SOPHOS

保障公共云安全：七个最佳做法

Sophos 白皮书 2019 年 6 月

目录

保障公共云安全:七个最佳做法 2

保障公共云安全的七个步骤 4

步骤 1:了解您的责任 4

步骤 2:为多重云制定计划 5

步骤 3:让一切可见 5

步骤 4:将合规性融入到日常流程中 5

步骤 5:自动化安全控制 6

步骤 6:保障所有环境的安全(包括开发和 QA) 6

步骤 7:应用您的本地预置安全知识 6

介绍 Sophos Cloud Optix 7

结束语 9

保障公共云安全:七个最佳做法

在确保公共云应用程序安全方面,您认为怎样才算成功?

也许是一年内不因数据泄露而上头条新闻。或者是了解企业的云基础设施足迹,从而准确确保其安全?也许您希望确保合规性审核一帆风顺?或者改善安全团队和合规团队之间的协作,并加强合规团队及开发团队之间的协作?

无论您想要怎样,本指南都可以帮助您。本文介绍保障公共云安全的七个最重要步骤,提供每个企业都可以遵循的实用指导,文中包含 SophosLabs 对于网络罪犯针对云实例的频率的威胁研究结果。本指南还介绍了 Sophos Cloud Optix 如何帮助企业解决安全和可见性挑战。

在 Amazon Web服务 (AWS)、Microsoft Azure 或 Google云平台(GCP) 加速新实例很简单。运营、安全、开发和合规性团队面临的难处在于跟踪此类环境中的数据、工作负荷和架构变化,保持所有内容的安全。

公共云提供商负责云安全(物理数据中心,隔离客户环境与数据),而确保您的云端工作负荷及数据安全的责任则完全在于您。就像您需要保障本地预置网络存储数据的安全一样,您也需要保障云环境的安全。对于这种所有权的分配存在一种广泛误解,造成的安全漏洞导致云工作负荷成为现在黑客们新的热门目标。

云安全中最严峻的挑战

考虑到公共云的简单性和经济成本，越来越多的企业转向 Amazon Web服务、Microsoft Azure 和 Google云平台并不令人意外。您可以在数分钟内启动新实例，在任何时候缩放资源，同时只需为您使用的内容付费，避免提前支付高昂的硬件成本。

虽然公共云解决了许多传统 IT 资源挑战，但也带来了新的麻烦。有效云网络安全的秘诀在于改善整体安全状态：确保架构安全，配置正确，具备对架构以及（最重要的）访问者的必要可见性。

听起来很简单，但实际并不如此。

云使用的快速发展导致数据碎片化分布，工作负荷分布在不同实例中，对于某些企业，甚至分布在不同平台中。平均来说，企业已经在两种公共云运行应用程序，同时正在实验另外 1.8 种公共云 [1]。这种多重云方法让 IT 团队面临的可见性挑战更加复杂，他们需要在不同平台之间跳跃才能完整了解云资产。

缺乏对云工作负荷的可见性带来了安全

和合规性风险：

暴露风险增加

更大的灵活性和加快产品与服务上市速度是促使企业转向公共云的主要因素。这样做通常需要 DevOps 方法的灵活性和响应速度。对于许多企业来说，这种新的开发和产品发布方法需要多个开发人员跨多个平台，甚至经常跨多个时区工作。

以往开发周期持续数月或者甚至数年，跟踪工作负荷并不是一个问题，但现在不是这样了。现在您需要跟踪多个版本发布 – 有时候甚至是在同一天。时刻跟踪快速架构变化、配置更新和安全组设置几乎是不可能的。所有这些最终导致暴露于网络威胁的风险增加，漏洞可能被快速利用。

对数据、知识产权和服务的威胁

就像企业享受公共云带来的自动化便利一样，网络罪犯同样乐享其成。现在的攻击者越来越仔细查探云环境，利用本机云提供商 API 自动部署新实例，攻破开放的数据库，更改安全设置，阻止合法用户存取。

为了量化问题，SophosLabs 最近在全球最流行的 10 个 AWS 数据中心建立了环境。研究发现：

- 2 小时内，全部 10 个数据中心都遇到登录尝试 [2]
- 每台设备平均每分钟遇到 13 次登录尝试，每小时约 757 次。

这些触目惊心的数字凸显出网络罪犯采用成熟自动技术，以云实例为目标的频率。安全团队的挑战在于在攻击者之前发现并修复潜在漏洞，实时发现异常（攻击者）行为以阻止攻击。

维持合规性标准

无论您的基础设施和数据在哪里，您都需要证明符合相关法规，包括 CIS、HIPPA、GDPR 和 PCI 或风险法规不合规性。

云端的挑战在于环境每天、每小时、甚至每分钟都在发生改变。每周或每月的合规性检查对于本地网络可能合适，但对于公共云来说完全不够。连续合规性分析需求对于手动或者用本机工具管理云环境的团队来说，会占用大量资源。此外，发现合规性问题后，大多数企业的安全、开发、运营和合规性团队并不在一起，这意味着要及时解决问题也存在困难。

保障公共云安全的七个步骤

步骤 1:了解您的责任

听起来很简单,但在云中处理安全的方式略有不同。Amazon Web服务、Microsoft Azure 和 Google云平台等公共云提供商采用共享责任模型 – 即,他们确保云安全,您负责云中的所有内容安全。

数据中心物理防护,虚拟分离客户数据与环境等方面 – 都由公共云提供商负责。

您可能得到一些基本防火墙类型规则,用于管理环境访问。但如果您不正确配置规则 – 例如,如果您保留端口对整个世界开放 – 那责任就是您的。所以您必须了解您的安全责任。

图 1 概要介绍这些共享职责 – 或者如果您愿意,此处观看视频。

共享责任安全模型	本地预置	公共云	为什么?
用户	■	■	执行身份验证,定义访问限制并跟踪凭证使用。
数据	■	■	阻止数据丢失,定义和实施哪些人可以访问哪些数据,确保满足合规性标准。
应用程序	■	■	通过政策、补丁和安全功能,阻止应用程序威胁。
网络控制	■	◪	跟踪和实施网络访问权限。
主机基础设施	■	◪	管理操作系统、存储解决方案和相关系统并确保其安全,阻止未打补丁的缺陷和权限提升。
物理安全	■	■	限制对系统和设计冗余的物理访问,防止单点失效。

■ 客户　　■ 平台提供商

图 1 Sophos 共享责任模型总结图。关于每个云提供商的具体版本,请访问 www.sophos.cn/public-cloud。

步骤 2:为多重云制定计划

多重云不再是一个可有可无的策略，而是成为必备策略。您可能因为许多原因希望使用多重云，如可用性、提高灵活性或功能。在制定安全策略计划时，首先假定您将运行多重云 – 即使现在不运行，未来也会运行。这样您可以保证您的方法不会过时。

思考您将如何在多个云提供商，不同系统和控制台之间管理安全、监测和合规性。管理体验越轻松，越容易缩短事件响应时间，提高威胁检测率，减少合规性审核麻烦，更不要说有助于挽留宝贵的团队成员了。

寻找支持在一个 SaaS 控制台内监测多个云提供商环境的无代理解决方案，减少管理多个云帐户和地区之间安全需要的工具、时间和人员。

步骤 3:让一切可见

如果不可见，就无法确保安全。所以，获得基础设施准确可见性是实现正确安全状态最大的障碍之一。

利用能够提供网络拓扑和通信流实时可视化视图，并且完全细分包括主机、网络、用户帐户、存储服务、容器和免服务器功能等信息在内的工具。

为了增强可见性，寻找能够发现架构内潜在弱点的工具，这样可以阻止潜在入侵点。潜在风险区域包括：

- 端口对公共 Internet 打开的数据库，可能允许攻击者访问
- 公共Amazon S3 Simple Storage Services
- 可疑用户登录行为和 API 调用 – 例如同时多次尝试登录同一帐户，或者用户同一天从世界不同地方登录。

步骤 4:将合规性融入到日常流程中

将工作负荷转移到云端，带来了在更加分布式网络中满足合规性法规的挑战，通常涉及定期开发版本发布。为了确保合规性，您需要创建云足迹的准确库存报告和网络图表，确保在动态环境中满足您的合规性清单。

在满足审核最后期限方面，通常企业从盈利的业务项目调动资源，追求短期修复。这不是更具有可持续性的长期做法，每日快照很快报废，并不能为 ISO 27001、HIPAA 和 GDPR 等标准提供必要的连续合规性监测。

寻找能够提供网络拓扑实时快照，自动实时检测云环境变化，支持您提高合规性标准而无需增加人手的解决方案。您还需要能够定制政策以满足您的部门或垂直行业的特定需求。

当然，报告只是合规性的一个方面。您还需要能够解决合规性违规的情况。问题在于，由于缺乏有效的协作渠道，通常难以让需要的运营、开发和合规性人员一起合作。

为了让解决合规性违规的过程顺利进行，找到能与现有票据解决方案整合的解决方案，包括可以用于创建、分配和跟踪问题到完成的提醒信息，确保重要任务从不丢失，即使是发布时。

步骤 5：自动化安全控制

自动化流程是 DevOps 的一大快乐。但就像您的团队享受自动部署基础设施模板和脚本，节约开发时间一样，您也应该考虑可以自动化哪些安全控制。

在 DevOps 协作框架中，安全是一个端到端集成的共享责任。这一思想造出了“DevSecOps”一词，强调在 DevOps 计划中奠定坚实安全基础的需要。

自动化安全的需求很明确，因为网络罪犯在攻击中越来越利用自动化技术 – 例如，利用盗窃的用户凭据自动配置操作实例，例如加密劫持、更改帐户设置或者撤销合法用户以避开检测。事实上，仔细研究云环境的密码、安全组设置和代码弱点已经是现在的常态。

对公共云环境的攻击取得成功有两个主要原因，一是架构配置不安全，二是威胁响应不能跟上攻击者的速度。安全控制自动化是解决这些问题的关键。

为了确保公共与环境的安全，寻找可以实现以下功能的解决方案：

- **自动修复用户访问弱点和资源**，以及从任何端口任何资源进入的问题
- **发现可疑控制台登录事件和 API 调用**，这些意味着攻击者正在使用共享或失窃的用户凭证
- **报告外发通信异常**，提醒企业加密劫持或数据泄露等活动
- 根据主机计算机示例行为**发现隐藏应用程序工作负荷**，凸显隐藏的暴露点（如数据库）

步骤 6：保障所有环境的安全（包括开发和 QA）

成为新闻头条的公共云数据泄露往往是攻击企业的生产云环境（您的客户使用的），但攻击者同样有可能是为了您的计算能力而来 – 您的环境和 QA 环境 – 用来执行加密劫持等操作。

您需要能够快速反应和主动保障所有环境（生产、开发和 QA）的解决方案。解决方案应该能够分析您的活动日志（例如 VPC 流量日志和云审核日志），找出已经发生的问题，例如防火墙打开了不必要的端口。同时，解决方案还应能够主动扫描存储库（如 GitHub）中的基础设施即代码 (IaC) 模板，与 Jenkins 等 CI/CD 管线工具集成。这样可以确保在部署到服务器前测线引入代码的漏洞，防止出现丑闻而跃上头条。

步骤 7：应用您的本地预置安全知识

在公共云指南中看到这句话可能很奇怪，但本地预置安全是数十年经验和研究的结果。在保护云服务器不受感染和数据丢失时，首先考虑您为传统基础设施怎么做的，然后对云进行调整：

- 下一代防火墙：在云网关设置 Web 应用程序防火墙 (WAF)，阻止威胁从最初入口进入云服务器。加入 IPS（有助于合规性）和外发内容控制以保护您的服务器/VDI。
- 服务器保护：在云服务器运行有效的网络安全防护，就像物理服务器一样。
- 端点保护：虽然网络可能在云中，您的笔记本电脑和其他设备却在本地，而这些都是网络钓鱼电子邮件或间谍软件盗窃云帐户用户凭证的对象。确保保持设备上的端点和电子邮件安全最新，阻止未经授权访问云帐户。

介绍 Sophos Cloud Optix：

让一切可见，保障一切安全

可见性是所有公共云安全证策和活动的基础。Sophos Cloud Optix 能够简化监测多个云提供商环境，包括 Amazon Web服务 (AWS) 帐户、Microsoft Azure 订阅、Google 云平台(GCP) 项目、Kubernetes 群集，以及开发代码存储库。这种卓越的可见性，加上合规性和 DevSecOps 证策控制与提醒，支持团队控制并放心建立云安全策略。

作为与本地公共云提供商 API 集成的无代理 SaaS 服务，Cloud Optix 能够自动生产架构的完整信息，包括完整库存和实时网络拓扑可视化（包括主机、网络、用户帐户、存储服务、容器和免服务器功能）。

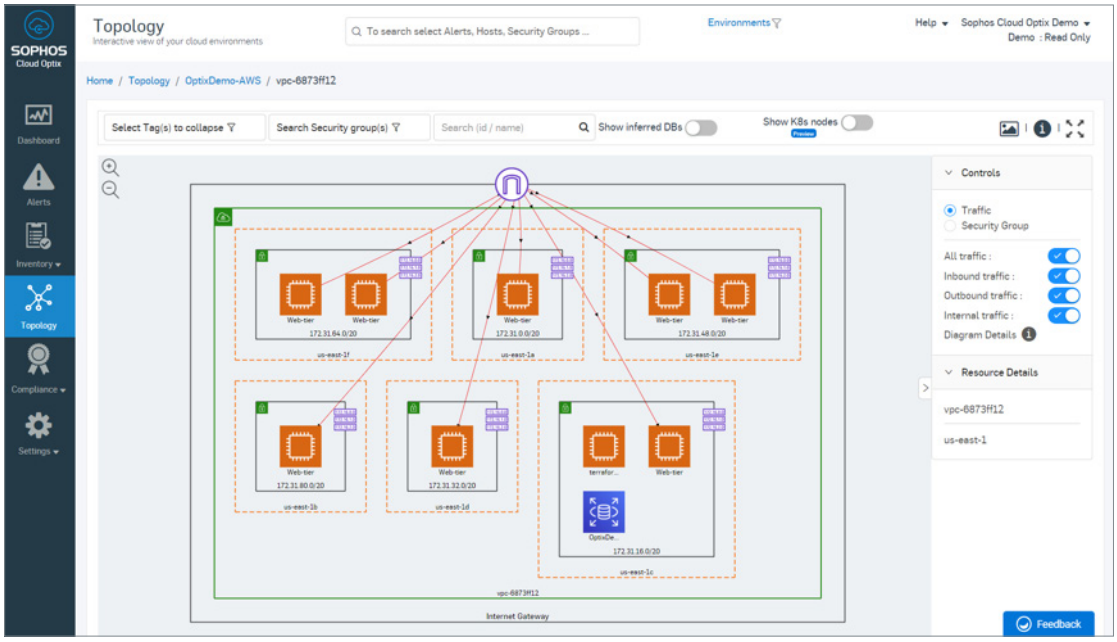

图 2显示 AWS 环境内的进入、离开和内部通信的 Sophos Cloud Optix 网络拓扑可视化。

不仅仅是简单配置检查

Cloud Optix 采用机器学习人工智能检查平台中的异常和安全弱点 – 监测网络流量、资源配置、用户登录事件和 API 调用、合规性状态、基础设施即代码 (IaaC) 存储库等，自动修复网络配置的意外或恶意变化的护栏。

环境相关提醒指示安全和合规性问题的根本原因，让您可以集中于需要安全更新的最关键方面，并且提供问题、修复步骤和受影响资源的说明。

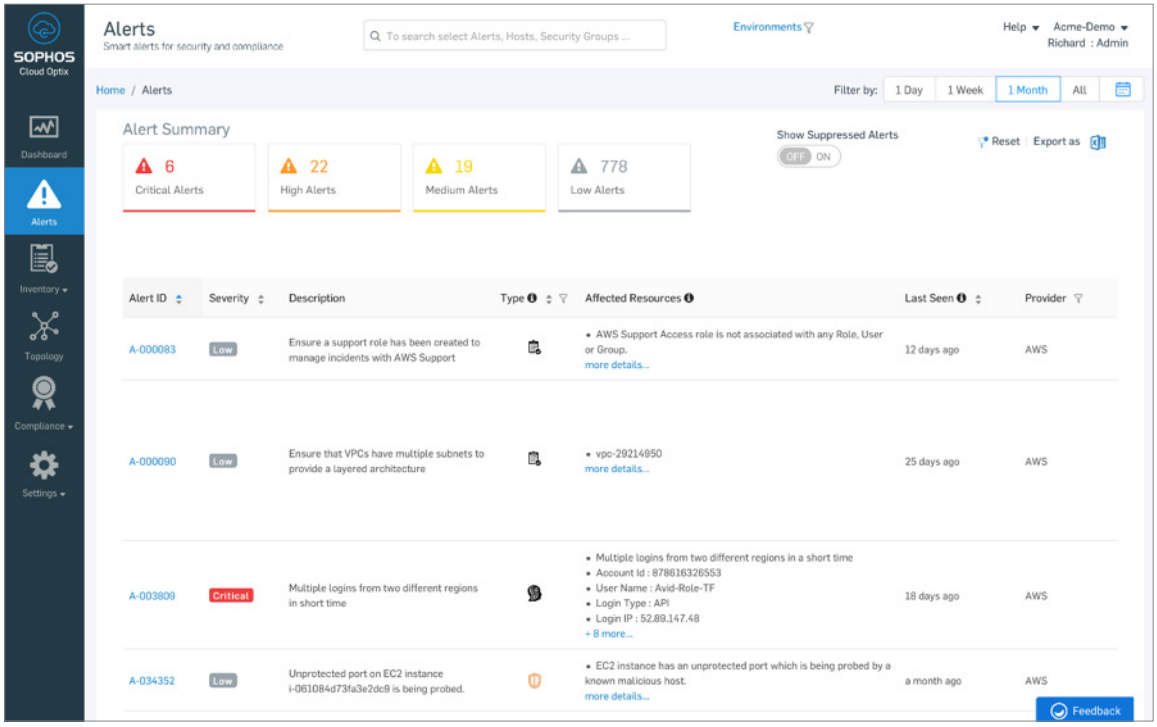

图 3Sophos Cloud Optix 提醒汇总，显示同一时间不同地区多个帐户登录的关键提醒。

依您的方式监测和响应

Cloud Optix 提供 Rest API，并与 Splunk、PagerDuty 和 Amazon GuardDuty 集成，可以在任何需要的地方提供实时提醒信息。通过与 Jira 和 ServiceNow 的内置集成，提醒信息甚至可以用于创建票据，然后跟踪直到完成，确保重要任务从不丢失，即使在发布期间也是如此。

全部内容通过一览无余的仪表板整合在按需报告中，您可以节约数小时或者甚至数天用来管理云安全状态的时间 – 帮助您实现保障公共云安全的七个最重要步骤。

了解更多

Sophos Cloud Optix 是适合正在使用或转向公共云的企业的理想解决方案。通过结合 AI 和自动化功能，让您的企业获得持续可见性，检测、响应和阻止可能导致暴露的安全和合规性弱点。

要更多了解 Sophos Cloud Optix，并在您自己的云环境开始免费无义务 30 天试验，或者观看在线演示，请访问 www.sophos.cn/cloud-optix。

结束语

从传统转向云工作负荷为所有规模的企业提供了海量机会。但是,如果您要保护基础设施和企业不受网络攻击,必须保障公共云安全。按照本指南中的七个步骤,您可以最大程度提高公共云安全,同时简化管理和合规性报告工作。

共享责任模型Sophos 如何帮助

	本地	公共云	为什么?	Sophos 协助
用户	■	■	执行身份验证,定义访问限制并跟踪凭据使用。	XG Firewall 和 Sophos UTM 通过 SSO 和 2FA 实施进入/发出身份验证,提供详细的访问报告。Sophos Cloud Optix 跟踪帐户凭证的共享或未经授权使用。
数据	■	■	阻止数据丢失;定义和实施哪些人可以访问哪些数据,确保满足合规性标准。	Sophos Cloud Optix 实现云中的合规性自动化、管理和安全监测,而 Sophos Safeguard、DLP 和 Sophos Mobile 帮助保护数据和确定访问权限。
应用程序	■	■	通过证策、补丁和安全功能,阻止应用程序威胁。	XG Firewall 和 Sophos UTM 的 IPS 以及 Sophos Server Protection 的 HIPS 和 Lockdown 防范应用程序攻击和意外应用程序暴露。
网络控制	■	◪	跟踪和实施网络访问权限。	XG Firewall 和 Sophos UTM 易于使用的界面、强大的数据包检查以及 Synchronized Security(同步安全)(仅 XG)帮助确保安全和管理网络访问,并实施网络权限。
主机基础设施	■	◪	管理操作系统、存储解决方案和相关系统并确保其安全,阻止未打补丁的缺陷和权限提升。	Sophos Intercept X 寻找漏洞攻击技术,防范零日威胁。Sophos Server Protection Lockdown 实施运行时限制,Sophos XG Sandstorm 阻止未知代码传播。
物理安全	■	■	限制对系统和设计冗余的物理访问,防止单点失效。	XG Firewall 和 Sophos UTM 都具有高可用性(High Availability)部署选项,用于物理设备和云平台。

■ 客户 ■ 平台提供商

图 4Sophos 如何帮助公共云共享责任模型

‘Sophos Cloud Optix 给我们团队带来了需要的 AWS 环境的实时智能和配置合规性状态的可见性，而且随手可得，在一个视图中实现了以前无法实现的监测和提醒。Sophos Cloud Optix 带给我们基础设施活动的全盘数据，让我们专注于综合防护。’

Ryan Stinson
安全工程经理
HubSpot Inc.

1 RightScale 2019 State of the Cloud Report from Flexera

2 自动攻击数据来源：暴露：云网络攻击热电，Matt Boddy，Sophos，2019 年 4 月

试用 Sophos Cloud Optix

www.sophos.cn/cloud-optix

中国（大陆地区）销售咨询
电话：400 650 6598
电子邮件：salescn@sophos.com

19-06-19 WP-ZHCN (RP)

SOPHOS