2018 西湖论剑·网络安全大会
West Lake Cybersecurity Conference

中奥科技
ChinaOly Technology

让政务充满AI — 数据治理与政务数据安全

主讲人：中奥科技创始人、总裁　沈贝伦

让政务充满AI
智慧政务 · 智慧交通 · 智慧市监

1

杭州中奥科技有限公司介绍

公司介绍

我们是

全国大数据行业智慧警务应用**前三强**

全国大数据企业**五十强**

中国大数据企业“智慧公安” **Top1**

“行业安全应用” **Top1**

我们有

200+系统，**800+**数据标准

2000亿+数据融合分析

全国警务大数据**30%+**的市场份额

我们为

公安、交通、政法、市场监管以及涉及安全的**政务行业**提供全方位的大数据解决方案，为用户提供数据采集、清洗、挖掘、分析及可视化**一站式**的综合服务。

我们的理念

愿景：让政务充满AI

我们的使命：引领数据时代，共建智慧城市

核心价值观：创新理念，卓越服务，成就客户，共同发展

我们的宗旨：以科技激扬梦想

企业精神： 更快，更高，更强

公司介绍

我们的资质

- 发明专利14项
- 软件著作权52项
- 省科技进步奖

我们的客户

- 客户遍布10多个省份
- 5个分公司
- 50%以上年增长率

让政务充满AI

智慧警务 · 智慧交通 · 智慧市监

2

数据治理中的安全防护

数据安全防护模式

目 标	数据安全防护，不受攻击
防 护 对 象	外部入侵者、黑客
理 念	区域隔绝、划分安全域
手 段	边界防护
融 合	管理与技术分离

现实数据安全面临的问题

使用过程中准内部人员和极少数内部人员的数据泄露

开发过程中的数据泄露

数据治理安全防护

目 标	数据安全使用
防 护 对 象	内部或准内部人员
理 念	数据分级分类、信息合理安全流动
手 段	安全管理和技术支撑
融 合	管理与技术深度整合

数据治理安全防护

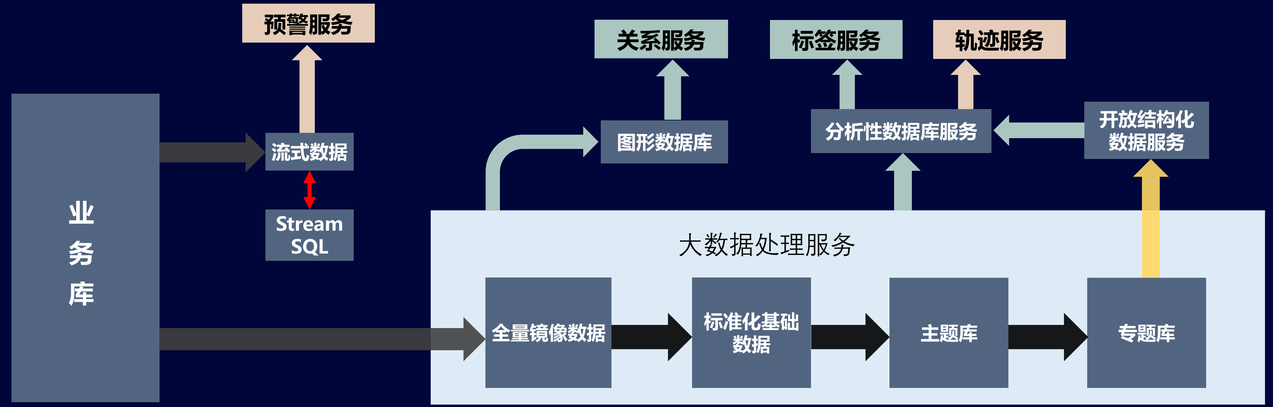
核心—— 以数据的安全使用为目的的综合管理理念

1. 数据的分级分类原则
2. 数据安全使用（管理）规范
3. 数据安全治理技术的导入
4. 数据安全使用规范的监督执行
5. 数据安全治理的持续演进

方式—— 数据状况梳理、敏感数据访问与管控、数据治理稽核

数据状况梳理	敏感数据访问与管控	数据治理稽核
敏感数据访问状况	敏感数据在线审批	权限管理与追踪
敏感数据分布状况	黑客攻击防御	日志管理
敏感数据访问账号及权限	数据存储加密和高效访问	全面审计
	数据模糊化和业务仿真	异常行为报警
	数据分发和溯源追踪	潜在风险预警

数据治理流程


预警服务
关系服务
标签服务
轨迹服务
业务库
流式数据
Stream SQL
图形数据库
分析性数据库服务
开放结构化数据服务
大数据处理服务
全量镜像数据
标准化基础数据
主题库
专题库

数据治理模式

数据源

- XX数据
- 互联网数据
- 物联网数据
- 社会化数据

结构化 / 非结构化 / 即时 / 批量

计算平台

- 实时分析服务
- 即时计算
- 静态脱敏
- 动态脱敏

安全数据

数据资源平台

数据治理	数据集成	数据预处理	数据仓库
数据标准管理	按照标准规范定义数据元	根据数据标准核定数据预处理规则	标准库表建设 数据资产标记 维护标准信息库
元数据管理	录入输入数据的元数据信息	录入处理表的元数据 纪录表元数据关联	纪录元数据变化事件 纪录元数据关联 数据稽查规则的设计
数据质量管控	执行数据稽查，确保数据合规	对被处理数据做质量检测 输出数据质量报告	实施数据质量检测 跟踪数据质量事件，发起事件回溯
数据血缘	纪录输入表初始根节点	数据血缘纪录 上下游血缘跟踪	数据血缘纪录 上下游血缘跟踪 数据搜索功能
数据生命周期管理	输入数据生命周期管理开始	生命周期记录	生命周期纪录 删除老化数据

专题数据 / 主题数据

数据支撑服务

- 元数据管理
- 数据目录
- 数据调度监测
- 数据标准管理

业务数据

应用系统

数据梳理

静态梳理

基于端口扫描和登录扫描的方式完成对敏感数据的存储分布状况、数据管理系统的漏洞状况、数据管理系统的安全配置状况的信息采集技术。

- 系统内的数据库列表，所分布的IP；
- 根据数据特征，发现系统内不同类别和级别的数据如何分布；
- 这些数据库中的安全漏洞和补丁状况，最严重的安全风险；
- 数据库的账号和权限信息，特别是敏感信息标的账号和权限信息；
- 数据库的安全配置状况。

动态梳理

基于对网络流量的扫描，实现对系统中的敏感数据的访问状况的梳理，包括：敏感数据的存储分布、敏感数据的系统访问状况、敏感数据的批量访问状况、敏感数据的访问风险。

- 哪些IP（数据库主机）是数据的来源；
- 哪些IP（业务系统或运维工具）是数据的主要访问者；
- 敏感数据是如何被业务系统访问的（时间、流量、操作类型、语句）；
- 敏感数据是如何被运维人员访问的（IP、用户、操作）。

敏感数据访问与管控

● 各政府职能单位信息汇聚采集、互联网入口公众信息采集等场景需求下，需要共享数据，但敏感数据不能全部开放。

动态脱敏：根据访问来源IP、应用系统、账户、时间等信息，对需要共享的敏感数据，按照数据的敏感级别和应用的需要，灵活的配置动态脱敏策略，实现外部应用能够安全可控的使用共享的敏感数据，防敏感数据泄露。

● 海量数据进行分析计算时，为保障数据的安全性。

静态脱敏：对静态数据进行包括屏蔽、变形、替换、随机等脱敏方式，防止大数据平台内部对隐私数据的滥用，防止隐私数据在未经脱敏的情况下流出。

● 为保障数据库的防御能力。

数据库防火墙：将数据库防火墙部署在应用系统和数据库之间，防护由于WEB应用漏洞、应用框架漏洞等原因造成的黑客攻击数据库，窃取敏感数据。

● 对外数据公开下载以及开发利用等服务场景下，为保障数据传递的安全性和可追溯能力。

数据水印：通过对原数据添加伪行、伪列，对原始敏感数据脱敏并嵌入标记等方式进行水印处理，保证分发数据正常使用。一旦信息泄露第一时间从泄露的数据中提取水印标识，通过读取水印标识，追溯数据流转过程，精准定位泄露单位及责任人，实现数据溯源追责。

数据治理稽核

异常行为分析

通过一些数据分析模型，对异常行为发现和定义。定义异常行为主要有两种方式：一是通过人工的分析完成；一是对日常行为进行动态的学习和建模，不符合日常建模的行为予以告警。

数据审计

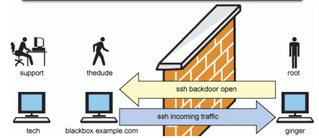
基于网络流量分析技术、高性能入库技术、大数据分析技术和可视化展现技术实现包含登录行为审计、操作行为审计、执行结果审计等日志审计功能；

日志中心

结合业务逻辑，利用可视化方式对数据库日志信息进行全面的展示与管理。

基于数据治理的应用开发模式

物理防护和防火墙



- 访问行为控制
- 危险操作阻断
- 可疑行为审计

数据安全治理

- 数据脱敏
- 数据状况梳理
- 标签服务体系
- 数据模型算法
- 数据高效服务
- 主题专题库
- 数据超级应用
- .....

数据服务

- 数据安全的稽核
- 数据水印
- 行为监测

对某些静态或实时的敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。

实现数据资产的“静态+动态”梳理，持续发现敏感数据，指定不同的敏感级别；对平台数据库系统中不同用户、不同对象的权限进行梳理并监控权限变化。

定期对账号和权限变化状况进行稽核，保证对敏感数据的访问在既定策略和规范内。

在输出数据中掺杂不影响运算结果的水印数据，用来记录分发信息，当已知泄密数据的样本时，可追溯数据泄露源。

对日常行为建模，从海量数据中快速发现异常行为和攻击行为，避免系统面临大规模失控。

3

政务数据安全治理案例

让政务充满AI

智慧警务 · 智慧交通 · 智慧市监

2018 西湖论剑·网络安全大会
West Lake Cybersecurity Conference

核心业务及产品体系

1 政务上云

中奥科技为政务云客户打造“云计算+政务”体系，提供上云咨询、架构设计、系统迁移、数据整合、应用融合、运行维护等一站式服务，让政务系统轻松上云稳健运行。

2 数据治理

数据治理以“三融五跨”为主旨，即技术融合、业务融合、数据融合，实现跨层级、跨地域、跨系统、跨部门、跨业务的协同管理和服务。数据资源以统一的标准进行归集、沉淀，形成统一标准的数据资源池，将数据资源加工为相应的主题库、专题库、标签体系以及资源目录等，结合标签、关系、预警、轨迹、日志分析与算法模型，对外提供服务，最终满足“预警、预测、预防”的数据资源使用需求。

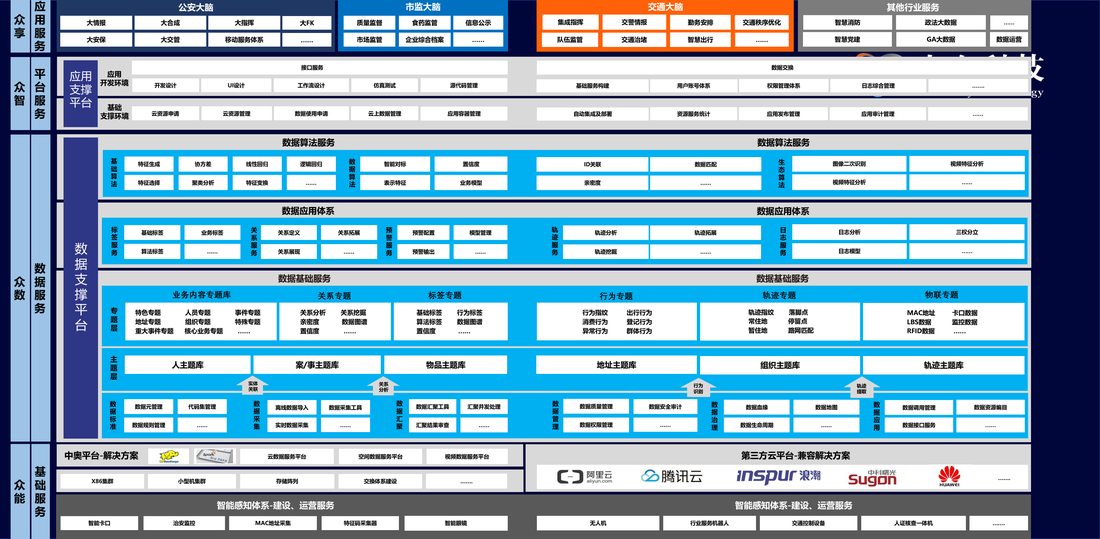
3 公安大脑

基于“人工智能+ 警务”架构
建设开放，透明，服务型智慧公安大脑

4 交通大脑

交通大脑助力解决城市交通管理顽疾
连接警方与民众
连接业务与业务
连接数据与服务

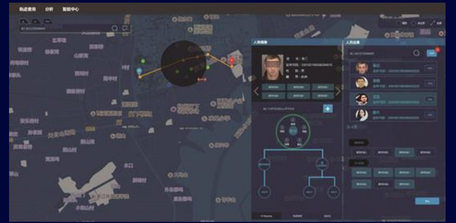
让政务充满AI
智慧警务 · 智慧交通 · 智慧市监



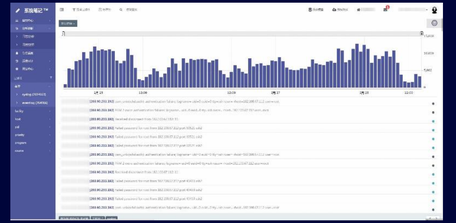
优势产品：五大服务中心

标签中心

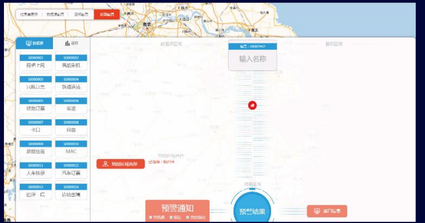
关系中心



轨迹中心



日志中心



预警中心

优势产品：智能设备

分析能力　自然互动　智能学习　知识共享　数据应用　……

让政务充满AI

智慧警务 · 智慧交通 · 智慧市监

智能算法

公安各警种业务

数据分析　算法模型

数据挖掘　机器学习

情报专题	时空轨迹分析	同行同住分析	落脚点预测	……
治安专题	人员多维研判分析	车辆多维研判分析	案件多维研判分析	……
重点人车	重点车辆警情分析	重点驾驶人警情分析	重点人车预警分析	……
交通专题	区域交通特征分析	实时流量分析	交通态势预警分析	……

典型案例

ZJ省公安云上公安智能防控

SX市公安信息化实战平台

ZJ省GA大数据平台
ZJ省公安厅FKB信息情报作战平台
ZJ省公安厅情报信息综合应用平台
HN省公安大数据实战应用平台
YN省JD大数据实战平台
HZ市公安局信息资源服务平台
BT市大数据研判平台
.....

THANKS
谢谢观看