

简译版

## 保护“多重云”安全

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	Same Trick, New Dog: Securing Multi-cloud from the Start		
原文作者	Michael Bushong	原文发布日期	2019 年 3 月 29 日
作者简介	Michael Bushong 是 Juniper Networks 企业云营销副总裁。 <a href="https://www.networkcomputing.com/author/michael-bushong">https://www.networkcomputing.com/author/michael-bushong</a>		
原文发布单位	Network Computing		
原文出处	<a href="https://www.networkcomputing.com/cloud-infrastructure/same-trick-new-dog-securing-multi-cloud-start">https://www.networkcomputing.com/cloud-infrastructure/same-trick-new-dog-securing-multi-cloud-start</a>		
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 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>		

## 保护“多重云”安全

Michael Bushong

2019 年 3 月 29 日

**“多重云”的前提是：资源（无论它们在何处）作为单一、融合的基础设施进行管理。但实现这一目标颇具挑战性。**

在过去的一年中，企业对“多重云”（multi-cloud）的态度有了明显的变化。几年前，企业 IT 部门仍在努力应对云策略，而现在，他们的关注点已从“如何迁移到云”转向“云将走向何方”。随着企业需求的变化和开放技术的激增，多重云作为“压轴大戏”的迹象越来越明显。

随着企业的关注点从云转向多重云，出现了一层新的复杂性。在单一环境中运行尚且面临挑战，跨多个环境运行则会放大这些挑战。在这些挑战中，最重要的就是多重云的安全性。

### 区分资源是否融合

在深入研究多重云安全性之前，我们需要区分“资源是否融合”这一问题。对于大多数企业而言，多重云之旅已经开始，多重云策略的采用通常不是刻意的决策，而是公司内部不同云计划的结果。

多重云的前提是：资源（无论它们在何处）作为单一、融合的基础设施进行管理。这允许以多种方式提供应用，同时又保持运营的一致性。如果“资源未融合”，每个云（或应用）就是独立运营和管理的。

### 运营一致性

运营一致性的概念对于保护多重云的安全至关重要。

我们考虑当前的企业 IT 安全环境：大中型企业都部署了数十种安全解决方案，他们的挑战不仅在于部署这些解决方案，还在于以一种既经济又一致的方式在庞大的基础设施中部署这些方案。

随着公司从云迁移到多重云，运营负担和风险也随之增加。保持强大的安全态势取决于在每个环境中一致地应用策略；而环境的增加会提高复杂程度。

这意味着，拥有多重云策略的企业需要将安全性作为重要的考虑因素。而没有多重云策略的企业需要考虑：如果采用多重云策略，他们的安全实践需要如何演变。早期未采用多重云策略的企业很可能会重新考虑多重云策略，而在各种限制下，他们的改变之路将会非常艰难。

## 分层安全

随着多重云迁移，企业也转向了面向微服务的架构。通过将应用程序分解为更小的部分和分布式通信，企业 IT 部门实现了横向扩展体系架构带来的巨大优势——但这也增加了攻击面。

随着基础设施越来越组件化，安全措施必须不断发展。对代理和应用进行微分段，是增加分层安全的有效手段。在多重云世界中，企业不仅要在一个云中实现分层安全，还要在多个云中实现分层安全。

当然，这会产生额外的运营成本，并且需要深思熟虑的运营控制方法。这样一来，无论底层基础设施如何，安全机制都可以进行统一管理。从本质上讲，安全策略和控制措施应该具有通用性——即，一次指定，然后在各处应用。

攻击者不关心应用是在 AWS 还是 Azure 的虚拟机或容器中。坦率地说，运营者也不必关心。

## 尽早考虑多重云问题

在经济繁荣时期，企业的 IT 支出会高一些。在某种程度上，这使安全思想得以蔓延。只要预算足够，这也是一种可持续的方法。

但在某些时候，企业的预算是有限的。此时，企业将被迫在预算和安全之间做出选择。那么，究竟是预算限制会占据主导地位，还是安全问题会占据主导地位呢？

实际上，不管企业怎么选，都是正确的；但是多重云肯定会加剧这种情况。企业应尽早考虑多重云运营对安全的影响。正如架构师所知的那样，从一开始就奔着一个目标进行设计，比半路改道要容易得多。

## 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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、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有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

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厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，为捍卫国家主权、安全和发展利益提供了有力支撑。

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的发言代表，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>