简译版

2021 年必不可少的五种云安全策略

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 Cloud Security Must-Haves in 2021		
原文作者	迈克尔·马西米（Michael Massimi）	**原文发布日期**	2021 年 3 月 24 日
作者简介	迈克尔·马西米是 IBM 云安全服务全球业务主管。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/posts/5-cloud-data-security-must-haves-in-2021/		
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	据估计，目前有 9.9 亿台配置错误的云服务器。除了云配置错误外，还有各种混合云和多重云问题。这么多问题很难同时解决。为了节省时间，提高生产力，企业应从五个基本概念入手，以改善云安全计划的成果。		
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。		

2021 年必不可少的五种云安全策略

迈克尔·马西米

2021 年 3 月 24 日

进行云迁移的企业，面临着大量令人困惑的流行语，包括“混合云”、“多重云”、“数字化转型”、“微服务”等等。即使在这种情况下，任何企业级云迁移策略都要考虑云数据的安全性。

许多企业认为，解决关键的安全和合规性需求是一个沉重的负担。这种担忧是合理的——据估计，目前有 9.9 亿台配置错误的云服务器。

除了云配置错误外，颇受关注的混合云和多重云问题还包括：

- 创建云就绪的安全策略
- 缺乏经验和专业知识，以及对技能的要求不断提高。
- 满足合规性要求
- 集中化的可见性和威胁管理
- 过多的新工具和技术
- 维护私有/公有云环境中的安全策略

这么多问题很难同时解决。为了节省时间，提高生产力，企业应从下述五个基本概念入手，以改善云安全计划的成果。

云监管策略

每个成功的云安全计划，其核心都是明确定义的策略，包括：

- 为云环境建立安全基线
- 了解企业有哪些关键数据，关键数据在哪里，以及谁有权访问这些数据。
- 确定安全性、合规性以及行业或法规要求。
- 开发正确的控制措施以满足这些要求

- 建立目标状态和路线图，并予以执行。

云原生安全

企业可能要考虑，来自云服务提供商（CSP）的云原生安全控制措施是否可行，或是否能够保护企业环境。CSP 的云平台中包含各种安全控制措施，这些控制措施可以提供许多优势，包括限制企业要管理的第三方许可证的数量、灵活的使用方式、易于集成等。

云原生安全策略需要考虑以下问题：

- 云原生控制措施是否足够成熟，或者能否提供适当的可见性，以满足企业的合规性要求？
- 哪些云原生控制措施最适合企业的混合云和多重云环境？
- 企业是否具备相关技能来管理新的、快速增长的安全技术？
- 如何正确设计、实施和配置这些控制措施，并将其集成到其他安全运营中？
- 如何处理所有新的云安全数据，可以采取什么决策或行动？

确定适合企业的云原生控制措施后，要想有效地管理这些控制措施，首先要确保企业具有适当的体系结构和策略来支持其业务和法规要求。此外，企业还应拥有一个强大的监管层，以便根据云原生数据和告警制定决策。

云安全态势管理

对于云网络安全计划而言，正确的配置和持续的云环境合规性至关重要，但是这可能很复杂，难以进行监控。企业中可能有多个团队或业务部门使用云服务，而且要遵守互联网安全中心（CIS）等组织的标准。如果云环境过于复杂，则无法快速获得云情境信息和关联信息，无助于企业检测和响应云安全问题。

企业应考虑进行云安全态势管理，来解决这些复杂性并实现以下目标：

- 连续监控实时云资产，以实现合规性、监管报告和审计目的。
- 通过敏捷的检测和对云配置错误的响应，来防止攻击。
- 不断强化安全性和合规性态势

- 嵌入安全见解，并针对云异常情况进行自动化处理。

云工作负载和容器安全

企业的应用程序容器环境可能面临以下问题：安全复杂性和可见性的挑战，在快速扩展和交付期间的测试时间有限，流量增加以及容器受到威胁等。容器环境的以下阶段可能会面临风险：

- 图像创建、测试和认证
- 图像存储注册
- 编排程序检索
- 用于部署的容器
- 用于管理的主机操作系统

幸运的是，企业已有措施可保护混合云和多重云环境的容器工作负载。经过全面的评估并创建策略后，企业需要在容器生命周期的所有阶段考虑集成服务、设计和实施以及持续的管理。具备这些功能后，企业将获得 Red Hat OpenShift，Kubernetes，Docker 和其他容器平台的以下安全优势：

- 增强现有云容器服务的安全状态
- 在混合云环境中托管安全服务
- 帮助实现容器环境的合规性要求
- 管理所有安全功能的单一面板

DevSecOps 和应用程序安全

开发团队主要致力于尽快为消费者开发新的应用程序和功能。运营团队则致力于确保系统的响应速度和稳定性。为了满足云中快速创新的需求，企业应集成开发和运营，以促进协同，在开发与质量之间取得平衡。

安全团队应确保，那些快速的应用程序部署没有漏洞，符合法规和公司的要求。

为了最大程度地满足安全团队的目标，企业应考虑转向 DevSecOps 方法。DevSecOps

是一套综合的实践，代表安全人员的文化、流程和技术水平。

通过将 DevSecOps 和安全开发实践添加到工作负载中，企业可以获得以下优势：

- 创建敏捷、精益和持续的反馈文化，使其与企业的安全策略、风险、监管和合规性要求保持一致。
- 使用现代工具实现每个流程的自动化，以提升处理速度，增强可靠性和安全性。
- 鼓励创新，通过反馈循环和协同增强自治性和安全部署。

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