简译版

保护云运营远离当今网空威胁的 5 种策略

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	5 Strategies to Secure Cloud Operations Against Today's Cyber Threats		
原文作者	克里斯·克里斯图（Chris Christou） 布拉德·博留（Brad Beaulieu）	**原文发布日期**	2020 年 2 月 20 日
作者简介	克里斯·克里斯图 Booz Allen 咨询公司的云安全总监。 布拉德·博留 Booz Allen 咨询公司的云安全工程师。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/cloud/5-strategies-to-secure-cloud-operations-against-todays-cyber-threats/a/d-id/1337033		
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。		

保护云运营远离当今网空威胁的 5 种策略

克里斯·克里斯图、布拉德·博留

2020 年 2 月 20 日

云曾经被吹捧为 IT 的灵丹妙药，但当恶意行为者利用其安全漏洞时，我们经常在新闻头条中看到云的另一面。这一点重复再多也不为过：在云环境与本地环境中保护数据和网络的方法是非常不同的。

曾经静态的本地基础设施元素现在被抽象为软件。保护云的安全必须适应不断变化（扩张或者缩减）的基础构架。在云中，您将需要更多地专注于应用程序、应用程序编程接口和用户角色。

根据我们在企业和政府云客户方面的经验，下面有五个小技巧可以重新强调并扩展基本策略。

1. 控制对云管理和配置工具的访问

由于云管理和配置工具——云服务提供商（CSP）控制台、命令行界面和应用程序编程接口（APIs）——为终端用户提供了极大的灵活性和自主性，因此，强大的基于角色的访问控制对于保护组织机构免受外部和内部的威胁至关重要。

- 使用双因子身份验证、数字签名和证书对特权用户进行身份验证与授权。
- 在授予云角色之前，必须对相关人员进行培训和技能评估。
- 严格区分用户和管理员凭据，并限制用户对生产系统的访问。
- 规范化帐户生命周期管理流程。

2. 加密敏感（或所有）数据

在云中，数据泄露和数据渗出是不可避免的。随着“动态数据和静态数据的概念变得模糊”，通过加密等技术保护传输中的数据变得更加重要。

加密所有敏感数据，并使用多个密钥对数据进行分段，以最大程度地减少泄露密钥对安

全的影响。应定期更换密钥，并使用强大的访问控制策略。

- 加密传输中的和静态的数据。
- 评估 CSP 网络加密（并非数据中心之间的所有网络流量都可以进行本地加密）。
- 评估原生云和第三方加密解决方案。

3. 使用自动化，以最大程度地减少因配置错误引起的人为错误

手动配置错误最终会导致人为错误，并带来以下后果：部署配置不一致、意外的数据泄露以及被恶意活动利用的漏洞。这是个很大的安全风险。根据 Gartner 的研究，几乎所有（99%）的云安全故障都是由人为的错误引起的。

通过预测试和配置审核，自动化可以确保部署和基础设施配置的正确。我们提出以下建议：

- 实现基础设施与平台构建、安全测试、安全防护和基线配置的自动化。
- 实现高可用性配置，以减少由于云提供商错误而导致的区域或区段不可用风险。
- 定期执行配置检查和例行危害评估。

4. 调整可见性和漏洞管理，以管理临时性和新型云资产

对于云解决方案——由于数据、系统和职责分散在各个环境中——组织机构可能缺乏足够的可见性来监控威胁和确保合规性。此外，涉及人工的漏洞检测和修复管理的传统方法在云环境中可能过于缓慢或繁琐，因为在云中，事件会以极快的速度在互连系统和数据之间移动。

资产迁移到云中会引发许多可见性问题：

- 您的基础架构是否允许跨云环境查看？例如，您是否有一个由日志、仪表板和报告组成的聚合系统，可以从网络设备、云基础设施、操作系统、应用程序等收集数据？
- 您是否了解您的云供应商的事件响应服务级别协议，以及如何将它们聚合到您自己的流程中？

组织机构需将漏洞管理工具扩展到容器和无服务器架构，并调整这些工具以适应快速的

基础设施部署周期和新的云服务。他们还将受益于代理和网络覆盖等内联服务，以便将流量复制到“透明”安全服务。

5. 在整个运营生命周期中实施改进措施

通常，初始云的实现只是一个开始。随着应用程序的引入，IT 团队需要不断改进。传统的“烟囱式”IT 运营可能会阻碍云敏捷性的发展。

DevSecOps 方法可以提供帮助。当您采用这种方法时，请执行以下操作：

- 配备现场可靠性工程师，使运营人员能够继续升级环境。
- 安全人员利用 DevSecOps 来进行开发和运营。
- 跟踪新产品和服务，制定未来集成的路线图。

基于这五个基本策略，组织机构不仅可以降低其面临的安全性和合规性风险，还可以获得云的许多好处：节约成本、降低总体拥有成本以及缩短价值实现的时间。

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，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万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