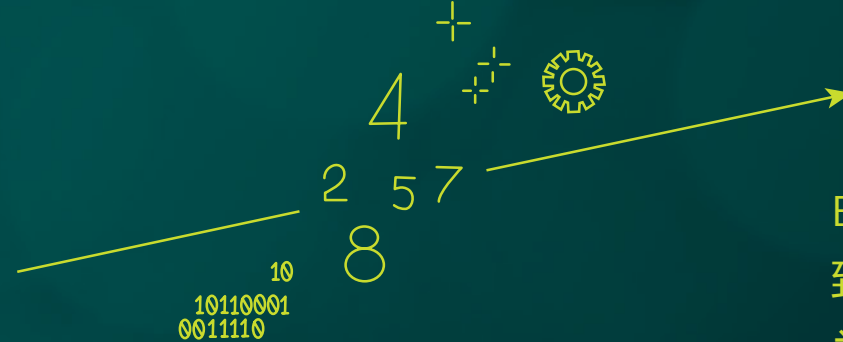
据美光 IT 总监 Brian Best 称，制造业 IT 部门以前缺乏对其 IT 运营的企业级可见性。为了保持在行业中的竞争地位，美光需要维持服务质量并革新其 IT 运营战略，以应对以下挑战：

- 数据孤岛限制了团队识别、解决和预防 IT 问题的能力
- 这种被动性 IT 监控方法阻碍了公司履行其主要使命 - 保障其制造工厂生产和运输晶圆，不会出现任何系统中断问题或意外的系统影响

业务影响

如今，在事件管理、警报和事件管理到问题和变更管理的方方面面，美光科技都依靠 Splunk ITSI。该解决方案帮助美光不仅获得亟需的实时可见性，还节省了时间并减少了 IT 事件对其业务的影响。总体而言，Best 指出，Splunk ITSI 帮助美光将影响 IT 业务的事件减少了 50% 以上，IT 事件的平均解决时间减少了 32%，重大 IT 事件的数量减少了 23%。Best 说：「我们不必等待网络工程师接听电话并告诉我们网络是健康的。每个人都能够自行查看。」

每天早上，根据 Splunk ITSI 数据提供的自定义报告，Best 和他的团队会收到一份 KPI 报告，通常会列明过去 24 小时内发出警报的前 10 项 KPI。如果 KPI 的警报次数达到一定量时，则需要解决该 KPI。Best 称，确实发生问题的情况下，所有团队都会参与进来，以确保不会遗漏任何关键问题。此外，Splunk ITSI 还提高了制造业 IT 团队构建仪表板的能力，仪表板可以提供环境的宏观视图。



事件分析帮助 ECONOCOM

为客户提供更好的服务

「得益于 Splunk ITSI 的集成机器学习，如今需要我们处理的事件数量减少了，简化的事件分析框架使我们平均耗时 8 分钟即可快速处理事件。这使得 SLA 性能提高了 15%。」

- Econocom 基础设施管理服务技术总监 **Laurent Amouroux**,

SLA 性能
提高
15%

事件总数
减少
60%

系统性能问题
引起的事件
数量减少
10 倍

Econocom 遍布 19 个国家，拥有 10000 名员工，收入达 25 亿欧元，致力于设计、资助和监督企业数字化转型解决方案。满足与这些服务相关的严格服务等级协议 (SLA) 对于 Econocom 的业务至关重要。

挑战

在使用 Splunk 之前，Econocom 运营团队有十几种不同监控和事件控制台。Econocom 操作员也缺乏以下能力：

- 在多个数据源中进行分析，加快事件调查的速度
- 使用业务服务上下文将数据可视化并进行容量规划
- 通过多个孤岛中的事件有效地衡量 SLA

业务影响

當 Econocom 的 IT 组织内多个不同团队在使用了 Splunk ITSI 数周后，Econocom 已经能够通过 Splunk ITSI 将其所有解决方案中的事件集中到一个解决方案中。Splunk ITSI 中的事件分析功能帮助 Econocom 更好地对客户的基础设施事件进行优先排序并更快地响应，最终提高服务质量。Splunk ITSI 还能让 Econocom 从事件管理流程中排除被认为是误报的事件，使事件总量减少了 60%，操作员也能够专注于真正重要的事件。

Econocom 使用 Splunk ITSI 之后，系统性能问题引起的事件数量也减少了 10 倍。Econocom 的方法包括在 Splunk ITSI 中使用自适应阈值，自适应阈值利用集成机器学习来学习正常行为。过去，CPU 峰值会导致突破阈值，无论这种情况是否真的表明存在问题。现在，Splunk ITSI 中的机器学习功能能够知道哪些峰值在某些情况下属于正常，从而防止突破阈值并减少正在创建的事件数量。

从交换机到仪表板：

通信领导者 找到了新的 解决方案



**平均识别时间
(MTTI) 和平均
解决时间 (MTTR)
急剧缩短**

「世纪互联非常注重客户体验，Splunk 确保了我们的最终用户对我们服务团队及互动感到满意。Splunk Enterprise 和 Splunk IT 服务智能为我们提供实时的高管级 IT 应用程序健康状况可见性。这确保了我们的销售代理可以随时获得对每个客户而言最重要的信息。」

- 世纪互联系统工程部经理 Tim Kerrigan,

自 1930 年以来，世纪互联已从乡村电话运营商发展成为遍布美国乃至全球的消费者、公司和企业宽带、安全、IT 服务和云提供商。

挑战

由于收购关系，世纪互联需要快速了解内部和第三方应用程序。收购之后，世纪互联呼叫中心面临诸多挑战，其原因不在于他们的系统跟不上，而在于他们的通话组合以及完成或修改订单的时间已经改变。世纪互联面临的挑战有：

- 搜集来自各种孤岛和遗留应用程序的信息
- 需要对 IT 和业务操作具有高管级可见性
- 呼叫中心和相关部门转向 IT 寻求帮助而不是独立评估自己的问题

业务影响

借助 Splunk Enterprise 而不求助 IT，呼叫中心可以通过实时仪表板查看自己与其他呼叫中心的比较情况。系统工程部经理 Tim Kerrigan 称：「他们可以扪心自问，我们在一个分流电话上接入 30 到 50 个人之前，程序上是否已经有所变更。」随着世纪互联几乎每个部门都有越来越多的用户部署 Splunk Enterprise，该公司最近将 Splunk ITSI 也添加到其工具库中，汇总一系列关键性能指标和粒度级细节以供高管审查。

到目前为止，能够接受 Splunk ITSI 处理的应用程序包括 XenApp 和一套其他的 Citrix 桌面和服务产品，以及允许多个外部应用程序连接计费系统的关键应用程序编程接口 (API)。将 2017 年其中一月与去年同比，监控改进使 IT 停机、MTTI 和 MTTR 都大幅减少。

环联投资 SPLUNK 解决方案

改善企业监控 提高机器学习 效果

**短短数分钟 (而非数小时)
内即可发现事件根本原因
并减少虚假警报的数量**

「了解客户量模式对企业而言非常重要。如果流量超出特定范围，则会创建警报。
Splunk 机器学习使我们能够尽早进行调查，以确保无缝的客户体验」

— 环联 Splunk 开发人员 **Steve Koelpin**

环联遍布全球 30 多个国家和地区，帮助企业管理风险，同时帮助消费者管理他们的信用、个人信息和身份。

挑战

环联为超过 10 亿的消费者和企业客户 (包括一级金融机构) 提供消费者报告、风险评分、分析服务等等。环联高级监控和运营架构师 Edward Bailey 一直在探索方法来改进：

- 外部客户流量的性能监控
- 客户交易量

业务影响

环联网站上的流量周期是多变的，一天和一周内特定时间的交易量会高于其他时间。借助部署的自动化和机器学习算法，该公司有了监控这些流量周期和交易的新方法。环联目前使用 Splunk ITSI 可视化和组合源自多个应用程序的机器数据，从而创建端到端交易流程。「Splunk ITSI 令我们对每个应用程序的健康状况有更深入的理解，」 Bailey 说：「其帮助我们快速确定根本原因，更快地解决问题。」

近来，环联分析师在解决大型银行客户的流量问题时，都会查看 Splunk 仪表盘。在已经了解一天中特定时间的预期流量的基础上，超出该预期流量数据的流量则被视为异常并生成警报。「了解客户量模式对企业而言非常重要。如果流量超出一定范围，就会创建警报，」 Koelpin 还称，「Splunk 机器学习使我们能够尽早进行调查，确保无缝的客户体验。」

SPLUNK ITSI

Splunk ITSI 是一种监控和分析解决方案，帮助您了解 IT 和业务服务，让您能够应用人工智能由被动 IT 方法转向主动甚至预测性 IT 方法。借助基于机器学习的人工智能，Splunk ITSI 可以在事件发生之前预测对服务的影响并减少事件杂讯，让您腾出时间将重心放在组织发展且保持敏捷性和竞争优势的举措之上。

如果您准备试用 Splunk ITSI，请[注册](#)在线 sandbox，了解如何应对事件风暴和其他 IT 挑战，进而将 IT 数据转换为商业智能。

有关更多客户案例，请[访问我们的网站](#)，了解其他行业如何使用 Splunk 软件获取解决最紧迫的业务问题。

Splunk ITSI 为您提供预测和预防

[→ 了解更多](#)

