云计算安全白皮书

先进计算产业发展联盟

2023 年 12 月

版权声明

前言

随着云计算的快速发展，传统行业在数字化转型的推动下，将业务和应用迁移到云上，开启了新的工作模式。相对传统模式而言，云计算具备的分布式、按需使用、易扩展、可重用等特性可以解决传统企业运营中面临的信息孤岛、成本高、资源浪费、效率低等问题。在享受各类云服务带来便捷体验的同时，云上数据的安全性成为了客户聚焦的核心问题，频发的云安全事件更是引发了广泛担忧。因此，云平台及云上数据的安全性成为云服务提供商亟待解决的问题。

本白皮书重点介绍了云计算安全市场的发展现状、安全威胁和挑战、安全参考框架以及未来的发展趋势。白皮书首先梳理了全球以及国内云计算安全市场规模以及重要方向，分析了当前云安全行业的政策环境，然后总结了云计算发展中面临的威胁及主要挑战，并针对这些挑战提出云计算安全的参考框架，介绍了云计算安全防护架构以及安全防护技术，最后对未来云安全产业的发展趋势进行了展望和预测。

编制单位：先进计算产业发展联盟

参编单位：浪潮电子信息产业股份有限公司、济南浪潮数据技术有限公司、曙光云计算集团有限公司

参编人员：邹小蔚、刘雁鸣、曹柱、梁媛、亓开元、吴栋、袁东海、冯振、张晓辉、董青、韩华珊

目　录

图 目 录

表 目 录

一、云计算安全行业发展现状

（一）云计算安全市场规模及发展趋势

在全球范围，云计算作为新兴产业之一，其在降本增效、便捷性、灵活性和扩展性方面的优势无可比拟，同时还通过对其他行业的带动和改造，使得云计算拥有了广阔的市场和美好的前景，这使得世界各国都将云计算行业作为首要发展目标，然而云计算安全问题也因为云的特性被无限放大，这也是互联网时代面临的一大难题，如信息共享、不同系统间对接后出现的个人隐私、业务数据泄露，配置错误、设备故障或资源耗尽导致的服务中断，以及针对开放接口的网络攻击、勒索病毒等问题，以各类安全事件的形式进入公众的视野。

表 1 近年来发生的云安全事件

序号	事件时间	云服务	事件内容	原因
1	2017.3.22	青云 QingCloud	用户业务及控制台无法访问	北京 2 区机房电力故障引发部分网关设备及计算节点重启
2	2018.6.27	阿里云	阿里云官网的部分管控功能，及 MQ、NAS、OSS 等产品的部分功能出现访问异常	上线自动化运维新功能时出现操作失误
3	2018.8.5	腾讯云	“前沿数控技术新媒体”公司存储在腾讯云上的数据无可挽回地全部丢失	因所在物理硬盘固件版本 bug 导致的静默错误影响，文件系统元数据损坏
4	2019.4.3	优刻得 UCloud	北京二地域外网虚拟网关（UVER）某集群发生转发异常	灰度集群的配置文件被错误推送到某个业务集群上，预定的回滚措施没能正常运

				行，导致转发异常
5	2020.3.3	微软 Azure	微软位于美国东部数据中心发生了 6 个小时的服务中断,从而导致美国北部的一些客户无法使用 Azure 云服务	微软称这次故障应归咎于冷却系统故障
6	2020.3.26	谷歌云	谷歌云宕机长达 14 小时，多个云服务无法访问	基础设施组件问题
7	2020.4.10	华为云	华为云出现大面积宕机，登录、管理后台无法访问，本次宕机持续约三小时	有消息称这次宕机主要是由于北京的机房出现故障导致的
8	2020.6.2	苹果 iCloud	苹果 iCloud 云存储服务宕机,导致一些用户无法顺利登录 iCloud 账户，无法访问 Web 应用程序和 iCloud 邮箱等其他产品，基于 iCloud 平台的 Apple pay 等服务的运行也不正常	不详
9	2020.6.9	IBM Cloud	IBM Cloud 发生长达四个小时的中断故障,导致多项托管于平台上的互联网服务中断，其中就包括知名科技新闻聚合网站 Techmeme	IBM 网站解释到，INM 网络运营团队调整了路由策略，处理了第三方提供商引入的问题，这次故障也得以解决
10	2020.8.10	多家云服务器	Muhstik 僵尸网络大肆攻击国内云服务器,有数千台服务器失陷	境外 IP 及部分国内 IP 针对国内云服务器发起的攻击，攻击者通过 SSH（22 端口）暴破登录服务器，然后

				执行恶意命令下载Muhstik僵尸网络木马，组建僵尸网络并控制失陷服务器执行SSH横向移动、下载门罗币挖矿木马和接受远程指令发起DDoS攻击
11	2021.12.7	亚马逊云	亚马逊云宕机长达两小时,关联的一些网站和服务瘫痪	不详
12	2021.12.11	Kronos私有云	云人力资源管理公司Kronos遭到勒索软件攻击,据Kronos声称，攻击者访问了Kronos私有云（KPC）云环境，并在部署勒索软件之前窃取了许多企业客户的员工数据信息	不详
13	2022.1.11	亚马逊AWS	美国数字化调度平台FlexBooker遭遇数据泄露,威胁分子闯入其AWS（亚马逊网络服务）服务器后，370万用户的敏感信息外泄	调查发现，该公司使用AWS S3存储桶来存储数据，但并未实施任何安全措施
14	2022.3.20	微软Azure	Lapsus$黑客组织入侵了微软的Azure DevOps服务器，窃取了37GB的数据，这些数据主要是微软各个内部项目的源代码,包括必应、必应地图和Cortana。黑客随后在其Telegram	利用微软内部一名员工获得对源码存储库有限访问权限

			频道上泄露了被盗数据	
15	2022.3.21	亚马逊 AWS	由于配置错误的 AWS S3 存储桶，土耳其飞马航空公司（Pegasus Airlines）泄露了约 6.5 TB 的数据，包括敏感的航班数据、源代码和机组人员的个人信息	包含飞马航空公司电子飞行包（EFB）信息的 AWS S3 存储桶没有口令保护
16	2022.6.30	阿里云	黑客从上海警方数据库窃取了超过 10 亿中国公民的数据，并企图向上海市公安局勒索约 20 万美元	攻击者从中国电子商务巨头阿里巴巴的子公司阿里云托管的一个数据库中窃取了数据 调查显示，数据库本身是安全的，但管理仪表板可以从开放的互联网随意访问
17	2022.9.24	微软 Azure	网络安全供应商 SOCRadar 向微软通报了一次重大数据泄露事件，声称属于 100 多个国家的 65000 多家公司的 2.4TB 微软客户数据被泄露。这起数据泄露事件被称为“BlueBleed”	Azure Blob Storage 存储桶配置错误
18	2023.5.12	丰田 Toyota Connected Corporation（TC）	日本丰田汽车公司 12 日承认，由于云服务平台设置错误，其日本车主数据库在近 10 年间“门户大开”，约 215 万日本用户的车辆数据蒙受泄露风险	该云环境中的设置错误是由于系统性质被设置为“公共”而非“私人”的人为错误设置导致的

表格数据来源：根据公开信息整理

云安全事件一旦发生，就会对企业造成不可挽回的巨大损失，为避免此类事件再次发生，越来越多的客户在挑选云服务商时将安全和稳定放在第一位，也因此催生出一大批提供云计算安全产品和服务的公司，有传统的安全厂商对其产品进行云化升级，以支持多租户、虚拟化等应用场景，如奇安信、深信服、安恒、绿盟、天融信、趋势科技等公司；也有新诞生的基于互联网基因的云安全公司，能够定制更加符合云环境的安全产品，如青藤云、云安宝等。除了直接面向最终客户销售云安全产品和服务的方式，行业内领先的云服务提供商如亚马逊、微软、谷歌、阿里云、华为云等公司，也通过与上述安全厂商合作的方式打造云安全生态，为云上客户直接提供可定制的云安全服务。随着各类云安全需求的涌现，加上国家战略和政策面的激励，企业加快了人才招聘和培养的进度，云安全也出现了很多细分领域，整个行业呈现出了高速的发展态势。

根据市场调研机构的数据显示，2020 年到 2022 年间全球云安全市场规模呈逐年递增趋势，2023 年受到俄乌冲突事件以及全球经济下滑趋势的影响增速有所放缓，预计全年规模将达到 131.5 亿美元。其中，公有云安全市场规模将达到 75.8 亿美元，占比 57.7%；私有云安全市场规模将达到 37.9 亿美元，占比 28.8%；混合云安全市场规模将达到 17.8 亿美元，占比 13.5%。预计 2024 年开始市场增长加速，到 2025 年全球云安全市场规模将有望超过 190 亿美元。

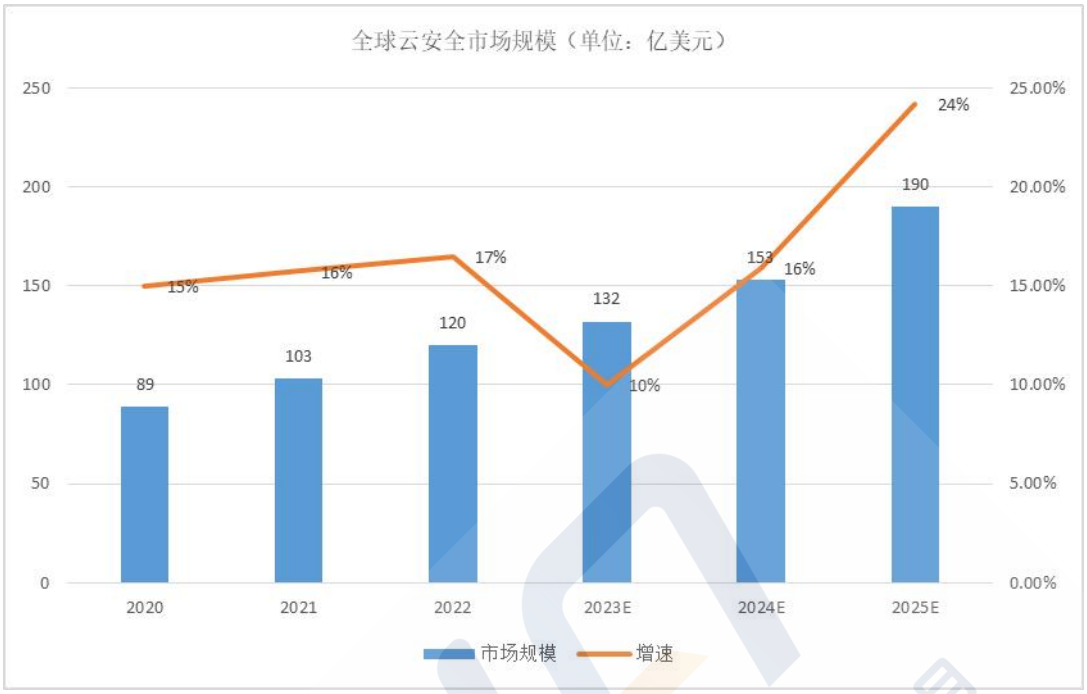

图 1 全球云计算安全市场规模增长情况

图片来源：公开资料整理

中国在全球云安全市场中占据重要地位，受益于政策和各方需求的推动，为我国云安全市场发展提供了良好的契机。2020 年以来，中国云安全市场规模呈现出快速增长的态势，2022 年在国家“东数西算”工程全面推进的战略驱动下，中国云安全市场规模达 181 亿元左右，同比增长约 47%，预计到 2025 年中国云安全市场规模将突破 470 亿元大关。

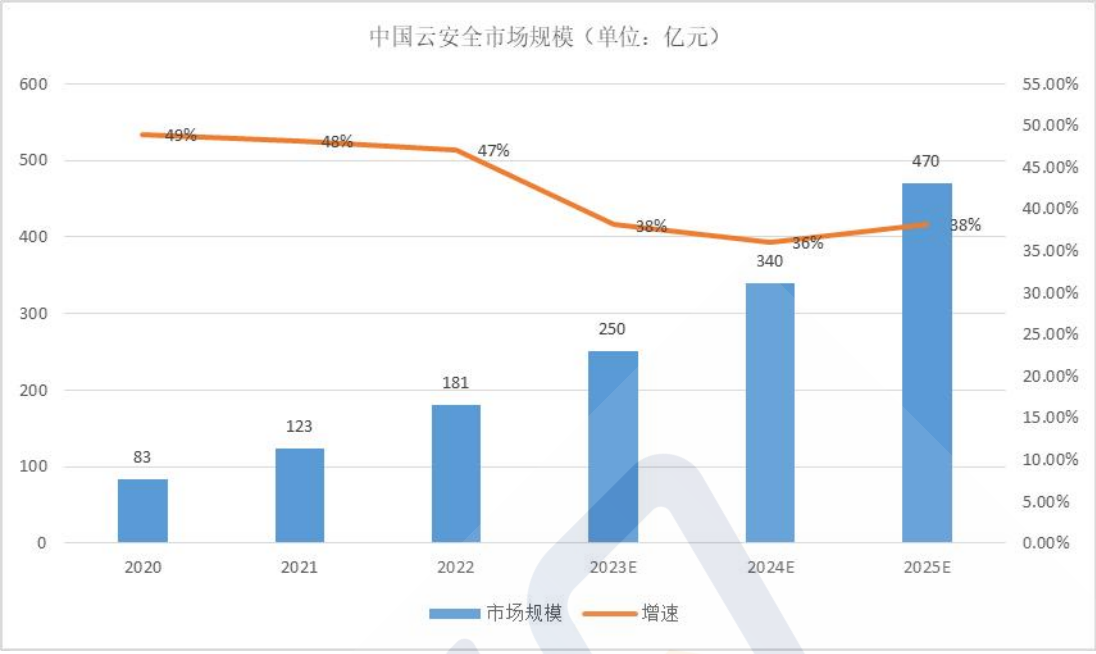

图 2 中国云计算安全市场规模增长情况

图片来源：公开资料整理

根据最新调查数据显示，2023 年中国云安全服务市场份额占比排名前三的分别是：数据加密服务（82.4%）、防火墙服务（76.8%）和身份认证服务（71.2%），其次为安全监测服务（65.6%）和安全审计服务（59.2%）。

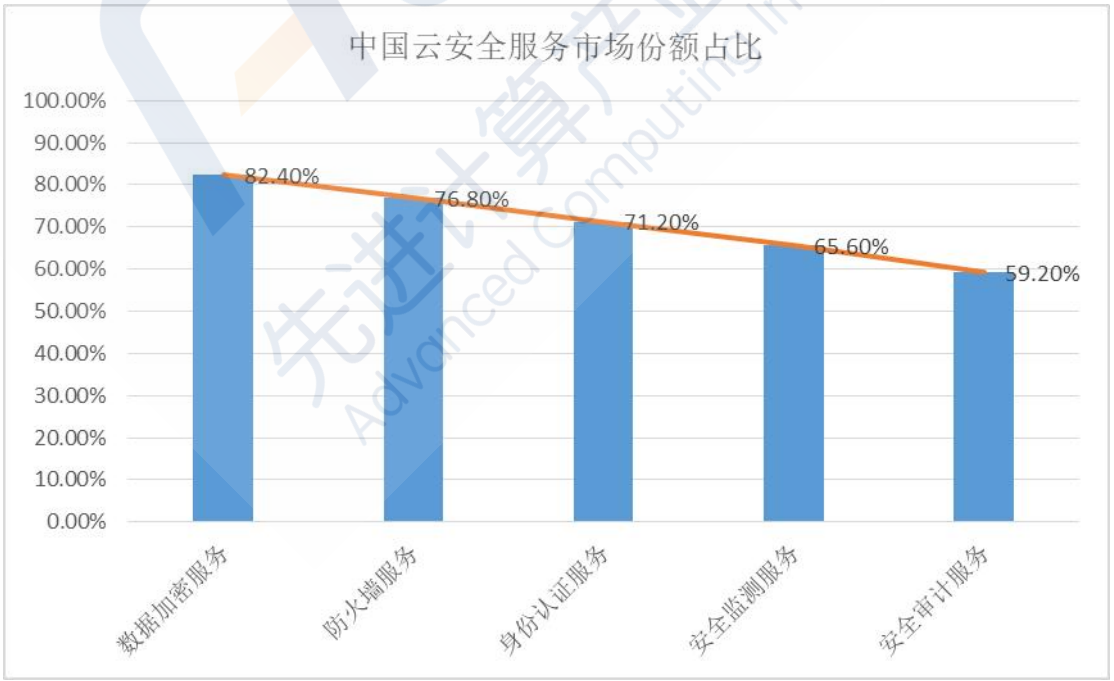

图 3 中国云安全服务市场份额占比

图片来源：公开资料整理

（二）云计算安全政策形势分析

中国政府高度重视云计算和云安全的发展，出台了一系列相关的法律法规，如《网络安全法》、《个人信息保护法》、《数据安全法》、《关键信息基础设施安全保护条例》等，以规范云计算行业的行为和责任，保护用户的数据和隐私。为指导具体工作的开展，国家多个部门都出台过云计算安全相关的政策文件。

2012 年 05 月，科技部发布《中国云科技发展“十二五”专项规划》时提出总体目标：到“十二五”末期，在云计算的重大设备、核心软件、支撑平台等方面突破一批关键技术，形成自主可控的云计算系统解决方案、技术体系和标准规范，引领云计算产业的深入发展。其中提到云安全相关的保障问题：“制定适应不同行业需要的云计算安全要求和评测方法标准，保障云服务的网络和信息安全。”

2015 年 01 月，国务院发布《关于促进云计算创新发展培育信息产业新业态的意见》，提出到 2017 年，云计算在重点领域的应用得到深化，产业链条基本健全，初步形成安全保障有力，服务创新、技术创新和管理创新协同推进的云计算发展格局，带动相关产业快速发展。其中格外提到——安全保障要基本健全，这是对于云安全相关概念的相对明确的定位：“初步建立适应云计算发展需求的信息安全监管制度和标准规范体系，云计算安全关键技术产品的产业化水平和网络安全防护能力明显提升，云计算发展环境更加安全可靠。”

2017 年 01 月，工信部印发《云计算发展三年行动计划（2017-2019

年）》，结合现有基础以及面临的问题和挑战，拟从提升技术水平、增强产业能力、推动行业应用、保障网络安全、营造产业环境等多个方面推动云计算健康快速发展。其中，对于保障网络安全方面，制定完善相关安全管理制度侧，具体提出要加大公有云服务定级备案、安全评估等工作力度，逐步建立云安全评估认证体系，推动云计算安全服务产业发展。支持企业和第三方机构创新云安全服务模式，推动建设基于云计算和大数据的网络安全态势感知预警平台，实现对各类安全事件的及时发现和有效处置。这是政策层面首次明确提出云上安全体系化建设。

2019 年 07 月，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部四部门联合印发了《云计算服务安全评估办法》，旨在提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，降低采购使用云计算服务带来的网络安全风险，增强党政机关、关键信息基础设施运营者将业务及数据向云服务平台迁移的信心。云计算服务安全评估面向云服务商，主要参照国家标准《云计算服务安全能力要求》、《云计算服务安全指南》，从系统开发与供应链安全、系统与通信保护、访问控制、配置管理、维护、应急响应与灾备、审计、风险评估与持续监控、安全组织与人员、物理与环境安全等方面提出要求。

2021 年 12 月，中央网络安全和信息化委员会印发《“十四五”国家信息化规划》，围绕确定的发展目标，部署了 10 项重大任务中，第四项培育先进安全的数字产业体系，培育壮大人工智能、大数据、区块链、云计算、网络安全等新兴数字产业。

2023 年 09 月，在中央网信办网络安全协调局的指导下，由中国网络安全审查技术与认证中心主办的“国家网络安全宣传周”云计算服务安全分论坛起草并组织 8 家云服务厂商签署了《云计算服务安全自律公约》。《公约》要求云服务厂商严格遵守国家云计算安全政策标准，积极申报云计算服务安全评估，自觉接受政府部门安全监管和社会监督，积极推动行业自律，以高水平安全保障高质量发展。

回顾云计算的发展史，总共经历了四个阶段：市场引入阶段（2007-2010）、成长阶段（2011-2015）、成熟阶段（2015-2017）、高速增长阶段（2017 至今）。在各个阶段中，除了有国家政策的加持，行业标准也起到了至关重要的作用，引导着云计算行业往规范和成熟的方向发展，这里梳理了国内外机构参加制订的云安全相关标准文件。

表 2 云安全相关标准文件

序号	机构名称	机构简介	发布标准
1	ISO/IEC JTC1	1987 年国际标准化组织（ISO）与国际电工委员会（IEC）联合组建了第一联合技术委员会JTC1，JTC1 是在原 ISO/TC97（信息技术委员会）、IEC/TC47/SC47B(微处理机分委员会)和IEC/TC83（信息技术设备)的基础上组建而成，负责 IT 领域的国际化标准。	• ISO/IEC 27017:2015《基于 ISO/IEC 27002 的云计算服务的信息安全控制措施实用规则》 • ISO/IEC 27018:2019《个人可识别信息（PII）处理者在公有云中保护 PII 的实践指南》 • ISO/IEC 27036-4:2016《供应商关系的信息安全—第四部分：云服务安全指南 • ISO/IEC 27009《ISO/IEC 27001 在特定行业/服务的认可的第三方认证中的使用和应用》 • ISO/IEC 17788:2014

			《信息技术 云计算 概述和词汇》 • ISO/IEC 17789:2014《信息技术 云计算 参考架构》 • ISO/IEC 17203:2017《开放虚拟机格式》 • 《云计算安全与隐私管理系统》
2	ITU-T	国际电信联盟（ITU）是联合国负责信息通信技术（ICT）事务的专门机构，成立于1865年，下设三个部门：ITU-R（无线电通信）、ITU-T（电信标准化）、ITU-D（电信发展）。	• 《云计算安全框架》 • 《云计算身份管理要求》 • 《云计算基础设施要求》 • 《电信领域云计算安全指南》
3	NIST	美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）直属美国商务部，从事物理、生物和工程方面的基础和应用研究，以及测量技术和测试方法方面的研究，提供标准、标准参考数据及有关服务。	• SP 500-292《云计算参考体系架构》 • SP 500-293《美国政府云计算技术路线图》 • SP 800-144《公有云中的安全和隐私指南》
4	ENISA	ENISA（The European Network and Information Security Agency）成立于2004年，总部设在希腊的伊拉克利翁。目的是提高欧洲网络与信息安全。	• 《云计算--信息安全保障框架》 • 《云计算--信息安全的好处，风险和建议》
5	TheOpenGroup	开放式组织联盟是厂家中立、技术中立的工业联盟，旨在开放标准和全球互操作性的基础上，实现企业内部和企业之间的无边界的信息技术交流。	• 《云安全和SOA参考架构》

		成员包括Oracle、IBM、HP等知名企业和政府机构 。	
6	CSA	云安全联盟（Cloud Security Alliance，CSA)成立于2009年4月，属于非盈利性组织，目标是推广云安全最佳实践和云安全培训。	• 《云计算顶级安全威胁》 • 《云计算关键领域安全指南》 • 《云控制矩阵》
7	OASIS	结构化信息标准促进组织（Organization for the Advancement of Structured Information Standards，OASIS）成立于1993年，是一个推进电子商务标准的发展、融合与采纳的非盈利性国际化组织。	• 《身份在云中的使用》
8	DMTF	分布式管理任务组成立于1992年，目的是联合整个IT行业协同开发、验证和推广系统管理标准，帮助全世界范围内简化管理，降低IT管理成本。	• 《云管理体系结构》
9	CCSA	中国通信标准化协会于2002年12月18日在北京正式成立，是国内企、事业单位自愿联合组织起来，经业务主管部门批准，国家社团登记管理机关登记，开展通信技术领域标准化活动的非营利性法人社会团体。	• 《移动环境下云计算安全技术研究》 • 《电信业务云安全需求和框架》
10	TC260	全国信息安全标准化技术委员会（简称信安标委，TC260）于2002年4月15日在北京正式成立。委员会是在信息安全	• GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》 • GB/T 28448-2019 《信息安全技术 网络安全等级

		技术专业领域内，从事信息安全标准化工作的技术工作组织。	保护测评要求》 • GB/T 31167-2023 《信息安全技术 云计算服务安全指南》 • GB/T 31168-2023 《信息安全技术 云计算服务安全能力要求》 • GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》
11	公安部第三研究所	公安部第三研究所创建于1978年，是公安部直属科研单位。	• 《网络安全等级保护2.0-云计算安全扩展要求》
12	云计算开源产业联盟（OSCAR）	云计算开源产业联盟（OSCAR）是由工业和信息化部信息化和软件服务业司指导，中国信息通信研究院联合多家云计算开源技术公司发起，中国通信标准化协会代管的，专注于云计算市场的开源产业联盟。云计算开源产业联盟担负了促进云计算开源技术和产品在中国的发展的使命，致力于培育中国云计算开源产业生态，引领行业最佳实践及制定产品评估标准，支撑政府政策制定。	• Q/KXY ZW021 《信息技术应用创新 政务云平台技术要求》 • Q/KXY ZW005 《政务云安全能力要求》

表格数据来源：根据公开信息整理

二、云计算安全威胁和挑战

（一）云计算面临的安全威胁

云计算面临的安全威胁可以从问题根源，即内因和外因两个方面来分析。内因通常是由于系统自身的健壮性不够、人为原因、管理和安全措施不到位等因素引起，如安全机制缺陷、虚拟化隔离失败、补丁升级

不及时、错误的操作和配置、缺少系统资源和网络的监控、缺乏数据安全管理机制与能力、未启用审计功能等；外因主要是接入互联网后面临的传统安全威胁，如信息泄露和篡改、恶意代码、各类 Web 攻击（如 DDoS 攻击、SQL 注入、XSS、CSRF、0-Day 等）、APT 攻击、黑客攻击等。

根据 Cybersecurity Insiders 安全社区发布的《2023 云安全报告》调查数据，76%的受访者极其或者非常担心云安全，24%的受访者报告称在过去 12 个月内经历过与公有云相关的安全事件。在受访者提到的云安全威胁中，云平台配置错误或设置错误排名最高，为 59%；随后依次为敏感数据泄露（51%）、不安全的接口/API（51%）和未经授权的访问（49%）。

（二）云计算七大安全挑战

除了以上威胁，云计算还面临着以下安全挑战：

- **风险集中：**云计算将数据集中在云端，容易成为黑客的攻击目标而遭受集中攻击，一旦发生事故，对整个系统影响重大。
- **定位困难：**云计算系统涉及组件众多，设计相对复杂，发生故障时想要快速精确的定位问题存在一定难度。
- **边界模糊：**云计算因使用虚拟化和分布式技术，边界变得更加模糊，传统的物理边界防护方式已经不再适用，需要使用更灵活和精细的防护措施。
- **未知风险：**云计算数据流动场景复杂，数据的访问方式多种多样，造成数据安全的风险难以有效识别，开放性带来风险的不确定性。
- **闭环缺失：**云计算安全体系建设随已跟随业务上云进程发展数年，

但大量安全设施分布分散，覆盖千差万别，缺乏较好的闭环管理能力。

- **开放风险：**云计算具有开放性的特点，对外提供大量 RESTful 接口，接口的安全性将对整个系统的安全性带来一些新的挑战。

- **取证困难：**云计算应用具有地域性弱、信息流动性大的特点，各地的安全政策不尽相同，在信息安全监管、隐私保护等方面可能存在法律风险。

三、云计算安全参考框架

（一）总体建设思路

云计算安全架构建设时，应将《网络安全法》、《密码法》、《数据安全法》等法律法规，《信息安全技术 网络安全等级保护基本要求》、《信息安全技术 云计算服务安全能力要求》等云计算安全标准作为指导依据；以云计算平台及云计算平台租户业务系统为保护对象；以控制云计算平台及云计算平台租户业务系统面临的安全风险为建设目标。从物理安全、安全技术、安全管理、安全运维等方面构筑云计算平台的总体安全体系架构。

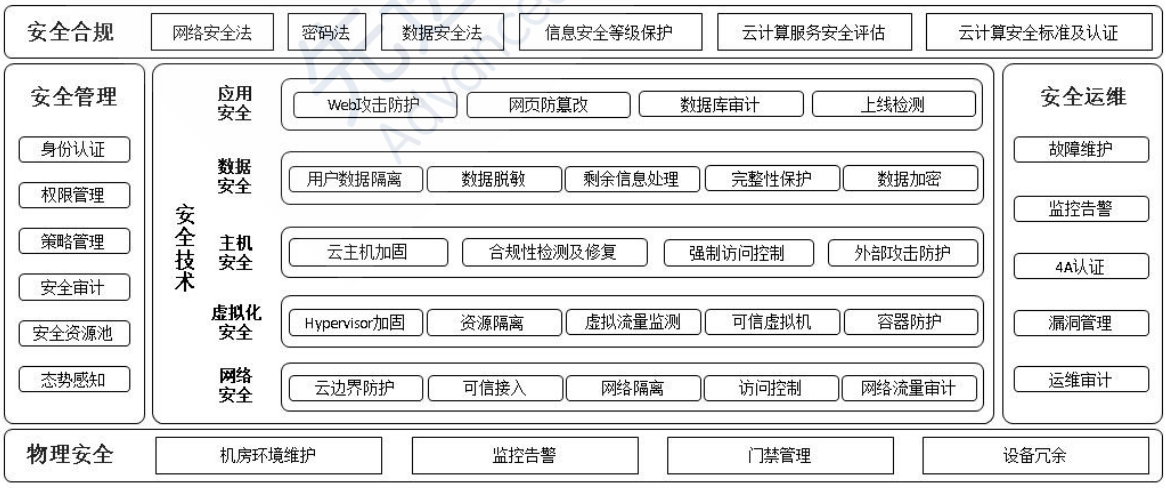

图 4 云计算安全架构

图片来源：根据公开资料整理

物理安全主要关注数据中心设施的安全，包括机房温度、电源、散热、防火、防盗等方面的防护，设备的冗余配置，以及配备的门禁系统和监控系统，以确保云平台稳定运行。

安全技术包含网络安全、虚拟化安全、主机安全、数据安全和应用安全五个方面。其中，网络安全包含云边界安全防护、可信接入、网络平面和租户网络的隔离、基于安全组的访问控制、网络流量审计等内容；虚拟化安全通过内核安全加固、虚拟资源隔离、虚拟流量监测、可信度量以及容器安全防护等手段实现；主机安全包含云主机加固、合规性检查、强制访问控制以及外部攻击防护等内容；数据安全贯穿云平台的整个生命周期，包含用户数据隔离、敏感数据保护、剩余信息保护、机密性 完整性保护等内容；应用安全包含 Web 应用防护、安全迁移、数据库审计、漏洞扫描等内容，提供面向租户的安全服务，保障租户应用和数据的安全。

安全管理包括用户身份鉴别和权限管理、安全策略管理、安全日志审计、安全资源池管理以及安全态势感知等内容，实现面向多租户的安全管理和安全可视化。

安全运维包括系统维护、监控告警、堡垒机、漏洞管理、运维审计等内容，覆盖了云平台运维整体流程。

（二）物理安全

GB50174-2017《电子信息系统机房设计规范》从数据中心的使用性

质和数据丢失或网络中断在经济或社会上造成的损失或影响程度，将数据中心划分为 A、B、C 三级：A 级为“容错”系统，可靠性和可用性等级最高；B 级为“冗余”系统，可靠性和可用性等级居中；C 级为满足基本需要，可靠性和可用性等级最低。A、B、C 三级具体要求如下表所示。

表 3 机房等级划分

标准项	A 级	B 级	C 级
定级标准	1 电子信息系统运行中断将造成重大的经济损失; 2 电子信息系统运行中断将造成公共场所秩序严重混乱。	1 电子信息系统运行中断将造成较大的经济损失; 2 电子信息系统运行中断将造成公共场所秩序混乱。	不属于 A 级或 B 级的数据中心应为 C 级。
选址	距离停车场不应小于 20m，距离铁路或高速公路的距离不应小于 800m,距离地铁的距离不宜小于 100m，在飞机航道范围内建设数据中心距离飞机场不宜小于 8000m	距离停车场不应小于 10m，距离铁路或高速公路的距离不应小于 100m，距离地铁的距离不宜小于 80m,在飞机航道范围内建设数据中心距离飞机场不宜小于 1600m	
机房专用空调	N+X 冗余	N+1 冗余	N
采用不间断电源系统供电的设备	空调末端风机、控制系统、末端冷冻水泵	控制系统	
变压器	2N	N+1	N
后备柴油发电机	（N+X）冗余	N+1	
UPS	2N 或 M（N+1）(M=2、3、4……)或一路(N+1) UPS 和一路市电供电	N+1	N
UPS 电池后备时间	15min	7min	无

表格数据来源：根据公开信息整理

数据中心等级最主要的衡量标准是由于基础设施故障造成网络信息

中断或重要数据丢失在经济和社会上造成的损失或影响程度。云计算主要机房用于承载关系民生的关键业务，所用机房应为 A、B 类标准机房。

基础设施及现场机房环境维护

机房现场日常维护时间：7×24×365。机房所提供的基础设施维护内容包括：对机房专有的配电系统、空调系统、消防系统、漏水检测系统及安防系统的日常巡检及保养维护。

建立积极有效的监控管理机制，通过场地与环境集中监控系统对相关设备系统进行监控和记录，及时处理发现的故障和隐患，以保障所提供的机房的基础设施和机房环境的稳定与正常。

供配电系统维护

机房维护人员负责机房所配备的冗余变压器、高压及低压配电系统、后备柴油发电机、UPS 的日常巡检与维护，定期巡检、记录机房配电系统的运行情况，发现问题及时处理。

空调系统

定时检查机房的环境温湿度，确保机房始终处于在 23℃±2℃之间、湿度在 55％±15％之间的恒湿、恒温状态。

定期记录空调系统运行情况，发现问题及时处理。

消防系统

定期巡检，记录消防系统的运行情况，定期组织进行消防培训和演练。

声光报警

对机房的 UPS、温度、电源等重要环境设施集中监控，并实现声光报警。

国密门禁与监控系统

为了响应 GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》对国家商用密码应用的要求，对于云平台的物理和环境安全，采取覆盖云平台机房的国密门禁系统和视频监控系统双策略。

部署国密门禁系统，采用对称密钥分散和对称加解密技术，实现一卡一密，确保人员身份的真实性。采用 HMAC-SM3 或 SM2 数字签名技术，对门禁系统人员进出记录做完整性保护，防止进出记录被篡改。

部署国密视频监控系统，支持视频录像的完整性保护，防止录像文件被篡改。视频监控系统包含支持密码模块的 IPC 网络摄像机、NVR 网络录像机、视频客户端。采用 HMAC-SM3 技术，实现实时视频流和视频录像的完整性保护。

门禁系统和视频监控系统均为独立闭环网络，通过交换机实现前后端的互联互通，不允许任何外部网络或设备接入。

（三）云计算安全技术

1、网络安全

云计算平台网络安全技术包括云边界防护、可信接入、网络隔离、访问控制以及网络流量审计。

云边界防护

在云平台边界网络环境中，对进出的流量进行安全检查和控制，以

确保云平台网络内外部的数据传输安全。主要包括边界防火墙、入侵防御系统、网络防病毒等技术手段，防止恶意攻击、病毒、恶意软件等威胁进入网络，云计算平台和用户数据不被泄露、篡改或窃取。为保证云计算平台网络边界安全，通常需要在网络边界部署 NGFW 下一代防火墙、IPS 入侵防御系统、AV 网络防病毒系统、流量控制系统等。 NGFW 下一代防火墙支持访问控制、静态的包过滤和动态包过滤等攻击防范能力；IPS 入侵防御系统通过实时、被动漏洞技术，实时发现网络环境的安全缺陷，对攻击流量进行阻断；AV 网络防病毒系统可检测网络传输中携带的病毒文件，并对非法流量进行阻断；流量控制系统可以监控网络流量、分析流量行为、设置流量管理策略。

可信接入

通过部署 VPN 或零信任设备，以通信链路加密的方式实现网络安全接入，包括身份认证（访问事前控制）、终端访问及数据传输（访问事中检查）安全、权限和应用访问审计（访问事后追查）、链路可用性保障。零信任设备同样具备安全防护、身份认证、数据加密、访问控制和实时监控等能力。

网络隔离

云平台建设时，将网络根据其承载的业务划分为不同网络，如管理网络、业务网络、存储网络等。默认情况下，不同网络之间不可相互访问，通过网络平面的隔离，确保管理流量不受用户业务流量的影响，以增强云平台管理操作的安全性。不同用户间的网络通过 VPC 技术进行逻

辑隔离，VPC 是建立在物理网络结构之上的虚拟网络，在 VPC 内部，用户可以自定义 IP 地址范围、网段、路由表和网关等，从而形成一个按需定制的虚拟网络环境，并与所有其它虚拟网络隔离，这种隔离确保用户虚拟机中的网络流量数据不能被其他虚拟机访问。

访问控制

云平台通过安全组对云主机的网络流量进行过滤，保护云主机通信安全。安全组是一种虚拟防火墙，包含一组访问控制策略，称为安全组规则，规则包含容许/拒绝访问云主机的 IP、端口等，支持设置入口和出口流量方向。对云主机有较高的安全要求时，可在安全组内定义多种规则，设置放行的 IP 和协议（如 TCP/UDP/ICMP/SSH/HTTP 等），定义哪些流量可以进入云主机内部，对云主机实现更细粒度的安全访问控制。

网络流量审计

网络流量审计通过对网络数据的采集、分析、识别，实时动态监测通信内容、网络行为和网络流量，发现和捕获各种敏感信息、违规行为，实时报警响应，全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析、评估及安全。

2、虚拟化安全

虚拟化环境相比于传统 IT 架构，系统密度大大增加。虚拟化主机间隔离水平较物理主机有所下降，为病毒木马传播和横向攻击降低了难度，一旦虚拟化环境中单台虚拟主机失陷，整个虚拟化环境都有可能面临被攻破的威胁。为此，需要针对虚拟化层部署有效的安全措施。

虚拟化加固主要通过在 Hypervisor（虚拟机监视器）层嵌入安全模块，实时监控 Hypervisor 层安全状态，保护核心数据的完整性，实现对 Hypervisor 层关键资源从内核层进行安全防护，防止黑客、恶意攻击人员对虚拟化层攻击，确保云平台安全可靠。

虚拟化资源隔离包括云计算平台内嵌的基础隔离机制和自动化隔离规则。云计算平台内嵌的基础隔离机制主要包括租户资源隔离、租户网络隔离；自动化隔离规则是指云计算平台针对同平台不同租户的外部网络地址配置自动化、默认的隔离规则，避免不同租户间的横向访问。

通过对虚拟主机之间的网络流量和数据进行收集、分析、检测，并针对异常流量进行阻断和告警，可帮助运维人员快速识别故障点和瓶颈，定位问题并采取补救措施，在发生攻击事件时可及时避免攻击链的蔓延和横向传播。

虚拟化平台层的安全防御构建的基础是可信计算能力。可信计算基于可信服务器和可信中间件，来构建可信赖的云数据中心基础环境，隔离可信计算资源和不可信计算资源，保证租户对底层平台安全的可见性，以及敏感数据/虚拟机仅运行在可信计算资源中，并采用自动化调度和扩展，无需管理员和租户干预。

容器可以看作是一种特殊的虚拟化，目前容器已广泛应用于各类云计算平台，尤其是云原生方向，因此容器的安全也不容忽视。容器的安全主要包括镜像安全扫描、镜像完整性保护以及安全上下文（Security Context）。容器镜像安全扫描通过使用 clair 等容器镜像扫描工具进行

安全漏洞扫描，防止存在恶意漏洞的镜像运行；容器镜像完整性保护通过哈希算法生成镜像的摘要值，并使用签名者的私钥加密镜像摘要值生成签名文件，签名文件一般随镜像一起上传。镜像签名验证时使用签名者的公钥解密签名文件得到镜像摘要值，并再次生成镜像的摘要值，将其与解密得到的摘要值进行对比，如相同则表明镜像未被篡改；容器安全上下文配置包括是否以特权模式运行、文件系统读写权限、运行容器进程的用户/用户组、Linux 强制访问控制和限制系统调用权限等。通过合理设置容器安全上下文，授予容器工作负载需要的最小权限，保证云平台自身的安全性。

3、主机安全

云租户在将业务系统托付给云平台后，最为关心的是云主机上数据的安全和隐私，云平台应保证云主机不被破坏，保证云主机内的数据不被破坏和泄漏。

云主机安全加固遵循安全最小化原则，关闭操作系统中未使用的服务组件和端口，仅授予管理员最小的权限集合；定期通过漏洞扫描发现主机中存在的安全漏洞，并实现识别、分析、响应、修复、验证的全流程闭环处理；通过白名单、完整性检测等方式实现关键组件的保护，实现对攻击的免疫；基于等保等合规要求制订安全基线，对主机操作系统、中间件、数据库等对象进行扫描，覆盖账号配置、口令配置、登录配置、SSL 配置等功能项，并提供自动化修复功能；在操作系统内核实现安全标记等强制访问控制机制，对系统关键目录、文件、注册表、进程、服

务等进行强制访问控制；提供主机防火墙功能，可针对主机实施点对点的访问控制，集成的非法网络外联检测功能可及时发现违规互联网接入；提供入侵检测功能，尤其是针对云主机的逃逸行为以及篡改行为进行检测，对入侵事件进行审计和告警，并根据设置自动阻断或使用其他响应方式；提供恶意代码防范能力，通过特征库比对的方式识别云主机中存在的恶意代码，对包含恶意代码的文件进行分类和隔离处理，为后续的人工研判提供依据。

4、数据安全

数据安全首先重点关注数据流转和访问对象，通过梳理业务流程和重要数据资产，识别重点保护对象。然后，对数据访问关键场景各个环节的数据安全风险进行识别，开展数据安全维度的风险分析，暴露关键业务场景中的数据安全风险问题。最后，提供有效的数据安全技术，包括数据隔离、数据脱敏、剩余信息保护、完整性保护、数据加密等多方面的能力。

用户数据隔离

支持用户针对重要数据按不同级别进行标记，以此来控制主体对客体的访问权限。每个用户仅能访问自己的数据及他人共享和授权的数据，比如用户创建的虚拟机、存储在设备和磁盘上的数据，其他用户未经授权不可随意访问。

数据脱敏

数据脱敏对敏感数据进行去标识化、匿名化处理，例如：固定值替

换、置空、乱序、统计特征保留等。其中数据溯源算法多样，需要支持伪行伪列、脱敏水印、内容修改水印等隐蔽性强、不易绕开的算法。脱敏算法可在不改变现有业务逻辑的前提下，保证脱敏后的数据保留原有业务逻辑特征，同时保证数据的有效性和可用性，使脱敏后的数据可以安全地应用于测试、开发、分析等不同应用场景。

剩余信息处理

云计算具有多租户和资源复用的特点，用户可根据需要随时申请和释放资源，同一主机上可能存在多个用户的资源，如果释放存储资源时没有及时清理用户剩余数据而随后又分配给其他用户，可能导致用户数据的泄露，带来严重的安全隐患。云平台应支持用户身份鉴别信息和敏感数据的存储空间被释放或重新分配前进行完全清除，通过写随机数和多次擦写的方式，保证用户数据不可以任何技术手段进行恢复。

完整性保护

采用数字签名技术保证数据来源的真实性以及数据的完整性。常见的如针对虚拟机镜像、快照和容器镜像生成数字签名后进行存储。在虚拟化场景下，云平台内跨主机迁移虚拟机时，为了防止虚拟机的数据在迁移过程中被篡改，需要对关键数据进行数字签名以保证传输过程中数据的完整性。

数据加密

云平台中的重要数据（如账号、密码、密钥、证书、License、授权凭据、重要业务数据、个人数据等）在传输和存储前需要通过安全加密

算法（如 AES256、SHA-256、SHA384、RSA-3072、ECDSA384 或 SM 国密算法等）进行加密，以避免产生数据泄露。云平台应为用户提供数据加密和密钥管理能力，并提供加密算法选择与强度分级等能力，保障用户数据的机密性。

5、应用安全

云上应用，以面向公众或特定群体访问的应用服务为主，对安全的要求相对较高。云平台通过集成 Web 防火墙、网页防篡改、数据库审计、应用上线检测等安全服务，以提升云上用户业务系统安全能力。Web 防火墙对 Web 攻击（如 DDoS、SQL 注入、XSS、CSRF、WebShell、中间人等）、恶意机器人扫描、非法访问、会话劫持等行为进行防御，通过旁路镜像主动防御、特征识别、算法识别、智能语义分析、智能封禁等技术手段，有效阻挡面向 Web 站点的各类攻击；网页防篡改对 Web 站点目录提供全方位的保护，防止黑客、病毒等对目录中的网页、电子文档、图片、数据库等任何类型的文件进行非法篡改和破坏；数据库审计服务记录关键行为日志，能够起到溯源和取证的作用；上线检测对即将上线发布的应用进行全面安全检查和评估，以规避潜在的安全配置风险。

（四）云计算安全管理

云安全管理系统为管理员提供用户身份安全策略、安全审计、安全产品管理、态势感知等功能。系统提供身份认证、密码复杂度、会话锁定、黑白名单等安全策略的配置以及安全事件的集中审计；系统实现对云防火墙、云杀毒、云主机加固、云数据库审计、云堡垒机等产品的统

一管理，并基于多个安全产品构建安全资源池，为云租户提供可定制的安全能力；系统提供态势感知等高级功能，聚合来自网络攻击、流量统计、病毒检测、云主机安全、应用识别、风险漏洞评估等安全大数据，构建安全地图，为云计算环境提供动态、整体地、多点联动地安全风险展现能力，大大提升了云计算平台的安全检测、威胁识别、风险分析甚至是安全预测的能力。

（五）云计算安全运维

云平台的运维工作，可能涉及到云服务商、云租户、云应用开发商、云第三方运维人员等。按照管理原则，可将以上角色分为两类：一是云服务商，负责云平台的正常运转；二是云上用户，包括云租户、云应用开发商、云第三方运维人员等，负责云上用户业务的正常运行。针对两类角色，需制定不同的云运维安全策略。

针对云服务商

针对云服务商，需搭建一个独立与业务的运维管理区，专门用于云平台安全运维工作。允许逻辑隔离的业务区域（即非涉密业务分区）共用一个运维管理区，需物理隔离的业务区域（即不同的涉密业务分区）需单独建设运维管理区。运维管理区负责对应业务区域的网络、安全、云计算平台管理。

运维管理区内提供运维堡垒机（运维审计）、设备监控、备份管理、漏洞扫描、网络审计、日志审计等功能。运维管理员必须通过运维堡垒机访问云平台实现运维操作：运维管理员首先登录堡垒机，并建立安全

加密的数据通道，再通过堡垒机发起到系统资源的运维访问。通过对设备监控、备份管理、漏洞扫描、网络审计、日志审计等功能的利用，实现云运维安全保障。

针对重要、敏感的云计算业务分区，运维管理区宜配置账号安全管控系统，以保证账号的安全性。

针对云上用户

云上用户主要是对托管的业务和服务进行运维管理。云上用户应使用云服务商提供的运维审计功能，以保证云上用户的运维操作被记录以便审计，包括使用运维平台和工具的时间、目标对象、命令记录、结果等信息，审计信息应至少保存六个月。建议支持对运维全过程的监控和录像功能，以避免运维过程黑盒存在的不确定性风险，以及出现问题后可以通过视频回放的方式进行根因回溯。

针对云上用户的运维审计功能，应使用独立于云服务商的运维堡垒机，可使用独立硬件设备或云安全资源池内的运维堡垒机功能模块。

针对重要、敏感的云上业务系统运维，云上用户宜使用云服务商提供的数据安全保护能力，包括数据库保护能力、数据脱敏能力等。

四、云计算安全发展趋势

（一）数据安全体系建设的需求

国家实施的“大数据战略”，实现了数据作为与土地、劳动力、资本沟通的要素市场。数据要素化，也将进一步促进数据的流通与共享。同时也带来了一些新的挑战，数据安全对经济影响生死攸关。由于政务数据的敏感性，如果政务数据被恶意分析利用，将会威胁到国家安全及公民合法权益，如黑客对政务站点的恶意攻击、不法分子窃取个人敏感信息，导致大规模泄露等。数据安全体系不同于传统的云安全体系，不再是独立模块的简单堆砌，而需要体系化、综合化地考虑建设方案。通过建设数据安全管理体系、数据安全技术体系、数据安全运营体系，满足数据安全立体化保障的需求。

（二）提高可用性和安全性之间的平衡

随着企业数字化转型和业务上云的持续推进，越来越多的用户转为在云上在线办公，需要通过以不同的方式访问云平台，为保证云上关键数据的安全，云平台通常会启用繁琐的验证流程或设置严苛的安全策略，这样会造成用户体验不佳，甚至有部分用户宁可选择牺牲安全性的代价来提高可用性，但事实证明一旦发生安全事故所付出的成本是非常惨重的。因此，在严格的安全协议和用户可用性之间找到最佳平衡点至关重要。比如在身份认证方面，可以考虑多使用生物识别技术，如面部识别、视网膜和指纹扫描，既能够保证安全认证的强度，又能简化用户的登录操作，以及使用 AI 技术来分析和预测用户的行为，而不是使用规则匹配

和策略管制的方式。这样，更容易达到可用性和安全性两者的平衡。

（三）零信任架构的应用

零信任模型是一种新的安全模型，这种模型颠覆了固有的安全边界的概念，即认为不存在绝对可信的内部网络，对所有的访问都应进行合法性的验证。零信任模型可以帮助组织更好地保护其数据和应用程序。它将每个访问尝试都视为潜在的风险，从而缩小了攻击面，防止威胁在网络中横向移动。近年来，零信任模型虽受到广泛关注，但因为零信任会带来现有架构的重大变更，并且对系统的稳定性和可用性影响未得到验证，各方还是持谨慎态度，随着相关技术的发展成熟，相信在未来零信任模型将得到更多应用。

（四）人工智能在云安全中的扩展作用

云平台每天需要处理海量的数据，传统的安全产品在功能和分析效率上都明显存在短板，需要通过多种安全产品的互补来完成威胁的分析和识别，并且还会存在遗漏的情况，而人工智能在提供正确数据的情况下，可以比人和普通软件更快、更准确地预测到潜在的安全威胁。并能够做出自动响应，向安全团队发送安全预警，从而避免安全事件的发生。机器学习算法还可以根据历史数据对平台安全性进行评估，促使平台部署更安全的防护措施。总的来说，人工智能技术可以帮助组织更好地保护其云环境，并提高其安全性和效率。

（五）基于云原生的安全技术兴起

根据百度百科的定义：云原生（Cloud Native）指的是基于分布部

署和统一运管的分布式云，以容器、微服务、DevOps 等技术为基础建立的一套云技术产品体系。简单来说，“云原生”顾名思义，就是“生在云上、长在云上”，就是利用原生的云化的能力来帮助开发者去提效，比如让应用程序可以更快开发上线、持续迭代和交付，为开发者提供一些开箱即用的能力如服务治理、DevOps 等。云原生安全以安全左移和运行时安全保障为核心理念，以 DevOps 流程为中心，构建整体安全体系，覆盖云原生的整个生命周期。未来，云原生安全将得到更多关注，相应技术将更加全面和成熟，并涵盖云原生技术栈的所有方面。

（六）安全合规方案的自动化

近年来云上数据泄漏事件增多，监管环境也变得更加严格，预计将来会陆续出台更为严格的监管法规，企业在安全合规方面的负担将加重。因此，将会产生自动化合规性解决方案的需求，以帮助企业应对监管合规性的挑战。这些解决方案可以自动化进行合规性检查和报告，减少人工错误和减轻企业的合规负担，简化合规性管理流程，并确保企业掌握最新的监管政策变化。随着时间的推移，自动化合规性解决方案将变得越来越重要。

（七）保护不断扩大的物联网生态系统

随着网络带宽的大幅提升和硬件设备的智能化改造，让“万物互联”的构想在未来能够成为现实，随着大量的设备接入到互联网，组成开放的物联网，使得攻击者有机会通过网络访问物联网中的设备。为了应对物联网设备面临的安全威胁，需要在云平台开发保护物联网的安全技术，

例如物联网设备的接入控制和标识技术、加密技术、基于区块链的身份验证技术等。总的来说，随着物联网设备的普及，保护物联网生态系统的安全性变得越来越重要，相应的安全技术将在未来得到更广泛的应用，以确保物联网设备的安全性和可靠性。

（八）基于 eBPF“零侵入”技术兴起

传统主机安全方案采用内核模块技术，内核模块可以实现高级别控制和丰富的功能，但代码编写不当的内核模块可能导致内核崩溃或引入安全漏洞。eBPF（extended Berkeley Packet Filter）技术提供了一种安全、可编程的方式来扩展内核功能，eBPF 程序在内核中运行时会受到严格的安全限制，因此不会对系统的稳定性和安全性产生直接影响，可以实现深度的系统观测能力和自定义扩展能力。近年来，eBPF 技术逐渐应用在安全领域，例如：基于 eBPF-LSM 技术的内核运行时安全方案 KRSI（Kernel Runtime Security Instrumentation）、云原生运行时防护方案等等，并且随着云计算和容器化技术的不断发展，eBPF 将会在安全领域应用场景中得到广泛应用。

（九）超融合架构实现软硬一体式安全

超融合（HCI）指的是一种将计算、存储、网络和虚拟化等多种技术集成于一体的 IT 基础架构，通过将服务器硬件、虚拟化管理软件以及分布式存储软件相结合，可达到简化部署和管理、提升性能和可靠性、易于扩展和维护、降低成本和资源消耗等目的。例如浪潮云海超融合产品 InCloud Rail，通过“硬件重构+软件定义”方式，使用服务器虚拟化软

件+带存储功能的服务器，使用分布式存储替代传统存储，并通过打通容器和虚拟机的资源池与管理调度逻辑，实现虚拟机+容器的一体化管理运维，具备云原生一体化、双站点备份容灾、多云管理、终端安全防护等多重能力。

超融合具有软硬一体的产品形态，需要兼顾两者，但不是单独考虑软件和硬件的安全再做加法，未来更多的是将软硬件当成一个整体，除了做好基础安全防护，还会站在业务的角度，从软件定义和协同管理层面评估系统的安全性和健壮性，对身份鉴别、权限管理、软硬件调度和资源管理等重要接口进行测试和加固。另外，超融合具有数据集中的特点，为避免发生数据泄露和恶意篡改事件，各厂商会加大对数据保护和安全合规方面的投入，包括在超融合产品中加入 HSM 以提升数据加密能力，以及设计研发数据保护相关的安全特性，并将其作为卖点。

（十）围绕“一云多芯”构筑整体安全方案

为了应对芯片领域的技术封锁和出口管制，国家大力发展芯片产业，截止目前，国内主流芯片架构已覆盖 x86(Intel/海光/兆芯)、ARM（FT/鲲鹏）、Alpha（申威）、MIPS(龙芯)、 LoongArch(龙芯)。在未来，多 CPU、多芯片共存是个长期趋势，为了处理好多芯共存、协同管理等问题，“一云多芯”技术应运而生。

所谓“一云多芯”，指的是使用一套云平台管理不同芯片架构的计算资源，实现异构资源的统一管理和调度，并通过云平台屏蔽底层架构差异，为用户提供体验一致的云计算服务。实际应用就是云平台基于统一

代码构建，覆盖主流芯片架构，并实现不同架构的识别、协同部署和管理，如浪潮云海“一云多芯”方案，使用基于 OpenStack 开源框架的云海 OS 平台，全面支持 Intel X86、海光、龙芯、飞腾、鲲鹏、申威等芯片架构的服务器，支持同一套源代码在不同 CPU 架构硬件上部署，统一资源调度，从而实现应用部署与服务器 CPU 路线的选择无关，并强化同指令体系下的迁移能力，在方案层完善跨架构迁移能力。

“一云多芯”是云和芯的融合，是平台+生态的协同。首先，随着技术的不断演进和迭代，硬件、云以及应用等产业链将实现上下游的共同协同，自顶向下，构建大生态，并通过各种组织和联盟来推进生态的建设以及提升供应链的安全；其次，随着基于云原生、人工智能的安全技术的发展，未来有更多高级安全特性可应用于软硬协同以及芯片安全领域；最后，云平台将充分发挥在“一云多芯”中的纽带作用，借助各类芯片提供的能力(如机密计算),配合云平台安全服务或第三方安全产品，保障不同架构切换时应用和数据的安全性。在标准和测评方面，目前信通院“可信云一云多芯测评体系”为业界第一个“一云多芯”标准体系，云平台通过《一云多芯技术能力要求》并达到先进级要求可获得信通院颁发的证书。在未来，将陆续发布更多“一云多芯”相关安全标准和规范，并建立起完善的认证流程和体系，以引导“一云多芯”技术更规范和快速的发展。

附录 1：术语表

表 4 术语表

序号	中文名称	英文名称	定义
1	云计算	Cloud Computing	通过网络访问可扩展的、灵活的物理或虚拟共享资源池的模式，资源可按需自助获取和管理。
2	公有云	Public Cloud	公有云,又称为共有云,指的是一种由第三方云服务提供商管理的云计算服务,该服务向公众开放。
3	私有云	Private Cloud	私有云是一种基于云计算技术的云服务模式,由企业或组织自己搭建和管理,用于提供计算资源和服务。
4	混合云	Hybrid Cloud	混合云由一个或多个公有云和私有云环境组合而成。
5	虚拟化	Virtualization	虚拟化,是指通过虚拟化技术将一台计算机虚拟为多台逻辑计算机。
6	多租户	Multi Tenancy/Tenant	多租户是一种软件架构，单个产品实例（SaaS）为多个用户提供服务，用户可按需购买使用产品资源，用户数据相互隔离。
7	东数西算	East Data and West Computing	即东数西算工程，指通过构建数据中心、云计算、大数据一体化的新型算力网络体系，将东部算力需求有序引导到西部，优化数据中心建设布局，促进东西部协同联动。
8	零信任	Zero Trust	零信任代表了新一代的网络安全防护理念，默认不信任企业网络内外的任何人、设备和系统，基于身份认证和授权重新构建访问控制的信任基础，从

			而确保身份可信、设备可信、应用可信和链路可信。
9	人工智能	Artificial Intelligence	人工智能是一种模拟人类智能的技术，它可以通过计算机程序模拟人类的思维和行为，实现自主学习、推理、判断和决策等功能。
10	云原生	Cloud Native	云原生是一种基于云计算的软件开发和部署方法论,它强调将应用程序和服务设计为云环境下的原生应用,以实现高可用性、可扩展性和灵活性。
11	物联网	Internet of Things	物联网是一个基于互联网、传统电信网等信息承载体，让所有能够被独立寻址的普通物理对象实现互联互通的网络。
12	超融合	Hyperconverged Infrastructure	超融合基础架构（Hyperconverged Infrastructure，HCI）是一种整合了计算、存储和网络功能的服务器架构。
13	虚拟机监视器	Hypervisor	一种运行在物理服务器和操作系统之间的中间层软件,可以允许多个操作系统和应用共享一套基础物理硬件
14	一云多芯	One Cloud, Multiple Cores	“一云多芯”是指使用一套云平台管理不同芯片架构的计算资源，实现异构资源的统一管理和调度，并通过云平台屏蔽底层架构差异，为用户提供体验一致的云计算服务。

表格数据来源：根据公开信息整理

附录 2：缩略语表

表 5 缩略语表

序号	英文缩写	英文名称	中文名称
1	MQ	Message Queue	消息队列
2	NAS	Network Attached Storage	网络附属存储
3	OSS	Object Storage Service	对象存储服务
4	SSH	Secure Shell	安全外壳协议
5	DDoS	Distributed Denial of Service	分布式拒绝服务攻击
6	AWS	Amazon Web Services	亚马逊网络服务
7	SQL	Structured Query Language	结构化查询语言
8	XSS	Cross Site Scripting	跨站脚本攻击
9	CSRF	Cross Site Request Forgery	跨站请求伪造
10	APT	Advanced Persistent Threat	高级持续性威胁
11	API	Application Program Interface	应用程序接口
12	UPS	Uninterruptible Power Supply	不间断电源
13	IPC	IP Camera	网络摄像机
14	NVR	Network Video Recorder	网络视频录像机
15	NGFW	Next Generation Firewall	下一代防火墙
16	IPS	Intrusion Prevention System	入侵防御系统
17	AV	Anti-Virus	防病毒

18	VPN	Virtual Private Network	虚拟专用网络
19	VPC	Virtual Private Cloud	虚拟专有云
20	IP	Internet Protocol	互联网协议
21	TCP	Transmission Control Protocol	传输控制协议
22	UDP	User Datagram Protocol	用户数据报协议
23	ICMP	Internet Control Message Protocol	Internet 控制报文协议
24	SSL	Secure Socket Layer	安全套接层
25	HTTP	Hypertext Transfer Protocol	超文本传输协议
26	IT	Information Technology	信息技术
27	HCI	Hyperconverged Infrastructure	超融合
28	eBPF	extended Berkeley Packet Filter	可扩展伯克利数据包过滤器
29	LSM	Linux Security Module	Linux 安全模块
30	KRSI	Kernel Runtime Security Instrumentation	内核运行时安全方案
31	HCM	Hardware Security Module	硬件安全模块
32	OS	Operating System	操作系统
33	DevOps	Development & Operation	开发和运维

表格数据来源：根据公开信息整理

附录 3：参考文献

【1】云计算安全白皮书(2018 年).云计算开源产业联盟,2018.8

【2】2023 年云安全行业现状与挑战.尚普咨询集团,2023.6.12

【3】全球及中国云安全行业分析报告.北京研精毕智信息咨询有限公司,2023.3.27

【4】2023 云安全报告.Cybersecurity Insiders,2023.4

【5】Burak Cinar.云安全的未来：趋势和预测,2023.8.8

浪潮电子信息产业股份有限公司

地址：山东省济南市高新区草山岭南路 801 号 9 层东侧

邮编：250101

电话：0531-85106144

网址：https://www.ieisystem.com/