CSA GCR cloud security alliance GREATER CHINA REGION ®

多云安全风险图谱

Multi-Cloud Security Risk Map

2021.06

（试读本）

致谢

云安全联盟大中华区（简称：CSA GCR）多云安全工作组在 2021 年 3 月 31 日成立。我们主要针对多云环境下的安全问题，凝聚产、学、研、用等领域的专家或单位进行研究、分析、制定和输出云安全领域最先进的方法或工具，并持续迭代优化。我们的工作目标是致力于提供产业合作平台，凝聚行业共识，解决企业上云所面临的安全问题，促进云安全生态的健康发展，助力中国企业成功实现数字化转型。多云安全工作组的原则：布道、合作、共赢、引领。目前多云安全工作组的 50 多位安全专家们，分别来自华为、腾讯、中国工商银行、360、深信服、启明星辰、顺丰科技、海尔、天融信、山石网科、塞宝认证中心、神舟数码、H3C、光通天下、三未信安、蔷薇灵动、易安联、东软、申石软件、联软科技等数十家单位。这一数字正在不断增加。

多云安全工作组的主要研究方向包括：SASE、云原生安全、多云安全风险、多云安全治理、多云安全与边缘计算、多云安全与自动化响应、多云安全与零信任等方向。

本白皮书主要由多云安全风险图谱小组专家撰写，并邀请联盟安全专家共同审核，感谢以下专家的贡献：

多云安全工作组组长：魏小强

白皮书作者名单：于继万、李程、彭汝张、杨天识、朱青、谢江、赵晨曦（以上排名不分先后）

贡献单位：360、深信服、e 签宝、启明星辰、华为、新华三、上海观安（以上排名不分先后）

审核专家：

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c-csa.cn/research/）上查看。

如本白皮书有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号

序言

企业云转型正在迈向多云时代，据研究估计，93%的企业正在采用多云战略。随着数字化转型的不断深入和应对全球卫生危机带来的新挑战及其对业务流程的影响，企业比以往任何时候都更多地开启或扩大多云战略，来应对诸多的数字化挑战，如地区合规、成本优化、灾难恢复、数据备份、应用弹性、客户体验和全球覆盖等。多云系统可以比内部单一 IT 架构更好地满足这些要求，因为公司可以挑选最好的服务并将其与已有的 IT 基础设施进行融合，减少重复造轮子的成本，更加敏捷的推动业务的发展。

但是，在多云环境下，数据、应用和平台可能分布在任何地方，包括分布在不同区域的公司内数据中心和多个云区间，以及同一区域的不同服务提供商的多云区间，安全挑战会成倍增加，如安全可见性、配置和集成风险、安全人才问题、多云迁移，以及还可能涉及的合规和数据安全隐私等问题。传统安全已经难以应对这些风险。多云的复杂环境的技术架构意味着企业的 CISO 们必须重新思考 ICT 安全的理念。如果不进行有效的安全管理和规划，多云环境可能是一个昂贵的努力，会导致事倍功半。想要在多云世界中取得成功，IT 和商业领袖需要解决这些挑战。

在本报告中，CSA 大中华区多云安全工作组分析了典型的多云应用场景和所面临的安全风险，同时提出思考：如何适应多云的未来？如何解决多云安全所面临的安全风险？这将是工作组下一个要研究的课题。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目　录

1. 摘要

多云战略已经成为企业实现数字化转型、增强自身竞争力和提升用户体验的优先选择。尤其是发生 COVID-19 公共卫生危机之后，这一趋势正在加速。本报告深入分析多云环境的典型应用场景，以及企业在实施多云战略时所面临的主要安全风险。本报告可作为企业实现多云安全战略的参考和指导。

2. 术语定义

多云：本报告中指企业在一个单一的网络架构中采用数据中心、私有云、专属云、公有云或者他们的任意组合所形成的复杂的 IT 环境。

影子 IT：未经公司 IT 部门许可和管理但是被企业各个部门或个人大量使用的 IT 服务或系统。如文件共享应用程序、社交媒体和协作工具等。

3. 多云环境典型场景

多云战略是企业实现数字化转型的必选项。企业采用多云环境的典型场景如下：

3.1. 本地负载的弹性扩展

本地弹性扩展是多云负载分担的特殊场景，用户将业务部署在本地私有云上，当访问流量激增，超过私有云的处理能力，会动态的将流量分流到公有云上，利用公有云资源丰富、易扩展等特性，满足业务的突发需求，当波峰过去之后，释放公有云的资源，满足业务需求同时节省成本。

3.2. 多云数据备份

数据备份是等保合规的明确要求，也是业务连续性和数据安全防护的最后手段，必须考虑多重防护。云灾备是数据备份的最佳选择，一方面云提供商有强大的运维能力，可以保障数据的安全性，另外一方面由于云上资源丰富，可以非常容易扩展，并且云上资源价格也更加低廉。

企业在上云的时候，可以将数据备份到不同的云上，从而避免将鸡蛋放在同一个篮子里面。对于使用私有云加公有云模式的用户，私有云部署业务系统

的热数据，利用公有云更加优惠的存储空间对温数据和冷数据进行备份不失为一种最佳的数据保护实践。

3.3. 多云主备容灾

企业业务系统灾难恢复一般采用主备架构。特别对于金融、银行、政府等越来越多的企业要求核心业务 7*24 不断网，不断电持续运行，甚至采用两地三中心的方案。在这种架构下，用户可以把备用的业务数据放在公有云上，借助公有云提供商的技术优势、灾备经验、运维管理等资源，快速实现数据灾难恢复，保障服务的连续性。同时，与全部使用私有云相比，多云的灾难恢复还可以降低运维工作量，节省灾备系统成本。在私有云数据中心发生重大灾难时，用户可以在公有云端利用云主机快速切换，将备份数据拉起，大幅降低 RTO，实现业务高可用。

3.4. 构建跨国跨区域系统

对于大型跨国企业和大型多分支企业，由于业务的地域范围广，需要构建跨国家、跨地域的业务系统，自有的私有云或单个公有云在部署的时效性和合规性不能满足业务的需求，多云可以解决之。

3.5. 多云数据分类存储

公有云由于 IT 基础设施由公有云厂商管理，用户无法管理，对存放在其上的数据安全有一定的顾虑；私有云是为一个客户单独使用而构建的，因而提供对数据、安全性和服务质量的最有效控制。

随着数据安全法律法规的推出，对数据的分类分级存储和保护也越来越重要，对于企业高密级、高敏感类的数据或国家行业组织认定的重要数据、核心数据，需要存放在本地私有云或数据中心，从而保证数据的安全性，对于非敏感和公开数据，可以存放在公有云上，方便用户更易访问和获取。

3.6. 多云开发测试生产分离

根据软件的生命流程，从开发、测试到生产是一个完整的流程，考虑到不同阶段对环境的要求不同，很多企业按阶段划分为开发测试云、生产云。开发测试过程一般需要灵活快捷的环境搭建，而且期间经常重构，这时公有云是个

不错选择；而一旦正式上线，则希望运行在安全稳定的环境中，就会考虑私有云。利用 DevOps 流程与工具，可以同时获得公有云灵活快捷和私有云安全稳定的好处。

3.7. 多云异构融合

在企业 IT 建设的过程中，会采用不同于公有云的云技术架构来建设私有云，企业在向公有云迁移时，需要考虑此类异构场景下多云的融合问题。

异构混合云在构建、管理和使用上都存在相当的复杂性，但是随着容器技术和微服务架构的发展，基于 PaaS 平台的应用混合正在成为主流的混合云形式，应用在异构云间的迁移会变得越来越容易。容器技术使得应用的可移植性不再是问题，微服务架构使得各个应用组件可以独立、分布式运行，轻量化的组件迁移会比单体架构的巨型应用的迁移更平滑。

3.8. 多云增强企业竞争力改善用户体验

多云模式可以帮助组织增强在数字化时代的竞争优势，提升用户的体验。随着组织逐渐把业务迁移到云端，数字时代的用户越来越适应随时随地访问任何应用和服务。移动办公，远程访问等已经成为客户的常规需求。利用多云的便捷性使产品更快地进入市场，使企业在快速开发新产品和服务的同时，能更快地响应客户的需求。

4. 多云安全风险

4.1. 多云安全人才不足

云安全人才本身就缺乏，多云安全的人才更加稀缺，多云本身也带来了新技术的要求，需要一定的学习周期以掌握不同云厂商的安全差异性。另外，当前云计算技术栈还远未达到标准化的阶段，不同层次的资源模型以及对应的 API 还缺乏统一的标准，这间接让多云学习成本加倍，需要相关组织推动该标准工作，降低多云的学习成本。

解决办法除了上面提到的大力推动标准化外，一方面对于传统网络安全专家主动参加相关培训和多实践是快速提高多云安全经验的最佳路径，目前主流云服务提供商都在官网上提供了大量的安全学习材料，安全白皮书、配置及最

佳使用实践等，另一方面面对云计算未来的原生化趋势，云计算技术栈自身也在快速演进，云已经成为数字社会的公共技术平台，企业需要在业务发展初期就应该规划好怎么让业务在多云生态环境下生长好。

4.2. 多云安全集成风险

多云对统一的账号管理和集中的安全运维带来挑战。多云账号相比单一云环境更加分散，分散的账号阻碍了用户对多云资产的统一管理，难以及时跟踪资产变化，加上各类 API 接口的不统一，这对 DevSecOps 交付模式是一大挑战。由此引发弱口令、Access Key 暴露、API 权限控制不当、服务不安全配置或误配置等安全问题

多云中间件的集成风险：大多数中间件自身具有自成体系的管理系统，比如数据库、不同语言的微服务框架、K8S 等，其自身内部的资源和对象缺乏和外部账号在控制策略上的统一，在多云架构下加大了集成的难度，，难以依赖统一的 IAM 账号权限体系来管理其资源。

多云安全集成的根本问题是不同云平台服务标准的不一致，通过第三方安全管理平台，统一服务标准，消除差异，为用户提供一致的接口，是解决多云集成风险的可行途径之一。

4.3. 多云安全缺乏可见性

当前安全架构人员缺乏足够的支撑来整体评估上云后业务的风险，即使在相同类别的云服务上，对一个厂商服务的风险分析也很难直接拷贝到另外一个厂商的同类云服务上。尤其是当前厂商为了完善生态提供的服务颗粒度越来越细，不针对每个云厂商提供的服务分析其技术实现，熟悉其整体的安全防护能力，想单独通过责任边界来解决客户的疑虑目前还存在落地实践问题，毕竟能力可以外包但责任无法转移。大量同质化第三方认证也不足以消除该问题，用户评判服务不透明部分的安全存在要么信任要么不信任的两难境地。

多云透明性的另外一个风险就是账号使用管理不到位而产生的，多云架构跨越多个云提供商，企业在云提供商中使用多个帐户，很难监视和管理这些帐户使用的大量服务（也称为影子 IT），企业需要应对这些服务传输到企业网络

外部和公共云的信息。如果这些信息离开企业不受控制，将会对企业带来巨大风险，特别是在那些高度监管的行业的企业。

解决多云透明性的核心在于有一套统一的标准，每一类服务的透明性需要技术上准确界定，在这个基础上明确责任边界。当前业界每层的责任共享模型里是有了一个初步的分界线，但未来需要进一步从审计角度细化不同层次不同类别不同颗粒度的透明性标准，并且通过商务来兜底，缓解用户的选择困境。

4.4. 多云安全治理风险

当前企业数字化和云计算技术发展都在加速，企业面临混合云、多云管理等复杂场景时，缺乏整体统一的多云安全架构，容易导致云上应用缺乏整体的安全规划、缺乏一致的安全策略编排、难以快速对齐云计算新技术演进带来的机会和风险，尤其当面临多种法律法规政策标准等合规监管条件下，如何能够做到兼顾合规与风险管控是极具挑战的事情。

公有云风险共担模型不统一也加重了该问题的风险，：虽然业界各家公有云厂商都有自己的公有云-租户风险共担模型，但模型并不统一，目前主要有两种云安全责任共担模型：一种是云服务商和云租户责任完全划清，分为云服务商安全责任+云租户安全责任两部分。另一种是云服务商和云租户之间存在责任共担部分，分为云服务商安全责任+共担责任+云租户安全责任三部分，国内的公有云厂商更倾向后一种方式，目前业界也缺乏统一的标准，这容易导致云租户在不同公有云之间进行应用系统部署、数据存储、安全资源共享时由于责任划分的不同导致产生风险黑洞。

安全策略统一规划在多云背景下除了继续提升安全治理部门在组织内的战略位置外，技术上依赖 4.3 节中的透明性解决，另外支撑租户安全策略规划落地需要不同云厂商安全架构模型的统一，零信任是一个方向。

4.5. 多云环境导致攻击面扩大

随着越来越多的组织采用云计算，企业越来越依赖应用程序编程接口(API)来弹性扩展当前服务。但多云下 API 的使用带来额外的风险，一方面暴露的 API 会让企业容易受到攻击，尤其是一些传统中间件服务，在 API 设计上还没

有原生化，直接对外开放接口会导致非常多的安全风险，另一方面跨服务 API 调用是云技术栈多的典型特点，服务与服务之间的调用如果在 API 细粒度权限策略上设置上（一般通过委托）没有遵循最小化原则，非常容易产生中间服务的越权访问。

多云互联会增加的另外一类攻击面是多个云互联自身引入的，这其中又分从公有云租户资源触发对本地私有云的攻击和从本地私有云触发对公有云租户资源的攻击。具体攻击形式取决于多云服务之间的防护短板。这类攻击目前集中在 DDOS 僵尸攻击、挖矿、勒索等，我们拿勒索病毒作一分析，存在以下三种攻击：

勒索病毒同步至云文件共享服务；

RansomCloud 攻击(针对云数据的勒索病毒攻击)；

租户公有云资源（比如 ECS）发起对本地数据的勒索病毒攻击。

解决或缓解此类攻击没有捷径，针对整个业务架构、流程做威胁建模，识别高风险攻击面并加以处理是必经之路，尤其是针对不同云服务边界。

4.6. 多云迁移安全风险

当前企业体系结构的复杂性构成了迁移到云的主要风险之一，如果要将公共云和私有云与本地资产混合在一起以创建混合云环境，需要重新设计内部体系基础架构，适应多云架构以解耦服务之间复杂的调用关系，最大程度地减少不同系统之间的不一致和互操作性问题，对于已经拥有微服务架构并使用 Kubernetes 或 Docker 引擎之类的工具来编排其容器的企业来说，迁移到云变得更容易，如果完全变动，可能会引入潜在的安全风险。

迁移到在不同云平台上，云服务相关配套的安全服务都需要重新设置，您需要有经验丰富的 DevOps 工程师和安全团队，他们可以进行必要的配置并确保云中数据的长期安全性，云服务提供商自身都提供了完整的安全能力，这些能力要发挥效果需要对该能力和您自身业务风险需要有正确理解，需要专业多云安全专家指导。

另外，迁移提供商客户退出后的数据残留处理边界模糊，如果迁移过程发生数据泄露，客户与云服务商之间的责任难以界定，迁移到新的提供商还会面临同样的问题，客户对数据和业务系统的控制能力减弱，数据所有权保障面临风险，目前缺乏比较标准的迁移后数据的删除标准，云服务的底层数据往往是共享存储，怎么删除不能恢复是一个大问题。不同云厂商满足的合规标准和策略也有区别，在选择不同国家云厂商时要仔细，必要时和厂家做详细的技术交流。数据跨境需要慎重考虑，必须有严格的计划和明确的迁移策略。

4.7. 多云安全配置风险

云错误配置是云安全的重要风险之一，由于云计算环境配置复杂，客户对云安全意识不强，疏于管理或配置不当等错误给攻击者创造了机会。在云环境下，尤其是多云环境，IaaS 和 PaaS 云安全配置的正确性和合规性极其重要。在多云架构下，由于云厂商为了提供更好的服务和体验，会在云服务上做很多优化和创新，提供的服务粒度也越来越细，如云防火墙服务不同云厂商的配置上就有很大差异，有基于五元组配置的，也有基于对象策略配置的，并且提供的安全能力也不尽相同，这些差异增加了配置正确性的难度。

另外，由于云是开放的技术平台，除了提供人机配置界面外，也提供配套的 API 接口，如果没有深入理解服务内部实现原理及其缺省实现，常常会有误配风险。

面对多云配置的复杂性、多样性、繁琐性，我们如何来保证配置的正确来满足合规与风险的要求是我们需要继续深入分析的问题。

4.8. 多云安全合规

合规意味着企业遵守了适用的法律法规及监管规定，例如国内的等保、数据安全法，美国《健康保险可移植性和责任制法案》（HIPAA）以保护个人与健康相关的信息，新加坡 MAS-TRM（技术风险管理）指南，以规范新加坡金融机构（FI）内的 IT 系统，以及作为全球最严格的数据隐私法之一的通用数据保护条例（GDPR），其主要目标是保护欧盟（EU）下所有个人和实体的个人数据。这些仍是传统的合规要求，并没有明确的针对云的合规要求，合规性在云服务

中是一个共享责任模式，云用户应始终对自己的合规性负责，其中的责任是通过合同，审核/评估，和具体的合规性要求的细节来确定的。

因此应该在选择云厂商之前，明确全部合规义务。了解评估和认证的范围，包括控制和系统特性/服务。云用户应评估云服务提供商的第三方认证，并将其与合规性要求保持一致。云用户应定义审计管理的范围，选择具有云计算经验的审核人员，确保他们了解云服务提供商提供的合规性证据，并有效地收集和管理这些证据。

5. 结语

本报告通过对多云的应用场景和多云安全风险的研究仅仅是开始。如何解决这些多云安全风险？企业应该采用什么样的多云安全架构来应对这些风险？以及企业如何构建自己的安全团队管理多云安全环境，将是我们下一个研究课题。

CSA GCR cloud security alliance GREATER CHINA REGION ®

多云安全风险图谱

Multi-Cloud Security Risk Map

官网: http: //c-csa.cn
邮箱: info@c-csa.cn