简译版

通过提高网络可见性来减少云超支

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	Reducing Cloud Overspend By Increasing Network Visibility		
原文作者	马格努斯·比约森（Magnus Bjornsson）	**原文发布日期**	2021 年 6 月 14 日
作者简介	马格努斯·比约森是 Men&Mice 公司的首席执行官。		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/cloud-infrastructure/reducing-cloud-overspend-increasing-network-visibility		
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	随着全球企业继续将云技术集成到基础架构中，这种集成的复杂性可能会导致云超支、收入降低和其他严重的安全问题。通过为网络管理员提供对这些环境的全面可见性，企业可以跨混合和多重云网络统一地址空间，并密切关注所有移动部分。随着云采用率的不断提高，企业需要接受和实施可扩展的网络编排平台，以优化其效率和运营。最重要的是，防止浪费性超支。		
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。		

通过提高网络可见性来减少云超支

马格努斯·比约森

2021 年 6 月 14 日

随着云采用率的不断增加，企业需要优化其效率和运营。最重要的是，要防止浪费性支出。

在数字时代，云技术的使用非常普遍。它们为全球企业提供了令人难以置信的网络和计算优势，包括提高效率、安全性、灵活性、移动性和协同能力。

随着新冠疫情的爆发，云技术的使用呈现出前所未有的增长，预计今后仍将呈指数级增长。根据 Gartner 公司的一份报告，到 2021 年，最终用户在公有云服务上的支出预计将增长 18.4%，达到 3049 亿美元。

不幸的是，云服务的大量使用也会带来问题，特别是在云支出方面。根据 Pepperdata 的数据，超过三分之一的企业的云预算超支高达 40%，而十二分之一的公司甚至超过了这一数字。

这种超支的一个主要原因是：云的使用缺乏集中可见性。这可能会导致重大的意外支出和整体性混乱。

逐渐复杂的云架构

很多企业同时使用多个云提供商的混合云和多重云架构，随着时间的推移，其云架构会变得越来越复杂。出现这种复杂性的原因是，他们将各种云模型、工具和软件集成到现有/新的数字基础架构中，导致网络管理员面临将这些解决方案整合到增强模型中的艰巨任务。

过度配置资源会导致投资回报率（ROI）降低。如果企业无法有效地管理这些复杂的基础架构（或者说多个离散和独立的基础架构），就会出现严重的云超支。此外，在基础架构迁移过程中，企业会使用传统数据中心进行运作（当企业准备过渡到复杂的多重云和混合环境时，就会发生这种情况），这会加剧这种超支。

导致超支的其他问题

更糟糕的是，由于没有通用的云供应商计费模型，混合和云环境也会导致过于复杂的计

费结构和支出。每个供应商都会提供不同的支付模式，而企业要使用多个供应商来获得不同的许可，满足各种使用模式（基于人员或部门）和需求。久而久之，其网络可见性就会变得模糊，导致企业在优化成本时面临更大的复杂性。

网络可见性：看得见才是王道

当企业缺乏完整的云可见性时，除了成本效率低下之外，还会出现其他问题，尤其是在运营方面。例如，重叠的地址空间会导致网络集成和迁移问题。当企业整合新的云结构时，他们要非常小心谨慎，以确保他们在整个基础架构中保持网络可见性并进行网络运营管理。

此外，复杂的多平台网络容易出现人为错误。从运营和安全的角度来看，人为错误会导致配置错误和组件故障。可见性有限引发的安全问题会带来漏洞，例如未被发现的老旧 DNS 记录。攻击者可以利用这些漏洞，他们只需伪造一个子域就能严重破坏企业的运营。

随着全球企业继续将云技术集成到基础架构中，这种集成的复杂性可能会导致云超支、收入降低和其他严重的安全问题。通过为网络管理员提供对这些环境的全面可见性，企业可以跨混合和多重云网络统一地址空间，并密切关注所有移动部分。随着云采用率的不断提高，企业需要接受和实施可扩展的网络编排平台，以优化其效率和运营。最重要的是，防止浪费性超支。

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