云计算标准和开源推进委员会

可信安全
TRUSTED SECURITY

云安全发展研究报告

（2024）

中国通信标准化协会-云计算标准和开源推进委员会

前 言

近些年，我国各行业上云用云进程加快，云计算承载的业务和数据规模不断提升，云安全成为影响企业生产经营的关键要素之一。随着政策法规不断完善、技术和市场逐渐发展，云安全体系优化变革面临新机遇。

本报告首先分析了政策法规、市场等因素为云安全发展带来的新变化。其次从云平台安全、云安全防护、云安全责任共担三大维度，对我国云安全产业的发展情况与关键举措进行观察和分析。在云平台安全方面，分析了云服务客户选云时的安全需求、用云的安全举措，同时梳理了云服务商安全能力框架。在云安全防护方面，剖析了云服务客户在云安全工具使用运营中的挑战和应对方案，同时梳理了我国云安全产品供应的现状与问题，为云安全厂商优化发展产品体系提供指引。在云安全责任共担方面，围绕原则、协作、实践三大视角，拉通云平台安全和云安全防护中的各关键环节。最后从技术理念、创新方式、产业供应、应用建设方面对我国云安全发展提出展望。

本报告的核心观点与重要发现:

- 云安全体系包括云平台安全和云安全防护两大部分，主要涉及云服务商、云安全厂商与云服务客户三大角色主体，各主体通过责任共担机制开展云安全工作。一方面，云平台安全是保障云上业务安全的基石，云服务商提供安全的云平台，

云服务客户安全使用云平台；另一方面，云安全防护能够满足云服务客户多样性安全需求，云安全厂商提供丰富的云安全工具，云服务客户围绕安全需求，依托工具、人员、制度构建云安全防护体系。

- 云安全责任共担机制通过四大原则和三大举措，提倡云服务商、云服务客户、云安全厂商等主体各司其职、协同开展安全工作，有效保证云安全体系的有效运转。
- 云安全在技术理念、创新方式、产业供应、应用建设等方面的发展体现在：零信任等综合性的云安全技术理念受到关注；自我突破和融合创新双向驱动云安全革新；产业供应向服务化和协同联动升级；安全建设需适应远程连接等上云新趋势带来的挑战。

在本报告编写中，中国通信标准化协会云计算标准和开源推进委员会面向四十余家云服务商和云安全厂商，以及七十余家云服务客户，通过问卷、访谈、交流会等形式开展了调查工作（以下简称“调查”），文中提及调查之处，数据和观点来自于对本次调查结果的整理。

目 录

图目录

一、云安全态势不断变化，多方携手筑牢防线

随着各国对云安全的重视程度逐步加深，企业云安全体系建设尤为重要。本章从政策和市场入手，分析我国与欧美近年云安全政策法规关注点、全球云安全市场概况，以及我国云安全技术发展情况，提升云服务客户携手云服务商和云安全厂商开展云安全体系建设的信心。

（一）云安全政策法规要求不断强化

1. 云上数据存储与传输涉及复杂管理要求

欧美重视云主权问题，云上数据流转面临复杂局势。数据安全是云安全的核心问题之一，云服务数据安全引发云主权顾虑。**一方面，欧美加强云主权管理，颁布若干云服务数据出境限制规则。**欧盟提出的《欧盟云服务网络安全认证计划草案》中要求，云服务数据需在欧盟存储和处理，欧盟以外的任何实体不得直接或间接、单独或共同对云服务提供商拥有有效控制能力。美国国会众议院通过的 H.R.7520《保护美国人免受外国对手侵害的数据法案》，核心一条是禁止美国数据经纪人把美国人的敏感数据传输给外国对手国家或者外国对手国家“控制或受其指示”的实体。**另一方面，云服务数据涉及出境需求，各国监管法律尚存差异。**欧盟《通用数据保护条例》（GDPR）要求，当个人数据从欧盟传输到第三国时，必须确保接收国的数据保护水平达到与欧盟相当的标准，或者获得数据主体的明确同意，并且这种传输必须基于特定的合同或法律义务。2023 年 5 月，Meta 位于爱尔兰的总部按美国《澄清境外数据的合法

使用法》要求，将欧盟用户数据传输至美国政府，这一行为违反了GDPR 关于跨境数据传输中，需确保数据传输的目标地达到欧盟所认可的标准和采取适当保障措施的规定，由于美国的数据保护标准未获欧盟认可，Meta 被欧盟隐私监管机构罚款 13 亿美元。

2. 重要数据分类新规明晰云安全合规工作

新国标助力企业云上重要数据分类分级。我国自 2016 年开始重视数据分类分级相关工作，2016 年 11 月《网络安全法》明确将“数据分类”作为网络安全保护法定义务之一，2021 年 9 月《数据安全法》确立了“数据分类分级保护制度”及其基本原则。2024 年 3 月 21 日，国家标准 GB/T 43697-2024《数据安全技术 数据分类分级规则》正式发布，对数据分级规则、数据分类分级流程、个人信息分类、重要数据识别、一般数据分级等作出系统性指导。其中，针对重要数据识别制定了指南，从多维度对数据进行综合定级。由于上云企业的云上数据所涉业务广泛，数据体量大、分布分散、状态动态变化，企业开展云上数据分类分级工作需多部门协作，难度较大，因此更为关注此标准内容。

3. 云的关键信息基础设施运营者面临多方责任划分难题

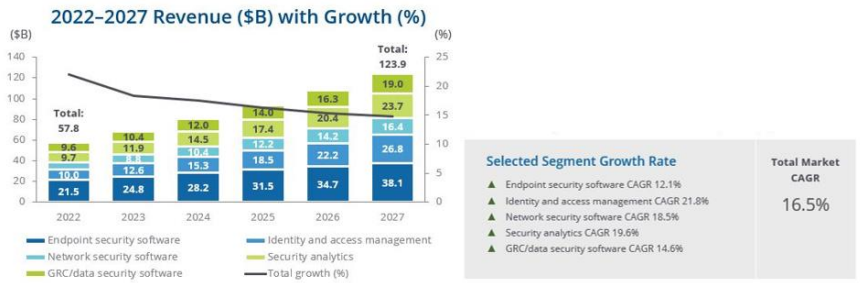
关键信息基础设施安全保护条例要求强化和落实关键信息基础设施运营者的主体责任。活跃用户超百万的云平台和大型云数据中心等关键信息基础设施的运营与使用，涉及云服务商、云安全厂商以及云服务客户多类角色，他们共同协作，以确保关键信息基础设施云上的安全与稳定，其中包括云平台的安全设计、安全工具的有

效性以及云服务安全配置等多个方面，他们之间在数据安全、业务连续性等方面所承担的工作有重叠，各方之间的安全责任需要得到明确界定。

（二）全球云安全市场增速保持放缓，仍保持一定增长率

安全即服务是安全产品云化后的表现形式，如云工作负载安全保护平台和云防火墙等，用户能够利用多安全领域的安全即服务解决云上安全问题，因此报告对安全即服务市场情况展开分析。

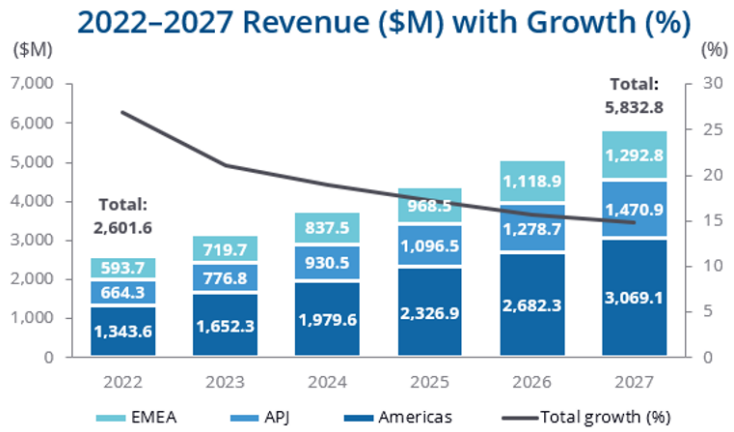
安全即服务市场增长趋势变缓。受到与新技术融合复杂性高、用户隐私合规要求高以及政策法规的不确定性等因素影响，安全即服务总市场增长率逐年缓慢下降，但仍保持在15%的增长速率。IDC发布的 2023-2027 全球安全即服务预测中给出了五种安全能力的CAGR（Compound Annual Growth Rate，复合年均增长率），其中，终端安全 CAGR 最低为 12.1%，身份和访问管理软件服务 CAGR 最高为 21.8%，网络安全、安全分析和数据安全 CAGR 位于其间，五种安全能力 CAGR 区间差值较小，表明五类安全即服务在市场采用方面表现相近，增长趋势趋同。



来源：IDC 2023 年 5 月

图 1 全球安全即服务收入概况

全球云工作负载安全市场增速放缓，我国公有云场景市场增速超过全球。IDC 调研如图 2 所示，2023 年全球云工作负载安全收入近 31.48 亿美元，相较于 2022 年实现了 21%的增长，美国云工作负载收入占比最高，高达 52% 已超过 2023 年占全球总收入半数，据预测 2024-2027 全球云工作负载安全总市场增长率将持续逐年降低。2023 年我国公有云[1]和私有云[2]云工作负载安全市场规模分别为 9.903 和 15.27 亿元人民币，相较于 2022 年增长率分别为 26.8%和 3.5%，我国私有云云工作负载安全市场竞争加剧，目前，各厂商主要通过拓展技术栈、覆盖专项场景、价格调整和下沉市场开拓等手段提升自身竞争力。



来源：IDC 2023 年 5 月

图 2 全球云工作负载安全收入概况

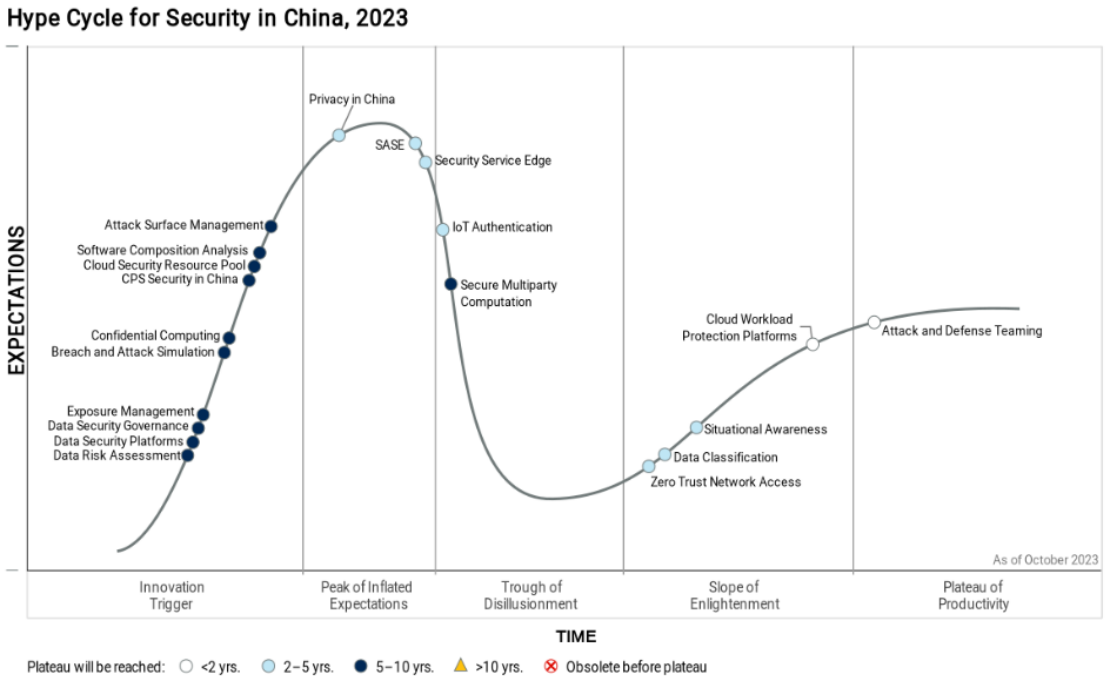
（三）我国云安全技术创新保持活力，产品加速升级

Gartner 发布的 2023 年中国安全技术成熟度曲线中（后简称“安全成熟度曲线”，如图 3 所示），云安全资源池、暴露面管理、攻击

[1] IDC, # CHC51233524，2024 年 6 月
[2] IDC, # CHC51544624，2024 年 6 月

面管理、SASE（Secure Access Service Edge，安全访问服务边缘）、SSE（Security Service Edge，安全服务边缘）和 ZTNA（Zero Trust Network Access，零信任网络访问）等云安全技术进一步迈向成熟，其中暴露面管理是 2023 年曲线新增技术。

暴露面管理迎来发展机遇。暴露面属于顶层概念，包含了攻击面、脆弱性、安全验证三项内容，暴露面管理得以发展的原因主要有三点：一是我国云计算蓬勃发展，云服务数量不断增加，云环境威胁多样化致使攻击面扩大、资产暴露面增大，暴露面管理势在必行；二是人工智能与生成式 AI 赋能暴露面管理，提升管理有效性，因此技术有广泛应用前景；三是随着安全验证技术能力提升，检出大量暴露面，暴露面管理可按威胁程度梳理优先级，并指引企业采取修复行动，提升企业安全防护能力。



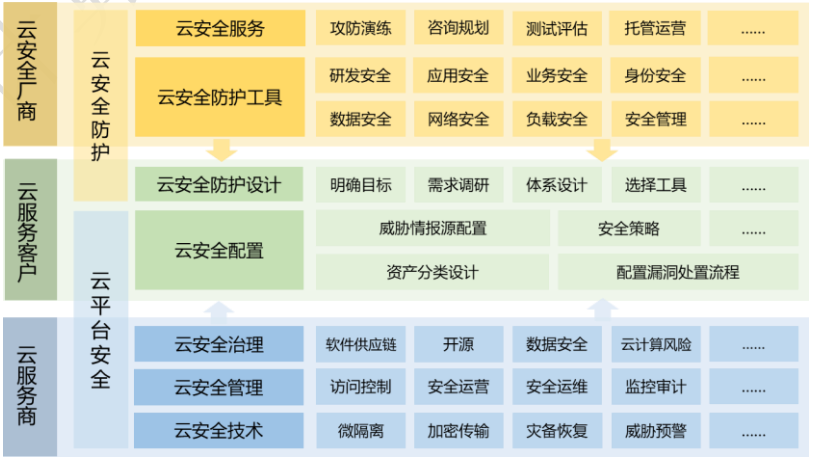
来源：Gartner 2023 年 10 月

图 3 2023 年中国安全技术成熟度曲线

基于零信任理念的相关技术五年内将达到生产成熟期。疫情期间远程办公需求加快了基于零信任理念的相关技术的成熟，SASE 整合多种边缘访问功能，是融合云网和安全的综合性服务，SSE 则侧重安全。安全成熟度曲线中 SASE 和 SSE 位于期望膨胀期，由于云网架构落地复杂性且涉及企业合规等问题，客户兴趣低于预期，与 2022 年相比正在从峰值下降，但 Gartner 仍旧认为未来 2-5 年，SASE 与 SSE 将成为主流趋势。同时，与 2022 年相比，ZTNA 已从泡沫破裂低谷期迈入稳步爬升复苏期，市场预期较为光明。

（四）三方主体携手筑牢云安全体系

随着我国云安全政策规范化，云安全技术多样化，云安全工作复杂化，为保证云上业务得以安全的开展，需要云服务商、云安全厂商与云服务客户三方共同努力，协同为云上价值创造提供有力保障。如图 4 所示，**云安全体系主要包括云安全防护和云平台安全两大方面，由三类角色按云上安全责任共担模型划分工作，协同完成两方面涉及的安全防护工作。**



来源：中国信通院

图 4 云安全体系架构

云服务商夯实云平台安全基座。一方面，云服务商布局计算、存储、网络等领域安全技术，提供多种安全技术，保障云平台资源安全性；提供丰富的云平台管理能力，保障云平台的安全访问、安全运营与安全运维，从管理上强化云平台安全；积极开展云环境安全治理，全方位提升云平台的威胁防护能力。**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，如提供策略管理、资产管理、威胁管理和漏洞管理等功能便于云服务客户进行精细化安全设置。

云服务客户安全使用云平台，按需建立云安全防护体系。一方面，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，如设置安全策略、设计资产分类分级依据、纳管威胁情报源和配置漏洞处置流程等，充分发挥安全功能成效保护云上资产。**另一方面，**构筑云安全防护体系，依托云服务商提供的安全底座，依据自身业务需求与安全目标，将云安全厂商提供的安全能力进行融合，构建适应自身的云安全防护体系。

云安全厂商提供高质量的云安全工具与服务。云安全厂商既可以由云服务商担任，也可以是专业的安全厂商。**一方面，**交付满足云服务客户安全目的的安全服务与工具，保障其安全地上云、用云。网络安全、数据安全和负载安全等工具能够保护云服务客户的云上资产，诸如 IAST（Interactive Application Security Testing，交互式应用程序测试）一类的研发安全工具能够为云服务客户提供安全的开发环境，云安全服务则践行专业人做专业事，帮助云服务客户以较

低时间成本达成最终安全目标。**另一方面，**保证安全服务与工具本身的安全性，发布前云安全厂商应开展全面的安全性验证和测试，确保安全服务与工具没有安全隐患，并持续更新、修补新的漏洞。

二、云平台安全是保障云上业务安全的基石

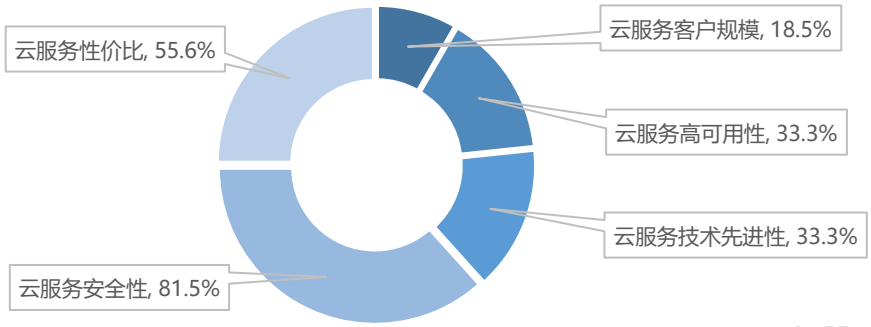
依托云服务扩展灵活、管理便捷等优势，越来越多的企业选择将数字资产和业务向云上迁移。云平台作为数字资产的载体，其安全性备受云服务客户关注，是保障云上业务安全的基石。云服务客户应关注选云、用云过程中的安全问题，云服务商则承担云平台建设、基础运营过程中的安全责任。本节首先梳理云平台安全发展现状，并从用户侧和供应侧两方面入手提出发展建议。

（一）云平台安全能力成为企业上云关键要素

云计算承载了大量企业核心数据和关键业务，安全风险代价高，上云企业安全意识不断提升，一方面对云服务供应侧的安全水平提出更多要求；另一方面云服务客户自身的安全用云能力不足以支撑日益增长的安全需求，亟需进一步优化增强。

云服务的安全性是企业选型关注重点。企业在选择和采购云平台时有明显的能力倾向，如技术先进性、安全性、性价比、客户规模、高可用等，其中云服务的安全性受到各行业用户的广泛关注。如图 5 所示，调查中超过 80%的云服务客户在计划采购云服务时将优先考虑其安全性，大幅超过第二优先级的性价比因素。此外，各行业对云服务安全性的需求侧重点不同，如政务、央国企上云首先应确保云基础设施的稳定性，提升跨系统跨部门的信息共享与业务

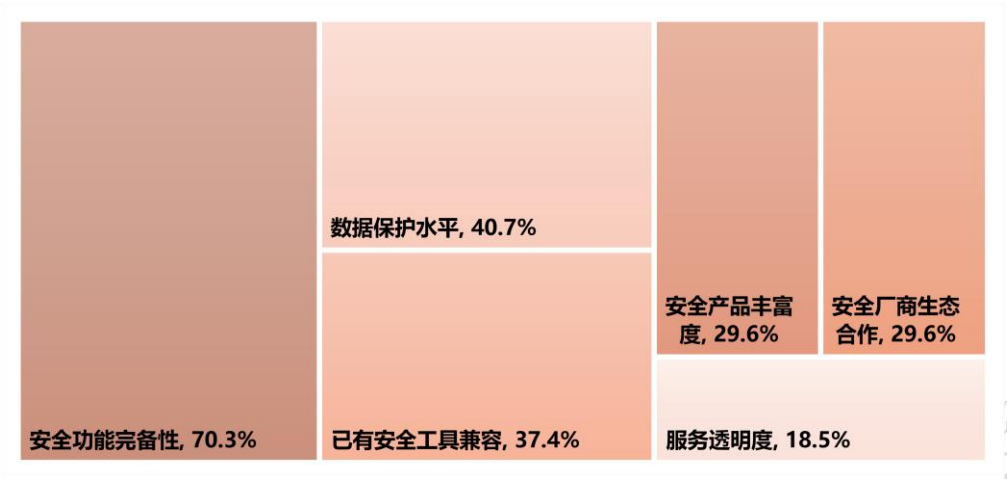
协同安全性；汽车行业更关注数据加密和隐私保护能力，期望搭建从车端到云端的多维度的数据安全体系。



来源：中国信通院

图 5 云服务客户计划采购云服务时优先考虑的因素

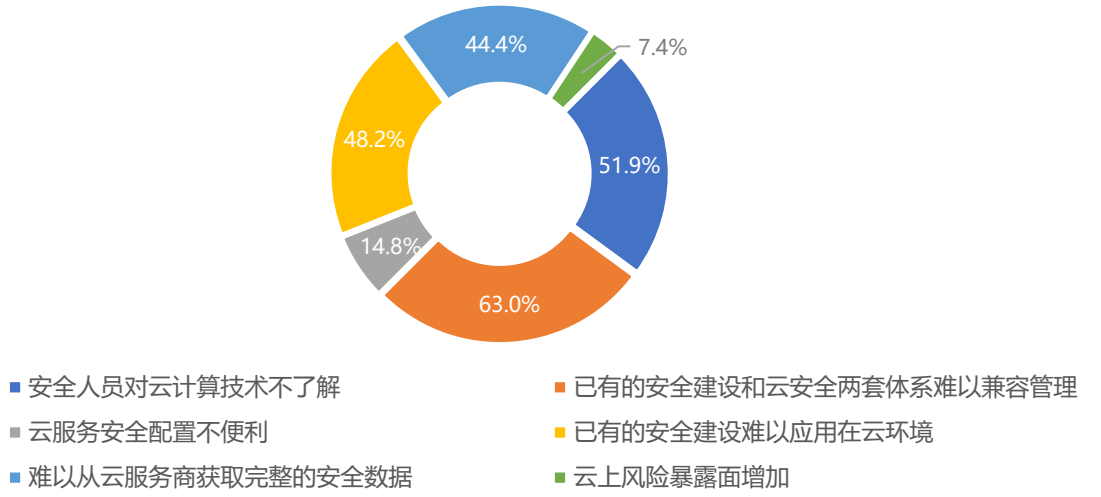
对云服务商的安全能力要求提高。为应对日益严峻的云安全风险，云服务客户对云服务商的安全能力提出了具体要求。**一是云服务商提供的安全功能完整性最受关注，**图 6 统计了云服务客户在采购云服务时对云服务商安全能力的关注度，70%的企业希望云服务商能够提供完备的安全功能，30%则期望有更多的安全选择。**二是云服务商数据保护能力至关重要，**数据要素价值不断提升，云服务客户对云服务商的数据保护水平提出了更高要求。不论是云平台运行数据还是云服务商内部数据，在采集、存储、传输、使用和销毁过程均应得到安全保障，其中 API（Application Programming Interface，应用程序编程接口）调用数据安全、个人信息保护等数据保护问题备受关注。**三是云上云下安全联动与风险透明化需求增加，**云平台建设过程中企业往往需要复用现有安全工具，或集成安全厂商的独立产品，云服务商应能够与安全厂商实现云上云下信息互通、风险透明，进一步提升云平台的安全可靠性。



来源：中国信通院

图 6 云服务客户对云服务商的安全能力关注度

安全顾虑影响企业上云意愿。如图 7 所示，多种安全因素降低企业上云的信心和意愿，可以总结为企业内部云环境和企业安全管理两个方面。**企业云平台建设方面，设备、平台、制度兼容性差。**上云转型需求迫切的企业普遍数字化程度较高，已经具备较为成熟的传统网络安全体系，企业业务向云平台迁移，必须面对已有安全建设在云环境中的适配问题。具体表现在云平台与已有安全设备和产品对接不通畅，集中式安全管理和云安全两套体系难兼容。**企业安全管理方面，人员、技术、消息协同性差。**企业上云后，云平台的运营维护至关重要，管理人员对云计算技术不了解、云安全意识不足导致的操作和配置不规范，使得风险暴露面增加。同时，企业与云服务商消息互通机制建立不完善，难以获取完整的安全数据，将影响企业安全评估和主动防御。



来源：中国信通院

图 7 云服务客户上云安全顾虑

（二）云服务客户应逐步提升云平台安全用云水平

云平台的安全性需要云服务供需双方共同维护，云服务客户用云的过程安全不容忽视，需安全合理的使用云服务，促进云上业务平稳运行。

建立安全组织架构，提升组织管理水平。企业应不断提升云的安全使用和运营能力成熟性，加强一体化管理水平。明确云平台使用规范，制定业务连续性计划、风险管理等方案。构建完善的组织管理架构，建立专门的云平台安全运营团队，负责日常监控、响应和改进工作。明确各部门、岗位的安全职责，确保安全责任落实到个人，并进行定期审查和考核。定期开展云安全意识教育和技能培训，提升云平台用户侧的安全威胁识别和应对能力。

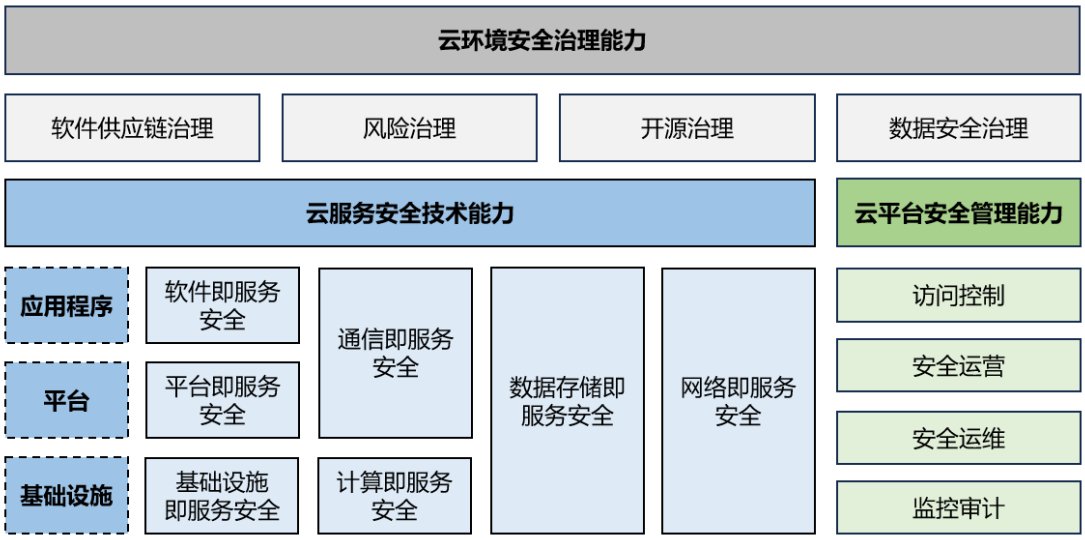
梳理云上资产配置，夯实安全基线。云服务客户应提升“用好云”的安全实践水平，任命相关安全管理和运营人员统筹管理云资产。安全人员基于云服务商提供的云服务安全功能，选择并安全配

置云平台，依据 CIS 安全基线和业务需求配置云上资产，安全高效利用云资源。

规范云平台使用过程，做好权限管理和事件响应。云服务客户应使用相关技术与工具确保云平台使用过程安全。实施严格的访问控制策略，如身份认证、权限管理、多因素认证等，确保只有授权用户可以访问敏感资源。同时与云服务商保持协同，在安全事件中及时响应并积极配合，提高双方协作效率。

（三）云服务商应落实云平台安全能力体系化和创新性

云服务商应积极响应云服务客户需求，补充能力缺口，融合新技术、新理念，建立覆盖技术、管理和综合治理的安全体系，如图 8 所示，筑牢安全顶层设计，确保云资源安全可信、云服务完整可用，提升云平台整体安全成熟性。



来源：中国信通院

图 8 云服务商安全能力框架

依托 ICT 新技术，保障云基础设施安全。云服务商应支持多种安全技术保障云服务的自身安全性，如支持微隔离能力、提供加密传输能力、具备数据灾备与恢复机制等。随着人工智能、算力网络等技术的深度发展，依托于高性能计算的新技术、新应用爆发式增长，为云计算安全带来了新的赋能方式。一是 AI 赋能现有安全技术，如结合大模型和威胁情报进行智能风险发现，实现自动化远程监控、识别安全风险、运营维护云平台。二是以算力网络为支撑试点新型安全技术，如引入云基础设施可信计算，确保执行计算任务的云资源逻辑组合不被篡改和破坏，实现硬件级安全和风险可溯源；算力资源联合底层通信网络，推广高性能隐私计算，深度保护云上数据安全。

实践安全管理新理念，维护云平台安全运行。云服务商应不断优化安全管理能力，以提升云平台自身安全性、可用性。一是建设基于零信任理念的安全管理体系，聚合身份安全、数据安全、网络环境安全、负载安全等安全数据，进行多源评估和统一策略管理，对基础资源、云服务、访问主体等进行综合评级，形成全平台零信任级别的安全管控。二是做好数据安全视角下的权限管理与审计。隐私驱动应用与数据解耦是优化和提高云平台安全韧性的关键手段，云平台应能够持续识别个人信息和敏感数据，做好独立的权限管理与审计，降低数据与基础设施的耦合度，助力数据要素的合法流通和合规利用。

引入安全治理新机制，打造云平台安全生态。云服务商应积极

探索组织内部与外部云环境安全治理措施，形成良好的安全生态。一是确定云安全治理目标，制定分场景、分阶段的安全能力提升计划，提出可落地的量化指标，如云平台安全功能成熟度分级、风险管理和灾难恢复计划，提升建设和治理云安全环境的科学性和积极性。二是引入开源治理和信息技术应用创新，编制企业级软件物料清单，提高软件供应链透明度，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。三是开展数据安全治理，实施精细化的数据分类分级、管理使用策略和安全评价机制，实现数据要素价值最大化。

三、云安全防护满足多样性安全需求

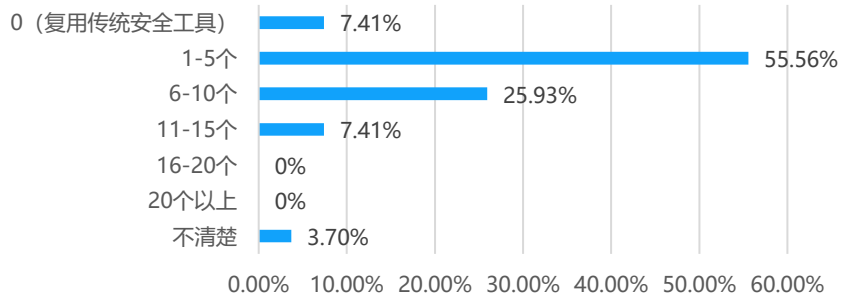
在维护云上业务安全的过程中，除利用云平台基础安全功能外，云服务客户可能还存在多种多样、增强的安全需求，需通过应用云安全工具或服务，开展持续的安全运营工作，构筑云安全防护体系。

（一）云上安全防护体系发展存在掣肘

在云安全防护的过程中，需要专业的人员使用相应工具，执行一系列良好的规范流程，通过安全运营维护云上业务安全。当前，云上安全防护工作在工具、人员、流程等方面仍存在诸多痛点。

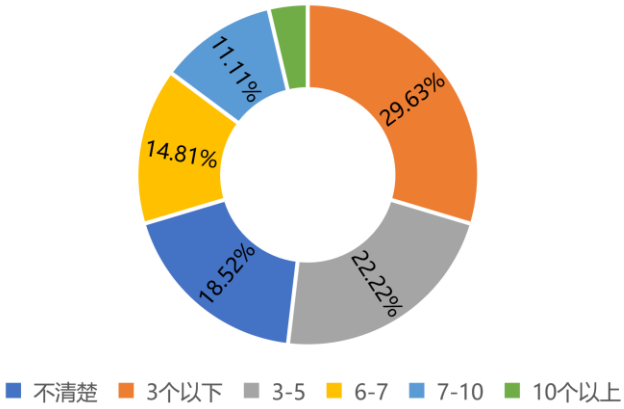
云安全工具方面，由于缺少理论与数据指导，在云安全工具的应用和研发中仍存在痛点问题。**一是用户侧安全工具应用尚存提升空间。一方面云上安全工具严重堆积。**根据调查显示，35%的组织具有超过6个云安全工具，在进行安全处理过程中，51%的组织需要

超过 3 个云安全平台进行联动处理，最多超过 10 个。**另一方面安全数据分析存在数据孤岛。**多个业务部门在使用不同云平台的过程中，部署的云安全工具与负责的监控人员可能不同，彼此割裂的局部数据分析难以察觉杀伤链离散威胁信号。**二是供应侧安全工具开发思路亟需纠正。一方面以新技术为驱动力开发的工具具有大量同质化功能。**在强调功能集成化的市场风气下，云安全厂商以新技术概念技术为基础研发推出的安全工具势必与已有工具产生功能重复。**另一方面不同云安全厂商间数据格式、接口不互通，全局安全分析存在壁垒。**云安全厂商通常会选择使用非通用的数据格式，降低接口兼容性，安全数据仅可以在同品牌供应商的工具体系中流通。根据调查显示，仅有 6.56%的云安全厂商认为自身产品可以覆盖用户需求，超 50%的用户接受 3 个以上云安全厂商的服务，在进行云安全防护体系建设过程中，势必面临不同供应商的安全数据无法流通的场景。



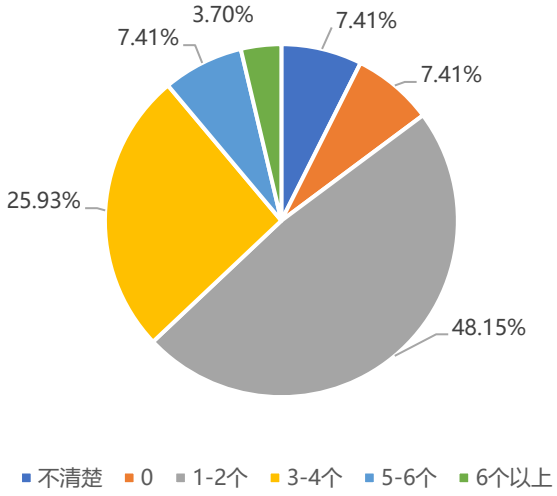
来源：中国信通院

图 9 云服务客户云安全工具数量



来源：中国信通院

图 10 常规云安全事件响应所需操作的工具数量



来源：中国信通院

图 11 进行云安全防护体系建设时使用的云安全厂商数量

云安全人员方面，由于云安全人才匮乏，安全团队的质量水平仍存在不足。**一是云安全团队规模有限，资深安全人员需要同时负责监控多个云安全工具。**根据统计数据显示，目前行业内拥有五年以上从业经验的人员仅有34.3%，超过30%的从业人员工作经验低于2 年[3]。云安全分析工作对从业者经验依赖极大，有限的资深从业者

[3] 工信部教育与考试中心、北京市海淀区互联网信息办公室、教育部高等学校网络空间安全专业教学指导委员会《2023 网络安全产业人才发展报告》

难以应付大量云安全工具带来的海量安全数据。**二是现有安全人才培养体系相对技术发展处于滞后状态。一方面传统行业对上云的认识与准备不充分，在适应新数字化环境中缺乏人才。**以工业设备MES（Manufacturing Execution System，制造执行系统）的上云为例，原本只擅长操作硬件的工作人员，在面对云端系统和电脑操作时显得力不从心。**另一方面教育体系更新换代速度较慢，相较于实际应用场景处于跟随状态。**在 AI 技术积极向各行业赋能的背景下，《2023 网络安全产业人才发展报告》显示仅有两成在校学生深入了解 AI 在网安领域的应用，三成左右的学校加入了 AI 方面的知识教学，未来网安行业对从业人员的需求将会向复合型人才转变。云安全团队将付出大量的时间成本学习新型工具的使用，无法第一时间发挥新型工具应有的能力。

云安全流程方面，由于云计算自身特点，传统流程体系无法充分适应云时代的安全需求，有待进一步完善。**一是云上威胁治理水平难以跟进项目扩张速度。**新项目为了抢占市场会尽可能压缩上线前的安全测试与防御部署流程。由于云上业务具备弹性扩展能力，云安全体系构建速度通常难以跟上云上业务扩张，因此业务可能会先于安全体系上线，形成安全隐患。**二是云安全事件处理流程缺乏便利渠道。**当发生云安全事件需要安全团队介入时，为了加快响应速度和减少所需的文书工作，业务团队与安全团队有时会倾向使用即时通讯手段跳过工单进行私下沟通。**三是云上攻防中防守方所处的不对称性被新兴技术进一步放大。**新兴技术武器化一方面提高了

攻击密度和复杂度，加大了攻击被检测到的难度；另一方面降低了发起攻击所需的时间与物资成本。

（二）云服务客户构建技术制度协同的安全运营体系

技术工具作为安全工作的基础决定了云服务客户安全能力的下限，积极应用人工智能技术可以极大程度上释放安全资源的价值，对抗面临的风险。

云安全数据分析与人工智能融合，提升安全工作效率和准确性。安全分析方面，将安全数据交由人工智能进行机器学习与分析，一方面解决了云计算暴露面过大带来的海量安全数据难以进行手动分析的问题，提高了安全数据的利用率，降低了人工分析可能带来的干扰；另一方面降低了数据分析环节对人工的依赖，将安全团队从重复的工作中解放出来投入更有价值的工作。同时算法模型可以通过安全数据进行调整与升级，不断提升应对新型威胁的能力。**安全处理方面**，人工智能通过对安全事件与威胁进行加权分析，以保障云上业务连续性为目标，对威胁进行综合定级。针对低危事件，自动联动安全组件根据编排剧本进行处理，达到即时响应；针对高危事件，将不同方案的处理效果与影响范围进行展示，交由安全团队验证并根据实际情况进行实施，有效的缩短响应窗口，将云上业务在安全处理中受到的影响降至最低。

安全运营制度规范作为安全工作的框架决定了用户安全能力的上限，合理规划组织内部各项制度规范可以从根本上降低人员过失带来的安全隐患。

对不同等级、不同岗位的人员组织针对性专项培训。面向领导层的云安全培训应从宏观视角出发，一是深入理解国家网络安全战略与政策，确保组织在网络安全方面的合规性；二是加深对云上风险与威胁的认识，了解组织当前的安全现状，端正对云上安全建设的态度；三是提升安全领导力，合理分配资源，积极自上而下推动云安全建设不断完善。面向安全团队的培训应以最新的云上威胁风向与实战对抗为主，了解攻防对抗技术与发展趋势，关注威胁风向预测攻击来源，以练代学从实战出发将理论与实际操作相结合提升实践经验。面向组织员工的培训除普及安全保密意识外，同样应该注重培养责任意识，将云安全责任从安全部门向外扩散，明确保护云安全人人有责。

将云安全防护视为长期战略目标，持续推进体系更替演化。云安全防护无法一蹴而就，是一个螺旋式上升的过程，因此需要不断对已有的云安全防护体系进行调整。**一是定期开展安全评估，根据自身安全态势与核心诉求调整资源投入方向，减少资源浪费。**云服务客户在进行安全防护建设的过程中应充分掌握自身现状，对安全建设目标进行优先级排序，将有限资源分配给适配自己当前需求的安全投资，而非一味追求先进的安全工具与技术手段。**二是将制度践行情况纳入考核指标，对人员和制度同时进行考察。**建立明确的流程管理，清晰定义各岗位角色在安全运营中的责任与义务，以流程文档的形式保证全部行为关键节点的可审可记录，避免事后溯源可能出现的责任不清与相互推诿。并且将流程执行情况以量化的形

式进行考核，一方面可以积极促进内部人员学习践行安全运营制度，另一方面也给后续的流程制度改进带来数据指导依据。

（三）云安全厂商多措并举精进发展策略

云安全厂商应积极探索适应新挑战的发展策略，以适应云安全市场格局、云服务客户需求、合规要求等外在环境变化，提升核心竞争力。

升级产品服务。匹配不同用户实际需求，提供分类、分级解决方案。在进行产品服务规划时，根据客户规模、行业、业务需求、信息化程度等维度灵活配置方案内容，从客户面临的实际风险出发，针对性进行产品开发，充分释放安全资源价值。**结合云安全产品与团队服务能力，推出面向云的网络安全服务。**梳理用户云安全防护新需求，促进传统安服转型升级，形成包含人员、技术和交付物在内的云计算安全服务解决方案，为用户提供 7*24 小时全生命周期的安全保障能力。

打造合作生态。避免一味追求“多且全”，发挥自身优势打造跨供应商的服务模式。提倡由综合型云安全厂商牵头、协同专精型云安全厂商构建合作互补生态，充分发挥各自优势，提供高质量的解决方案。**开放接口互通，提升兼容性，使安全组件间的数据流通成为可能。**通过关联来自不同安全组件、不同安全域的安全数据，提供孤岛破冰能力，以多维度对攻击进行溯源，合并同源或同类型的攻击告警，打破安全数据孤岛，提升云安全能力。

释放数据价值。一是打通跨行业情报交流渠道，摆脱技术不对

称，从高维视角出发，挖掘未来安全态势与攻击技术演变方向，博采众长，预测可能的威胁来源与演化方向，明确安全技术研发目标。**二是加强安全数据利用率，摆脱成本不对称**，将已知的全量攻击行为进行切片分析，明确攻击者的历史与常用入侵手段，用最直接、高效的解决方案阻断非法行为，有效节省资源的投入。

四、责任共担有效促进云安全体系运转

与传统数据中心相比，上云后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是必然选择。云服务商、云服务客户、云安全厂商等主体各司其职，协同开展安全工作，才能有效保证云安全体系的有效运转。

（一）规范指南不断完善，但行业意识和能力仍不足

近些年，产业多方积极编制标准、研究报告以促进云计算相关主体提升责任共担意识，但发展态势仍存在改善空间。

规范指南不断丰富，提升行业共识。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。《云安全责任共担模型》围绕上云用云的新场景、新风险，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，从云服务客户、云服务商和云安全厂商三大角色视角出发，围绕云服务、云软件、云软件+服务托管等模式给出责任共担实践参考。

行业客户责任共担意识和实践能力仍有提升空间。随着云计算产业不断发展，在政策标准引导下，各行业上云进程加快，但云服务客户对云安全责任共担的认知和实践能力仍不乐观，在调查中有45%的云服务客户不了解或不认可责任共担模式，52%的云服务客户与云服务商发生过责任纠纷。同时，随着各行业用云程度不断加深，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，但目前仅有1/3的受调查企业建立了企业内各部门间的责任划分机制。

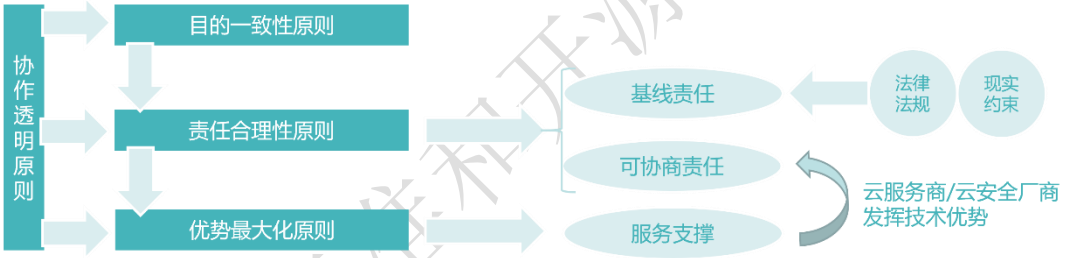
（二）三大举措夯实云安全责任共担机制

为夯实云安全责任共担机制，各主体应充分了解和理解责任共担机制的基本原则，信息互通，不断增强责任承担实践能力。本节概括总结了云安全责任共担机制的三大关键举措，因篇幅有限，具体实施细节可参考相关标准指南[4]。

明基线，以基本原则指导云安全责任主体各司其职。云安全责任共担涉及云服务客户、云服务商、云安全厂商等责任主体，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。在基本原则指引下，云安全责任共担既包含一定的基线——各主体应该承担，也存在一些弹性——协商一致后确定主体，具体原则包括：**一是目的一致性原则，**各主体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

[4] YD/T 4060-2022《云计算安全责任共担模型》标准
《云安全责任共担模型》研究报告

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。**二是责任合理性原则，**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。**三是优势最大化原则，**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，可以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。**四是协作透明原则，**各主体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，主体间应提升信任度，建立透明、及时的信息传递和联动响应机制。



来源：中国信通院

图 12 云安全责任共担基本原则

重协作，云安全责任主体应建立信息传递机制。一是云服务商和云服务客户之间的信息传递机制。云服务商应将用户信息处理情况、云服务等级协议、云平台安全举措、可能影响云服务客户云上业务的重大变更和安全情报信息等及时、透明的告知客户；云服务客户应及时获取云服务商告知的信息并采取应对举措，如更新漏洞补丁，同时在发现云平台存在缺陷风险时可及时告知云服务商并让其优化，以防影响自身云上业务。**二是云服务客户和云安全厂商之**

间的信息传递机制。云安全厂商应将用户信息处理情况、服务支持情况（尤其是远程服务的基本情况）、可能影响云服务客户的重大变更和安全情报信息等及时、透明的告知客户；云服务客户应及时获取云安全厂商告知的信息并采取应对举措，如接收到勒索情报时采取防勒索应急预案，同时在发现云安全工具存在缺陷风险时可及时告知云安全厂商，避免软件供应链安全事件的发生。**三是服务商生态圈的沟通协作。**以云为中心建立覆盖多个云服务商、云安全厂商等在内的生态圈，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。

理细节，按场景探索细粒度云安全责任共担实践。在云安全责任共担基本原则之下，不同业务场景、安全目标、现状能力等因素会影响主体间的责任划分，各主体承担的具体责任细节会存在差异。因此，各主体不仅应具备责任共担意识，更要注重责任共担经验的积累，将实践转化为知识，以知识指导日常云安全工作的开展。**一是面向重点场景识别责任清单**，如针对软件供应链安全、数据安全等云环境易面临的风险场景，明确各主体应承担的细粒度责任举措，当风险事件发生时能够迅速响应、发生后也可以准确定责。**二是借鉴行业案例，提前制定预案**，梳理云计算安全相关纠纷案例，分析纠纷原因、判决结果等情况，将案例中责任模糊环节与自身责任承担现状进行对比，针对相似的薄弱点补齐责任清单和相应能力，规

避同类风险事件的发生。

五、云安全趋势展望

结合对调查情况的分析，本章从技术理念、创新方式、产业供应、应用建设等维度对云安全发展趋势进行展望。

综合性云安全技术理念受到关注。云安全新理念、新技术不断涌现，企业盲目追求、应用过多的新技术，往往带来安全成效低、资源浪费等问题，能够缓解多方面安全风险的综合性云安全技术理念成为更多企业的选择：**一是零信任。**云计算打破了传统网络安全边界机制，东西向流量安全、远程访问安全等需求迫切。零信任秉持“持续验证，永不信任”的思想，能够指导身份安全、云工作负载安全、数据安全等多个维度的能力变革，是弥补边界安全局限性的关键举措。**二是 Web 应用程序与 API 保护（WAAP）。**微服务、DevOps 等云计算技术的应用促使 API 成为核心应用资产。而随着网络中 Bot 流量激增，应用面临频繁的刷单、恶意爬虫等威胁。WAAP 在传统的 Web 应用防护（WAF）基础上，整合 API 安全和 Bot 防护能力，更加满足云时代应用安全防护需求。**三是云原生应用保护平台（CNAPP）。**当前，云工作负载保护（CWPP）、基础设施即代码（IaC）等云原生应用安全能力相对孤立，企业开发人员体验差、风险响应效率低。CNAPP 通过整合各孤立能力，以保证跨开发和运行时的云原生应用安全。

自我突破和融合创新双向驱动云安全革新。一方面，**对云安全技术突破的期望度较高。**超四成受调查者认为，以提升云安全效能

为导向的技术创新是关键，同时还有四成受调查者认为通过理念创新指导现有技术重组也是未来发展的重要方向。另一方面，**“云安全+”的融合创新将为产业带来活力**。2023年至今，网络安全保险政策相继发布，作为 ICT 和金融的融合产物，是一种事后风险转移的有效手段。中国信通院牵头的“云安全及互联网平台运行安全”保险入选了工信部网络安全保险典型服务方案目录，未来在政策指引下，云安全保险将不断优化创新，迎来新的发展契机。

产业供应向服务化和协同联动升级。当前，我国云安全产业形成了覆盖负载安全、应用安全、安全服务等领域的完善产品供应体系，云服务客户在采购众多产品工具后面临安全运营人员不足、工具孤立未充分发挥作用等痛点。为了提升云服务客户侧安全工作的成效，**一方面服务赋能是关键，**依托供应侧安全专家能力实现持续的安全运营，三分之二受调查者认为云安全托管模式是未来的主要趋势。**另一方面产品工具应强化协同联动，**调查显示选择单一还是多个云安全厂商的比例接近，倾向性并不明显。无论哪种选择，协同联动都是提升产品工具服务质量的必然要求。对于选择单一厂商的企业，厂商自身工具的统一数据格式和联动优势是主要决策因素；对于选择多厂商的企业，在避免过度依赖的目标下，也更倾向使用可以跨厂商协作的产品工具。

企业安全建设需适应上云新趋势带来的挑战。近些年，各行业上云程度不断加深，企业安全建设的视角将随着上云态势的变化不断丰富。**一是应用 MaaS 等新型云服务的安全挑战。**人工智能算法模

型部署在云端，通过模型与计算资源结合催生出新型服务 MaaS（Model as a Service，模型即服务）。由于 MaaS 向公众暴露的接口日益增多，攻击者可以利用大模型生成侧技术实施攻击，如通过在提示词后增加一些不规则后缀，绕过大模型的拦截策略，从而生成预料之外的内容。**二是云远程连接场景激增的安全挑战。**扩展海外业务、采用外包服务团队等需求增加了云的远程连接频率。云远程连接的通信关系复杂，透明度不高，数据在传输过程中易遭受篡改、拦截或滥用等风险。

编制说明

本报告研究过程中获得了众多企业帮助，在此表示感谢：阿里云计算有限公司、华为云计算技术有限公司、腾讯云计算(北京)有限责任公司、中国电信集团有限公司、中国移动通信集团有限公司、中移（苏州）软件技术有限公司、联通数字科技有限公司、北京天融信网络安全技术有限公司、北京升鑫网络科技有限公司、奇安信网神信息技术(北京)股份有限公司、360 数字安全集团、北京启明星辰信息安全技术有限公司、新华三信息安全技术有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、江苏易安联网络技术有限公司、国网电商科技有限公司、上海安几科技有限公司、河南能睿科技有限公司、中国铁塔股份有限公司、北京山石网科信息技术有限公司、数篷科技(深圳)有限公司、深圳竹云科技股份有限公司

可信安全

CONTACT US

若您对本报告有任何建议，请与我们联系：
hanfei@caict.ac.cn