全知科技
QUAN ZHI TECH

数据在流动，可见才安全

Gartner推荐

政务数据共享安全实践分享

全知科技（杭州）有限责任公司
产品市场总监--申杰

全知科技
QUAN ZHI TECH

目录
CONTENTS

全知科技
QUAN ZHI TECH

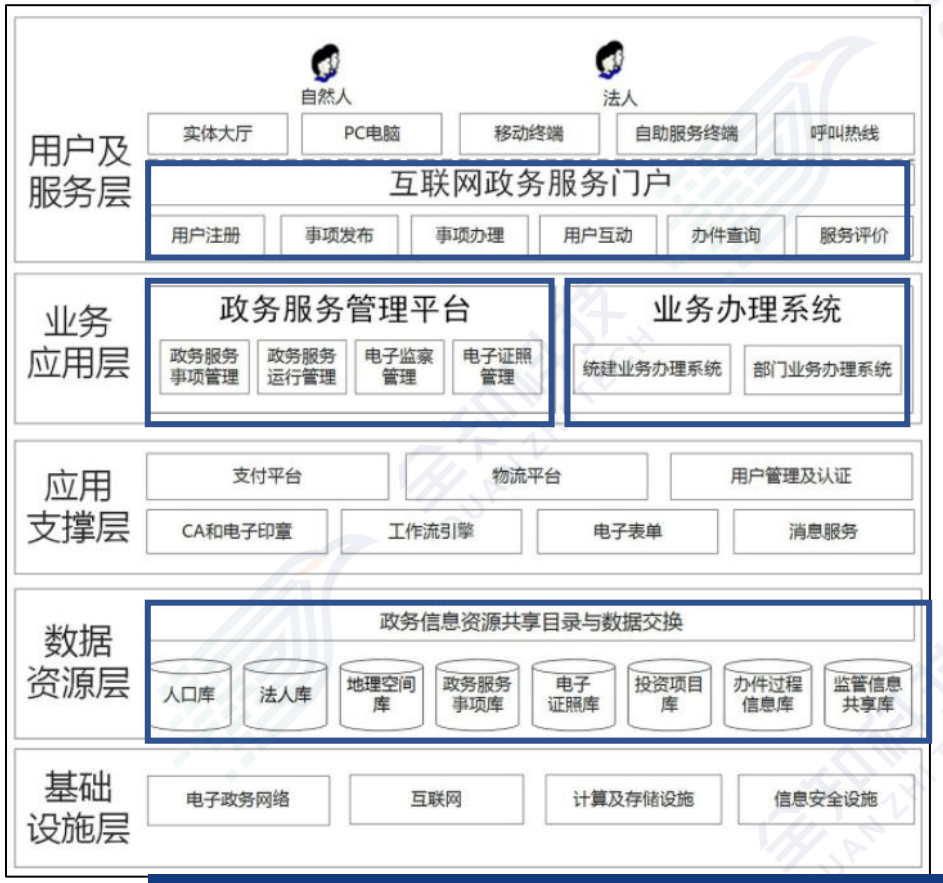
业务现状观察

1

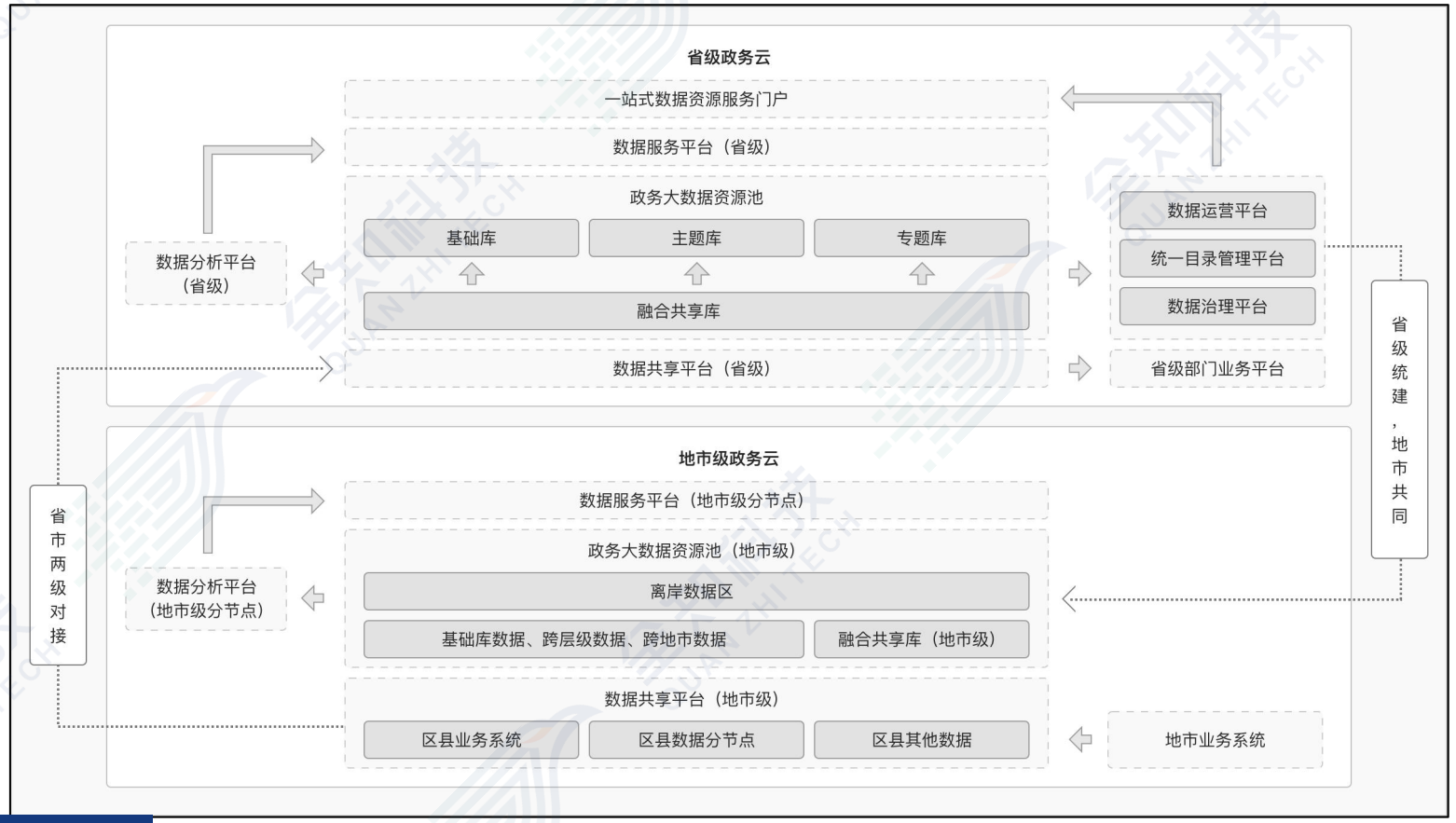
互联网+政务服务的落地 – 一体化在线服务平台

全知科技 QUAN ZHI TECH

“互联网+政务服务”平台技术架构图



省市平台对接示意图



涵盖43个国务院部门，31个省（自治区、直辖市）和新疆生产建设兵团

① **纵向贯通**：打通国家、省、市、区（县）四级网络
② **横向打通**：实现各级部门单位间的互联互通
③ **平台建设**：打破信息孤岛，实现数据共享交换

政务大数据的数据流转

全知科技 QUAN ZHI TECH

大数据资源为核心

大数据理念为引导

大数据技术为支撑

碎片化信息 → 统一化平台

公共服务：让数据多跑路、让群众少跑腿

政府决策：用数据说话、用数据决策

产业转型：激发业务创新、提升核心价值

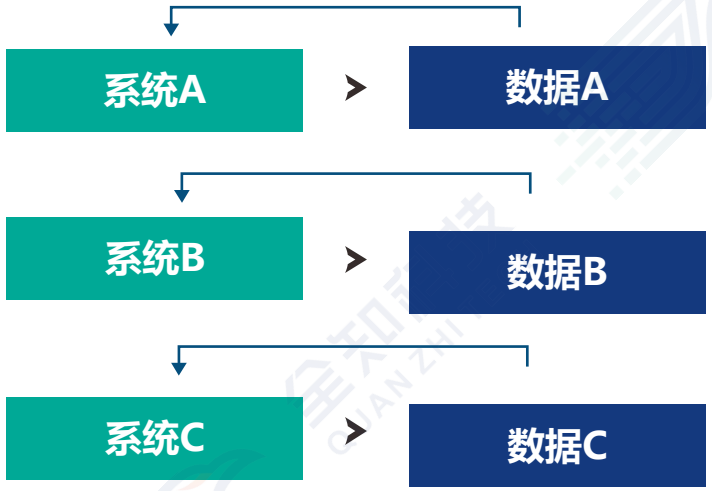
从大数据集中到大数据运营

- 目标、架构和资源统筹规划
- 数据共享

- 大数据为核心、大连接为基础、大安全为保障，实现大协作

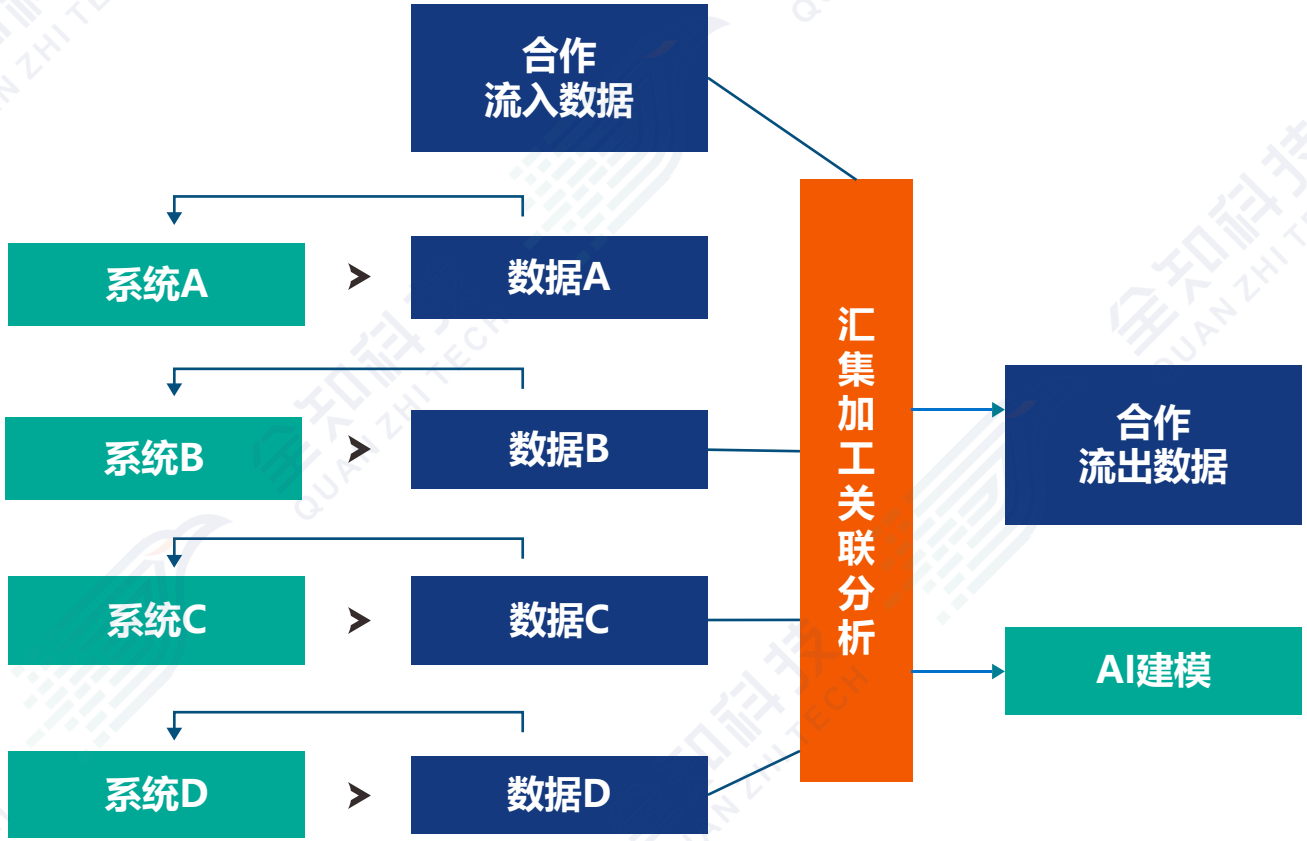
数据的整合、流通、共享开放和深度利用，贯穿新一代政务信息化建设各环节

DT时代的数据流动



IT时代：业务数据化

数据以信息在计算机系统中承载的方式存在，数据来源和使用单一，也没有形成复杂的上下游关系



DT时代：数据业务化

数据通过业务采集和多种外部来源渠道汇集、多维度加工、回流业务系统、以及各种系统数据不断加工和使用形成了非常复杂的上下游消费链路以最大化数据的价值同时流出体系。数据的管理、用途授权控制、业务使用流动的保护风险都非常复杂。

全知科技
QUAN ZHI TECH

数据安全挑战

2

政务行业开展数据安全的驱动因素

全知科技 QUAN ZHI TECH

政务行业在数据安全领域面临的挑战

01.政策驱动

国家顶层规划、重要政策文件中明确指出，要加强数据安全防护能力，保障**重要公开数据、个人隐私数据**安全。

02. 合规驱动

以**数据安全法**和**个人信息保护法**为代表的一系列法律法规的颁布，增大了数据合规和数据安全风险。

03.事件驱动

黑客、勒索病毒、突发的**数据安全事件以及数据泄露事件持续上升**，将对公众社会甚至是国计民生造成极大的负面影响。

04.风险驱动

随着**“互联网+政务服务”平台**的广泛应用，很好的推动了政务大数据的整合与使用，但同时也面临更大的安全风险。

数据安全风险

全知科技 QUAN ZHI TECH

互联网+政务

案例一：

某政务平台的举报中心存在互联网未鉴权接口，可批量拉取举报人隐私信息，涉及个人姓名、手机号、身份证、举报内容和举报奖励（涉及5万+条举报人信息）

案例二：

某政务的居家养老平台大屏存在互联网未鉴权风险，可任意访问老人的姓名、手机号、身份证号码和实时的经纬度信息

案例三：

某省级互联网政务的数据管理平台收集了大量的政务数据，异常开放到互联网侧，未鉴权，可通过可枚举ID遍历敏感数据

网格化管理

案例一：

某政务楼长APP系统，登录界面可绕过，直接查询该市2000多万的公民信息（姓名、手机号、身份证号码、家庭住址），其中系统自动标记出来200多万儿童信息

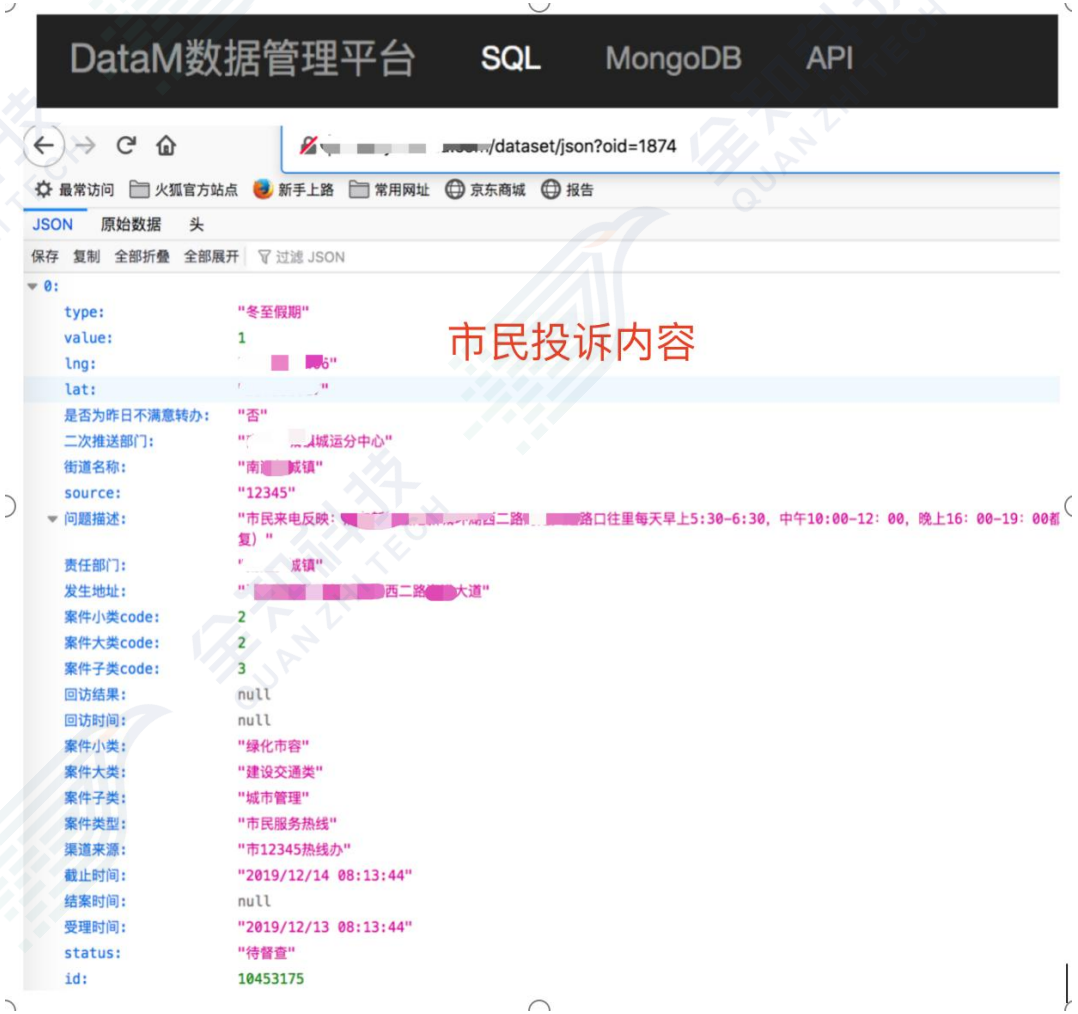
案例二：

某政务系统供应商的服务器私自与政务平台某接口持续通信，长时间慢速调取公民信息，包括公民姓名、身份证号、地址等

数据安全风险

居家养老的手环监控平台

互联网+政务的数据管理平台



全知科技
QUAN ZHI TECH

解决方案剖析

3

数据安全法解读

全知科技 QUAN ZHI TECH

第一章 总则

第三条：数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第三章 数据安全制度

第二十一条：各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护…

要求数据需要分类分级

第四章 数据安全保护义务

第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

要求对数据暴露面要有缺陷（弱点）评估能力

数据泄漏、数据篡改、数据违规使用

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

要求敏感数据使用需要留痕

第六章 法律责任

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

数据安全治理和保护体系建设思路

全知科技 QUAN ZHI TECH

①数据安全咨询服务

- 数据安全整体规划
- 数据安全战略
- 数据安全方针
- 安全治理规划

②数据安全体系建设规划

管理

- 数据安全评估
- 数据安全管理体系设计
- 数据安全架构建设

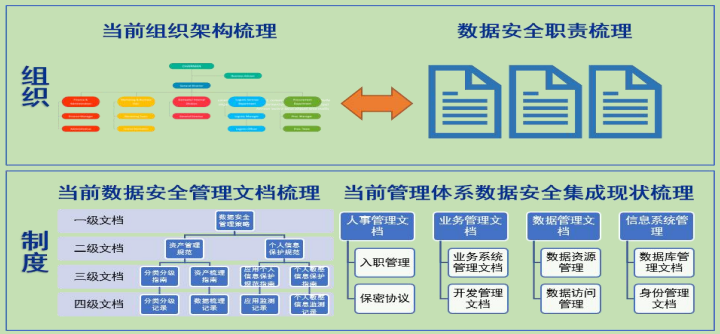
技术

- 数据安全治理工具
- 数据安全保护产品

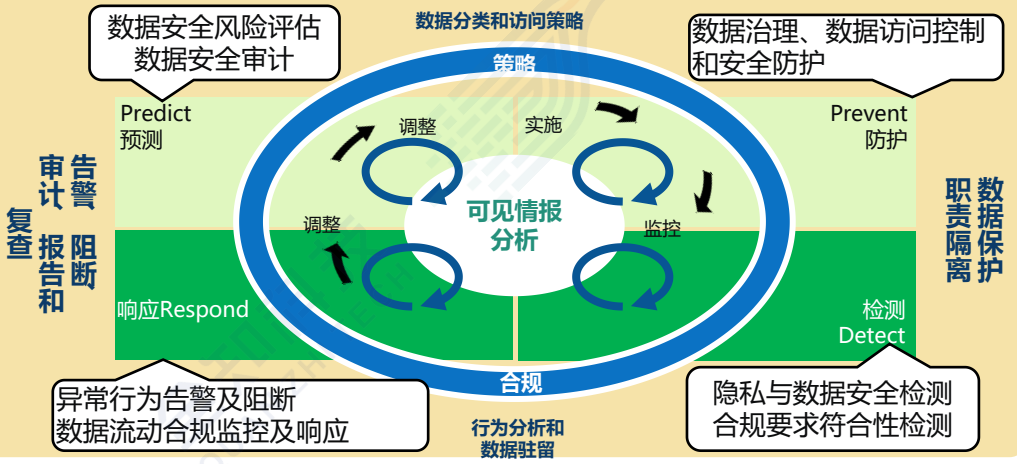
运营

- 数据安全运营保障
- 数据安全评估/改进

③数据安全管理体系建设



④数据安全技术体系建设



⑤数据安全运营体系建设

- 数据安全防护策略
- 日志监测与响应
- 审计与定则
- 数据可用性保障
- 数据安全应急事件响应
- 数据安全评估与改进
- 数据安全培训

数据安全服务框架

全知科技 QUAN ZHI TECH

咨询规划

数据安全规划

- 数据安全方针
- 数据安全战略
- 安全治理规划

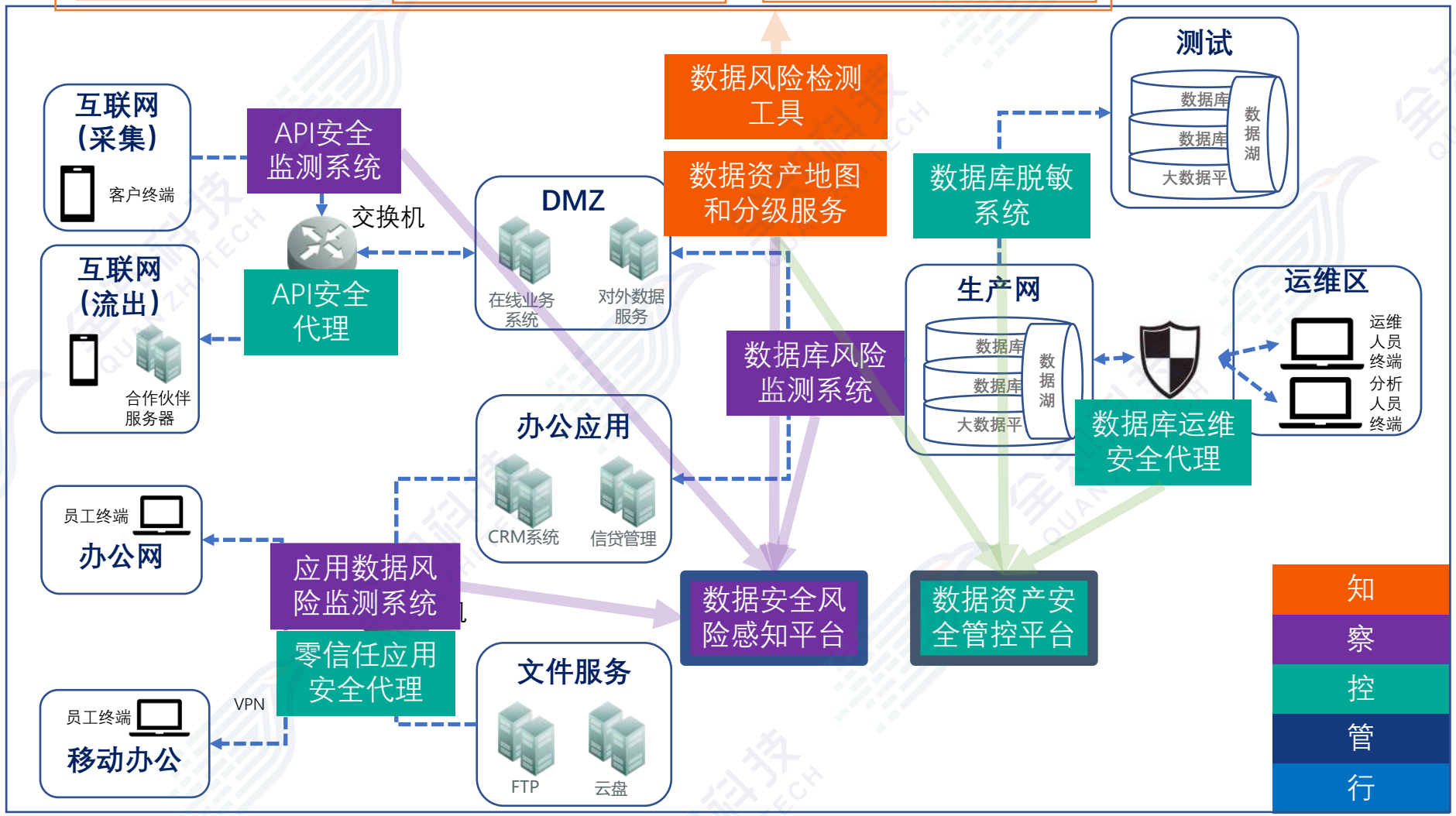
- 组织建设
- 人员能力
- 制度流程
- 技术工具

数据风险测评体系

管理风险评估：组织 | 制度

数据处理活动风险评估：采集 | 存储 | 使用 | 共享 | 开放 | 开发

专项风险评估：App隐私合规 | 个人信息保护 | 数据出境



数据安全运营体系

- 数据分类分级运营
- 数据风险评估运营
- 数据风险监测运营
- 隐私合规风险运营
- 数据泄漏应急运营
- 数据安全管理运营

数据安全服务实施过程

基于数据与风险视角，结合企业现状，通过现状调研、分类分级、差距比对、管理评估和技术测评等方式，绘制企业数据安全全景图，梳理企业数据安全能力图谱，构建企业数据安全建设路线规划。

	3.1 需求范围分析	3.2 数据分类分级	3.3 差距和风险评估	3.4 数据安全体系建制	技术体系完善	评估指标建立
项目组人员	· 组建项目团队 · 召开项目启动会议 · 前期意识培训	· 组织数据资产的调研和梳理 · 自动化工具部署及应用 · 制定数据分类分级标准	· 组织完成管理、技术现状的访谈和调研 · 识别合规差距 · 数据安全风险监测工具的部署及应用 · 编写调查资料、汇总风险发现	· 完成数据安全管理体系整体设计 · 根据差距和风险评估结果，制定具体改进课题 · 提供行业优秀实践参考 · 编制具体制度文件和规范，深化课题实施 · 提供制定和规范的实施培训	· 识别现有安全技术的风险防护效果 · 结合差距和风险评估、管理制度要求，形成安全技术系统框架和实施指引	· 管理要求和数据安全规划目标，制定能力评估指标 · 协调、组织，确保执行后能力评估指标有效性
各部门负责人 安全负责人	· 分配项目资源 · 安排项目培训	· 组织协调本部门梳理数据资产 · 明确各类各级数据的安全管理要求	· 组织协调本部门核心人员参与调研和评估 · 配合数据安全风险监测工具的实施和运营活动，从业务视角协助风险发现	· 组织协调本部门、本安全领域人员参与体系细化改进，参与各级文档的编制和讨论 · 评审体系改进方案	· 组织识别主要数据应用场景，提供现有安全防护能力 · 提供技术实施规划和方向建议	· 组织收集数据安全能力评估指标在管理、技术、人员等层面的要求
技术骨干 安全执行人员	· 参加培训	· 组织和收集数据资产 · 积极配合数据资产分类分级制度落地	· 积极配合风险评估和现状调研 · 组织和收集现状材料	· 参与体系细化改进讨论 · 配合完成体系改进具体执行方案	· 参与现有安全技术风险防护效果分析	· 参与数据安全能力评估指标制定，提供执行意见
知识转移	· 数据安全规范对标 • 项目目标	· 数据资产梳理指导	· 数据安全风险评估培训 · 风险处置意见指导	· 数据安全管理系统贯标培训	· 数据安全技术培训	· 安全指标运营指导
	对齐目标	摸清家底	发现差距和风险	细化数据安全管理要求	技术能力落地	明确考核机制

数据安全服务清单

全知科技 QUAN ZHI TECH

24+套管理&技术服务方案，全面保障各场景下数据安全

服务交付物			
风险评估&分析服务	**数据分级实施服务**	**制度体系建设服务**	**技术体系建设服务**
数据安全现状调研报告	数据分类分级标准和管理细则	数据安全规划报告	数据安全技术体系概要设计方案
数据安全差距分析报告	数据资产盘点和分类分级结果	数据安全能力图谱	数据安全技术体系概要实施方案
数据安全风险库	数据分类分级清单	数据安全建设路线图	护网及API接口管理技术方案
风险应对措施或缓释措施建议	敏感数据分布报告	数据安全监督管理与机制	内部人员数据管理技术方案
重要风险场景数据安全管控机制	敏感数据操作视图	数据安全管理办法、制度、规范	外部数据交易管理技术方案
数据安全风险评估报告	数据资产清单	数据安全风险防控与措施	敏感数据脱敏技术方案
…	…	…	…

管理制度合规提升

全知科技 QUAN ZHI TECH

数据安全管理制度架构表

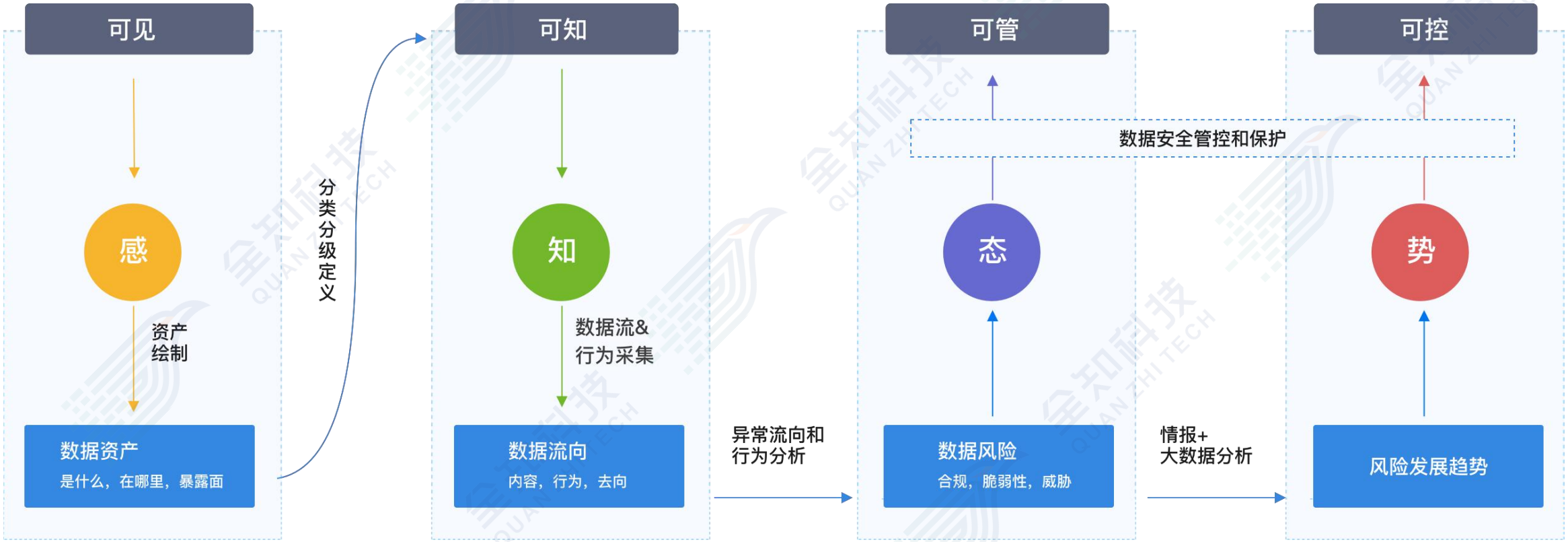
序号		管理领域	文件级别	文件编号	文件名称	管理范围	备注
1	策略和风险管理	安全策略	一级		数据安全管理策略	数据安全整体管理策略，数据安全管理体系的规划、建设、运行和改进	
2			二级		数据安全管理办法	数据安全管理框架，管理领域划分，各管理领域的基本要求	必要
			二级		数据安全组织管理办法	明确数据安全归口管理组织和职责，规范各专业的分工和协作机制等工作	必要
3		数据安全风险管理	二级		数据安全风险评估管理办法	明确评估的基本概念、要素关系、分析原理、评估方法、实施流程、实施要点和工作形式等要素	数安法要求
4		数据资产管理	二级		数据资产安全管理办法	定义数资产的管理的原则，资产的责任部门、资产生命周期	必要
5			二级		数据安全接口管理办法	定义接口的类型与安全级别，接口的生命周期管理过程。及安全设计原则等。	必要
6			三级		数据分类分级管理办法	定义组织范围内的数据分类分级标准，给出数据分类分级的基本原则、维度、方法、示例等	数安法要求
7		数据采集安全管理	二级		数据采集安全管理办法	规范数据采集格式、数据标签、数据审查校验等方面相关安全要求 –数据采集规则:采集目的、采集 –数据采集溯源：采集源识别和 制、采集源安全管理要求等内容 –采集岗位职责:负责采集相关工 –数据采集评估:风险评估方法、 要求等 –采集过程保护:防护数据类型、 合规性说明:相关法律法规和监 ……	
8		数据传输安全管理	二级		数据传输安全管理办法	规范数据传输过程中可以标准化 他安全相关安全要求 –加密传输的数据范围 –传输数据的加密 –加密技术要求及介绍 –调用接口加密机监控 可用性及性能要求（可选）	
9			三级		数据跨境安全管理规范	规范涉及数据跨境传输的安全要	
						规范存储平台安全机制、数据安全防护技术等相关安全要求 –存储介质定义	

数据安全管理制度架构表

序号		管理领域	文件级别	文件编号	文件名称	管理范围	备注
17		数据删除和销毁	二级		数据删除和销毁安全管理办法	–存储介质 –数据库和容器 –审批和审计	DSMM
18	数据应用安全	数据应用安全	二级		云计算数据安全管理规范	主要包括客户数据保护、云服务业务数据安全、云上资产管理	
19			三级		终端办公安全管理规范	主要包括组织内部业务终端、瘦客户机、计算机终端等设备使用过程中的数据安全	必要
20					大数据安全管理规范	主要包括客户数据保护、云服务业务数据安全、云上资产管理	
21		个人信息安全	二级		个人信息数据安全管理办法	针对个人信息在数据生命周期内的安全管理要求	个保法二审稿要求
22	数据安全保障	供应商数据安全管理	二级		供应商数据安全管理办法	供应商数据安全管理的要求和技术防护	
		合作商及人员数据安全管理	二级		合作商及人员数据安全管理	合作商及人员的数据安全管理的要求和技术防护	必要
23		数据安全事件管理	二级		数据安全事件管理办法	数据安全事件的申告、取证、处置和报告要求	数安法要求
24		连续性管理	三级		数据安全应急预案	应急响应与灾难备份标准用于规范数据安全事件的应急响应管理、处置措施，规范灾难备份及恢复工作的目标和原则、技术要求以及实施方法	数安法要求
25		数据安全检查评估	三级		数据安全监测规范	明确数据安全监测预警与处置系统及其技术要求	数安法要求
			三级		数据安全运营规范	明确数据安全运营中工作及指标等要求规范	必要
26			三级		数据安全检查规范	明确日常运营中的数据安全检查要求	
27			三级		数据安全审计规范	明确数据安全审计的周期、审计方式、审计流程等	数安法要求

数据流动安全监测方法论

全知科技 QUAN ZHI TECH



察 – 数据流动风险监测

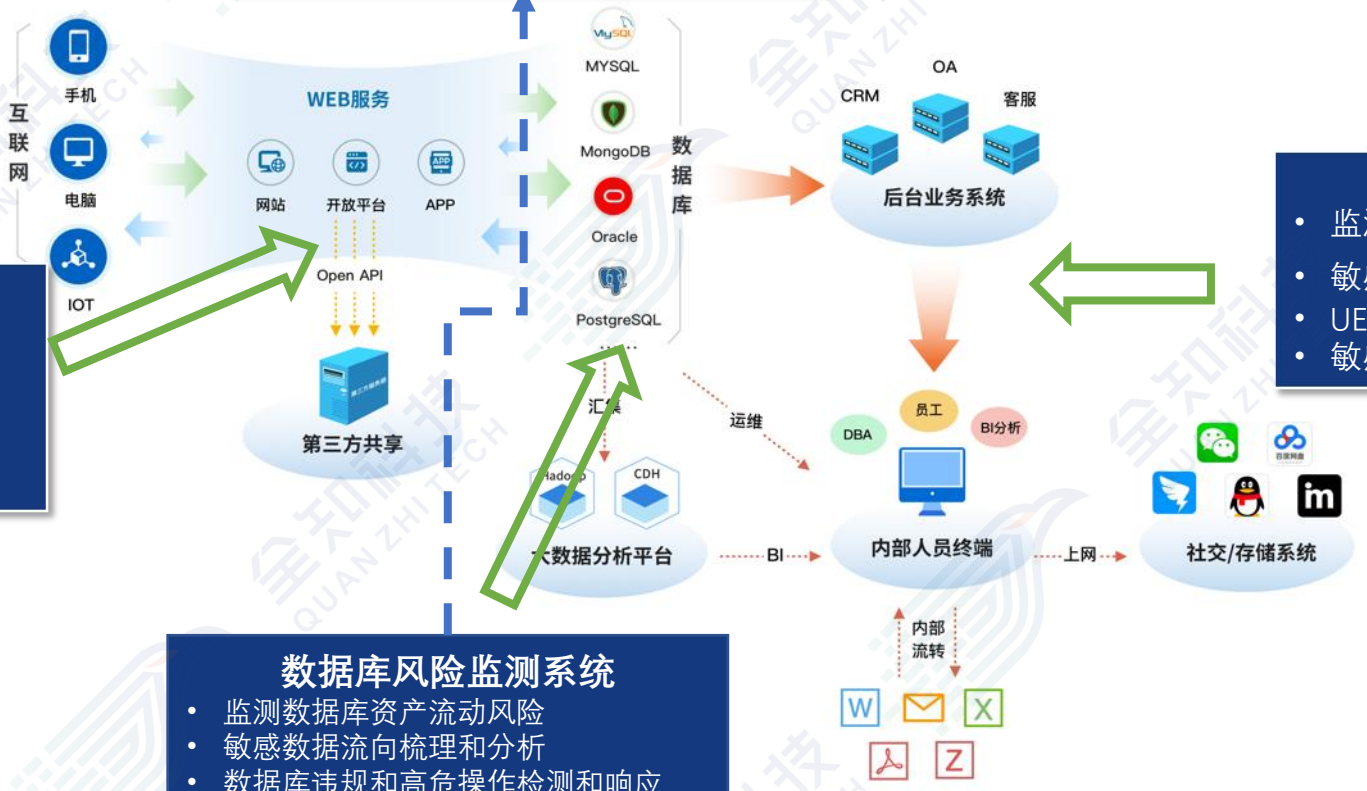
数据流动风险监测体系**以单点数据安全风险监测能力建设为基础**，如应用数据风险监测、API数据风险监测、数据库风险监测等，并逐步建立起来一套**以数据为中心的风险态势感知体系**，用于数据安全宏观趋势研判和决策

数据资产地图系统

- 支撑数据资产发现和高效的数据分类分级
- 数据服务发现和资产扫描
- 多元化数据分类分级模版
- 算法驱动的数据分类分级策略

数据安全风险感知平台

- 汇聚单点数据安全产品的能力
- 数据安全治理驾驶舱
- 数据安全风险运营中心



API数据风险监测系统

- 监测互联网API暴露面数据风险
- 数据暴露面梳理
- 数据API弱点检测
- 数据攻击检测和响应

应用数据风险监测系统

- 监测办公应用场景的数据流动风险
- 敏感数据和文件流动分析
- UEBA
- 敏感数据流动溯源分析

数据库风险监测系统

- 监测数据库资产流动风险
- 敏感数据流向梳理和分析
- 数据库违规和高危操作检测和响应

知源 - 数据资产地图系统

全知科技 QUAN ZHI TECH

产品简介

“数据资产地图系统”是一款面向企业数据发掘并进行自动化数据分类分析的产品。系统致力于梳理并标识数据，实现在复杂环境下自动化扫描并识别其中的敏感业务信息，通过数据的分类分级梳理过程中搭建数据标准，实现数据口径的统一。

数据服务发现

- 优质且智能化的数据服务扫描能力可将企业繁琐且巨量的数据服务发现并扫描。

敏感数据的自动化识别

- 通过敏感数据自动化识别能力，可对海量的数据资产自动化分类分级，实现了在基础零业务打扰的情况下，在扫描的同时完成对数据资产的自动化标识。

智能分析引擎

- 智能分析引擎以多维度的规则匹配与机器学习能力深度学习企业的数据资产业务场景，形成一套贴合客户实际业务场景的算法模型，使自动化分类分级更精准。

分类分级可视化

- 完系统将分类分级结果以多个维度进行可视化呈现，提供了以数据清单维度的分级结果、标签分类维度的分级结果、数据分级维度的识别结果。

知形 - 应用数据风险监测系统

全知科技 QUAN ZHI TECH

产品简介

“应用数据风险监测系统”是一款将企业业务应用系统中的人、数据和风险进行闭环链接的产品。自动化梳理用户与访问数据的关系，实时监控发现用户访问数据的风险，并当数据发生泄露时及时进行事件泄露溯源。全时态数据守护，让敏感数据流动全留痕。

梳理用户数据关系

- 自动识别用户账号，自动关联产出账号-人员-组织架构的关系。
- 识别用户获取数据的行为特征以及获取的数据量。
- 产出可视化用户获取数据的关系图谱。

实时行为风险发现

- 实时风险检查策略对用户行为进行实时检查，识别类型包括：管理合规类、数据拉取类、异常特征类，三大类28小类风险场景，可帮助客户自动识别行为风险。

数据泄露溯源

- 业务访问行为全留档，针对泄露场景，提供数据泄露人员定位，泄露面影响评估，泄露源系统发现。

知影 – API风险监测系统

全知科技 QUAN ZHI TECH

产品简介

“API风险监测系统” 核心以数据为中心，通过对Web、APP、小程序、IoT等应用系统的流量分析，从而实现API数据暴露面的治理和对数据攻击行为持续发现。部署在企业互联网出口，实时监控企业API的数据暴露面以及被攻击情况。

发现全量API

- 在复杂多变的系统环境中自动发现公开的、私有的、面向合作伙伴的所有API并识别敏感数据暴露面，建立API清单，对API进行分类分级。避免安全管理盲区，降低API的数据泄露和合规风险。

弱点发现-API安全隐患检测

- 根据API的原始请求和返回发现识别API弱点并提供相应整改意见，及时修复降低API弱点被利用的风险。完整覆盖owasp检测。

风险发现

- 内置大量基于上下文的数据攻击风险规则，帮助用户发现有价值的数据泄露风险，精准定位数据泄露源头。
- 通过无监督学习算法对API接口进行攻击学习，识别API扫描、试探等的攻击风险。

开放数据订阅

- 支持对发现的重要数据同步到第三方平台，可以通过syslog/kafka方式将指定的API资产、弱点或风险等信息同步给客户，助力客户及时发现弱点和攻击的变动情况，推动进行统一安全运营。

知踪 - 数据库风险监测系统

产品简介

“数据库风险监测系统”是一款实时监控并记录针对目标数据库系统各类操作的流量分析系统。多维度处理分析操作行为与敏感数据流动监控，精准预警风险，对数据库进行动态保护。

数据生命周期全管理

- 针对元数据和敏感数据，分期其产生、使用、修改、消亡等生命周期情况。有助于帮助用户理解数据的完整态势。

数据流动态势全掌握

- 数据流动态势分别从全数据维度和敏感数据维度，刻画数据流动态势，包含使用者，使用量，TOP使用者占比。清晰刻画出这几者之间的使用趋势，并实时的展示每个数据库的被访问情况以及受攻击情况。

数据挖掘全发现

- 针对数据的深度挖掘基本靠数据挖掘模块来实现，通过数据挖掘模块可以创建新的分析任务，并执行任务，最终获得分析结果。分析任务类型有用户画像分析、元数据溯源、数据溯源。

合规报表全统计

- 根据等保、SOX、PCI-DSS、GBDR等国家及行业法案制定安全报表且开放数据订阅。根据用户提交的报表调度任务，生成用户所需要的报表。报表内容格式有报表模板来定义。报表内容范围和时间范围由用户创建报表任务时指定。

全链路数据流动安全管理平台体系

全知科技 QUAN ZHI TECH

全链路数据流动安全管理平台体系

平台管理

- 告警与订阅
- 报表管理
- 可视化定制
- 用户管理
- 权限管理
- 审计管理

扩展能力

- 流量分发
- 推送安装
- 探针监控
- 自定义接口

数据流动审计与运营

全链路敏感数据留痕溯源分析

- 应用审计溯源
- 大数据平台操作溯源
- 数据库操作溯源
- 第三方数据共享溯源

统一运营

- 资产运营
- 风险运营
- 常态运营
- 风险评估报告

数据流动风险管控

- API安全网关
- 应用数据网关
- 数据运维管控
- 大数据平台管控
- 数据脱敏

数据流动风险监测

- 互联网开放风险监测
- 内部员工风险监测
- 面向运维侧风险监测
- 大数据平台风险监测
- 数据外发风险监测

数据流动风险评估

应用服务弱点评估

- 数据权限风险
- 数据暴露面
- 异常数据流向
- 高危数据行为

大数据/数据库风险评估

- 大数据/数据库脆弱性
- 大数据/数据库基线核查
- CVE漏洞
- 账户弱口令

数据合规评估

- 数据采集合规
- 数据存储和删除合规
- 数据使用利用合规
- 数据共享合规
- 数据出境合规
- 数据主体权利知情、响应合规

数据流动刻画

- 数据权限关系
- 数据暴露面
- 数据映射关联可视
- 数据流向

数据资产底账梳理

应用服务资产台账梳理

- 应用API清单
- 文件、邮件清单
- 双向敏感数据识别
- 数据分类分级

敏感数据分类分级

- 敏感数据规则
- 数据分类分级
- 敏感数据打标
- 数据清单开放

数据库资产梳理

- 数据库资产清单
- 数据表
- 数据字段
- 数据库访问情况

全知科技
QUAN ZHI TECH

成功案例介绍

4

客户案例 - 某市信息安全管理中心

本项目为某市电子政务外网监测服务项目主要采用驻场运营监测，系统通过旁路镜像的方式，在电子政务外网所有出口节点部署全知应用数据安全产品，获得所有出口流量进行不间断的流量数据监测，监测设备总带宽确保可满足客户提出的监测要求。

针对政务外网总计部署**5套数据安全监测平台**，分别对**XX区及市政务资源中心政务外网数据流量（约15G）**进行全天候监测分析，并安排专业数据安全风险检测人员，对数据安全监测平台分析出来的风险问题进行分析、测试，监测的数据主要为电子政务外网流量中包含的个人敏感信息。

全知科技提供专业技术人员进行驻场服务，驻场人员跟踪运营监测情况，进行数据风险监测和分析，提供风险预警，为重大风险和事件提供应急响应，针对重大风险提供改进建议，并通过监测验证处置和改进效果。

运营服务中将定期生成数据安全运营监测**周报、月报**，对流量监测的结果进行集中呈现；监测报告可从系统、机构和委办局多维度开展，内容可包括接口梳理、应用梳理、数据安全事件记录、主体画像、风险发现、威胁发现、脆弱性分析、数据暴露面、重大事件处置等。

（一）电子政务应用数据安全风险监测

（二）重点委办局数据安全风险评估

（三）政务类APP个人信息安全影响评估

（四）数据安全培训

（五）数据安全相关地标编制

（六）应急响应支撑

敏感接口梳理	敏感操作审计	数据风险预警	泄露事件响应	威胁特征分析	运营监测报告
采用自动化接口发现技术，将网络流量中大量的URL进行聚合归类，提取参数配置，还原接口的技术设计形式；按照接口资源类型展示各类接口	基于自主研发的日志结构化引擎，自动将网络上流动的敏感数据进行记录。通过应用层账号关联分析技术，从网络流量中还原真实系统的账号并记录。	对数据行为建立基线：包括用户基线、接口基线、系统基线，并利用前沿的异常检测技术，从多个维度来识别异常数据访问行为，对高风险行为进行预警。	通过线索溯源以泄露的数据内容为线索，在系统中进行回溯，将所有访问过泄露内容的记录都提取出来，然后做集中度分析，进而一步步聚焦嫌疑人和泄露路径。	产品自动记录一段时间内所有事件完整的请求内容，当发生诸如业务数据被篡改等违规行为，可依据参数特征进行全流量检索。。	定期（日、月、年）对运营监测情况进行汇总和报告，报告可从系统、机构和委办局等多维度开展，内容覆盖所有监测情况，并可通过汇总和对比，为针对性的处置提供依据。

数据资产监测	通过运营监测获取流量数据后，通过对数据的识别、梳理、分析和统计，形成全流量的数据资产汇总，以丰富的图表形式为用户提供可视化的数据资产的安全监测。

客户案例 - 某市信息安全管理中心

全知科技 QUAN ZHI TECH

数据安全监测工作成果：

自2020年第四季度至2021年第一季度期间，总计检测并验证**183个数据安全风险隐患，其中171个高风险，12个中风险，发送通报数量152份，数据安全风险类型主要为密码数据传输未加密、接口未鉴权、数据伪脱敏等。**

风险类型	风险数量
密码数据传输未加密	43
接口未鉴权	40
敏感数据未脱敏|伪脱敏暴露	29
接口返回密码信息	19
敏感信息可遍历	14
账号无强口令策略	12
接口单次可返回1000条数据	9
账号弱密码	7
登陆认证不合理	4
IP调取数据超5000条	2
敏感数据未脱敏	2
敏感数据内容返回过多	1
敏感数据伪脱敏	1

典型风险

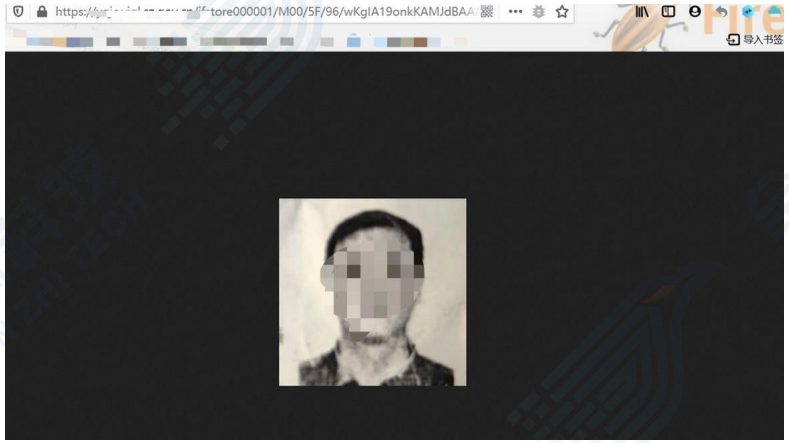
全知科技 QUAN ZHI TECH

事件描述：

某**疫情防控(新冠肺炎)**监测与数据分析平台某接口存在接口未鉴权、单次可返回1000条数据等漏洞，接口缺乏鉴权机制，系统接口无需进行登陆校验，即可访问相应的系统接口；可对请求的pageSize参数进行修改，修改参数后可根据数据库中的数据量返回相应的数据，容易导致**一次性请求超过1000条敏感数据**的行为发生，造成数据一次性可被泄漏条数过多，泄露疫情数据包含姓名、手机号码、身份证号、地址、用户头像等，存在较高安全风险。

接口未鉴权

单次可返回1000条数据



疫情相关漏洞

典型风险

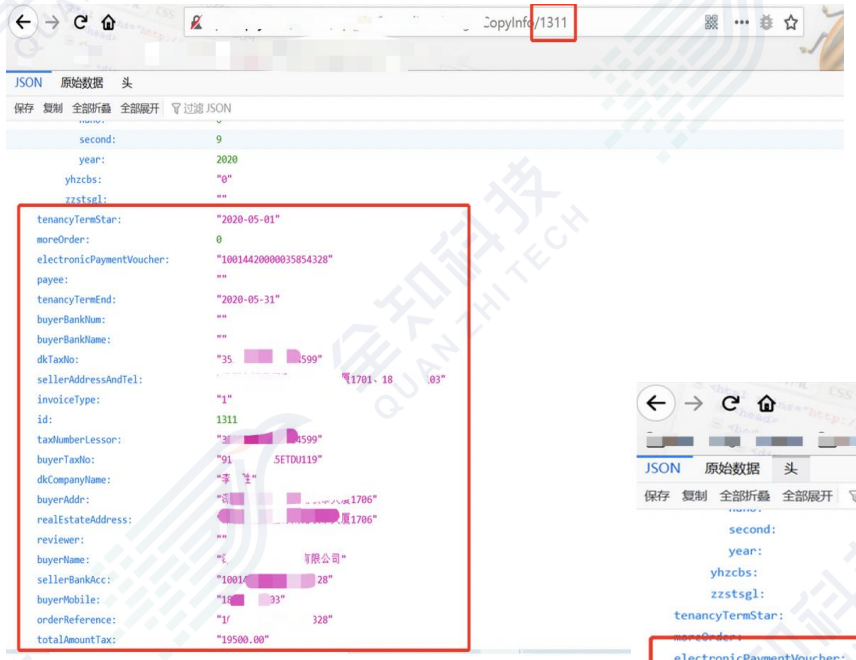
事件描述：

某政数局某服务商的某后台管理系统与某政数局基础信息平台长时间进行数据通信，调取该接口上的**公民敏感信息**，包括**公民姓名、身份证号、地址等**，该服务商的**系统数据库开放在互联网**上，**未做鉴权**，导致数据库被恶意攻击者写入了**后门代码，疑似存在数据安全泄露事件**。此外，在某政数局基础信息平台的某接口中，还发现存在**未鉴权、可遍历**等漏洞，恶意攻击者无需进行登录校验即可遍历访问该接口获取**大量公民敏感信息**。

典型风险

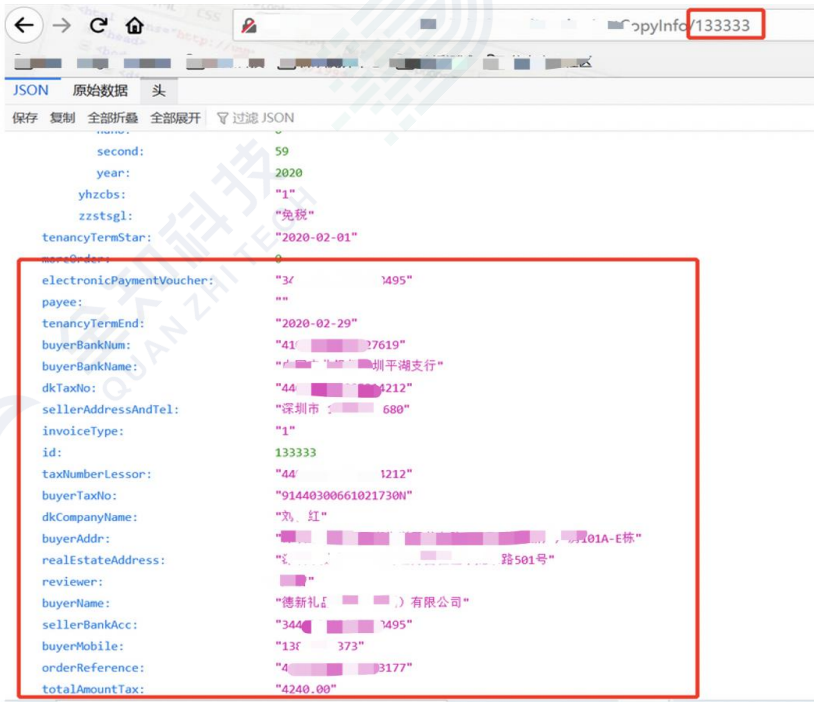
事件描述：

某国资委下属公司个人出租房屋电子发票系统某接口存在**敏感信息可遍历、接口未鉴权**等漏洞。存在漏洞的接口：缺乏鉴权机制，系统接口无需进行登陆校验，即可访问相应的系统接口；且可根据URL传输的数字参数进行遍历，通过遍历可获取系统中**姓名、身份证号、手机号码、银行卡号、地址、电子邮箱等敏感数据**，攻击者或恶意破坏者可通过对这类参数进行遍历操作，从而获取系统中其他人的数据或系统所有的数据，初步估计通过遍历操作可获取**十万条以上的数据，存在较高安全风险。**



接口未鉴权，遍历十万条以上的数据

敏感信息可遍历



典型风险

➢ 接口：

http://XXX.XX.79.175:166XX/api/User/UserLogin

API所属系统：某省全员新冠病毒核酸检测平台

➢ 风险说明：

1）查询接口参数可遍历，可获取大量敏感信息，可以查询账号关联医院内进行核酸检查人员的详细个人信息，包括个人姓名、年龄、性别、证件号、手机号、住址、核酸检测结果等个人敏感信息。

➢ 治理建议：

对于系统中的接口，尤其是敏感接口需要进行梳理和监测管理，避免敏感接口存在的安全漏洞，导致系统中的敏感数据泄露

➢ 验证截图：

敏感数据泄露：核酸筛查人员姓名、年龄、性别、证件号、手机号、住址、核酸检测结果等个人敏感信息

典型风险

➢ 接口：

http://XXX.XXX.100.117/sso/api/v1/login/$(string)

API所属系统：XX农村“三留守”人员信息管理系统

➢ 风险说明：

1）在登录接口的请求中存在弱密码，弱密码可能通过账号暴力破解的方式被破解；
2）可获取三留守人员的个人信息数据；

➢ 治理建议：

需要对用户的密码做规则限制，避免使用易于被他人猜测出的密码，对于已经存在的弱密码，需要及时进行修改。对于未及时修改的密码，需要对登录接口访问进行监控，及时发现帐号被暴力破解登录或帐号登录异常的风险

➢ 验证截图：

帐号：XXXXX000000
密码：111111

Thanks

新一代数据安全引领者

☎ 400-100-9516

杭州·北京·上海·广州·深圳·南京·成都