

基于eBPF零侵扰的交易全链路 监控实践

数智驱动，价值创造

2026年8月



- 
- 01 背景痛点 ○
 - 02 体系重构 ○
 - 03 落地实践 ○
 - 04 建设成效 ○
 - 05 未来规划 ○

一、建设背景：监管战略指引，行内发展需要

监管、行业政策/标准指引

- **强化数字驱动的金融业务运营体系**-----《做好金融“五篇大文章”》

综合运用数字技术手段，赋能经营决策、资源配置、业务改造、风险管理、产品研发等各环节，提升数字化经营服务能力。强化科技和数据双轮驱动，加强前沿数字技术研发和创新应用，夯实数据治理能力基础，依法合规推动公共数据向金融机构赋能应用。

- **强化运维安全与自主可控**-----《金融科技发展规划（2022-2025年）》

聚焦于“安全、稳定、自主可控、智能高效”四大原则，强调基础设施韧性、全生命周期数据安全、业技融合运维与国产化替代，明确“深化业技融合，稳妥推进AI在运维监控与故障预测中的应用”要求。

行内发展需要

- **新一代架构升级**-----以云原生为核心的全栈信创分布式架构

构建了基于云平台、分布式微服务及单元化的自主可控技术体系，“两地四中心”高可用布局，具备近6级的国标容灾能力。架构更复杂使得运维难度增大，交易传导路径更长，业务连续性保障需要配套的工具进行辅助。

- **构建全新智能运维体系**-----推动运维规范化操作，促进运维模式变革

当前零散化的运维管理工具布局，距离建设一体化智能运维的整体规划目标仍存在明显差距，现有运维体系架构无法与IT运维全生命周期管理流程实现高效数据互通与功能联动。

一、业务痛点：旧体系已成发展“关键瓶颈”

核心痛点：智能运维体系架构缺失

在新一代建设前，我行运维领域沿用“桥”方案，尚未完成体系化、平台化的智能运维整体框架搭建。无法有效支撑向预测性、主动性、数据驱动的新型智能运维方向转型升级。



运维流程流转衔接不足

运维管理流程分散在不同系统中，管控链路未在工具层面闭环。



运维领域业技融合不足

运维类业务需求质量参差不齐，兼具技术与业务能力的复合型人才短缺。



运维数据规范化有待提高

运维数据标准缺失，口径不统一，监控、配置等数据无法形成资产。



运维工具支撑能力薄弱

缺少专业智能运维工具能力，尚未覆盖故障定位、自动巡检等核心智能运维场景。

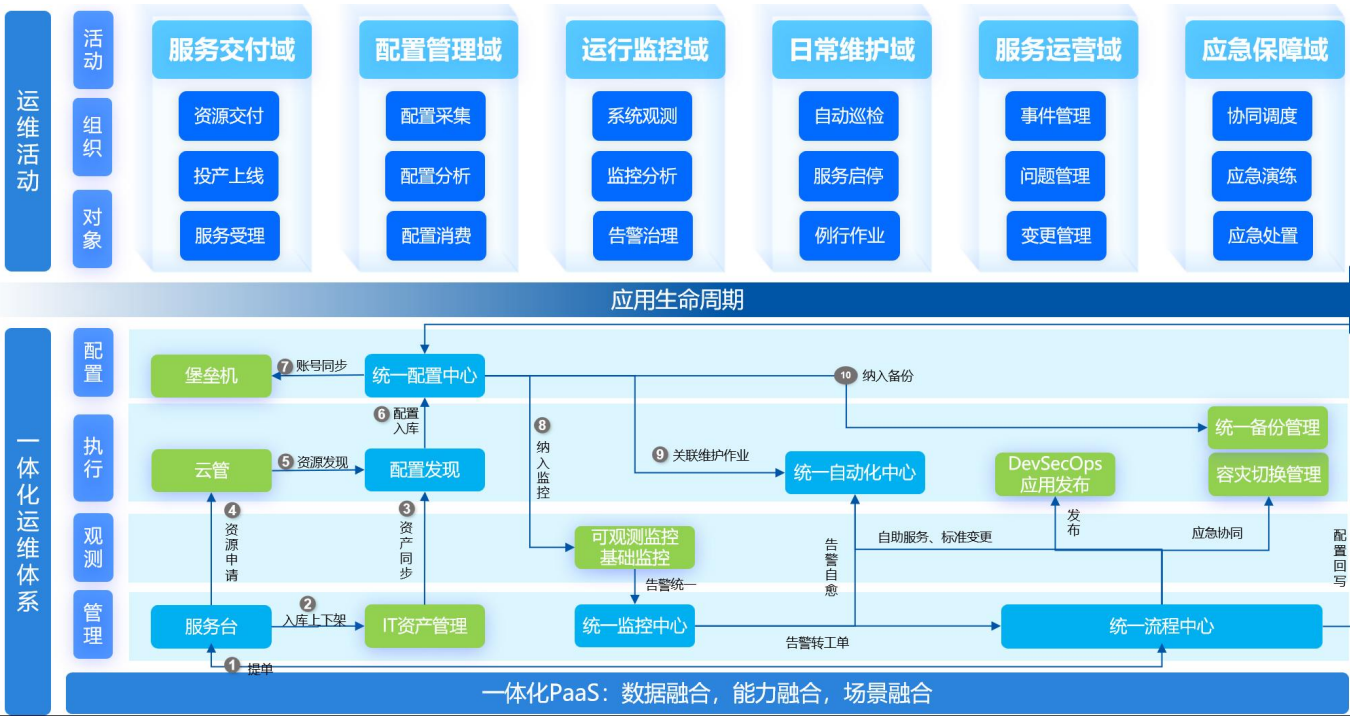
二、体系重构：建设蓝图（1416模型）



二、体系重构：分层解耦，能力聚合



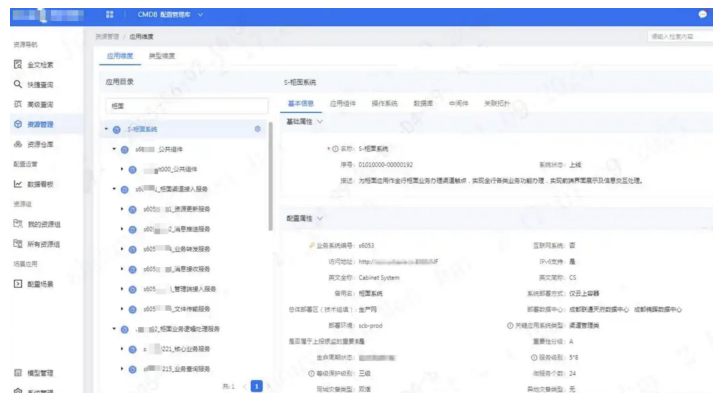
二、体系重构：构建数字化基础底座，助力智能运维转型



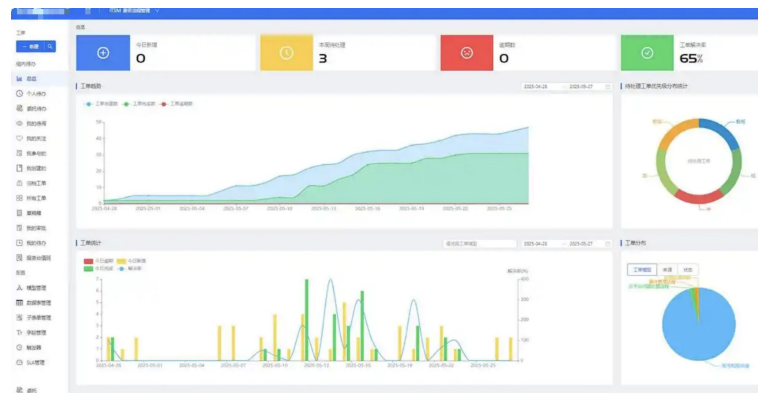
- ✓ 构建统一的运维门户和智能运维数据底座，实现云上云下统一资源配置管理、集中告警管理、流程管理、可视化管理等，打通数据中心的“监、管、控”相关工具，打破多元异构数据壁垒。

- 企业级配置管理中心
 - ✓ 统一数据标准：持续运维数据规范治理，API对接+Agent扫描和人工核检双轨校验机制提高数据质量
 - ✓ 全域覆盖：基础设施层（IaaS）、平台层（PaaS）、应用层（SaaS）
- 统一监控管理中心
 - ✓ 整合现有监控工具，实现统一告警源接入、告警生命周期管理与指标阈值体系建设。
 - ✓ 全链路贯通式故障预警：在运维数据治理的基础上，结合各运维工具，助力故障处理与根因定位。
- 统一流程管理中心
 - ✓ 科技流程中心：统一IT运维服务入口，实现流程的闭环管理。
- 统一可视化管理中心
 - ✓ 实现业务监控、交易监控、资源监控、网络监控等及时、准确、直观的多维度展示。

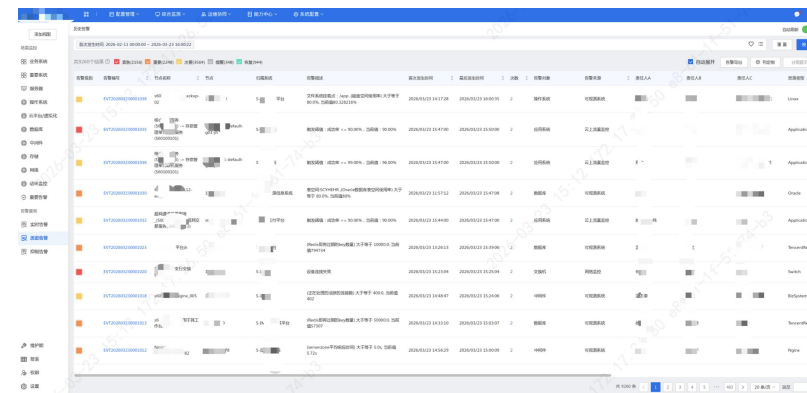
二、体系重构：聚焦“监、管、控、营、析”一体化能力打造



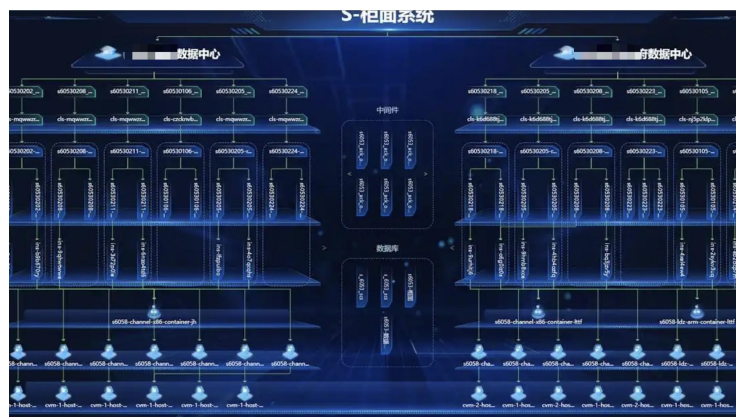
企业级配置管理中心



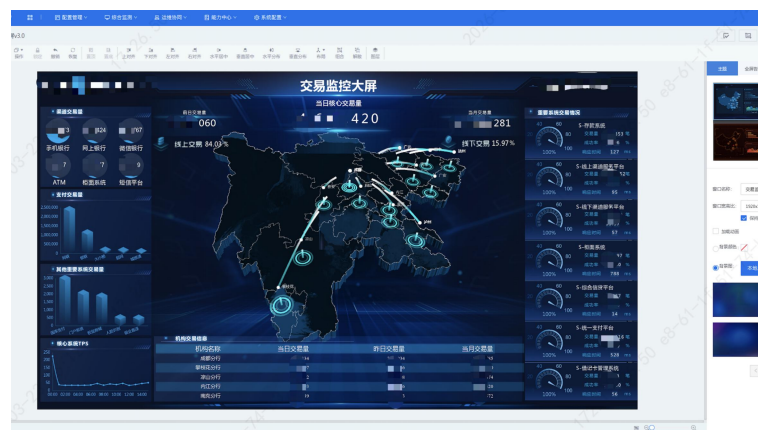
统一流程管理中心



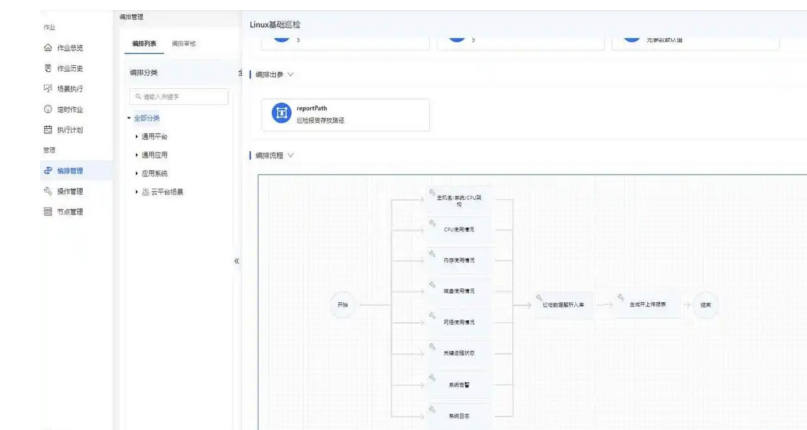
集中告警管理中心



业务全息拓扑概览



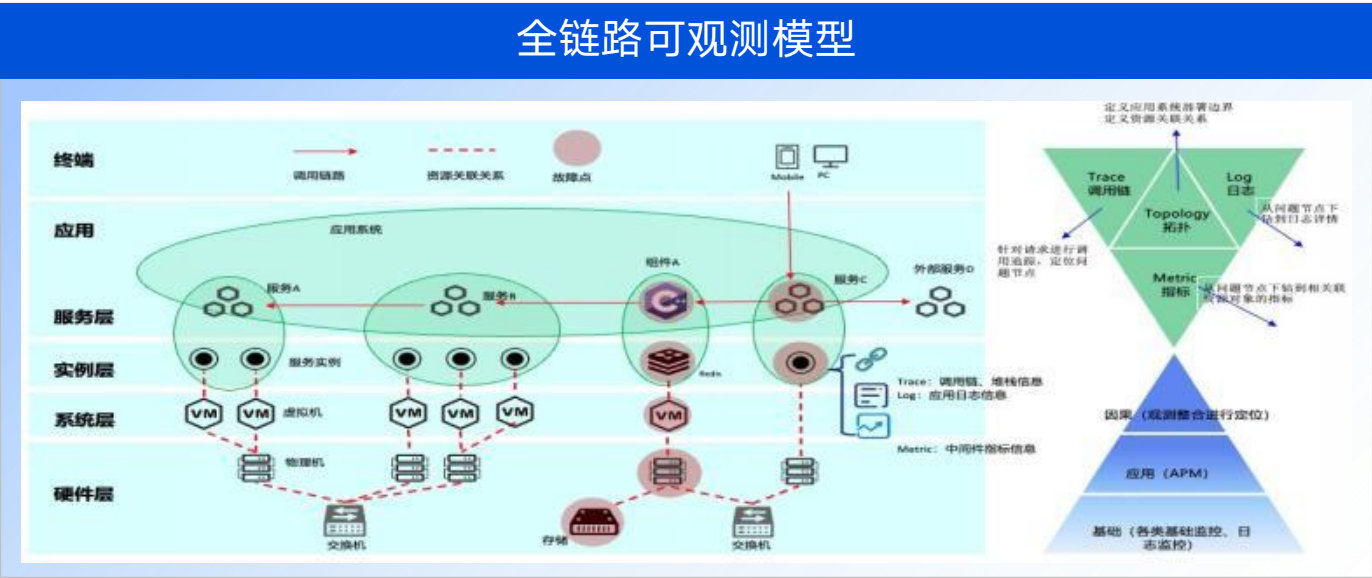
可视化管理中心



自动化管理中心

三、全链路监控：基于eBPF零侵扰的可观测实践

全域部署eBPF内核级旁路探针，零侵扰采集、端侧实时报文解码；通过关键字段智能映射，自动关联追踪 ID，实现端到端全链路监控；全面覆盖新建系统、存量系统、标准化产品（如数据库、中间件等）。



低侵入

相较传统APM监控：无需业务代码改造，无需重启应用，对应用零侵入，无稳定性和采样率担忧。



高时效

相较日志监控：无需业务进行日志规范化改造，高一致性结构化数据，秒级数据呈现。



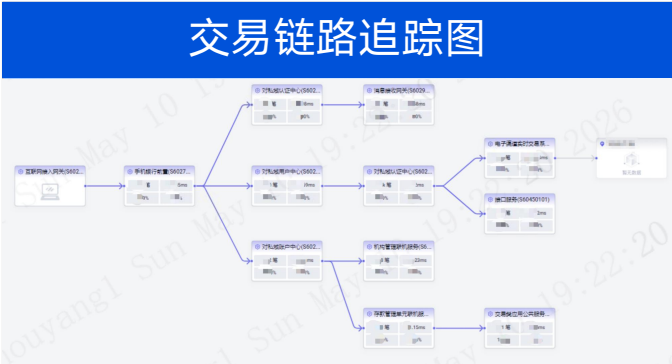
无盲点

相较TAP镜像流量监控：无硬件依赖，低部署成本，无流量监测盲区（云内东西向流量），无遗漏的覆盖业务全部交互数据。



低开销

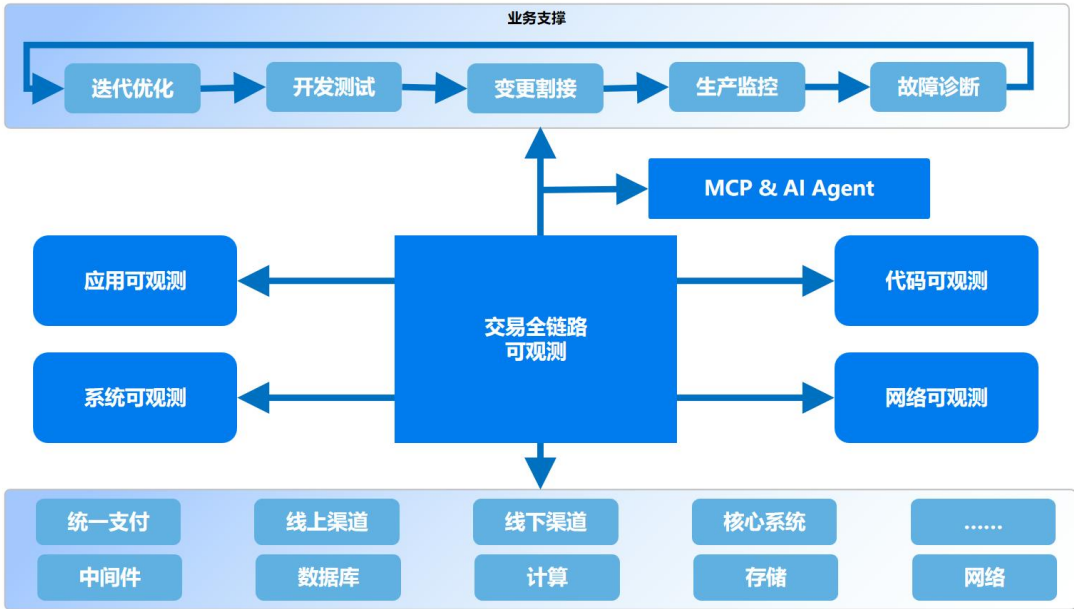
Agent分布式部署，实现协议识别、解码、结构化转换等策略前置，降低网络传输和服务端处理压力，开销低、性能高。



三、全链路监控：云原生、AI原生技术架构

业务架构

- **一轴四维可观测：**以“交易全链路可观测”为轴线，以“系统、应用、代码、网络”四个维度的精细化监控为辐射的全方位可观测体系。
- **AI技术赋能驱动：**标准化的 MCP 协议打通可观测底座与大模型之间的桥梁，为 AI Agent 提供高保真的全息语境。
- **全生命周期支撑：**支撑业务系统的开发测试、变更割接、生产监控、故障诊断、迭代优化的全生命周期保障。



应用架构

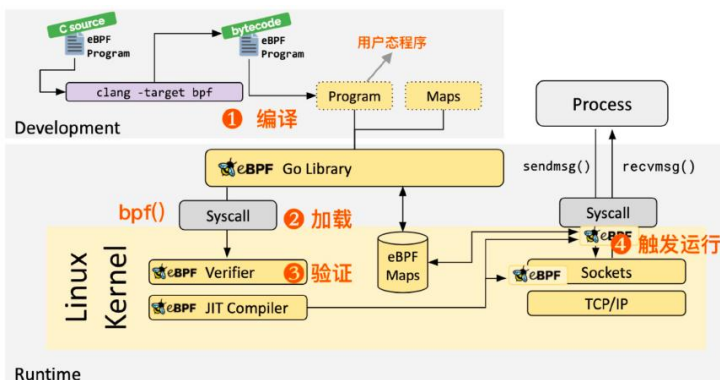
- **采集层：**全环境兼容，OneAgent兼容各类信创硬件、操作系统、数据库、中间件，支持KVM、VM、BM、K8s、物理网络全环境。
- **平台层：**全面AI原生化，包含分析平台与AI智能体：分析平台依托分布式数据库提供多维度数据分析与语义化标签注入，并支持MCP标准接口；AI智能体提供“智能故障诊断、健康巡检”等能力。
- **应用层：**以业务场景为驱动，提供全栈可观测支撑能力，实现以业务交易为中心的全链路观测分析与业务保障。



核心建设思路：“全栈全链路感知、全栈业务上下文关联、AI 原生”

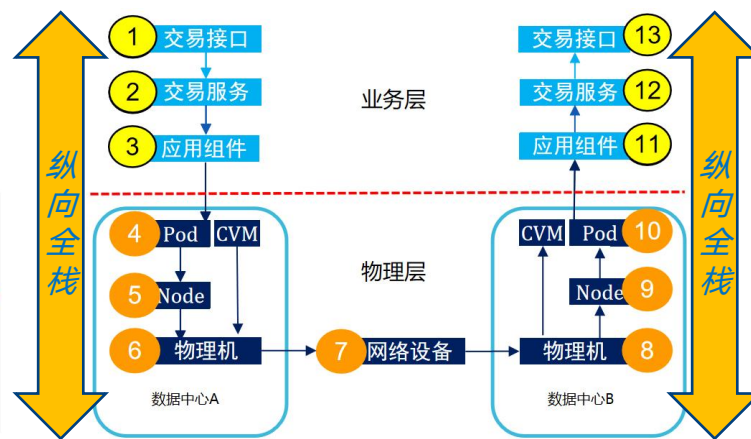
三、全链路监控：内核级零侵扰采集，破解全栈全链路覆盖难题

eBPF零侵扰采集



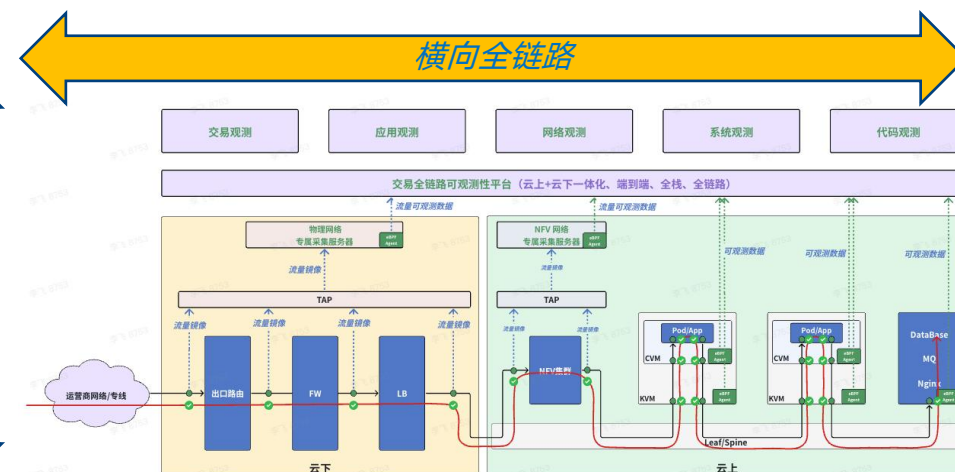
- 高性能采集：**基于JIT技术，采集性能媲美内核原生代码和内核模块，资源开销小于1%。
- 安全采集：**基于eBPF的Verification 机制，采集程序代码受控安全运行，无内核崩溃或进入死循环风险。
- 热加载采集：**可观测数据采集程序动态热插拔，不重启系统、不重启应用、不侵入代码，对业务无干扰。

纵向全栈覆盖



- 纵向全栈覆盖：**覆盖交易、应用、容器、CVM、物理机、网络设备。
- 全环境兼容：**无缝兼容Java、Go、Python、C/C++ 等主流开发语言，以及中间件数据库。
- 全信创兼容：**无缝兼容鲲鹏、麒麟等信创国产软硬件。

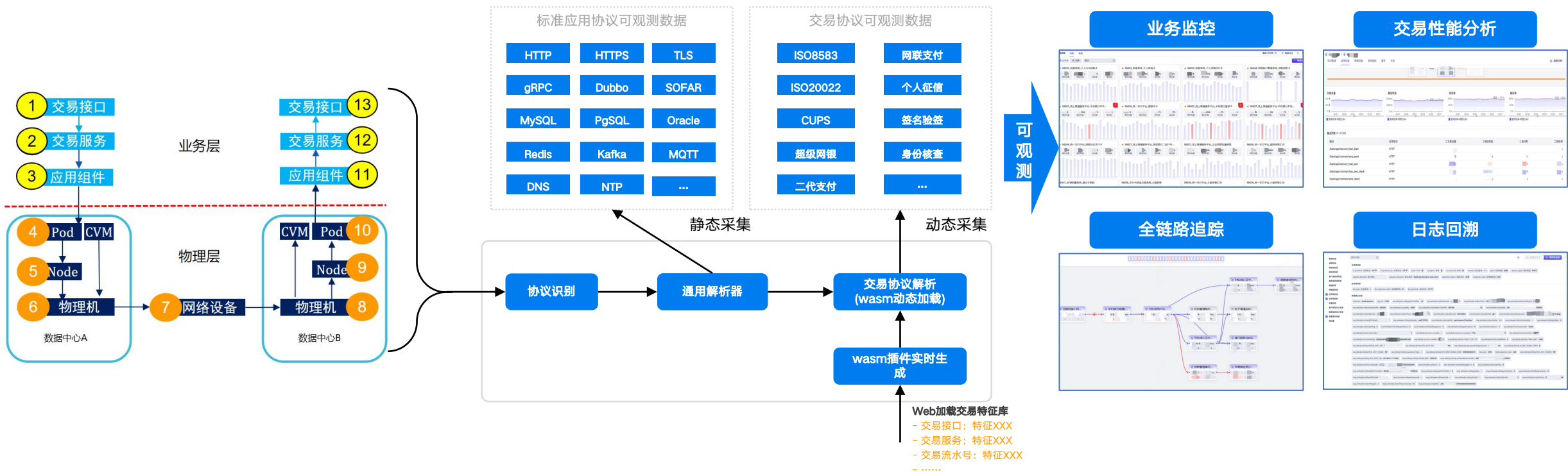
横向全链路、五大维度观测数据



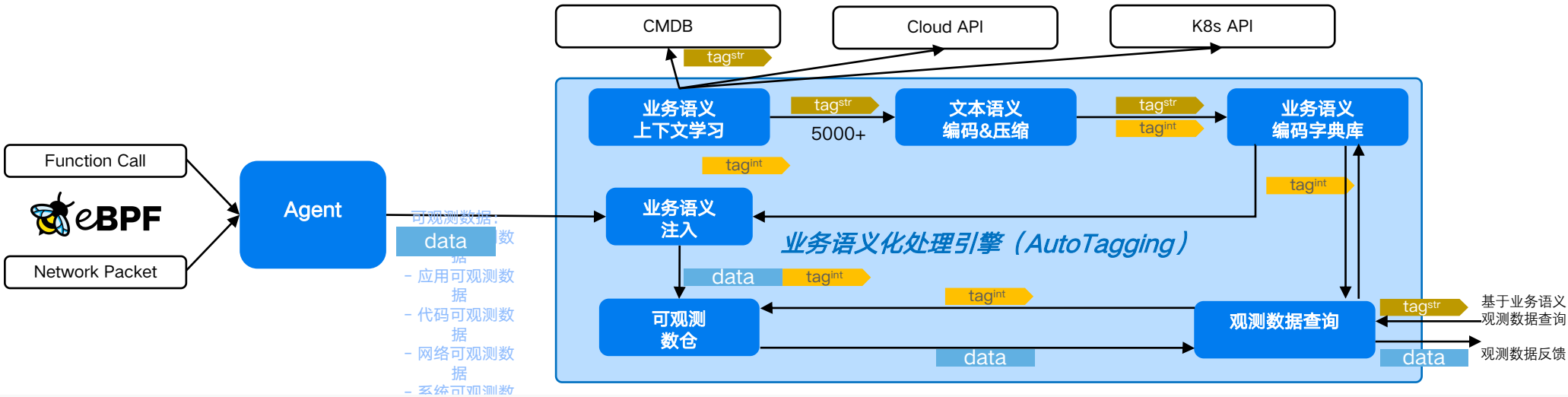
- 横向全链路覆盖：**覆盖数据中心云下、云上全链路。
- 五大维度观测数据：**
 - 交易观测——交易成功率、响应率、响应时长、交易追踪等交易精细数据
 - 系统观测——系统指标、系统日志、系统事件等系统精细数据
 - 应用观测——应用指标、应用日志、应用追踪等应用精细数据
 - 代码观测——函数级堆栈性能剖析等代码精细数据
 - 网络观测——网络性能、网络日志、网络追踪等网络精细数据

三、全链路监控：Wasm可编程协议扩展，敏捷适配复杂金融协议

- 引入 WebAssembly (Wasm) 轻量级可编程扩展引擎作为采集端热插拔核心组件：无需重新编译或重启主程序，即可针对行内私有协议、信创厂商自研中间件协议等非标场景，快速开发并动态下发定制解析插件。
- 协议适配周期由传统方案的1个月以上大幅压缩至1天左右，使监控覆盖能力能够敏捷追随业务系统迭代演进，显著降低长尾协议的接入门槛与持续维护成本。



三、全链路监控：业务语义化处理引擎，兼顾数据价值与存储效能

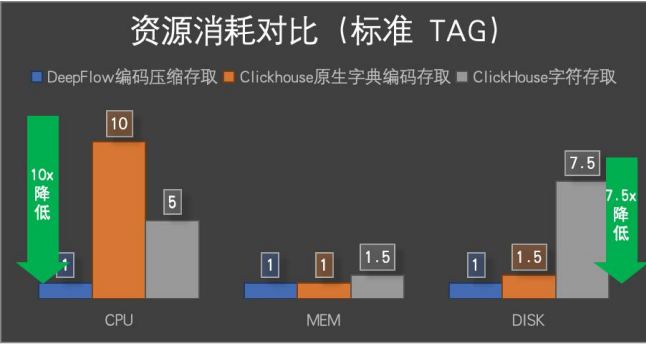


- 自动化业务语义实时学习：具备强大的外部上下文同步能力，实时对接并学习 CMDB、各类云平台管理 API 及 K8s 集群 API 资源元数据、业务元数据。
- 自动化文本语义编码：构建支持 5000+ 以上维度的超大规模业务文本语义编码体系，通过自研压缩算法将海量业务语义标签的存储开销极限压缩至极限，在确保全量标签细节的同时极大提升了查询检索效能。
- 自动化观测数据清洗与标签注入：依托分布式处理引擎实现实时观测数据清洗治理，动态执行毫秒级 AutoTagging 业务语义标签注入，确保多维度观测数据在入库前即具备清晰的业务上下文。

30+资产语义标签

资源池	网络资源	容器资源
区域	VPC	容器集群
可用区	子网	容器节点
云平台	CIDR	命名空间
租户	IP地址	容器服务
云资源	NATGW	Ingress
宿主机	ALB	Workload
云服务器	...	POD

资产标签注入性能对比（10倍提效）



5000+业务语义标签

K8s labels	Annotations *
app	biz/terminalType
version	cicd/deploymentId
env	...
owner	OS ENV *
stage	MODULE_NAME
commitId	...
...	...

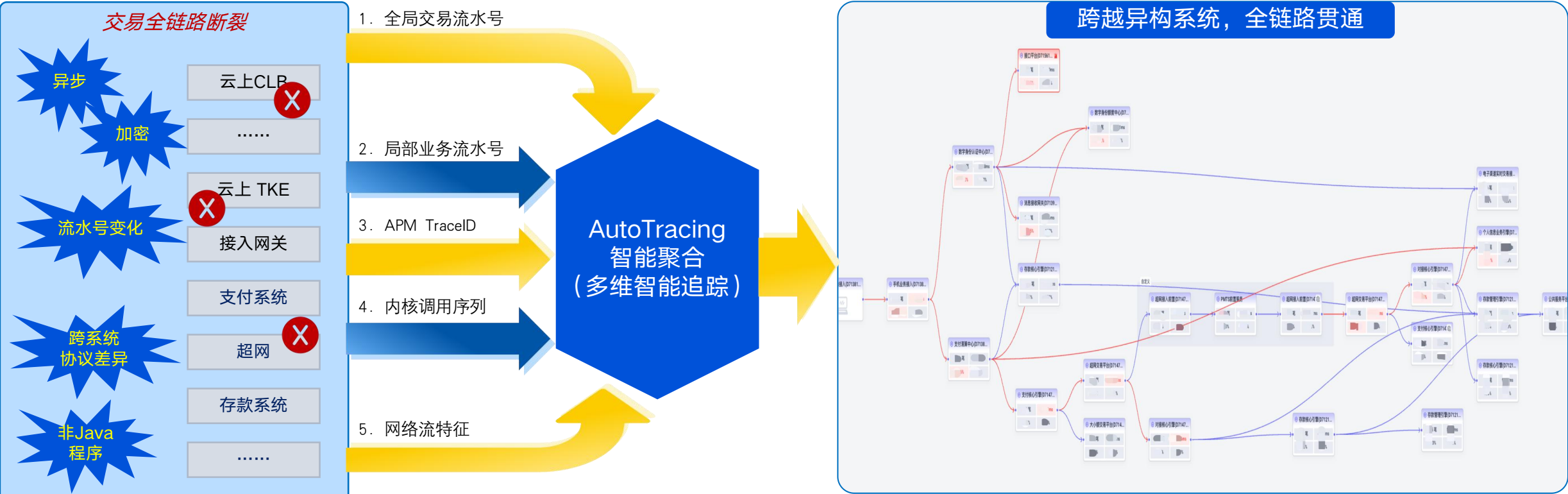
业务标签注入性能对比（50倍提效）



三、全链路监控：AutoTracing多维智能追踪，跨越异构系统ID孤岛

- ① 全局交易流水号——>实时解析行内通用协议报文，提取全局交易流水号——>行内通用协议端到端串联
- ② 局部业务流水号——>实时解析 ISO-8583、网络、超网、特殊业务等协议报文，自动精准提取业务标识——>私有协议串联
- ③ APM TraceID 融合——>原生解析 SkyWalking 标准头字段，新旧系统平滑共存——>存量 APM 投资保护
- ④ 内核调用序列关联——>基于 eBPF 系统调用特征自动生成 syscall_trace_id，无 ID 场景零侵扰兜底——>信创中间件/无 ID 系统
- ⑤ 网络流特征拼接——>综合 TCP SEQ + 时间戳 + 五元组构建调用拓扑，覆盖 Overlay/Underlay 全网络层——>跨物理机/容器网络关联

跨越 5 种 ID 格式体系 · 零行代码改造 · 全链路毫秒级自动关联还原



三、全链路监控：AI原生MCP数据底座，打通智能运维最后一公里



① LLM 不直面原始数据 → 稳定可解释，推理成本低

② 观测工具统一封装 → 可复用、可验证、可演进

③ 生产动作受审批、审计、回滚约束 → AI 不直接改生产

④ 案例、规则、业务口径持续沉淀 → 经验转化为组织资产 15



四、建设成效：体系升级带来的核心价值提升



交易场景全链路



业务系统可观测



配置纳管



监测能力



生产事件下降



可故障恢复

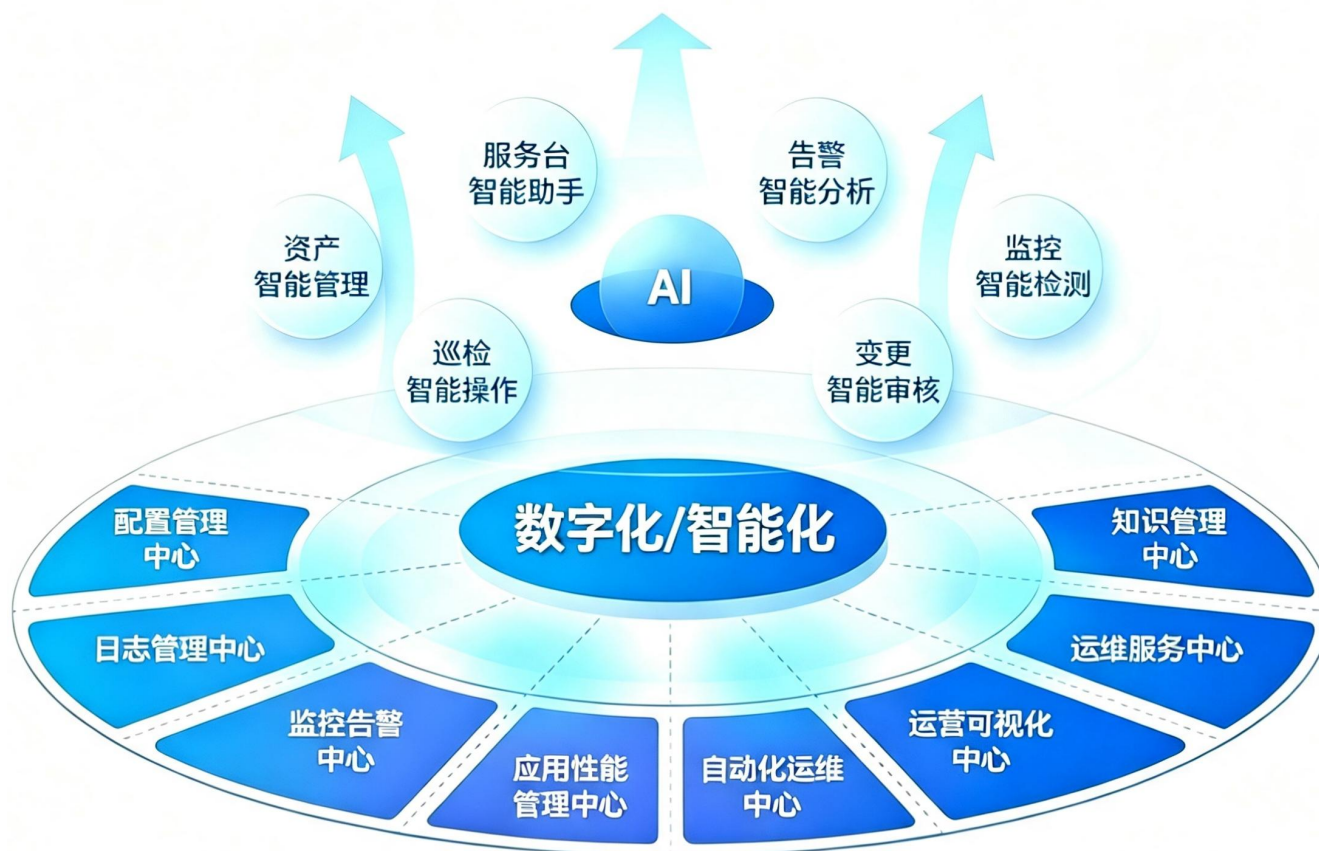
直接成效

- **业务稳定性显著提升。**依托全链路监控、智能巡检、事前预警，提前规避大量潜在风险，生产事件显著下降。
- **排障效率大幅优化。**故障定界时间从小时级压缩至分钟级，定位时长缩短80%以上，处置效率提升60%以上，运维工作从“被动救火”转向“主动优化”。

管理效益

- **运维流程全面闭环标准化。**实现故障全流程留痕沉淀，完成故障经验的闭环复用，有效减少同类故障重复发生，支撑运维治理能力持续迭代提升。
- **运维深度赋能业务。**打破运维与业务的壁垒，通过链路数据、业务数据联动分析，精准挖掘性能瓶颈，为研发迭代、业务优化提供有力的数据支撑。

五、未来规划：迈向数字化、智能化运维



➤ 纵向深耕：筑牢运维能力底层根基

强化垂直工具专业管控能力，打磨监控、故障处置、变更管控核心模块，做深技术底座补齐能力短板。

➤ 横向融合：打破跨域能力壁垒

推进标准化的运维数据治理，进一步融合“监、管、控、营、析”等核心工具能力，实现多系统深度联动与协同发力。

➤ 智能发展：驱动运维模式持续升级

依托治理后的运维数据，借助AI能力构建多维度“运维智能体”，实现异常识别、根因分析等智能化场景，推动运维模式由人工处置向智能运维升级。

感谢聆听

T H A N K Y O U F O R L I S T E N I N G

