HUAWEI | CAICT 中国信通院

云安全责任共担模型

2024年7月

华为云计算技术有限公司

中国信息通信研究院云计算与大数据研究所

前 言

近年来，云计算成为千行百业数字化转型的重要支撑，承载海量业务和数据，其安全性影响着企业的生产经营及社会稳定。与传统数据中心相比，云服务商与云服务客户对云及云上资产的可见性不同，云安全工作无法仅由某一方承担完成，云安全责任共担模式成为行业共识。

随着政策标准不断完善，外部安全态势日益严峻，各行业云计算应用程度加深，云安全责任共担面临新的发展需求。本报告以应对新态势为关键，建立了云安全责任共担 2.0 体系，旨在提升云服务客户责任共担意识，促进云服务客户、云服务商、云安全厂商在责任共担中充分识别自身定位、发挥作用价值，协同推动云安全工作高质量开展。

首先，报告提出云安全责任共担四大基本原则，以责任划分合理条件下如何高质量开展云安全工作为根本目的，理清云安全责任共担关键环节；其次，报告给出云安全责任共担实施参考，探索云服务客户、云服务商、云安全厂商落实云安全责任共担机制的举措手段。最后，报告对云安全责任共担发展进行了展望，剖析标准规范、保险机制、生态建设等方面的意义价值与发展方向。

目 录

一、新态势：云安全责任共担模式面临新展需求

近年来，我国云计算产业持续高速增长。据统计[1]，2022 年，我国云计算市场规模达 4360 亿元，同比增长 35.0%，产业发展势头强劲。千行百业以云计算为技术底座开展数字化转型，云安全成为保障业务和数据的关键。

与传统数据中心相比，云计算存在运营方与使用方分离、数据保管权与所有权分离等情况，**云服务商与云服务客户对云及云上资产的可见性不同，云安全工作必然无法仅由某一方承担，云安全责任共担模式成为行业共识。**同时，随着政策标准不断完善，外部安全态势日益严峻，各行业云计算应用程度加深，云安全责任共担也呈现新的发展态势。

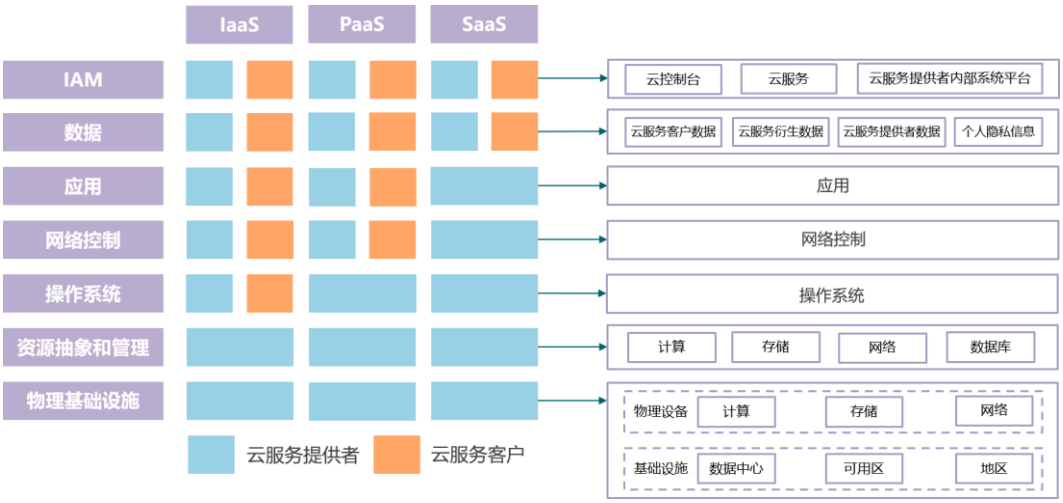
（一） 政策标准为云安全责任共担提供更坚实的发展基础

政策法规加强对多方主体安全建设的指引，云服务客户不可因上云而将责任全部转包。云服务客户上云后，部分 IT 资源的运营和管理模式与传统数据中心相比发生变化，一些安全责任转移至云服务商，但仍有一部分责任需由云服务客户承担。近几年，我国安全政策法规不断健全，对上述责任给出了更加明确的要求与指引。《网络安全法》对网络运营者等主体的法律义务和责任做了全面规定，是云服务商承担责任的最小集合；《数据安全法》对在我国境内开展数据处理活动的组织做出了数据安全权责规定，云服务客户上云后，虽然业务数据

[1]中国信息通信研究院《云计算白皮书（2023 年）》

在云平台中存储和传输，云平台由云服务商运维运营，但云服务客户仍应承担数安法规定的数据安全责任；2022 年 11 月，国务院新闻办公室发布《携手构建网络空间命运共同体》，白皮书强调“构建安全共同体和责任共同体”，“倡导开放合作的网络安全理念”，要求“发挥各主体作用，建立相互信任、协调有序的合作”。云安全领域涉及云服务客户、云服务商、云安全厂商等多个主体，坚持白皮书提及的共同体基本原则，是保障云上业务和数据安全的必然选择。

多项标准规范推动建立云安全责任共担共识。YD/T 4060-2022《云计算安全责任共担模型》行业标准建立了公有云的安全责任共担模型，在厘清云计算安全责任的基础上，充分识别云服务商和云服务客户两大主体间的责任分担方式；GB/T 31168-2023《信息安全技术 云计算服务安全能力要求》国家标准给出了不同云能力类型中云服务商和云服务客户安全责任的控制范围。上述标准的发布实施一定程度上提升了行业对云安全责任共担模式的认识与认可。



来源：YD/T 4060-2022《云计算安全责任共担模型》

图 1　云计算安全责任共担模型

（二） 安全风险加剧，对云安全责任共担提出更明确的发展要求

云安全配置风险凸出，“建好云”和“用好云”并重。云服务客户因不熟悉云环境进行错误配置，如开放过多访问端口、设置过低的权限控制，将导致数据泄漏等事件发生。调查显示[2]，不合理的安全配置是过去一年中导致公有云发生安全事件的最主要因素。规避云安全配置风险不能仅靠云服务客户或云服务商的单方努力，双方必须推动能力提升，承担各自的责任。**一方面，**云服务商应“建好云”，优化云服务安全功能的设计，为云服务客户提供完善的、易用的用户友好型安全功能；**另一方面，**云服务客户应“用好云”，基于云服务商提供的云服务安全功能，建立合理的配置规范并切实执行。

软件供应链风险频发，云计算上下游应急响应与协作需求迫切。近年来，软件供应链攻击规模持续增长，调查显示[3]，过去三年全球软件供应链攻击的平均年增长率高达 742%。云计算在企业数字化转型过程中扮演越来越重要的角色，提质降本增效的同时也带来了复杂的软件供应链风险。**一方面**企业上云方式多样，云服务商、云软件等成为攻击企业的跳板，2021 年 5 月云服务商 Everis 被入侵，导致北约云平台相关数据泄露。**另一方面**公有云等模式下，云平台的基本运维和运营由云服务商开展，企业不掌握源码，对云平台控制力低，当一些重大安全漏洞被披露时，企业可能无法确认漏洞是否波及自身使用的云服务及云上业务。为有效规避软件供应链安全事件，云服务商、

[2] Cybersecurity Insiders《2023 Cloud Security Report》
[3] Sonatype《8th State of the software supply chain》

云服务客户、云安全厂商等需形成上下游沟通渠道，在发生软件供应链安全事件时及时沟通、联动处置，控制事件危害的传播。

云上勒索软件攻击形势严峻，联防联控成为必然。当前，勒索软件攻击对信息基础设施等领域造成严重影响，据预测[4]，勒索软件损失到 2031 年将达到 2650 亿美元。云服务因分布式、弹性易扩展等特性，易受到勒索软件攻击，为云服务客户带来业务中断、经济损失等危害。防范勒索软件风险要求云服务客户建立覆盖人员、技术、制度等多个维度的完备安全体系，同时也离不开云服务商的有效支撑。**一方面**，数据备份等手段是抵御勒索的有效机制，而备份数据的可用性、完整性依赖于云平台的技术架构。**另一方面，**云平台承载海量租户，云服务商在云平台中能监测到更多全网安全信息，当发现潜在的勒索威胁时可及时与云服务客户预警沟通。

（三） 行业用户共担意识仍存提升空间，实际需求为云安全责任共担指明发展方向

随着云计算产业不断发展，在政策标准引导下，各行业上云用云程度不断加深，云服务客户对云计算的了解以及对云安全责任共担的认知有一定增强，《中国私有云发展调查报告（2023 年）》显示，42.3%的受访用户表示接受与云服务商共同承担责任，这一比例较 2021 年提升了 2.7%。但从调查数据可以看出，仍有一半以上用户对云安全责任共担的认知不够清晰，同时在责任共担模式应用过程中，云服务

[4] 世界经济论坛《2022 年全球网络安全展望报告》

客户也面临诸多实践痛点，对云安全责任共担模式提出了更切实的需求和期望。

不同行业上云形式复杂，多主体安全责任划分需求迫切。各行业在推进数字化转型的过程中，结合业务需求和安全要求，常选择多云/混合云的部署模式，需与多个云服务商建立安全责任划分机制。同时，云安全建设涉及网络安全防护、数据保护、安全审计等多个方面，云服务客户往往整合多家云安全厂商能力，也需进一步明确各厂商的责任范围。如何建立和实现与多个云服务商、云安全厂商的责任共担协作机制成为云服务客户的迫切需求。

企业内云安全涉及多个相关部门，需通过责任划分推动各方落实安全举措。随着各行业用云程度不断加深，企业不仅仅购买计算、存储、网络等云服务资源，更加侧重基于微服务、DevOps 等云计算技术重构软件架构，单体软件实现微服务分布式部署，传统线下业务也不断迁移至云上。仅依靠安全部门进行网络安全防护难以有效应对云带来的安全挑战，云服务客户的安全工作需融入软件开发、业务运营等各个环节，要求安全部门、开发部门、业务部门、运维部门等多个部门的参与，通过梳理各部门安全责任以推动相关人员提升安全意识、落实安全举措十分必要。

二、新态势：建立云安全责任共担 2.0 体系

过去几年，云安全责任共担相关的标准规范、模型实践侧重云服务商与云服务客户间的责任划分，范围聚焦在基础设施能力类云服务、平台能力类云服务、应用能力类云服务中，目的是理清双方责任边界。随着政策标准、外部安全态势、各行业上云情况的变化，云安全责任共担也面临新的发展需求，本报告以应对新态势为关键，建立了云安全责任共担 2.0 体系，与以往相比，**2.0 体系具备如下新特征：**

一是增加关注主体，考虑云安全厂商角色在责任共担中的定位作用，适应云服务客户安全建设发展的需求；**二是明确基本原则**，以责任划分合理条件下如何高质量开展云安全工作为根本目的，强调最大化发挥各主体优势、协作保障云上业务和数据安全，加强各主体对责任共担的理解；**三是剖析云安全服务和云运维运营服务对云安全责任共担的影响与作用**，在以往聚焦资源类云服务的责任共担实践基础上，进一步扩展保障类云服务。

（一） 明确云安全责任共担主体角色

在以往的云安全责任共担体系中，往往关注云服务客户和云服务商两类主体，随着安全需求和工作的复杂化发展，云服务客户使用的云安全服务增多，云安全厂商在责任共担中的作用凸显。本报告提出的 2.0 体系中增加云安全厂商这一主体角色，进一步贴合上云用云时的实际安全场景。

云服务客户：使用云服务的企事业客户和个人客户。云服务客户

可能购买和使用不同类型的云服务，如基于基础设施能力类云服务开发应用软件，或直接使用应用能力类云服务。

云服务商：提供云服务的组织机构。云服务商可以提供基础设施能力类云服务、平台能力类云服务、应用能力类云服务中的一种或多种云服务，或云运维运营服务。对于仅提供平台能力类云服务或应用能力类云服务的云服务商，其基础资源可以是基础设施能力类云服务/平台能力类云服务，也可以是物理机等非云服务资源。

云安全厂商：提供云安全服务的组织机构。云安全厂商可以提供云工作负载保护、云网络防护、数据安全、安全运营等一种或多种云安全服务，服务可以是技术工具，也可以是人员服务。云安全厂商主要包括两类，**一类是云服务商**，在为云服务客户提供云服务的同时提供原生化的云安全服务；**另一类是传统安全厂商**，将已有安全工具云化改造或面向云场景开发新的云安全服务。

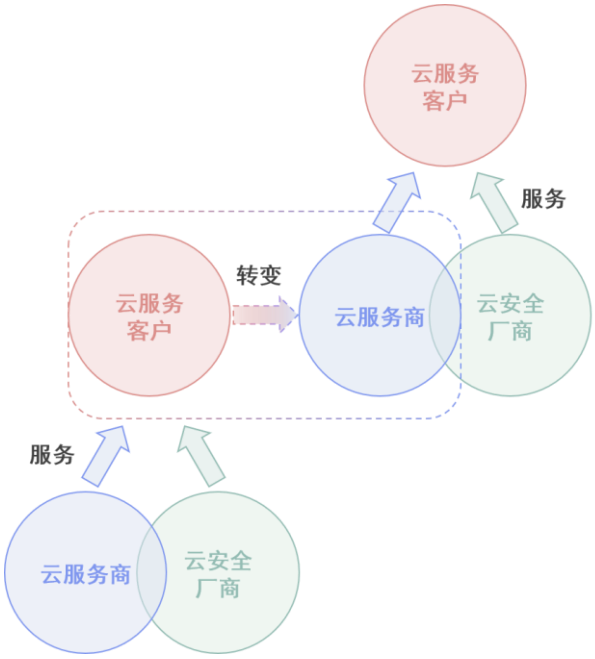


图 2　云安全责任共担主体

一个组织机构可能同时承担一种以上的主体角色，如云服务商为云服务客户提供云安全工具或人员服务，则云服务商同时承担云安全厂商的职责；云服务客户基于基础设施能力类云服务或平台能力类云服务开发应用软件后，对外提供应用能力类云服务服务，则云服务客户也作为应用能力类云服务的云服务商承担一定的职责。组织机构需充分识别自身所涉及的主体角色，了解各主体角色应承担的不同责任，在角色转换时做好充分准备。

（二） 遵循四大云安全责任共担基本原则

云安全责任共担涉及三类主体角色，各主体间的责任不能盲目、随意分配，应遵循一定的基本原则。在以往的发展中，部分主体对云安全责任共担机制存在认识不深、误解等情况，如认为责任共担是某些主体不想负责的说辞。为了进一步明晰云安全责任共担的必要性与价值，本报告围绕其内涵总结出四大原则，以强化各主体对责任共担的充分理解与践行。

目的一致性原则：云服务客户、云服务商、云安全厂商的共同目的是保证云服务客户云上业务的安全稳定运行。云安全责任共担模式的意义并不是强调某些主体可以不承担一些责任，而是希望在合理化、最大化各方优势力量的前提下，主体们各司其职，协同推动云安全工作的高质量开展。

责任合理性原则：云服务客户、云服务商、云安全厂商对云及云上资产的可见性不同，法律法规规定的责任义务也不同，云安全责任

必然无法完全由某一方负责，各主体应在满足法律法规要求、上云实际情况的前提下合理划分安全责任，承担一定的安全责任基线，如公有云的物理基础设施安全由云服务商负责，云上业务数据的安全管理由云服务客户负责。

优势最大化原则：云服务商、云安全厂商在云计算和云安全领域具备较强的技术优势，在责任合理性前提和云服务客户授权下，厂商应充分发挥社会责任感，最大化释放技术优势价值，为云服务客户提供更多的服务，如云运维运营服务、云安全服务等，助力云服务客户保障云上业务安全稳定，降低网络和数据安全风险，提升云安全工作效率。

协作透明性原则：云服务客户、云服务商、云安全厂商在协同开展云安全工作时，对云及云上资产的控制度不同，所掌握的安全信息也存在差异，为了有效规避复杂的安全风险事件，提升主体间的信任度，需建立透明、及时的信息传递和联动响应机制。

（三） 依据云计算的服务类型和服务模式开展云安全责任共担

1、云计算的服务类型影响云安全责任范围

云服务客户使用不同类型的云服务，云安全责任共担各主体的责任范围存在差异，各主体应根据云服务类型合理开展责任共担工作。在以往的云安全责任共担体系中，往往关注基础设施能力类云服务、平台能力类云服务和应用能力类云服务，随着上云进程的加深，云服务客户使用的云服务类型不断丰富，不再局限于资源类云服务。本报

告提出的 2.0 体系增加对云安全服务和云运维运营服务的考虑，以探索这两类云服务对责任共担的影响与作用。

基础设施能力类云服务：为云服务客户提供能配置和使用计算、存储或网络资源的云服务。

平台能力类云服务：为云服务客户提供编程语言和执行环境的云服务。

应用能力类云服务：为云服务客户提供应用的云服务，如协同办公服务、运营管理服务等。

云安全服务：为云服务客户提供保护云上负载、网络、数据以及应用等安全能力的服务，能够更有效的帮助云服务客户承担其安全责任。

云运维运营服务：为云服务客户提供云资源的监控与维护、计量与优化等管理能力的服务，能够更有效的帮助云服务客户提升用云过程的安全。

在上述所有的云服务类型中，基础设施能力类云服务、平台能力类云服务、应用能力类云服务是**资源类云服务**；云安全服务、云运维运营服务是**保障类云服务**，为资源类服务及其上业务的安全提供帮助支撑，辅助云服务客户履责。服务商提供云安全服务和云运维运营服务时，其责任范围与云服务客户购买服务的目的对象保持一致。同时，云服务从基础设施能力类到平台能力类，再到应用能力类，云服务商对云的控制范围逐渐扩大，所承担的责任增多，云服务客户承担的责

任则变少，保障类服务涉及支撑的责任范围也变小。

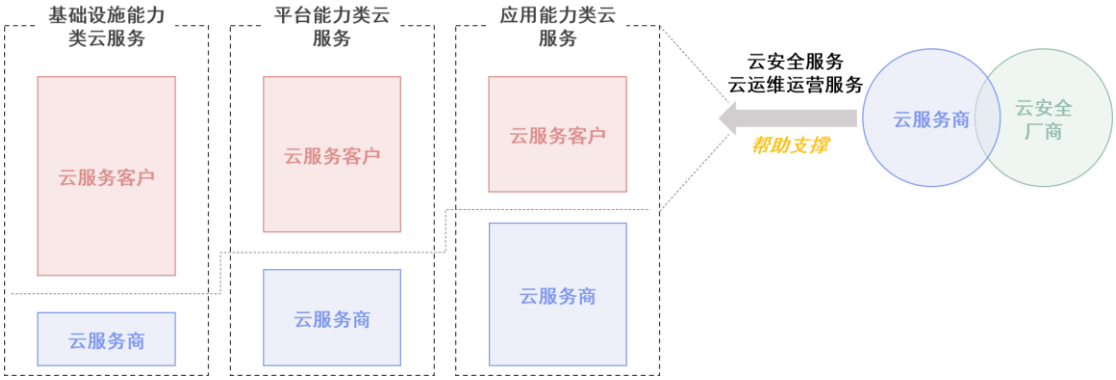


图 3　云计算的服务类型对主体安全责任范围的影响示意图

2、云计算的服务模式影响云安全责任范围

由上一节分析可以看出，资源类云服务影响着云服务商和云服务客户间的安全责任划分，进而影响云服务客户购买支撑类云服务的需求与目标。在此基础上，从云计算的服务模式视角看，云服务客户与云服务商间的不同合作模式，其对云的控制程度有差异，也将进一步影响安全责任范围，主要包括三类：

一是云服务模式：云服务客户采购和使用资源类云服务，资源被云服务商控制，如公有云和专有云，云服务商负责云平台所依赖的底层资产及云平台的日常运营。

二是云软件交付模式：云服务客户采购资源类云软件，资源由自身控制，如私有云，云服务客户自行负责云平台所依赖的底层资产及云平台的日常运营。

三是云软件交付+服务托管模式：云服务客户采购资源类云软件，资源由自身控制，但因自身能力有限等原因，云服务客户无法或不愿自行负责云平台所依赖的底层资产及云平台的日常运营，通过采购云

运维运营服务，引入云服务商协助其开展运维运营工作。典型的场景如政务云，云软件部署在客户的数据中心环境中，云服务商按服务协议规定的内容驻场或远程进行政务云的运维运营，政务云中业务和数据的最终安全责任主体仍为云服务客户。

云安全的最终目的是保障云服务客户云上资产的安全稳定。资产作为被保护对象，以其视角识别云安全责任共担的关键环节，能够更加完备的构建云安全责任共担体系。云环境下涉及的资产主要包括:

一是机房基础设施，包括数据中心基础设施，计算、存储、网络等物理设备和架构。**二是虚拟化基础设施资源**，包括虚拟资源管理平台、基础设施能力类云服务，如虚拟机、块存储等。**三是平台软件**，包括用于应用开发和部署的软件工具与组件，可以是平台能力类云服务，或云服务客户自行部署在基础设施能力类云服务之上的软件工具与组件，如容器、云数据库、中间件等。**四是应用软件**，包括云服务客户基于云计算开发或部署的应用软件、开放 API 和应用能力类云服务（SaaS）。**五是业务数据**，指云服务客户的业务数据。

针对上述资产，**对于云服务模式**，云服务商负责云服务及其所依赖的底层资产自身的安全，包括设计、开发、运营、下线各环节的安全；云服务客户负责安全的使用云服务，对部署在云服务之上的资产安全负责，往往通过采购云安全服务实现，责任范围如图 4 所示。

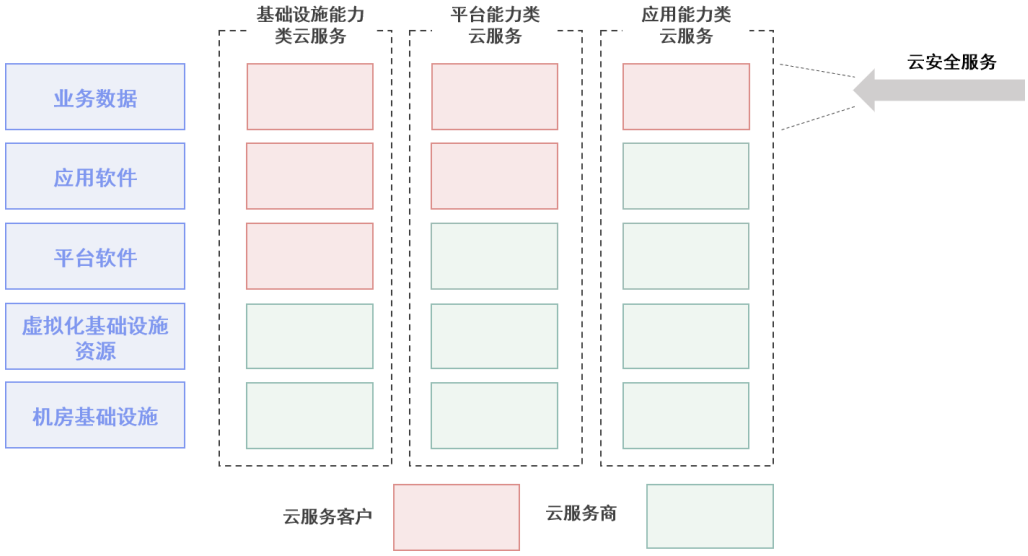


图 4　云服务模式对主体安全责任范围的影响示意图

对于云软件交付模式，云服务商负责云软件自身的安全，不承担云平台所依赖的底层资产及云平台日常运营的安全责任；云服务客户负责安全的使用云软件，对云软件部署的环境及其承载的资产安全负责，往往通过采购云安全服务实现，责任范围如图 5 所示。

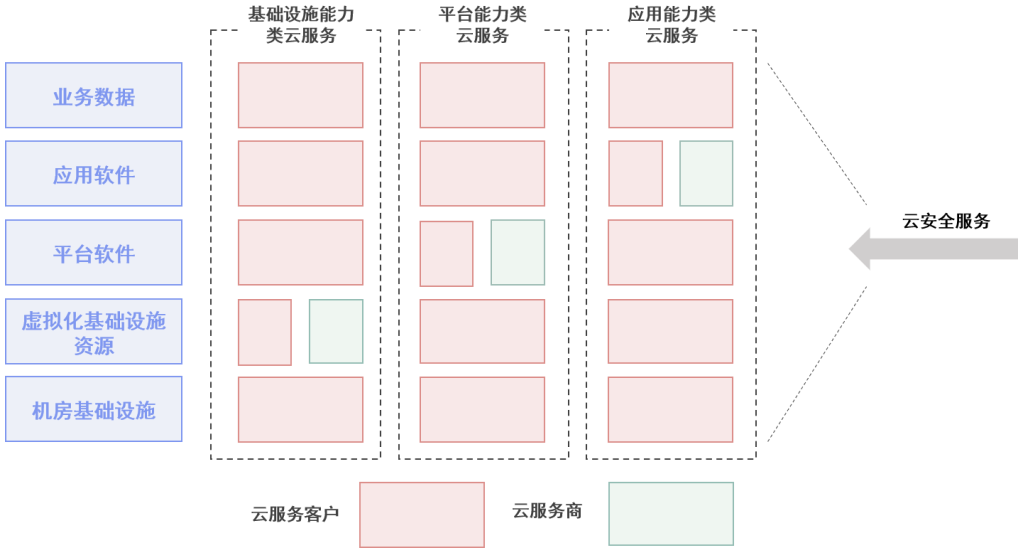


图 5　云软件交付模式对主体安全责任范围的影响示意图

对于云软件交付+服务托管模式，云服务商负责云软件自身的安全；云平台所依赖的底层资产及云平台日常运营的安全责任由云服务

客户负责，云服务商通过云运维运营服务的形式提供支撑；对于云软件部署的环境及其承载的资产安全由云服务客户负责，云安全厂商通过云安全服务的形式提供支撑，责任范围如图 6 所示。

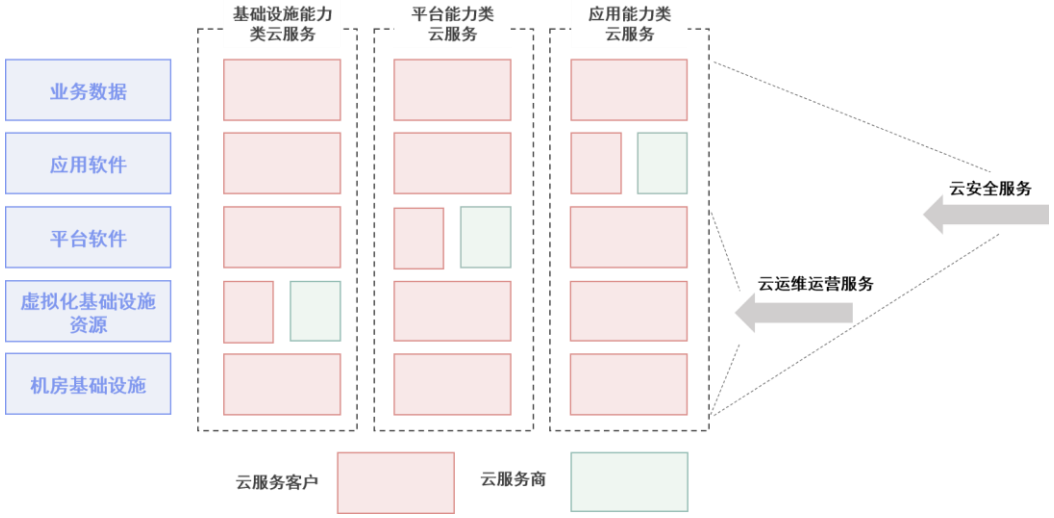


图 6　云软件交付+服务托管模式对主体安全责任范围的影响示意图

（四）　构建云安全责任共担三大关键环节

在上一节分析中，云计算的服务类型和服务模式影响各主体安全责任的范围，在责任范围内，各主体需开展的举措可归纳为三个关键环节：

一是云服务商与云服务客户责任共担，实现云平台的安全建设与使用。针对云平台，**云服务商对提供的云平台安全负责**，一方面确保云平台本身的安全性，另一方面为云平台构建合理的安全功能以供云服务客户使用。**云服务客户对云平台的安全使用负责**，通过利用云服务商提供的云平台安全功能，对使用的云服务进行合理的安全配置，安全功能只有被云服务客户充分利用，才能发挥其价值。

二是云安全厂商与云服务客户责任共担，夯实云环境的安全防护

体系。对于云上的业务和数据资产，**云服务客户对其安全防护负责**，明确安全目标，依托云安全厂商提供的安全服务构建云安全防护体系。**云安全厂商对所提供安全服务的质量负责**，交付满足云服务客户安全目的的安全服务，且保证安全服务本身的安全性。

三是云安全责任共担各主体建立信息传递机制。云服务客户、云服务商、云安全厂商对云及云上资产的可见性不同，各自的安全能力和优势也存在差异，所掌握的与云安全相关的信息各有侧重。为了保障云安全责任共担机制更有效的运行，各主体应建立信息传递机制，将必要的安全信息透明传达至应知方，如资产的基本信息及变化、各方关键的行为活动、来自外部的重要情报等。

基于本章分析，云安全责任共担 2.0 体系如图 7 所示。2.0 体系涉及四大方面：1）**四项基本原则**，指导云安全责任共担机制的开展；2）**三类责任共担主体角色**，一个组织机构可能同时承担一种以上的主体角色，如云服务商同时作为云安全厂商；3）**责任共担范围**，云计算的服务类型和服务模式决定各主体的责任范围；4）**三大关键环节**，一是云服务商与云服务客户责任共担实现云平台的安全建设与使用，二是云安全厂商与云服务客户责任共担夯实云环境的安全防护体系，三是云安全责任共担各主体建立信息传递机制

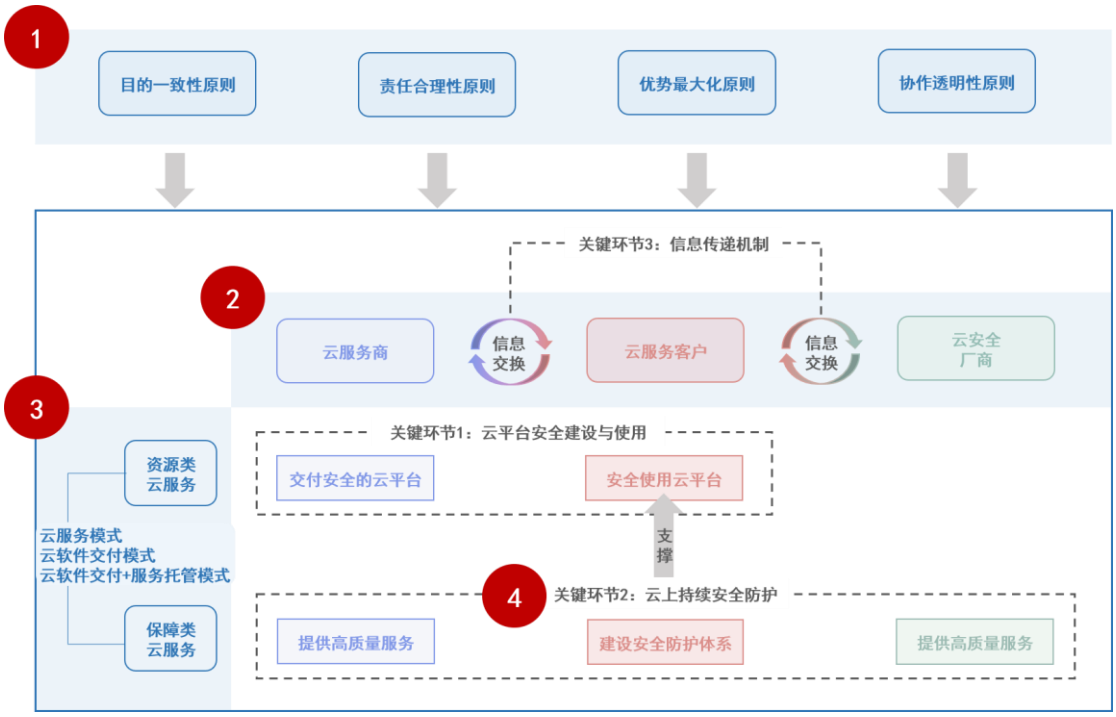


图 7　云安全责任共担 2.0 体系

三、云安全责任共担实施参考

（一）夯实云平台安全建设与使用能力

云平台底层的机房基础设施安全依托于数据中心的建设与运营。机房基础设施安全是确保上层业务正常运营的基石，责任方应具备架构建设、人员管理、机房管理、设备运维、应急响应等安全能力，与传统数据中心差异不大，本报告不做展开。

云平台的安全由云服务商和云服务客户共同保障，其责任共担既要求云服务商确保企业自身和云平台的安全性，又需要云服务客户安全的配置和使用云平台。不同的云计算的服务类型与服务模式下，云服务商和云服务客户所承担的安全责任不同，应逐步搭建并完善安全治理框架，引导双方正确识别和承担安全责任。

1、云服务商提升云平台自身安全性

云服务商应建立企业级安全治理体系和安全管理框架，筑牢顶层设计，科学规划责任分配；安全治理体系和安全管理框架的构建应充分引入零信任等新安全理念，将新理念与各项安全工作深度融合，并随着理念的创新不断优化完善；在安全治理体系和安全管理框架指引下，开展云平台安全、供应链安全、隐私保护、安全开发、访问控制等各领域的安全工作，涉及到的责任包括：

1）安全组织架构：建立企业多级安全架构，包括决策层、管理层和执行层；划分岗位并明确职责，如首席安全官、运维人员、审计人员等。

2）安全管理制度：依据法律法规和业务需求制定管理制度；整合隐私保护、风险管理、业务连续性管理、项目管理等形成全平台治理体系。

3）供应链安全：应制定供应链安全的策略，编制软件物料清单，维护供应商管理机制；对产品和服务采购进行安全管理，以确保产品和服务的安全性；明确与研发外包合作开发相关的信息安全管理原则和总体要求。

4）安全开发：确保云服务或软件在规划、设计、开发、部署、运维和用户支撑环境的规范性和安全性；提供软件开发过程中潜在异常问题的处理办法；建立内部测试及验收措施，确保生产环境变更和发布安全。

5）访问控制安全：建立细粒度的身份权限管理体系，最小化授权；灵活运用访问控制模型，动态、持续对访问行为进行控制，提高访问控制效率和安全性。

云平台应具备基础安全能力，为云服务的部署、运行、维护提供高效稳定的云环境，确保用户访问和使用云平台交互流畅，涉及到的责任包括:

1）云平台基础架构安全：实现虚拟资源在网络层的逻辑隔离；提供分布式部署，保障应用多活；形成容灾、备份、恢复、监控、迁移等解决方案保障数据安全。

2）云服务功能安全：提供云平台和云服务的访问控制、身份鉴

别、数据保护、安全审计、安全运行与安全策略管理等功能，支持用户管理和配置，保障云服务使用过程安全。

3）公有云安全运营和运维：实施证书与密钥管理保护信息安全；定义安全配置基线并定期审查；支持日志和监控，记录事态和生成相关证据；提供备份功能，防止数据的丢失。

2、云服务客户增强云平台安全使用能力

云服务客户应承担安全使用云平台的责任，与云服务商协同保障云服务安全性，提升云资源利用率，促进云上业务平稳运行。**1）应合理选择并安全配置云平台，**选择与自身需求相匹配的资源，基于安全基线配置云平台和服务；**2）应正确使用并及时维护云服务，**使用云平台符合相关要求规范，正确使用和操作云服务与应用，与云服务商保持协同；**3）建设成熟的组织管理机制，**制定安全管理制度，明确岗位职责，落实组织与云服务商、组织内各部门责任划分；**4）构建持续的安全运维运营体系，**具备一定的安全团队或人员，能够充分使用云安全服务并对安全事件进行快速响应，在自身无法配备安全团队时可引入外部专家服务；**5）不断提升自身安全能力，**管理者需明确责任共担的重要性和必要性，在提升驱动力或技术基础不足时，可引入外部专业资源开展安全咨询或培训，确保相关人员的安全意识、技能和经验达到要求并不断提升。云服务客户安全责任具体要求如表 1 所示。

表 1 云服务客户安全责任

云服务	客户责任
管理安全	1、 建立组织内部安全管理制度，明确云安全责任人; 2、 遵守当地法律法规和云平台用户协议; 3、 正确评估上云需求，选择合适的云服务; 4、 引入安全咨询和培训机制，不断提升企业安全水平; 5、 建立安全运维运营团队，或引入外部专家服务;
网络安全	1、 根据业务安全需求，选择合适的网络类型; 2、 正确配置防火墙，包括安全组、IP 黑白名单等，减少非必要端口暴露; 3、 合理管理公网 IP，关注云主机、负载均衡、NAT 等公网 IP 绑定情况;
计算安全	1、 选择功能、性能与需求相符的计算资源; 2、 合理选择与配置操作系统，包括系统文件权限、账户分配、更新规则等; 3、 开启镜像备份并关注备份情况;
存储安全	1、 确保数据访问安全，合理使用访问凭据，开启凭据轮转; 2、 执行数据变更、迁移、销毁等敏感操作时明确操作后果; 3、 合理配置数据备份并关注备份情况;
访问、授权、认证	1、 合理配置 IAM，确保用户权限分配最小化; 2、 妥善保存凭证和密钥信息，视情况开启多因子认证; 3、 配置远程访问方式和参数，关闭非必要服务; 4、 使用 API 和 SDK 服务符合规范要求;
安全与审计	1、开启审计功能，定期查看日志记录; 2、留意安全通知和平台告警，及时更新云资源版本，安装补丁修复漏洞。

（二）共筑云上持续安全防护体系

1、识别云安全防护能力域，打造安全履责能力

云服务客户在履行划分至自身的云上安全责任时存在挑战。**一方面**，云计算环境与传统 IT 架构相比更加复杂，云计算技术迭代十分迅速，云服务客户关于云上安全管理方面的知识储备很难做到面面俱到。**另一方面**，日益增长的云上安全管理需求也对云服务客户的安全防护能力提出了更高的要求，愈发严峻的云上安全态势需要通过不同能力域、不同类型的云上安全服务协同防护，增加了云服务客户的安全建设难度。

为了保障云上业务和数据的安全，云服务客户侧应当构建完善的安全防护体系。

基础安全能力域是保证云上安全的基石，主要包括：1）**云工作负载安全能力**，保证基础设施层中虚拟机、平台软件层中容器和容器编排服务的安全，实现对云工作负载不区分位置的统一安全管理与操作；2）**云网络安全能力**，对网络流量的监控与过滤，完成对不同地域与不同云平台上的统一网络安全管理；3）**应用安全能力**，一方面对应用进行防护，保证与外界的直接交界面安全，另一方面对 API 进行全面安全管控，防止潜在的安全威胁；4）**数据安全能力，**对数据流转全生命周期建立安全防护，保证数据收集、存储、处理、传输、共享、销毁阶段的安全，确保数据的安全性、可用性、完整性；5）**身份与访问管理能力**，以身份为核心，通过统一接入、统一访问控制和权限体系，提供一致的安全管控，并通过对云计算内用户、工作负载、应用等对象进行监控记录，保证所有行为的可追溯性。

安全全局化能力域是对抗高级威胁的有效手段，主要包括：1）**全局数据分析与展示能力**，通过将不同位置、不同功能的安全数据进行汇总分析，可以有效打破数据孤岛，充分发挥安全数据价值，深度挖掘潜在安全隐患，并给事件溯源提供清晰的证据链；2）**全局统一操控能力**，通过集中控制平台统一下发安全指令、修改安全策略、执行安全操作，优化重复的无意义操作，节省安全处理所需要的事件。

安全自动化能力域将全方位提高安全效能，主要包括：1）**自动化数据分析能力**，通过既定的策略与机器学习能力，帮助安全团队进行安全数据的预处理，将安全团队从重复的数据筛选工作中解脱出来，着眼于真正的威胁上；2）**自动化安全处理能力**，将常见安全操作以剧本的形式进行整理，通过对安全工具的编排实现对常见重复性安全威胁的秒级响应。

表 2 安全服务与安全能力对应关系

	资产清点	漏洞管理	配置核查	基线管理	流量分析	入侵防护	数据加密	数据可用性	访问控制	权限控制	行为审计	可视化展示	统一操作	自动化分析	自动化响应
主机安全工具	√	√	√	√		√					√		√		
容器安全工具	√	√	√	√		√					√		√		
云工作负载保护平台	√	√	√	√		√					√		√		
云防火墙			√	√	√	√			√			√			
抗DDoS工具					√	√			√						
网络入侵检测工具					√	√			√						
API安全工具	√		√	√	√	√						√			
云应用防火墙	√	√	√	√	√	√			√	√					
网页防篡改	√					√		√							
加密中台							√	√							
数据脱敏工具							√	√							
数据备份与恢复工具								√							
IDaaS			√	√		√			√	√					
堡垒机	√								√	√	√		√		
态势感知平台			√		√							√			
安全运营中心	√		√	√	√				√			√			
UEBA						√	√				√	√		√	√
XDR	√	√	√	√	√	√			√		√	√	√	√	√
SOAR				√		√			√				√		√

2、依托云安全服务构建安全防护体系

云服务客户的云上安全防护体系依托云安全厂商提供的云安全服务构建，主要包括两种路径：一是使用云服务商提供的更加原生化的云安全服务；二是选择具备定制化解决方案的安全厂商。云服务客户在进行云安全服务选型时应充分考虑自身实际生产场景与业务需要，选择云安全厂商。

选择云服务商作为云安全服务供应商主要有以下优势：1）**数据格式统一**，云服务商在进行产品开发时具有统一的设计规范，各产品与接口生成的数据均参照固定模板生成，因此在云安全服务调取数据时不需要对数据进行归一化整理，避免了可能产生的信息丢失，可以更好地理解安全数据产生的根本原因；2）**集中的安全管控**，一方面云服务商提供的云安全服务通过云平台的统一身份认证体系进行登录，用户切换服务时无需重复输入身份鉴别信息，另一方面云服务商自身云安全服务间接口开放数据互通，可以满足全局数据分析与统一安全操作的需求；3）**以保证业务连续性为导向的处理原则**，当前安全事件影响云服务客户业务连续性，导致业务质量下降或中断时，云服务商的安全解决方案具备直接协调云服务侧资源的能力，通过备份恢复或业务迁移等手段先恢复业务正常运行，避免云服务客户核心利益持续受损；4）**原生化安全体系发展具有前瞻性**，云计算技术发展十分迅速，技术开发主要以云服务商为中坚力量，云服务商的云安全服务具备关于新型技术的一手资料，包括但不限于开发理念、基础架

构、技术特性、可能存在的薄弱点等关键信息，同步开发适配的安全服务或对原有服务进行调整，使安全建设不落后于业务创新。

选择安全厂商作为云安全服务供应商主要有以下优势：1）**定制化程度高**，安全厂商具有大量的研发资源与经验，可以根据需求，对现有云安全工具进行定制化开发，充分适配云服务客户的实际安全需求，节约安全成本；2）**开放独立的技术架构**，工具安全功能的实现没有特定的依赖与从属关系，拥有独立的运行的能力，避免了因为绑定关系而导致的工具不可用情况的产生。同时，安全厂商可以细分为综合型安全厂商与专精型安全厂商。**综合型安全厂商具有成熟的统一解决方案**，具备对传统 IT 架构进行安全防护的能力，可以帮助企业建设云上云下统一的安全防护体系。**专精型云安全厂商具有快速的产品迭代能力**，技术聚焦于对当前领域的持续研究与现有产品的更新迭代，可以快速针对此领域威胁的变化做出响应。

在安全服务完成交付与部署后，为避免产生无意义的纠纷，云安全厂商与云服务客户之间也应进行责任划分，明确自身的责任。

云服务客户主要负责安全服务履约过程中的责任：1）**对由操作不当而引发的安全事件负责**，客户应遵循安全服务的基本使用原则，按照说明进行操作；2）**对由维护不当而引发的安全事件负责**，客户应对安全工具进行日常运维，以保证安全工具底层依赖的基础设施正产运转、安全策略的有效性，同时客户也应及时向供应商反馈在使用过程中发现的问题，以便供应商及时对安全服务进行修复更新。

云安全厂商主要负责安全服务部署前交付与服务期内的售后支持方面的责任：1）**应保证交付工具符合验收标准**，安全能力满足客户需求，可用性与稳定性高于 SLA 承诺的数值；2）**应保证工具有良好的易用性**，通过说明书、讲解视频、培训教学等方式降低客户操作难度与学习成本；3）**应保证安全服务的安全可靠**，在交付时无已知漏洞，并在合同期内提供如漏洞补丁等服务以保证安全服务的稳定性；4）**应在服务期内持续提供技术支持**，定期更新升级规则库保证工具先进性，通过远程或驻场的形式及时解决客户反馈的问题。

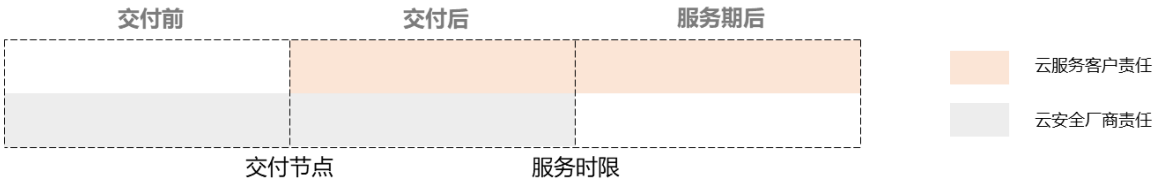


图 9　云安全工具责任划分

（三）多主体建立信息传递机制，促进云安全责任共担协同

云服务客户安全意识增强，对云上资产的安全性需求也不断提升，针对复杂多样的云上业务和数据，云服务商和云安全厂商推出了众多安全服务。云服务客户在接入安全服务时往往涉及到新的安全问题，特别是当云服务客户选择云平台以外的第三方安全服务时，可能需要兼顾云服务商和云安全厂商的安全责任要求。为促进云服务和安全服务高效协作，提升业务安全性，云服务客户与云服务商、云安全厂商之间应建立必要的信息传递机制，为多方信息互通和责任划分为提供参考。

1、云服务商和云服务客户之间的信息传递机制

云服务商和云服务客户在采购、提供、运营云服务的过程中，应主动提供必要的信息并知晓相关规定以提高协作效率。双方的信息传递与协作责任如表 3 所示。

表 3 云服务商和云服务客户之间信息传递与协作责任

协作内容	协作过程	云服务商	云服务客户
用户信息处理	通知、选择、收集	告知用户信息收集范围、用途等，提供隐私政策声明	提供和授权必要信息，确保信息真实可用
	使用、留存、处置	告知用户信息使用方式和主体、留存位置和形式、处置方式和期限	授权信息使用、留存、处置，依据留存和处置规则管理信息
	信息公开披露	告知用户公开披露场景和内容，审查公开场景的合法合规性	知晓信息披露规则并选择性授权
	数据跨境转移	告知用户跨境传输场景，与用户签订数据转移协议，遵循当地法律法规	知晓数据跨境转移规则并选择性授权
	委托处理	告知用户委托处理情况，限制委托方使用的信息在用户授权范围内	知晓委托处理规则并选择性授权
云计算技术服务	网站与账号服务	提供云平台服务条款、保密条款等，明确使用网站和账号所涉及的法律问题	在服务条款和法律法规范围内使用云平台和账号
	云服务订阅与变更	告知用户服务订阅规则、付费方式、违约责任等，明确双方的权利和义务	知晓云服务订阅与变更要求，恰当地选择和使用云服务
	云服务退订与终止	告知用户服务退订规则、资源处理方式等，明确双方的权利和义务	知晓云服务退订与终止要求， 对主动退订或终止服务的后果负责

	服务等级协议	提供各类云服务的 SLA 协议，内容变更应及时告知用户	知晓 SLA 协议内容，服务等级未达标时依据协议提出赔偿申请
	第三方支持	提供第三方服务接入（API、SDK 等）说明，和安全风险提示	在合规范围内使用第三方服务接入，承担数据云外安全责任
安全合规	监管合规	确保云平台符合所在地安全监管要求，为用户实现合规目标提供帮助	应用部署、功能使用、数据上传等操作应符合监管要求
	信息透明	在确保云平台安全的前提下不断提升信息透明能力	主动了解并合理使用公开信息，促进业务开展安全高效

2、云安全厂商和云服务客户之间的信息传递机制

云安全厂商和云服务客户在采购、提供、运营安全服务的过程中，应主动提供必要的信息并知晓相关规定以提高协作效率。双方的信息传递与协作责任如表 4 所示。

表 4 云服务客户和云安全厂商之间信息传递与协作责任

协作内容	协作过程	云安全厂商	云服务客户
用户数据处理	通知、选择、收集	告知用户信息（包括云平台信息）收集范围、用途等，提供隐私政策声明	提供和授权必要信息，确保信息真实可用
	使用、留存、处置	告知用户信息（包括云平台信息）使用方式和主体、留存位置和形式、处置方式和期限	授权信息使用、留存、处置，依据留存和处置规则管理信息
安全工具	接入远程工具	告知用户工具接入方式、认证方式、安全覆盖范围等，	提供必要的身份认证信息，遵循最小授权原则开

		提供工具安全性、合规性证明	放云平台接口，协商工具使用和管理方式
	部署云上工具	告知用户工具部署位置、运行机制、安全覆盖范围等，提供工具安全性、合规性证明	提供必要的身份认证信息，协商工具使用和管理方式
	旁路监测工具	告知用户监测范围、监测结果处理方式等，提供工具安全性、合规性证明	遵循最小授权原则开放云平台接口，协商工具使用和管理方式
安全服务	持续性交付	明确服务范围、周期，提供服务方案和协议	明确安全需求，提供必要的信息和支持，持续关注并反馈服务效果
	交付物	明确交付内容、时间，提供服务方案和协议	明确安全需求，提供必要的信息和支持
安全一致性	功能适配	提供安全产品和服务说明，确保云平台支持且符合用户需求	根据信息安全三要素和最小授权原则选择适当的安全产品
	消息传递	及时处理威胁告警、漏洞信息等并告知用户	及时关注相关的威胁告警、漏洞信息等
	补丁更新	及时更新产品补丁并告知用户	关注补丁更新动态，及时下载并安装

四、云安全责任共担发展建议

强化标准引领作用，提升云服务客户安全责任意识与能力。我国云安全责任共担相关标准建设已初步具备多项成果，但仍有进一步完善的空间。对于云服务客户，云安全责任共担的关键不仅仅是了解云服务商和云安全厂商应该提供什么，也应聚焦于理念文化和落地实施层面，深切理解云安全责任共担的必要性与意义，了解自身应该做什么、怎么做。未来，云安全责任共担标准体系可聚焦于云服务客户的实际需求与挑战，一是提升责任共担的思想意识，企业层面理解重视、积极开展责任共担工作，个体层面业务、研发等各领域人员安全意识不断提升，促进安全融入云服务客户云上业务的方方面面；二是夯实相关人员的云计算技术素养，指导其安全用云；三是强化相关人员的安全能力，指导其更高效的使用安全服务、响应安全事件。

完善保险机制，构建事前、事中、事后云安全闭环体系。事前的安全建设以及事中的安全响应无论如何完备充分，都无法百分百保证能够抵御风险事件、不遭受任何损失。保险作为一种风险转移的手段，应用在云计算等信息技术安全保障场景中，能够提供事后的经济保障，与企业开展的各项安全工作互补形成闭环。2023 年 7 月 10 日，工信部、国家金融监督管理总局发布了《关于促进网络安全保险规范健康发展的意见》，为网络安全保险发展提供了相关政策支持。中国信通院也联合保险服务机构共同研究探索云保险、信息技术应用服务保险等创新险种，保障云服务商云平台运营以及云服务客户应用云服务中

的安全。未来，在政策和市场需求的引导下，保险服务机构将进一步优化核保、承保、理赔、风险量化等流程，与云服务客户、云服务商、云安全厂商协同合作，完善云安全责任共担体系。

促进云服务商与产业多主体生态圈建设，提升安全能力整体水平。云服务客户上云用云过程中面对的供应商不仅仅包括云服务商和云安全厂商，还可能涉及云管理服务提供商（MSP）、集成商、设备商等，任何一个环节存在安全薄弱点，都有可能影响云上业务和数据安全，各方孤立、分别开展工作也将影响云安全工作的效率效果。未来，以云为中心建立更加丰富的生态圈十分必要，一方面推动各类衍生设备、服务与云的原生融合，实现各主体、各环节安全能力的拉通对齐，为云服务客户提供一致、完整、体验高的产品服务；另一方面鼓励各云服务商间互联互通，缓解云服务客户多云/混合云难管理等痛点。

五、结语

“十四五”时期，云计算迎来新发展阶段，只有充分发挥云安全责任共担模式作用与价值，才能更好的保障千行百业云上业务与数据安全。在此过程中，云服务商、云服务客户、云安全厂商等主体应充分发挥各方优势，提升云安全责任共担意识和能力，统一安全目标，协同推动云安全工作的高质量开展，有效应对日益复杂的网络安全挑战。

附录：云安全责任共担模式在多场景下的应用案例

报告第二章给出了云安全责任共担 2.0 体系的基本框架，围绕云安全中配置风险、软件供应链风险、勒索风险等重点场景，本章进一步识别了风险场景中各主体应承担的细化责任，作为 2.0 体系应用的示例。

（一）云安全配置风险场景

为规避云安全配置风险，云安全责任共担各主体的责任共担示例如表 5 所示。

表 5 云安全配置风险场景下责任共担示例

	云服务模式下责任	云软件交付模式下责任	云软件交付+服务托管模式下责任
云服务商	1、保障机房基础设施的安全建设和运营; 2、保障虚拟化平台的安全建设和运营; 3、**为云服务设计、开发完备的安全功能**供云服务客户使用，如访问控制功能、身份鉴别功能、数据加密功能等。	1、保障交付的云软件安全性，包括无高危漏洞、架构安全等。 2、**为云服务设计、开发完备的安全功能**供云服务客户使用。	1、保障交付的云软件安全性，包括无高危漏洞、架构安全等。 2、按 SLA 提供云运维服务，**依据云服务客户安全配置规范配置云服务**。
云服务客户	1、**合理配置和使用云服务的安全功能**，如设置细粒度访问控制权限、关闭不必要开放端口、设置数据加密算法等;	1、**合理配置和使用云服务的安全功能**; 2、**可购买云安全配置检查相关产品**辅助检测不合理配置; 3、保障机房基础设施的安全建设和运	1、**按业务需求明确云服务安全配置规范**; 2、**可购买云安全配置检查相关产品**辅助检测不合理配置; 3、保障机房基础设施

	2、**可购买云安全配置检查相关产品**辅助检测不合理配置; 3、可购买其它安全服务实现云服务及其上业务的安全防护，如 DDoS 检测等。	营; 4、可购买其它安全服务实现整个云环境的安全防护。	的安全建设和运营; 4、可购买其它安全服务实现整个云环境的安全防护。
云安全厂商	1、提供满足 SLA 的云安全配置检查产品。	1、提供满足 SLA 的云安全配置检查产品。	1、提供满足 SLA 的云安全配置检查产品。

（二）软件供应链风险场景

为规避软件供应链风险，云安全责任共担各主体的责任共担示例如表 6 所示（表 5 中已列出的基础责任在此不再赘述）。

表 6 软件供应链风险场景下责任共担示例

	云服务模式下责任	**云软件交付模式下责任**	**云软件交付+服务托管交付模式下责任**
云服务商	1、在**云服务的软件依赖组件暴漏安全漏洞**时，及时修复并告知云服务客户潜在风险; 2、当**云平台被入侵且可能影响云服务客户云上业务**时，及时防护并告知云服务客户潜在风险; 3、当**云服务商发生重大变更可能影响云服务客户业务连续性**时，提前告知云服务客户变更计划。	1、在云服务客户存在需求时，向云服务客户**提供云软件的软件物料清单**; 2、在云软件发现安全问题时，**及时修复并提供补丁包**。	1、在云服务客户存在需求时，向云服务客户**提供云软件的软件物料清单**; 2、在云软件发现安全问题时，**及时修复并提供补丁包**; 3、**强化云运维服务人员的培训教育，制定规范化服务方案**，避免服务人员成为软件供应链攻击的突破口。

云服务客户	1、针对云服务可能存在的软件供应链风险，**制定应急响应方案，**如服务迁移等; 2、**及时接收云服务商和云安全厂商告知信息并依据应急响应方案采取措施**; 3、**可购买软件供应链安全相关产品**辅助防范软件供应链风险,如IAST、SAST、RASP 等。	1、针对云软件可能存在的软件供应链风险，**制定应急响应方案**; 2、依据软件物料清单，在发现云软件依赖组件暴漏安全漏洞时，**及时告知云服务商和云安全厂商并要求其协助实施应急响应方案**; 3、发现云软件问题时，**及时告知云服务商和云安全厂商并要求其解决优化**; 4、**接收云服务商和云安全厂商提供的补丁包并及时安装**。	1、针对云软件可能存在的软件供应链风险，**制定应急响应方案**; 2、依据软件物料清单，在发现云软件依赖组件暴漏安全漏洞时，**及时告知云服务商和云安全厂商并要求其协助实施应急响应方案**; 3、发现云软件问题时，**及时告知云服务商和云安全厂商并要求其解决优化**; 5、**接收云服务商和云安全厂商提供的补丁包并及时安装**; 6、**建立第三方人员安全管理规范**，加强云运维运营服务人员的管理。
云安全厂商	1、提供满足SLA的软件供应链安全产品。 2、在**云安全服务的软件依赖组件暴漏安全漏洞**时，及时修复并告知云服务客户潜在风险; 3、当**云安全厂商发生重大变更可能影响云服务客户业务连续性**时，提前告知	1、提供满足SLA的软件供应链安全产品。 2、在**云安全软件的软件依赖组件暴漏安全漏洞**时，及时修复并告知云服务客户潜在风险; 3、当**云安全厂商发生重大变更可能影响云服务客户业务连续性**时，提前告知	1、提供满足SLA的软件供应链安全产品。 2、在**云安全软件的软件依赖组件暴漏安全漏洞**时，及时修复并告知云服务客户潜在风险; 3、当**云安全厂商发生重大变更可能影响云服务客户业务连续性**时，提前告知

	云服务客户变更计划。	云服务客户变更计划。	云服务客户变更计划。

（三）云上勒索风险场景

为规避云上勒索风险，云安全责任共担各主体的责任共担示例如表 7 所示（表 5、6 中已列出的基础责任在此不再赘述）。

表 7 云上勒索风险场景下责任共担示例

	云服务模式下责任	云软件交付模式下责任	云软件交付+服务托管模式下责任
云服务商	1、 云平台具备数据加密、数据备份、访问控制等**数据安全能力**; 2、 当时监测到云平台内发生勒索事件时，及时**将情报信息向云服务客户预警**。	1、 云平台具备数据加密、数据备份、访问控制等**数据安全能力。**	1、 云平台具备数据加密、数据备份、访问控制等**数据安全能力**; 2、 按SLA提供云运维服务，**依据云服务客户要求合理开展数据备份等工作**。
云服务客户	1、 **合理制定防勒索方案**，并基于云平台数据安全能力落实相关方案，如数据备份策略; 2、 接收到云服务商或云安全厂商的情报信息后，**及时排查是否存在被勒索风险，采取应急响应举措**。 3、 **可购买云上防勒索相关产品**辅助预防	1、 **合理制定防勒索方案**，并基于云平台数据安全能力落实相关方案; 2、 接收到云安全厂商的情报信息后，**及时排查是否存在被勒索风险，采取应急响应举措**。 3、 **可购买云上防勒索相关产品**辅助预防和响应勒索事件。	1、 **合理制定防勒索方案**，并基于云平台数据安全能力落实相关方案，部分方案可在云服务商运维运营服务人员的协助下开展; 2、 接收到云安全厂商的情报信息后，**及时排查是否存在被勒索风险，采取应急响应举措**。 3、 **可购买云上防勒索**

	和响应勒索事件。		**相关产品**辅助预防和响应勒索事件。
云安全厂商	1、 提供满足SLA的云上防勒索产品。 2、 当监测或收集到勒索攻击情报信息时，及时**向云服务客户预警**。	1、 提供满足SLA的云上防勒索产品。 2、 当监测或收集到勒索攻击情报信息时，及时**向云服务客户预警**。	1、 提供满足SLA的云上防勒索产品。 2、 当监测或收集到勒索攻击情报信息时，及时**向云服务客户预警**。

编制人员

邹　丰　　耿　涛　　孔　松　　韩　非　　王睿宁

若您对本报告有任何建议，请联系：
wangruining@caict.ac.cn