通过不断演变的云安全战略实现业务发展

2020 年 3 月 17 日 | 作者：Ali Robles | 阅读时间：3 分钟

我们都听过“城堡与护城河”的比喻，它描述的是传统的集中式网络安全方法。随着云安全性在现代环境中的重要性日益提升，我认为我们应在关于安全性的类比中增加一个元素，即“雾”。有时雾很浓，您几乎看不到前方或内部情况。

在您迁移到云端时，安全性和可视性是您绝对不能轻视的两个要素。

为什么云安全非常重要？

云技术正在不断发展；从长远来看，发展业务的唯一方法就是围绕您的云环境制定适当的安全战略。MarketWatch 调查结果显示，2019 年，全球云计算市场规模为 627.3 亿美元，预计到 2026 年底，将达到 3837.8 亿美元，从 2021 年到 2026 年的复合年增长率 (CAGR) 为 29.2%。

云安全是迁移到云端的主要障碍之一，因此任何组织都不能忽视云安全。尽管在所有受访组织中，有 75% 的组织会在 2020 年部署多云模型，但仍有 80% 的企业工作负载尚未迁移到云端。唯一的方法就是制定明确的云安全战略；无论组织的规模或成熟度如何，都需要在混合多云环境中具有良好的可视性。

让我们看一下最常用的云平台和云服务类型，然后深入探讨一下我个人认为的几个最常见挑战，以及如何帮助您的安全团队更好地应对这些挑战，而无论您的工作负载位于何处或“雾”的密度如何。

不同类型的云部署

在四种主要类型的云平台（私有云、公有云、混合云和多云）中，混合云和多云是最受所有行业和规模的组织欢迎的云平台。

混合云是一种混合使用内部私有云和第三方公有云服务并通过编排将两者集成到一起的环境。

在多云模型中，组织会利用两个或多个云平台来执行各种任务。不希望依赖单个云提供商的组织可以选择使用多个提供商的资源，进而从每种独特的服务中获得最大收益。

关于云服务，Gartner 的调研结果显示，软件即服务（SaaS）产品仍然是最大的细分市场，并且预计将会继续稳定的市场增长。第二大市场是基础设施即服务(IaaS)。

四个关键的云安全挑战

无论您的组织使用哪种云模型或类型，安全都是不容忽视的一个要素。在谈及安全性时，组织目前面临着诸多挑战，但就我个人的观点而言，以下四个是最关键的挑战。

1. 缺乏专业知识

安全专业知识，或者说安全专业知识缺乏仍然是一个关键问题。无论您处在云之旅的途中还是刚刚踏上旅程，您都需要配备了合适安全工具的合适人员，确保您的团队能够跟上这一快速发展的技术。

2. 可视性

可视性是您的团队需要解决的首要挑战之一，因为您无法控制不可见的事物。若要在攻击生命周期的早期识别威胁和异常，重要的一点就是：无论您采用何种云部署模型，安全团队都必须全面了解整个环境中的系统、网络、应用和活动。

3. 管理合规性

管理合规性是组织的另一个大问题。公司需要跟上不断变化的法规和标准，其中某些法规和标准因行业或国家/地区而异，例如 GDPR、FISMA、SOX、HIPAA、ISO 27001、PCI 等。如果组织无法跟上步伐，就可能会面临严重的合规和监管罚款。

4. 缺乏控制

缺乏控制也是要考虑的挑战之一。如果您与其他每个组织一样也使用公有云服务，则您的组织将不会拥有云服务运行所在硬件、软件或应用的所有权。您需要确保您的云提供商具有适当的安全态势。

通过不断演变的战略保护您的云环境

企业需要借助正确的工具来获得更好的可视性，并快速检测和解决威胁，无论威胁发生在何处。若要实现实时威胁检测，团队可能需要与 Amazon Web Services (AWS)、Azure、SalesForce.com、Office 365 和 IBM Cloud 等云服务以及传统内部基础架构深度集成的解决方案。

根据您的云服务模型，您的组织将会与您的云供应商共担一些责任。不过我认为，您的安全团队应不断监控并优化其云安全流程。如果您拥有 SIEM 即服务解决方案，便可帮助您的安全团队应对不断增长的威胁、复杂的安全项目和合规性要求，而无需考虑技能短缺或管理多个供应商和产品的挑战。

目前组织会采用不同类型的云部署和服务模型，并且仍有大量工作负载保留在内部环境，因此威胁形势每天都在变得愈发复杂。在准备或加强云迁移时，适应不断发展的安全战略至关重要。

Ali Robles

IBM Security 安全智能产品营销总监

Ali 拥有 20 多年的市场营销经验，曾在拉丁美洲、中东和非洲从事产品营销工作，之后负责全球范围的营销业务。她在安全领域拥有超过 7 年的经验，主要专注于 SaaS 和云，而且会积极与其他地区的同事开展协作。