启明星辰
www.venustech.com.cn

启明星辰|大模型应用安全|深度应用安全基座系列白皮书

AI就绪的安全数据通层

AI-R-SDLayer V1.0

AI-Ready Security Data Layer

启明星辰信息技术集团股份有限公司

2025年2月

版权申明

免责申明

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京启明星辰信息安全技术有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京启明星辰信息安全技术有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈：

信箱：北京市海淀区东北旺西路 8 号中关村软件园 21 号楼启明星辰大厦　邮编：100193 电话：010-82779088

传真：010-82779000

您可以访问启明星辰网站：www.venustech.com.cn 获得最新技术和产品信息。

目录

1 公司简介 1
2 背景与战略意义 3
2.1 政策及行业环境 3
2.2 技术趋势 4
2.3 挑战 6
2.4 战略意义 8
2.5 市场分析 9
2.6 行业发展及数据标准现状 10
2.6.1 国内外厂商大数据平台建设理念 10
2.6.2 数据标准现状 12
3 定义与建设思路 14
3.1 定义 14
3.2 发展愿景 15
3.3 建设思路 16
4 技术架构与关键技术 19
4.1 技术架构设计 19
4.2 关键技术 19
5 中国移动及启明星辰的实践案例与技术积累 23
5.1 典型案例 23
5.1.1 AI-R-SDLAYER DAAS 服务助力一体化云原生安全平台建设 23
5.1.2 AI-R-SDLAYER DAAS 服务赋能安全能力平台构建智能化安全运营体系 24

5.1.3 AI-R-SDLAYER 赋能智能威胁情报体系，构建自主进化型防御能力.....25

5.1.4 AI-R-SDLAYER 作为大数据能力底座赋能运营商行业安全数据中心.....28

5.2 技术积累奠定 AI 就绪的安全数据通层建设基础.....28

6 大模型时代企业管理者的十大倡议.....30

1 公司简介

启明星辰公司成立于 1996 年，由留美博士严望佳女士创建，是国内最具实力的、拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。2010 年 6 月 23 日，启明星辰在深交所中小板正式挂牌上市。

启明星辰拥有完善的专业安全产品线，横跨防火墙/UTM、入侵检测管理、网络审计、终端管理、加密认证等技术领域，共有百余个产品型号，并根据客户需求不断增加。启明星辰解决方案为客户的安全需求与信息安全产品、服务之间架起桥梁，将客户的安全保障体系与信息安全核心技术紧密相连，帮助其建立完善的安全保障体系。

自 2002 年起，启明星辰就持续保持国内入侵检测、漏洞扫描市场占有率第一。近年来，发展成为国内统一威胁管理、安全管理平台国内市场第一位，安全性审计、安全专业服务市场领导者。目前，公司在全国各省市自治区设立三十多家分支机构，拥有覆盖全国的渠道和售后服务体系。

长期以来，启明星辰公司得到了党和国家领导人的关怀与鼓励。2000 年 1 月，江泽民、李岚清、曾庆红等党和国家领导人亲切视察启明星辰公司；2003 年 1 月，胡锦涛总书记亲切接见了启明星辰公司 CEO 严望佳博士。

凭借多年来的潜心研发，启明星辰获得国家规划布局内重点软件企业，国家火炬计划软件产业优秀企业，中国电子政务 IT100 强等荣誉，及拥有最高级别的涉及国家秘密的计算机信息系统集成资质证书。

启明星辰目前是我国规模最大的国家级网络安全研究基地。完成包括国家发改委产业化示范工程，国家科技部 863 计划、国家科技支撑计划等国家级科研项目近百项。创造了

百余项专利和软件著作权，参与制订国家及行业网络安全标准，填补了我国信息安全科研领域的多项空白。

作为信息安全行业的领军企业，启明星辰以用户需求为根本动力，研究开发了完善的专业安全产品线。通过不断耕耘，已经成为在政府、电信、金融、能源、交通、军队、军工、制造等国内高端企业级客户的首选品牌 ： 启明星辰在政府和军队拥有 95%的市场占有率，为世界五百强中 80%的中国企业客户提供安全产品及服务；在金融领域，启明星辰对政策性银行、国有控股商业银行、全国性股份制商业银行实现 90%的覆盖率。在电信领域，启明星辰为中国移动、中国电信、中国联通三大运营商提供安全产品、安全服务和解决方案。

作为北京奥组委独家中标的核心信息安全产品、服务及解决方案提供商，奥组委唯一信息安全供应商，启明星辰受到独家官方授权，全面负责奥运会主体网络系统的安全保障，得到了国家主管部门的大力嘉奖。此外，启明星辰还为上海世博会、广州亚运会等多项世界级大型活动提供全方位信息安全保障。

在公司快速稳定发展的同时，启明星辰公司坚持以爱心回馈社会，截止目前，已累计资助贫困学子、受灾、贫困群众上亿元人民币，并在江西、青海、新疆等地援建了 5 所希望小学。

启明星辰公司将秉承诚信和创新精神，继续致力于提供具有国际竞争力的自主创新的安全产品和最佳实践服务，帮助客户全面提升其 IT 基础设施的安全性和生产效能，为打造和提升国际化的民族信息安全产业第一品牌而不懈努力。

2 背景与战略意义

2.1 政策及行业环境

AI 就绪的安全数据通层（AI-R-SDLayer，AI-Ready Security Data Layer）的建设立足于国家数字经济发展的大方向，结合行业标准化发展的实际需求以及中国移动 BASIC6 战略，旨在通过整合与优化数据资源，为数字化转型和智能化发展提供有力支撑。

国家层面，近年来持续强化数据要素在数字经济中的核心引擎作用。《“十四五”数字经济发展规划》明确提出数据要素是数字经济深化发展的核心；《数字中国建设整体布局规划》提出“夯实数字基础设施，强化数据资源体系建设”；《“数据要素 x”三年行动计划（2024—2026）》聚焦数据要素赋能经济社会高质量发展，为平台建设提供了政策保障。

行业层面，中国信通院及相关政府机构通过大数据白皮书、《GA/T 1393-2017 公共安全行业标准》和《GB/T 40298-2023 大数据平台数据治理规范》等推动平台技术标准化和数据治理规范化，为大数据平台建设提供了指引。

在中国移动 BASIC6 战略框架下，大数据（B）是推动整体战略落地的关键要素。AI 就绪的安全数据通层通过以下方式助力 BASIC6 战略：

- **B（大数据）**：大数据是 BASIC6 的核心，通过构建统一数据底座，整合海量异构数据资源，实现集团级数据共享和协同分析。
- **A（人工智能）**：AI 就绪的安全数据通层可以为 AI 模型提供高质量的训练与推理数据集，提升模型的精确度和智能化水平。
- **I（能力中台）**：通过数据治理和标准化能力支撑中台服务，强化跨部门的数据协作与资源调度能力。

- **C（算力网络）**：优化数据流通与分布式计算能力，为多云环境下的资源高效调度提供支持。

AI 就绪的安全数据通层的建设聚焦中国移动战略需求，结合国家数字化发展的政策导向，通过统一数据治理和跨平台资源整合，逐步打造一个数据驱动、安全智能、全域协同的新型安全基础设施。该平台不仅将支撑 BASIC6 的核心需求，还将在未来推动更广泛的智能化和数据要素价值释放，为集团战略的全面实施奠定基础。

2.2 技术趋势

AI 就绪的安全数据通层的构建，不仅需要紧密结合最新的技术发展趋势，更应深刻把握这些技术在构建安全数据基础设施中的独特价值。从“数智基建”到“数据编织”，再到“数联网”，这些前沿理念为安全大数据的智能化、协同化和高效化提供了新的路径。

2024 年，Gartner 提出的“数智基建”是一种聚焦于数据、分析和人工智能生态建设的新型部署模式。它整合了分析型数据库、元数据管理、数据质量控制和数据虚拟化等核心能力，旨在为多样化的数据分析与 AI 应用场景提供统一的技术底座。在多云及跨云环境日益普及的今天，“数智基建”通过部署方式的灵活性，支持企业快速适应复杂的数据管理需求，尤其在生成式 AI 的落地中提供了强大的支撑。“数智基建”的理念为 AI 就绪的安全数据通层的建设提供了方向，确保数据在多源异构和高并发环境下保持一致性和高效流转，并为后续智能分析功能奠定了基础。

数据编织作为一种新型的数据管理设计，强调通过智能化的集成管道和语义增强，提供灵活且可扩展的数据服务能力。它通过主动元数据驱动和知识图谱构建，不仅降低了传统数据治理的复杂性，还能够自动化地适配多云或混合云环境中的动态数据需求。数据编织为 AI 就绪的安全数据通层解决数据孤岛和多源数据协作难题提供了突破口，通过动态化

的数据集成与调度能力，AI 就绪的安全数据通层能够支持复杂场景下的数据关联分析和实时交付，同时减少不必要的数据复制，优化资源利用效率。

数联网通过构建跨行业、跨领域的集约化数据流通网络，推动数据要素的高效流通。其核心能力包括数据接入的标准化、流通处理的多形态支持，以及面向场景化的数据交付能力。数联网不仅是一种技术实现，更是推动数据资源优化配置的实践路径。

在 AI 就绪的安全数据通层中，数联网的理念为跨部门、跨系统的数据共享和流通提供了参考模型。通过灵活的数据权限管理和动态资源分配，平台可以支持复杂的多方协作需求，同时确保数据流转的高效性和可靠性，为多维度的安全分析和业务联动创造可能。

Gartner 在 2022 年的战略技术趋势报告中提出的网络安全网格架构（CyberSecurity Mesh Architecture，CSMA），旨在应对传统安全工具孤立运行和协同不足的问题。作为 CSMA 的核心数据支撑层，AI 就绪的安全数据通层通过统一的数据采集和治理，打破了数据孤岛，实现多源异构数据的高效整合与流转，同时提供跨域数据整合、分布式计算和元数据驱动治理能力，为 CSMA 的智能化分析和动态响应奠定了坚实基础。AI 就绪的安全数据通层的分布式架构支持安全数据在多云环境中的实时共享与协作，有效提升了 CSMA 在统一策略管理、智能威胁感知和动态扩展方面的效率与适应性。通过提供全面而准确的数据支持与智能化能力，AI 就绪的安全数据通层不仅赋能安全工具的有机聚合，还为网络安全的深入应用和复杂业务场景的动态扩展提供了重要支撑，是实现 CSMA 不可或缺的关键基石。

结合以上技术趋势，AI 就绪的安全数据通层在构建安全数据基础设施中扮演着不可或缺的角色。从“数智基建”的灵活部署和统一底座建设，到“数据编织”的动态集成和智能化治理，再到“数联网”的高效数据流通和场景化交付，这些理念为平台的规划和设计提供了明确的方向。同时，网络安全网格架构（CSMA）的提出进一步强化了平台在安全

数据协作中的价值。通过整合多源数据、优化资源调度和提升智能化分析能力，AI 就绪的安全数据通层不仅为安全工具的协同与扩展奠定了技术基础，也为多场景安全需求的实现提供了全方位支持，成为推动安全大数据技术迈向智能化、高效化的关键推动力。

2.3 挑战

在中国移动 BASIC6 战略的引领下，建设 AI 就绪的安全数据通层已成为提升数据利用效率和强化网络安全能力的重要举措。随着业务规模的快速扩展和网络威胁的不断升级，现有数据管理与安全运营模式面临数据分散、协同不足等瓶颈，迫切需要通过统一的 AI 就绪的安全数据通层破解这些难题，为更高效的数据治理与安全运营奠定基础。以下将聚焦当前面临的主要挑战，进一步阐明建设 AI 就绪的安全数据通层的必要性。以下为当前面临的主要挑战：

- **复杂攻击难以检测，全面元数据支持迫在眉睫：**网络安全攻击日益复杂，攻击者采用高级持续性威胁、0 Day 漏洞利用、多阶段渗透及分布式攻击等策略，其隐蔽性和破坏性显著增强。这种复杂攻击场景需要全面、精准的元数据支持，确保安全团队能够及时捕获威胁信号并快速做出响应。如果缺乏充足的元数据，安全团队将难以及时、准确地识别和响应威胁。
- **跨区域与长周期攻击，亟需 AI 就绪的安全数据通层支持：**攻击者经常利用分布式网络、代理服务器等手段进行跨区域攻击，并通过长期潜伏逐步渗透系统。这种攻击方式大幅增加了威胁溯源和防御的难度。面对这种挑战，只有强大的 AI 就绪的安全数据通层能够整合多源异构数据，并提供统一的数据分析能力，从而有效支持安全团队对高级威胁的精准识别和联动防御。

- **数据分散阻碍安全分析，流通与沉淀不足：**当前，各业务数据系统独立运行，导致数据分散、标准不统一，形成了数据孤岛，阻碍了跨系统的关联分析。此外，由于缺乏长期数据沉淀，导致数据积累严重不足，这进一步限制了安全团队的深度分析和威胁预测能力。统一的数据管理机制不仅能够提升数据流通效率，还能通过沉淀高质量历史数据，为复杂分析场景提供有力支持。
- **研发成本高企，重复建设阻碍资源整合：**各业务部门均独立开发维护数据系统，存在功能重复开发和资源浪费的现象。此外，重复建设还增加了运营成本，不利于系统的协同管理与整合发展。通过构建统一的大数据能力底座，可以有效减少重复建设，提高资源利用率，并显著降低整体运营成本。
- **数据瓶颈限制 AI 应用拓展：**人工智能在网络安全中的应用依赖高质量且语义一致的数据支持。然而，现有系统中数据分散且质量参差不齐，难以满足 AI 模型在训练和推理阶段的需求。数据语义不一致进一步削弱了模型的泛化能力，限制了智能化威胁检测和分析的效果。构建统一的 AI 就绪的安全数据通层能够为 AI 应用提供一致、高质量的数据支撑，显著提升智能化能力。

面对复杂多变的网络安全环境和日益增长的数据需求，AI 就绪的安全数据通层的建设既是应对现有挑战的迫切需求，也是推动数据价值转化、支撑智能化发展的关键手段。通过解决数据分散、标准不一等痛点，平台将为智能化安全运营和 AI 创新赋能提供有力支撑。

2.4 战略意义

AI 就绪的安全数据通层在数据治理、资源优化、技术创新和数据流通等方面具有重要战略价值。通过强化元数据驱动、实现资源高效配置、支撑数据与智能深度融合，以及推动数据要素流通，为企业提供了面向未来的核心竞争力。

首先，AI 就绪的安全数据通层通过强化元数据驱动的数据治理能力，建立数据全生命周期管理机制，显著提升数据质量和数据积累效益。元数据作为连接多源异构数据的核心枢纽，不仅能够统一标准、优化数据整合，还为数据的一致性和高效流转提供了技术保障。这一能力对于企业在应对复杂数据环境时尤为重要，有助于数据资产的价值释放，支撑业务的深入分析与智能决策。

其次，AI 就绪的安全数据通层在降低研发和运营成本方面发挥重要作用。一方面，通过统一架构减少公司内部大数据平台和组件的重复建设，优化资源分配，业务部门可使用 AI 就绪的安全数据通层的底层架构，避免重复开发。另一方面，作为数据基础设施，平台通过 PaaS 服务形式提供数据采集、治理、分析和共享能力，借助分布式架构实现资源的高效调度与分配，降低运维成本，提升资源利用效率。

在技术创新领域，AI 就绪的安全数据通层为“数据+AI”的深度融合提供了坚实基础。高质量数据是人工智能技术发展的前提，平台通过跨域数据整合、数据质量优化和高效流转，为 AI 模型的训练和推理提供全面的数据支持，从而推动智能威胁感知、动态策略优化等领域的技术创新。AI 就绪的安全数据通层的智能化能力不仅提升了企业技术竞争力，也推动了数据与智能的深度融合，为新一代数字化技术的发展开辟了新路径。

此外，AI 就绪的安全数据通层在加强数据要素流通和价值释放方面具有不可替代的作用。通过构建高效的企业数联网，平台打通了跨系统、跨部门的协作壁垒，实现了数据的

共享与精准流转。这种数据流通能力不仅提升了内部业务的协同效率，还为构建跨行业、跨领域的数据生态体系奠定了基础，助力数据要素的高效配置与市场化运作。

综上所述，AI 就绪的安全数据通层在数据治理、资源优化、技术创新和数据流通方面展现出战略意义。它的建设将推动企业从数据孤岛走向协同创新，从资源分散迈向高效利用，从单点技术突破迈向智能化发展，为企业在数字经济时代占据制高点提供了坚实支撑。

2.5 市场分析

随着网络安全需求的持续增长和大数据技术的快速演进，AI 就绪的安全数据通层在安全大数据市场展现出广阔的发展前景。作为智能化、数据驱动的核心基础设施，AI 就绪的安全数据通层通过独立产品化、跨产品集成化以及内部价值转化等模式，不断拓展应用场景并提升市场竞争力。

在独立产品化方面，AI 就绪的安全数据通层可作为标准化的安全数据解决方案，提供高效能的数据存储、计算与分析能力，以满足安全数据管理和智能分析的需求。同时，平台通过构建统一的数据治理体系，实现数据的标准化管理，增强数据的可用性、安全性和共享能力。

在跨产品集成化方面，AI 就绪的安全数据通层作为底层大数据能力支撑，广泛融入各类安全产品体系，实现数据的高效存储、智能分析和安全运营协同。这一模式不仅提升了安全产品的整体竞争力，还推动了跨产品的数据融合，为复杂安全场景提供更精准的威胁检测、溯源和响应能力。

在内部应用价值方面，AI 就绪的安全数据通层通过数据的集中治理和智能流转，提升安全运营效率，优化资源利用，降低运营成本。同时，平台依托高效的数据流通和深度整

合能力，促进数据在不同业务场景间的协同应用，实现安全数据的价值最大化，助力安全体系向数据驱动、智能协同的方向持续演进。

2.6 行业发展及数据标准现状

2.6.1 国内外厂商大数据平台建设理念

在信息安全行业，大数据技术正成为提升威胁检测、风险管理和安全运营能力的核心推动力。为了应对多源异构数据整合、安全分析智能化、数据流通与治理的复杂需求，众多领先厂商推出了安全数据中台，提供集成化、智能化的解决方案。以下重点分析部分国内外代表厂商的安全业务大数据产品及其特点。

Palantir：专注于数据整合、分析与智能化应用，其 Foundry 平台通过整合企业数据湖和仓库资源，提供强大的双向数据流与细粒度的数据治理能力。2023 年推出的人工智能平台（AIP）集成了大语言模型，进一步增强了数据驱动的智能分析和业务决策能力，为企业提供更高效的安全大数据管理和应用。

Palo Alto Networks：Strata Logging Service（原 Cortex Data Lake）通过统一的数据湖架构，整合分散的安全数据资源，显著提升了威胁检测和分析能力。平台自动化的数据收集和规范化治理能力为安全运营提供了更高效的支持，同时为 AI 驱动的复杂安全场景奠定了坚实基础。

CrowdStrike：Falcon 平台凭借单一代理和统一控制台的架构，在网络安全管理中实现了高效的整合与优化。平台通过统一的安全视图和简化的资源配置，大幅提升了安全运营效率，降低了系统部署与维护成本，为企业的安全能力提升提供了极高的灵活性。

Databricks：Databricks 以统一格式和开放引擎的数据湖范式引领行业，通过完整技术栈覆盖从数据治理到大模型应用的全链条能力。平台通过结构化与非结构化数据的联合

召回、实时和离线分析能力，为企业在数据智能化和安全分析领域提供了强大的技术支持。

安恒：数盾数据安全管理平台面向全流域安全数据治理，提供资产识别、动态数据风险分析与态势感知能力。平台通过数据的全面梳理和建模，实现动态防护与业务安全协同，支持复杂安全业务的数据管理与智能分析，提升企业安全数据应用的整体效率。

亚信：AISWare Data OS 和 AISWare Data Infrastructure 以数据要素为核心，构建跨场景、跨平台的大数据基础设施。AISWare Data OS 以元数据驱动覆盖数据全生命周期管理，提供全景化操作能力；AISWare Data Infrastructure 通过湖仓一体化架构和多模数据管理能力，为企业提供高效的大数据协作和分析支持，推动智能化应用场景的进一步落地。

腾讯 T-Sec：T-Sec 的安全湖基于云原生技术，整合安全数据接入、存储、分析和告警能力，构建高效湖仓一体化安全分析平台。平台通过灵活的插件化应用开发能力，支持企业在复杂场景下实现高性能的数据协作和快速响应，为安全大数据的智能分析提供全面支持。

当前安全大数据产品在以下几方面展现出核心竞争力：

- 统一数据底座构建：采用统一数据湖或湖仓一体架构，通过多源异构数据整合与规范化处理，为跨域分析和协同应用奠定基础。
- 智能分析与优化能力：引入 AI 技术优化数据分析流程，特别是在威胁感知、动态风险评估和实时分析场景中展现出显著优势。
- 数据积累的重要性：在安全大数据领域，数据积累已成为提升平台价值的关键要素。长期稳定的数据积累不仅支持精准建模和风险预测，还为大规模 AI 训练和业务优化提供了不可或缺的基础。

- 业务场景支持能力：围绕复杂安全场景的需求，提供定制化的数据服务与分析能力，以增强业务敏捷性和系统响应能力。

未来，安全大数据产品将进一步加强数据积累和长期价值转化能力，推动从功能性优化到智能化决策支持的全面发展，为企业提供更高效、更可靠的数据驱动解决方案。

2.6.2 数据标准现状

在全球数字化发展和云网融合的背景下，数据标准已成为多源异构数据协作与价值挖掘的核心要素。国内外在语义规范、接口规范和数据标准规范方面的探索，为 AI 就绪的安全数据通层的构建提供了重要参考。

语义规范旨在为数据共享和安全能力联动提供统一的语言与表达方式。国际上，2017 年由美国国家安全局（NSA）牵头推出的 OpenC2 规范，通过标准化“动作-目标”编排语言，促进了防火墙和沙箱等安全产品的自动化联动。

接口规范为不同系统间的数据交换和功能集成提供技术支持。国际上，TAXII 和 OpenDXL 是威胁情报共享和安全协作的典型接口规范，至 2020 年 OpenDXL 已被 4000 多个组织使用。中国已在安全日志、恶意程序样本等信息互通方面发布了接口行业规范，如 YD/T 3496-2019《Web 安全日志格式及共享接口规范》、YD/T 2849-2015《移动互联网恶意程序疑似样本报送接口规范》等，初步实现了安全日志和恶意程序样本信息的接口共享标准化。此外，中国通信标准化协会（CCSA）启动了 SOAR、SASE、安全中台等新安全技术产品与其他类安全功能间的接口规范化研制，为新型安全技术的应用奠定基础。

数据规范领域，国际标准有 STIX（结构化威胁信息表达）和 OpenIOC（开放威胁指标）等，这些标准通过定义威胁情报的格式和序列化规则，实现威胁情报的交流共享。中

国已面向威胁情报、WEB 漏洞、终端漏洞、源代码漏洞等形成了国家标准和行业标准，为安全产品间交互共享各类漏洞威胁信息提供了规范化格式，相关标准包括 GB/T 28458-2012 《信息安全技术 安全漏洞标识与描述规范》、GB/T 36643-2018 《信息安全技术 网络安全威胁信息格式规范》、YD/T 3448-2019 《联网软件源代码漏洞分类及等级划分规范》、YD/T 3667-2020 《移动智能终端漏洞标识格式要求》、YD/T 3955-2021 《WEB 漏洞分类与定义指南》 等。

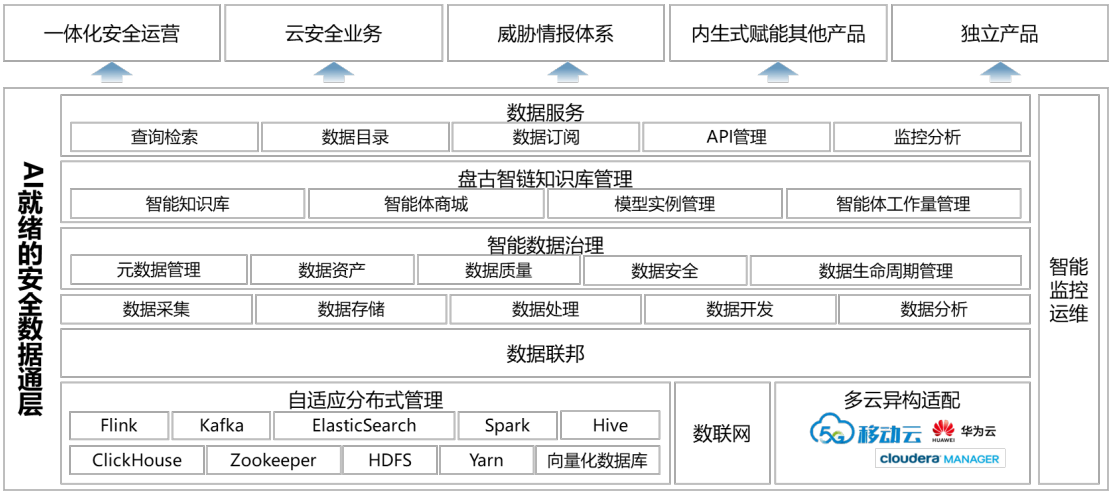
AI 就绪的安全数据通层需积极吸收国内外的经验与实践，在语义、接口和数据规范三方面推动数据标准化的落地与优化。通过标准化的推进，平台将更好地支持数据资源的高效流通与价值挖掘，为业务智能化和安全运营提供坚实保障。

3 定义与建设思路

3.1 定义

AI 就绪的安全数据通层（AI-R-SDLayer）是一款面向智能化、数据驱动和全域协同的安全数据基础设施，基于元数据驱动的数据治理能力，构建高质量、安全可信的数据底座，为大模型提供 AI 就绪数据，支撑智能安全分析与自动化运营。平台整合多源异构数据，通过统一的数据模型、主动元数据治理和智能分析，实现日志、流量、资产、漏洞、用户行为等安全数据的标准化管理，并依托数据编织与联邦查询技术，打破数据孤岛，实现跨业务、跨平台的数据共享与威胁情报协同。AI-R-SDLayer 结合云原生架构和多云环境的高适应性，提供从数据采集、存储、处理、分析到服务化的全流程数据管理，构建企业级数据资源的统一管理与智能治理体系。

AIR - SDL 内置私域安全知识库和安全知识图谱，其中盘古智链知识库管理子系统作为私域安全知识库的重要组成部分，基于 DeepSeek 等前沿大模型技术构建，沉淀企业安全经验，并结合大模型的语义解析能力，提升威胁检测、攻击溯源和安全策略优化能力。通过智能知识库管理、智能体商城、模型实例管理和智能体工作流等功能，实现知识的全生命周期智能化管理，为安全分析提供更精准、高效的知识支撑。



3.2 发展愿景

AI 就绪的安全数据通层作为企业级数据管理的核心基础设施，承载着推进数据治理、赋能技术创新的战略使命。在中国移动 BASIC6 战略框架下，平台以大数据（B）、人工智能（A）、能力中台（I）和算力网络（C）为依托，全面构建高效的数据管理与流通体系，推动数据价值的深度挖掘与转化。

支撑大数据（B）：AI 就绪的安全数据通层通过统一治理和流通，整合多源异构数据，建立标准化模型和集中管理机制，显著提升数据的一致性与可用性，推动数据从被动存储向主动价值挖掘转变。

赋能人工智能（A）：平台优化了数据采集、治理和标注，为 AI 模型提供高质量的数据资源，并通过实时数据流通和分布式处理，显著提升 AI 推理的响应速度和应用效率。此外，AI 就绪的安全数据通层还将引入 AI 技术来优化自身功能，提升数据质量管理和智能运维水平，形成数据与智能的深度融合。

服务能力中台（I）：平台通过高效灵活的数据服务，降低能力中台的数据处理复杂性，支持其快速响应业务需求。标准化的数据接口与流程进一步优化了开发效率，提升了业务扩展能力和协同水平。

优化算力网络（C）：平台通过智能化的多云资源调度和高性能数据处理能力，提升了算力网络的计算效率与资源利用率。数据分层存储与优化技术确保了算力与数据需求的精准匹配，推动计算资源的高效利用。

推动数联网与数据要素化：AI 就绪的安全数据通层通过数据标准化与网络化，实现跨部门、跨业务的数据互联互通，推动数联网基础设施建设。同时，平台通过赋能数据要素

市场化，提升数据资源的经济价值与市场效益，为集团在安全数据生态领域的布局提供技术支持。

结合 BASIC6 战略，平台将不断深化数据治理、优化资源配置、支撑技术创新，进一步助力集团抢占行业制高点，为智能化、协同化的安全数据生态建设注入持续动能。

3.3 建设思路

AI 就绪的安全数据通层（AI-R-SDLayer）的建设，旨在通过构建数据驱动、安全智能、全域协同的新型安全基础设施，突破传统安全体系的局限，实现从“以态势感知为中心”的传统安全模式向“威胁情报驱动”和“数据驱动”的安全体系升级，并推动安全架构从功能组合向数据驱动的根本性转变。面对高级持续性威胁（APT）、0 Day 漏洞利用、供应链攻击等新型威胁，传统的态势感知模式已经难以满足精准检测与快速响应的需求。因此，AI-R-SDLayer 的核心建设思路在于，以高质量的安全数据为核心，通过统一治理、智能分析和全域共享，构建精准、实时、高效的安全能力体系，使安全决策能够依托数据智能优化，实现从被动监测向主动预测和实时联动演进。

在这一框架下，数据成为安全运营的第一生产力。过去，安全体系往往围绕功能组件进行建设，SIEM、XDR、UEBA、流量检测等各类安全产品各自独立运行，数据割裂、协同不足，导致安全运营难以形成统一视角。AI-R-SDLayer 通过构建统一的安全数据底座，打破各类安全数据的壁垒，将日志、流量、资产、漏洞、用户行为等多源异构数据进行标准化整合，并通过主动元数据治理确保数据质量、时效性和一致性，打破安全数据孤岛，构建跨平台、跨业务、跨安全场景的数据联通机制，使安全分析能够基于全域数据进行智能化、精准化的判断。

相较于传统安全体系的功能割裂问题，AI-R-SDLayer 通过数据驱动的安全架构，让各类安全产品不再依赖各自独立的数据存储和计算资源，而是基于同一数据底座进行动态调用和分析。这一变革，使得安全运营能够突破数据孤岛的限制，在同一平台上进行统一的安全数据治理、分析和共享，使安全运营的精准性、效率和智能化程度大幅提升。同时，依托数据编织与联邦查询技术，平台能够在跨区域、跨业务、跨平台的安全环境下，实现分布式威胁情报的智能联动，使安全团队能够基于全域视角精准判断威胁的本质、扩散路径与潜在影响。

在智能化安全体系建设中，私域知识库的构建成为关键支撑。面对复杂多变的攻击形态，企业需要沉淀自身的安全经验，使安全情报不仅来自外部情报源，还能结合企业自身的安全事件、策略调整和历史威胁数据，形成更精准的威胁认知。AI-R-SDLayer 通过安全知识图谱，将威胁情报、攻击链条、资产变更、行为模式等数据进行深度建模，使安全团队能够基于全局知识进行智能决策。这一机制不仅提升了攻击溯源和风险评估能力，也为 AI 安全模型的训练提供了更贴合实际业务场景的高质量数据，使安全分析更加精准、高效。

在智能化与大模型结合方面，AI-R-SDLayer 以大数据计算+AI 分析能力，支撑上层安全应用的数据处理需求。平台不仅提供基础的数据存储与计算能力，还支持多模数据分析，结合 AI 进行安全异常检测、数据关联分析、知识提取等智能化任务。借助大模型的语义解析能力，AI-R-SDLayer 进一步提升对复杂安全事件的自动化分析与趋势预测能力，使安全团队能够在数据驱动的基础上形成更智能、更精准的安全决策。

从架构设计角度来看，AI-R-SDLayer 是一个全域联动、智能驱动的安全数据基础设施。它不仅服务于单一安全产品，而是作为底层支撑平台，赋能 SIEM、XDR、SOC、UEBA、流量检测、威胁情报分析等各类安全工具，使其不再依赖独立的功能逻辑，而是

基于统一的数据基础进行协同计算和智能分析。这种架构设计，使安全能力不再受限于单一产品的视角，而是能够形成跨平台、跨业务、跨场景的综合安全分析能力，使安全运营更加敏捷、高效、精准。

AI-R-SDLayer 的建设，不仅是对传统安全架构的升级，更是安全运营范式的深刻变革。以数据驱动为核心，AI-R-SDLayer 让安全体系从割裂走向协同，从静态走向智能，从孤立走向开放，最终构建一个能够自学习、自适应、自优化的智能安全生态。未来，随着 AI-R-SDLayer 的不断演进，它将成为安全运营的核心支撑，推动企业安全能力迈向更高层次，为数字经济时代的安全挑战提供强有力的技术保障。

4 技术架构与关键技术

4.1 技术架构设计

AI 就绪的安全数据通层通过 PaaS 层、DaaS 层和智能监控运维三个核心功能模块，实现多云环境下的数据管理、治理、开发和运维，满足企业在数据整合、安全分析和智能化运营中的多样化需求。

4.2 关键技术

高性能可编排的智能多源异构数据数据捕获与富化引擎：具备强大的数据采集能力，能够智能连接多种数据源，通过可视化界面实现高效任务编排，支持离线和实时同步，可

对数据进行灵活转换、清洗与聚合，其分布式架构确保了高性能与可扩展性，单机性能卓越，有力推动企业数据采集流程的自动化、高效化与精准化。

元数据驱动的数据治理与全生命周期管理：以元数据为驱动核心，全方位覆盖数据全生命周期，从创建、存储到使用和销毁，进行统一管理与精细治理，构建数据标准体系，保障数据质量，优化数据存储，确保合规使用，实现数据资产价值最大化，为企业提供坚实的数据治理基础与决策支持。

云地一体与多云适配的分布式动态计算与资源调度技术：以智能感知与自动调整能力脱颖而出，并非简单的资源堆砌，而是深入理解业务需求和运行环境的复杂多变性。在云环境中，无论是公有云、私有云还是混合云架构，都能精准感知资源负载、数据流量和任务优先级的动态变化。通过持续监测和分析，它能够自动优化集群配置，动态分配计算、存储和网络资源，实现资源的弹性伸缩。不仅如此，它还具备独特的组件自适应编排功能，根据不同的应用场景和业务需求，自动组合和调整分布式组件的协作方式，确保系统在各种复杂情况下都能保持高效稳定运行，为企业提供高度灵活、智能且可靠的分布式管理解决方案，有效提升企业数字化业务的敏捷性和竞争力。

可定制可组装式面向业务的数据元件生产：深度挖掘并解析各类数据源，匠心打造可复用、可移植且类似容器化的数据元件。这些元件仿若智能积木，工厂配备的多功能工具集，支持用户以高度自定义的方式进行元件的创建、精细加工与全面管理，轻松构建个性化数据集市或数据集。用户可按需灵活编排组合，高效搭建贴合业务需求的专属数据应用场景，极大增强数据开发自主性，显著提升应用灵活性与响应速度，为企业在数字化转型之路上提供强劲助力，使其能精准把握市场变化脉搏，快速适应并引领业务发展新趋势。

异构多数据源融合查询与一站式高性能智能分析引擎：作为企业数据查询的统一门户，向上提供了标准化、简洁化的查询接口，有效屏蔽了底层数据源的复杂性和异构性。

无论是关系型数据库、非关系型数据库还是其他数据存储形式，用户只需通过统一的查询语言和操作方式，即可便捷地获取所需数据。它整合了分布式查询引擎，能够自动优化查询路径，智能分配计算资源，实现对大规模数据的高效检索和精准分析，极大提升了数据查询的效率和准确性，为企业决策提供及时、可靠的数据支持。

高性能分布式向量数据库：AI-R-SDLayer 通过分布式向量数据库构建高效、安全的数据通层，赋能安全运营的实时检索、异常行为分析与智能威胁识别能力。其核心能力包括多源异构安全数据的向量化建模，支持日志、流量、攻击情报、用户行为等数据的高维特征匹配与相似性搜索，突破传统结构化存储的局限，实现精准的威胁检测与态势感知。结合联邦学习与隐私计算，AI-R-SDLayer 在保障数据安全的同时，实现跨平台安全情报协同，支持大规模分布式计算，动态优化检测策略，提升安全运营的响应速度与防御能力，构建智能化、自适应的安全数据基础设施。

智能化私域知识管理与高效向量检索引擎：盘古智链知识库管理是一套基于 DeepSeek 等前沿大模型技术构建的分布式私域知识库管理系统。它借助强大的自适应集群管理能力，能够便捷地接入分布式向量数据库，实现海量知识向量数据的高效存储与快速检索。 通过智能知识库管理功能，在知识录入时，DeepSeek 自动识别数据类型和关键信息，结合盘古元数据管理平台的标准规范添加精准元数据标签；实时监测数据源变化进行知识更新；依据多维度数据自动筛选清理陈旧知识。智能体商城基于 DeepSeek 能力开发，提供涵盖多业务场景的智能体应用，支持企业按需选择、定制和灵活组合。模型实例管理对 DeepSeek 和分布式向量数据库的实例进行实时监控、调度、扩展收缩以及故障检测恢复。智能体工作流通过可视化界面编排智能体，实现大模型与知识库的高效协同，且支持动态调整，为企业提供精准的知识支撑。用户使用自然语言就能快速获取知

识，而智能更新机制会依据业务变化和用户反馈，实时优化知识图谱与向量数据，保障知识的时效性和准确性，助力企业通过知识驱动实现创新发展。

存算分离的多级实时协同全域数据联邦治理与计算分析技术：向下具备强大的数据整合与连接能力，通过先进的虚拟化技术，能够实时、动态地接入和整合分布在不同地理位置、不同系统中的各类数据源。构建了统一的数据视图，允许在不进行数据物理迁移的情况下，跨系统、跨平台地执行复杂查询和联合计算，实现多源数据的关联分析和协同处理。同时，其高效的数据转换和适配机制确保了数据的一致性和兼容性，充分挖掘数据的潜在价值，打破数据孤岛，有力推动企业数据的共享与协作，加速数字化创新进程。

5 中国移动及启明星辰的实践案例与技术积累

5.1 典型案例

AI 就绪的安全数据通层在安全技术和数据治理领域持续深耕，为多项核心业务系统提供了大数据能力支撑。本节将通过一体化云原生安全平台、安全能力平台、威胁感知体系和运营商行业安全数据中心这些典型案例，深入展示 AI 就绪的安全数据通层在助力企业应对复杂安全场景、优化资源配置和推动智能化发展中的关键作用，进一步彰显了其在构建企业级大数据能力底座中的战略意义与技术潜力。

5.1.1 AI-R-SDLayer DaaS 服务助力一体化云原生安全平台建设

一体化云原生安全平台作为技术原生、安全内生的核心安全基础设施，其建设过程中面临高效数据治理、跨资源池协同、安全内生能力、安全数据智能化等多方面挑战。AI-R-SDLayer DaaS 服务以分布式安全湖仓与数据联邦为核心能力，提供稳定、智能的数据支撑与技术保障，助力平台实现高效、安全的数据管理体系。

在架构设计上，AI-R-SDLayer DaaS 服务 通过 分布式安全湖仓 体系，实现了从边缘节点 到 中心节点 的全域数据治理和智能分析。边缘节点部署 轻量级数据采集与处理能力，支持动态策略调整，提升资源池的协同管理能力，确保数据采集与处理的灵活性与高效性。枢纽节点 作为数据处理的核心，整合分散的运维任务，降低系统管理复杂度，提高资源调度效率。中心节点 负责集中数据存储与分析，提供稳定的业务连续性支持，并增强跨资源池的灾备能力，提升系统的可靠性与扩展性。

数据联邦能力贯穿边缘、枢纽与中心，构建高效的数据调度与协同分析机制。在边缘节点完成数据预处理、去噪分析的基础上，中心节点通过智能调度策略，实现全域数据的高效整合与智能分析。这一数据联邦架构突破了传统数据孤岛的限制，有效提升了跨资源池的数据流通效率，使得资源协同管理更加智能化、敏捷化。

依托 AI-R-SDLayer DaaS 服务，一体化云原生安全平台不仅提升了资源池的高效管理能力和智能化数据处理能力，还优化了资产管理体系，为长期稳定运营奠定了坚实的技术基础。这一成功案例充分展示了 AI-R-SDLayer 在大规模安全技术平台建设中的战略价值与技术应用潜力，进一步推动了安全数据治理向智能化、标准化、自动化方向迈进。

5.1.2 AI-R-SDLayer DaaS 服务赋能安全能力平台构建智能化安全运营体系

AI-R-SDLayer DaaS 服务通过提供高质量的数据支撑和创新的技术能力，赋能安全能力平台的建设，打造了集数据、模型、能力于一体的智能化安全运营体系。通过元数据驱动的整合能力和云原生的架构支持，安全能力平台实现了安全大数据的高效治理与价值转化，推动了公司在安全领域的技术创新与业务领先。

AI-R-SDLayer 以元数据驱动的一体化整合为核心，实现了安全能力平台安全数据能力、安全大模型能力和安全原子能力的有机融合，有效解决了多源数据语义不一致的问题。通过对技术元数据、业务元数据和管理元数据的统一治理，平台确保了数据的一致性与高质量管理，为安全能力平台的各项安全功能提供了可靠的数据支持。这种数据治理能力不仅提升了安全能力平台的协同分析效率，也为安全能力的深入应用奠定了基础。

AI-R-SDLayer 在数据要素流通方面发挥了关键作用，为安全能力平台构建了高效的数据共享和价值转化机制。平台支持数据在安全运营体系中的高效流转和融合，推动中台

能力向“高价值”方向转化，为安全运营业务的持续创新提供动力。特别是在云原生安全业务需求的支持下，平台通过弹性伸缩与高可用架构，为安全能力平台实现智能化、一体化的能力提升提供了坚实保障。

高质量的数据支撑使得安全能力平台在安全大模型的训练与优化中具备了强大的优势。平台通过完善的数据积累和处理能力，提升了安全模型在威胁情报分析和异常检测等关键领域的精准性与泛化能力。依托这一能力，安全能力平台在安全运营中实现了更高效、更智能的威胁应对与策略优化。

AI-R-SDLayer 的盘古智链知识库为安全能力平台提供了丰富的安全知识支撑，通过智能体商城中的各类智能体应用，如告警研判智能体、情报融合智能体等，助力安全能力平台更高效地进行威胁情报分析和异常检测。智能体工作流实现了大模型与知识库的协同，优化了安全分析流程，提升了安全运营体系的智能化水平。

通过 AI-R-SDLayer DaaS 服务的强力赋能，安全能力平台构建了一套高效协同的安全大数据体系，不仅满足了云原生化的安全业务需求，还推动了安全运营的智能化发展。这一案例充分体现了 AI-R-SDLayer 平台在安全技术领域的核心价值与应用潜力。

5.1.3 AI-R-SDLayer 赋能智能威胁情报体系，构建自主进化型防御能力

在大模型技术重构网络安全攻防规则的背景下，构建私域威胁情报中心并打通 AI-R-SDLayer 成为新型防御体系的关键。传统威胁情报体系面临滞后性和泛化性问题，难以应对 AI 驱动的深度伪造和高级威胁等复杂攻击。而通过人工智能技术，结合大模型的多模态

推理能力，整合内部终端日志、业务流量等动态数据，实现 AI-R-SDLayer 与威胁情报通层的高度协同，从而提供即时、精准的威胁响应，增强企业的防御能力。

1、人工智能技术驱动安全数据与威胁情报动态协同

AI-R-SDLayer 提供数据传输与存储能力，威胁情报通层负责情报的收集、生产、处理、分析、应用和反馈，确保信息从原始数据到情报的有效输出，实时感知全网安全态势并提供精准响应。人工智能技术的引入促进了 AI-R-SDLayer 与威胁情报通层的紧密协同，通过深度学习动态数据和历史行为模式，提升威胁识别与预测能力。实时分析海量数据，迅速捕捉新兴威胁。结合内部设备反馈，快速处理与智能分析数据，动态调整模型，迅速识别新型攻击，提高防御响应速度、精准度，减少人工干预，提升防护效率，形成闭环防护机制。

2、从“无安全数据通层”到“有 AI 就绪的安全数据通层”的转变

传统的企业安全架构中，多源异构数据常常处于分散状态，形成了数据孤岛。信息碎片化使得安全团队难以对威胁进行快速研判，同时也阻碍了大模型对攻击链的全局建模。AI-R-SDLayer 通过统一的数据治理框架，整合不同来源的数据，并通过隐私计算技术保障数据安全，可以实现 PB 级实时数据的高效清洗、关联与上下文增强，为智能威胁情报中心提供持续演进的训练数据。

智能威胁情报中心实现全面的威胁分析和快速响应，通过引入大数据与人工智能技术，赋予威胁情报自动化处理能力。提升威胁情报的准确性与时效性，在威胁发生初期便能预警潜在风险，并自动分析与封堵网络攻击，从而实现更精准、更快速的网络威胁预测与响应。基于 AI-R-SDLayer 和威胁情报通层的双重协同，使得企事业单位能够在复杂多变的安全环境中，实时洞察潜在威胁，提升防御能力。

3、构建以“智能威胁情报中心”驱动的防御体系

构建以“智能威胁情报中心”驱动的防御体系，通过实现基础数据与威胁情报的深度融合，打破信息孤岛，提升情报共享与协同防护能力。人工智能技术的引入，使威胁情报体系具备智能分析与自我演进能力，推动防御体系实现实时响应与全生命周期防护。通过深度整合商业、开源及自产情报，构建高覆盖、高精度的威胁情报知识库，在复杂环境中精准识别和应对威胁。

- 自动化数据处理与清洗：通过自动化的数据清洗与处理，去除噪声信息，提升情报的高精度与高价值。能够快速分析出有价值的威胁数据，减少人工干预，提高数据处理效率，保证情报为决策提供及时且可靠的支持。
- 智能化事件关联与分析：利用行为分析与关联分析，高效识别攻击模式与攻击源。通过分析攻击链条的各个环节，能够精确分析攻击手法，识别潜在威胁，支持安全团队采取针对性防御措施，提升 APT 攻击等复杂攻击的防御能力。
- 自主学习与预测能力：通过对历史攻击数据的深度学习，能够精准预测未来攻击趋势，生成攻击画像，并提供预警。在应对零日漏洞和高级持续性威胁（APT）时，具备更高的预判与防护能力。
- 动态威胁知识图谱：利用多模态分析与深度学习构建动态更新的威胁知识图谱，实时整合各类威胁数据。帮助安全团队全面理解威胁态势，自动调整防护策略，使防护体系始终处于最优状态。
- 自适应与持续优化：通过持续学习与数据反馈，能够自适应并优化防护规则，快速响应动态安全威胁。在任何时刻、任何场景下，能够提供最有效的防护，帮助企事业单位应对复杂和多变的安全挑战。

5.1.4 AI-R-SDLayer 作为大数据能力底座赋能运营商行业安全数据中心

AI-R-SDLayer 作为安全大数据能力底座，为运营商行业安全数据中心（以下简称“安全数据中心”）提供了强有力的技术支撑。通过元数据驱动的数据治理能力，AI-R-SDLayer 帮助安全数据中心实现了对多源异构数据的高效整合和质量提升，构建了统一的安全数据标准和贴源目录体系，彻底解决了安全数据孤岛问题。

在资源调度方面，AI-R-SDLayer 的分布式架构支持安全数据中心动态扩展和高效资源分配，使其能够应对复杂的安全数据场景需求。借助 AI-R-SDLayer 的能力，安全数据中心实现了跨部门、跨系统的数据共享和服务交付，不仅提升了数据流转效率，还为安全业务的智能化分析提供了强大支持。

依托 AI-R-SDLayer，安全数据中心构建了覆盖数据采集、治理、共享的全流程能力，显著增强了安全数据服务的灵活性和响应速度，为公司内部及外部市场提供了高效可靠的一站式安全数据解决方案。

5.2 技术积累奠定 AI 就绪的安全数据通层建设基础

AI 就绪的安全数据通层的规划根植于多年来在数据采集、大数据基建以及数据共享与流通领域的技术积累。这些关键技术专利的突破，不仅展现了在大数据核心能力上的深厚积淀，更为平台的建设提供了高效、可持续的技术支持。

在数据采集领域，针对多源异构数据和复杂场景的需求，平台实现了卓越的技术积累：《一种实现高灵活性和高性能的 DAG 配置方式的流处理架构》通过 DAG 可视化配置，实现灵活高效的数据流处理，支持离线和实时数据的高性能采集同步，同时具备算子灵活扩展和按需资源分配等优点；《一种复杂日志高性能混合解析方法和系统》通过灵活

配置解析规则，实现对多种格式日志的高效解析，同时利用缓存机制与分段式解析，确保处理性能与扩展能力。《一种关联数据补全引擎设计方法》借助持久化键值存储和低延迟类 SQL 查询技术，提供实时、高性能的关联数据补全能力，为数据采集提供强有力支撑。

在大数据基础设施建设方面，平台通过创新专利推动高效数据存储和处理能力：《一种动态配置 Clickhouse 物化视图的方法》针对动态变化的业务需求，提供灵活的物化视图动态管理 SDK，实现高效的 OLAP 分析支撑，满足实时性与性能需求。《一种基于 ClickHouse 的分布式部署高性能读写分离方法》优化 ClickHouse 分布式集群的写入和查询能力，实现海量数据的高并发、高速处理，并显著提升扩展性和稳定性。

在数据共享与流通方面，平台针对数据安全和敏感信息保护领域提出创新解决方案：《基于部分鲁棒的对偶概念分解脱敏算法》通过对复杂数据的敏感类型分析与精准脱敏，为数据共享过程中的安全性提供多层次保护，支持数据高效流通与利用。

这些技术积累为 AI 就绪的安全数据通层的规划与建设提供了核心支撑，使平台能够从根本上解决数据孤岛、高效协同与智能化分析等行业痛点，加速大数据技术与实际场景的深度融合。

通过以上技术积累，平台在数据采集、存储与共享等环节实现了全链条的创新与优化。采集模块提供灵活的跨源数据接入与解析能力，基建模块保障了高性能数据存储与处理，流通模块则在数据共享的安全性与敏感信息保护上实现突破。这些技术在提升数据处理能力的同时，也为企业在数据价值挖掘和智能化业务拓展方面提供了坚实支撑，全面赋能 AI 就绪的安全数据通层的建设与发展。

6 大模型时代企业管理者的十大倡议

在大模型时代，数据已成为企业最重要的战略资产，安全与智能化运营的融合成为企业竞争力的关键。随着大模型技术的广泛应用，数据基础设施的建设不仅要支持高效的数据处理、分析和治理，还需具备 AI 赋能能力，以提升业务智能化水平。AI 就绪的安全数据通层（AI-R-SDLayer） 作为企业大数据治理、安全分析、AI 就绪数据管理的核心基础设施，为企业提供数据整合、智能分析和实时联动能力，助力安全体系向数据驱动、智能协同演进。面对企业数字化转型的挑战，管理者需要从安全、数据、业务、技术、运营、财务等多个角度进行布局，确保数据资产能够在高效管理、安全防护、智能分析、提质增效之间取得平衡。

面对大数据与 AI 深度融合的趋势，我们向企业管理者提出以下十大倡议，助力企业提升数据资产的价值，构建数据驱动的安全运营体系、优化 AI 就绪数据管理、提升业务安全智能化水平，为企业在大模型时代的持续增长提供战略方向。

一、以数据驱动安全战略，加速企业智能化与安全能力融合

面对日益复杂的安全威胁，企业管理者应推动从被动防御向数据驱动、智能安全、自动化运营发展。CEO 需要将 AI 安全数据治理作为企业战略核心，将安全能力与业务增长深度结合，确保企业的数据资产在安全可控的同时，实现最大化的商业价值。AI-R-SDLayer 提供的数据治理与智能分析能力，能够提升企业安全运营的主动性和自动化水平，推动企业实现数据赋能安全、智能驱动决策 的全新发展模式。

二、构建高弹性智能安全数据架构，优化 AI 与大数据融合能力

在大模型时代，企业 CTO 需推动 AI 就绪的安全数据通层（AI-R-SDLayer）作为企业大数据与安全计算的底座，优化数据架构，使其能够灵活适应 AI、自动化安全运营、智

能分析等前沿技术需求。AI-R-SDLayer 通过分布式计算、数据编织、存算分离、多云资源调度，提升数据存储与计算的扩展性，让 AI 模型能高效利用高质量数据进行推理与分析。同时，CTO 需推动数据安全与业务系统深度融合，确保 AI 能够在数据合规的基础上释放更大的安全价值。

三、以数据治理为核心，提升数据流通与共享能力

CIO/CDO 需要推动企业建立统一的数据治理体系，确保数据质量、数据安全、数据合规，为 AI 训练、安全分析、业务运营提供可信的数据支撑。AI-R-SDLayer 通过智能数据治理、数据质量管控、跨平台数据共享，帮助企业解决数据孤岛问题，提升数据可用性，并确保数据在多场景下的高效复用。企业的数据治理不仅是安全合规的需求，更是 AI 训练、智能分析、精准决策的核心驱动力，CIO/CDO 需推动数据治理向智能化、自动化、可视化方向发展，以增强企业在 AI 时代的数据竞争力。

四、推动安全数据通层建设，实现全集团安全数据资源整合，夯实数据+AI 驱动的安全能力体系

CDO 需推动企业安全数据资源的统一管理与标准化治理，确保数据资产在 AI 时代发挥最大价值。当前公司不同部门积累了大量有价值的安全数据资源，但数据孤岛现象制约了安全能力的整体提升。这些数据资源既有标注的样本数据，也有未标注的安全语料数据，对于人工智能模型的训练优化具有重要价值。通过建立统一的安全数据通层，可实现三大核心价值：一是构建覆盖全场景的安全数据湖，为 AI 模型训练提供高质量数据燃料；二是建立跨部门协同机制，通过多维数据关联分析提升威胁检测准确率；三是形成标准化数据服务能力，支撑自动化安全运营体系建设。安全数据通层将严格执行数据安全管控措施：实施数据分级分类管理，建立细粒度访问权限矩阵；对跨部门数据调阅实行"申请-审

批-授权-审计"全流程管控；采用加密传输、脱敏处理等技术保障数据流转安全；定期开展数据安全风险评估与合规审计。

五、构建智能化安全运营体系，提升威胁检测与自动化防御能力

CISO 需要推动企业安全运营从传统的日志分析与规则检测向 AI 智能检测、数据驱动防御、自动化响应发展，借助 AI-R-SDLayer 的数据治理、威胁情报共享、安全知识图谱，构建实时监测、威胁预测、自动响应的智能安全运营体系。面对 APT、0Day 攻击、供应链攻击等高级威胁，CISO 需利用 AI 大模型与 AI-R-SDLayer 的联邦查询能力，构建全局化的安全态势感知能力，实现基于数据智能的实时防御，提升企业安全运营体系的协同效能。

六、推动数据安全合规与隐私保护，提升数据要素市场化能力

在数据安全与合规管理方面，CSO 需确保企业数据安全管理符合全球及国内的数据安全、隐私保护标准，在安全合规与数据流通之间取得平衡。AI-R-SDLayer 通过数据加密、权限隔离、隐私计算、数据水印等技术，确保数据在存储、处理、分析、共享等环节的全生命周期安全可控。CSO 需推动企业从单一安全防护向数据要素化、安全合规智能化发展，使数据能够在保护隐私的前提下，实现安全共享和价值变现，为企业构建可信的数据资产管理体系。

七、释放数据资产价值，优化 AI 训练与数据智能决策能力

CDO 需要推动数据资产化、数据智能化、数据驱动决策，确保 AI 模型能基于高质量、安全合规的数据进行训练，提高数据的复用性与分析价值。AI-R-SDLayer 提供数据标准化管理、智能数据编排、AI 就绪数据治理，助力企业构建 AI 训练数据湖、企业级安全知识库、实时数据流通体系，提升 AI 在智能风控、精准营销、智能安全运营等领域的应用效果，推动企业数据价值最大化。

八、优化大数据基础设施成本，提升数据资产 ROI

CFO 需要推动企业在数据管理与 AI 计算资源配置上实现降本增效，确保数据基础设施具备高效存储、智能计算、弹性扩展能力。AI-R-SDLayer 通过数据湖仓一体化、存算分离、资源池化调度，帮助企业降低数据存储与计算成本，提升数据资产 ROI。同时，CFO 需推动企业基于数据价值评估模型，优化 AI 训练与安全分析的预算投入，确保 AI 计算资源的合理配置，使数据安全、数据分析、数据存储的投入产出比最大化。

九、推动企业 AI+安全融合，提升自动化安全运营能力

企业管理者需要推动安全运营从人工监测、事件响应向 AI 智能决策、自动化防御、实时响应转型，利用 AI-R-SDLayer 提供的高质量数据进行自动化威胁检测、智能关联分析、实时安全响应，确保企业在面对新型安全威胁时，能够基于 AI 智能决策快速采取行动，降低运营成本，提高安全运营效率。

十、构建智能化安全运维体系，提升 AI 在安全管理中的应用

企业的 IT 运维、安全管理、风险控制等工作，需要更强的自动化与智能化能力，AI-R-SDLayer 可通过 AI 大模型、数据治理、自动化运维，帮助企业构建智能化的安全管理体系。企业应推动 AI 在安全运维、风险预警、合规管理等场景中的应用，借助智能分析与自动化运营能力，提升企业整体的安全管理水平，使企业能够在最少的安全运营成本下，实现最优的数据安全保护效果。