简译版

# 确保安全的情况下加速混合云之旅

**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** | Accelerate Your Hybrid Cloud Journey With Security Confidence | | |
| **原文作者** | 乔治·米娜（George Mina） | **原文发布日期** | 2021 年 5 月 20 日 |
| **作者简介** | 乔治·米娜是 IBM 公司战略联盟项目总监。 | | |
| **原文发布单位** | Security Intelligence | | |
| **原文出处** | https://securityintelligence.com/posts/accelerate-hybrid-cloud-journey-security-confidence/ | | |
| **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** | 随着混合环境的迅速采用，安全团队需要跨本地和云环境实施开放和统一的安全方法。该方法能够将不同的威胁源和云服务与高级分析相连接，从而打破各个团队之间和各个工具之间的孤岛。该方法的基本要素是，跨分布式工作负载提高可见性并集成安全工具。 | | |
| **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。 | | |

# 确保安全的情况下加速混合云之旅

乔治·米娜

2021 年 5 月 20 日

企业正在加速进行云迁移，以推动其业务创新和客户体验。在 LogicMonitor 公司 2020 年的调查中，有 74%的受访者认为，在未来五年内 95%的工作负载将会迁移到云中。随之而来的是，安全团队不仅要应对复杂 IT 环境中不断增长的威胁，还要应对云迁移带来的网络安全挑战。

## 常见的云安全挑战

1. 使用多个安全工具扩展环境，会造成安全态势的脱节。
2. 缺乏对整个威胁环境的可见性，会阻碍威胁调查和响应。
3. 难以跨所有环境和团队创建统一的安全方法。

## 开放和统一的混合云安全方法

随着混合环境的迅速采用，安全团队需要跨本地和云环境实施开放和统一的安全方法。该方法能够将不同的威胁源和云服务与高级分析相连接，从而打破各个团队之间和各个工具之间的孤岛。该方法的基本要素是，跨分布式工作负载提高可见性并集成安全工具。

### （1）建立可见性

随着越来越多的工作负载迁移到云中，了解“谁”在使用“什么”以及“为什么”使用是很重要的。这包括具有统一的云访问和使用情况视图，以及具有适当的策略和控制措施来授予和拒绝访问。为了建立可见性，供应商开始与云服务提供商合作，合作方向包括云原生服务在内的各种技术。这样一来，企业可以创建一种开放式的方法，该方法专注于深度、广泛的技术集成，能够补充其现有的云技术，同时加快其云计算之旅。

### （2）集成和调整安全工具

跨用户、数据、端点和网络获得可见性，对于了解威胁并确定其优先级至关重要，尤其是在混合云环境中。全球托管安全服务提供商 ReliaQuest 将威胁管理平台与全天候技术团队

相结合，强调跨多重云环境获得集中可见性的重要性。

最近，ReliaQuest 首席技术官乔·帕特洛（Joe Partlow）在接受 Information Security Media Group 采访时指出：“93%的企业具有云战略，而大多数企业对其整个企业的可见性只有40%左右。”

“所以说，企业面临很大的可见性差距。对很多企业来说，集中式数据记录是沉重的负担，他们要进行大量的集成和关联，要处理大量的数据——这都需要花费大量的时间。但是，这是必须要做的。”帕特洛说道。

在整个威胁环境中建立了可见性，安全团队就可以采用涵盖云原生服务的解决方案，通过单一面板提供可重复的安全成果。例如，安全人员可以将云配置错误和可疑用户活动自动关联到特定攻击。

## 通过云市场加速数字化转型

随着企业将更多的工作负载迁移到云中以扩展业务，他们开始扩展对云市场的使用，以满足其安全需求。第三方云市场（例如 AWS Marketplace）是安全专家寻找、购买和部署企业运营所需软件和服务的一种热门方式。

“安全是客户进行云部署的首要考虑因素，他们正在寻找与 AWS 本地服务互补的解决方案以改善云安全状况。”AWS Marketplace、服务目录和控制塔业务开发总监克里斯·格鲁斯（Chris Grusz）说。“通过与 IBM 开展技术合作，我们可以帮助客户利用更广泛的混合云威胁监控技术和高级分析技术，从而实现可重复的安全成果和无缝的客户体验。”

越来越多的企业希望简化和扩展其在整个环境中的安全可见性，因此，采用一种开放和协同的安全方法比以往任何时候都更为重要。这种方法利用云市场，跨威胁管理和数字信任域提供安全成果。以下是 AWS Marketplace 中一些帮助加速云计算之旅的例子。

### （1）跨整个威胁环境的可见性和控制力

通过与云原生服务的深度集成（包括高级规则、报告、已保存的搜索和云仪表板），将可见性扩展到最严重的威胁，使安全团队轻松实现威胁可见性并对其进行优先级排序。

### （2）扩展的数据保护

帮助客户在云中扩展和创新，同时在整个数据保护之旅中保护敏感数据。

### （3）安全无缝的身份和访问管理

跨混合环境为应用程序和资源提供单点登录和多因子身份鉴别，同时增强云原生控制措施。

### （4）欺诈检测和基于风险的高级身份鉴别

在客户混合云之旅（包括跨云原生服务的深度和广泛集成）中，帮助客户检测欺诈行为，对用户进行身份鉴别并建立身份信任。

开放协同的安全方法能够为企业赋能，使其随着业务需求的发展不断推进云安全状况。通过与 IBM 合作，云服务提供商能够为客户提供更无缝的体验，并在客户进一步进行云迁移时降低安全复杂性。

# 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