

简译版

如何应对应用程序监控挑战

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Managing Today' s Application Monitoring Challenges		
原文作者	杰森·霍沃思(Jason Haworth)	原文发布日期	2022 年 1 月 2 日
作者简介	杰森·霍沃思是 Apica 的解决方案工程副总裁。		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/networking/managing-today%E2%80%99s-application-monitoring-challenges		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	自疫情爆发以来，企业对应用程序测试和监控的需求日益增加。如今，远程访问应用程序的人数比以往任何时候都要多，因此企业在发展业务的同时还需要保护这些应用程序。本文分析了企业制定测试和监控策略时面临的五个挑战。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

如何应对应用程序监控挑战

杰森·霍沃思

2022 年 1 月 2 日

自疫情爆发以来，企业对应用程序测试和监控的需求日益增加。如今，远程访问应用程序的人数比以往任何时候都要多，因此企业在发展业务的同时还需要保护这些应用程序。在下文中，我们将分析企业制定测试和监控策略时面临的五个挑战。

挑战 1：管理成本

我们从利益相关者最关心的问题开始：了解应用程序监控的成本。这包括硬件采购和运营成本，也包括为 Web 应用程序创建工作流所花费的时间成本和其他费用。

现实情况是，大多数 IT 团队一直被要求用更少的资源做更多的事情。因此，IT 团队应采用一种能够减少运营摩擦的测试和监控解决方案，以使用最低的成本提供最多的功能。举例来说，“与第三方应用程序性能监控工具集成”等功能有助于 IT 团队减少购买工具的数量，帮助员工从繁琐的手动任务中解放出来，从而降低成本。

挑战 2：确保可扩展性

可扩展性与成本问题密切相关。对于很多企业来说，在开发过程中编写代码来检查应用程序功能是一回事，在生产中进行扩展是另一回事。为了应对该挑战，企业应进行综合监控（synthetic monitoring）。通过综合监控，企业可以模拟用户旅程，准确地分析用户如何在世界任何地方（在受控和可变环境中）访问企业应用程序。这种方法不仅能够监控本地和 Web 应用程序，还能够监控端点和网站。该方法有助于识别可能影响用户体验的关键因素，包括限制页面加载时间的基础设施、传输网络不稳定和第三方服务集成等。如果无法全面查看应用程序的所有相关项，则无法了解问题的全貌。

挑战 3：通过自动化手段提高效率

企业应提高应用程序的开发效率，这是一项重要的战略，需要企业转变其思维方式。企业应从应用程序开发早期就进行监控（“左移”），以便了解应用程序在当今复杂企业环境中的行为。企业应实现应用程序测试的自动化，以确保部署应用程序时不会遇到任何令人不

快的意外。通过这种主动测试，企业可以从用户的角度了解应用程序应如何运行，以满足用户的需求。

此外，如果正确实施，这些自动化工具有助于企业进行“右移”测试，以确保原始性能能够在实时环境中良好运行。此外，企业需要一个完整的“软件开发生命周期”（SDLC）测试和监控解决方案，以获得产品生命周期各阶段的关键洞察力。为满足这一需求，应用程序所有者应采用自动化工具来简化脚本编写需求，这些工具可以自动将开发周期早期使用的测试脚本导入生产阶段，同时将其集成到现有技术平台中，以节省时间和资金。

挑战 4：解决安全问题

安全始终是企业的头等大事。在开发测试和监控策略时，IT 团队需要记住几个关键因素。每个企业都有其独特的需求。但是，许多企业都需要监控通过单点登录、PIV 智能卡或其他技术访问的应用程序。企业另一个常见的需求是保护凭证，这些凭证能够访问受防火墙保护或使用第三方案（如 CyberArk）的库。通过模拟检查，企业可以确保用户数据的安全性，这对于维护应用程序环境的安全非常重要。此外，这也有助于将多个安全漏洞纳入监控计划中。企业应开发一种能够灵活地与任何制造商的工具配合使用，并提供频繁更新和支持的解决方案，以跟上不断变化的安全需求。

挑战 5：报告工具

即使测试和监控功能配置正确，企业也很难有效地分析它们产生的数据。随着网络基础设施越来越复杂，越来越多的应用程序被采用，监控解决方案产生的数据量也在迅速增长。尽管企业有大量的信息，但他们仍然缺乏真正的洞察力。在许多环境中，信噪比太高，监控无法带来真正的价值。企业真正需要的是，能够帮助其处理棘手业务问题的洞察力。

在评估测试解决方案时，企业应考虑它们的报告功能，以及集成和分析各种来源数据的能力。有效的分析包括针对不同利益相关者创建量身定制的报告，以便他们（而非技术专家）能够理解这些报告并据此采取行动。

结论

随着 IT 应用程序环境的发展，用户需求也在不断变化。客户和员工习惯于随时随地访问应用程序，他们不喜欢遇到访问中断或性能下降问题。为应对这些挑战，企业需要一个强

大的监控策略。企业应在用户旅程的每一步采取主动的测试和监控方法，以保护应用程序并保持关键功能不间断地运行。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：<http://www.antiy.com>（中文）

<http://www.antiy.net>（英文）

安天企业安全公司更多信息请访问：<http://www.antiy.cn>

安天移动安全公司（AVL TEAM）更多信息请访问：<http://www.avlsec.com>