Gdevops

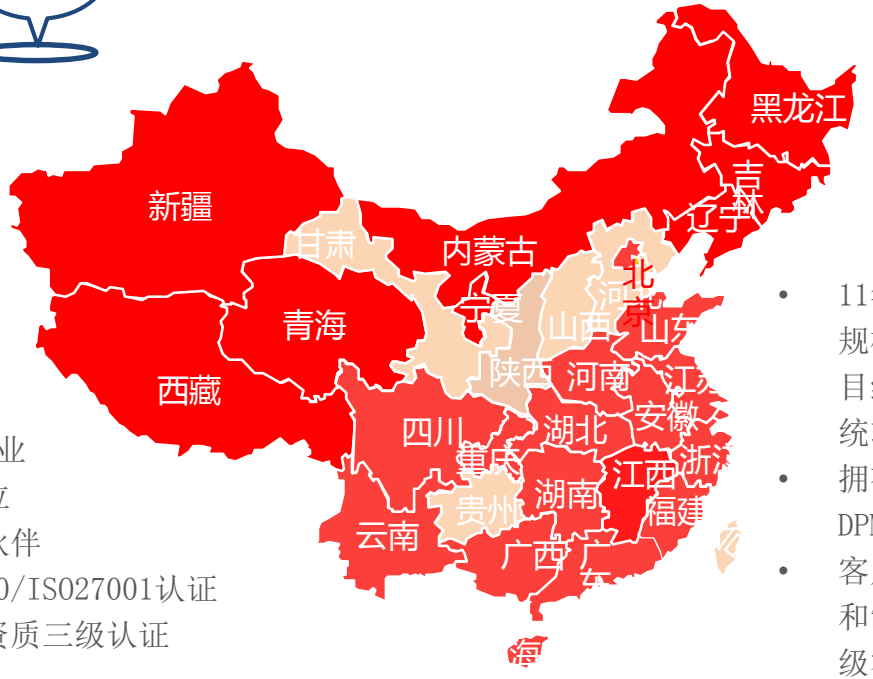
全球敏捷运维峰会

洞察数据，精准分析

演讲人：谢涛（上海新炬/轻维软件）

- 在上海、广州、深圳、北京、杭州、成都、长沙、合肥、昆明、南昌等全国21个主要城市设立了分支机构
- “世界级产品 + 本地化服务”双轮驱动，三线专家团辐射支持

本地化



资质

- CMMI5国际认证企业
- ITSS全权成员单位
- Oracle白金合作伙伴
- ISO9001/ISO20000/ISO27001认证
- 系统集成及服务资质三级认证
- 上海市明星企业
- 上海市守合同重信用企业

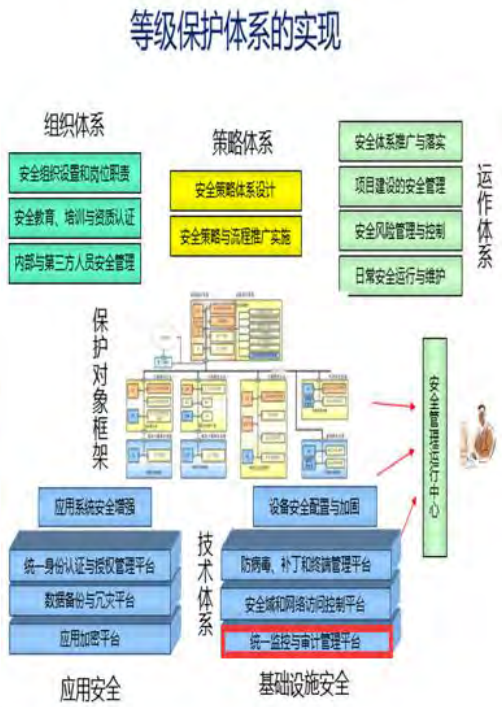
能力

- 11年大型系统平台运维经验，位列全球TOP10规模的系统建设及运维经验、 1000+运维项目经验、 900+专业技术人员，全国最大的系统软件服务商
- 拥有多个自主研发的产品， 如AMP、APM、DPM、IVORY、数据资产管理系列等
- 客户覆盖运营商、金融、电力、交通、政府和制造等各类企事业单位，已超过100家企业级客户

日志：记录下系统所有设备的所有行为

故障定位　　性能瓶颈　　日志审计　　安全事件　　隐患发现

网络安全法关于日志审计的解读



各大行业与日志审计的主要内容

法律法规	相关条款	与日志审计相关的主要内容
《中华人民共和国网络安全法》	第二十一条	采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；
《信息系统安全等级化保护基本要求》	对于网络安全、主机安全和应用安全部分	从二级开始，到四级都明确要求进行日志审计。
ISO27001:2013	A12.4 日志和监视	系统管理员和系统操作员活动应记入日志，并对日志进行保护和定期评审
《企业内部控制基本规范》	第四十一条	企业应当加强对信息系统的开发与维护、访问与变更、数据输入与输出、文件存储与保管、网络安全等方面的控制，保证信息系统安全稳定运行。（注：间接要求安全审计）
《商业银行内部控制指引》	第一百二十六条	商业银行的网络设备、操作系统、数据库系统、应用程序等均当设置必要的日志。日志应当能够满足各类内部和外部审计的需要。

法律法规	相关条款	与日志审计相关的主要内容
《银行业信息科技风险管理指引》	第二十五条	对于所有计算机操作系统和系统软件的安全，在系统日志中记录不成功的登录、重要系统文件的访问、对用户账户的修改等有关重要事项，手动或自动监控系统出现的任何异常事件，定期汇报监控情况。
	第二十六条	对于所有信息系统的安全，以书面或者电子格式保存审计痕迹；要求用户管理员监控和审查未成功的登录和用户账户的修改。
	第二十七条	银行业应制定相关策略和流程，管理所有生产系统的日志，以支持有效的审核、安全取证分析和预防欺诈。
《证券公司内部控制指引》	第一百一十七条	证券公司应保证信息系统日志的完备性，确保所有重大修改被完整地记录，确保开启审计留痕功能。证券公司信息系统日志应至少保存 15 年。
《互联网安全保护技术措施规定》（公安部 82 号令）	第八条	记录、跟踪网络运行状态，监测、记录用户各种信息、网络安全事件等安全审计功能。
萨班斯（SOX）法案	第 404 款	公司管理层建立和维护内部控制系统及相应控制程序充分有效的责任；发行人管理层最近财政年度末对内部控制体系及控制程序有效性的评价。（注：在 SOX 中，信息系统日志审计系统及其审计结果是评判内控评价有效性的一个重要工具和佐证）

目录

01 运维体系

02 异构大数据

03 ITOA

04 IVORY

05 案例

01

运维体系

运维体系建设的四个阶段

PART ONE
01
基础管理

基础设备监控
智能告警
ITIL流程

PART TWO
02
解决方案与工具

企业资产配置与管理
性能管理
容量管理
故障管理
自动化运维
日志分析

PART THREE
03
平台整合

SAAS
PAAS
Cloud化
大数据分析
综合网管
管理制度化

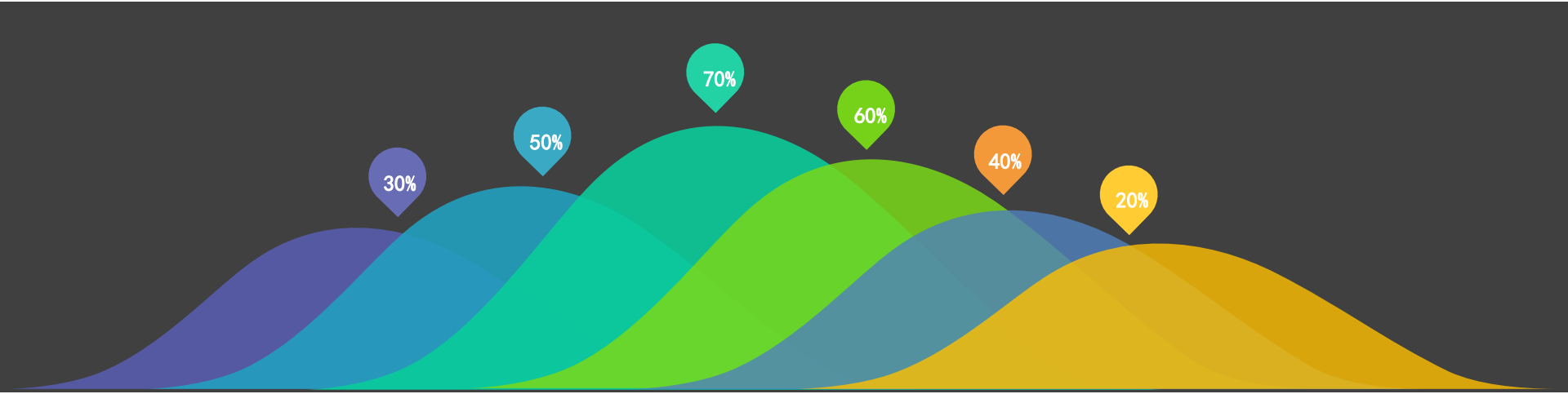
PART FOUR
04
以业务维度为核心

业务感知
关联分析
闭环管理
持续改进与优化
人工智能

02

异构大数据

传统企业运维数据的困境



数据沉睡

海量的数据在沉睡，不知道如何发挥作用

收集困难

数据量大，种类繁多，各种机器数据隔离严重

无法展现

大数据难以通过普通的报表展现，无法帮助业务人员得到有价值的数据

分析缓慢

受限于数据的大小和格式，分析的速度非常缓慢

数据丢失

数据来源复杂，在传送时容易积压、丢失。

安全管控

数据量太大，对安全事件管理力度不大，无法统计


以前以为孤岛就是数据的全部
数据关联是大数据的关键
大数据的速度、性能与资源消耗如何平衡

异构数据OLAP

数据集中

PART ONE
01

PART TWO
02

快速搜索

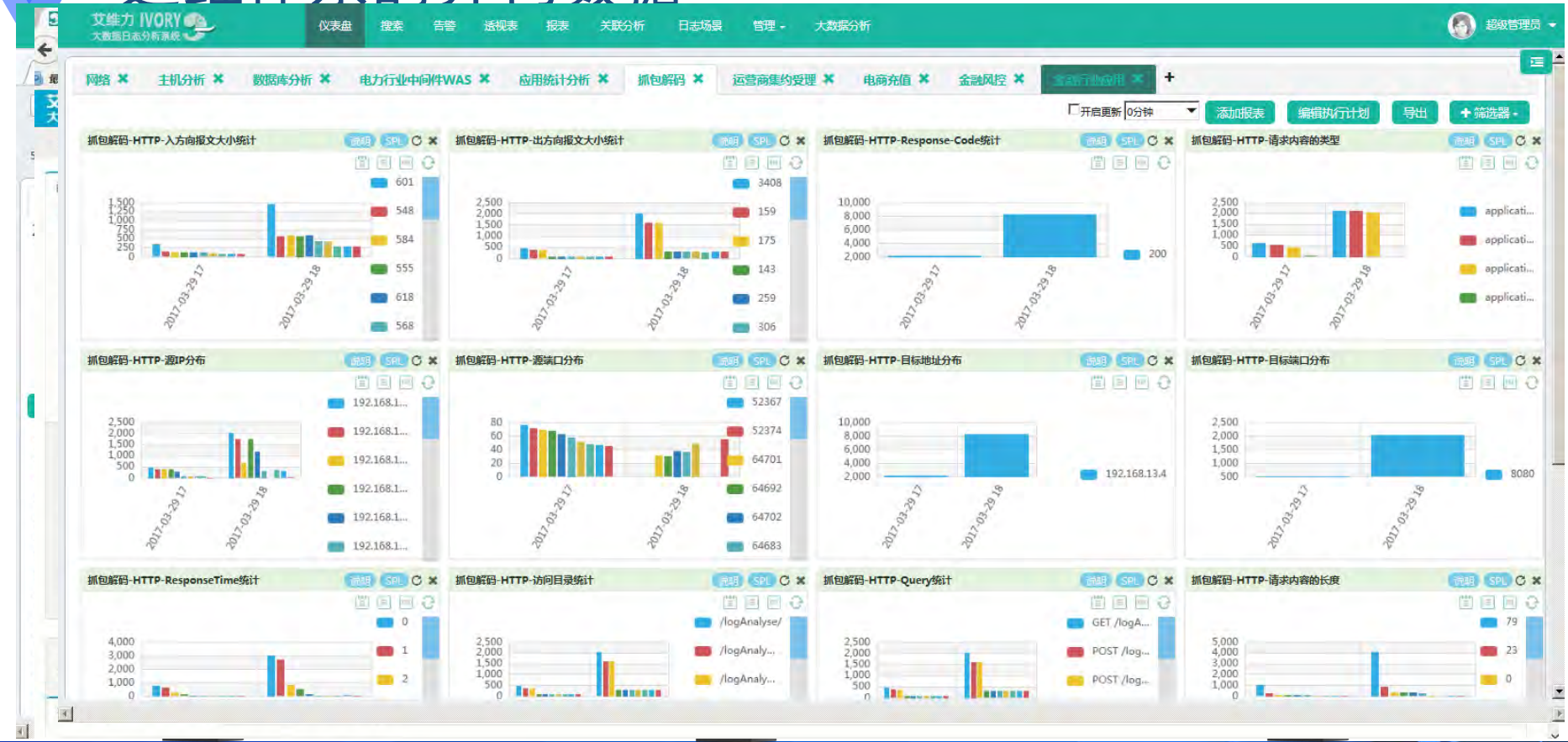
统一格式

03
PART THREE

04
PART FOUR

关联分析

运维体系的异构数据


艾维力 IVORY
大数据日志分析系统
仪表盘
搜索
告警
透视表
报表
关联分析
日志场景
管理
大数据分析
超级管理员
网络
主机分析
数据库分析
电力行业中间件WAS
应用统计分析
抓包解码
运营商集约受理
电商充值
金融风控
开启更新
0分钟
添加报表
编辑执行计划
导出
筛选器
抓包解码-HTTP-入方向报文大小统计
抓包解码-HTTP-出方向报文大小统计
抓包解码-HTTP-Response-Code统计
抓包解码-HTTP-请求内容的类型
抓包解码-HTTP-源IP分布
抓包解码-HTTP-源端口分布
抓包解码-HTTP-目标地址分布
抓包解码-HTTP-目标端口分布
抓包解码-HTTP-ResponseTime统计
抓包解码-HTTP-访问目录统计
抓包解码-HTTP-Query统计
抓包解码-HTTP-请求内容的长度

03

ITOA

IVORY在同类产品中的优势--兼顾非结构化和数据库格式

IVORY

可以接近硬盘读写I/O的极限

数据库结构化数据利于BI分析

机器对文本的读写性能远胜于传统数据库，但是数据库格式化的数据才能真正实现商务智能分析

文本领域的BI分析-数据透视表

可拖动字段

可用鼠标拖动相关字段进行类似EXCEL的表单展示

多种展现模式

支持二维报表，多维报表，饼状图，趋势图，直方图，分区图，散点图等

支持多维分析

行、列、数据均可放入多个字段进行多维分析，灵活设置多种分析维度

简单易用

用户无需技术背景就能分析，让业务人员轻松利用海量数据进行BI分析

04

IVORY

与开源ELK对比

无资源控制

没有消息队列缓存

告警功能弱

用户认证及权限管理

不支持关联统计分析

无自身监控能力

无商业化支持

无机器学习

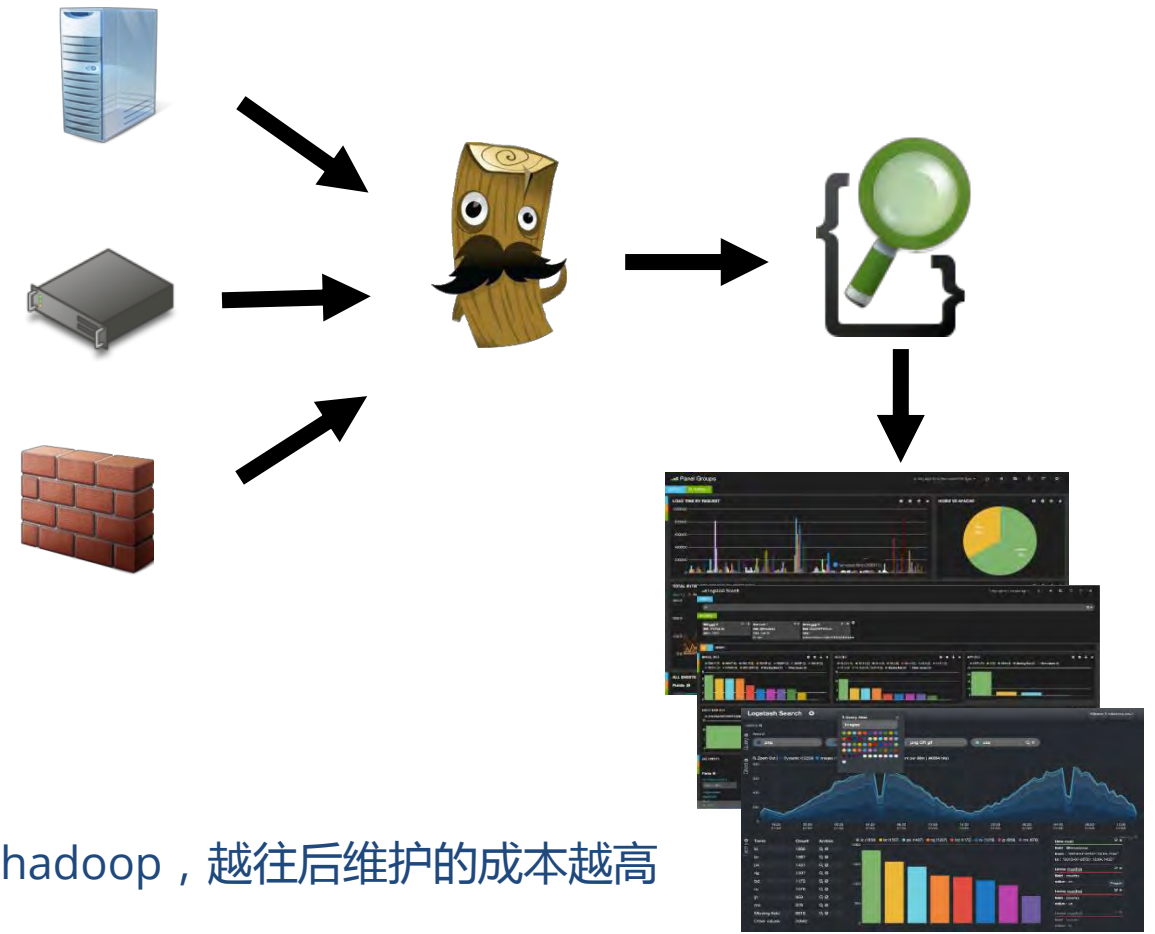
无运维场景

无行业经验积累

难以定制性开发

无数据脱敏

无法即开即用



类似开源软件hadoop，越往后维护的成本越高

IVORY大数据分析

利用大数据技术进行集中管控，提升运维效率，实现 ITOA。

海量数据

T级数据实时处理

搜索定位

数十亿数据可暴力扫表

无序数据结构化

独有多种算法

权限管理

与IT系统的权限对接

函数语言

编写脚本进行复杂分析

机器学习

Yahoo开源的机器学习

即开即用

匹配数百种主流数据源

运维场景

多年运维场景的积累

端到端服务

产品+定制化+服务

运维能力集成


艾维力 IVORY
大数据分析系统
仪表盘
搜索
告警
透视表
报表
日志场景
分析
管理
超级管理员
数据流确认
分析标签
时间轴分析
返回
下一步
时间范围
2017-03-05 14:00:00
2017-03-05 17:00:00
查询
严重
警告
提醒
一般
良好
无日志
2017-03-05 14:18:00.000
2017-03-05 14:36:00.000
2017-03-05 14:54:00.000
2017-03-05 15:12:00.000
2017-03-05 15:30:00.000
2017-03-05 15:48:00.000
2017-03-05 16:06:00.000
2017-03-05 16:24:00.000
2017-03-05 16:42:00.000
2017-03-05 17:00:00.000
网络
存储
主机
数据库
中间件
Web
应用
标签名：数据库异常监控
触发原因：计数:9504 大于 阈值:1

基于egads和arima智能算法的异常检测和状态预测


IVORY大数据可视化大屏
最近7天流量趋势
Traffic trends in the last 7 days
500,000
400,000
300,000
200,000
100,000
0
0918
0919
0920
0921
0922
0923
0924
接入机器数
4000
5000
存储节点数
300
800
服务端数量
0
600
守护进程数量
2000
3000
zookeeper数量
600
700
kafka数量
500
900
最近24小时流量趋势环比
Recent 24 hour traffic trends
60,000
50,000
40,000
30,000
20,000
10,000
0
00:00
04:00
08:00
12:00
16:00
20:00
24:00
MEM
10%
19887
254
16
19887
254
80%
32288
存储引擎
3225
688
ZOOKEEPER
存储E3B
存储E5S
存储E6S
存储E36
服务端E
服务端D
服务端C
服务端B
服务端A
服务端
业务系统
业务系统
服务系统
业务系统
服务系统
业务系统
总数据量
TOTAL DATA
5362G
总索引数
NUMBER OF INDEXES
2300
总分片数量
NUMBER OF SHARES
4698
告警分类
Alarm classification
访问量异常告警
超时告警
监控系统流量告警
集约服务告警
外联支付系统告警
企业总线系统告警
日志分组流量昨天今天对比
Log packet yesterday, today
CRM系统
计费系统
CRM系统01
平台监控
PLATFORM MONITORING
外联支付系统
18
主机
22
数据库
130
中间件
集约服务系统
8
服务器
36
中间件
136
存储引擎

研究方向

行为分析与建模

对用户、软件或网络行为进行分析和建模。实现对异常操作行为的识别和检测。

应用故障预测

学习并识别应用故障，分析应用故障的发生模式，对应用故障的产生进行预测。

网络与系统安全

研究网络安全管理、网络入侵检测和预警等技术。

信息安全监管

研究信息安全监管中的代理技术、隐藏信息的检测与攻击、网络敏感信息的监控、应用领域的信息监管等新技术

据分析体系建设步骤

01 **集中管理/快速搜索**

搭建起大数据存储平台，实现对各类数据的采集和集中存储、提供大数据搜索和分析能力。

02 **数据规范化**

建立数据规范，实现数据信息的标准化，标签化等提升数据含金量。

03 **场景的建设和展现**

根据业务内容，设计分析场景，通过分析平台的数据统计分析功能，实现对业务数据的实时可视化展示。

04 **人工智能/业务感知**

引入人工智能，平台自主学习和对业务进行分析，挖掘更多分析场景。从业务的角度分析问题，深度挖掘，直达根因。

05

案例

案例分享

中国移动 China Mobile

广东 浙江 山东 四川 安徽

博时基金

景顺长城 Invesco Great Wall

中国南方电网 CHINA SOUTHERN POWER GRID

中国电信 CHINA TELECOM

服务平台的广泛应用

IVORY日志大数据分析平台，已在多家大型企业使用，主要涉及电信、金融、交通、政府等领域，典型客户包括博时基金、景顺长城基金管理有限公司、湖南电信、山东移动、广东移动等。客户每天采集处理入库的日志量最高达3.8T，实现T级别日志数据查找秒级响应的速度，并为客户提供第三方日志分析专家顾问服务

洞察数据，精准分析

Gdevops

全球敏捷运维峰会

THANK YOU!