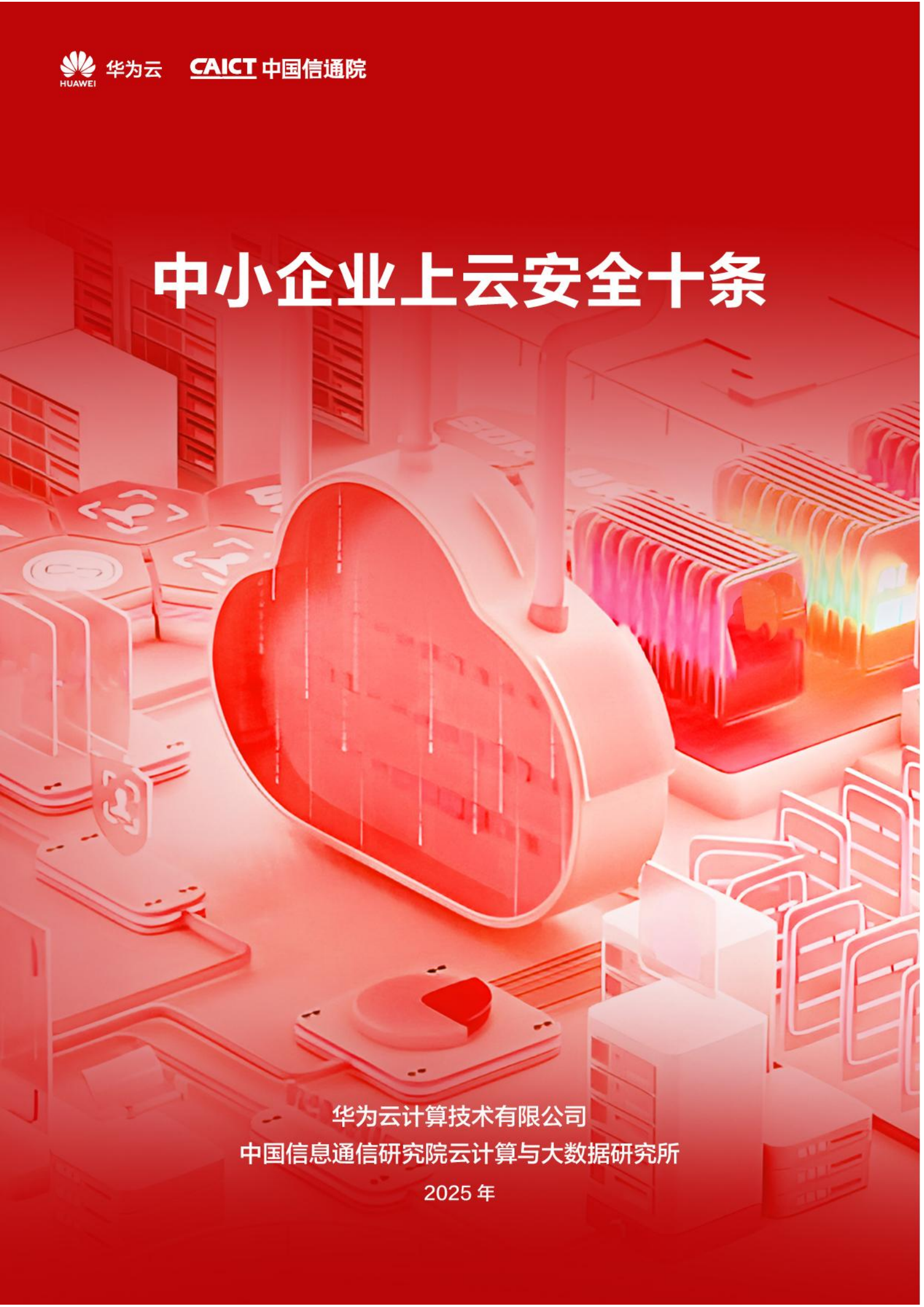
华为云 HUAWEI CAICT 中国信通院

中小企业上云安全十条



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

2025 年

版权声明

前言

在数字化转型浪潮中，上云已成为中小企业提升竞争力、实现业务创新的战略选择。在中小企业业务加速向云端迁移的背景下，中小企业如何应对上云安全挑战、筑牢持续运营的安全基石，成为亟待解决的关键议题。

在此背景下，为引导中小企业客户提升上云安全意识和安全防护能力，中国信息通信研究院与华为云计算技术有限公司联合开展了中小企业云上安全的相关调研，对中小企业云上安全现状进行分析。并基于中小企业的特质和上云安全的挑战和需求，评估分析形成中小企业上云十条风险与处置十条，旨在引导中小企业客户提升上云安全意识和安全防护能力。

本文首先分析了国内相关政策与中小企业自身原因的上云驱动因素，并对比中小企业与大型企业在安全建设中的差异。分析中小企业在组织架构、技术能力、链属角色等方面的特点，并探讨其对中小企业云上安全建设的优劣影响，梳理中小企业上云面临的十类安全风险与二十四项安全风险项，基于风险发生可能性、威胁演化严重性、防御措施落地难易程度三维度综合评估“中小企业上云安全风险关键十条”，依据十条风险，给出阶段性处置的策略，形成体系化的风险应对框架。最后对全文进行总结，并对中小企业上云安全配置给出实践指南。

编制人员

邹 丰、耿 涛

吴倩琳、王睿宁、吴诗浩、侯庆茹、孔 松、郭 雪、杨王颖

目录

图目录

表目录

第一章 中小企业积极向云拥抱

1.1 外驱内需双轮驱动中小企业上云

中小企业上云的驱动力主要来自两方面：一方面受政策推动，政府鼓励企业数字化转型，上云是重要路径；另一方面是自身发展的内在需求，上云能够助力中小企业实现业务拓展、降本增效，提升竞争力。

1.1.1 政策外驱助力中小企业上云

国家政策通过多种方式支持中小企业上云。2024 年 12 月，工业和信息化部、财政部、中国人民银行、金融监管总局四部门发布《中小企业数字化赋能专项行动方案（2025—2027 年）》，明确提出到 2027 年实现中小企业上云率突破 40%的目标。**一是在财政激励层面，该方案明确**支持地方探索“上云券”“算力券”等优惠政策措施，为中小企业上云用算提供支持。鼓励算力中心提供“随接随用、按需付费”的云端算力服务，降低中小企业用算成本。**二是技术赋能维度上，该方案**提出面向小微企业推广普惠性“上云用数赋智”服务，加快中小企业内外网升级改造，提升数字化基础水平等。**三是在试点示范方面，**国家以“百城”试点为核心，分批支持 100 个城市开展深度改造，细化《实施指南》并推广成功经验，形成可复制的“点线面”转型路径。

各地围绕中小企业上云需求，构建起“资金引导—平台赋能—生态协同”的立体化支持体系。一是在资金引导层面，多地通过补贴降

低企业上云门槛。四川省对数字化改造达标企业按不超过投入50%给予最高100万元补助，覆盖软件、云服务等支出；黑龙江省将试点城市不低于80%的支持资金用于企业数字化改造，直接补贴云服务购买、设备升级等环节；山东省统筹中央预算内资金与税收优惠政策，为中小企业“上云用数赋智”减轻成本压力，湖北省则对集群内创建智能工厂、数字化车间的企业给予奖励，引导其优先应用云制造服务。**二是在平台赋能方面，各地着力搭建技术载体。**河北省扩大上云供给资源池并制定产品目录，提供共享订单、集中采购等标准化云服务；江苏省鼓励平台企业开放共享云平台，推出低代码驱动工具降低开发门槛，促进企业间业务数据互通；四川省建设制造业赋能平台提供全流程改造服务；湖北省在特色产业集群部署工业软件平台，推动企业共享云端资源；山东省优化算力枢纽布局，为中小企业提供低成本算力支撑。**三是在生态协同领域，各地注重构建融合发展生态。**江苏省支持“链主”企业开放数据接口，带动上下游中小企业通过云平台实现供应链协同；河北省打造产业链数字化协同平台，推动钢铁、装备等行业开展云端协同研发生产；河北、山东等地通过标准贯标、“百城千园行”等活动推广云平台应用场景，推动数据要素与工业制造融合，形成可复制的行业上云模式。

表 1 国内相关政策与内容

时间	地方	政策名称	内容
2024.12	江苏省	深化制造业智能化改造数字化转型网络化联接三年行动计划（2025—2027年）的通知	推动创新型中小企业初始级转型。每年推动约1万家创新型中小企业在产品设计、生产管控、营销管理、仓储物流和财务管理等应用场景，实施设备和业务上云，实现单个细分场景的效率提升。
2025.4	江苏省	《江苏省数字经济高质	鼓励平台企业创新发展。支持平台企业发

		量发展三年行动计划（2025－2027 年）》	挥市场和数据优势，加大科技创新投入，鼓励商业模式创新，提升数字技术和产品服务水平，面向中小企业开放共享创新资源。强化平台经济领域数据要素供给，引导企业开放数据服务，鼓励建设开放共享云平台，提供低代码驱动的数字化平台工具，促进企业间业务、数据和生态互联互通。
2024.9	四川省	成都市支持中小企业数字化转型城市试点若干政策措施	支持数字化转型改造。支持企业在试点期内开展数字化改造，对改造后达到验收标准的企业，按照不超过企业改造投入 50%的比例，给予最高 100 万元的资金补助。数字化改造投入包括企业在数字化改造中购买相关软件、云服务及传感器、网关等必要的数据采集传输设备，以及相应的数字化服务支出等。
2024.10	四川省	《四川省加快制造业智能化改造数字化转型行动计划(2024—2027 年)》	增强中小企业数字化转型能力。推行普惠性上云用数赋智服务，大力发展“小快轻准”数字化产品和解决方案，推动 50 万家中小企业上云用平台。
2024.11	黑龙江省	《黑龙江省中小企业数字化转型城市试点政策实施细则(试行)》	城市试点统筹使用支持资金，按照“企业出一点、供给方让一点、政府补一点”的原则,安排不低于 80%的支持资金开展中小企业数字化改造工作，包括数字化改造相关的软件、云服务支出，网关、路由等必要的数据采集传输设备支出，以及咨询诊断等服务支出;安排不高于 20%的资金用于支持数字化转型生态建设，包括用于优化服务商产品供给、支持上云上平台、培育“链式”转型模式及综合服务等工作。
2025.1	河北省	《河北省数字技术赋能制造业高质量发展实施方案》	开展企业“上云用数赋智”行动。扩大企业上云供给资源池规模，制定企业“上云上平台”产品目录。鼓励大中型企业基于云平台开展共享订单、集中采购、共享制造等新模式应用；推动中小微企业利用云化订阅式产品服务，提升企业经营水平。上云企业突破 15 万家，工业设备上云率达到 50%以上。
2024.12	山东省	《关于促进实体经济和数字经济深度融合培育发展新质生产力的实施方案》	加强政策支持。统筹中央预算内资金、超长期特别国债、地方政府专项债券等政策性资金，支持符合条件的数实融合重点项目建设。统筹中央中小企业数字化转型城市试点资金，支持中小企业“上云用数赋智”，全面落实国家关于企业数字化转型

			相关税收优惠政策。
2025.3	湖北省	《湖北省中小企业特色产业集群高质量发展工作方案（2025-2027年）》	在省级以上特色产业集群部署一批工业软件平台，引导数字化服务商面向集群企业推出云制造服务平台，支持集群企业创建智能工厂、数字化车间。
2024.8	天津市	天津市工业技术改造行动方案（2024—2027年）	加快推动中小企业数字化转型，推动智改数转网联在中小企业先行先试
2025.4	河南省	河南省数据要素市场培育行动方案（2025—2027年）	推进数字化转型发展。开展工业互联网平台提升、中小企业数字化赋能等专项行动，依托省数字化转型促进中心等载体，围绕重点产业链推进省级工业互联网平台建设，打造一批数据赋能典型案例，增强全产业链数据归集处理和融合复用能力。
2024.12	贵州省	《贵州省中小企业公共服务体系建设实施方案》	数字化转型服务。围绕中小企业发展需求，开展数字化赋能专项行动，推广《中小企业数字化转型典型案例》、《中小企业数字化水平评测指标》、《中小企业数字化转型指南》，引进数字化服务商或平台深化合作，在研发、生产、运维等场景提供专业化服务。组织数字化服务商和专家团队深入企业开展数字化水平诊断，加强对中小企业数字化转型的培训引导，推动设备上云和业务上云，助推中小企业转型升级。
2025.2	广东省	《广东省建设现代化产业体系2025年行动计划》	加快数字化转型。扎实推进4个国家级、14个省级中小企业数字化转型城市试点工作，加快建设一批跨行业跨领域工业互联网平台。发挥链式改造带动作用，引导企业加大数智技术、绿色技术应用，促进中小企业数字化转型，加快发展新产品、新工艺、新设备、新材料，推动1万家工业企业技改数转。
2025.2	福建省	《福建省加快推进数字化全面赋能经济社会高质量发展总体方案》	深化“千员万企”数字化诊断行动，加强智能装备、核心软件、工业互联网等技术集成创新，推动福州、厦门、泉州、龙岩开展国家中小企业数字化转型试点城市建设；加快规上企业数字化转型全覆盖，支持企业建设一批智能产线、智慧车间、“黑灯工厂”，到2026年全省关键业务环节全面数字化企业占比超71%。
2025.4	海南省	中共海南省委办公厅 海南省人民政府办公厅关于打造新质生产力重要实践地的意见	支持海口开展中小企业数字化转型试点，打造一批制造业数字化转型“灯塔”企业。

2024.5	广西	重庆市经济和信息化委员会关于印发重庆市中小企业数字化转型工作方案（2024—2027 年）的通知	推动中小企业触网上云用数赋智。鼓励中小企业应用市级平台相关产品，引导中小企业找准数字化转型应用场景，应用 SaaS 化产品，逐步推动企业数字化转型发展。聚焦企业研产供销服等关键业务环节，引导服务商研发攻关一批“小快轻准”产品与解决方案，为企业提供一批优质数字化转型服务产品。

1.1.2 发展内需推动中小企业上云

中小企业上云通过优化资源配置、降低硬件运维成本、提升业务效率质量、增强数据安全等维度实现降本增效。一是优化资源配置，中小企业业务规模小、市场响应快，需求波动频繁。云计算弹性伸缩功能可按需自动调整计算资源，诸如服装加工小企业，旺季时快速增加云服务器应对订单激增，淡季减少资源降低成本，按实际用量付费模式极大减轻资金压力，降低 IT 成本，同时集中管理各类 IT 资源，提高利用率，减少浪费。**二是降低硬件和运维成本，**中小企业无力承担高额硬件采购、机房建设及专业运维团队成本。中小企业上云则无需投入大量资金购置硬件设备，能够避免设备折旧损耗，同时云服务商的专业团队负责运维，中小企业无需投入大量运维人力成本。**三是提升业务效率和质量，**中小企业追求快速迭代、精准营销以在市场立足。中小企业可利用云平台的开发工具、数据处理能力和自动备份恢复功能，满足对高效业务部署、精准数据挖掘和业务连续性的内生需求，推动业务流程优化、精准营销和创新发展。**四是增强数据安全与可靠性，**中小企业自身缺乏完善的数据安全防护体系，难以抵御网络攻击和数据丢失风险。云服务商完善的安全防护体系和数据备份恢复功能，保障数据安全，降低数据丢失风险。

中小企业乘云而上解锁业务增长新势能。一是上云驱动智能营销与精益生产。在市场营销环节，中小企业受限于资金与技术，未上云时难以像大型企业那样开展全面数据采集与分析，上云后，中小企业利用云端数据湖可整合客户行为数据，通过 AI 对数据进行分析和挖掘，构建用户画像，实现精准营销和个性化服务。在生产制造环境，中小企业传统本地 IT 系统性能不足，难以应对设备传感器每秒产生的海量实时数据，上云后，基于云端流计算引擎，AI 得以实时分析处理这些数据，精准优化生产流程、把控产品质量，让中小企业在资源有限的情况下，也能实现高效生产运营。**二是"上云"破除信息孤岛，驱动企业协作与共享增效。**未上云时，中小企业在信息、能力上的孤立形成难以逾越的“数字鸿沟”，信息上，数据分散、流通不畅，上下游信息脱节；能力上，研发、运营等能力不足，难以独立突破技术与市场瓶颈。云计算的出现，为打破这些无形壁垒提供了强大引擎。基于开放的云平台，不同领域的中小企业能够信息共享，例如，小型电商零售企业可以通过云平台与多家物流企业实现数据共享和业务协同，零售企业能够实时查询物流企业的车辆位置、配送进度等信息，而物流企业则可以提前获取零售企业的订单波动情况，合理调配运力，优化配送路线。

1.2 中小企业和大型企业云上安全建设与运营有显著差异

中小企业与大型企业的根本性差异影响云安全建设策略。中小企业和大型企业在组织建设、技术能力、资金投入、合规遵从、生态协同五方面因自身特质差异，双方在云安全的建设方面也存在差异。

组织建设方面：一方面，中小企业组织架构相对简单，安全决策和执行流程短；大型企业组织架构较为复杂，通常设立多类型安全部门，如网络安全部、数据安全部、安全合规部等，分工明确且审批流程较长。另一方面，中小企业安全团队人员精简，由少数具备多领域技能的人员组成；大型企业安全团队规模庞大，成员涵盖攻防专家、安全架构师等细分领域人才。

技术能力方面：一方面，中小企业优先采用云服务商原生安全工具与开源方案构建轻量化防护体系，通过基础加密、访问控制等手段满足核心数据保护需求；大型企业通常采购并部署先进的、功能全面的云安全工具，根据业务类型与数据等级，差异化安全策略。另一方面，由于中小企业安全技术人员较少，且需要同时承担网络维护、系统管理与安全防护等多项工作，难以持续跟进先进的安全技术；大型企业通常在网络安全、数据安全、安全合规等领域布局专业人员，专注细分技术领域，在先进的漏洞挖掘、高级威胁分析等方面具备深厚的技术功底。

资金投入方面：中小企业资金相对有限，强调成本效益，优先选择标准化安全服务而非定制化方案，重点覆盖数据泄露防护、服务可用性保障等生存性指标；大型企业资金雄厚，能够投入大量资金用于云安全建设，如进行定制化的安全解决方案，满足其复杂的业务和安全需求。

合规遵从方面：中小企业通常依赖外部顾问或云服务商的指导来满足合规要求，更多地关注基本的合规要求，采取相对简化和被动的

合规策略；大型企业拥有专业的合规团队和法律顾问，能够全面、深入地开展合规管理，确保云环境运营的合规性和安全性。

生态协同方面：中小企业依赖云服务商的安全能力，自身对软件供应链风险的控制力较弱；大企业则通过生态合作共享威胁情报，并主导软件供应链安全标准制定，降低整体云上安全风险。

表 2 中小企业和大型企业安全建设与运营差异

		中小企业	大型企业
组织建设	组织架构	**相对简单**，安全决策和执行流程短，响应速度快。	**较为复杂**，会设立多个安全部门，分工明确，审批流程较长。
	安全团队	**架构精简**，由少数具备多领域技能的人员组成。	**规模庞大**，成员涵盖攻防专家、安全架构师等细分领域人才。
技术能力	技术方案	优先采用**云服务商原生安全工具与开源方案构建轻量化防护体系**，通过基础加密、访问控制等手段满足核心数据保护需求。	**采购和部署先进的、功能全面的云安全工具**，能够制定精细化安全策略，根据业务、数据和用户角色差异化配置。
	技术人员	**安全技术人员较少**，且需要同时承担网络维护、系统管理与安全防护等多项工作，**难以深入钻研单一安全技术领域**。	**具备网络安全、数据安全等领域的顶尖人才**，这些专业人员专注于细分技术领域，在漏洞挖掘、高级威胁分析等方面**具备深厚的技术功底**。
资金投入		**资金相对有限**，强调成本效益，选择标准化安全服务而非定制化方案，重点覆盖数据泄露防护、服务可用性保障等生存性指标。	**资金雄厚**，能够投入大量资金用于云安全建设，如进行定制化的安全解决方案，满足其复杂的业务和安全需求。
合规遵从		**依赖外部顾问或云服务商指导满足合规要求**，关注基本合规要求，采取简化、被动的合规策略。	**有专业合规团队和法律顾问**，全面、深入进行合规管理，确保云环境合规性和安全性。
生态协同		**依赖云服务商安全能力**，自身对供应链风险控制力较弱。	通过**生态合作共享威胁情报**，**并主导供应链安全标准制定**，降低整体风险。

总结如表 2 所示，上述根本性差异塑造了中小企业云安全建设策略：“高度关注致命安全风险，暂时容忍非致命性安全风险”。中小企业需要将其有限的资源高度聚焦于可能导致企业业务中断、核心数据泄露、巨额罚款等生存性威胁上，对于可能造成工作不便、效率降低、声誉轻微受损或非核心数据泄露等非致命性风险，中小企业通常采取有限度容忍的态度，并非忽视风险，而是在资源刚性约束下的理性妥协。

第二章　中小企业上云安全特质影响与风险分析

2.1　中小企业特质对云安全工作开展带来影响

中小企业具有组织架构扁平化、安全团队精简、技术能力有限、资金投入谨慎及生态协同依赖性强等特质，这些特质又在一定程度上对云安全工作的开展产生了多方面的影响，且每一种影响均涵盖积极与消极两个层面。

一是扁平化组织架构。优势是安全决策敏捷，安全文化渗透迅速。中小企业云上安全决策通常可由技术负责人直接推动，无需复杂审批流程便能快速启用云安全工具，以降低攻击窗口期；此外，中小企业员工人数较少，上云安全政策、意识培训等能够快速覆盖，由高层领导直接传达可以减少信息衰减，全员安全文化渗透速度快。**劣势是管理权力集中导致安全角色模糊。**受限于人员配比，IT 管理员兼任安全职责，云上安全决策更依赖个人，云上安全建设更依赖云服务商文档和社区支持，专业深度不足；此外，由于管理权力的集中，难以实施最小权限原则，容易发生内部威胁或误操作。

二是技术架构依赖外部赋能。优势是第三方安全赋能更加专业。专业的云服务商年度投入大量资金进行安全研发，可为中小企业提供难以自建的高级防护能力，如零信任、AI 驱动的威胁检测等。**劣势是若选用多家云服务商，上云安全责任分散，持续累积技术债务。**中小企业通常拼凑使用若干低成本 SaaS 服务满足办公协作、客户管理、财务管理等需求，安全责任分散且第三方服务漏洞可能影响核心业务；此外，中小企业为快速上线业务，通常云安全配置够用即可（如延迟

打补丁），以及业务增长后因成本或功能需求叠加不同技术栈的云服务，无法统一管理，持续积累架构债务。

三是单一业务系统。云安全建设呈现靶向性优势。中小企业云安全设计通常与其依赖的单一业务深度耦合，可针对核心业务设计精准控制，如 WAF 规则可以完全围绕该业务的 API 特征定制，与通用规则相较更为精准。**劣势是系统重要性高度集中面临重大安全风险。**一旦攻击者通过 DDoS 攻击或弱口令爆破攻破中小企业核心系统，可直接窃取全部业务数据，企业业务或将停摆，可能直接导致客户流失或瘫痪整个企业运营。

四是链属角色较为弱势。优势是可学习链主能力，借势提升基础安全。作为供应链中的链属企业，需要满足链主企业的安全审计要求，在梳理链主企业相关的安全条款时，标注可复用部分同步完成自身基础安全配置，如日志留存 6 个月等，省去自主规划成本。**劣势是合规话语权低，响应链主需求需要投入更多资源。**在面临供应链中链主企业的合规压力和要求条款时，中小企业的话语权低，如满足链主的安全要求时需要投入更多的资源等；以及在接入大客户系统时，为兼容其老旧云安全协议，必须采用客户指定方案，无法实施自身产品已集成的、现代化的云安全协议。

五是合规以完成基础要求为主。选择性响应安全与合规要求短期有成本优势。中小企业通常会积极响应强制性要求，如《网络安全法》、《个人信息保护法》等，实现基础合规即止步，对于行业性标准等则选择性响应，主要原因是开展全面合规费用高昂，中小企业选择性地

降低上云初期云安全投入成本，实现基础防火墙、备份等基础要求，减少在高级威胁检测系统的投资，将更多资源聚焦核心业务更有利于发展；此外，不做过于细致的安全策略如数据分类分级，直接加密所有数据可规避组织内部复杂流程。**仅完成基础合规存在长期风险劣势。**选择性合规也将导致安全防护不全面，易使自身成为攻击目标，提升数据泄露事件发生概率，从而违反《个人信息保护法》、《数据安全法》等法规，面临高额罚款。

2.2 中小企业上云安全风险十大类别

从安全风险的威胁对象与应用场景的视角出发，对中小企业上云后面临的安全风险进行系统性梳理，形成十大安全风险类别。

身份安全风险：访问控制的“守门人”失效。身份安全风险威胁对象聚焦于云环境中用户账号、设备身份、云工作负载身份、应用身份等，涉及上述身份在云环境中进行访问控制过程的风险，包括识别、认证、授权等，若身份管理不善，可能导致攻击者进入云环境，致使业务控制权丧失。

数据安全风险：数据全生命周期失控。数据安全风险威胁对象聚焦云上数据资产，涉及数据全生命周期过程中面临的安全风险结果，包括数据泄露、篡改、丢失、勒索等威胁，影响中小企业关键信息的保密性、完整性和可用性，致使核心资产清零。

应用安全风险：业务逻辑的“隐形漏洞”。云上应用安全风险威胁对象聚焦云上业务系统、应用层 API、应用能力类型云服务等服务，涉及云上服务系统调试接口暴露、云服务不可用或被篡改等威胁，可

能导致应用或 API 被攻陷进而长时间停服，影响业务正常运行。

计算安全风险：计算资源的“非法征用”。计算安全风险威胁对象聚焦云主机、裸金属服务器等计算资源，涉及云服务器账号被爆破、云计算资源被占用、云服务商被入侵等安全风险，可能导致云服务器成为恶意攻击的跳板，致使计算资源的非常规损耗。

存储安全风险：结构化与非结构化数据的“裸露”。存储安全风险威胁对象聚焦云存储（块存储、对象存储等）、云数据库等存储资源，存储安全风险涉及云存储被勒索、公开，云数据库不可用、被篡改等，可能导致机密文件被下载，影响企业发展。

网络环境安全风险：流量的“污染与中断”。网络环境安全风险威胁对象聚焦云网络、流量负载均衡器等，涉及云网络环境的稳定性与安全性，大规模 DDoS 攻击可能导致网络流量被污染，从而影响网络服务响应速度，致使企业业务的正常通信被中断。

软件供应链安全风险：来自源头的“信任危机”。软件供应链安全风险威胁对象聚焦中小企业使用的云服务、第三方付费软件、免费开源软件等，涉及中小企业在开展自身业务时所使用的上述服务或软件存在漏洞或被植入后门，甚至底层云服务不可用，相关安全风险将从软件供应链传递至中小企业云环境中。

合规安全风险：踩踏红线的“代价”。合规安全风险威胁对象聚焦中小企业本身，在上云开展业务过程中中小企业需要遵守法律法规、行业相关管理办法等，若企业未能满足相关合规要求，可能面临法律诉讼、罚款、声誉损失等后果。

审计安全风险：追溯能力的“失明”。审计安全风险威胁对象聚焦中小企业的安全风险追溯能力，若审计安全措施不到位，可能导致审计日志被篡改或丢失，无法有效追溯安全事件和违规行为，影响企业的安全管理和合规性。

安全管理风险：人与流程的“失控”。安全风险管理威胁对象聚焦中小企业的管理体系，无论是因为人员行为偏差或安全审查流程不合理导致的安全事件，概因企业管理体系存在缺陷，安全机制存在漏洞，进而导致威胁发生，是中小企业稳定运营不可忽视的风险类别。

中小企业在上云时，依据需求选择不同类型的云服务，不同类型云服务与上云安全风险类别对应关系如图 1 所示。

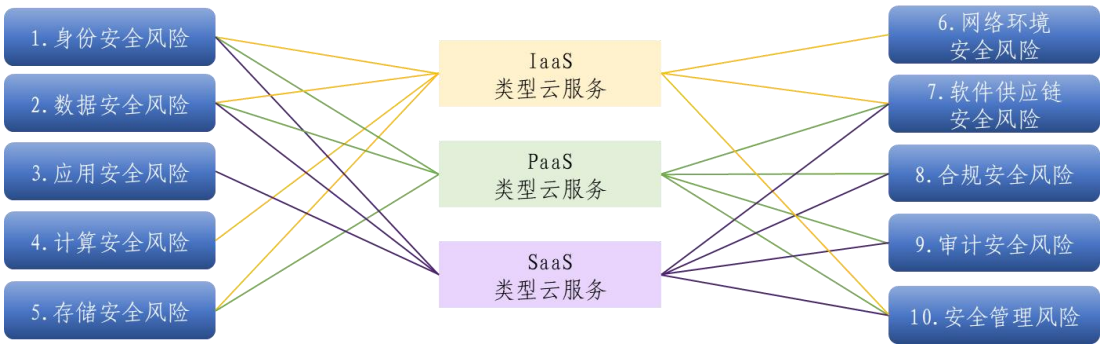


图 1 云服务类型与上云安全风险类别映射关系

第三章 中小企业上云安全风险十条

3.1 中小企业选用不同云服务类型面临不同安全风险

上节总结了上云十大安全风险类别，每类安全风险中包含若干安全风险条目，表 3 总结了中小企业上云安全风险条目，共计 24 项。

表 3 上云安全风险分类总结

十大安全风险类别	上云安全风险条目
身份安全风险	1. 资源越权访问：权限过大 2. 账密泄露：明文贴电脑、AK/SK 被公开 3. 账号暴力破解：弱密码、未开启多因子认证
数据安全风险	4. 数据泄露 5. 数据篡改 6. 数据丢失 7. 数据勒索
应用安全风险	8. 云上业务系统或 API 未启用身份验证暴露公网：调试接口暴露 9. 云上业务系统或 API 不可用 10. 云上业务系统或 API 被篡改
计算安全风险	11. 云服务器被爆破成功：开放高危端口 12. 云服务器资源被恶意占用
存储安全风险	13. 云存储勒索：锁存储 14. 云存储服务被公开：设置错误 15. 云数据库不可用 16. 云数据库被篡改
网络环境安全风险	17. 网络不可用 18. 网络慢（可能是网络攻击导致的）
软件供应链安全风险	19. 第三方云服务组件存在漏洞或被植入后门 20. IaaS、PaaS、SaaS 服务商被入侵
合规安全风险	21. 数据出境面临的存储位置不符合法规要求 22. 日志存储时间不够
审计安全风险	23. 无日志，无法追溯异常
安全管理风险	24. 内部威胁与误操作

中小企业上云面临多项上云安全风险，根据安全风险与云服务能力类型的映射情况，发现部分风险与云服务能力类型有关，部分与其无关。IaaS 主要涉及底层计算、存储、网络资源的安全风险，PaaS 主要涉及开发和运行平台的安全风险，SaaS 主要涉及应用程序层的

安全风险，还有部分风险是跨模型的通用风险，一方面指上述三类能力类型云服务均会涉及的风险，另一方面风险独立于云服务，例如涉及管理、合规、人员和供应链等领域。

中小企业上云选择云服务能力类型的过程本质是在业务需求、技术能力、成本压力三者间寻找最优解。如表 4 所示，中小企业根据业务需求的定制化程度、自身技术实力的强弱、可接受的成本三维度选择不同能力类型的云服务。**选择 IaaS 的主要因素是业务需要绝对控制权，**此能力类型下中小企业技术能力要求高、成本压力大，通常一些特殊行业会做此选择，如医疗行业，一是医疗影像系统软件依赖特定 Linux 内核参数需直接访问 GPU 物理资源，二是要满足药监局数据本地化要求等。**选择 PaaS 主要因素是开发效率优先于底层控制，**此能力类型下中小企业核心诉求是，解决自身技术短板以加速业务迭代，例如为应对流量暴增场景，直接使用 Serverless 函数计算自动扩容，补足无容器开发与运维经验的缺失。**选择 SaaS 主要因素是解决通用型需求，**此能力类型下中小企业通常具有通用型管理需求，例如部署 CRM、OA、企业通讯服务等，此外也有部分应用能力类云服务可以帮助中小企业转嫁合规成本，例如满足《电子签名法》的电子合同 SaaS 平台，满足医疗合规要求的电子病历 SaaS 系统等。

表 4 中小企业云服务类型三维决策模型

	业务需求			技术能力			成本压力		
	高度定制	部分定制	标准化高	专业	中级	基础	难以承受	可以协商	长期订阅
IaaS									
PaaS									
SaaS									

中小企业使用 IaaS 可能面临的安全风险有八项：一是云服务器被爆破成功，若用户配置端口不当，可能将 SSH/Telnet 等高危端口开放。**二是云服务器资源被恶意占用，**若用户监控不当或未设置资源配额，恶意软件可能滥用虚拟资源。**三是云存储被勒索，**若用户访问策略配置不当或未启用存储备份，可能导致云存储权限被劫持。**四是云存储服务被公开，**若用户对存储桶访问权限错误配置，可能导致存储桶向公众开放。**五是网络不可用，**若用户配置 VPC 有误，或云服务商物理网络故障，则将导致网络不通。**六是网络慢，**若用户未配置流量清洗规则，或云服务商未提供基础 DDoS 防护，则将导致网络因遭受网络攻击而响应缓慢。**中小企业使用 PaaS 可能面临的安全风险有三项：一是云数据库不可用，**若用户容量规划、连接池配置不当，或云数据库服务供应商未提供多可用区部署能力，将增加云数据库不可用风险。**二是云数据库被篡改，**若用户未遵循最小权限原则配置权限，则将增加云数据库数据被篡改风险。**三是第三方云服务组件存在漏洞或被植入后门，**若用户在平台上使用开源云服务组件（组件存在漏洞），或云服务商未对云市场上架的云服务组件进行安全审核，则将增加业务被入侵风险。**中小企业使用 SaaS 可能面临的安全风险有**

三项：一是 SaaS 未启用身份认证导致账号被接管，若用户被钓鱼或撞库，则将增加云服务账号被攻击者接管风险。**二是 SaaS 被篡改，**若用户授权组织内存在后门的第三方办公应用与云服务集成，则将增加云服务被篡改风险。**三是 SaaS 不可用，**若用户遭遇安全攻击、云服务商资源出现故障或限制等，则将增加云服务因组件故障或被恶意阻断引发的不可用风险。

涉及数据管理、合规实践、身份配置和供应链的风险与云服务能力类型无关，属于通用云安全风险。共计十二项：**一是资源被越权访问，**任何类型云服务均存在访问控制问题，若用户未遵循最小权限原则配置权限，则将增加资源被越权访问风险。**二是账密泄露，**任何类型云服务均存在访问凭据管理问题，若用户将 AK/SK 公开或将密码贴至电脑，均增加账密泄漏风险。**三是账号被爆破，**任何类型云服务均存在弱密码、未启用多因子认证等问题，若用户未设置强密码策略，均易增加账号被爆破风险。**四是数据泄露，**数据未经授权被访问可发生在云存储、云数据库或 SaaS 应用中，若用户未对数据进行加密或访问控制，易增加数据泄漏风险。**五是数据篡改，**任何类型云服务中数据均存在被非法修改的可能性，若用户未开启完整性校验，数据篡改发生概率或将提升。**六是数据丢失，**云存储、云数据库均存在数据的意外删除或损坏，若用户未配置备份或快照，数据将难以找回。**七是数据勒索，**任何类型云服务均存在被勒索软件加密数据的可能性，若用户未部署防勒索方案，如不可变存储，则将增加数据被勒索概率。**八是云服务商被入侵，**在用户角度，云服务商被攻击属于供应链风险，

云服务商应向用户承诺云服务可用性。**九是数据出境面临的存储位置不符合法规要求，**若用户未选择合规区域存储数据，将面临监管处罚。**十是日志存储时间不足，**用户对日志管理不足将影响所有云服务的日志审计和问题追溯，若未设置留存 90 天策略或将面临法律追责。**十一是无日志记录，**若用户未对运维所需日志进行记录，将无法对云服务产生问题进行追溯。**十二是内部威胁与误操作，**员工的错误或恶意行为均会对云服务的安全运行产生影响，若云服务未实施权限分离或敏感操作二次审批，则将提升相关行为被执行风险。

3.2 中小企业上云安全风险关键十条

中国信通院围绕中小企业上云安全风险开展调研，基于调研结果、访谈内容和专家评审综合评估筛选出中小企业上云安全风险关键十条，并从这十大安全风险发生的普遍性、威胁演化的严重性和防御的落地难度三个维度展开探讨。

安全风险发生的普遍性，考量中小企业上云的实际场景中安全风险出现的频率与广泛程度，发生越普遍则风险越关键。**威胁演化的严重性，**考量安全风险发生后为中小企业直接带来的经济损失、对业务连续性的干扰程度、法律后果、品牌形象影响四方面，造成结果越严重则风险越关键。**防御措施的落地难度，**考量中小企业为应对安全风险，需实施技术的复杂度、人力的投入、成本开销三方面，防御落地难度越高则风险越难被抵抗。依据上述维度对十大安全风险开展研究，安全风险发生的普遍性如表 5 所示，威胁演化的严重性如表 6 所示，防御措施的落地难度如表 7 所示。

表 5 安全风险发生普遍性及其说明

安全风险	关键依据	发生可能性
网络慢（网络攻击导致）	特定 DDoS 攻击影响才显著	★★
数据丢失	需要极高权限	★
内部威胁与误操作	误操作易发生	★★★★
资源越权访问	访问控制配置复杂易出错	★★★
云上业务无身份认证暴露公网	攻击门槛低	★★★★
账密泄露	凭证管理不当较为常见	★★★
账号暴力破解	自动化工具攻击持续发生	★★★★★
数据泄露	攻击链较长	★★
第三方组件漏洞	高危漏洞频现然而修复滞后	★★★★★
云服务器资源恶意占用	监控部署不足难以发现	★★★★
等级说明： ★：年发生概率接近零 ★★：年发生概率极低 ★★★：年发生概率较低 ★★★★：年发生概率较高 ★★★★★：年度必然发生		

表 6 威胁演化严重性及其说明

安全风险	典型后果场景	后果严重性
网络慢（网络攻击导致）	交易失败率提升+用户流失	★★☆
数据丢失	核心数据库删除	★★★★★
内部威胁与误操作	管理员删库+篡改日志	★★★★
资源越权访问	越权下载用户数据	★★★☆
云上业务无身份认证暴露公网	攻击者操控业务系统	★★★★
账密泄露	攻击者快速接管资源	★★★★
账号暴力破解	攻击者尝试接管资源	★★★
数据泄露	商业机密被公开	★★★★★
第三方组件漏洞	漏洞有一定概率被恶意利用	★★★☆
云服务器资源恶意占用	云上业务卡顿	★★
等级说明： ★：可快速恢复		

★★：影响局部业务
★★★：引发客户诉讼
★★★★：业务长期停摆
★★★★★：企业生存危机

表 7 防御措施落地难度及其说明

安全风险	防御措施	防御难度
网络慢（网络攻击导致）	启用 DDoS 防护+弹性带宽	★★
数据丢失	配置自动备份+手动备份	★
内部威胁与误操作	权限最小化+操作审批流程	★★★★
资源越权访问	RBAC 角色分离+权限最小化	★★★
云上业务无身份认证暴露公网	强制身份验证	★★
账密泄露	凭据管理+凭据轮换	★★
账号暴力破解	MFA+登录失败锁定	★
数据泄露	DLP+存储加密	★★★★
第三方组件漏洞	镜像扫描+SBOM 管理	★★★★
云服务器资源恶意占用	进程白名单+资源监控告警	★★★
等级说明： ★：运维友好 ★★：运维可实施 ★★★：需要安全专家 ★★★★：重度依赖资源 ★★★★★：耗费极大资源		

基于上述三个维度综合评估得到中小企业上云安全风险十条的风险严峻程度，如图 2 所示，并按风险严峻程度排序，从这十大安全风险发生的普遍性、威胁演化的严重性和防御措施的落地难度三个维度进行探讨，具体如下：

一是第三方云服务组件存在漏洞或被植入后门：风险普遍性方面，根据《2025 年度开源安全和风险分析报告》的数据显示，81%的代码库存在高风险或重大风险漏洞，而中小企业若缺乏供应链安全管理，易使用含高危漏洞组件的开源或第三方组件而发生安全事件，此类风

险每年必然发生。**威胁严重性方面**，高危漏洞或组件后门被利用后，易引发核心数据窃取、服务瘫痪等威胁，导致经济与声誉受损、客户诉讼等，且业务中断修复周期较长。**防御措施的落地难度方面**，组件漏洞扫描工具等技术成本适中，但安全审计流程繁琐且需规范实施，完整落地难度较大。

二是内部威胁与误操作。风险普遍性方面，中小企业的权限分配机制松散甚至无需审批，常存在过度授权现象（如运维人员可直连生产数据库操作），导致内部员工能无意或恶意执行不安全操作，此类风险的发生概率较高。**威胁严重性方面**，内部员工可能会泄露、删除重要数据，篡改文件或植入后门，直接对中小企业业务造成破坏带来经济损失。**防御措施的落地难度方面**，实施最小权限原则需要投入精力去设计、实施、监控复杂的内部行为管控措施，部署后还需要持续维护和审计，云环境的动态性与复杂性更将管控难度放大。

三是数据泄露：风险普遍性方面，数据是中小企业的核心资产，安全防护是重中之重，故因数据未加密或权限管控松散导致的数据泄露发生的概率极低。**威胁严重性方面**，数据泄露直接引发经济损失和业务负面影响，如客户索赔、竞争失利等，以及声誉损害等。**防御措施的落地难度方面**，专门用于数据防泄漏防护的高级工具如企业级 DLP、高级 UEBA、加密密钥管理系统价格昂贵，策略定制需要专业知识，维护时需要甄别误报，处理负担重。

四是云上业务系统未启用身份验证暴露公网：风险普遍性方面，国内扫描机器人日均探测 IP 可超 8000 万次，企业若未开启接口身份

认证，其新开公网端口 24 小时内必遭扫描，导致未设防的 API 或调试接口直接暴露攻击面，此类风险的发生概率较高。**威胁严重性方面，**攻击者可轻易通过未保护 API 批量窃取数据、篡改业务逻辑，造成经济损失和业务崩溃，并且将导致企业品牌信任度大幅下降。**防御措施的落地难度方面，**启用 API 密钥认证、IP 白名单等措施技术可有效应对该风险，需要运维人员具备一定专业知识，防护措施落地难度尚可。

五是资源越权访问。风险普遍性方面，中小企业为求便捷默认使用 Administrator 等高权限账号，开发测试环境与生产环境混布，但由于此类违规操作多集中于内部特定场景，且外部攻击者通常优先选择更具普遍性、更易探测到的攻击面，所以此类风险的发生概率较低。**威胁严重性方面，**高权限账号被攻击者利用后，对数据窃取、恶意篡改等危害随攻击者操纵的账号权限等级升高呈指数级增长。**防御措施的落地难度方面，**与实施最小权限原则类似，实施 RBAC 角色权限分离、细粒度管控可有效降低风险，但中小企业难以投入人力去制定、维护精细化的权限管控。

六是云服务器资源被恶意占用：风险普遍性方面，企业因安全漏洞未修复或云资源日志审计缺失，导致漏洞易被利用，而漏洞主机 24 小时内被植入挖矿脚本概率超 70%，此类风险发生的概率较高。**威胁严重性方面，**资源被占用导致服务器负载升高、服务响应缓慢甚至崩溃，引发局部业务中断或恶意扣费，且数据窃取或资源滥用可能引发合规风险和声誉损害。**防御措施的落地难度方面，**攻击方通过低

成本方式实现高度隐蔽的攻击，中小企业往往缺失专业的监控工具与专业人员，若需要建立快速止损能力，需要一定程度的人力物力投入。

七是账密泄露：风险普遍性方面，中小企业安全意识不足，员工复用密码率超过 60%，且因多人共享账号等情况出现，导致云服务访问密钥易泄露，但当前攻击者通常借助自动化工具，依据常见弱密码字典、已泄露的知名企业账密库等资源尝试登录攻击，所以此类风险的发生概率较低。**威胁严重性方面，**账密泄露将导致攻击者接管账号，可实施数据窃取、资源滥用等操作，直接造成数据泄露损失与业务系统瘫痪，导致企业声誉的降低。**防御措施的落地难度方面，**启用账号登录日志审计等措施的成本较低，提高员工安全意识需企业自上而下推广，整体防御措施落地难度尚可。

八是账号暴力破解：风险普遍性方面，国内僵尸网络持续对 RDP/SSH 等端口发起爆破攻击，许多中小企业因未启用多因子认证、弱密码检查等防护措施，易遭受系统被恶意控制等事件，此类风险每年至少发生一次。**威胁严重性方面，**云上相关账号被破解后，攻击者可实施数据篡改、内网渗透等操作，直接导致企业经济损失、业务中断及声誉受损。**防御措施的落地难度方面，**开启多因子认证、强制定期改密等防护实施的成本较低，基础运维人员便可实施。

九是网络慢。风险发生普遍性方面，中小企业带宽预算有限，易受低成本 UDP 洪水攻击，通常云服务商会为中小企业提供基础的 DDoS 防护能力，因此此类风险发生的概率极低。**威胁严重性方面，**网络卡顿直接降低办公效率，交易类业务（电商、金融）可能因延迟

导致订单流失，并且会导致客户体验下降，长期影响企业竞争力。**防御措施的落地难度方面**，启用云平台提供的 DDoS 防护并购买弹性带宽可以有效缓解此类安全风险，基础运维人员便可实施。

十是数据丢失。风险普遍性方面，云服务商通常能够为中小企业提供较为完善的云平台冗余机制，但人为误删偶有存在，此类安全风险通常若干年发生一次。**威胁严重性方面**，无论是遭受云上攻击或执行误删除操作均易导致数据丢失，为中小企业带来巨大经济损失和市场信誉的损害。**防御措施的落地难度方面**，云服务商通常可提供多种数据防丢失措施，如数据备份与恢复、数据加密等，中小企业通常配置自动备份或手动进行备份便可抵御此类风险，基础运维人员便可实施。

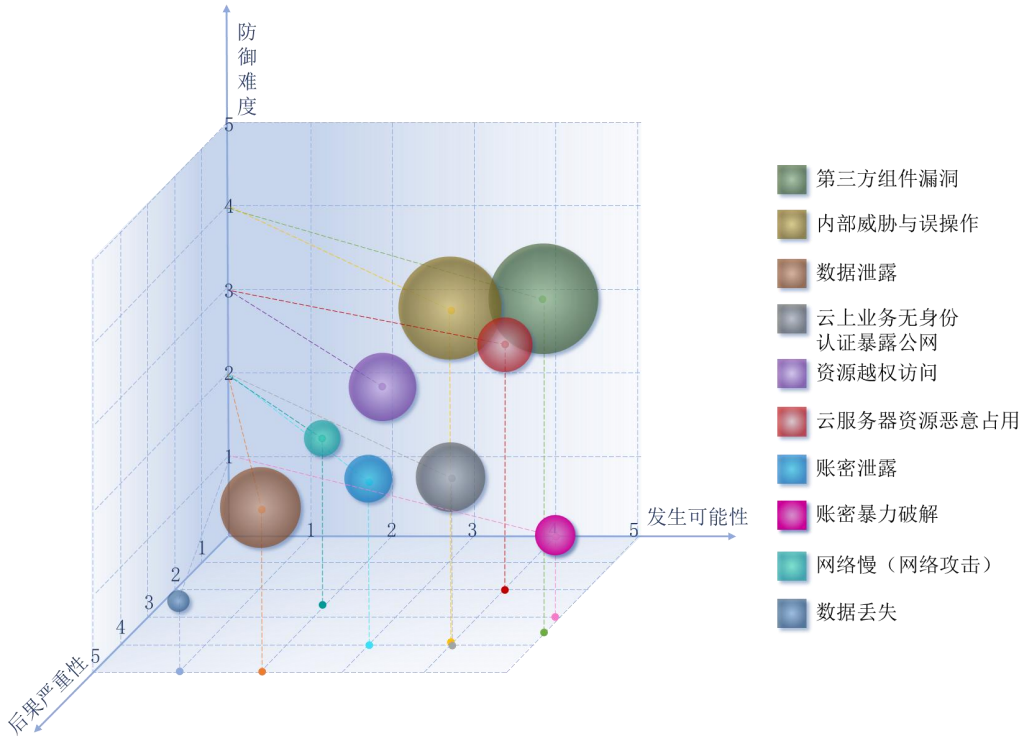


图 2 中小企业上云安全风险严峻程度三维图

第四章 中小企业上云安全风险处置十条

3.2 节中阐述了中小企业上云安全风险十条，总结于表 8 中，对应上述十条安全风险，从“可立即行动项”到“长期投入项”考虑安全风险处置建议，通常每条安全风险存在多种处置方式，按照处置方式出现频率由高至低，频率相同则可立即行动项优先，再相同则解决的风险排序靠前优先，得出中小企业上云安全风险处置十条，如表 9 所示。

表 8 中小企业上云安全风险十条

风险排序	安全风险	风险排序	安全风险
风险 1	第三方组件漏洞	风险 6	云服务器资源恶意占用
风险 2	内部威胁与误操作	风险 7	账密泄露
风险 3	数据泄露	风险 8	账号暴力破解
风险 4	云上业务暴露公网（且未启用身份认证）	风险 9	网络慢（网络攻击导致）
风险 5	资源越权访问	风险 10	数据丢失

表 9 中小企业上云安全风险处置十条

排序	处置方式	频率	类型	说明
1	访问控制	8	立即行动项	风险 1~8 涉及
2	监控与审计	7	需长期投入	风险 2~6、8、9 涉及
3	身份认证	6	立即行动项	风险 1~4、7、8 涉及
4	网络隔离	4	立即行动项	风险 3、4、6、9 涉及
5	数据加密	4	中期行动项	风险 3、4、7、10 涉及

6	员工培训	2	需长期投入	风险 2、7 涉及
7	漏洞管理	2	需长期投入	风险 1、9 涉及
8	备份与冗余	2	中期行动项	风险 3、10 涉及
9	DLP 防护	1	需长期投入	风险 3 涉及
10	DDoS 防护	1	立即行动项	风险 9 涉及

中小企业上云安全风险处置的分阶段执行建议，将结合是否可立即执行（即技术落地难度、资源投入多少）和处置方式的覆盖面（即频率排序）两个维度展开。

4.1 处置十条分阶段执行建议-立即行动项

立即行动项共四项，可被优先执行主要有三方面原因：**一是投入产出比高。**无需额外付出工具成本，可依赖云平台原生功能提升能力，配置耗时人天短。**二是能够阻断大部分常见攻击。**开启 MFA 便能解决暴力破解问题，设置网络隔离便能阻断威胁横向移动，按最小权限原则授权便能降低越权操作发生可能性。**三是满足合规基础。**执行后可满足相关合规要求。四项立即行动项分别为访问控制、身份认证、网络隔离、DDoS 防护。

处置方式一：访问控制—通过权限最小化，限制攻击面和内部误操作影响范围。企业通过明确各岗位的职责与对应的云资源访问需求，完成人岗权限绑定，确保 “岗有权、权在岗”，并且依据“最小权限原则”，为不同角色的用户分配完成任务所需的最低权限。例如，财务人员仅被赋予访问财务相关云资源的权限，开发人员仅能开展开发测试操作。实施访问控制并践行权限最小化，不仅可以减少黑客通

过窃取账号可访问的系统范围，限制“攻击面”，还能有效降低员工误操作（如误删关键数据、误改系统配置）影响所波及的范围。

处置方式三：身份认证—通过反复确认操作者身份真实，增加攻击者攻击难度。中小企业实施身份认证时，可先搭建基础的账号管理体系，为每位员工创建独立账号并明确账号归属，同时规范密码策略。此外，可以要求用户在登录或执行敏感操作时，提供两种及以上独立的身份验证要素，通过多重身份验证机制强化身份核验流程，增加攻击者攻击难度。例如，除了常规的账号密码外，还需配合短信验证码、指纹识别、动态口令等，确保操作者身份的真实性。若攻击者想突破认证，不仅需要窃取密码，还需获取用户的手机、生物特征等其他验证信息，大大提高攻击难度。

处置方式四：网络隔离—通过设置网络分段隔离关键资产，缩小攻击暴露面。依据业务功能、数据敏感程度等维度，将云网络划分为不同的逻辑或物理子网，并通过划分 VPC、访问控制列表等技术手段，严格限制各网段之间的流量交互。例如，黑客入侵了企业的公开 Web 服务网段，也会因网络隔离策略无法直接访问后端数据库服务器。由此当某一网段被入侵时，该处置方式可有效阻碍攻击者向其他区域渗透，从而避免“单点突破、全网沦陷”的风险。

处置方式九：DDoS 防护—通过流量清洗过滤恶意攻击流量，保障网络服务正常运行。梳理网络流量基线（如日常访问峰值、核心业务端口流量特征），并利用基础的流量清洗功能进行恶意攻击流量的初步防护。在此基础上，通过对进入云服务器的网络流量进行实时分

析，自动识别并拦截异常流量，仅允许正常业务流量通过，确保服务器、应用系统的网络带宽和资源不被恶意占用。例如，当黑客发动UDP洪水攻击时，防护系统会识别出异常的UDP包特征，自动阻断来源IP或引导流量至清洗节点进行净化。如此，当在网络服务及服务器等资源遭受攻击时，能有效规避因恶意流量冲击导致的系统全面瘫痪或业务停滞等问题。

4.2处置十条分阶段执行建议-中期规划项

中期行动项共两项，在中期执行主要有三方面原因：**一是需要轻度规划。**诸如备份周期、加密密钥的轮换策略需要根据业务定制。**二是需要投入一定成本。**云存储跨区费用相比于单一区域略有上浮。**三是存在一定技术依赖。**HTTPS的部署需要应用进行适配。两项中期行动项分别为数据加密和备份与冗余。

处置方式五：数据加密—能够保障数据机密性，令数据难以被利用。对存储于云端的数据及传输中的数据，运用加密算法进行处理，将原始数据转换为不可读的密文形式。例如，用户将业务文件上传至云服务器时进行加密存储，当数据在公网传输时，也能通过HTTPS进行加密传输，确保数据在“存储态”和“传输态”均以密文形式存在。数据加密后，由于缺乏解密密钥，攻击者即便通过入侵服务器或拦截网络流量获取数据，所获也仅是乱码密文，无法直接获取或利用其中的信息。

处置方式六：备份与冗余—能够保障数据可用性，即便数据丢失也能找回。对核心数据定期创建副本，并将副本存储在与原始数据不

同的物理位置或云端区域，保障数据的实时可用性。例如，企业可定期将云端数据库备份至另一个区域的存储桶，当主数据因攻击、误删或硬件故障丢失时，能快速从备份副本中恢复数据，避免业务中断。通过数据备份，即使原始数据丢失或被破坏，仍可依托备份副本完成数据还原，将损失控制在最低限度。

4.3处置十条分阶段执行建议-长期运营项

需长期投入项共四项，需长期投入主要有三方面原因：**一是人力依赖。**需要专业的安全人员具备深厚的技术背景和丰富的实践经验，才能有效管理和维护云安全。**二是属于固化流程。**审计与培训的开展需要纳入企业长效的 IT 管理流程中。**三是成本爬升。**随着云计算的发展，新的安全技术与工具不断涌现，企业需要持续投入资金以应对复杂的网络安全威胁。四项需长期投入项分别为：监控与审计、员工培训、漏洞管理、DLP 防护。

处置方式二：监控与审计—能够提供威胁发现和事后追溯能力。通过部署日志监控、流量分析、行为审计等工具，对云环境中的用户操作行为、网络流量变化等进行实时监测与记录，并依据这些记录开展审计。例如监控到异常登录尝试、数据高频下载等潜在威胁，平台能及时发出告警，并且在安全事件发生后，记录审计能有效地回溯事件发生的全过程。通过监控与审计，企业能精准定位攻击源头、明确责任归属，同时复盘安全漏洞，为后续优化安全策略提供依据。

处置方式七：员工培训—能够提升员工安全意识，降低人为风险的发生。针对员工开展组织性、持续性的网络安全知识与技能培训，

中小企业通过定期组织安全培训课程、案例分享、模拟演练等活动，向员工普及上云安全基础知识，如常见的网络钓鱼邮件识别、弱密码的危害、规范操作准则等，帮助员工掌握安全操作规范。通过培训提高组织安全意识，能减少员工有意或无意的行为所导致的安全隐患，从人员层面筑牢企业上云安全的防线。

处置方式八：执行漏洞管理—能够减少已知漏洞被利用的可能性。通过定期检查云服务器操作系统、核心应用程序的版本信息，关注云服务商发布的漏洞或补丁公告，及时下载修复补丁，确保关键组件无已知漏洞。若资源允许的情况下，企业可通过专业漏洞扫描工具对云上资产主动开展全面扫描，并评估漏洞的危害等级与影响范围，最后通过升级版本、调整配置等方式进行补充修复。通过持续执行漏洞管理，企业能够及时堵住安全缺口，降低黑客利用已知漏洞发起攻击的概率，保障云上业务系统的安全性与稳定性。

处置方式十：执行 DLP 防护—能够及时发现并阻止数据泄露行为。可先评估云服务商提供的基础数据安全功能，利用其内置的策略对云上存储的数据进行初步扫描与分类，并设置关键词告警来进行数据泄露防护。此外，企业可以通过利用专业的 DLP 技术与工具，对云上数据的全生命周期活动进行防护。例如限制非授权人员访问、实时监测文件外发等，一旦检测到未授权传输等违反既定的安全策略的行为，系统会立即发出警报，并自动采取阻断、加密等措施防止数据泄露。通过 DLP 防护的规范执行，企业能全方位加强企业云上数据活动的安全性，降低数据泄漏风险。

第五章 总结

中小企业上云后要利用好自身优势，关注上云安全风险十条，使用安全风险处置十条快速将企业的云安全建设推向安全水位线之上。

中小企业要好好利用自身特质引导云安全向好建设。中小企业与大型企业在组织架构、技术架构、云安全建设目标、供应链中位置、合规响应程度五方面有显著差异，但中小企业可以利用差异特质加速自身云安全建设。一是利用扁平化组织架构加速云安全部署决策；二是使用云服务商提供的云服务时，清晰自身安全责任边界，积极承担相关云上安全工作；三是围绕自身云上业务需求设计安全防护能力，利用云服务商能力构建双活应用，降低单点故障发生产生的影响；四是借助链主安全需求同步提升自身安全合规基础；五是积极关注安全相关法律法规、条款，做好国家强制性要求，在能力范围内满足与自身有关的所有推荐性要求。

按照能解决上云安全风险十条（图 3）的数量以及对应安全风险严峻的程度排序，形成了安全风险处置十条，中小企业可以结合云服务配置实践指南按需落实，图 4 总结了安全风险处置十条及重要性。

图 3 中小企业上云安全风险十条

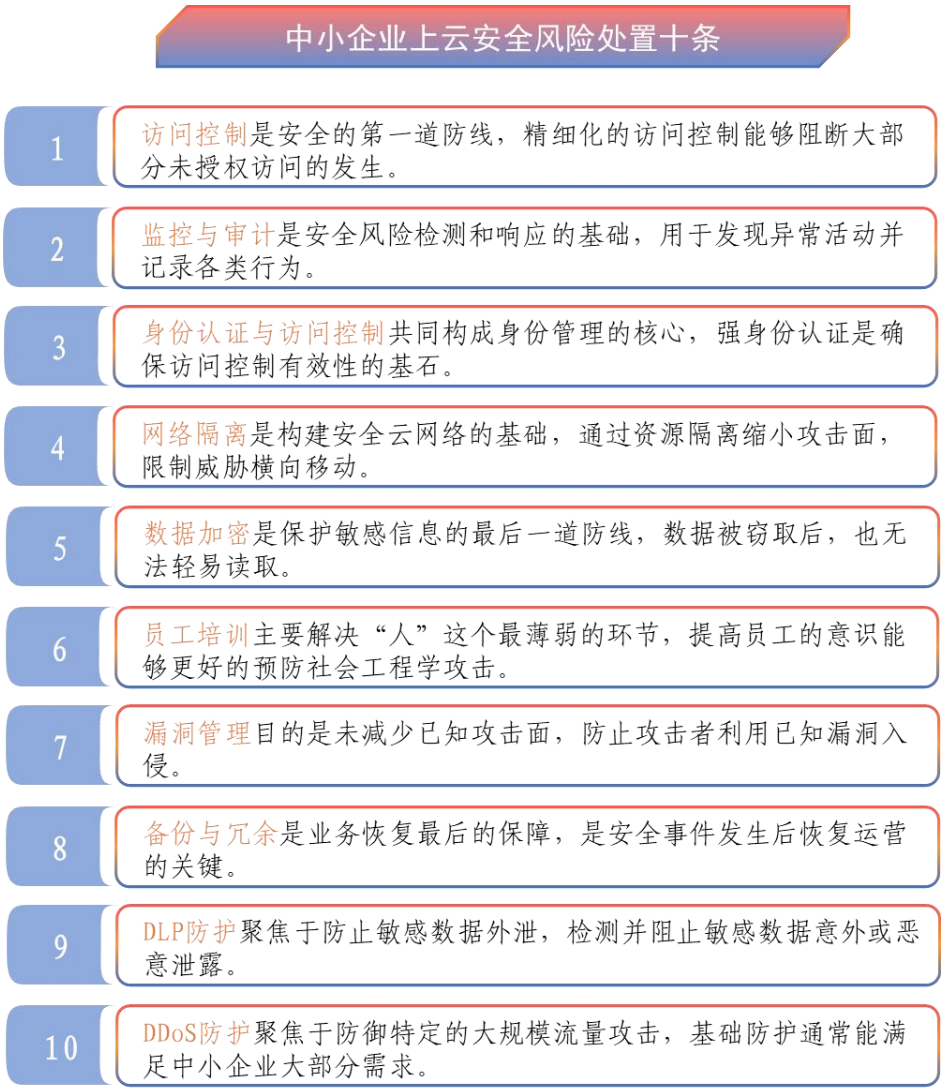
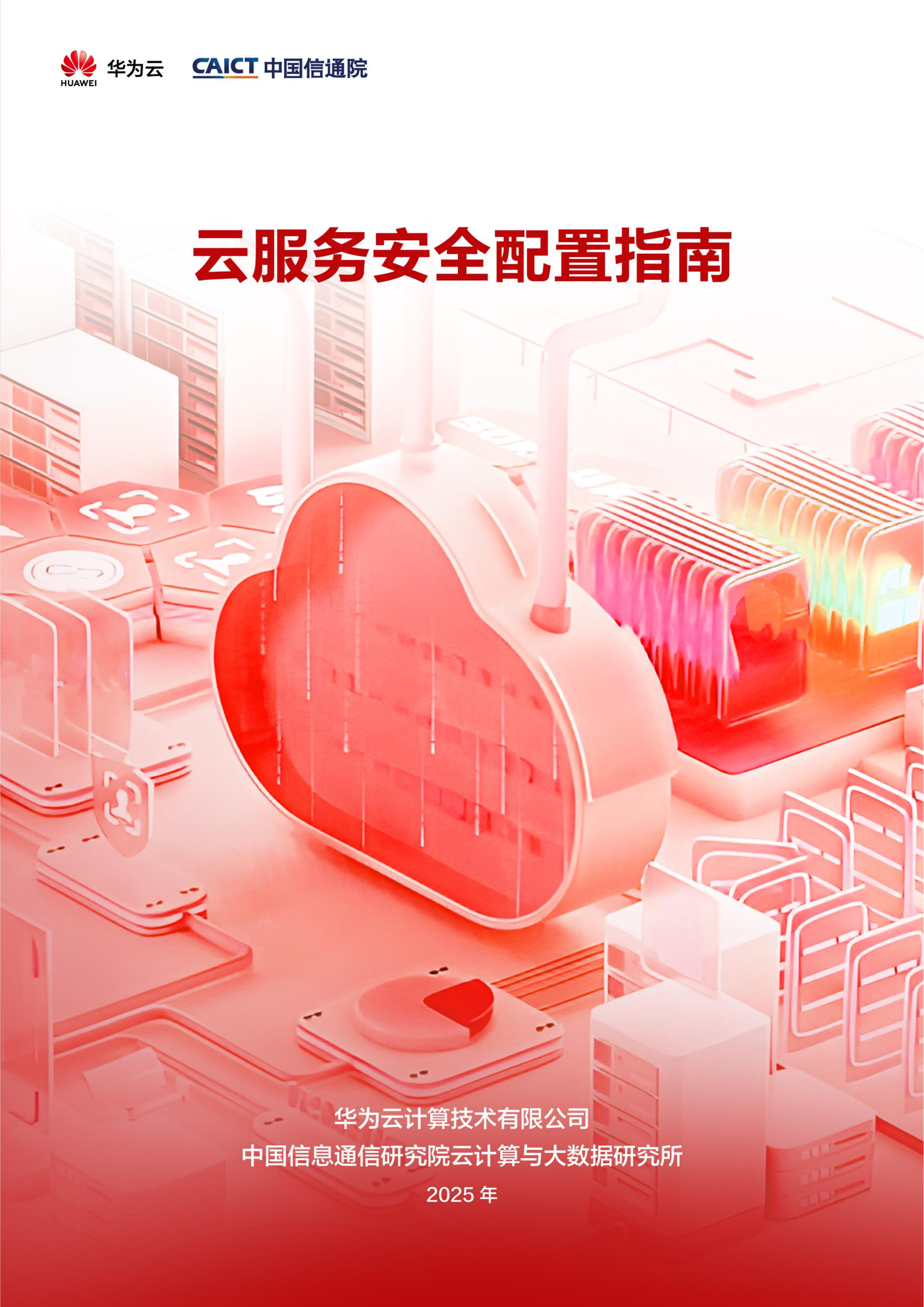


图 4 中小企业上云安全风险处置十条

华为云 HUAWEI CAICT 中国信通院

云服务安全配置指南



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

2025 年

第一章 概述

1.1 原则

云服务安全配置实践指南（简称“实践指南”）以重点云服务为对象，以解决“中小企业上云安全风险十条”为建设目标，以“中小企业上云安全风险处置十条”为实施路径，梳理头部云服务商安全配置实践，结合现有行业标准规范，识别出云服务在两个“十条”大纲下更细化的安全配置指引，形成行业通用、可落地操作的云服务安全配置共识文件。根据云服务使用普及程度和安全需求情况，实践指南覆盖计算、存储、数据库、日志与监控、网络、企业应用等方面的安全配置。

1.1.1 使用建议

云服务安全配置实践指南提供一套实用且易于遵循的安全配置框架，助力构建更安全的云计算环境，适用于为中小企业在云平台建设、使用和维护过程中提供安全配置参考。

实践指南并不是所有可能的安全配置的详尽列表，建议客户将本指南作为一个起点，并根据实际需要在此基础上进行补充或裁剪。

1.1.2 规则定义

指南给出不同云服务的精细化安全配置参考，每项实践细则均包含处置十条、安全效果、检查方法和配置方法等四部分，各部分内容描述如下：

- 处置十条：描述该配置项对应处置十条的内容

- 安全效果：描述该项的配置原因以及安全效果
- 检查方法：描述用户查看当前安全配置的操作方法
- 配置方法：给出具体操作步骤，引导用户进行安全配置

第二章 配置指南

2.1 身份访问与管理

2.1.1 开启多因子认证

处置十条	[1]访问控制
安全效果	用户登录控制台时除需要提供用户名和密码外，还需提供其他形式验证码，只有全部验证通过才能获得访问权限，提升了身份验证的准确性和安全性
检查方法	1、 使用管理员账号登录控制台； 2、 通过用户中心或产品列表进入统一身份认证/访问控制界面； 3、 检查安全设置中是否已开启除登录密码以外的其他验证方式。
配置方法	1、 使用管理员账号登录控制台； 2、 通过用户中心或产品列表进入统一身份认证/访问控制界面； 3、 进入安全设置中“多因子认证”板块； 4、 选择合适的验证方式（推荐使用 MFA、手机验证）； 5、 按照提示进行首次验证，完成开启多因子认证功能。

2.1.2 密码策略配置

处置十条	[1]访问控制、[3]身份认证
安全效果	密码策略强制用户使用特定的密码规则（如密码复杂度、更换周期等），增加账号密码体系攻击者破解的难度，从而降低用户账号和云平台被恶意访问的风险
检查方法	1、 使用管理员账号登录控制台； 2、 通过用户中心或产品列表进入统一身份认证/访问控制界面； 3、 检查安全设置中“密码策略”板块相关策略是否配置。

配置方法	1、 使用管理员账号登录控制台； 2、 通过用户中心或产品列表进入统一身份认证/访问控制界面； 3、 进入安全设置中“密码策略”板块进行配置： （1） 密码复杂度配置：选中大写字母、小写字母、数字、特殊字符复选框中的至少 3 项，最小长度不小于 8 字符； （2） 密码有效期配置：限制密码最长使用时间（建议不超过 180 天）； （3） 历史密码重复配置：限制新密码不能与最近的历史密码相同（建议重复次数设置为 3）； （4） 登录失败处理配置：限制登录验证失败次数，超出限制后锁定当前账户一段时间。

2.1.3 访问权限策略配置

处置十条	[1]访问控制、[5]网络隔离
安全效果	通过访问权限策略限制具有特定属性的用户访问云平台，并遵循最小权限原则，仅赋予用户完成工作所需的最低限度权限，避免权限过度集中与滥用
检查方法	1、 使用管理员账号登录控制台； 2、 通过用户中心或产品列表进入统一身份认证/访问控制界面； 3、 进入“用户”板块，检查每个用户账号是否绑定符合工作所需的访问权限。
配置方法	1、 使用管理员账号登录控制台； 2、 通过用户中心或产品列表进入统一身份认证/访问控制界面； 3、 进入“用户”板块，根据用户需求添加相应权限，并删除不必要的权限， 4、 如需自定义权限策略，进入“权限管理”板块，选择新建策略： （1） 如通过可视化视图创建，按照所需最小范围选择服务、操作、资源和条件策略； （2） 如通过脚本视图创建，应确保不使用“*”代替参数值，并检查语法是否有误。

2.1.4 敏感操作保护

处置十条	[1]访问控制、[3]身份认证
安全效果	用户在进行敏感操作或重要操作时，云平台应启用二次验证机制，通过 MFA、短信认证等方式确保用户身份合法且操作无误
检查方法	1、 使用管理员账号登录控制台； 2、 通过用户中心或产品列表进入统一身份认证/访问控制界面； 3、 检查安全设置中“敏感操作保护”相关功能是否开启。
配置方法	1、 使用管理员账号登录控制台； 2、 通过用户中心或产品列表进入统一身份认证/访问控制界面； 3、 进入安全设置中“敏感操作保护”板块，开启相关功能； 4、 根据用户需求配置验证方式和保护范围： （1） 推荐使用 MFA、短信验证方式； （2） 建议覆盖云平台支持的全部敏感操作类型。

2.1.5 用户管理安全配置

处置十条	[1]访问控制、[3]身份认证
安全效果	降低子用户自主管理访问控制相关功能的范围，仅管理员账号可修改涉及高安全风险的 IAM 功能，如子用户授权、创建密钥、重置密码等内容
检查方法	1、 使用管理员账号登录控制台； 2、 通过用户中心或产品列表进入统一身份认证/访问控制界面； 3、 检查安全设置中“子用户管理”相关板块配置情况。
配置方法	1、 使用管理员账号登录控制台； 2、 通过用户中心或产品列表进入统一身份认证/访问控制界面； 3、 进入安全设置中“子用户管理”相关板块进行配置： （1） 不允许用户自主管理密钥； （2） 不允许用户自主修改用户信息； （3） 建议按需关闭其他选项，最小化子用户权限。

2.2 计算安全

2.2.1 密钥安全登录

处置十条	[1]访问控制、[3]身份认证
安全效果	用户远程登录云服务器时使用云平台生成的密钥对代替用户名/密码验证，防止由于密码被拦截、破解造成的信息泄露，从而提高云服务器的安全性
检查方法	1、 登录控制台； 2、 进入云服务器管理界面，在导航栏中选择密钥对； 3、 查看是否已创建密钥对并绑定云服务器，确认用户是否已保存密钥私钥。
配置方法	1、 登录控制台； 2、 进入云服务器管理界面，在导航栏中选择密钥对； 3、 选择创建密钥对，根据需要填写名称、密钥内容等信息（或导入已有密钥对）； 4、 确认创建密钥对，浏览器将提示下载私钥文件，用户仅有一次下载机会，请确认妥善保管； 5、 选择已创建的密钥对，绑定目标云服务器实例（原有的用户名/密码登录方式可能失效，请留意提示信息）； 6、 重启目标云服务器实例，使用已下载的密钥私钥进行登录，确认是否配置成功。

2.2.2 虚拟机防火墙配置

处置十条	[5]网络隔离、[8]漏洞管理
安全效果	保持虚拟机防火墙服务开启，监控虚拟机出入网络流量，降低网络攻击风险
检查方法	#以 CentOS 7 为例# 1、 使用管理员账号登录云服务器； 2、 输入命令<systemctl status firewalld>查看防火墙是否为运行中： （1） 返回<active (running)>为运行中； （2） 返回<inactive (dead)>为已停止； 3、 输入命令<systemctl is-enabled firewalld >查看防火墙服务是否开机自启： （1） 返回<enabled>为自启； （2） 返回<disabled>为不自启。
配置方法	1、 使用管理员账号登录云服务器；

	2、 输入命令<systemctl start firewalld>开启防火墙服务（无返回值）； 3、 输入命令<systemctl enable firewalld>设置开机自启（可能返回<Created symlink>信息）； 4、 根据上述检查方法再次确认是否配置成功。

2.2.3 虚拟机日志与审计服务配置

处置十条	[2]监控与审计
安全效果	保持虚拟机系统日志和审计服务开启，监控安全事件、跟踪非法访问和操作，并为合规性审计提供重要数据
检查方法	#以 CentOS 7 为例# 1、 使用管理员账号登录云服务器； 2、 输入命令<systemctl status rsyslog>查看系统日志服务是否为运行中，输入命令<systemctl status auditd>查看审计服务是否为运行中： （1） 返回<active (running)>为运行中 （2） 返回<inactive (dead)>为已停止； 3、 输入命令<systemctl is-enabled rsyslog>查看系统日志服务是否开机自启，输入命令<systemctl is-enabled auditd>查看审计服务是否开机自启： （1） 返回<enabled>为自启； （2） 返回<disabled>为不自启。
配置方法	1、 使用管理员账号登录云服务器； 2、 配置系统日志服务： （1） 输入命令<systemctl start rsyslog>开启系统日志服务（无返回值）； （2） 输入命令<systemctl enable rsyslog>设置开机自启（可能返回<Created symlink>信息）； 3、 配置审计服务： （1） 输入命令< systemctl start auditd>开启系统日志服务（无返回值）； （2） 输入命令< systemctl enable auditd>设置开机自启（可能返回<Created symlink>信息）； 4、 开启根据上述检查方法再次确认是否配置成功。

2.2.4 软件更新

处置十条	[8]漏洞管理
安全效果	软件和服务定期发布版本更新，可能包括已知漏洞安全补丁、依赖库更新、系统性能优化等，及时下载更新能够保持操作系统安全性、可用性
检查方法	#以 CentOS 7 为例# 1、 使用管理员账号登录云服务器； 2、 输入命令< yum check-update>查看是否有待更新项。
配置方法	1、 使用管理员账号登录云服务器； 2、 输入命令<yum update>安装可更新的内容； 3、 建议每个月执行一次。

2.3 存储安全

2.3.1 对象存储安全配置

2.3.1.1 存储加密

处置十条	[4]数据加密
安全效果	启用存储桶的服务端加密，用户在上传对象时，数据会在服务端加密成密文后存储，降低存储内容泄漏风险
检查方法	1、 登录控制台； 2、 进入对象存储管理界面，选择目标存储桶； 3、 在存储桶概览界面中选择“基础配置”，检查“默认加密”是否为“已配置”状态。
配置方法	1、 登录控制台； 2、 进入对象存储管理界面，选择待操作的存储桶； 3、 在存储桶概览界面中选择“基础配置”，开启“默认加密”功能； 4、 选择服务端加密“SSE-KMS”或“SSE-OBS”； 5、 选择合适的加密算法和加密密钥，或创建新的加密密钥； 6、 确认操作，完成配置。

2.3.1.2 访问安全

处置十条	[1]访问控制、[5]网络隔离
安全效果	通过禁止匿名访问、使用安全协议、开启防盗链等方式提高存储桶访问过程的安全性
检查方法	1、 登录控制台； 2、 进入对象存储管理界面，选择目标存储桶； 3、 匿名访问：在存储桶概览界面中选择“访问权限控制”，检查“桶 ACLs”是否配置公共权限为“公共读”或“公共读写”，用户权限是否授权给匿名用户； 4、 安全协议：在存储桶概览界面中选择“访问权限控制”，检查“桶策略”中 SecureTransport 是否配置为 True； 5、 防盗链：在存储桶概览界面中选择“防盗链”，查看防盗链“白名单 Referer”/“黑名单 Referer”配置信息。
配置方法	1、 登录控制台； 2、 进入对象存储管理界面，选择待操作的存储桶； 3、 匿名访问； 4、 安全协议：在存储桶概览界面中选择“访问权限控制”，在“桶策略”中修改“SecureTransport”配置为 True； 5、 防盗链：在存储桶概览界面中选择“防盗链”，根据规则填写合适的参数： （1） 白名单 Referer：允许来自列表中的网站的请求访问，否则将拦截 （2） 黑名单 Referer：不允许来自列表中的网站的请求访问，否则将放行； （3） 空 Referer：通过浏览器地址栏直接访问资源的请求（建议设置为不允许）。

2.3.1.3 版本安全

处置十条	[6]备份与冗余、[9]DLP 数据防丢失
安全效果	版本控制适合需留存变更记录的存储对象，保留存储对象的多个版本，提升数据异常场景快速恢复能力； WORM 策略适合仅支持读取不支持删除和修改的存储对象，可以确保指定时间内不能覆盖或删除指定对象版本，避免因数据篡改、丢失或恶意删除造成的损失。
检查方法	1、 登录控制台； 2、 进入对象存储管理界面，选择目标存储桶；

	3、 版本控制：在存储桶概览界面中查看“多版本控制”功能是否启用； 4、 WORM：在存储桶概览界面中查看是否支持“WORM 保留策略”并且已配置。
配置方法	1、 登录控制台； 2、 进入对象存储管理界面，选择待操作的存储桶； 3、 版本控制：在存储桶概览界面中选择“多版本控制”并启用，在不需要版本控制时可暂停功能； 4、 WORM：在存储桶概览界面中选择“WORM 保留策略”，配置保留策略和保留期限（如不支持，可能是存储桶创建时未选择该功能）。

2.3.2 云硬盘加密配置

处置十条	[4]数据加密
安全效果	存储保密性要求较高的业务数据应选择加密的云硬盘，使用加密算法对数据在存储层进行静态加密，即使硬盘物理损坏或被非法获取，未授权者也无法读取原始数据。
检查方法	1、 登录控制台； 2、 进入云硬盘管理界面，选择磁盘列表； 3、 查看目标云硬盘是否加密。
配置方法	1、 登录控制台（多数云硬盘仅支持在创建时进行加密，已有云硬盘无法直接加密）； 2、 进入云服务器或云硬盘管理界面，新建资源； 3、 在云硬盘创建界面选中“加密”，并选择加密密钥，如无加密密钥可通过 KMS 服务创建； 4、 如需加密已有硬盘中的内容，可对挂载目标云硬盘的云服务器创建“私有镜像”，使用该镜像重新创建云服务器，并确保创建时云硬盘“加密”功能已选中。

2.3.3 云备份安全配置

2.3.3.1 备份加密

处置十条	[4]数据加密、[6]备份与冗余
安全效果	云备份通过多地存储实现数据冗余，支持快速恢复以减少业务中断损失，确保备份数据加密能更进一步提升数据安全性和业务连

	续性。
检查方法	1、 登录控制台； 2、 进入云备份管理界面，选择备份目录； 3、 进入目标备份的详情信息，查看绑定的磁盘是否为加密盘。
配置方法	1、 登录控制台（多数云硬盘仅支持在创建时进行加密，已有云硬盘无法直接加密）； 2、 进入云备份管理界面，新建备份存储库； 3、 存储库需绑定云硬盘，在创建界面选中“加密”，并选择加密密钥，如无加密密钥可通过 KMS 服务创建。

2.3.3.2 备份锁定

处置十条	[6]备份与冗余、[9]DLP 数据防丢失
安全效果	开启云备份锁定或 WORM 功能，数据在写入后无法被修改或删除，满足企业合规审计要求，并防止重要数据被误删或恶意删除。
检查方法	1、 登录控制台； 2、 进入云备份管理界面，选择备份目录； 3、 查看目标存储库的详情信息，检查是否开启备份锁定。
配置方法	1、 登录控制台； 2、 进入云备份管理界面，选择备份目录； 3、 进入需要开启锁定的目标存储库的详情信息，选择开启备份锁定（开启锁定后无法关闭）。

2.4 数据库安全

2.4.1 加密通信配置

处置十条	[4]数据加密
安全效果	云数据库的传输层加密协议是保障数据在传输过程中安全性的重要技术手段，用户通过互联网访问数据库资源时，数据在客户端与服务器之间以密文形式传输，避免传输过程中被窃听。
检查方法	1、 登录控制台； 2、 进入云数据库管理界面，选择目标数据库实例； 3、 查看云数据库基本信息界面，检查是否开启 SSL 连接。
配置方法	1、 登录控制台； 2、 进入云数据库管理界面，选择目标数据库实例；

	3、 进入云数据库基本信息界面，选择开启 SSL 加密（可根据需要选择加密链路和证书）。

2.4.2 避免绑定公网 IP

处置十条	[5]网络隔离
安全效果	将云数据库实例部署在内网环境中，避免绑定公网地址，用户不能通过互联网直接访问资源，以防止未授权的访问或 DDos 攻击等风险。
检查方法	1、 登录控制台； 2、 进入云数据库管理界面，选择目标数据库实例； 3、 查看云数据库网络连接基本信息，检查是否绑定 EIP。
配置方法	1、 登录控制台； 2、 进入云数据库管理界面，选择目标数据库实例； 3、 进入云数据库基本信息界面，解绑对应的 EIP； 4、 根据需要配置合适的内网 IP。

2.4.3 修改数据库默认端口

处置十条	[7]DDoS 防护
安全效果	数据库默认端口容易受到监听和攻击，修改默认端口为非常用端口，能够提高数据库服务安全性，同时可以避免端口冲突。
检查方法	1、 登录控制台； 2、 进入云数据库管理界面，选择目标数据库实例； 3、 查看云数据库连接信息中“数据库端口”部分，检查绑定端口是否为默认端口（常见默认端口：MySQL/3306、PostgreSQL/5432、Redis/6379、MongoDB/27017）。
配置方法	1、 登录控制台； 2、 进入云数据库管理界面，选择目标数据库实例； 3、 进入云数据库连接信息中“数据库端口”部分，根据需要修改默认端口（建议修改为不常用端口，避免使用其他服务默认端口和系统占用端口）。

2.4.4 密码策略配置

处置十条	[1]访问控制、[3]身份认证
安全效果	密码策略强制用户使用特定的密码规则（如密码复杂度、更换周期等），增加账号密码体系攻击者破解的难度，从而降低用户账

	号和数据库被恶意访问的风险。
检查方法	1、 登录控制台； 2、 进入云数据库管理界面，选择目标数据库实例； 3、 进入云数据库“账号管理”板块，查看账号配置是否符合业务需求，以及对应密码是否过于简单。
配置方法	1、 登录控制台； 2、 进入云数据库管理界面，选择目标数据库实例； 3、 进入“账号管理”板块，根据需求创建新账号或对已有账号重置密码，新密码应满足以下要求： （1） 密码复杂度配置：选中大写字母、小写字母、数字、特殊字符复选框中的至少 3 项，最小长度不小于 8 字符； （2） 密码不能与账号名相同； （3） 不同账号应使用不同密码； （4） 定期修改密码（建议不超过 180 天）。

2.4.5 备份策略配置

处置十条	[6]备份与冗余
安全效果	定期对云数据库进行备份，当数据库故障或数据损坏时，可以通过备份文件恢复数据库，从而保证数据可靠性。
检查方法	1、 登录控制台； 2、 进入云数据库管理界面，选择目标数据库实例； 3、 进入云数据库“备份恢复”板块，查看是否已配置备份策略。
配置方法	1、 登录控制台； 2、 进入云数据库管理界面，选择目标数据库实例； 3、 进入“备份恢复”板块，开启备份策略（一般为同区域备份），按需选择备份时段（建议选择非业务高峰期）、备份周期、备份保留天数等； 4、 如需进一步提高数据安全性，建议开启跨区备份功能，用户需提前在目标区域开通存储服务。

2.5 日志与监控安全

2.5.1 云审计服务配置

处置十条	[2]监控与审计

安全效果	云日志审计服务能够关联云平台上各类云产品，追踪当前用户操作记录并整合，服务具备对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。
检查方法	1、 登录控制台； 2、 进入云审计服务管理界面； 3、 查看是否开通云审计服务，通过导航栏窗格进入“事件列表”，检查是否存在事件数据。
配置方法	1、 登录控制台； 2、 进入云审计服务管理界面，开通云审计服务； 3、 记录的事件信息在云审计服务中留存时间有限，为长期留存相关数据，可配置云审计事件转储至对象存储： （1） 通过导航栏窗格进入追踪器页面，开启转储功能； （2） 选择存储位置和目标； （3） 配置保存周期和安全措施； （4） 可在目标“追踪器”页面查看转储的内容。

2.5.2 云日志服务配置

处置十条	[2]监控与审计、[6]备份与冗余
安全效果	云日志服务支持各类云产品和云服务日志的接入，支持大规模日志检索、统计和可视化，帮助用户进行风险分析和安全告警。
检查方法	1、 登录控制台； 2、 进入云日志服务管理界面； 3、 查看是否开通云日志服务，以及关键业务资源是否接入云日志服务。
配置方法	1、 登录控制台； 2、 进入云日志服务管理界面，开启云日志管理服务； 3、 为云服务开启云日志服务：建议将关键业务涉及的云服务接入云日志服务统一管理： （1） 建议接入的云服务包括但不限于云服务器、VPC、负载均衡、云数据库、云 WAF 等； （2） 进入对应的云服务管理界面，选择目标实例的日志板块进行配置，不同产品功能名称可能不同，一般为“日志管理”、“流日志”、“日志审计”等。 4、 确保日志存储时长符合要求：进入“日志管理”板块，选择对应的日志组，根据业务需求修改“日志存储时长”； 5、 启用日志转储：需长期留存的日志可转储至对象存储，进入“日志转储”板块，配置相关参数，转储任务状态为“正常”时，表示转储任务创建成功。

2.6 网络安全

2.6.1 限制 SSH 远程访问

处置十条	[7]DDoS 防护
安全效果	SSH 协议提供远程连接并管理主机的功能，在网络攻击中经常作为资源扫描和暴力破解的入口，通过限制 SSH 协议访问，避免端口暴露公网，能够提升云资源的访问安全性。
检查方法	1、 登录控制台； 2、 进入网络管理界面，选择 VPC 板块； 3、 在访问控制列表中选择对应的 ACL 或安全组,查看详情界面； 4、 检查安全规则是否配置了源地址为 0.0.0.0/0 或::/0 的 SSH 协议规则； 5、 检查默认端口 22 端口相关的配置源地址是否合规。
配置方法	1、 登录控制台； 2、 进入网络管理界面，选择 VPC 板块； 3、 在访问控制列表中选择对应的 ACL 或安全组,查看详情界面； 4、 在“入方向规则”页签进行配置，根据界面提示修改相关参数，建议使用白名单放通规则，并配置源地址为特定 IP 或 IP 段。

2.6.2 避免管理端口和高危端口暴露

处置十条	[7]DDoS 防护
安全效果	为方便用户管理，部分云服务支持向公网开放远程端口，端口被非法利用将对云平台和业务系统造成严重威胁。一般情况下，可避免开放对外远程管理端口和高危端口，如业务必需，应根据最小化开放原则执行。
检查方法	1、 登录控制台； 2、 进入网络管理界面，选择 VPC 板块； 3、 在访问控制列表中选择对应的 ACL，查看详情界面； 4、 检查安全规则是否开放了高危端口，以及高危端口入方向 IP 配置是否遵循最小化开放原则： （1） 常见高危端口包括：20、21、135、137、138、139、445、389、593、1025； （2） 常见远程管理端口包括：23、177、513、3389、4899、6000-6063、5900、5901。
配置方法	1、 登录控制台； 2、 进入网络管理界面，选择 VPC 板块； 3、 在访问控制列表中选择对应的 ACL，查看详情界面；

	4、 在“入方向规则”页签进行配置，关闭不必要的管理端口和高危端口，并对必须开放的端口配置业务所需特定 IP 或最小的 IP 段。

2.6.3 对等连接最小化配置

处置十条	[5]网络隔离
安全效果	VPC 对等连接实现跨地域 VPC 之间的私网互通，限制对等连接的网段范围，避免非必要的私网访问，能够有效减少因权限配置不当造成的数据和隐私泄露。
检查方法	1、 登录控制台； 2、 进入网络管理界面，选择 VPC 板块； 3、 通过导航栏窗格进入“对等连接”详情界面； 4、 检查是否配置相关功能，配置范围是否符合业务需求。
配置方法	1、 登录控制台； 2、 进入网络管理界面，选择 VPC 板块； 3、 通过导航栏窗格进入“对等连接”详情界面： 4、 在对等连接列表中，修改目标对等连接的子网范围和其他参数，并删除不必要的对等连接。

2.7 企业应用安全

2.7.1 云上应用安全防护配置

处置十条	[7]DDoS 防护、[10]员工培训
安全效果	企业在云上搭建软件平台、业务系统、云上网站等应用，应确保其应用层面的安全性，使用应用防护产品、规范化应用安全配置，避免应用遭受网络攻击。
检查方法	1、 登录控制台； 2、 进入目标应用； 3、 查看是否具备应用安全防护措施，如接入应用安全防护产品、应用层安全认证、应用访问控制限制等；
配置方法	1、 登录控制台； 2、 进入目标应用，可根据需求使用以下防护措施： （1） 在 web 服务器前部署云 web 应用防火墙产品，开启云 WAF 服务，将云上应用接入云 WAF，配置相应安全策略； （2） 对 API 接口启用令牌认证，设置请求频率限制，防止暴力破解和 DDoS 攻击；

	（3） 对 Serverless 资源设置 VPC 内网访问，禁止公网直接调用，通过 API 网关统一管理访问权限。

2.7.2 第三方资源安全配置

处置十条	[8]漏洞管理、[10]员工培训
安全效果	企业因业务需要可能涉及使用非云平台提供的镜像、代码库、数据包等资源，在导入和使用第三方资源或开源资源前，应进行安全扫描，审查资源来源，避免存在未知的漏洞和后门威胁。
检查方法	1、 登录控制台； 2、 查看目标资源的成分、来源、内容等是否符合业务要求； 3、 检查云平台对第三方资源的授权范围、安全监控、安全协议等是否合规。
配置方法	1、 登录控制台； 2、 使用（云平台提供的）安全检测工具（如云安全中心、数据安全中心的）对第三方资源进行安全检测； 3、 根据业务需要配置定期扫描策略等。

2.7.3 第三方应用安全配置

处置十条	[8]漏洞管理、[10]员工培训
安全效果	企业因业务需要可能涉及使用非云平台提供的软件、组件、程序等应用，在安装和使用第三方应用或开源应用前，应进行安全检查和配置，限制应用使用范围，避免存在未知的漏洞和后门威胁。
检查方法	1、 登录控制台或第三方应用； 2、 检查第三方应用自身安全配置是否合规； 3、 检查云平台对第三方应用的授权范围、安全监控、安全协议等是否合规。
配置方法	1、 登录控制台或第三方应用； 2、 参考上文章节，开展第三方应用涉及的身份访问与管理、日志与监控、业务系统安全管理等配置。

若您对本报告有任何建议，
请联系：wushihao@caict.ac.cn