简译版

在多重云环境中保护数据

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	Securing Data in a Multicloud Environment		
原文作者	苏·波伦巴（Sue Poremba）	**原文发布日期**	2020年7月13日
作者简介	苏·波伦巴是一位作家，专长是网络安全和技术领域。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/best-practices-securing-data-multicloud-environment/		
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		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

在多重云环境中保护数据

苏·波伦巴

2020 年 7 月 13 日

根据 Flexera 公司《2020 年云状态报告》，多重云环境已经成为企业的标准，有 93%的企业正在使用此方法。多重云战略中的公有云服务越来越受欢迎——Gartner 预测，2020 年公有云服务的收入将超过 2660 亿美元。

Gartner 研究副总裁西德·纳格（Sid Nag）在去年的正式声明中表示："下一代解决方案几乎都是云增强解决方案，这意味着它们基于云平台的优势来提供数字业务功能。"

每一种下一代解决方案都会带来下一代安全挑战。但是，云应用并不总是以安全性为中心。多重云环境需要使用多个公有云服务，因此更需要安全性。

80%的公司使用公有云来存储敏感数据。但是，这些企业中有 52%遭遇了数据泄露事件。多重云方法能够提供很多优势，包括提高效率和节省成本，但是也带来了一些安全挑战。因此，企业需要了解相关风险，以便从多重云策略中获得最大收益。

接下来，我们将分析多重云环境中可能出现的六种安全挑战，并给出改善安全最佳实践的建议。

1. 依靠供应商来处理安全问题

云供应商已采取安全措施来保护基础架构。企业通常认为这些安全措施能够覆盖其数据和应用程序。实际上，安全是供应商与企业的共同责任，而使用"平台即服务"（PaaS）或"基础架构即服务"（IaaS）的企业责任会更大。企业应清楚地了解供应商的安全保护措施，并与他们合作寻找合适的安全工具来保护其数据和应用程序。

2. 遵守合规规定

大多数企业都必须遵守数据合规性法规、行业标准以及州和联邦法律。每当企业将敏感数据存储在公有云中时，就有可能无法保持合规性。企业应将敏感数据保存在离内部控制最近的服务器中，以保持合规性。在多重云环境中，企业的合规性工作应保持一致。

3. 访问控制

太多的员工能够访问与其工作无关的云数据和应用程序。这使得云面临滥用和网络威胁风险。信息技术（IT）团队应实施更严格的控制措施，并使用身份和访问管理（IAM）工具监控员工的访问权限。

4. 可见性

云服务几乎具有无限的可扩展性，多重云环境可以包括数十个平台。但是，企业是否对其整个环境具备可见性呢？如果企业的网络监控程序无法提供较高的可见性，就会为攻击者敞开大门，这些攻击者渴望利用巨大的、不受监控的攻击面。企业应考虑部署工具，例如“安全编排、自动化和响应”（SOAR）工具，以改善事件响应或安全信息和事件管理（SIEM）。这将有助于收集整个环境中的实时信息，包括日志管理和安全事件通知。

5. 漏洞管理

应用程序和软件都会存在漏洞。要发现这些漏洞，需要经常进行测试。威胁情报软件、定期进行渗透测试和软件扫描可改善漏洞管理。将漏洞管理视为锁上大门，以防止攻击者轻松访问企业环境。

6. 历史数据保护

很多云安全工具都专注于实时数据的使用，而不是深层存储的历史数据。根据数据隐私法，历史数据可能不符合新的合规性规则或标签不正确，从而使其更容易受到攻击。保护历史数据的最佳安全实践包括：改进数据分类以检测不同级别的敏感度，创建数据丢失防护（DLP）策略以在数据泄露时制定行动计划。鉴于标准工具可能无法满足企业的需求，因此企业应确保 DLP 工具可以自定义。

多重云环境对安全决策者带来了独特的挑战。因此，企业必须利用最佳安全实践来保护数据免受网络犯罪分子的侵害。

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