擎创科技

擎创夏洛克® AIOps
一体化数智运维管理白皮书

以客户成功为本

上海擎创信息技术有限公司
www.eoitek.com

info@eoitek.com
4008-215-724
上海浦东新区祖冲之路2290号展想广场1802室
北京市海淀区苏州街16号神州数码大厦10层1002
深圳 · 广州 · 成都 · 南京 · 郑州 · 长沙 · 乌鲁木齐 · 宁夏

擎创科技

ABOUT US 关于擎创

擎创科技，作为国内首批智能运维AIOps解决方案提供商，致力于通过提升企业客户对运维数据的洞见能力，为运维降本增效，充分体现科技运维对业务运营的影响力。

公司自主研发的产品 — 擎创一体化数智运维管理平台，为企业IT运维提供一体化的运维管理及智能可观测能力。在运维数据中台和AI算法服务的支撑下，整合告警、监控指标、日志等多维数据，实现业务全链路观测、综合排障分析、告警全周期管理、应用风险预警、数智化运维管理以及擎智运维大模型应用等场景，助力企业数字化转型。

使命
助力企业提升运维数据洞见力，优化运维效率，提升对业务运营影响力

愿景
成为运维管理软件行业的领跑者

价值观
以客户成功为本

智能运维AIOps领域的领跑者

9 年 2016年 成立于上海	5 亿+ C轮，累计 融资超过5亿	100 + 超过100家 行业龙头客户	8 次 Gartner AIOps领域 标杆服务商	40 + 智能运维领域发明 专利和知识产权
100 + 全面信创适配 支持主流产品	2 个 复旦大学共建 智能运维实验室 金融运维实验室	2 个 信通院AIOps 成熟度认证	3 个 智能运维 运维数据治理 团体标准	20 + 入选各类行业 权威案例库

金融大数据 智能运维实验室（北京）

复旦大学 产学研共建

大数据智能分析 开放实验室（上海）

双态运维联盟 Bimodal Operation Alliance

上海大数据联盟

NIISA

SIG

CONTENTS 目录

数字化时代运维的挑战和发展趋势

传统运维的痛点

智能运维建设中的挑战

发展趋势：一体化数智运维体系

业务感知笼统

- 监控工具众多，竖井数据孤立
- 缺少关键系统的重点画像
- 交易变化感知不直观、交易链路跟踪难
- 缺乏从交易、应用系统到基础资源的全面感知

事前预测困难

- 仅依靠单指标预测，手段单一
- 缺乏关键风险指标的定义
- 运维数据达不到时效性要求

事后分析不全

- 数据品类不齐全，难以全面回溯
- 关键的分析数据未作持久化和版本管理
- 故障分析经验难以被挖掘和沉淀

事中定位低效

- 缺乏各应用系统的架构和业务链路视角
- 缺乏对多系统故障的业务影响评估手段
- 缺乏对故障的综合分析及定位手段

数据治理不体系

- 运维数据量大、类别多且非常分散
- 数据清洗、标签、格式化处理工作量大
- 缺乏数据质量、数据生命周期管理的总体数据治理规范

按专业分工
局部建设点状工具和场景

建设中遇到的挑战

·工具很多，但难以融合形成联动能力
·运维数据的质量难以支撑复杂场景
·运维数据的管理配套措施跟不上场景需求
·建设投入不够有针对性，未能达到业务连续性要求

权威咨询机构AIOps观点和报告

Gartner《2024年中国基础设施成熟度曲线》报告摘选

中国的智能运维

企业投入的主要推动因素

· 业务视角的“可观测性”：企业对此期望越来越高。运维人员能够通过这些技术详细了解其业务应用和最终用户体验。

企业投入的主要阻碍因素

·数据质量较低：智能运维项目需要质量较高的数据。分散的系统和未经治理的数据将对分析结果产生负面影响，降低用户满意度。
·定制需求过多：中国企业经常需要通过定制化和集成项目进行规模化、端到端的本地部署。对于供应商和客户来说，成本可能过高。

使用建议

·智能运维是以提升业务价值为目标，而不仅仅是一项有吸引力的新技术。
·如果有可能，先试点带有AI功能的监控工具，再实施智能运维平台项目。
·避免对智能运维平台产生立即实现无人值守运维的期待，但可利用此类平台有效加速和增强现有运维团队工作能力和交付。

中国的应用性能监控与可观测性

随着持续的数字化转型，企业应用架构从单体应用向云原生应用过渡，导致原本的APM解决方案出现不足。甲方客户要求APM供应商为其产品添加可观测性功能。此外企业机构也在将APM推向服务器端以外的领域，以期优化业务成果、增强用户体验、提高应用性能。APM和可观测性解决方案支持企业考察现代应用的端到端性能，并对其进行详细检查，以快速确定影响服务的中断和其他系统运行状况问题。

企业投入的主要推动因素

·统一监控：新型APM和可观测性工具更加统一。共享通用数据模型的平台必须执行相关性分析以及应用性能监控的其他关键功能。
·智能监控：使用日志、跟踪、指标和多种其他类型的遥测，为运营和监控团队使用智能运维（AIOps）技术赋能，在大容量、多维的数据集中发现更多模式。

企业投入的主要阻碍因素

·业务情境：中国可观测性的应用已经从技术情境（从技术角度查看一个系统的运行情况）发展到业务情境（数字业务的透明度情况）。IT领导人面临做出这一转变的挑战。
·关注点差异：基础设施和运营监控的内容与业务部门关心的内容之间往往存在重大脱节（例如双方所关注的指标不同），可能会对企业产生显著的负面影响。
·架构更新：容器、微服务和云原生等现代架构在中国IT运营环境的采用速度快于监控策略的发展速度。这导致了可见性的技术和平台差距、团队考核绩效挑战，以及技能/流程缺口。

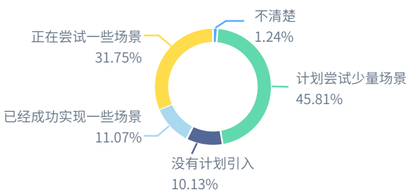
使用建议

·选择能够帮助将应用性能与业务目标关联起来的供应商。选择能够提供可执行的解决方案（而不仅仅是无休止地深入挖掘更多数据）的供应商。

云计算开源产业联盟 CAICT 中国信通院《中国AIOps现状调查报告（2024）》摘选

当前企业运维现状

·故障恢复时间长：现阶段五成企业故障恢复时长一般为1小时至4小时内（51.05%），仅少数企业可做到10分钟内快速恢复（8.09%）
·逐渐体系化：智能运维正从单一场景向体系化发展，产品趋向于构建统一平台
·开展数据治理：企业已逐渐意识到数据质量对于智能运维效果的重要性，超八成企业已开展了运维数据治理活动
·实现可观测难：挑战与困难主要集中在数据来源多、标准难以统一、整合困难方面(62.12%)。企业需要进一步提升底层数据的融合关联能力，才可取得更好的可观测建设果成效。
此外，主动观测能力不足、无法及时发现和预测潜在的问题，占比56%。
·运维大模型应用：越来越多的企业已将运维大模型相关场景能力的建设列入未来计划，近五成的企业表示今年将计划建设少量大模型场景能力，三成企业正在建设相关场景能力，已有少量企业表示已成功实现一些场景。



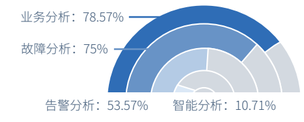
AIOps发展趋势和挑战

·数据质量：企业AIOps的应用效能在很大程度上受限于其所依赖的数据质量。尽管AIOps在自动化故障检测、预测性维护和优化决策方面展现出巨大潜力，但数据的完整性、准确性、时效性、多样性、标准化、安全性和标注质量等方面仍面临挑战。数据的不完整可能导致分析结果的偏差，而错误或滞后的信息可能延误故障响应。多样化数据源的整合困难和缺乏标准化也限制了AIOps的自动化和规模化应用。
·多样化应用场景和数据治理：未来，企业将专注于在多样化的应用场景中建设智能运维能力，并致力于通过强化数据治理来提升数据的准确性和完整性。

智能运维国标工作组《中国智能运维实践年度报告(2022-2023)》摘选

企业客户最关心的智能运维场景

选择最多的是业务分析方面，占比78.57%;其次是故障分析方面，占比75%;
占比第三是告警分析，占比 53.57%，专门反馈智能分析的比例只占10.71%。
业务场景是客户使用数据和产生数据的一个必要环节，也是智能运维的一个核心对象



企业客户对智能运维未来2-3年的期待

·数据治理：客户关注数据质量的提升和数据全生命周期管理,关注监控告警数据和配置数据。正是由于监控告警数据和配置数据严重制约了智能运维场景建设，才有了如此迫切的需求。在运维数据治理的实践中，数据治理和数据消费场景紧密结合，并行建设、边用边治理，脱离消费谈治理、脱离治理谈消费都会得不偿失。
·故障应急：关注根因定位最多，其次是故障自愈和故障预测。说明故障根因定位是故障应急场景的痛点，通过智能化手段赋能故障定位、提高效率是亟待解决的问题。

擎创一体化数智运维解决方案

展现层

智能交互式运维：基于大模型的智能交互式运维将ChatOps理念与AI能力相结合，通过自然语言交互界面实现运维任务的智能化处理和自动化执行

消费场景层

场景应用

业务全链路观测	通过综合利用调用链、日志、指标、配置、网络等不同领域的运维数据，构建以业务为观测视角的横向到边，纵向到底的端到端链路，提升了多系统同时告障时的业务影响分析能力以及快速故障定界能力
综合排障分析	旨在快速恢复业务连续性为目的，联动各领域运维数据，集成多种智能化分析能力，并以业务应用视角为驱动，帮助运维人员提高故障定位的效率
告警全周期管理	贯穿从告警产生、流转、分析、处置等环节，可以对运维工具的异常输出进行集成和治理，融合机器学习和专家知识赋能一线运维、并通过集成自动化第一时间恢复业务可用性
应用风险预警	构建业务运行风险体系，提供业务系统健康度的趋势分析和预测能力，及早发现系统隐患
数智化运维管理	通过系统画像、领导视图等运营分析场景，管理者可实时全面了解数据中心运行健康和风险。构建面向运维成本管理的数据、流程的工具集，从财务角度出发，对IT资源投入产出效能进行管控分析，辅助决策
擎智大模型应用	利用自然语言交互简化运维数据查询，智能故障诊断和预案匹配，并提供集中式运维知识管理和咨询

运维服务

运维数据服务	运维数据服务的重要性在于将数据消费过程规范化、配置化和便捷化，有效解决了数据服务最后一公里依赖开发的问题
算法服务	基于机器学习的算法服务，提供异常检测、趋势预测、日志聚类、告警分类、关联分析和根因定位等能力
智能体服务	基于大模型的IT运维综合服务，具备自主感知、智能分析、决策规划和执行能力，能理解复杂运维状态和需求，自主执行多步骤任务，实现运维流程的自动化、智能化和优化

基础能力层

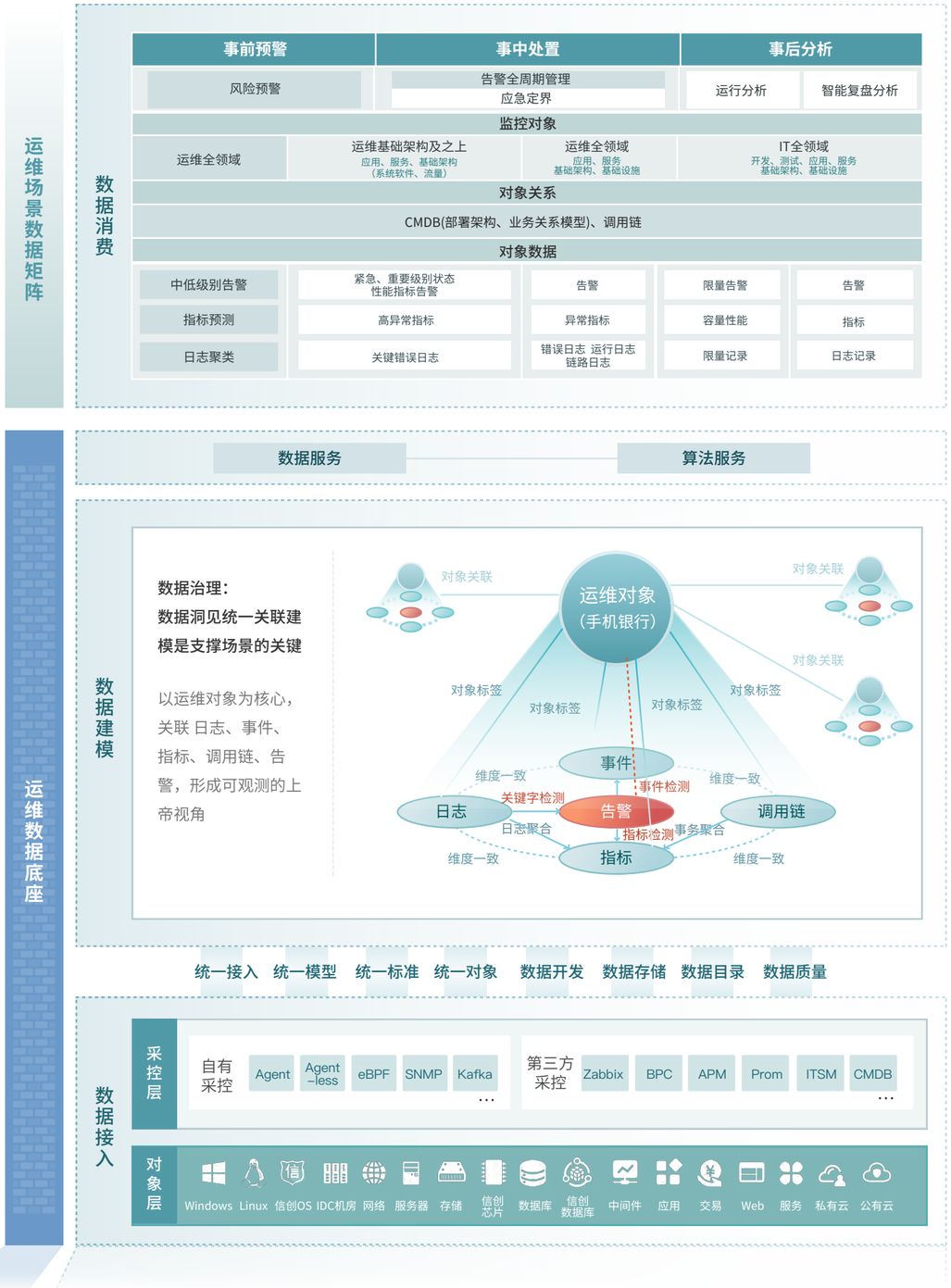
数据能力

数据中台	整合数据治理最佳实践；数据生命周期及数据质量管理；提供数据集市服务接口
对象模型	对接和纳管CMDB模型；基于运维对象为中心建模；内嵌对象模型最佳实践
全景观测	基于eBPF提供云原生监测能力；侵入式/非侵入式的链路追踪能力；异常告警识别及分析诊断能力
知识图谱	告警及运维知识的经验提炼总结；故障处理、应急处置操作推荐；对外部系统的知识服务化提供

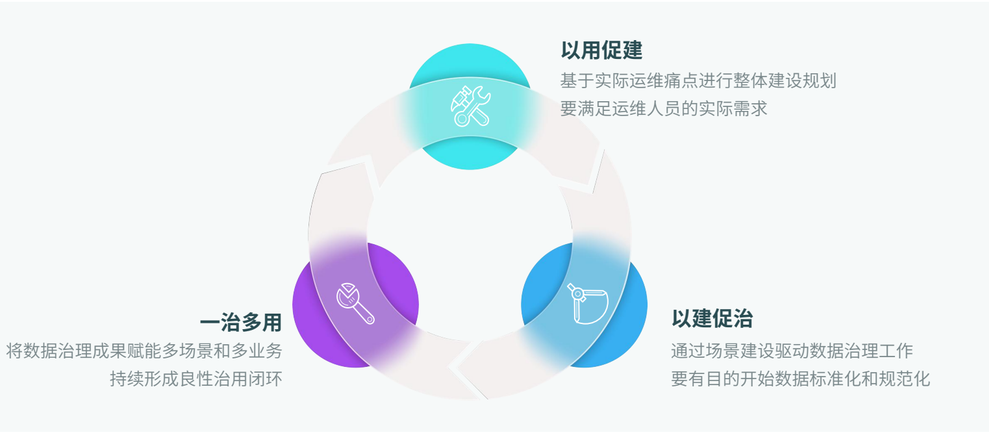
采集管理

兼容自有采控和第三方采控工具；支持Agent和Agentless；整合主流的第三方工具：Zabbix、BPC、APM、Prometheus、日志、告警、ITSM、CMDB

运维数据底座：构建一站式的运维数据专属底座



数据治理：建设思路

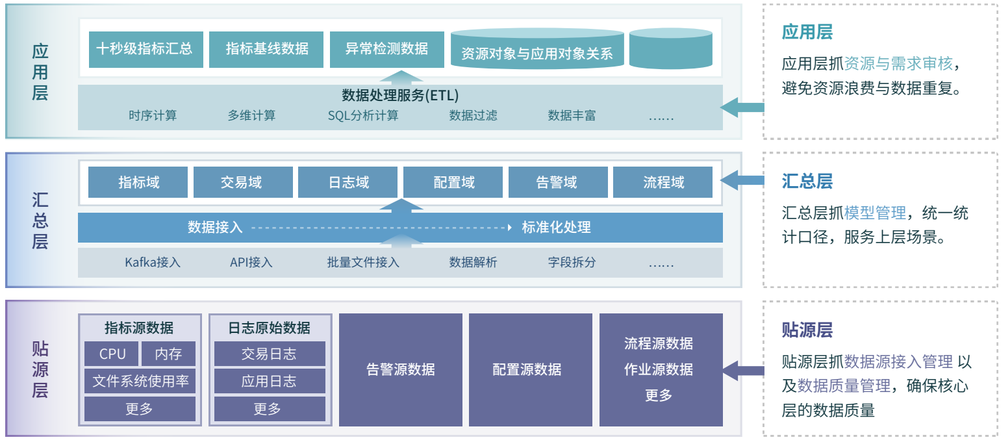


数据治理：建设路径

运维数据治理

2022年，中国计算机用户协会审计分会发布《金融机构信息系统运维数据治理能力成熟度评估规范》的团体标准。该标准确立了金融运维数据治理能力的成熟度模型和框架，规定了运维数据治理能力成熟度评估与持续改进的要求，适用于金融及相关机构信息系统运维数据治理能力的成熟度评估，也适用于信息系统运行过程中设计的非运维数据治理。
通过对自身运维数据治理能力的评估，可明确与成熟度等级评定的差距及改进，为未来的业务连续性管理发展路径提供指导性参考。

分层分域数据治理



应用层
应用层抓资源与需求审核，避免资源浪费与数据重复。

汇总层
汇总层抓模型管理，统一统计口径，服务上层场景。

贴源层
贴源层抓数据源接入管理 以及数据质量管理，确保核心层的数据质量

全面安全和质量保障的数据消费服务

全面安全和质量保障的数据消费
数据服务中心提供数据服务目录和数据对外订阅能力，实现消费方对指定数据的快速订阅和消费。

数据服务目录

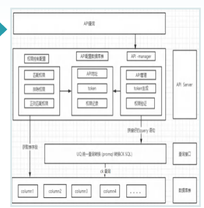
资产目录与数据服务相结合
数据服务目录生命周期管理
数据目录发布管理
数据API发布

数据自助订阅

自助选择服务目录
自助选择数据
数据服务周期管理

数据权限分配

基于数据属性的权限分配
基于数据属性的规则匹配
基于数据数据表的权限分配



数据自由消费

可提供标准的API服务、kafka等对外数据消费接口
可通过基于数据数据消费可通过内置可视化工具直接做数据查询、数据分析

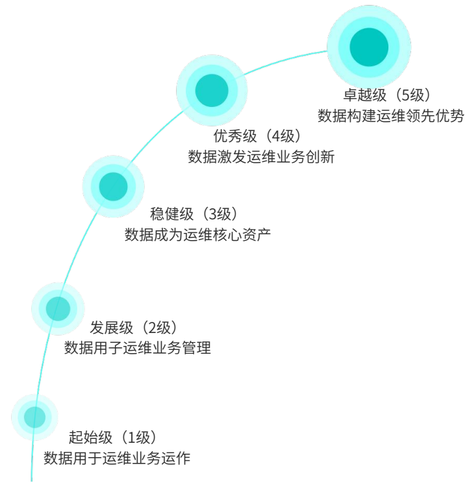
运维数据治理能力成熟度模型

治理能力成熟度等级

整体反映一个组织对运维数据治理过程与效果的能力水平，成熟度等级由低到高划分为起始级（1级）、发展级（2级）、稳健级（3级）、优秀级（4级）、卓越级（5级），其中高成熟度等级包含自身及其之下等级的全部要求。

治理能力成熟度模型

运维数据治理能力模型包含运维数据治理能力框架和运维数据治理能力成熟度等级。运维数据治理能力框架中的能力域、能力项与运维数据治理能力成熟度等级定义映射形成运维数据治理能力成熟度模型。



运维数据治理能力成熟度评估示例

评估方法详见《金融机构信息系统运维数据治理能力成熟度评估规范》

	能力域	能力项	能力项分值	能力域分值	成熟度
运维数据治理能力成熟度——示例	运维数据治理战略	战略规划	2	(2+2)/2=2	发展级
		专项投入	2		
	运维数据治理组织	组织建设	3	(3+2+3)/3=2	稳健级
		制度建设	2		
		流程管理	3		
	运维数据标准规范	数据资产目录	2	(2+3+3+3)/4=3	稳健级
		数据标准	3		
		数据模型	3		
		数据分布	3		
	运维数据质量管理	需求管理	2	(2+2+3+2)/4=2	发展级
		质量检查	2		
		质量分析	3		
		质量提升	2		
	运维数据生命周期	生命周期定义	3	(3+3+2)/3=3	稳健级
		生命周期管理	3		
		生命周期运维	2		
	运维数据安全管理	安全策略	3	(3+2+3+4)/4=3	稳健级
		安全管控	3		
		安全审计	4		
		合规管理	3		
	运维数据应用场景	数据服务	2	(2+2+3+2)/4=2	发展级
		数据审计	2		
		运维服务	3		
		业务运营	2		
	运维数据管理平台	数据集成	2	(2+2+2+2)/4=2	发展级
		数据建模	2		
		数据分析	2		
		数据共享	2		

数据治理成熟度分布图

数据治理持续服务–评估及认证

擎创科技为标委会授权指定评估单位，联系我们评估认证

标准评估内容边界

顶层设计（战略对齐、组织配套、架构承接）
规范指引（运维数据标准规范、数据管理规范、数据应用规范）
运维数据管控框架（统筹规划、构建运行、监控评价、改进优化）

标准评估应用范围

计划在智能运维场景下建立对应运维数据治理体系的组织
评估自身运维数据治理条件和能力的组织
运维数据治理能力需方和供方评价
第三方评价和认定运维数据治理能力

*以上图片仅为示意图

智能运维场景

业务全链路观测

场景简介

业务全链路是通过综合利用调用链、日志、指标、配置、网络等不同领域的运维数据，构建以业务为观测视角的横向到边，纵向到底的端到端链路，提升了多系统同时告障时的业务影响分析能力以及快速故障定界能力。

业务影响分析：以入口系统以及交易码构建业务场景，实现从点状业务系统到链状业务场景的预警以及影响分析能力，协助生产运行团队快速识别受影响的业务范围以及严重程度，为生产召集、应急恢复等操作，提供快速精准的决策依据。

快速故障定界：实时分析支撑业务场景的业务路径以及应用路径，当业务场景出现故障时，精准识别故障路径、推荐异常终点，自动汇总错误以及性能缓慢热点，实现从业务、应用、到基础架构的纵向下钻分析，关联分析链路、指标、日志等相关运维数据，协助二线运维团队快速确定故障边界，提高应急排障效率。

典型用户画像

面向生产运行部

提供面向业务视角的预警以及影响分析能力，协助生产运行团队掌握受影响的业务范围以及严重程度，辅助生产运维决策。

面向应用二线运维

通过对业务以及应用路径的实时分析，基于路径以及多维智能算法，自动识别以及推荐异常终点，实现横纵两向的下钻以及关联分析，协助应用二线运维人员快速识别根因故障边界，提高应急排障效率。

用户痛点和期待

客户痛点

·**业务影响分析难：**在云原生以及微服务架构下，系统的广度与深度不断增加，调用关系日益复杂，生产事件的影响越来越大，业务影响范围以及程度的分析复杂性大大增加。

·**故障定界难：**云化背景下微服务架构日益复杂，存在新老架构相互调用，横向排障困难，故障定位效率低。

客户期待

·**建立端到端分析能力:**通过整合调用链、日志、指标、配置、网络等不同领域的运维数据，实现横纵两向的端到端分析能力，提升多系统同时告障时的应急处置效率。

·**提升业务影响分析能力：**构建面向业务场景的预警以及影响分析能力，协助生产运行团队快速识别业务的影响范围以及严重程度，辅助生产应急决策。

·**提升多系统同时告障时的故障定界能力：**通过对数据进行端到端智能分析，协助二线运维人员快速确定故障根因边界，提升应急排障效率。

场景价值特性

场景价值

业务运行端到端分析：构建了从业务、应用到基础架构等不同层面的横纵两向的端到端分析能力。

提高应急排障以及处置效率：多系统同时告障时，快速判定业务影响范围以及严重程度，精准识别故障交易以及应用路径，自动推荐可疑异常终点，提升运维人员的应急协同排障以及处置效率。

场景特性

聚焦企业应急排障以及处置流程：聚集一线生产运行以及二线应用运维团队在多系统同时告障时的业务影响分析、生产召集、根因系统确定等疑难关节，提供快速、准确的决策处置支持，提高应急处置效率。

数据兼容范围广、适应性强：可综合利用调用链、日志、网络等不同领域数据构建完整业务链路，适应企业转型期的数据不规范、质量不高的特点。

故障定界高效、精准：依托交易以及应用路径自动识别与分析算法，从复杂的蜘蛛网状拓扑中，快速提取链状的故障路径，自动确定路径的异常终点。

场景相关产品

智能观测中心　运维数据中台

案例成果

项目方：某国有大行

用户主要痛点

·**业务影响分析困难：**生产运行部仅知道受影响的系统数量，难以找到重点，只能广播式召集

·**多系统横向排障困难：**二线应用/系统部依赖经验判断上下游影响关系，逐个系统进行排查，基于经验粗估原因，处置方案无把握，中间牵扯大量的一二线之间的重复沟通成本

诊断和建议

·基于调用链数据实时生成的系统调用路径，提供了多系统告警拓扑，自动识别与凸显异常路径，提高生产运行团队的业务影响分析能力以及召集效率

·梳理关键业务场景，确保对应系统的链路数据全覆盖，实现关键业务场景的自动故障根因分析，提高对关键业务的保障质量

·通过数据治理，关联调用链数据、日志数据、指标数据、配置数据、告警数据，辅助运维人员进行横纵两向的下钻关联分析

建设收益

·**提供了统一且完整的业务影响认知:**面向一线生产运行部以及二线运维团队提供了统一且完整的业务影响分析视图，提高了一线生产运行团队的召集效率

·**提升了复杂故障的排查能力：** 综合利用链路、指标、日志、配置等领域的运维数据，实现从业务、应用、到基础架构的纵向下钻分析，关联分析链路、指标、日志等相关运维数据， 协助二线运维团队快速确定故障边界，提高应急排障效率

建设挑战

·**海量运维数据，**例如调用链数据每秒超过400万，对底层大数据的处理效能以及稳定性要求极高

·**数据不一致，**例如调用链中数据(来自软件开发中心) 与 监控系统数据不一致

建设步骤和内容

一期

交易链路的端到端分析，兼容云上与云下，基于调用链数据、日志数据、指标数据实现了交易链路的端到端追踪。协助一线值班团队定位多系统异常根因，提高客诉问题的排查效率，辅助二线运维团队查看故障系统上下游，寻找错误、性能热点，定位故障对象。

二期

梳理了18个关键业务场景，实现关键业务的一键根因诊断；优化业务影响分析旅程与体验，基于系统调用路径，提供系统级别的告警拓扑，聚焦故障路径以及异常终点，增强从业务场景到链路的下钻分析能力。

可观测系统架构

智能运维场景

综合排障分析

场景简介

“垂直专业工具多，关联分析能力弱”是运维组织进行跨领域故障排查时经常存在的问题，夏洛克综合排障中心以快速恢复业务连续性为目的，联动各领域运维数据，集成多种智能化分析能力，并以业务应用视角为驱动，帮助运维人员提高故障定位的效率。

典型用户画像

一线值班人员/事件经理

负责对告警进行操作和处理、了解故障严重性和影响范围、判断是否需要应急协同，在事后需要牵头进行故障复盘

领域专家

对一线人员反应的故障问题进行快速定位，找到可快速恢复业务的处置方式并执行解决

应急指挥

在较为严重或复杂的故障处置过程中，进行应急指挥及调度，分析决策支持

用户痛点和期待

客户痛点

垂直专业工具多，关联分析能力弱，难以快速定位故障原因

没有统一的观测平面，沟通成本大，协作效率低

数据分散，未以业务视角建模，难以支撑复杂场景

客户期待

需要对故障进行快速分析，推荐故障原因和处置建议

期望能从业务应用视角出发自顶向下来排障和指挥

能快速总结影响面，并在事后形成复盘和知识沉淀

场景价值和特性

场景价值

- 提高故障定位效率
- 帮助业务及时止损
- 降低协作成本
- 沉淀排障经验

场景特性

- 快速故障定界：一键推荐可处置的对象
- 解决多种故障场景：集成多种排障能力
- 提升排障体验：统一故障描述和交互方式
- 业务应用视角驱动：全面观测回溯

场景相关产品

综合排障中心　运维数据中台　运营决策中心

综合排障分析中心

告警中心	总览观测视角	应用健康总览 / 应用架构总览 / 业务健康总览
	故障分析工具	业务影响评估 / 告警根因 / 告警时序分析 / 链路诊断 / 业务路径分析 / 交易多维分析
	故障分析助手	一键式分析 / 综合故障报告 / 故障回溯
变更平台	专业领域视角	交易 / 应用服务 / 系统软件 / 网络 / 存储 / 物理机
	运维数据中台	数据集成 | 数据模型 | 数据开发 | 数据服务

案例成果

项目方：某国有大行

用户主要痛点

该国有大行信息化边界遍布全球，期望在3年内完成全面云化转型、一体化运维平台建设，以及运维信创的改造

总行层面：

·运维监控缺乏统一视角，难以全面把控IT系统运行状况。

·存在超过40种不同的运维工具，导致运维环境复杂，工具间协同困难

·面对跨领域故障时，排查和解决时间较长，影响业务连续性。

分行及分支机构层面：

·缺乏统一的运维规划，各地运维标准不一致

·总行难以对分支机构提供有效的运维支持，造成资源浪费和效率低下

诊断和建议

一体化运维项目建设的关键不仅是运维技术的提升，重要的是整个组织对于运维管理方式的转型，这背后必须有破除部门墙和数据井的决心，驱使其愿意举数据中心之力来提升运维数据底座能力，在功能规划中为跨部门协作移除边界，做务实的智能化设计，去解决一线运维的实际问题，同时为日常运维管理职责做出更明确的分工，最终才能达到到AIOps赋能运维事务的目的

建设收益

·**统一监控告警体系：** 云上云下全覆盖，应用、业务、运行、分支机构等运维视角全覆盖，应用监控颗粒度各个交易维度，故障发现时效性达到秒级

·**排障效率大幅提高：** 一体化监控告警平台和智能化运维中心提供了统一观测平面和分析工具，故障平均排查时间减少至原来的1/6

·**运维模式转型：** 工具+流程+数据联合驱动运维生产力

建设挑战

·运维应用场景多，包含统一门户、一体化监控告警、链路分析、智能化分析、运维数据平台等10大模块和数十个应用场景

·数据治理范围广，纳管全行的运维数据，数据总量约4PB，日增超40TB，为了支撑监控、告警、调用链、智能化、报表、日志查询等多种运维场景，需要持续进行数据治理

·运维建设转型快，建立全行级的运维工具专属团队，深入各部门一线统筹规划建设全行运维共性需求

建设步骤和内容

一期

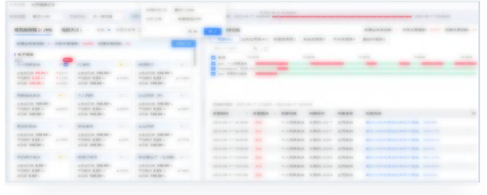
建设运维数据、自动化等基础能力底座、覆盖事中处置的大部分场景，总行应用&分行试点

二期

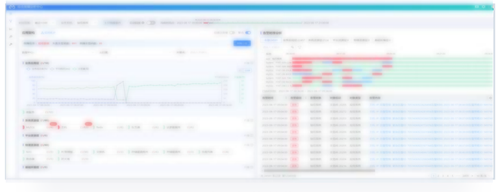
完善数据关联性，构建全景可观测、链路分析、智能化分析及故障自动化处置能力，分行全面推广

三期（建设中）

通过持续性数据治理，结合智能化赋能并联动各运维场景的能力

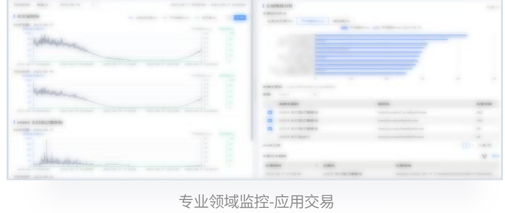


应用健康总览



应用架构总览

告警根因分析



专业领域监控-应用交易

*以上图片仅为示意图

智能运维场景

告警全周期管理

场景简介

随着企业内数字化应用架构变得越来越复杂，运维团队需要处理的告警呈指数级增长，企业期望从告警产生、流转、分析、处置等环节有一套贯穿全生命周期的解决方案，可以对运维工具的异常输出进行集成、对多源告警进行治理、使用机器学习及专家知识分析问题、并提供自动化集成能力第一时间自动恢复业务可用性。

典型用户画像

一线值班人员

7*24H值班、负责对告警进行操作和处理、根据情况发起工单申请、判断是否需要应急

领域专家

对一线进行支持、白名单确认（如过滤规则、维护窗口）策略管理（压缩、处理、知识总结等）

应急指挥

应急场景下进行应急指挥及调度，分析决策支持

告警治理岗

负责对告警数据及监控工具平台的日常运营，进行告警治理及督办

用户痛点和期待

客户痛点

缺乏统一的告警治理、管理体系
告警协同分析和处置能力不足
真正的故障告警被淹没，多监控工具告警数据分散
自主可控，信创替换

客户期待

告警信息丰富，驱动流程化告警管理，充分发挥历史故障、专家经验价值
在大量分散的告警数据中，识别相互影响关系，提升分析排障效率
多维度运维数据联动探查，辅助快速定位故障边界并及时修复

场景价值和特性

场景价值

- 整合来自不同监控系统的告警，实现统一管理与智能化收敛
- 告警联动事件单，构建全生命周期告警流程闭环管理
- 算法自动化告警分层、标签化，辅助快速故障定界分析
- 多维度运维数据协同分析，辅助应急处置，快速恢复业务

场景特性

- 算法加持，自动化收敛压缩、时序标签
- 融合拓扑数据，根因告警评分，自动定界
- 可编排式告警数据治理，快速完成多源数据统一
- 可扩展自定义插件，灵活的业务扩展能力

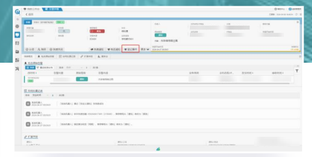
场景相关产品

告警辨析中心　运维数据中台

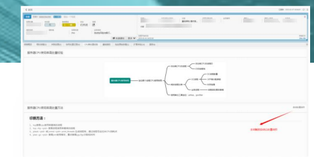
案例成果

项目方：某城商行

指标数据联动



登记事件（开单）



知识库及处置动作

用户主要痛点

·近30套监控工具所产生的告警数据分散割裂
·维护期阶段，无有效手段进行告警屏蔽
·大量噪音告警难以通过监控工具自带的规则配置进行有效抑制

建设收益

·**多源统一纳管：**来自于各一级监控系统功能的告警进行统一汇集、展示、处置
·**降噪聚焦、集中处置：**告警丰富/过滤/压缩/告警通知/告警处置/告警恢复
·**快捷分析：**相似推荐、变更关联、监控指标联动分析
·**智能辅助：**专家场景挖掘，AI智能聚类压缩，智能标签化

诊断和建议

·拉通CMDB数据，对告警进行一致化的数据丰富
·以应用、管理组织维度，对告警进行分类聚类压缩
·联动工单平台，结合内部流程，完成告警的全生命周期跟踪

建设挑战

·CMDB数据准确度欠佳，需要对关键CI属性进行前置梳理
涉及跨部门监控告警信息对接，采用标准化告警字段对齐数据差异
·30+告警来源，告警样例、字段标准化复杂度高

建设步骤和内容

一期

一级监控告警统一化接入与丰富
告警压缩（智能聚类演示，快速标识压缩，专家规则压缩）
变更关联，相似告警关联
告警通知（内部IM、短信）、转派与处置
指标数据联动
告警数据报表分析

二期

更多监控源接入
联动工单平台，完成告警→开单→关单闭环
通知增加，智能外呼，通知数据分析
通知能力联动值班表
告警管理移动端

三期（规划中）

建设配置拓扑关系的告警定界分析
基于告警的核心应用健康分析，影响范围分析
综合排障分析处置

*以上图片仅为示意图

智能运维场景

应用风险预警

场景简介

本场景主要面向业务系统，围绕风险指标、健康度风险模型、风险识别矩阵三块来构建信息科技风险防控管理体系，形成“事前预警、事中监控、事后分析”的自动化监测和健康度可视化能力，为生产事件风险识别、风险防控洞察保驾护航。强化三道防线风险管理联动，建立三道防线“监督、检查、评估、整改”的闭环机制，提升二道防线的生产运营风险管控能力。

风险预警：实现智能风险点探查、指标故障阈值条件设定及指标基线偏离度计算，针对风险点，提前向生产运行部门发出风险预警提示
风险监控：实现在风险事件期间，依托运维大数据及健康度风险模型算法，对风险进行识别和通知，对故障点进行排查和定位，提升事中风险定位的能力
风险复盘：围绕数据分析中心、报表统计中心等功能，实现对生产问题进行复盘和评估，通过历史数据实现模型、参数、规则等进行优化完善，提升风险监测能力

典型用户画像

面向行领导及风险管理部

从全行整体视角，掌握重点系统健康度全貌、重大风险事件及影响面，辅助生产运营决策

技术人员
主要面向金融科技部

通过应用九宫格等页面，围绕技术、业务、服务等指标维度进一步对故障系统定位、风险识别

后台管理人员
主要面向风险管理部内部

在风险事件后可通过平台后台能力，实现问题复盘、模型调参与试算、规则优化和统计分析的能力

用户痛点和期待

客户痛点

·**风险管理要求提升：**监管机构及管理层对信息科技风险管理二道防线要求提升，要求进一步加强风险评估和监测力度，提升信息科技风险管理能力
·**现有机制难以总体把控：**传统信息科技生产运营风险管理场景中，二道防线主要通过手工方式采集运营及运维指标数据，存在数据时效性较差、准确度底，监测范围有限的问题，难以对全行的生产运营风险进行总体把控

客户期待

·**建立常态化风险监测能力：**通过数据聚合、分析、结合AI算法模型，提升自动化监测风险及时预警、通知能力，提升事前风险预警能力
·**提升风险场景化分析能力：**构建场景化分析能力，提升事中、事后场景化风险定位能力；通过智能化数据分析，为故障定位提供宏观的证据链，辅助各平台快速解决问题
·**提升生产运营风险管理能力：**实现生产系统数据的融合贯通，打破各自为政，信息孤岛，促进生产系统数据标准化，提升二道防线的生产运营风险管控能力

场景价值特性

场景价值

- 数据赋能风险，防范于未然
- 事件的吹哨人，生产运营全掌控
- 全维度视图，全面数据透视，风险有踪，数据可循

场景特性

- 风险指标体系成熟健全，快速赋能落地
- 完备的评估模型，精准感知数据背后的隐藏风险
- 开箱即用的数据模型，强大的数据中台快速完成数据加工与消费
- 便捷的沙盒模拟、数据验证，辅助模型精调

场景相关产品

运营决策中心　运维数据中台　智能观测中心　告警辨析中心

案例成果

项目方：某农村商业银行的风险管理部

用户主要痛点

信息科技风险指标和生产事件都是依赖科技部上报风险管理部，无法保证真实性和准确性，缺乏二道防线的自动化监测机制和风险评估分析依据

建设收益

·面向信息科技的风险预警在同行业界没有任何参照建设经验，在业内属于创新
·自系统上线至今，面向业务风险预警年度达50+余次，现风险管理部面向信息科技风险管理的重要手段和业务受灾面评估的重要依据
·实现各运维监控系统的数据融合，有效推动源头数据标准化，提升数据质量
·实现面向重大风险事件及影响面总体掌控，降低业务连续性风险。构建一、二、三道防线“监督、检查、评估、整改”的风险闭环机制，辅助客户提升二道防线自动化管控水平

诊断和建议

·融合运营、运维动静双态数据，根据风险指标体系梳理数据鸿沟并补充数据维度和采集范围
·借助历史数据及故障事件单数据，构建模型训练集，完成评估模型训练
·利用专家经验构建测试数据集及回测工具，沙盒验证，反复调优风险模型

建设挑战

·运维数据不规范的清洗与推动源头数据治理
·多运维监控工具的数据融合
·源头不同监控频率的数据归一化处理
·多维数据分钟级计算与实时监测

建设步骤和内容

一期

1、建章立制
构建“事前预警、事中监控、事后分析”闭环风险管理体系
2、搭建平台
实现覆盖A+、A类应用系统的纳管和数据融合与多维分析。通过风险健康度模型，形成面向业务的风险监测体系、全景可视化及告警通知能力
3、场景建设
1）构建全景应用墙可视化，面向监控管理人员，从全行整体视角掌握重点系统运行的健康度全貌，重大风险事件和影响面分析，辅助生产运营决策
2）构建应用九宫格等大屏，面向技术运维人员，提供“健康体检”一站式多维分析可视化视角，辅助一道防线综合排障与问题定位，提升处置效率
3）面向风险管理人员，依托后台能力对实现风险事件的后评估量化

二期

1、扩大纳管范围
由A+、A类系统扩大重点逐步覆盖到重要B类系统的纳管，同时实现村行重要应用系统的纳管，满足监管要求
2、平台能力提升
增加健康度模型试算模块，完善模型参数，进一步提升风险事前预警准度
3、场景能力建设
1）实现硬件存储容量的监控预警，通过健康度模型识别因为存储容量带来的业务风险预警监控
2）实现季度关键风险监测可视化建设，通过季度风险监测报告，有效发现生产系统的隐患，降低业务连续性风险

三期（建设中）

1、扩大监控场景
由应用层监控扩大到基础设施、核心网络与生产变更的监控，通过丰富可视化监控场景，进一步提高二道防线对科技风险的自动化监测覆盖面，扩大风险监测范围，提高风险对业务影响面的全面分析与整改
2、新增数据分析中心
围绕历史生产问题，构建风险评估模型，提升事后复盘分析统计与风险评估能力，反向监督科技监测数据质量问题整改，覆盖面查漏补缺，进一步提升风险管理水平

智能运维场景

数智化运维管理

场景简介

将分散存储于不同的系统之中的数据，通过统一的平台来整合和监控这些数据，从顶层的全局视角来综合分析这些数据背后的含义和价值，进而提升决策的效率和质量。以低代码平台为底座，运营分析业务目标为导向，运营数据为抓手，可视化的形态提供管理和决策依据。

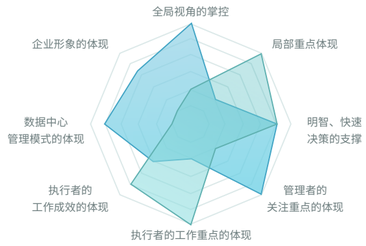
典型用户画像

管理者

运维管理部领导　生产运行部领导　风险管理部领导

执行者

运维一线人员　机房值班人员　技术人员



用户痛点和期待

管理者：掌握全局视角

客户痛点

无法感知到管理方向是否与现状匹配，无法及时掌握执行者的执行成效

客户期待

体现管理者关注重点，提供个性化的全局视角
为运营决策提供精准的数据支撑

执行者：工作重点的体现

客户痛点

无论IT建设投入多少，始终没有适合运维领导关注的视角

客户期待

掌握运维管理的整体情况
明智、快速处理的支撑

场景价值和特性

场景价值

生产运行：在生产运行方面，重点监测业务系统、基础设施异常状态，数据中心的服务质量、资源利用率等关键运维指标，实现故障定位和预测、容量评估、配置优化、节能降耗等，助力运维人员提升运营效率。

经营决策：在经营决策方面，进行服务需求评估、目标考核、投资规划、业务规划等方面的支持，通过业务量预测、成本分析、价值评估等手段，提供决策依据，以指导数据中心战略发展方向。

场景特性

全面的监控与分析能力：利用先进的数据采集和分析技术，能够实现对业务系统、基础设施的全方位监控，及时发现异常状态，并提供可视化的展示，帮助管理者快速把握运维状况。

资源优化与节能降耗：对数据中心资源进行优化配置，提高资源利用率，同时实现节能降耗，降低运营成本。

高效的执行者支持：为一线运维人员提供直观的工作指导和快速处理工具，提升运维效率和服务质量。

灵活的配置与扩展：系统设计灵活，能够根据客户的不同需求进行快速配置和扩展，适应不断变化的运维环境。

场景相关产品

运营决策中心　运维数据中台

案例成果一

项目方：某头部农村商业银行

运维门户

应用系统运行月报

生产环境运行日报

用户主要痛点

·各专业领域工具已基本全覆盖，缺少一体化可视化与分析能力
·缺少理论及工具，实现运维服务向“场景化、平台化、智能化”转变

建设收益

·多维度运维数据分析，充分挖掘运维数据价值
·累计接入60+套业务系统的61个指标，指标实例30W+
·累计接入8套告警源，190+套系统应用日志数据，完成告警日志统一分析呈现
·累计接入完成40+批处理作业数据接入与实时跟踪
·已接入变更、问题、事件类数据，完成运行看板分析

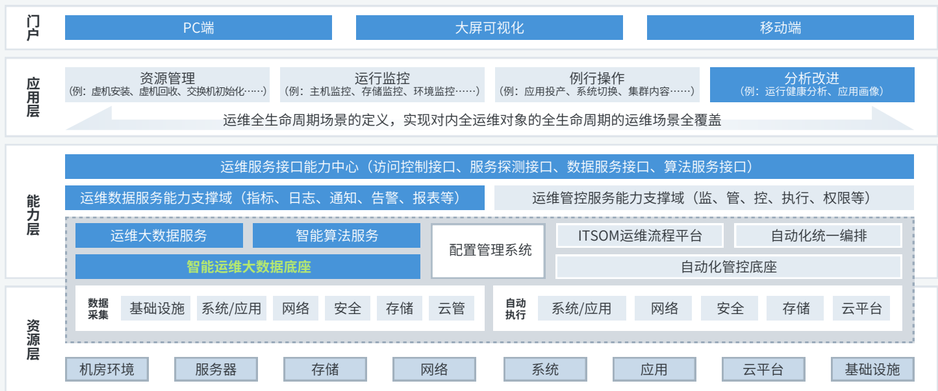
诊断和建议

·构建智能运维大数据平台，“分层分域”规划运维数据
·三层设计：基础能力层、运维场景层、门户层
·两域建设：运维数据服务能力支撑域和运维管控服务能力支撑域

建设挑战

·配置类数据、操作类数据，工具对接难度巨大，需要平衡项目目标与数据接入范围
·链路数据规范性不高，需要持续对数据源头进行治理改造

建设步骤和内容



*以上图片仅为示意图

案例成果二

项目方：某城市商业银行

用户主要痛点

·**无统一门户管理：**各监控工具独立，相互间没有相互的联动；需要单独登录系统进行运维工作

·**缺乏运维数据分析手段：**竖井工具造成了数据割裂，排障操作繁杂，无运维场景支持，故障定位效率低下

·**缺乏网络流量分析工具：**无整体网络流量分析工具，出现网络问题，排查困难

建设收益

·**数字化：**配置数字化、流程数字化、知识数字化、监控数字化

·**标准化：**日志规范、业务流水、交易流水、流量镜像

·**可视化：**机房可视化、大屏可视化、应用拓扑可视化、运营分析可视化

诊断和建议

·通过对报文和日志进行规范化改造，进而实现业务系统问题快速定位

·通过对运维数据的收集和分析，将交易指标同服务器指标相结合，为业务系统的优化提供支撑

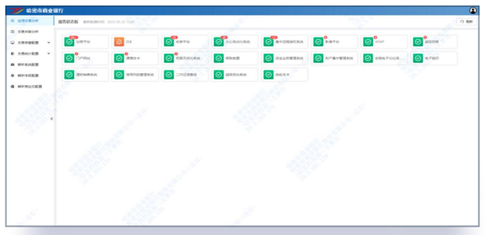
·建立统一的镜像流量网对生产网络的镜像进行管理和分配

建设挑战

·各系统对日志数据的存储方式、位置各不相同，因此面向数据的搜索、事件定位等处理效率偏低

·网络流量实时性要求较高，要求秒级变化，平台架构设计复杂

建设步骤和内容



*以上图片仅为示意图

案例成果三

项目方：某城市商业银行

用户主要痛点

实时运营数据需要依靠人工查询获取，无有效直观工具呈现企业形象数据，缺少合适的渠道和媒介进行展示

建设收益

·完成运维、运营的全维度关键数据收集与呈现

·建设多种运营主题数据分析展示，强化团队内部自我驱动动力

·业务运行领导驾驶舱，辅助精准决策和战略规划

诊断和建议

·通过数据计算中台层，拉齐数据维度以及降低数据的访问复杂度

·构建统一的数据对外消费方式，提升对数据的访问效率和容量

建设挑战

·运营数据与运维数据的安全管理要求差异，对平台的数据架构设计带来一定的复杂度

·超宽屏显示，对单屏展示数据的量、实时性、性能都提出了高要求

建设步骤和内容

一期	告警统一治理及重要事件跟进处置跟踪 业务数据形象大屏 关键日数据屏（年终结算）
二期	运维排班多屏联动（含手机端） 领导专用数据驾驶舱（运营数据）

案例成果四

项目方：某金融清算中心

用户主要痛点

·大量数据孤岛存在，无法集中展示数据

·缺少带有运维经验的专业的展示工具，数据呈现效果达不到要求

建设收益

·数据的集中，统一展示

·日常运维投放，关键指标上屏

·重保时期的重点保障跟踪

·领导视角，运筹帷幄

诊断和建议

·建设底层数据平台，数据集中处理存储

·按难易度、重要度梳理数据范围，并分步骤交付

建设挑战

·数据源、数据种类繁多，调研复杂度高

·实时数据展示，秒级变化诉求量大

·数据交互动效需求复杂，并涵盖大量逻辑计算处理

建设步骤和内容

一期	全中心基础监控，操作系统、中间件、数据库、网络硬件覆盖；全中心集中告警统一管理平台信创监控工具上线；数据中台建设，集中纳管数据可视化大屏展示

*以上图片仅为示意图

智能运维场景

擎智运维大模型应用

大模型赋能运维大数据平台

· 当前基于定制开发和配置开发的数据消费方式，其灵活性和效率上仍有很大优化空间
· 自然语言转查询/接口技术将显著降低数据消费门槛，提升用户体验

运维数据智能体
对运维数据的常用统计分析和工具调用做到语言交互即得

交互式运维
最近10分钟有多少三级以上告警，并按业务系统排名
最近一周，手机银行延迟最高的业务类型Top10
请对最近10分钟的告警做一下根因分析

定制化开发
根据明确需求开发，能解决问题，但灵活性不足，响应不及时，成本高

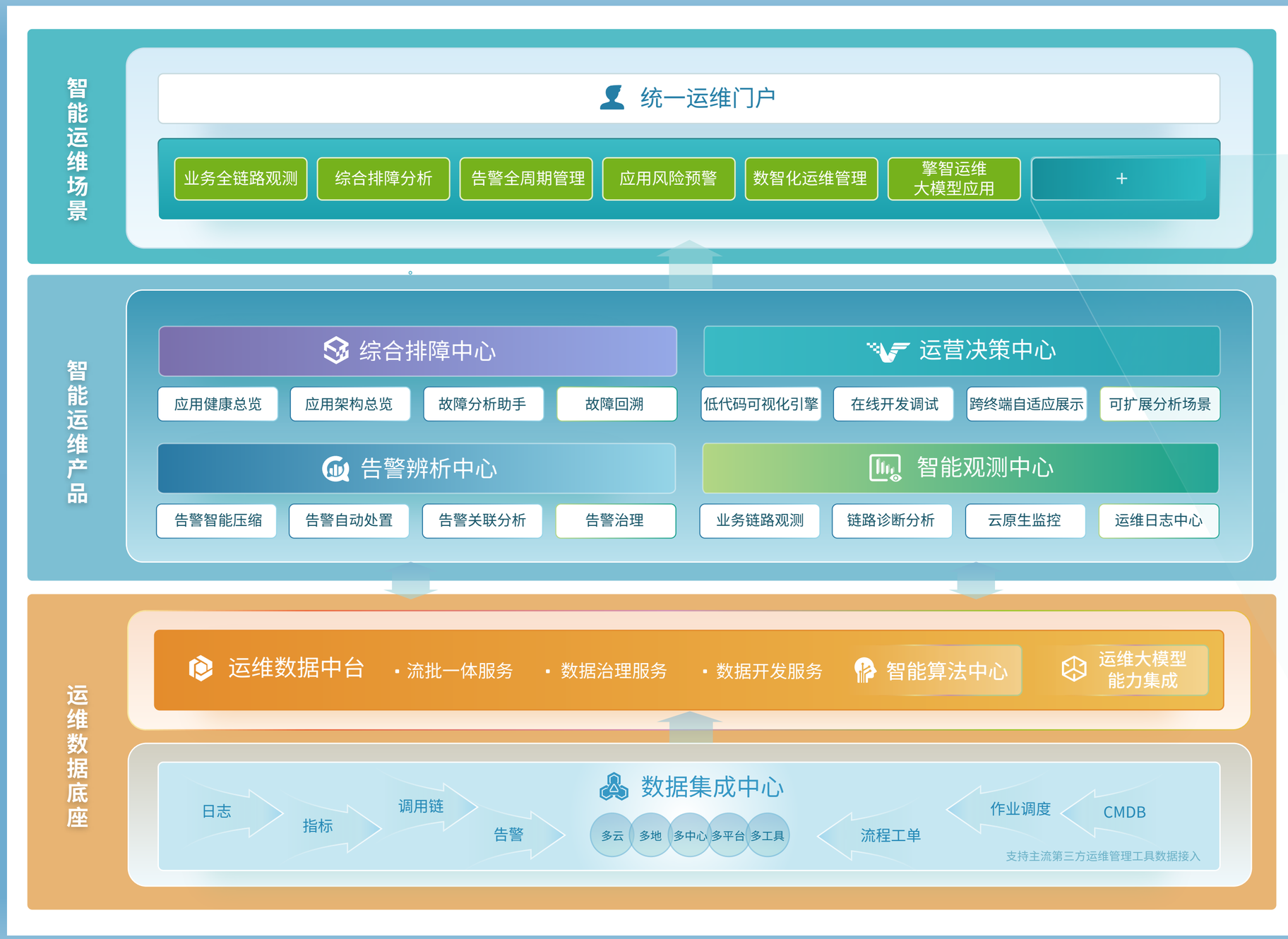
配置化开发
能缓解和减少定制化开发的比率，但仍做不到随用随用

场景相关产品

运维大模型能力集成

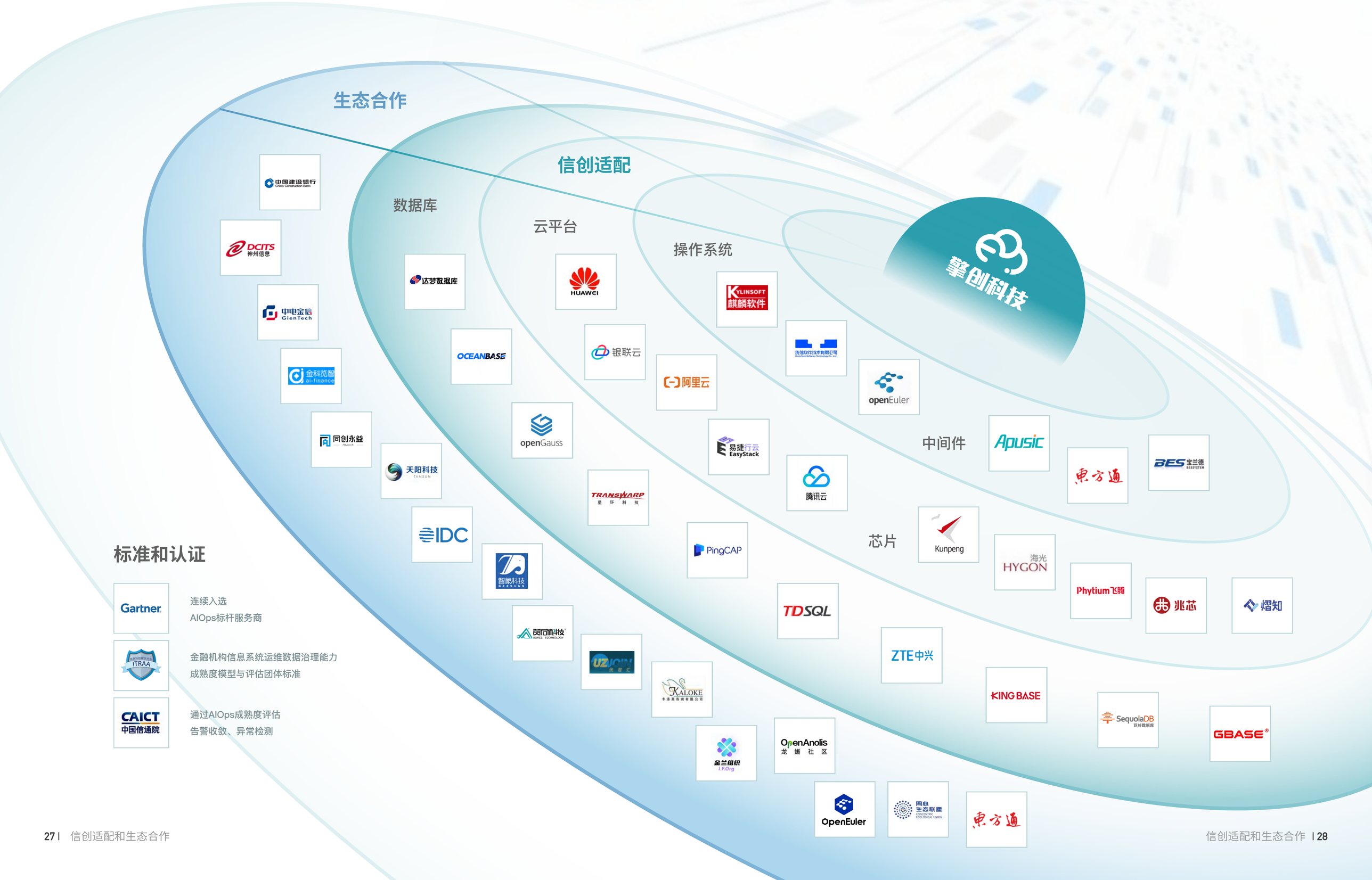
*以上图片仅为示意图

擎创产品架构



自定义智能场景+

信创适配和生态合作



标准和认证

Gartner
连续入选
AIOps标杆服务商

ITRAA
金融机构信息系统运维数据治理能力
成熟度模型与评估团体标准

CAICT 中国信通院
通过AIOps成熟度评估
告警收敛、异常检测

发展历程&客户

2016
擎创科技成立
获百万级天使轮融资

2017
夏洛克AIOps系统正式发布
银联成为首批客户

2018
与复旦大学开展产学研合作
成立大数据智能分析开放实验室
获千万级A轮融资

2019
成立金融大数据
智能运维实验室（北京）

2020
获得“国家高新技术企业”
“上海市软件企业”认定
获亿元B轮融资

2021
业务高速成长
设立多处办事处
获5亿元C轮融资

2022
参与起草多项智能运维
及数据治理国家级行业标准
建立信创生态圈

2023
发布擎智运维大模型
致力行业前沿技术探索

2024
入选金电实验室
金融信创优秀解决方案
（2份）

众多头部银行客户共同选择

以行业龙头用户为起点建立行业标准

金融银行

证券资管

政府及企业

运营商

保险基金

能源交通

客户评价

某国有大行
应急定界·全息监控

本次项目进行监控场景的统一和丰富多样的展示视图极大的提升了实际运维工作的排障效率，缩短了排查时间，可以很快速的响应和处理一般的生产时间。但实际情况毕竟千差万别，针对综合运维场景分析方面目前只有时序分析和同源分析不足以面临这么多复杂的情况，希望在大数据，CMDB情况下探索更多成体系或智能化的分析方法开发出来，逐步做到遇到各种问题都可以迅速命中分析场景并快速处置的目标。

某头部农商行
风险预警

目前系统基本达到事前预警和事中监控的能力，并且后台模块可以实现模型参数在线配置、健康评分试算的能力。目前平台已进入运营阶段，希望让健康度模型变得更智能化，可以通过学习历史数据后自动反馈到模型，自动调整现有模型的规则、参数。从而进一步提升模型的准度和命中率。
构建自动调参模型能力，结合现有评分模型，构建自动调参模型和反馈机制，通过自动学习历史数据，实现自动调参和评分校准，包括评分所有参数、权重的自动调整，进一步提升模型的准度和命中率。

某头部城商行
领导驾驶舱·运营分析

领导驾驶舱能够让领导全方面把控行内经营状况，运维可视化也帮助运维人员实时了解系统健康情况，辅助进行系统问题定位，提高风险识别能力和运维效率，加强平台组件和内置场景的丰富性，便于快速完成整体大屏的拼接上线。

某头部券商
FinOps

低效资源闭环处置优化了原来管理员通过报表分析低效资源，人工发起回收流程的离线繁琐过程，通过一个流程涵盖数据采集、分析、处置、回收、结果展示的整个流程，持续高效的完成低效资源回收工作。