# 制造业数据安全防护解决方案

2023 年 4 月

# 目录

# 1 项目背景

近年来，我国围绕“加快数字化发展，建设数字中国”战略目标，持续出台数字化转型相关政策，驱动传统产业数字化转型，推动数字化赋能千行百业。数字化技术持续创新并加速向制造业领域融合深入，为数字经济提供新的发展活力，促进数字红利加速释放。制造业生产与数字技术走向互联，信息不断开放，高效利用数字技术已成为当前制造业生产的必要条件，在利用数字技术提高生产力的同时，制造业信息系统面临着日益严峻的数据安全威胁。

为有效保障数据安全，支撑国家战略落地及内部业务使用，国家出台的《数据安全法》对数据安全制度及数据安全保护义务从多个角度进行明确要求，通过确立数据分级分类管理以及数据安全管理各项基本制度，落实数据活动的组织、数据安全保护义务及责任，坚持安全与发展并重，锁定支持促进数据安全与发展的措施，来保障数据安全、确保业务稳定运行，是组织需严格遵循且持续保障的。为落实《中华人民共和国网络安全法》、《中华人民共和国数据安全法》等相关法律法规，保障组织的数据安全、促进数据合理有序流动、为数字经济高质量发展提供有力支撑，需建设满足现状同时具有可持续发展的数据安全防护体系。

# 2 现状分析

## （1）网络现状分析

在制造业网络架构上，一般分为工厂外的公众互联网和工厂内网两部分，在工厂内网，从数据生产、采集、传输及使用等方面划分为现场级的现场控制网，车间级的生产管理网，工厂级的办公管理网 3 个区域。

现场级的现场控制网主要用于对现场设备进行管理和控制，采集现场的数据并进行组态处理，同时可对现场的设备运行状态实时监控。

车间级的生产管理网主要作为生产的通讯网络，利用车间工程师站对现场接口机采集的数据进行管理分析，下达生产指令数据，对生产工艺参数进行控制。

工厂级的办公管理网，作为传统的 IT 办公管理网，主要用作日常办公、财务管理、供应链管理等。

具体情况如图 1 所示。

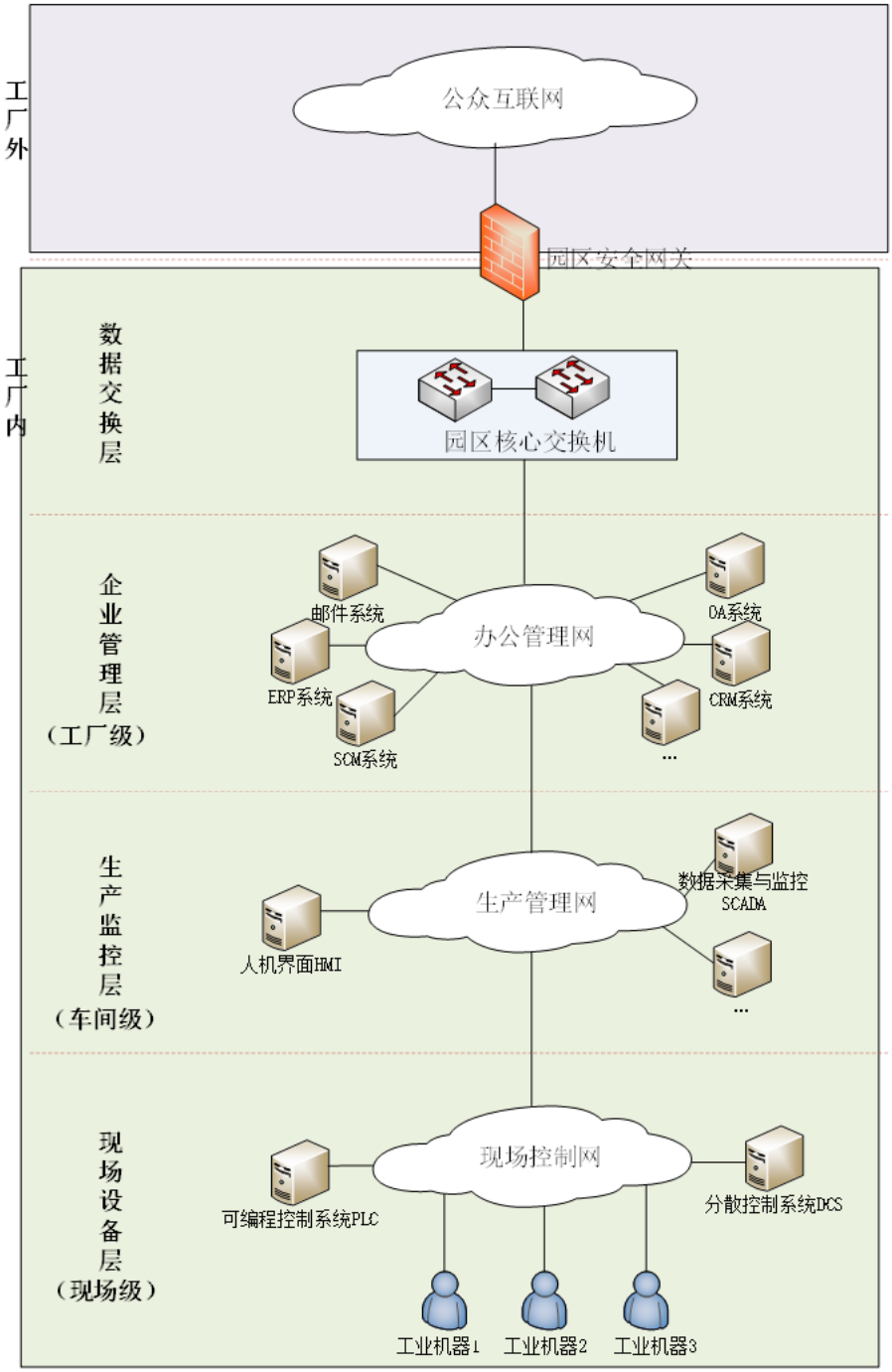


图 1 网络拓扑示意图

## （2）业务现状分析

制造业生产控制系统由于工程建设周期，设备技术需求等原因可能会涉及多种不同品牌，比如霍尼韦尔、西门子、横河、艾默生、AB、ABB 等。生产控制系统具有多样的品牌及型号可能带来多种设备漏洞，如果缺少必要的防护则很可能被不法分子利用攻击。

车间用于生产管理的各工程师站、操作员站多以 Windows 为主，包含多个操

作系统版本。如有已经停止服务的老旧系统版本，存在很大被攻击的风险。作为数据采集、加工和存储的重要环节，安全防护已十分迫切。

### （3）数据安全现状分析

经过调研，目前工厂现场控制网、生产管理网、办公管理网均生产、存储多种数据，大多数企业还并未参照《工业领域重要数据和核心数据识别规模（草案）》进行相应的分级分类。

作为现代化工厂，工厂内包含数控机床等各型设备，其相关生产工艺数据易被犯罪分子利用并对控制系统发起攻击，易造成停工停产，设备损坏等经济损失，如在生产安全要求较高的车间可能会引起人员伤亡等难以估量且无法挽回的损失。此类高价值、涉及国家安全、公民安全的数据为核心数据。

在生产中形成的物料数据、产能情况等直观数据，在办公管理网中财务数据、供应链数据、客户数据等管理经营数据，关系到企业发展的较高价值数据，属于重要数据。

生产现场车间温度数据、设备运行状态数据等不会对企业发展安全造成影响的数据，属于一般数据。

工厂在办公管理网、生产管理网、现场控制网已部署一定的安全防护能力，在网络区域边界已部署有工业防火墙等安全设备，不过对生产、管理数据的全生命周期的防护不足，缺乏数据层的攻击检测手段和数据访问控制手段等。

## 3 风险分析

基于上述现状，我们分析在数据生产、数据存储、数据处理运维、数据运营工作环节下安全防护相对薄弱，主要存在以下风险。

### （1）数据生产环节

数据生产环节数据风险主要来自于数据采集、生成工作，采集数据的安全与生产环境密不可分，如对于采集的数据的环境安全无法保障，使得生产和采集的数据就受到污染，从而导致后面几个阶段的安全防护毫无价值。

数据采集阶段的风险分析应从终端系统、网络设备、生产系统如 DCS 系统、PLC 等设备方面入手，检查是否有必要的终端防护能力，移动介质净化管控手段，

漏洞扫描挖掘能力，访问控制能力等。

## （2）数据存储环节

数据存储阶段应保证存储过程的保密性、完整性，对于数据存储阶段风险分析应从身份鉴别和访问控制机制，存储数据的加密机制，对核心、重要数据备份机制等。

## （3）数据处理运维环节

**1）数据处理环境风险**

数据在通过不可信或较低安全的环境进行传输时，容易发生窃取、篡改等安全问题，数据在传输阶段应加强边界防护能力，具备威胁探测防御能力、设备审计能力，设备漏洞扫描挖掘能力等。

**2）数据运维风险**

在数据运维中，数据库用户账号有泄露风险或数据库用户越权查看敏感数据的风险，对数据运维应具备必要的数据脱敏能力。

**3）数据提供和公开风险**

数据提供和公开如管理不当，容易造成数据使用和提供过程的数据泄漏，并且无法进行追溯，在该阶段应具备数据脱敏能力，数据水印添加溯源能力，数据操作审计能力等。

**4）数据销毁风险**

针对数据层面进行数据销毁，应具备相应的过程控制与监测机制，具备事前监管审批确认、事中访问控制审计、事后回溯分析能力。

**5）数据使用加工风险**

在数据对外提供和使用前需要进行数据加工处理，一方面需要保证加工数据的环境本身具有一定的恶意代码防护、身份鉴别、访问控制能力，保障环境的安全可靠；另一方面，对于加工的制造业数据应具备必要的数据脱敏能力，数据分发水印添加能力，数据操作、流转的审计能力。

## （4）数据运营环节

制造业生产往往生产、操作站点多、分布较广的特点，造成各层级数据分散，

缺少数据的统一管理和分析措施，无法形成整体分析和防护体系。

生产过程的各类数据会经历生产、存储、运营等过程，在此过程中缺少数据安全感知、告警、审计溯源处置体系，无法达到“事前预防+事中防范+事后溯源取证”的立体防御效果。

# 4 解决方案设计

## （1）制造业数据安全技术体系设计

制造业数据安全技术体系设计，以自身网络现状及业务情况为基础进行全面纵深防御建设，以实现厂内的制造业数据安全可视、安全可控、安全可管。首先，从数据安全基础环境开始建设，保障整个数据流所处网络环境安全可信；其次，对于重要及核心数据进行细致化的防护建设，防止数据破坏、数据泄漏等事件的发生；最后，通过搭建制造业数据安全运营中心，对整个厂内的基础环境态势、数据安全态势进行可视化展示，切实提升全厂安全指挥调度和应急响应能力。

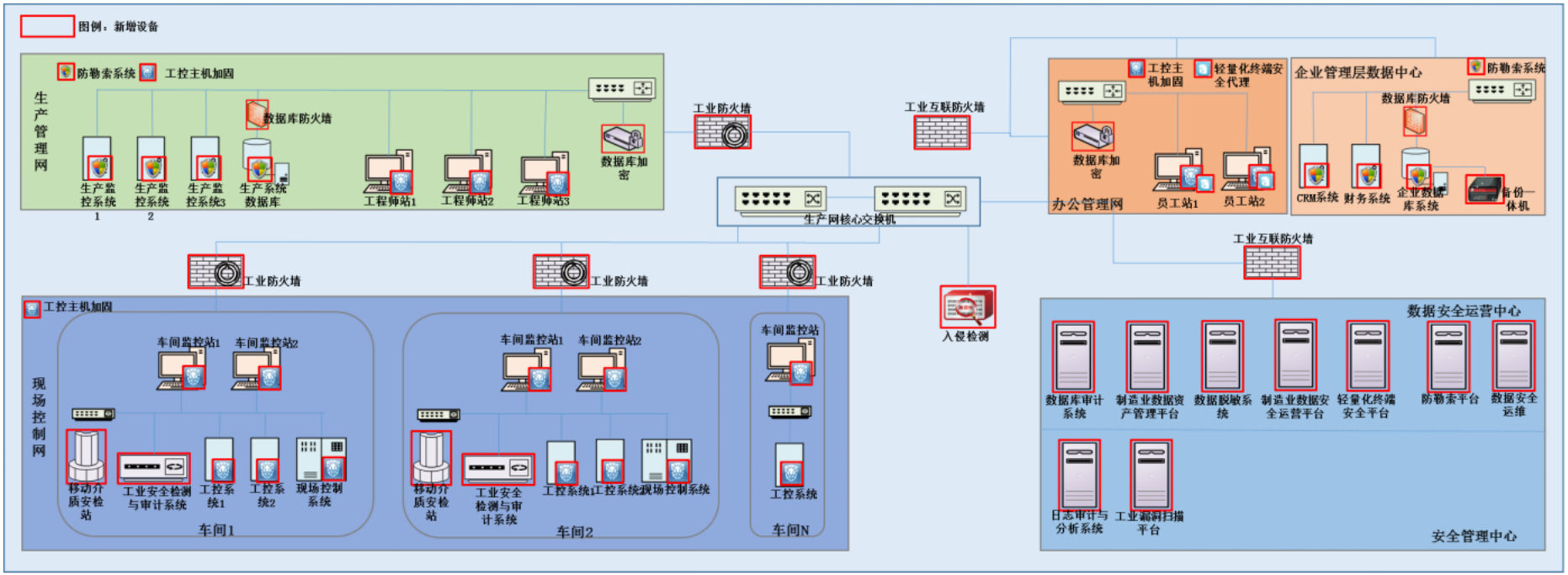


图 3 数据安全技术部署拓扑

## 1）重要及核心数据防护能力建设

基于数据安全基础环境的建设使得厂内网络整体具有一定的安全防护能力，不过制造业生产数据作为最重要的资产，对于重要及核心数据的存储、使用、传输、提供等阶段还需要进行更为细致化的防护。

（a）在安全管理中心部署一台数据库审计系统，将厂内核心交换机上数据访问流量镜像过来，从而对数据库的进出流量进行审计，及时发现流量中存在异常操作指令及 SQL 注入等恶意攻击。

（b）在数据安全运营中心中部署数据脱敏系统，通过多种脱敏方案，实现脱敏后的数据仍然可以保留原有的语义和关联关系，保证数据在各个场景中的可用性、规范性以及真实性，测试、数据分析等多种场景下的数据安全性和有效性。

（c）在安全管理中心部署数据安全运维系统，通过独立和统一的身份认证、权限控制、脚本审核和管理、交互式脱敏、以及数据运维操作台，构建安全的数据运维环境。数据库用户账号有泄露风险或数据库用户越权查看敏感数据的风险。

（d）生产管理网和办公管理网数据服务区前部署数据库防火墙。控制数据访问行为，主动实时监控、识别、告警、阻断针对数据库的安全威胁。

（e）对厂内网中 OA 服务器、邮件服务器、财务服务器、终端机等系统部署防勒索软件，通过勒索检测、关键业务数据保护、关键数据保护和关键数据备份等多个维度的防护机制，来防止勒索病毒攻击从而造成数据无法解密的情况。

在安全管理中心部署防勒索管理平台，对企业中的防勒索软件进行统一管理、统一策略配置，及时收集防勒索软件产生的日志和告警并根据风险等级快速给出处置措施。

（f）在生产管理网和办公管理网数据服务区前部署数据库加密设备，保障数据的机密性和完整性。

（g）在生产管理网和办公管理网重要数据留存终端上部署轻量化终端代理，避免终端在使用过程中留存的重要数据泄露。

（h）在企业管理层数据中心部署备份一体机，对重要系统数据进行备份。

## 2）制造业数据安全管理中心及运营中心建设

在基础环境全面建设及重要核心数据细致化防护建设完成后，需要对数据安

全健康指数进行统一的汇总展示，打造一个全局视角的制造业数据安全运营中心，包括制造业数据资产管理平台、数据安全运营平台。通过制造业数据安全运营中心的建设可切实提高厂内对数据和环境的安全感知能力，有效提高全厂的指挥调度及响应处置效率。

（a）在数据管理中心部署一套制造业数据资产管理平台；通过对厂内数据梳理及价值分析进行自动化分类分级，同时结合人工判定辅助，确保最基础的数据识别工作的安全可靠，从而保障整个数据安全防护体系的持续性及可靠性。

（b）在数据管理中心部署制造业数据安全运营平台；以数据的全局视角将厂内所有数据全生命周期的状态进行展示，包括数据画像、数据流向、数据风险、数据溯源等维度，从而对重要及核心数据可能存在的风险并给出相应的解决建议。

## （2）制造业数据安全运营服务体系设计

### 1）数据安全评估

从组织到人员，从制度到技术来评估制造业数据安全情况。通过访谈、文档查阅、系统查看和利用检测工具等方法调研工厂内相关的保护制度、安全规划和流程，以及监管现状和当前工厂具备的能力现状，进行现状的情况梳理，并利用相关的评估工具识别问题，依据问题编制整改建议，并持续跟进评估。

最后结合工厂当前的组织结构、人与水平、技术能力、制度情况，编写数据安全评估报告，反馈出当前的安全现状和问题及风险点，提供相关的整改建议，确定整改落实情况，给出最终的评估结果。

### 2）数据安全资产梳理

以法律法规要求、行业标准为基础，明确该企业所拥有的数据资产详情，以此为基础建立相关安全策略和规章制度。

针对于数据资产梳理服务，通过技术人员的对工厂的资产情况进行摸查，确定资产情况，以及敏感数据的分布情况，然后针对这些数据分阶段进行梳理，逐步细化，最后形成相应的数据资产清单，针对不同的数据形成相关防护策略，确定敏感数据情况，从而实现数据的分类分级，数据的合规管控。

### 3）数据安全运营保障

保障日常的安全使用和维护。组建一支专职或第三方的技术精湛、专业、稳定的技术团队，多位在网络、主机、数据库、安全等多个领域具体丰富的实践经验的资深工程师。并对该队伍进行工具、交通、财力等进行专门保障。

### （3）制造业数据安全管理体系设计

以合规要求、风险要求、业务要求为驱动，不断利用计划-保护-评价-改进-管理模型，持续改进相关管理办公和管理规章制度。

针对于工厂的数据安全管理制度方案，相关制度体系需要覆盖数据全生命周期的内部和外部场景，做好事前防范、事中管控和事后稽查与审计。事前防范中，基础部分需明确组织责任管理、人员岗位管理、数据资产管理、人员的教育培训管理、保密管理和分类分级管理；对外部则需明确数据出境规范要求、合作方调研审查的制度（如有数据处境相关场景）。事中管控基础部分要确定人员及权限管理、个人信息保护管理和合规评估管理制度，企业内部需明确数据的采集管理、传输管理、存储管理、使用管理、开放共享管理和销毁管理制度；对外同样需明确数据出境规范要求、合作方调研审查的制度（如有数据出境先关场景）。在事后稽查与审计中，基础则需具备安全审计管理、应急处置管理、投诉举报管理、监督检查考核问责管理制度，对外需明确合作方考核制度。

## 5 产品清单

| 序号 | 设备名称 | 部署目标 | 单位 | 部署位置 |
|---|---|---|---|---|
| **制造业数据安全产品** | | | | |
| 1 | 制造业数据资产管理平台 | 通过主动扫描方式与数据库协议分析，结合高效数据识别与可视化等技术，实现自动化数据分类分级及数据资产动态分析。提供相关接口以便快速打通安全链上下游能力，为全局性数据态势感知与数据精准差异化管控提供有效支撑。 | 台 | 部署于数据安全运营中心。 |
| 2 | 制造业数据安全运营平台 | 统一数据分类模型管理；数据安全风险态势感知；统一数据安全风险分析；敏感数据形态及运行轨迹可视化展示；数据安全日志关联分析；平台配置管理。 | 台 | 部署于数据安全运营中心。 |
| 3 | 轻量化终端安全代 | 对敏感数据智能标注；敏感数据形态变化跟踪；敏感数据运行轨迹跟踪；敏感数据隐写变形跟踪； | 点 | 部署于生产控制网，具有重要数据的主机系统 |

| 序号 | 设备名称 | 部署目标 | 单位 | 部署位置 |
|---|---|---|---|---|
| | 理 | 敏感数据数字水印跟踪。 | | 上。 |
| 4 | 数据脱敏系统 | 静态脱敏系统，提供多种脱敏方案，保证脱敏后的数据仍然可以保留原有的语义和关联关系，保证数据在各个场景中的可用性、规范性以及真实性。 | 台 | 部署于数据安全管理中心；对于需要外发的数据进行脱敏。 |
| 5 | 数据库审计系统 | 实时监控记录用户对数据库的所有访问行为，并对数据库所遭受的风险行为进行告警，提供丰富的日志检索和多维度的统计报表，实现对事故的追根溯源。 | 台 | 部署于数据安全管理中心；对所有访问数据进行审计和记录。 |
| 6 | 数据库防火墙 | 基于身份鉴别和行为分析的主动防御机制，主动实时的监控、识别、告警、阻断针对数据库的安全威胁，实现数据库的行为特征分析、访问行为监控和危险操作阻断。 | 台 | 部署于数据服务区数据库服务器前；对所有访问数据进行检测和防护。 |
| 7 | 数据库加密 | 保护数据库内部重要数据的安全。重要数据以密文的形式存储，保证即使在存储介质被窃取，或数据文件被非法复制的情况下，保障数据安全。 | 台 | 部署于数据服务区，对重要敏感数据进行加密防护。 |
| 8 | 备份一体机 | 备份管理软件，实现数据库备份和回复，实现操作系统下的整机备份和裸机恢复，支持文件备份和恢复。 | 台 | 企业管理网数据中心。 |
| 9 | 数据安全运维 | 提供统一的组织管理方式，批量的管理各类运维账号。针对每个运维账号的使用人员，采用多种组合的认证方式，能够唯一认证用户身份，并监控运维账户的每一个操作和 SQL 的执行，能够精细化的控制运维账号的权限最大化的减少了敏感数据的暴露面，防止数据在运维环节被越权访问和非法窃取。 | 台 | |
| 10 | 防勒索系统管理平台 | 对企业中的防勒索软件进行统一管理、统一策略配置，及时收集防勒索软件产生的日志和告警并根据风险等级快速给出处置措施。 | 台 | 部署于数据安全管理中心；<br>对防勒索软件进行统一管理。 |
| 11 | 防勒索系统 | 通过勒索检测、关键业务数据保护、关键数据保护和关键数据备份等多个维度的防护机制，来防止勒索病毒攻击从而造成数据无法解密的情况。 | 点 | 对于内网重要服务器进行部署；防止重要数据被加密和破坏。 |
| **安全运营服务** | | | | |
| 1 | 数据运营咨询服务 | 咨询服务、梳理服务、管理体系、报告。 | 项 | 包括数据梳理、管理体系搭建、报告材料编写等。 |

# 6 客户效益价值

## （1）合规性收益

紧跟政策法规指导思想，贯彻落数据安全国家政策文件的根本要求，履行社会责任，避免数据安全期泄露威胁。

## （2）安全性收益

以数据安全为底座，保障组织数据安全机密性、完整性、可用性，保障业务持续稳定运行。

通过建设数据安全体系，加强了业务保护能力，加大了数据防护范围，加深了数据保障能力，弥补了传统防护技术短板，提升组织整体应对能力，在业务与数据之间建立“内城护城河”，有效解决新技术风险对数据的破坏行为。

## （3）经济效益收益

数据已成为驱动业务、经济发展的核心要素，保障其安全是关注重点。数据安全以数据为核心，通过对业务场景数据梳理，建设动态的、可持续的数据安全体系，从而实现企业业务线稳定的、持续的释放数据价值。通过数据安全建设，减少因数据破坏造成的经济损失，同时提升数据经济竞争能力。