云安全责任共担模型

2024年7月

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。

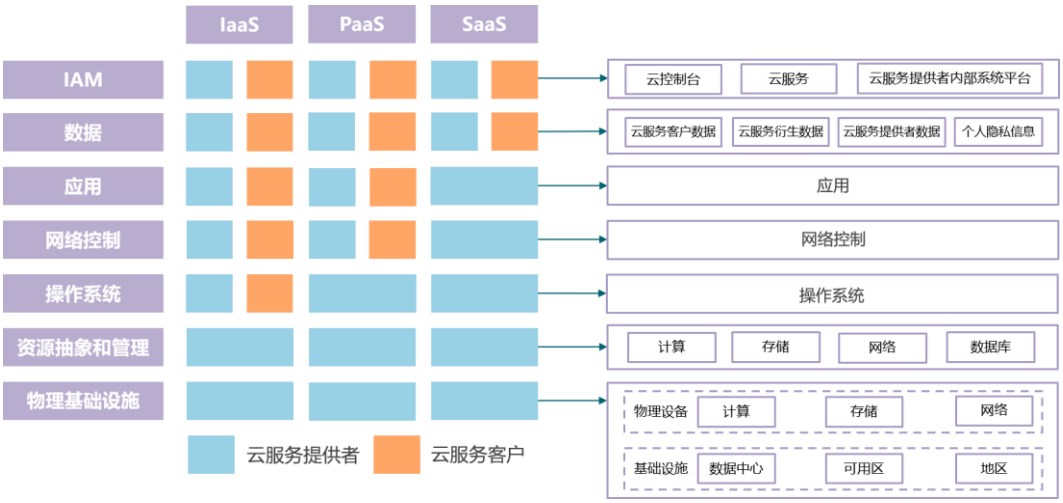
（一） 政策标准为云安全责任共担提供更坚实的发展基础

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。

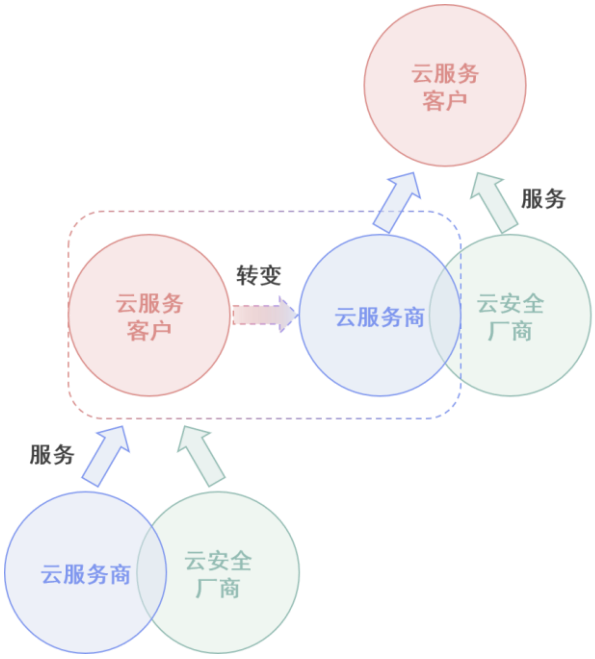


图 2　云安全责任共担主体

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。

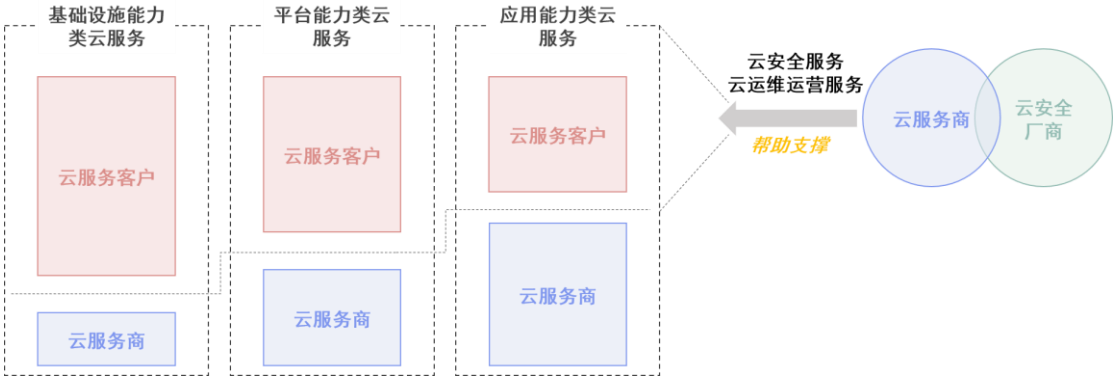


图 3　云计算的服务类型对主体安全责任范围的影响示意图

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。

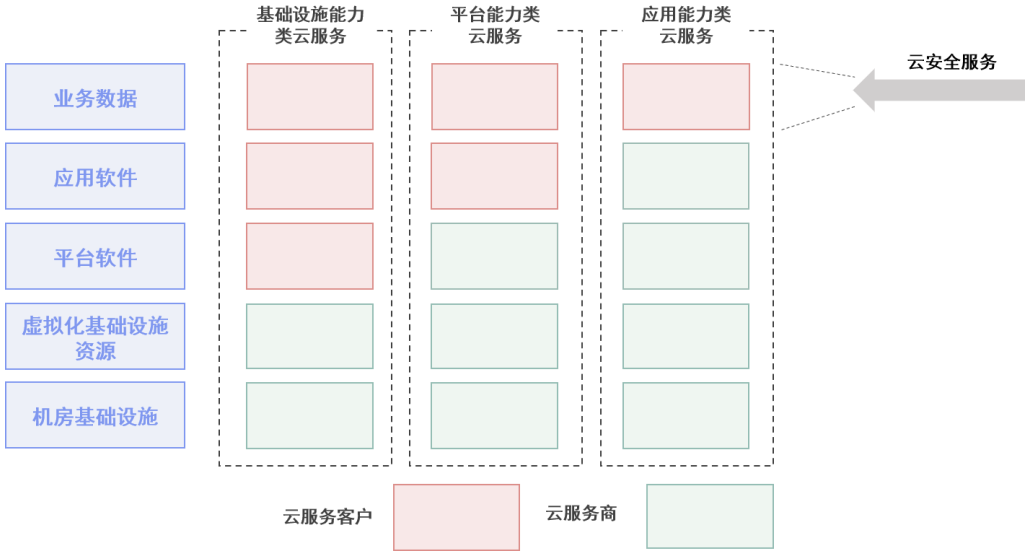


图 4　云服务模式对主体安全责任范围的影响示意图

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。

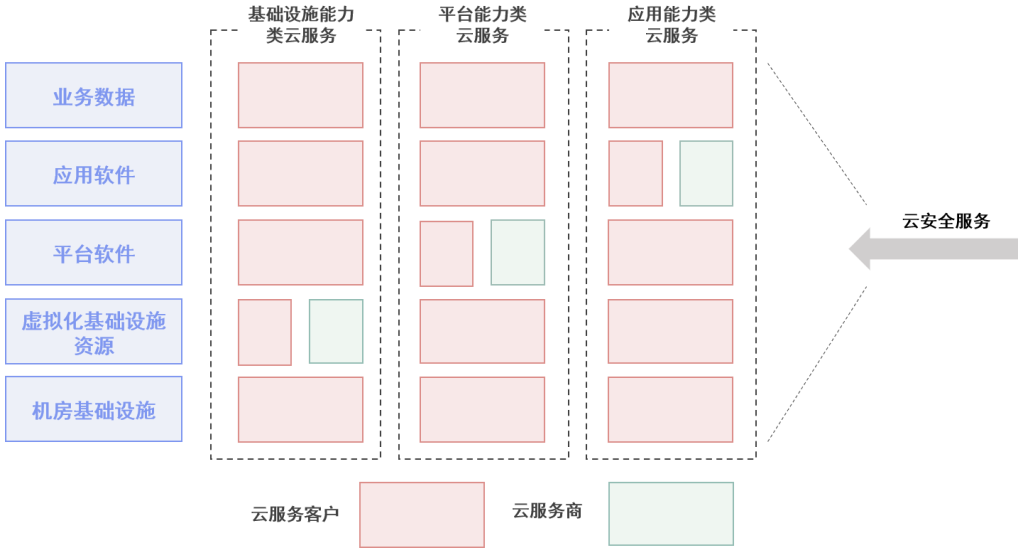


图 5　云软件交付模式对主体安全责任范围的影响示意图

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。

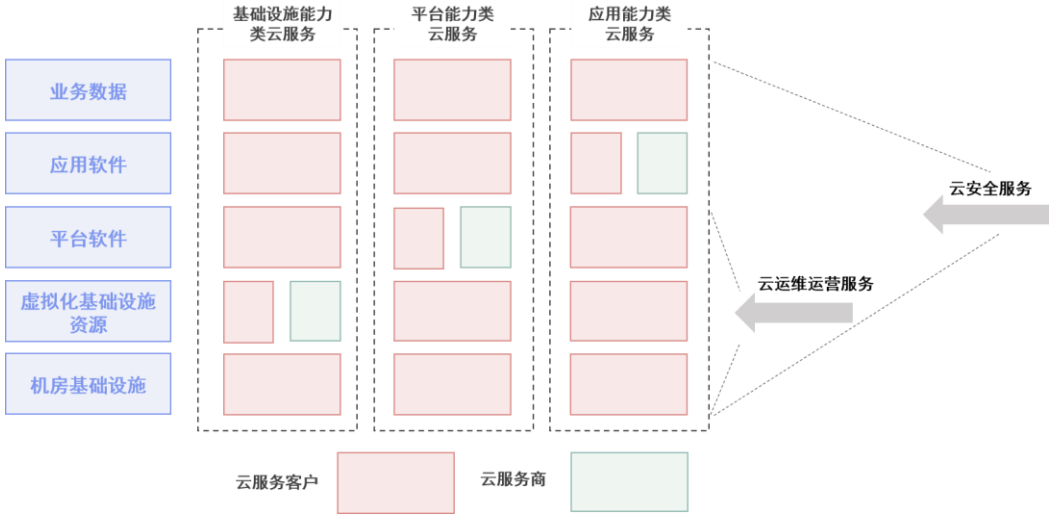


图 6　云软件交付+服务托管模式对主体安全责任范围的影响示意图

（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

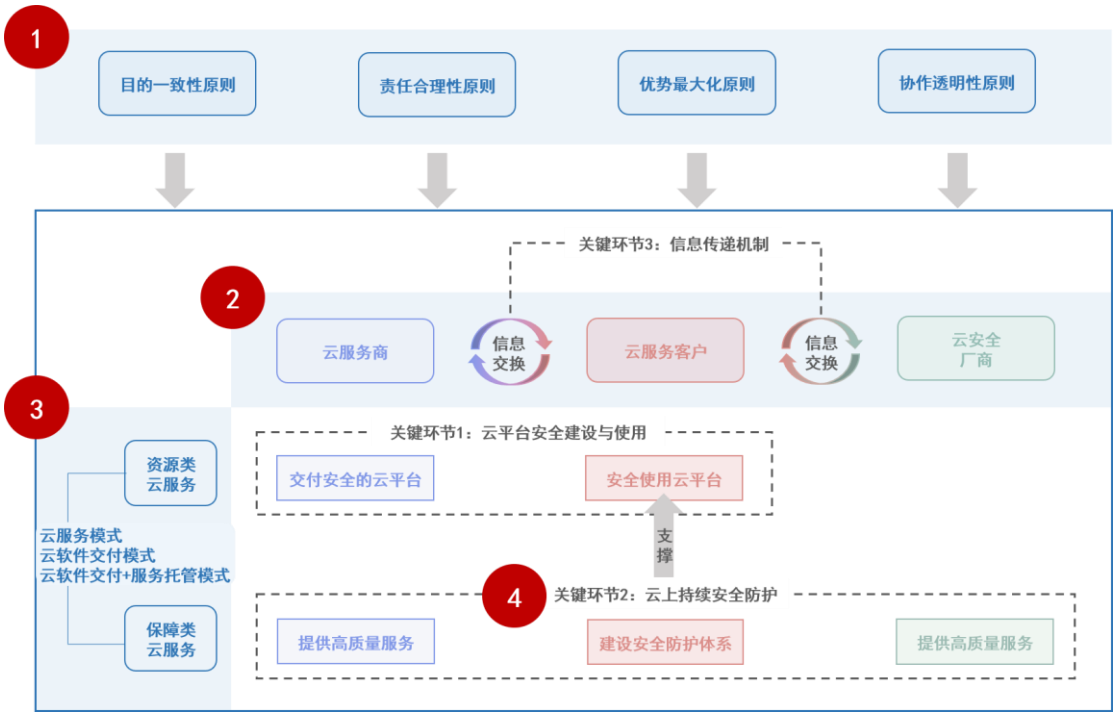


图 7　云安全责任共担 2.0 体系