FORTINET

云安全分析和策略管理

安全架构师应在解决方案中寻求哪些优势

目录

要点综述

组织在大规模部署各种公有云平台的过程中，遇到了日益复杂的安全问题。各个云提供商的原生安全工具各不相同，并且互不兼容。跨所有云的风险管理导致多云环境中的安全操作既耗时又低效。此外，攻击面不断扩大，组织必须确保自己远离云平台应用编程接口 (API) 和用户界面 (UI) 带来的风险。配置和管理错误以及应用本身都可能会带来这些风险。

本文讨论了负责保护公有云基础设施的安全团队面临的五个关键用例：(1) 风险管理，(2) 数据安全，(3) 流量分析和调查，(4) 威胁检测和响应以及 (5) 合规性。五个用例均涉及云环境面临的独特挑战。它们的首要安全任务便是整合安全架构，以实现集中可见性和控制。由于各个公有云之间的差异，集中可见性和控制是无法通过手动实现的。整合架构可帮助组织主动、系统地应对这些挑战，从而提高运营效率并降低风险。

83%

到 2020 年，83% 的企业工作负载将在云中运行，63% 的 IT 专业人员认为安全性是其中最值得关注的问题。[1]

简介：应对云蔓延趋势

组织扩大了公有云计算的部署规模：2019 年，全球公有云服务市场预计将增长 17.3%，达 2,060 亿美元，其中基础设施即服务 (IaaS) 增长速度最快，达到 27.6%。[2] 简单数字背后是云平台势不可挡的吸引力。无论采用哪种云服务（IaaS，PaaS，SaaS），组织都能快速部署，动态扩展，仅支付已使用的容量及节省部署成本和人力成本。

但十年甚至更久之后，云资源激增，许多组织将遭受所谓的【云蔓延】的困扰。大多数组织都运营着多个云，网络安全团队常常难以跟踪资产并准确识别这些动态环境中的风险。由于多部门参与云采购，并且 IT 部门通常不是最终决策者，最终加剧了这一问题。此外，各个公有云提供商的内置安全工具都有自己的工作方式，跟踪不同的安全数据集。

本文介绍了公有云安全领域的五个关键用例，并讨论了每个用例的有效解决方案应具备的特征。

“今年，IaaS 收入预计增长 27.6%。” [3]

风险管理：云配置的企业视图

当今市场瞬息万变，仅遵从固有的规则和标准是不够的。每个组织都必须评估其网络风险态势，并根据其风险承受能力，制定安全计划。组织面临的风险主要是由于云管理平台和应用组件中的系统配置错误造成的。[4] 报告显示，70% 的云数据泄露源于配置错误，该数字同比增长了 424%。[5]

在本地静态环境中，可使用配置管理数据库 (CMDB) 解决这些问题。但快速变化的云服务和配置带来了新的挑战。多云服务造成了碎片化的可见性，而且云部署动态多变，组织很难一致地评估其安全状况，最终为日益复杂的基础设施带来了配置错误风险。

要解决这些问题，首先应建立集中可见性，并跟踪整个云基础设施的配置状态和态势的变化。有了这个大的视图后，云安全解决方案应能够执行全面的风险评估，生成风险评分并提供最佳实践建议以进行改进。评估完成后，应持续监控组织的云基础设施，以确保及时标记并解决问题。最后，使用分析工具来帮助安全团队了解在整个多云环境中配置更改的生命周期。

“云技术是 2019 年企业数字化 转型的重中之重。”[6]

数据安全：持续监控数据丢失和恶意软件

云基础设施的无序蔓延会导致用户跨云基础设施存储数据集时，以无序的方式存储未经过请求的数据集。潜在恶意代码可能会因此被嵌入文件，带来巨大的未知风险，并增加数据泄漏的风险。如果是后者，就需要一个覆盖整个云基础设施所有文件和存储的整合视图。除了全面的多云文件扫描和监控解决方案以外，其他任何方法都无法识别危险的文件传输模式。

如今，威胁的数量越来越多，代价也越来越昂贵。2018 年第四季度，FortiGuard 实验室检测到近 3.4 万个新型恶意软件变种，比第一季度增长了 128%。[7] 新研究发现，2018 年，典型组织的网络犯罪成本为 1,300 万美元，较 2017 年增加 12%，较五年前增加 72%。[8] 因此，扫描云存储中的文件是防止高风险内容传播的唯一方法。

为了保护多云基础设施中的关键数据，组织需要能够持续监控 (1) 存储的文档，以识别恶意软件；(2) 带有敏感数据的活动，以识别和调查环境中的数据泄漏。

“随着越来越多的设备和关键数据迁移到云端，恶意攻击的类型可能不会发生很大变化，但攻击方式却一定会发生变化。” [9]

流量分析和调查：借助全面视图检测攻击

云蔓延存在两个问题，即潜在的配置错误导致网络入侵风险增加和组织无法充分监控网络流量。问题的根源在于安全团队成员通常没有现成的公有云资产和资源可用，当然无法随时监控这些资源的变化。[10] 即使拥有准确的资产数据，监控各个云内部和云之间的流量以及检测流量中的可疑活动也需要特定的工具。

为了有效地检测和补救网络入侵并保护关键服务，安全团队需要能够查看所有云资源的当前拓扑结构、监控和分析网络流量，以及深入研究可疑的特定服务和流量模式。具体来说，他们需要能够可视化网络流量，以便更有效地区分错误配置和恶意流量模式。

近 45% 的安全架构师认为他们的组织在处理安全问题时应化被动为主动。[11]

威胁检测和响应：集成智能和实时共享

随着组织将更多应用迁移至公有云，并且使用更多云原生服务，复杂性日益增加。复杂性增加造成配置错误机率增加。鉴于此，特别是考虑到当前复杂的威胁形势，组织亟需一种集成式威胁检测和响应方法。公有云威胁产生的原因多种多样，包括云本身的错误配置、使用易受攻击的软件版本以及执行云应用中的不安全代码。

组织首先要做的应该是阻止网络犯罪分子利用这些漏洞。安全团队需要能够识别和隔离威胁，并有效地进行补救。安全团队进行安全调查时，需要有安全工具简化他们的工作，以便为 DevOps 团队提供有意义且用户友好的洞察。

威胁类型从十年前的 50 种增加到了目前的 100 多万种[12]

合规性：用于快速补救和审核准备的集中报告

随着越来越多法规的出台以及媒体对组织网络安全问题的愈加关注，合规性日益成为几乎所有组织的头等大事。《欧盟通用数据保护条例》(GDPR) 等较新法规对不合规行为处以高额罚款，其他司法管辖区也在制定类似法规。[13] 别的一些法规也会带来挑战，例如支付卡行业数据安全标准 (PCI DSS) 可能导致企业无法接受信用卡和借记卡，这对许多企业来说都是灾难性的。

各种各样的要求使合规性和审计准备工作变得复杂，消耗了许多组织员工的宝贵时间。由于每个云提供商和 IaaS 解决方案的报告工具和事件数据都相互独立，各不相同，因此多云基础设施的合规报告更加复杂。与此同时，公有云增加了攻击面，带来了新的威胁载体，因此也需要纳入合规性评估中。

与我们描述的其他业务需求一样，高效的合规报告需要一个集成多云架构的综合框架以支持集中可见性和策略管理。这种可见性应包含公有云环境历史快照维护能力。安全团队必须寻找一款具有现成策略的强大报告工具，以满足各种法规和标准要求。报告需要能够设置为定期运行，以便安全团队能够快速发现违反策略的行为，从而采取补救措施。这些流程还需要做到自动化，从而为负担过重的安全团队减负，同时最大程度降低风险。

“在过去的一年中，法律和网络安全团队花费在响应入侵上的时间增加了20%。”[14]

结论：集成是关键所在

本文的每一页都在强调公有云资源安全控制的集成，这是确保公有云安全的重中之重。集成可帮助组织保护数据、防止入侵、抵御高级威胁以及满足审核员的要求。由于公有云基础设施是在应用和网络系统之外配置的，而且它们内置的安全工具使用的方法各不相同，因此手动集成几乎是不可能的，并且鉴于当今网络威胁的演变速度，手动集成在效率上也注定跟不上。组织显然需要一种专用工具来统一提供可见性和控制，以确保公有云管理界面和 API 安全无虞。

使用多个云、多种服务的组织必须寻求一款统一的安全工具，它需要与每个主要云平台原生集成，能够实时整合来自每个云平台的威胁情报，对云内部和云之间的流量进行智能监控，并具备强大的报告和分析工具。只有通过对整个基础设施的完全可视化和集中控制，组织才可以在不增加风险的同时，充分利用云计算的巨大优势。

“在数字企业中，现有孤岛的战略融合将带来更丰富的客户体验，实现业务加速和运营敏捷性。”[15]

1 Louis Columbus，2020 年，83% 的企业工作负载将在云中运行，福布斯，2018 年 1 月 7 日

2 Louis Columbus，2018 云计算预测和市场预测综述，福布斯，2018 年 9 月 23 日

3 Andy Patrizio，云计算公司，Datamation，2019 年 1 月 9 日

4 Asher Benbenisty，解决策略配置错误，离漏洞远一点，Infosecurity，2018 年 10 月 30 日

5 Phil Muncaster，随着云错误配置的激增，泄露事件记录下降了 25%，Infosecurity，2018 年 4 月 6 日

6 2019 年网络未来调查，德勤，2019 年 3 月

7 2018 年第四季度威胁态势报告，Fortinet，2019 年 3 月 12 日

8 网络犯罪成本：第九次年度网络犯罪成本研究，埃森哲和波耐蒙研究所，2019 年 3 月 12 日

9 Rich Campagna，恶意软件的云之旅，Infosecurity，2017 年 9 月 28 日

10 Chris Purcell，多云蔓延是否正在吞噬您的资金？ CIO，2018 年 9 月 17 日

11 安全架构师与网络安全状况，Fortinet，即将出版。

12 Dave DeWalt 和 David Petraeus，网络安全大周期余波，Optiv，2017 年 9 月 7 日

13 Kassidy Kelley，CCPA 遵从从数据清单评估开始，TechTarget，2018 年 12 月

14 2019 安全研究：加拿大组织的网络弹性，Scalar，2019 年 2 月

15 Benson Chan，数字化转型重塑一切，Strategy of Things，2017 年 9 月 7 日

FORTINET

www.fortinet.com

377156-A-0-EN

2019 年 9 月 21 日上午 10:54

eb-fortiCWP 云安全用例