2024.07

工业领域云安全实践指南

中国通信标准化协会 云计算标准和开源推进委员会
西门子（中国）有限公司
合作发布

云计算标准和开源推进委员会

SIEMENS

版权声明

序　言

胡建钧

副总裁兼首席网络与信息安全官

西门子（中国）有限公司

近年来，随着“十四五”规划的深入推进，工业与新一代信息技术的融合发展步入快车道。云计算作为数字化转型的基石，为工业企业带来了前所未有的机遇，同时也带来了新的安全挑战。如何有效保障工业企业上云安全，已成为业界关注的焦点。

然而，工业领域上云后的安全体系建设尚处于探索阶段，缺乏系统性的指导文件。本指南正是在此背景下应运而生，旨在为工业企业构建安全可靠的云环境提供参考和借鉴。

本指南立足于工业上云的实际需求，从政策解读、风险挑战、安全模型、实践案例等多个维度，全面阐述了工业领域云安全建设的核心理念和关键举措。指南不仅对云安全治理、组织架构、技术体系、运营流程、生态建设等方面进行了深入分析，还结合上云前、中、后不同阶段，提供了详细的参考实践，具有很强的指导性和可操作性。

本指南的发布，是西门子践行“网络安全为数字化旅程保驾护航”理念的又一重要体现。西门子坚信，数字化世界的发展离不开网络安全，也积极参与到构建安全网络空间的行动中，并与多方全球生态合作伙伴共同发起了“信任宪章”，在中国依托“西安社”这一生态社群

平台，链接本地合作伙伴与客户，致力于提升网络安全意识，制定清晰的网络安全义务，共同推动网络安全行业发展。希望本指南能够为广大工业企业提供有益参考，助力企业安全、合规、高效地利用云计算技术，加速数字化转型进程，为实现高质量发展提供加速度，注入新动能！

目 录

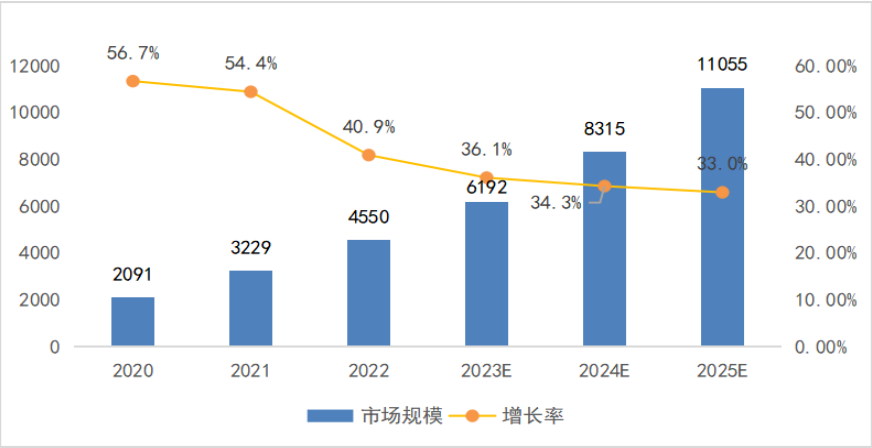
图 目 录

一、数字化转型浪潮袭来，工业上云势头日益增强

近年来，随着工业领域数字化转型不断深化，利用云计算进行技术革新、业务按需快速定制等带来的效率提升和成本优势愈发凸显，上云成为企业实现可持续发展目标的关键，通过培育新质生产力，大力推进新型工业化进程。

（一）上云政策与云计算的蓬勃发展协同驱动工业企业上云

我国云计算市场呈稳定增长态势，细分领域 PaaS、SaaS 增长潜力大。据中国信通院《云计算白皮书（2023 年）》显示，2022 年我国云计算市场规模达到 4550 亿元人民币，较 2021 年增长 40.9%，全球云计算市场同期增速为 19%，与其相比，我国云计算市场处于快速发展期，预计 2025 年将突破万亿元大关。细分领域中，2022 年公有云 IaaS、PaaS 和 SaaS 市场增速分别为 51.21%、74.49%和 27.57%，其中，PaaS 市场受容器、微服务等云原生应用带来的刺激，增长强势，结合人工智能大模型等发展趋势，未来几年将成为增长主战场。



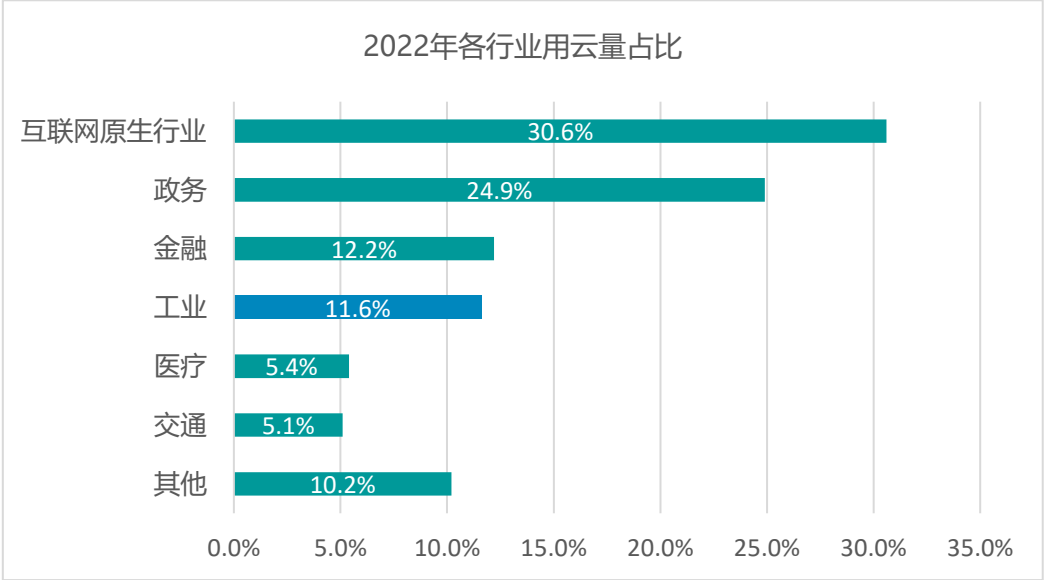
数据来源：中国信息通信研究院

图 1 我国云计算市场规模及增速（市场规模单位：亿元）

我国工业上云利好政策持续释放。一方面，工业互联网顶层设计不断完善。工业互联网是新一代信息技术与工业系统深度融合的产物，云计算是新一代信息技术变革的重要支撑，工业上云为工业互联网向好发展提供强有力驱动。2017 年国务院印发《关于深化“互联网+先进制造业”发展工业互联网的指导意见》，成为推动我国工业互联网发展的纲领性文件。2020 年 12 月，工业和信息化部发布的《工业互联网创新发展行动计划（2021-2023 年）》中指出，要加快工业设备和业务系统上云上平台，到 2023 年工业企业及设备上云数量比 2020 年翻一番，以推动工业互联网发展。**另一方面，全国各地方接连推出工业企业上云政策，加速工业企业数字化转型。一是多省市推出工业企业上云行动计划。**为支持工业领域数字化转型，促进工业经济高质量发展，我国多省市工信厅印发工业企业“上云上平台”工作方案和行动计划，明确年度工业企业上云数量等要求。**二是全国各地加码工业企业上云资金投入，鼓励地方工业企业上云。**各省市通过“云使用券”补助、事后奖补以及评级奖励等方式，为购买基础设施类、平台系统类和业务应用类云服务的工业企业提供实质资金补贴。

云计算引发工业深刻变革，工业上云需求涌现。我国 2022 年工业行业用云量占比可观，中国信通院发布的《2022 年中国云计算发展指数》显示，中国云计算应用已从互联网拓展至传统行业，2022 年工业用云量占比已达到 11.6%，已成为继互联网原生行业、政务与金融行业的第四大上云行业。工业对云计算的需求来自三方面：**一是敏捷、灵活的研发需求。**云计算引发软件研发范式变革，**一方面，**随着应用

从单体架构向微服务架构转变，越来越多工业软件希望通过更敏捷的方式进行研发，拆分独立任务并以用户需求为导向快速响应需求变化。**另一方面，**随着云原生等新兴技术的逐步成熟，工业 PaaS 平台和 SaaS 应用得以发展，希望面向公众提供灵活的工业开发平台和丰富的工业应用模板。**二是生产方式与先进技术结合需求。一方面，**在传统的工业生产流程中，数据获取依赖于人工或传感器采集，其数据分析处理能力有限。工业企业希望使用弹性的计算与存储能力支持更多、更复杂的数据处理工作，配合数据挖掘和机器学习算法，令数据的价值得到发挥。**另一方面，**传统工业生产流程中设备的监控通常需要使用专用硬件，成本高且难以大规模部署。工业企业希望将智能设备、传感器等联网以实现远程监控，通过实时监控和数据分析，实现生产流程的动态优化。**三是工业服务提供方式从线下向线上转变需求。**工业的主要特性是提供生产服务，传统的线下服务是重要组成部分，包括设备调试、生产线的巡检、故障排查、咨询培训等，但线下方式需要较高的人工成本，且没有标准化的服务流程，极大地限制了服务效率与质量管理。因此，工业企业希望将工业服务从线下向线上转移，通过远程的方式提供标准化的服务流程，以保障生产的稳定性和连续性。



数据来源：中国信息通信研究院

图 2 2022 年各行业用云量占比

（二）工业上云为企业提供动能，助力企业创新发展

1、 工业上云促进企业 IOT 要素全面升级

云计算作为融合技术和行业应用的核心平台，加速推动汽车、钢铁、能源等传统行业生产要素和生产环节的数字化进程，从基础设施灵活性、生产效率和管理质量三方面提升企业核心竞争力，大力推进工业现代化体系建设，加速新质生产力发展。

一是云计算为大规模工业应用软件提供强大计算与存储能力，提升基础设施的可扩展性和灵活性。随着工业领域的业务复杂性和多样性的增加，工业应用软件需求不断增长。一方面，传统 IT（Information Technology，信息科技）系统需要大量的软硬件投入，而云计算可以按需提供弹性的计算与存储能力，满足工业应用对资源的及时需求。另一方面，云计算可以支持 OT（Operational Technology，运营技术）应用和服务的运转，如工业自动化、工业作业监控和设备实况监测等，

从而提升 OT 系统的效能。

二是云计算为工业系统提供强大的数据处理和分析能力，促进 IT 与 OT 集成和协同。在工业生产过程中，大量工业设备与传感器互连，实时交换共享海量工业数据，云计算因其分布式与边缘化特性，可以在网络边缘提供强大的数据处理和分析能力，支持工业设备的连通与数据价值的挖掘，帮助企业实现数据共享和流程协同，优化生产效率。

三是云计算加速工业技术、经验和知识的沉淀，提升管理水平。云计算支持将大量的工业技术原理、行业知识、模型工具等封装成为微服务组件，以规则化、软件化、模型化的形式供开发者使用，同时提供资源管理、服务编排、工程管理等服务，通过集中化的管控提升管理质量。

2、 工业上云激发数据要素价值释放

工业互联网的高速发展正推动制造业从传统生产要素驱动向数据要素驱动转变，加速数据要素投入生产的三次价值释放[1]。

一是业务数据上云支撑业务贯通，满足生产需求并提升业务运行效率。业务数据上云属于工业企业上云的第三阶段，在经历了基础设施上云和设备上云之后，这一阶段企业的关键目标是深入挖掘业务需求，为企业创造价值。随着工业发展，无论是离散行业、流程行业或是混合行业，PLC, DCS（Distributed Control System，集散控制系统）和 SCADA（Supervisory Control And Data Acquisition，数据采集与监视控制系统）所需控制的数据体量越来越大，例如汽车生产、机械制

[1] http://www.caict.ac.cn/kxyj/qwfb/bps/202301/t20230107_413788.htm，《数据要素白皮书（2022 年）》

造、制药、食品生产等企业运营过程中，会产生大量、高价值数据，然而传统工控系统仅将生产指标数据用作监控，数据价值未被充分挖掘，提升数据价值成为业务刚需，从而催生工业边缘实现数据的云边协同，在现场即可处理大量数据满足生产需求，并将数据传输至数据中心加以分析，优化业务流程。

二是云计算支撑数据智能决策，优化工业决策与生产。从自动化到智能化是从局部优化向全局优化的过程，工业互联网平台利用云平台实现供应商、生产者和消费者的互联互通，通过人工智能、大数据等技术辅助数据的挖掘和利用。例如，广东作为中国制造业强省，大力推进工业互联网应用，支持企业利用云计算与人工智能等技术进行智能化改造，实现提质、降本、增效的管理目的。如消费者对产品的生产过程提出质量追溯需求时，工业互联网平台可智能化地采集、传输、处理、操作产品全生命周期数据，对其进行实时分析并构建生产质量模型，实现对异常品的定位和全流程的品质监控。通过上云打破企业信息孤岛，整合产业链上下游，从单条作业流水线优化，向供应商、生产者和消费者的集成优化转变。

三是云计算赋能工业数据流通，数据普惠促进经济创新发展。云计算提供了随时随地可接入的网络，为工业数据要素的开放、共享和交易提供有力支撑。基于云计算、区块链和隐私计算等技术构建的国家工业互联网大数据中心，支持面向全国范围内工业企业提供数据交易服务，实现不同企业、不同区域间的工业数据要素流转，在全国范围内形成研发、生产、运输、原材料供应、销售等一体化的创新发展

新局面。例如，上海作为中国的金融、贸易和航运中心，在工业上云领域注重打造智能制造公共服务平台，支持企业实现设计、生产、销售等全流程智能化。

3、 工业上云助推工业数字化绿色化融合

绿色低碳发展是当今时代科技革命和产业变革的方向，绿色经济已成为全球产业竞争重点。《“十四五”工业绿色发展规划》和《工业领域碳达峰实施方案》中均提出加快云计算、大数据等信息技术在绿色制造领域、绿色低碳升级改造中的应用，云计算已成为工业数字化、智能化、绿色化融合发展的坚实底座。

一是云计算与工业深度融合，赋能绿色制造。一方面，提高资源利用率。云计算通过虚拟化技术将服务器资源整合，集中化地提供冷却，通过资源的共享，降低硬件设备的废弃物排放，如散热、电力等能源消耗，实现资源的高效利用。**另一方面，优化能源消耗。**云计算可以智能地调度资源，将算力需求有序引导至算力充沛的数据中心，实现算力集约化发展。“东数西算”工程极大优化了数据中心建设区域在我国的布局，充分利用了西部丰富的太阳能和风能等绿色能源，提升数据中心的绿色能源使用比例。

二是重点用能设备上云，提升数字化碳管理水平。工业设备上云后，通过云上智能能源管理工具，实时感知、监测并分析设备的能源消耗数据，推动企业构建碳排放数据计量、监测、分析体系，及时预警超出门限的用能设备，发现能源使用不合理之处。如通过分析工业生产环节设备能源消耗数据，找出能源浪费环节，提出改进措施，提

升能源利用效率。工业设备上云可提升企业碳排放的数字化管理、网络化系统以及智能化管控水平，辅助制定更为科学有效的节能减排策略，加速数字赋能工业绿色低碳转型进程。

4、 工业上云加速商业模式的变革和创新

云计算为工业提供了数字化的技术底座，加速了数字要素对传统要素的替代步伐，改变了企业与其利益相关者共同创造价值的模式，主要体现在对外提供服务的模式和对内运营管理的模式两方面。

一是云计算降低工业用户获取网络资源服务的成本，创新工业服务模式。一方面，传统工业设备安装调试、故障维修、工艺咨询等服务通常以线下方式开展，云计算支持企业在云端搭建工业服务平台，工业产品的功能和服务可通过云端进行交付和提供，积累线上用户的使用信息，及时对用户需求进行反馈，降低产品成本的同时提升用户体验等附加值。**另一方面，**工业属于产业链链条较长的行业，云计算支持工业企业建立开放式商业平台，令其可与产业链上的合作伙伴协作，共同向用户提供完整的工业解决方案。

二是云计算加速企业信息化进程，构建全新的运营模式。内部管理流程方面，工业企业需要打通供应链上下游的生态合作伙伴、供应商和最终用户间的数据断层，为采销一体化提供统一数据标准，云计算助力工业企业搭建数据中台，统一供应链上下游编码和产品标识，降低内部流程耗时。**内部生产流程方面，**云计算可以智能化的管理物料、设备、车间、仓储等环节，与企业业务流程管理系统结合，促进企业内部信息共享，实现业务流程的自动化和优化。

二、工业上云面临安全、门槛高、合规与时效四类风险挑战

（一）工业上云面临多样化攻击与高门槛挑战

云环境面临多样化攻击手段。一是利用上云后的工控设备脆弱性发起攻击。2022 年 9 月黑客组织 GhostSec 声称其破坏了以色列多达 55 个 Berghof PLC（Programmable Logic Controller，可编程逻辑控制器），该 PLC 可通过互联网访问且使用了简单的访问凭证，黑客获取其控制面板权限后可改变水中的氯含量和 PH（Pondus Hydrogenii，酸碱度）值，进而影响工业生产。**二是通过云勒索软件进行攻击。**2021 年 3 月电脑巨头 Acer 遭遇 REvil 勒索软件攻击，攻击者利用 Acer 域内的微软 Exchange 服务器安全漏洞窃取数据并加密锁定目标设备，对其进行勒索，赎金高达 5000 万美元。**三是利用云计算新技术的漏洞发起攻击。**容器、微服务等技术的应用导致企业资源暴露面增加，其分布式特性更使得检测和遏制攻击愈发困难，如 2021 年 Docker Hub 上的部分容器镜像被内置挖矿程序，下载总数超 2000 万次。**四是通过云端大流量对云存储发起攻击。**诸如控制信息、工艺参数和工况状态等敏感工业数据在云端存储，诸多云服务需访问数据以推进生产流程，分布式拒绝服务攻击会通过大量访问导致存储服务故障，从而影响工业生产效率。

企业上云用云门槛增高。一是上云成本超预算风险。我国工业企业上云起步相对较晚，但在政府的大力推动下，我国工业企业上云的发展速度正在逐步加快，当前我国工业企业上云主要解决流程自动化

运转的业务需求，云成本的管理仍处于后置监控阶段，正面临云资源浪费、云账单数据挖掘分析不到位、云成本优化流程管理不健全，以及多云环境下统一管理成本高等问题。**二是云供应商锁定风险。**工业企业遍布全球各地，使用单一云供应商可能会面临在某地域无数据中心可用的困境，导致企业无法迁移其工作负载。**三是多云环境增加统一管理复杂性。**不同云服务提供商具有不同的管理界面、API 和工具，提升了跨云环境的统一管理与监控难度。企业需要投入更多的时间和资源来掌握多个云服务提供商的管理方式，或者寻找能够跨多个云环境进行统一管理的第三方工具。

（二）业务跨境企业面临严格安全合规与即时性要求

工业全要素的泛在互联与工业数据的开放流动均得益于工业上云，然而拥有跨境上云业务的本土企业与上云的跨国企业，在开展业务时要符合各国家、司法管辖地的法律监管要求和规定，敏感业务数据的云上存储与流动、跨国多云平台的运营将为企业乃至国家安全带来挑战。

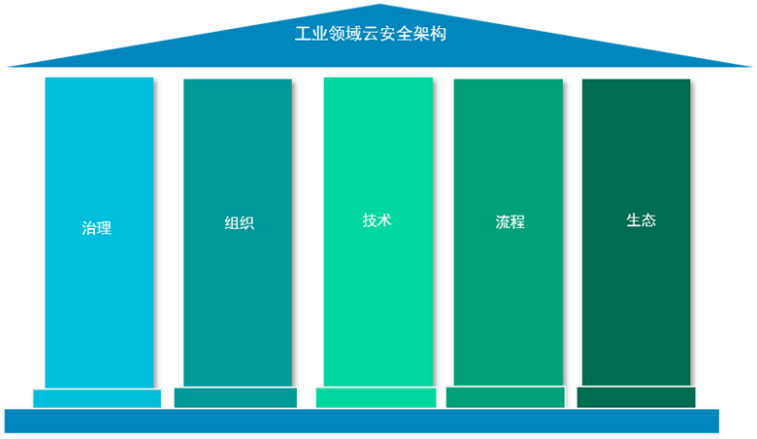
各国数据安全法律尚存适用冲突，企业数据跨境存储与流通面临安全考验。2023 年 5 月 22 日，Meta 因将欧盟用户数据跨境传输到美国违反 GDPR（General Data Protection Regulation，通用数据保护条例）规定，罚款近 12 亿欧元。美国《澄清境外数据的合法使用法》要求美企必须将储存在境内外的数据提交给政府。然而 GDPR 规定允许科技公司在提供适当的保障措施及法律救济措施的前提下，将数据转移至其他国家。欧盟监管机构以美国无法确保数据出境之后其保

护水平不低于欧盟标准为由，开出了 GDPR 生效五年来的最高罚单。因此企业在开展跨境业务时，需考虑所涉多国的法律法规要求。

跨国多云平台运营对企业业务支持的即时性提出高要求。企业上云后需要对云上资产进行可持续运营，包括监控和管理云上应用性能和可用性，跨国运营、跨团队管理的多云平台在应用升级、扩展和迁移时，需克服人员层面如时差和团队协作，以及技术层面如云异构等不同层面带来的挑战。

三、构建五维模型，提升工业领域云安全防护力

随着工业数字化转型进程的不断深化，云计算作为支撑数字化的重要基础设施底座，其重要性不断提升，越来越多工业数据、设备和应用迁移到云端，云安全的重要性日益显著。基于云安全工作考虑，构建“工业领域云安全框架”，如图 3 所示，该框架主要从治理、组织、技术、流程以及生态五个维度着手，提升企业云安全水平，为工业领域云计算环境组成对象提供全方位的安全保障。



来源：西门子（中国）有限公司

图 3 工业领域云安全框架

（一）治理维度：构建工业领域云安全治理体系

主动与全球云安全监管合规标准对齐，构建全面系统化的云安全管理框架，覆盖 IT 和 OT 层面，推动外部法规的内部化落地。一是明确云安全总体策略，包括制定企业云安全工作的总体目标，工作原则和安全框架等，为云安全体系建设提供顶层指导。在总体目标方面，明确对云端、边缘层资产的机密性、完整性和可用性，确保业务连续性和合规性等方面目标，为后续云安全工作推动提供总体指引；在云安全工作原则方面，明确云安全工作的基本原则，至少应包括最小权限原则、身份验证与访问控制原则、深度防御原则、持续监控与风险评估、业务连续性与恢复处置原则，以确保相关安全措施符合最佳实践和行业标准；在云安全框架方面，制定针对云端基础设施、主机安全、数据安全、应用安全以及边缘层安全的管理框架和控制措施，为云安全体系建设过程中提供更具体的指导和依据。**二是梳理适用的云安全合规要求，结合企业自身情况，明确具体云安全管理要求。**企业需要明确适用不同国家/地区的法律法规和工业领域的监管要求，覆盖云上网络安全、数据安全等内容，例如欧盟 GDPR、CCPA（California Consumer Privacy Act，加利福尼亚州消费者隐私保护法案）、HIPAA（Health Insurance Portability and Accountability Act，健康保险携带和责任法案），以及中国信息安全等级保护要求和关键信息基础设施安全保护要求等；同时结合自身实际需求，如工业控制数据会随着业务流程或生产过程在多云间进行流转等特点，梳理云安全管理基线，为云安全管理活动中的各类内容建立统一管理制度，提出基本的安全管

理要求。

来源：西门子（中国）有限公司

图 4 工业领域云安全管理体系

（二）组织维度：构建工业领域云安全组织架构

充分考虑云计算带来的网络化组织结构，构建人员完备、责任清晰、结构设置合理的 IT/OT 信息安全组织架构，提供坚实的组织保障与人员支撑。在工业领域，跨国公司虽然能享有全球供应链与采购网络带来的成本优势，但跨国团队的云应用升级、扩展和迁移等运营管理操作却面临诸多不便。为克服时差、协作不便等挑战，需要建立一个责任清晰、结构合理的组织架构。**云安全组织架构建设包含组织结构和安全责任两个维度。组织结构维度，一是，**确保配备专职的云安全管理岗位及人员，如系统管理员、安全管理员和审计管理员等，负责监控和应对云安全威胁，及时采取必要的安全措施，确保企业在云环境中的数据与应用得到充分的保护；**二是，**加强云安全管理组织同集团管理层、业务部门负责人、各职能部门及各供应商的沟通与合作，

定期召开工作协调会议；**三是，**加强内部云安全管理部门同业界专家、外部安全组织、监管机构的合作与沟通，建立外联单位清单。**安全责任维度，内部责任划分方面，**上云前明确云安全管理部门的工作内容和应承担的安全职责，定义各部门尤其是关键岗位的云安全责任，落实问责制度；**外部责任划分方面，**工业领域 PaaS 和 SaaS 类云服务较多，为明确与不同云服务商之间的安全责任划分，企业应与云服务商达成明确的责任划分协议。

来源：西门子（中国）有限公司

图 5 工业领域云安全组织架构

（三）技术维度：构建工业领域云安全技术体系

建立符合业界标准、适用 IT 与 OT 结合的云安全技术体系，以保障云上业务系统安全运行。在工业上云的过程中，横跨 IT 和 OT 基础设施，连接人、机、物和系统等各种对象，因此需要针对工业环境的独特性和复杂性，从边缘防护、基础设施防护、平台应用防护三个维度建立一个适应工业需求的云安全技术体系。

来源：西门子（中国）有限公司

图 6 工业领域云安全技术体系

边缘防护保障 IT 与 OT 设备建立安全连接。在工业上云的过程中，边缘防护需要关注以下几个方面：**一是边缘数据处理安全，**边缘计算设备直接与生产现场的设备相连，处理的原始数据可能包含敏感信息。为了确保数据处理过程的安全和可追溯，采取数据加密、访问控制和数据水印等技术，保护数据在处理过程中的机密性和完整性，防止未经授权的访问和数据泄露。**二是工控协议设计安全，**工控协议自身的安全设计、协议实现的正确性与安全性、协议与系统的兼容性以及协议的可扩展性是确保 IT 与 OT 设备间通信安全的必要条件。因此，在工控协议设计过程中，需要充分考虑上述因素，确保协议能够有效地保护通信数据的安全性和可靠性。**三是数据集成安全，**工业数据集成平台通常连接不同工业设备和系统，需确保平台本身的安全性、通信协议的安全性和数据处理过程的安全性，通过采用数据加密、访问控制、审计日志等，保障数据在传输和存储过程中的机密性和完

整性。**四是接入安全，**为了确保只有合法的实体可以接入云边，需要采用访问控制隔离技术手段，实现准入认证。通过对设备的身份进行验证和授权，以及实施网络安全隔离等措施，仅通过认证的设备才能获得访问权限并接入云边，从而确保系统的安全性。

基础设施防护保障信息科技资源安全。在工业上云的过程中，基础设施防护需要关注以下几个方面：**一是机房基础设施安全，**机房物理选址应远离自然灾害高发区，机房物理环境指标如温湿度、空气质量等处于适宜状态，采取必要的备份供电系统和冗余设备等措施来确保供电的稳定性，严格限制机房进出人员，对机房内重要设备进行全天候实时监控。**二是虚拟资源安全，**保障虚拟计算、存储、网络资源的安全，及时对虚拟机补丁进行管理，并开展安全更新，定期对虚拟机备份操作，确保发生安全事件时能够及时恢复数据，通过虚拟网络隔离实现虚拟机隔离，并对虚拟机间传输的数据进行加密。**三是接入安全，**使用多因素身份验证、设置访问权限和角色分配等措施，严格控制虚拟资源的访问权限。同时，应使用专有网络进行连接，在基础设施层面限制未经授权的访问以防止潜在的入侵行为，从而保障信息科技资源的安全性。

平台应用防护保障工业数据流转安全与工业软件研发阶段的安全。一是数据安全，对设备采集数据、设备运行数据以及业务系统数据等在采集、存储、传输、使用、交换、销毁等环节引入安全措施。**数据采集过程中，**应加强企业敏感数据收集人员、设备的管理，并对收集来源、时间、类型、数量、频度、流向等进行记录。**数据传输过**

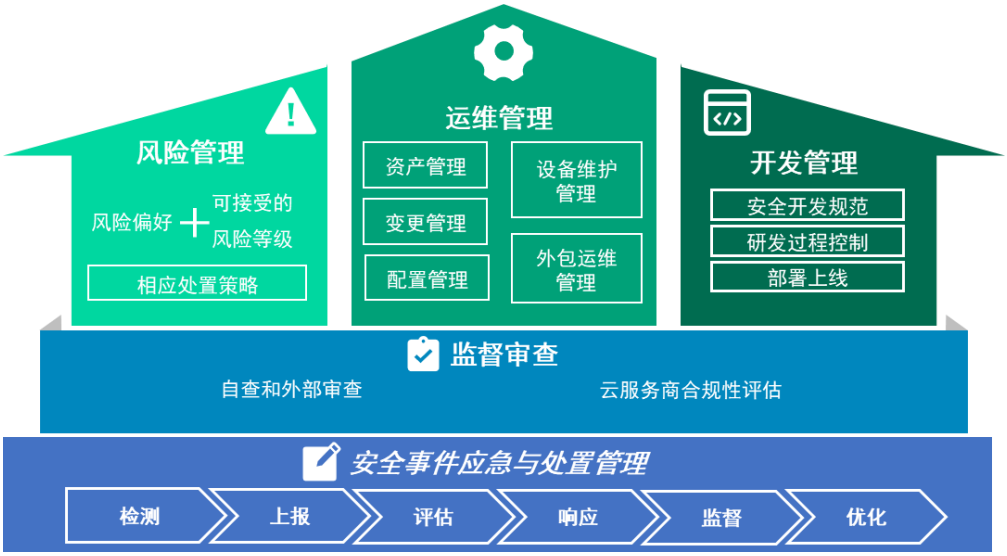
程中，应采用校验技术、密码技术、安全传输通道或者安全传输协议等措施传输企业敏感数据。**数据存储过程中，**应采用校验技术、加密存储等安全存储管控措施，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试。**数据使用过程中，**应采用数据匿名化、数据脱敏等技术，防止隐私泄露，并实施必要的权限控制，保障数据在授权范围内被访问与处理。**数据交换过程中，**应与数据获取方签订数据安全协议，对数据获取方数据安全保护能力进行核验，保障企业提供的敏感数据可安全地进行交换。**数据销毁过程中，**数据处理者应当建立数据销毁制度，明确销毁对象、规则、流程和技术等要求，并对销毁活动进行记录和留存。**二是研发安全，**在工业软件研发过程中，需开展安全需求分析和风险消减设计，并对源码进行安全扫描和功能模块的安全性测试。在应用发布前对安全节点进行检查，以确保研发过程全生命周期安全。**三是安全运营，**梳理组织的各类工业资产与云上资产，完善云上云下资产统一管理体系以减少“影子 IT”，为网络与应用设置基本安全策略，摸排云上软件基础安全配置，对 IT 和 OT 资源进行威胁和漏洞管理，从工业软件收集数据进行安全分析、威胁溯源等，保障工业 PaaS 平台或 SaaS 应用安全运行。**四是安全接入，**通过统一设备身份认证，禁止未认证终端接入云端，避免因设备漏洞被利用而导致的威胁渗透风险。同时，应使用加密通讯保障工业数据在终端与云端间传输过程的机密性与完整性。

（四）流程维度：构建工业领域云安全运营流程

充分考虑云计算为云上系统带来的互联互通性，构建完备的信息

安全运营的流程体系，辅助云上安全管理流程的持续改进。安全运营在维护 IT 和 OT 资产方面发挥至关重要的作用，除了基础的安全防护技术之外，应考虑为风险管理、安全运维、安全开发、安全审计和应急响应与处置建立完备的制度体系，促进安全策略、安全组织和安全技术的深度融合，为工业企业数字化转型提供有力保障。**一是风险管理，**梳理受保护的 IT 和 OT 资产，并定期开展资产识别，结合其对业务安全的影响程度进行分类，根据企业自身风险承受能力，确定风险偏好和可接受的风险等级，针对不同等级的风险制定相应的处置策略。**二是运维管理，**建立包含资产管理、设备维护管理、变更管理、外包运维管理、配置管理相关制度为云上应用或平台进行运维。资产管理可实现云上云下各类资产的全生命周期管理，通过定期维护工业设备，正确配置工业软件，确保整个工业系统的正常运行，在开展变更时对变更进行合理性审核，对步骤进行记录，便于跟踪和管理。此外，对外部供应商包括云服务商、工业设备供应商等进行管理与监督，确保其按照事先约定的要求和标准执行运维任务，并与企业内部的安全运维体系协同工作。**三是开发管理，**制定安全的开发管理规范和流程，根据工业场景特点，建立安全开发规范，包括安全编码、安全配置、安全开发工具使用、安全风险消减设计等；在研发过程中，对软件版本进行控制，对依赖组件与代码进行审查，制定代码审核机制以及代码合入准则；软件部署上线前，规范发布流程，提供安全回滚和备份机制。**四是监管审查，**一方面，对于企业自身而言，定期开展安全自查和外部审查，检查安全工作落实的有效性，配合政府监管部门

开展安全审查或取证。另一方面，对于企业所使用的云服务供应商，定期对其服务进行合规性评估。**五是安全事件应急与处置管理，**针对工业系统中可能出现的各类安全问题，建立安全事件的检测、上报、评估和响应流程，监督安全事件的处置进度并对其复盘，持续优化和改进响应流程。



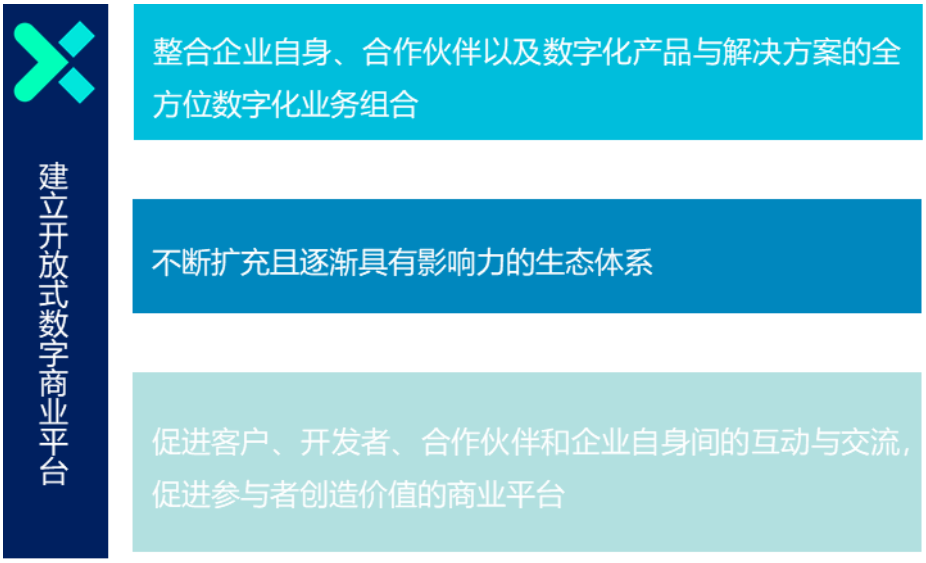
来源：西门子（中国）有限公司

图 7 工业领域云安全运营流程

（五）生态维度：构建工业领域云安全生态链条

充分考虑云计算为生态间协作带来的便利性，链接工业产业链上下游企业间的协同合作，实现资源共享和价值创造。建立开放式数字商业平台，一方面赋能工业用户，提供安全解决方案，另一方面为自身、工业合作伙伴和安全供应商带来商业价值，通过将产业链上各环节安全解决方案组合，提供一站式解决方案，协同为工业用户提供安全服务和产品，充分释放工业企业自身与安全生态伙伴各自优势。**一是打造先进多样的数字化业务组合。**一方面，建立安全的开放式数字

商业平台底座，保证提供服务的云平台安全。另一方面，验证生态合作伙伴所提供产品或服务的安全性，共同打造模块化、端到端的数字化业务组合。**二是打造开放互利的生态合作体系。**积极引入合作伙伴，发展协同机制，通过共享安全信息、技术合作、安全风险共担等共同应对工业安全威胁。**三是打造持续迭代的数字商业平台。**打造集探索、教育、交流和交易功能于一体的平台，通过一站式解决方案，向用户提供更加全面的服务，覆盖产业链上、中、下游，赋能工业用户运营各环节，提升工业用户体验。



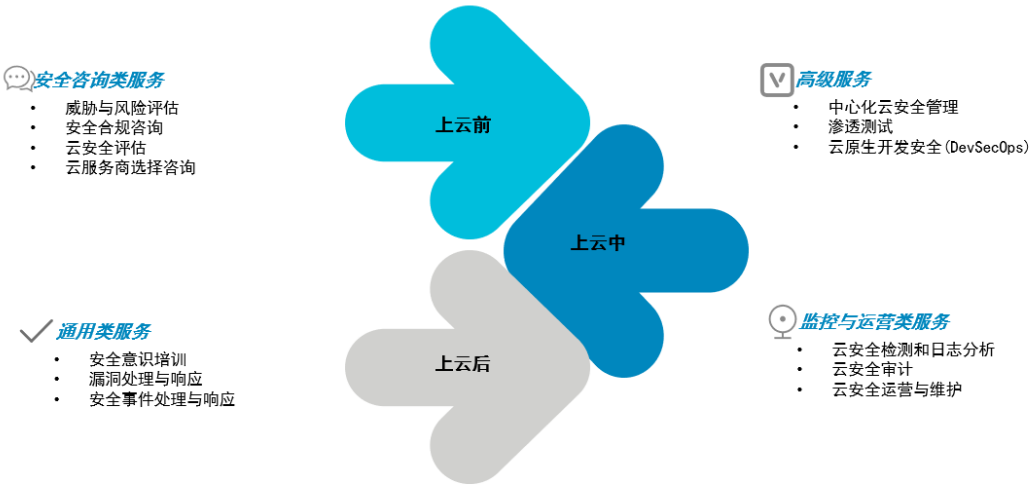
来源：西门子（中国）有限公司

图 8 工业领域云安全生态链条

四、工业领域云安全参考实践

为了更好的应对工业企业上云后的安全挑战，企业可在“工业领域云安全治理框架”的指导下，基于企业自身业务特征及上云的不同阶段，弹性灵活地选择云安全实施方式。云安全实施方式主要分为两种：**一是技术积累深的企业自行建设，**通过加大研发及相关资源投入，

加强自身云安全人才储备等方式，获得定制化程度较高的安全解决方案；**二是借助生态赋能，**考虑安全投入及效能，选择优势互补的合作伙伴，采纳专业的云安全服务及技术解决方案，高效补齐云上安全短板，覆盖安全咨询、运维管理、安全培训等方面。两种实施模式互不冲突，灵活互补。

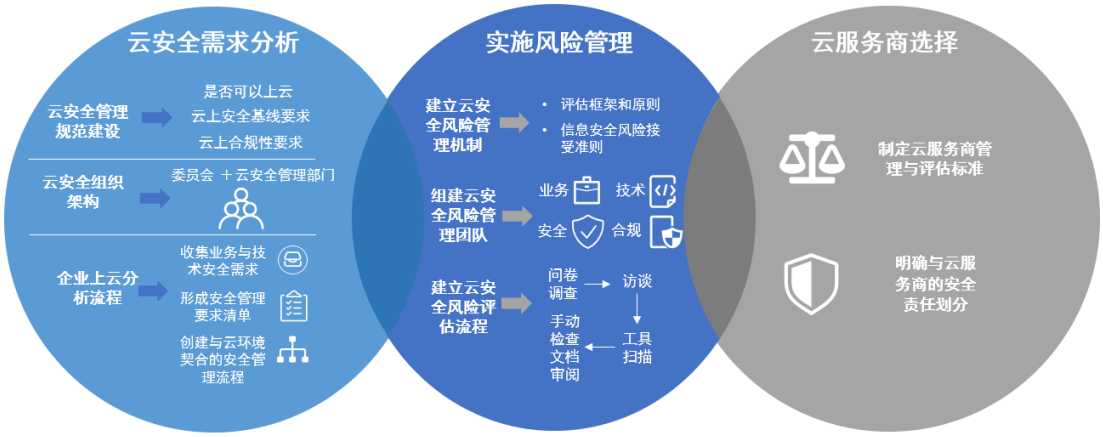


来源：西门子（中国）有限公司

图 9 云安全服务目录

（一）上云前：规划策略，评估风险

工业企业从传统信息化模式向云计算模式迁移，需要开展深入的需求分析与风险评估，以帮助企业了解自身业务、技术等方面的需求，梳理上云过程中可能遇到的风险，提前规划相应的应对策略，并审慎选择云供应商，为云安全活动的实施打下坚实的基础，保障其业务免受不必要的风险和损失。



来源：西门子（中国）有限公司

图 10 上云前安全准备

深入开展云安全需求分析，明确工业企业上云安全目标。[2]**强化云安全管理规范建设，**明确企业能否上云，以及上云安全目标，制定云上资源管理、数据安全保护、应用程序迁移等规范，形成云上安全基线标准要求、合规性要求等适用于云计算环境的安全方针，指导云安全管理方向，提升管理能力。**明确云安全组织架构，**建立云安全管理委员会，该委员会由业务部门、云安全管理部门等相关部门的核心成员共同组成，负责进行重大云安全决策和资源协调。同时，设立云安全管理部门，专职承担日常云安全管理事项，包括安全策略制定、安全事件响应、定期安全检查等，为云安全管理提供坚实的组织保障。**建立企业上云需求分析流程，**收集业务与技术安全需求，同时考虑资产敏感度、法律法规或标准中的安全要求等，形成安全管理要求清单，结合云环境特点，创建与云环境契合的安全管理流程，覆盖安全管理组织、网络安全、数据安全、开发安全、身份与访问管理、隐私保护

[2] 本段部分内容参考 GB/T 31167-2023 6.5 需求分析

与合规等内容。

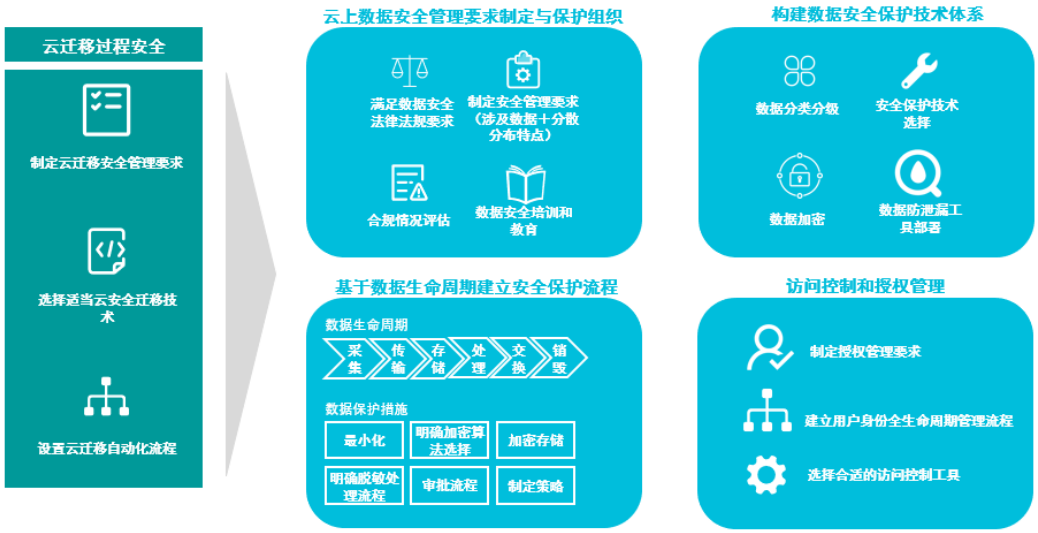
实施风险管理，识别并应对潜在安全威胁与风险，为工业企业上云的后续活动保驾护航。建立云安全风险管理机制，一是以安全目标和策略作为风险评估基准，明确风险评估的目标、范围、方法和时间计划，建立云安全风险评估框架和原则，指导风险评估工作开展；二是制定企业的信息安全风险接受准则，根据自身的风险承受能力确定风险偏好和可接受的风险等级，在投入有限的资源时做出更加合理的安全决策。**组建具备专业技能和经验的云安全风险管理团队，**由业务、技术、安全、合规等领域的专家组成，负责识别上云过程中可能面临的多种安全风险，制定风险控制措施，监控云环境的安全风险状况并定期开展安全风险状况评估，为风险管理工作的全面落实提供有力保障。**建立云安全风险评估流程，**明确风险识别、评估和应对具体步骤和方法，包括确定评估范围；通过问卷调查、访谈、工具扫描、手动检查文档审阅等方式，匹配分析脆弱性和威胁，识别潜在信息安全风险，风险源可以来自相关标准的要求、安全事件、内审结果等；综合考虑风险的原因、发生的概率、带来的影响、现有的管理措施等因素对识别出的安全风险进行分析和定级，评估风险的严重程度；对于不同等级的风险，结合企业的风险偏好，制定不同的处置策略，定期检查风险处置措施的有效性。

基于上云需求选择安全、合规的云服务商，共同定义安全责任，维护云环境的安全与稳定。制定云服务商管理与评估标准，一是对云服务商的资质和云服务合同提出要求，确保云服务商具备必要的技术

能力和服务水平，同时保证合同条款的公平性和合规性；二是制定详细的云服务商评估标准，包括对云服务商的资质、技术实力、服务水平、合规性、安全事件响应等进行全面评估。**明确与云服务商的安全责任划分，**与云服务商共同制定可用性保障措施和标准，约定服务等级协议（SLA）、云服务商架构的高可用性等，确保包含针对未达到服务水平的处罚或退出条款。

（二）上云中：平稳迁移，纵深防御

工业企业通过迁移至云环境，可以享受更为灵活、高效的资源服务，然而云环境具有的强分布式与高弹性特点，令上云后的工业设备间交互与云上应用服务间的依赖关系更为复杂，提升了云安全防护的难度。确保工业企业上云过程的安全可控，构建云上纵深防御能力，对于保障云上信息资产的安全和业务的稳定运行至关重要。



来源：西门子（中国）有限公司

图 11 上云中安全保护

关注云迁移过程安全，保障业务上云后正常运行。制定云迁移安

全管理要求，根据不同应用和系统的不同架构、数据量、安全需求等特点，定制化迁移策略和计划，包括评估迁移风险、确定迁移顺序、制定测试计划、规划备份策略等。**选择适当的云安全迁移技术，**识别不同应用程序向云上迁移的安全风险，例如业务中断、网络中断、数据丢失等，选择适当的技术解决方案，例如采用增量迁移技术、使用专用网络、使用安全的传输通道传输数据等。**设置云迁移自动化流程，**通过设计自动化脚本为应用程序固化迁移路径，内容包括网络、安全、监控以及配置管理等内容，使应用程序能够自动、快速地迁移到云上，监控安全与合规性需求及事件，并有助于减少人为因素导致的安全风险。

强化云上安全冗余能力，构建多层次化防护。设计安全架构，设计高可用冗余架构，实施工控网络和企业内网分区隔离管理，注重主机层面的安全加固和防御能力提升，采用严格的应用安全策略，并设计设备层的身份鉴别机制。**采用安全技术，**网络层采用 VPC 进行分区隔离并采用边界防火墙、入侵检测系统和入侵防御系统等以检测和阻止网络攻击；主机层定期推送安全补丁，及时修复安全漏洞，加强主机安全防御能力；应用层部署应用防火墙、应用安全扫描和漏洞修复工具，防范应用层面攻击和漏洞利用；设备层采用强密码策略、多因素认证等身份鉴别方式，防止未授权访问或恶意控制等。**建立安全弱点识别与防御体系动态调整机制，**定期开展安全评估识别云平台与云应用系统弱点，调整云上受保护资产范围，防御体系下云安全工具联动，及时响应新的威胁，持续提升安全防御能力。

强化企业云平台数据安全保护，确保云上数据资产的机密性、完整性和可用性。制定云上数据安全管理要求，一是满足对标地域的数据安全法律法规要求，例如识别数据跨境传输场景并进行风险评估与合规申报；二是针对上云业务中涉及的数据，结合云上数据分散分布的特点，制定云上数据安全管理要求。**建立数据安全保护组织，**识别数据安全法律法规，对公司内部的数据安全合规情况以及员工按照管理与合规要求的履职情况等进行评估；提供数据安全培训和教育，提高员工的安全与合规意识。**构建数据安全保护技术体系，**一是全面梳理数据并进行分类，识别出重要数据和敏感数据等，基于数据特点，采取针对性的安全保护技术；二是通过加密算法和协议对数据进行加密，包括对传输中的数据加密和对静态存储中的数据加密；三是部署数据安全防泄漏工具，识别和监测敏感信息，一旦检测到异常行为或潜在的数据泄露风险，立即发出警告，由安全团队进行处理。**建立数据全生命周期安全防护流程，**在采集阶段遵循最小化原则，获得数据主体的明确授权同意，确保数据收集来源的合法性并与用户隐私政策一致，公开告知用户数据收集的目的、范围和使用方式等；在传输阶段，明确加密算法的选择、传输协议的安全、加密通道的设置、完整性验证；在存储阶段，实施加密存储、不同级别的数据按照分类分级标准隔离存储、多重备份；使用阶段，数据共享、转让、对外提供等符合当地法律法规要求与合同约定；在数据处理阶段，明确数据脱敏处理流程，定义数据分析安全要求，规范数据使用，制定数据处理环境的安全控制措施并设置数据导入导出审核流程；在数据交换阶段，

定义数据共享场景并明确相应审批流程，制定数据接口安全控制策略；在数据销毁阶段，设置数据销毁策略，明确数据销毁场景、销毁对象、销毁方式和销毁要求，并建立数据销毁审批流程。

访问控制覆盖身份全生命周期，规范主体访问行为。制定授权管理要求，梳理工业流程涉及的用户角色，定义用户角色的职责和权限范围，明确添加、修改或删除角色和权限的方式，规定用户角色分配流程，并设立权限验证与审计机制。**建立完整的用户身份全生命周期管理流程，**涵盖权限申请、审批、分配、回收以及过期处理等各个环节，严禁账号共享行为，针对个人信息处理岗位人员的变动情况，如调离岗位或终止劳动合同，及时调整和更新其关联的权限配置，定期进行权限复核，并保存详细的检查记录，以确保权限管理的有效性和合规性。**选择适合的访问控制工具，**部署基于零信任理念的 IAM 实现身份生命周期管理和权限集中管理，并通过 PAM 监控和保护具有特权访问权限的用户。

（三）上云后：持续优化，安全用云

安全上云标志着云安全管理的新起点，尽管在上云中已经构建了多层次的云安全防护体系，但云安全仍需持续关注和努力。工业企业在迁移至云端后，仍需持续加强云资源的运维工作，并不断提升员工的安全意识，从而构建一个日益完善的安全防护网络，以有效地防御各种潜在的安全风险。

来源：西门子（中国）有限公司

图 12 上云后安全管理

基于应用开发平台对工业软件的研发流程实施安全管控。一是开发阶段，在镜像创建之前排查配置编排文件及镜像的安全风险，包括 IaC（Infrastructure as Code，基础设施即代码）相关的配置部署脚本，如 Dockerfile、K8S Manifests 等，以及镜像安全，如容器、操作系统镜像和镜像仓库的安全扫描，并嵌入 DevSecOps 流水线。**二是发布部署阶段，**在容器运行之前预防容器配置及容器编排平台生态（K8S 组件）安全风险，检测主机层面操作系统漏洞；**三是运行阶段，**实施主机入侵检测及容器运行时安全检测，同时对微服务应用进行类型识别与安全漏洞检测，建立容器东西向网络安全隔离策略，实施集群的统一安全检测和合规审计。

持续开展安全运维，即时发现和处理潜在隐患，以适应不断变化的安全威胁环境。一是安全态势监控。工业企业应部署安全检测和日

志分析工具，实时监控云环境中的异常活动和潜在威胁，收集并分析各种日志和安全事件信息，掌握云环境状态，以及时发现可疑行为，并迅速采取相应的处置措施；**二是加强云安全漏洞管理。建立漏洞管理流程，**明确漏洞的发现、报告、修复和验证环节管理要求，明确漏洞扫描频率并制定详细的漏洞扫描计划；**选择合适的漏洞扫描工具，**发现云环境中的各类安全漏洞，并结合机器学习和人工智能，进行大量的安全数据分析，自动发现新的和未知的漏洞，提高漏洞扫描的效率和准确性。**三是建立事件响应机制。制定事件响应管理规范，**明确事件发现、事件报告、事件处理等环节的要求，并规定在发生安全事件后与外部供应商和内部人员之间的协作方式，确保在发生安全事件时能够迅速、有效地应对；**组建事件响应团队，**由专业的技术人员、安全管理人员和管理层组成，具备快速响应和处置能力，负责处置各类安全事件，能够迅速分析事件原因、定位攻击源头并采取有效的措施进行处置。**四是开展安全审计。制定云安全审计政策和规范，**明确审计的目标、范围、方法和频率，全面深入地审查云环境的安全状况；**设立云安全审计团队，**明确团队成员的职责和角色，定期审计公司云安全策略的执行情况；**采用自动化审计工具，**如配置核查工具、漏洞扫描工具、日志分析平台等，提高审计效率和准确性，将审计工具与其他安全防护措施（如防火墙、入侵检测系统等）相集成，实现安全信息的共享和联动处置；**制定详细的云安全审计流程，**包括审计计划的制定、审计实施、结果分析和报告编写等步骤，评估和验证安全策略和流程、数据安全、隐私保护、基础设施安全、服务可用性和性能、

安全事件和漏洞监控、安全日志等，识别潜在的安全隐患和漏洞，建立审计问题的跟踪和整改机制，确保审计发现的问题得到及时有效的处理，实现对云服务的全面安全管理。

加强安全培训，提高员工云安全认知水平和威胁防范能力。完善培训管理流程，明确培训目标和内容，确保培训的针对性；定期更新培训内容，保障培训的时效性；评估培训效果，确保知识传递的准确性，例如通过考试、问卷调查等方式；建立培训反馈机制，为员工提供培训反馈渠道，以优化培训流程和内容。**建设专业培训团队，**由具备云安全专业知识和丰富经验的人员组成云安全培训团队，以有效传达安全知识。

五、工业数字化转型云安全发展趋势及建议

（一） 工业领域云安全技术发展趋势

零信任升级云安全防护理念，助力工业实现面向资产的安全检测与防护。随着工业数字化转型走深向实，工业设备、软件与数据的上云进程逐步加快，工业资产安全防护成为重中之重。**云下资产方面，**工业设备通过物联网网关与云端连接，此间通讯协议复杂，且终端设备安全防护能力弱；**云上资产方面，**工业领域云环境中的数据和应用程序不断变化，需要持续监控其安全状态。零信任秉持“持续验证，永不信任”的理念，默认不信任任何接入终端，对访问终端与被访问资源进行持续的安全评估和验证，依托工业控制安全态势感知系统的AI（Artificial Intelligence，人工智能）安全监测，灵活的为多种工业场景提供精细化安全策略与基于时效性的访问控制，能够保障工业领

域云上云下资产访问的全流程安全。

生成式人工智能激发云安全赋能业务潜力，通过自然语言交互在工业现场提供安全咨询。工业领域大多数产线员工缺乏安全背景，生成式人工智能可以将工业领域 IT 与 OT 安全的经验和知识沉淀形成大模型，基于生成式人工智能的虚拟专家助手可以显著提高云安全操作和管理的效率和质量。**一是**虚拟专家助手可以立即响应安全事件和查询，无需等待人工干预，这有助于迅速应对潜在的威胁和问题；**二是**虚拟专家助手可以全天候工作，不受时间限制，能够处理来自全球不同地区的安全事件和请求；**三是**虚拟专家可以支持多种语言，使其在全球范围内更易于使用；**四是**生成式 AI 可以不断学习和改进，从新的数据和安全事件中不断积累经验，提高其识别威胁和问题的准确性；**五是**生成式 AI 可以与其他安全工具和系统集成，提供更全面的安全解决方案。

（二）工业领域云安全产业发展建议

规范保障，完善工业领域云安全标准体系构建。随着全国新型工业化推进大会的成功召开，我国将持续提升工业现代化水平，工业产业将继续朝向数字化与智能化方向发展，工业设备、工业软件与工业数据上云将持续加速。目前，大部分已发布和在研标准均针对云计算安全，如国家标准《信息安全技术 云计算服务安全指南》和《信息安全技术 云计算服务安全能力要求》，通信行业标准《云安全成熟度模型》，也有少部分针对工业设备上云安全标准，如《工业互联网设备上云安全技术要求》，尚未构建针对工业领域的云安全标准体系，

而工业领域因其时延敏感、工控稳定性高等特殊要求，在上云后对信息安全与通信安全都有特殊诉求，如工业数据传输环境和工业设备与网络所处运行环境等，加快具有针对性的标准研制和规范工作，构建成熟度评价体系，对推动工业领域云安全发展具有重要意义。

科技赋能，推动云安全技术应用成为工业发展的内生动力之一。随着云计算技术的不断发展，云安全技术涌现，工业企业应积极使用云安全技术提升工业领域云服务的安全性和稳定性。通过开展容灾备份与恢复演练保障业务连续性，维持工业制品生产效率；采用高效的工控数据加密技术优化系统性能，降低性能损失。同时，通过规模化地使用云安全技术，提升工业信息化水平，为企业创造更加灵活和安全的 IT 环境，快速搭建安全的工业应用与服务，进一步推动工业创新与发展。

引领布局，加速云安全与工业产业链协同发展。工业用户需求已经从单一的产品向产品及服务方向升级，工业上云促进企业 IOT 要素全面升级、激发数据要素价值释放、变革工业商业模式，最终推动工业企业从提供产品的服务向提供用户所需的产品及服务转变。工业企业应利用其处于价值链上游的优势，主动联合云服务商、安全厂商增值工业价值链，以整合的工业产品与云安全服务向用户提供一站式解决方案，在此过程中，云安全应与先进制造、信息科技等技术融合发展，力争在生产企业的核心竞争力中占据一席之地。

附录

案例一：自动垃圾分拣

某电子制造业灯塔工厂在数字化转型过程中，希望通过上云赋能生产提效及业务创新。利用工业相机与工业边缘设备将图像数据传输到某云服务提供商云端，通过机器学习智能识别危险废物，实现自动化垃圾分类。

随着工业边缘设备的规模化使用，云上资产规模迅速增加，为工厂基于云的安全运营带来挑战：**一是云上资产可见性缺失。**一方面，工厂在数字化转型前的传统资产管理系统不适用于云环境，工厂难以对现有云上资产进行管理。另一方面，工厂多云的选择为云上资产管理带来管理复杂性的挑战。**二是资产配置合规风险提升。**传统资产配置措施主要面向 IT 与 OT 设备，无法匹配云上新增资产的配置合规检查需求，造成云上资产配置合规风险提升。

灯塔工厂通过以下手段解决上述问题。**一是提升云上资产可视化能力。**开放式数字商业平台 Xcelerator[3]面向工厂提供云安全管理解决方案，通过对业务部署非侵入式的代理，云安全管理平台可收集工厂在云上的资产信息，建立实时更新的云资产目录清单，统一管控云资产所属的云服务账号，资产的类型，详情信息等，帮助工厂实时获得云上资产分布及安全风险全貌。**二是基于自定义合规模板的云上安全合规监控。**基于云安全防护平台提供的云上配置合规模板，如 SOC2、等保 2.0 等，结合工厂安全实践积累的自定义规则，形成一套完整的

[3] Siemens Marketplace (siemens-x.com.cn) 致力于打造先进多样的数字化业务组合和开放互利的生态体系。

配置合规规则库，以此为基础进行持续配置合规检查，最大程度降低工厂云资产配置的安全合规风险。

案例二：设备故障自动检测

某电子制造业企业产品生产过程中遇贴片机故障，产线需要找到高级工程师，根据机器所报错误代码人工分析问题原因。为提升生产效率，该企业在某云服务提供商云端建立云上知识图谱，产线人员可自己根据错误代码按故障知识库进行处理，快速、高效修复贴片机故障。

随着云上知识图谱的内容不断丰富，以及使用知识图谱的产线人员不断增多，企业需管理的云上数据资产与运营的云账号体量增大，为云上安全运营带来挑战：**一是云上业务数据安全风险。**故障解决技术与经验沉淀而成的知识图谱需要在云端存储，若安全防护措施不到位，存在数据泄露风险。**二是云基础设施存在权限管理风险。**为运营知识图谱，企业开通了若干公有云账户，尚未严格按权限需求进行权限分配，存在过度授权，使攻击者有机可乘。

该电子制造业企业通过以下手段解决上述问题。**一是云上数据安全管理助力工厂保护重要业务数据及隐私数据。**云存储安全防护平台通过持续检测存储在云上对象存储中每个存储桶内的数据，及时发现隐私数据、重要业务数据及恶意文件等数据，实时监控数据泄露风险，保护工业重要业务数据及隐私数据云上数据安全。**二是云基础设施权限管理。**基于最小权限授权原则对云账户的云资源和数据访问权限进行持续监控，及时发现过度授权账号并定期清理非活跃账号，保障多

个云账号权限策略管理一致性

编委会

胡建钧，侯文胜、郭雪，陈蓓华、刘亚兴，吴倩琳，孔松，郭代飞、闫韬、杨荣举，房婧婧，齐麟，浦炜、袁赛东、曹雷、邓瑶，郑雅茹，赵蒙、莫宁琛、王斌、裴旭、许智、赵志成、周鹏程、姚盛楠

关注
CAICT
可信安全

关注
西安社
企业微信

访问西门子
Xcelerator
小程序

联系我们

若您对报告有任何建议，请与我们联系：

cybersecurity.cn@siemens.com