简译版

2022 年值得关注的三个云安全趋势

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	3 Cloud Security Trends to Watch in 2022		
原文作者	大卫·比森（David Bisson）	**原文发布日期**	2022 年 1 月 18 日
作者简介	大卫·比森是一位信息安全记者 。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/3-cloud-security-trends-2022/		
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	2022 年，企业和机构很可能会将更多服务转移到云中。ITProPortal 的数据显示，IT 部门 28%的支出将转移到云服务，这将导致 1.3 万亿美元的支出。网络安全网格、多重云和混合云安全策略以及云原生工具可以帮助他们做到这一点。		
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。		

2022 年值得关注的三个云安全趋势

大 卫 · 比 森

2022 年 1 月 18 日

进入 2022 年，许多企业都在考虑云安全问题。早在 2021 年 4 月，Gartner 就预测到，2022 年全球最终用户在云管理和安全服务上的支出将达到 1800 万美元，比前两年增长 30%。

那么在 2022 年，企业和机构会在哪些方面进行云安全支出呢？总的来说，有三个趋势值得关注：网络安全网格、混合和多重云环境，以及云原生工具和平台。

1. 网络安全网格

在 2022 年 TOP 战略技术趋势列表中，Gartner 将网络安全网格定义为“一种灵活、可组合的架构，能够集成广泛的安全服务。”网络安全网格提供了一种在所有相关环境中（包括云环境）验证身份、情境和策略遵守情况的方法。因此，企业可以将网络安全网格架构作为其防御策略的一部分。

首席信息安全官尼尔·哈珀（Niel Harper）对此表示赞同。

“我们的目标是将封装数据中心的边界转移到……不在本地或不在同一网络上的身份和对象。特别是，用户可以随时随地使用各种设备访问对象。”他说，“网络安全网格还能帮助企业将云服务纳入其零信任架构，并采用自适应访问控制，对身份和对象进行更精细的分析。”

为了实现这一点，企业应投资于一系列控制措施。这些控制措施可以帮助企业将零信任、云安全和其他计划结合在一起。哈珀指出了与云相关的两个关键措施——云访问安全代理和云基础设施授权管理。此外，端点检测和响应，多因子身份验证等措施也包含在内。

2. 混合和多重云环境

网络安全网格等防御方案不仅能够支持零信任策略，还有助于保护混合和多重云环境。

越来越多的企业和机构转向混合和多重云策略。我们以混合云为例。Cofense 公司报告称，到 2022 年，90%的企业将使用混合云策略来满足他们的需求。一些企业的策略包括公有云和私有云服务，另一些企业的策略包括云端和本地资产，还有一些企业的策略可能包括

上述两者。

多重云的情况与此类似，该战略包含多个云服务。在一项针对 IT 领导者的调查中，95%的受访者表示，他们会将多重云作为 2022 年的战略重点。约 96%的受访者表示，云安全是首要考虑因素。只有 54%的受访者表示，他们对执行防御计划所需的工具或技能非常有信心。但是，也有 76%的受访者表示，他们觉得团队没有在多重云项目上投入足够的资金，导致他们无法做好防御数字威胁的准备。

也就是说，混合云和多重云环境给企业带来了安全挑战，它们增加了企业环境的复杂性，从而降低了企业的可见性。

为了应对这些挑战，企业可以考虑使用第三方云市场，例如 AWS Marketplace。这些资源能够为安全团队提供可以在云中使用的软件和服务。

3. 云原生工具和平台

Gartner 还强调了云原生平台的重要性。这些平台使企业和机构能够构建充分利用云的应用程序架构。毕竟，企业的内部团队可以充分保护本地资产，却无法同样地保护云资产。这是因为，共享责任模型规定信息安全人员仅“在云中”提供安全性。云服务提供商负责云的安全性或保护物理主机，这种划分限制了内部团队对安全工作的控制程度。

要想充分利用云原生工具和平台，企业需要了解他们需要负责防御边界的哪一部分。然后，为这一部分配置正确的工具。如果不这样做，企业或机构就会存在能够被攻击者利用的云漏洞和错误配置。如果发生云安全事件，企业的恢复成本会更高。

为什么说云安全很重要?

2022 年，企业和机构很可能会将更多服务转移到云中。IT 部门 28%的支出将转移到云服务，这将导致 1.3 万亿美元的支出。

企业领导者需要保护基于云的服务。网络安全网格、多重云和混合云安全策略以及云原生工具可以帮助他们做到这一点。

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