

简译版

增强企业云安全的三个最佳实践

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	Three Best Practices to Enhance Your Organization' s Cloud Security		
原文作者	阿肖克·桑卡尔 (Ashok Sankar)	原文发布日期	2022 年 4 月 4 日
作者简介	阿肖克·桑卡尔是 ReliaQuest 的产品和解决方案营销副总裁。		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/cloud-infrastructure/three-best-practices-enhance-your-organization%E2%80%99s-cloud-security		
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	企业的未来在于云，他们必须将云安全视为重中之重。此外，企业应全面了解其安全环境并采取本文所述三项最佳安全实践，以获得真正、持久的网络安全态势：（1）消除盲点；（2）统一检测、调查和响应流程；（3）熟悉云提供商的安全策略。		
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。		

增强企业云安全性的三个最佳实践

阿肖克·桑卡尔

2022 年 4 月 4 日

在过去的几年里，越来越多的企业加速迁移到云，这一趋势没有任何放缓的迹象。事实上，2021 年的一项研究发现，93%的企业采用多重云战略，而 87%的企业拥有混合云战略。

但是，云的采用会增加企业的网络安全风险。企业需要了解并解决其云迁移战略可能存在的安全漏洞，以便在不影响企业安全的情况下成功进行云迁移和运营。

为确保在云迁移时能够妥善保护数据，安全团队和领导者可以采取以下三个最佳实践。

1. 消除盲点

企业无法保护他们看不到的东西——没有可见性，就无法实现云安全。Ponemon 最近的一项研究显示，只有不到 33%的受访者表示有信心了解企业使用的所有云计算应用程序、平台或基础设施服务，而表示能够保护这些内容的受访者比例就更低了。另外 62%的受访者表示，覆盖差距和缺乏可见性，使得他们很难在多重云环境中保护数据和应用程序。

要想创建强大的安全程序，获得云可见性是非常必要的。这种可见性的优势包括：

- 降低风险：有助于安全团队主动采取措施来减轻威胁。
- 威胁猎杀：有助于安全团队搜索异常行为和攻击共性，从而清除安全威胁。
- 更快的响应：在对抗威胁时，快速响应至关重要；通过将可见性与自动化相结合，安全团队可以快速收集数据并采取行动。
- 简化云管理：增强可见性有助于安全团队更好地管理复杂的云环境。

2. 统一检测、调查和响应流程

除了可见性，有效检测、调查和响应威胁的能力也很重要。如今，企业的安全团队面临大量需要防御的威胁和大量需要管理的安全工具，这导致误报、告警疲劳和倦怠等情况不断出现。

出现这些问题的根本原因是：检测内容不正确，检测效率低。很多时候，企业部署的检测规则不够具体，在检测高级威胁时覆盖性不足。另一个原因是缺乏有效的分析。很多时候，分析师没有获得正确的情境信息，这会导致噪音增加。他们采用“转椅式方法” (swivel chair approach) 从多个来源收集相关数据，有时会遗漏重要数据，导致检测结果不理想。而手动、不一致的响应流程，也会进一步损害企业的安全态势。

为了实现有效的安全运营，企业需要统一检测、调查和响应流程，并确保这些流程的一致性和自动化。企业应帮助分析师从手动、重复的任务中脱身，以便他们可以专注于更高优先级的任务。

3. 熟悉云提供商的安全策略

企业还应了解其云提供商的安全策略。“共担责任模式”划分了公有云服务商和客户的安全义务。

- 公有云服务提供商负责确保“云”的安全性
- 客户负责在“云中”的安全性

具体情况取决于企业使用的云提供商。但是，要想在公有云中确保安全性和合规性，云提供商和客户都需要采取安全措施。通过了解云提供商的策略，企业可以确定他们需要关注哪些方面。无论企业使用 AWS、Azure 还是 GCP 作为其云提供商，熟悉他们的策略都至关重要。举例来说，AWS 负责保护运行云服务的硬件、软件、网络、设施和其他物理基础设施。相比之下，客户的义务则取决于他们选择的云服务类型（“基础设施即服务” [IaaS]、“平台即服务” [PaaS]或“软件即服务” [SaaS]）。此外，选择的云服务类型不同，客户需负责的配置也不同。通过与第三方合作，企业可以更全面地了解威胁情况，从而轻松有效地管理云安全问题。

企业的未来在于云，他们必须将云安全视为重中之重。此外，企业应全面了解其安全环境并采取上述安全实践，以获得真正、持久的网络安全态势。

安天简介

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。通过 20 余年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势，打造了面向服务器、云、虚拟化、容器和传统办公节点等提供全防御能力覆盖的智甲安全产品家族，满足客户对于包括终端杀毒、终端防护 (EPP)、终端检测与响应 (EDR)、云工作安全防护 (CWPP) 等系统安全层面需求；整合强化包括 ATID 威胁情报门户、追影沙箱和捕风蜜罐等产品在内的威胁情报板块产品，有效提升客户情报赋能和自主情报生产能力；基于流量产品探海有效应对客户对于网络威胁检测与响应 (NDR) 和网络流量分析 (NTA) 的安全需求，相关产品可以实现交叉联动，统一管理，形成面向从勒索软件到高级威胁 (APT) 的纵深安全防线。同时打造威胁对抗、威胁猎杀、威胁巡检服务三款主打安全服务，辅以平台支撑、快速到达的轻量级垂直响应服务，以运营模式有效支撑应对综合威胁对抗能力升级。

安天为网信主管部门、军队、部委、保密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，已连续七届蝉联国家级网络安全应急支撑单位。安天参与了 2005 年后历次国家重大政治社会活动的安保工作，获得杰出贡献奖、安保先进集体等荣誉称号；自 2015 年来，安天的产品与服务为包括载人航天、探月工程、空间站对接等历次重大航天飞行任务，以及大飞机首飞、主力舰护航、南极科考等重大任务提供安全保障支撑。

目前，安天的威胁检测引擎为全球超过一百万台网络设备和网络安全设备、超过三十亿部智能终端设备提供了安全检测能力，已经成为“国民级”引擎。

安天已发展成为以哈尔滨为总部基地，建有六地研发中心、两个控股子公司，参与一个国家工程实验室建设，拥有两个省级工程中心和重点实验室、一个博士后创新创业基地和多个高校联合实验室的集团化创新企业，同时在地多设有办事处和应急响应站，为客户提供全面的安全服务与技术支持。

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>