Preparing the Long Journey for Data Security

Xiaosheng Tan

Xiaosheng Tan

30+ Years experience from Ant-Virus to Cyber Security

Founder and CEO of Beijing Genius Cyber Tech Co.,Ltd（北京赛博英杰科技有限公司）

Founder of ZhengQi cybersecurity training camp（正奇学苑）

Served as Technology President and Chief Security Officer of Qihoo 360

Deputy Secretary General of China Computer Foundation(CCF)

Honored as the 10 best Cybersecurity professionals of China in 2018

Honored as high-end leading figure of Zhongguancun in 2012

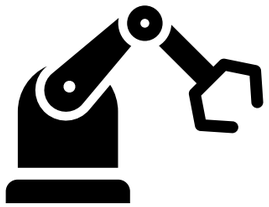
The Government

5 Key Factors of Production

Land

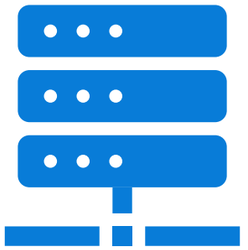
Labor

Capital



Technology

+



Data

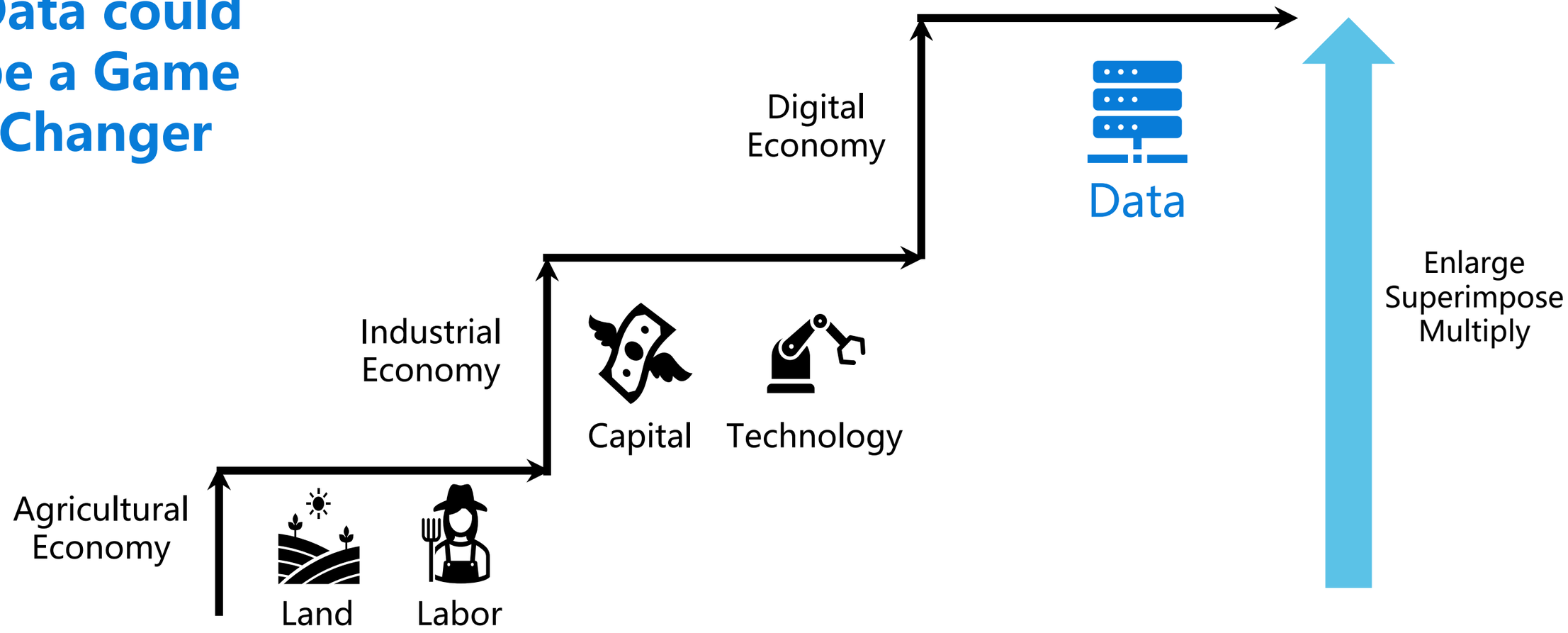
"Opinions of the Central Committee of the Communist Party of China and the State Council on Constructing a More Complete System and Mechanism for the Market-oriented Allocation of Factors" ——March 30th 2020

《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》

http://www.gov.cn/zhengce/2020-04/09/content_5500622.htm

- Promote the open sharing of government data
- Elevate the value of social data resources
- Strengthen the integration and security protection of data resources

Data could be a Game Changer



“Digital Economy, Elevating It to a National Strategy”

“Continue to become stronger, better and bigger our country ‘s digital economy “
----January 15th 2022， Xi Jinping

http://www.gov.cn/xinwen/2022-01/15/content_5668369.htm

The Fifth Plenary Session of the 18th Central Committee of the CCP

Implement the national cyber development strategy. and the national big data strategy

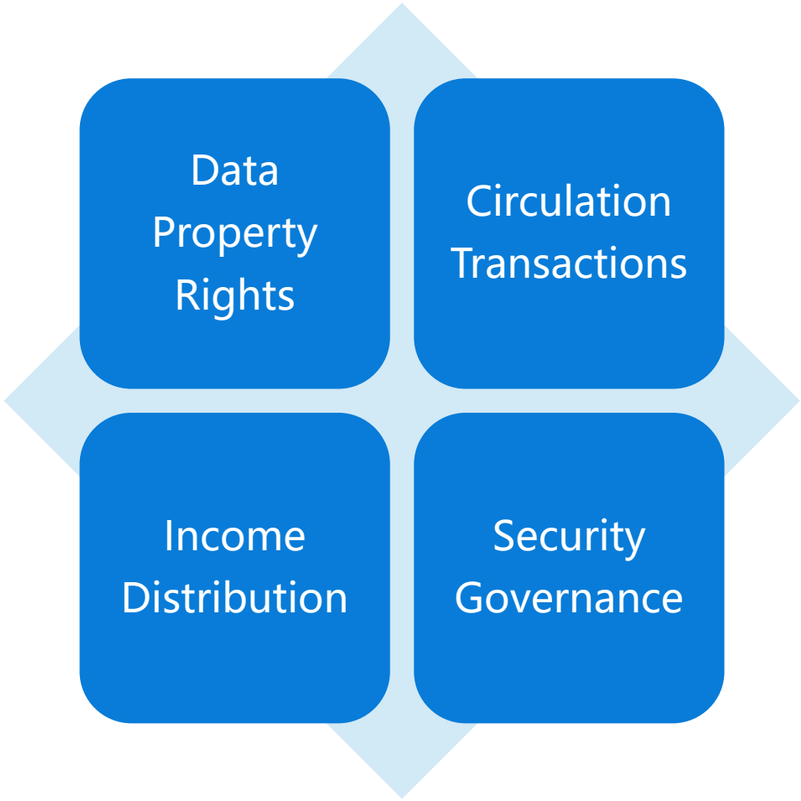
The Fifth Plenary Session of the 19th Central Committee of the CCP

Develop the digital economy, promote digital industrialization and industrial digitization, promote the deep integration of the digital economy and the real economy, and create an internationally competitive digital industrial cluster.

The 20th Central Committee of the CCP

Accelerate the development of the digital economy, promote the deep integration of the digital economy and the real economy, and create an internationally competitive digital industrial cluster”

“Twenty Data Measures”

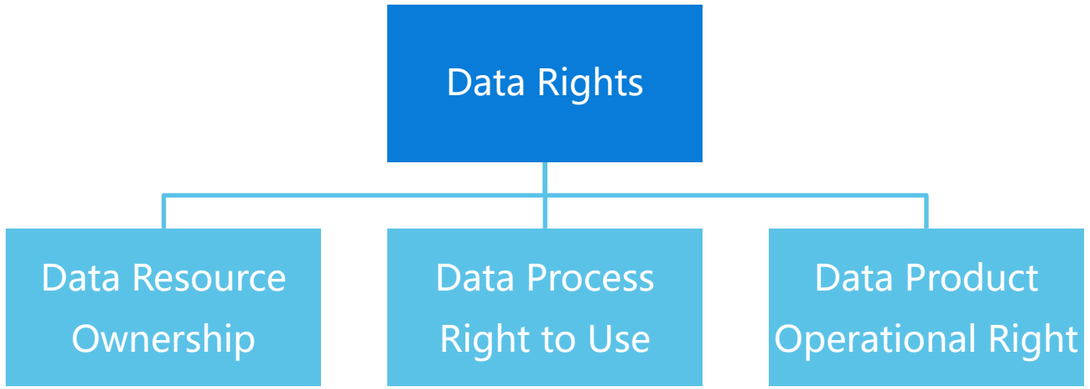


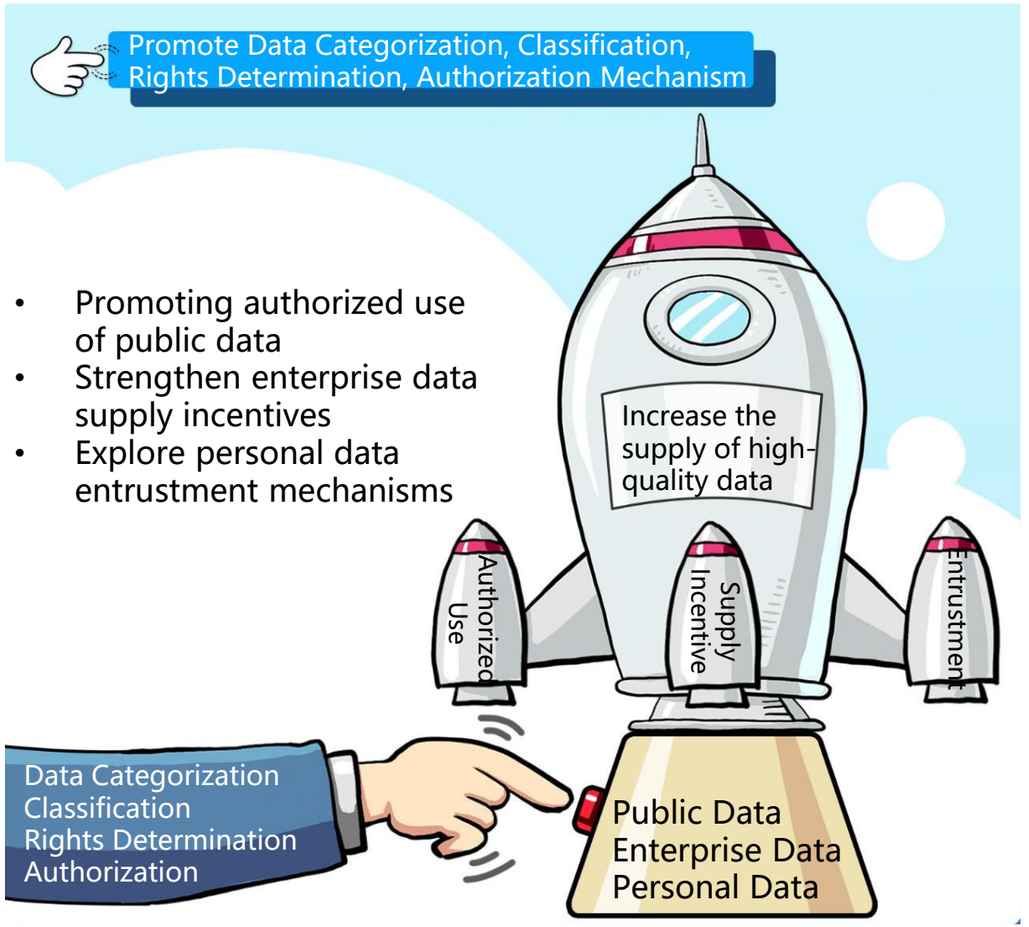
“Opinions on Building Basic Systems for Data to Maximize the Role of Data Elements” (关于构建数据基础制度更好发挥数据要素作用的意见),

----the Central Committee of the Communist Party of China and the State Council，Dec 19th 2022

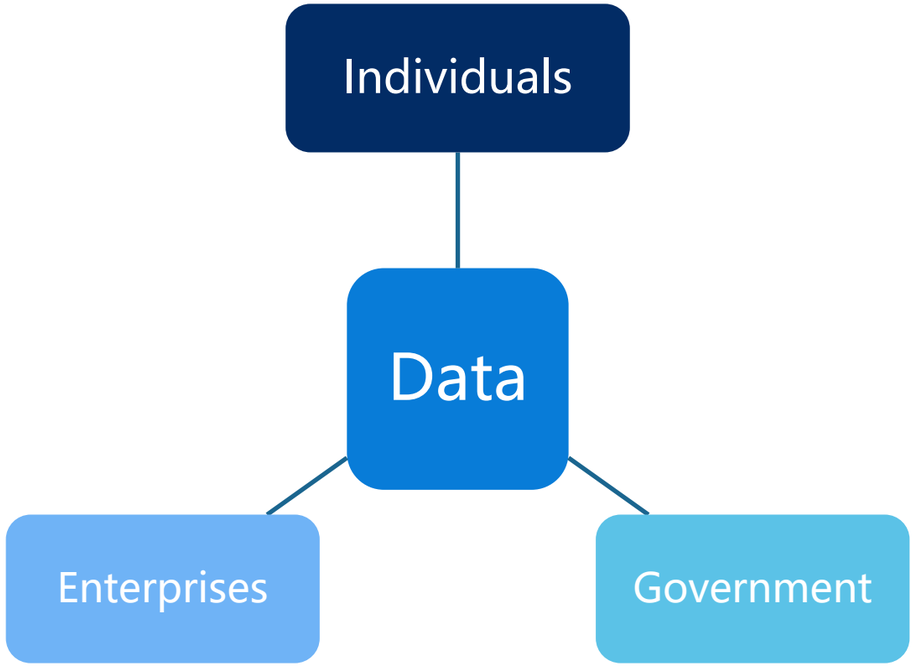
Data Property Rights (3-7)

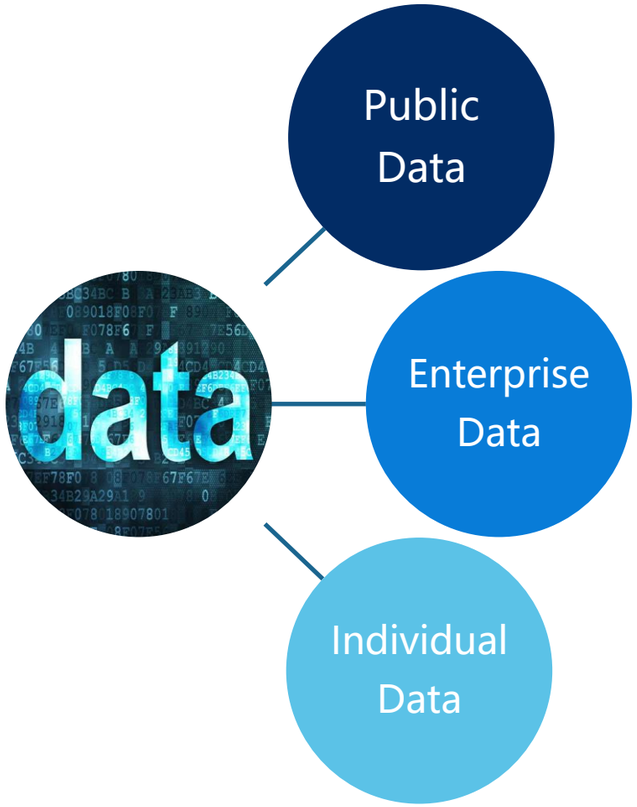
3 Rights Separation

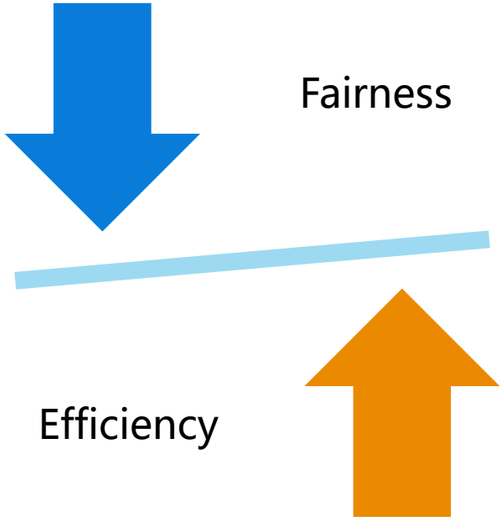




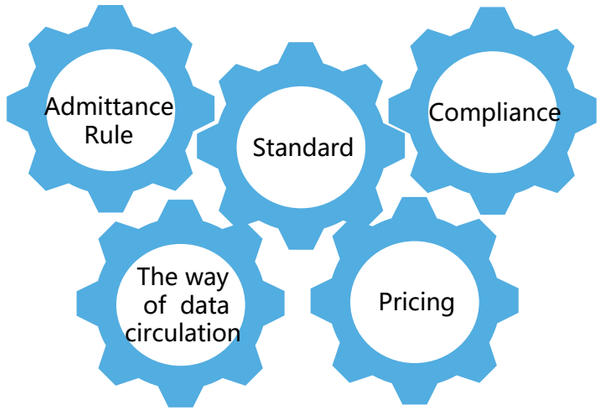
Challenges



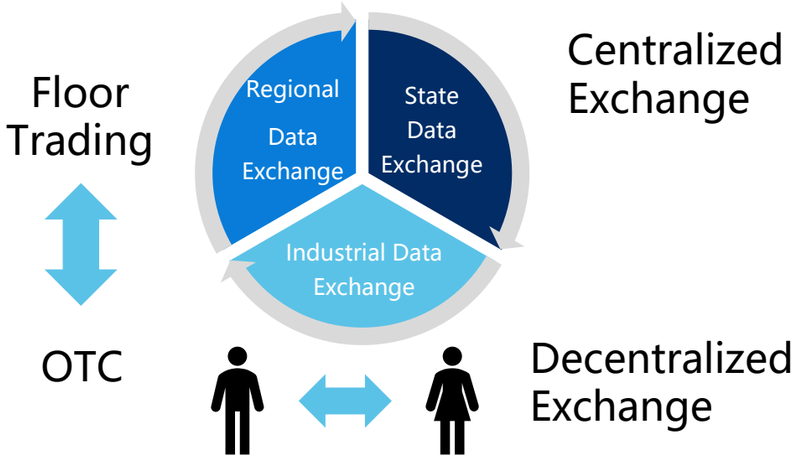




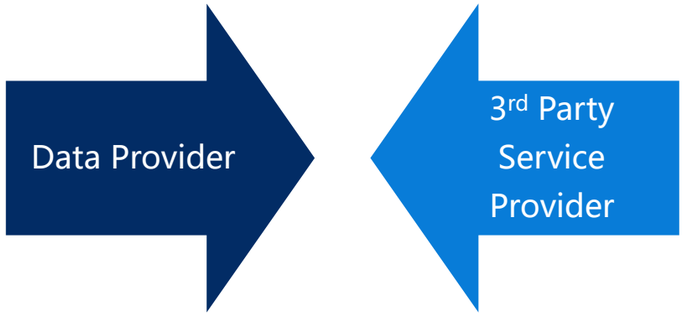
Circulation Transactions（8-11）



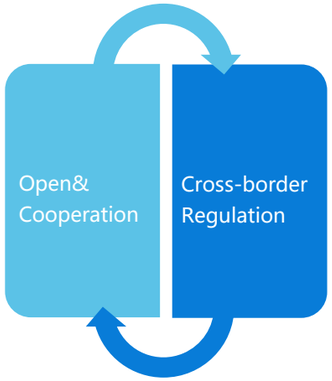
8：Improve the full data process compliance and supervision system



9:Build a standardized and efficient data exchange

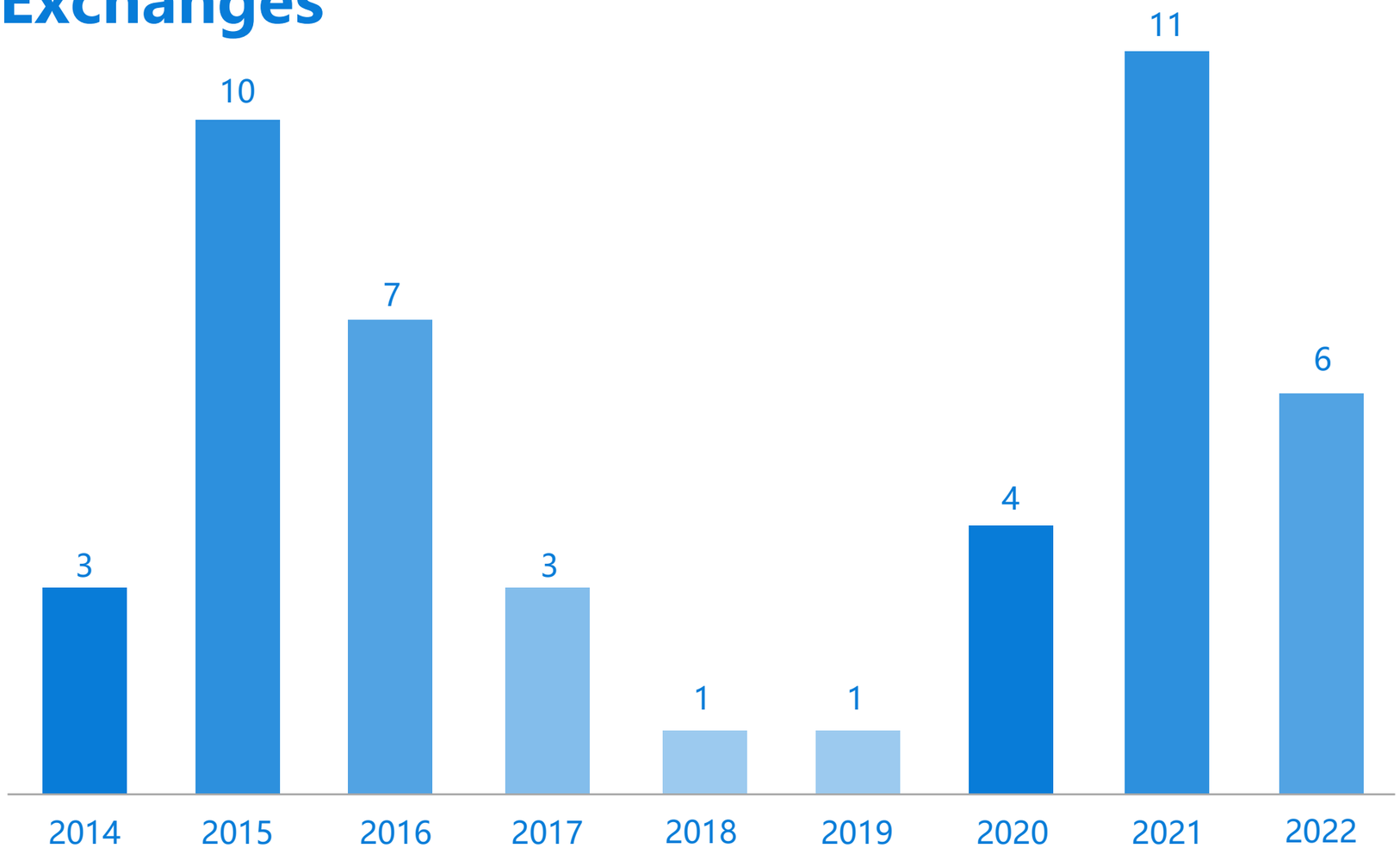


10: Cultivate data transaction circulation and transaction service ecology



11: Build a data security compliance and orderly cross-border flow mechanism

40+Data Exchanges

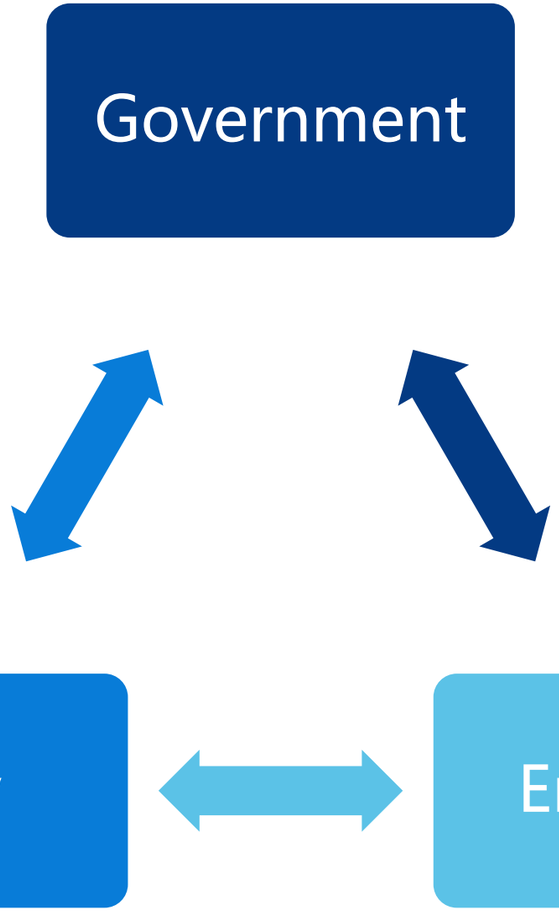


Income Distribution (12-13)

The market evaluates the contribution and determines the reward mechanism according to the contribution. According to the principle of "whoever invests, who contributes, who benefits", promote the data element benefits to be reasonably inclined to the creators of data value and use value

Make better use of the guiding and regulating role of the government in the distribution of income from data elements. Pay more attention to public interests and relatively disadvantaged groups. Improve the overall digital literacy of society, eliminate the digital divide, ensure people's livelihood and well-being, and promote common prosperity

Security Governance (14-16)

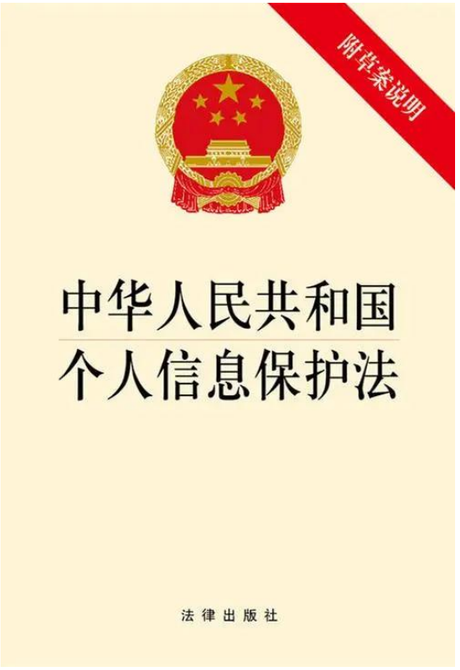


The Laws

Cyber Security Law

Cryptography Law

Data Security Law



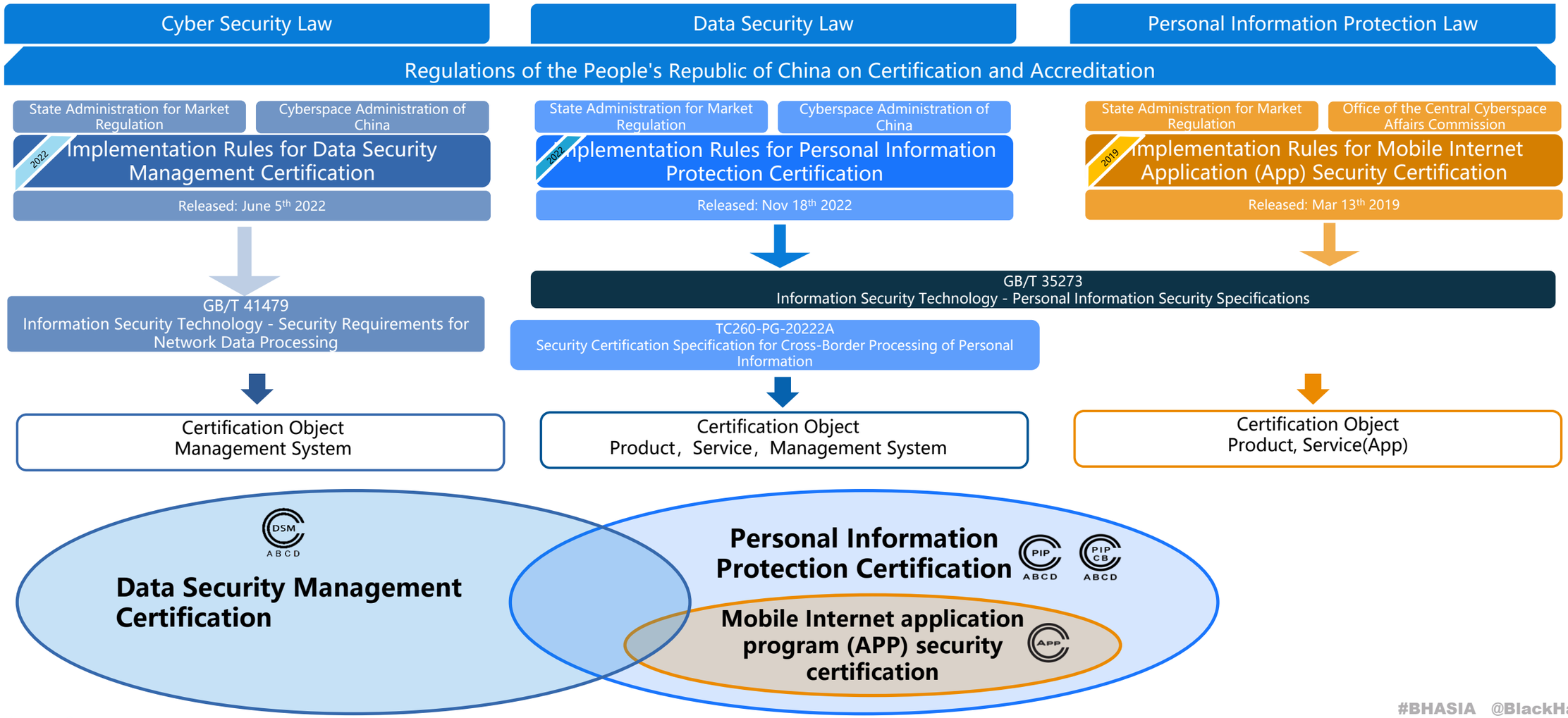
Personal Information Protection Law

4 Laws

4 Regulations of Data Security in China

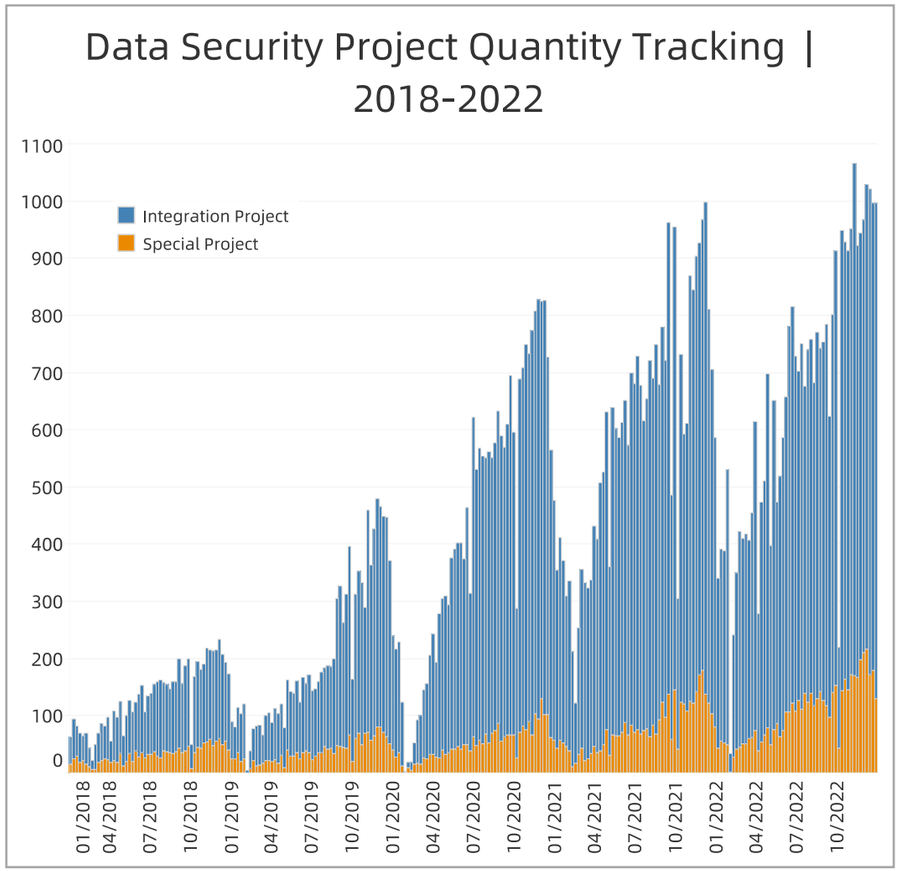
- Regulations on the Classified Protection of Cybersecurity
- Regulation on Protecting the Security of Critical Information Infrastructure
- Regulation on the Administration of Commercial Cipher Codes
- Draft Regulations on the Administration of Network Data Security(For public comments)

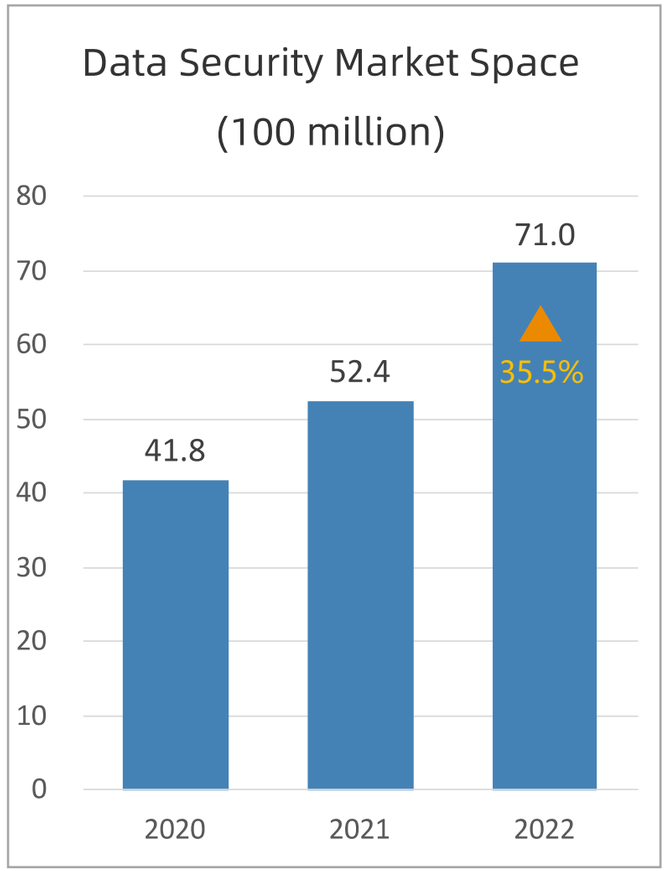
3 Certifications on Data Security in China

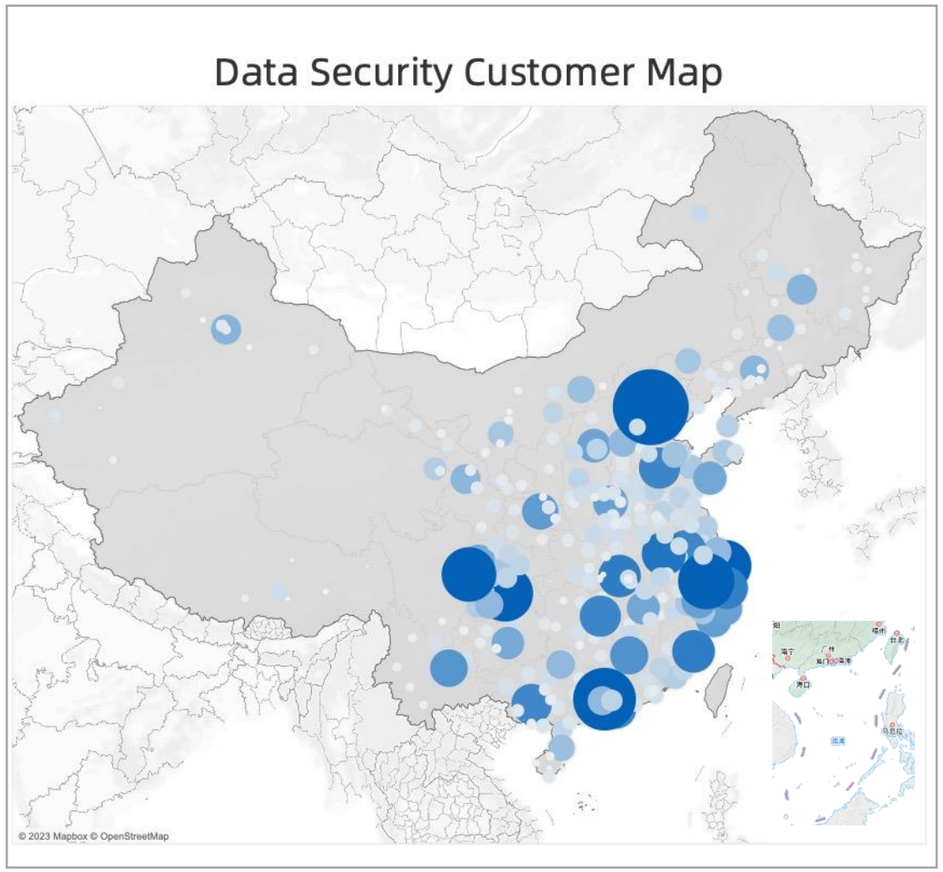


The Market

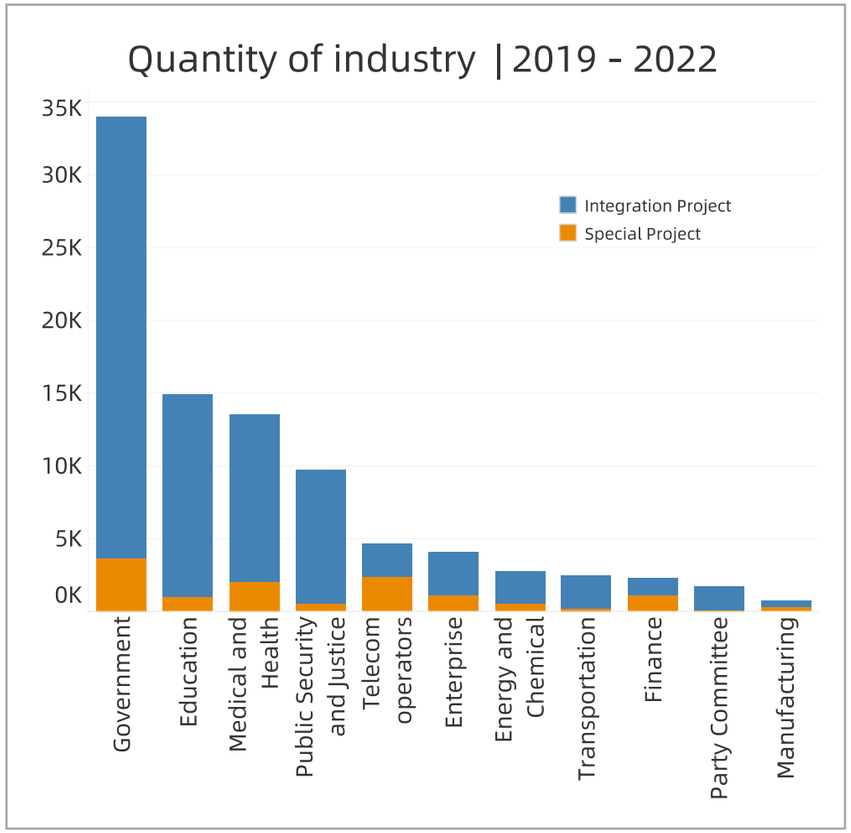
Fast Growing， Unbalanced in Geography

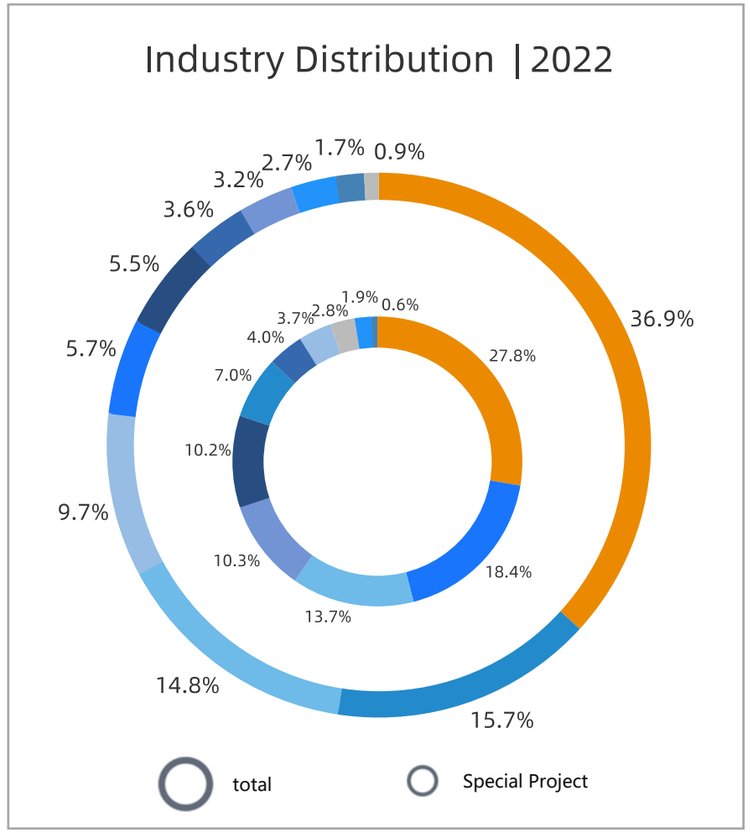


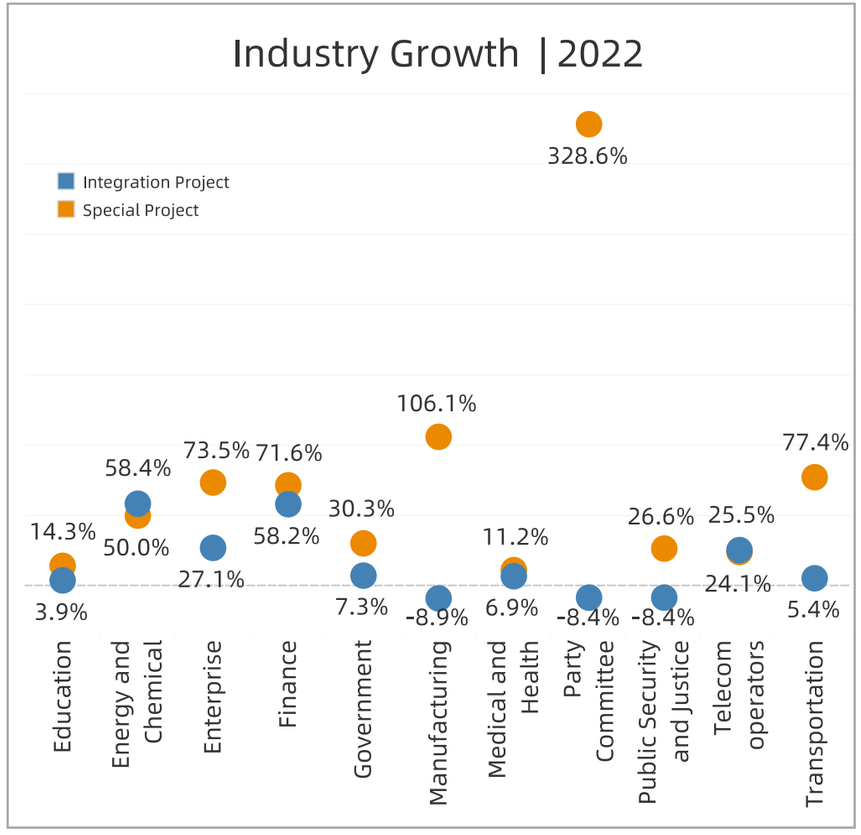




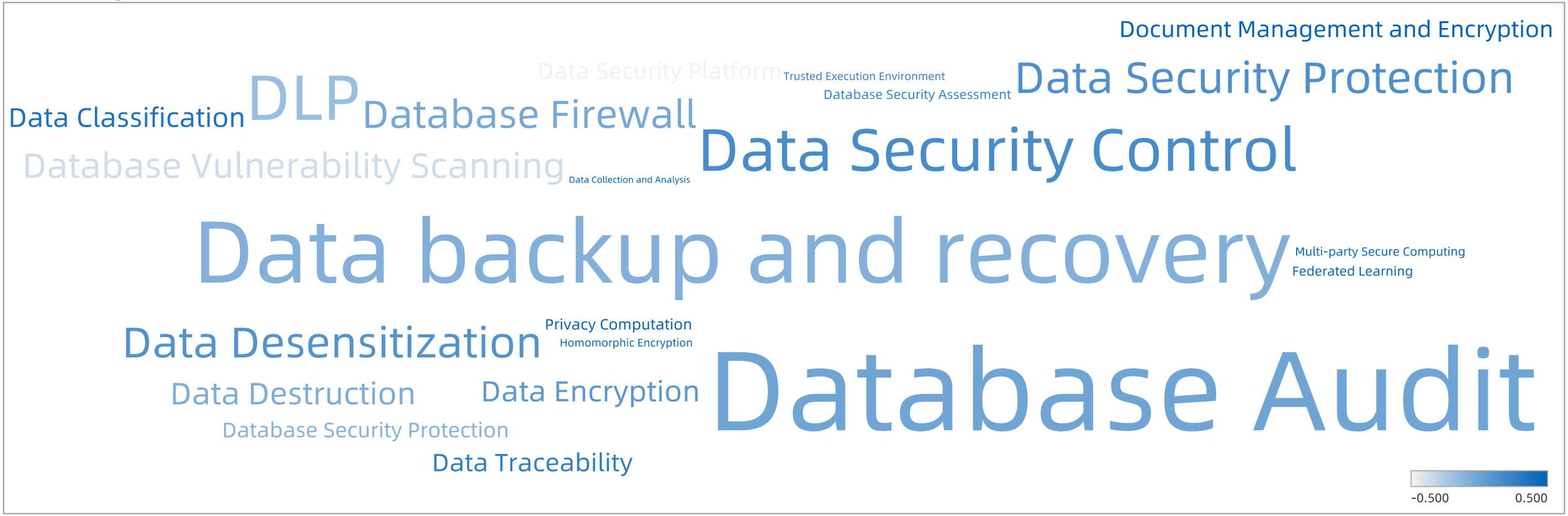
Government, Carriers, Financial sections are the pioneers





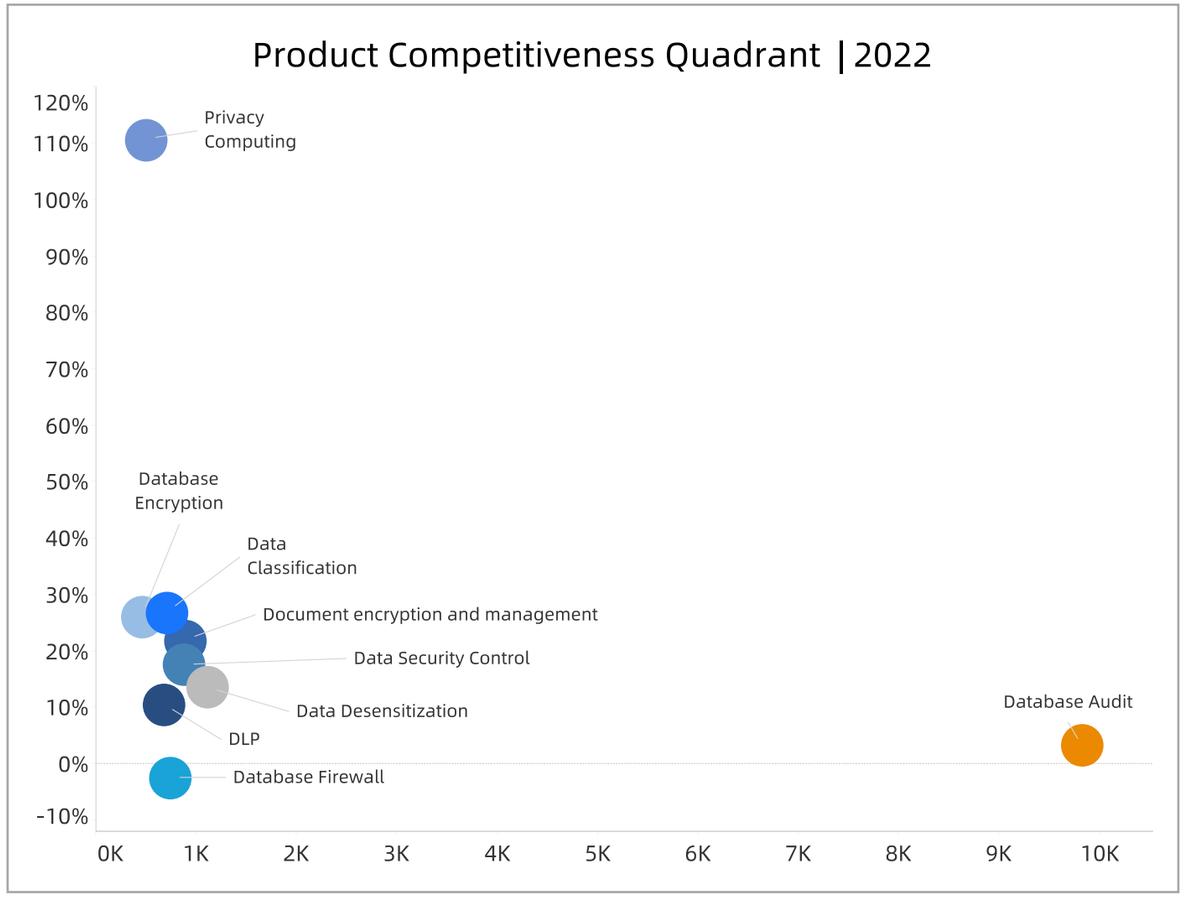


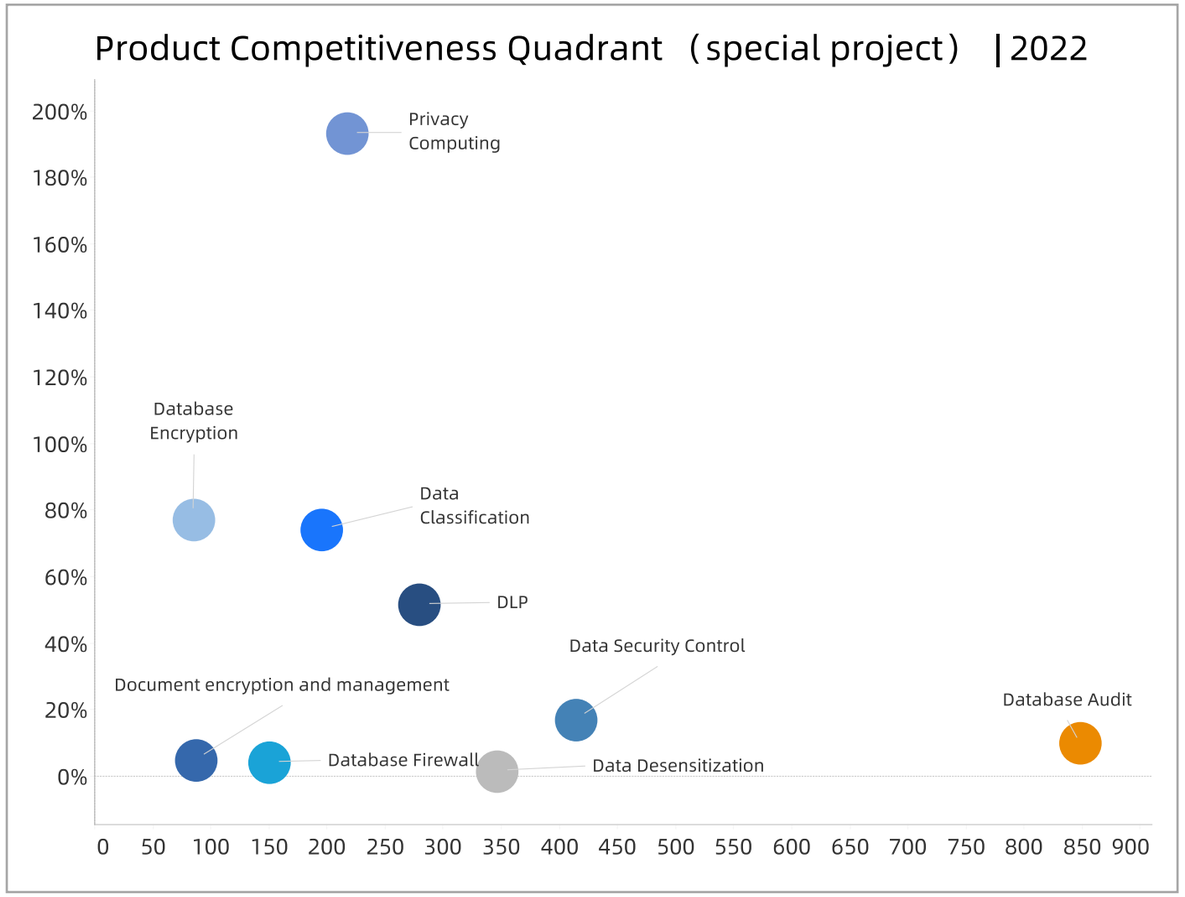
Data Categorization and Classification, Privacy Enhanced Computing and Data Security total solution are hot words in 2022



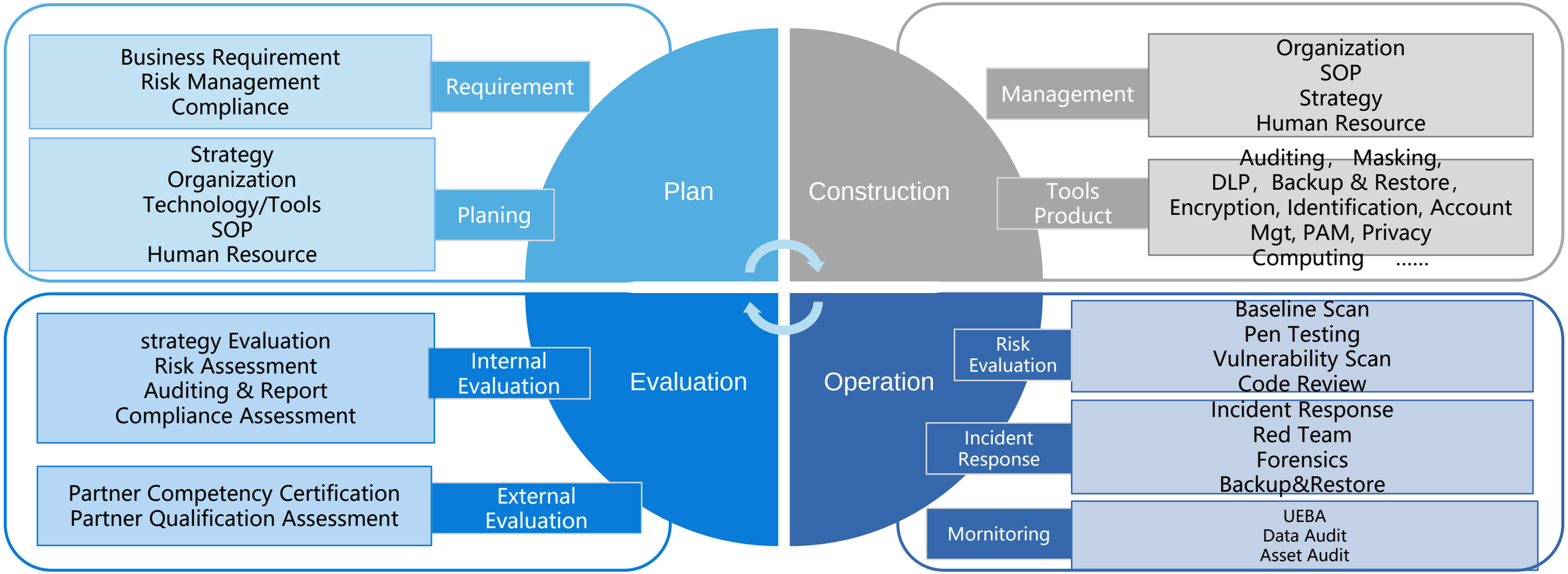
The font size indicates the heat level, and the color depth indicates the high growth rate

Data Security shift from buy products to build systems

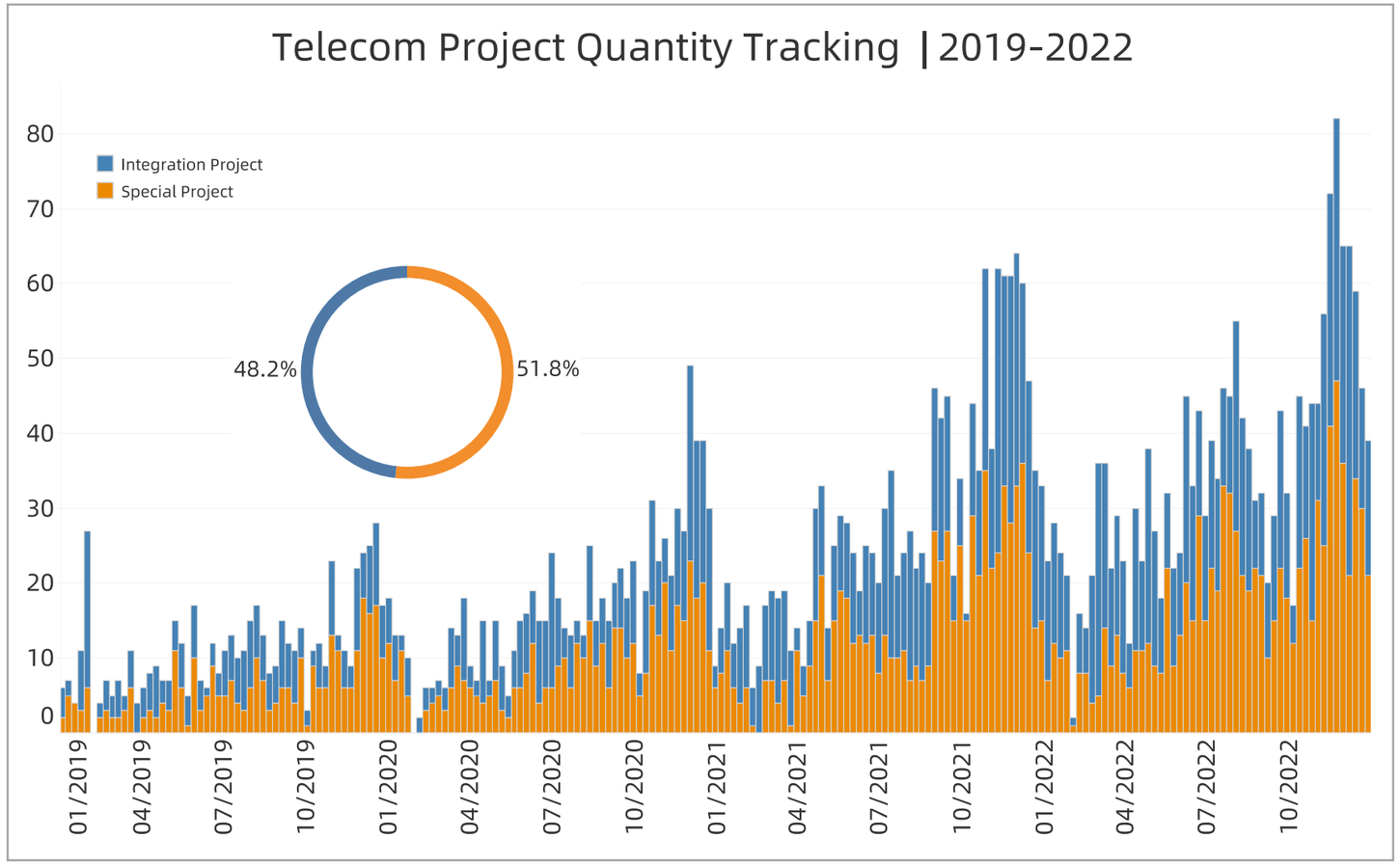


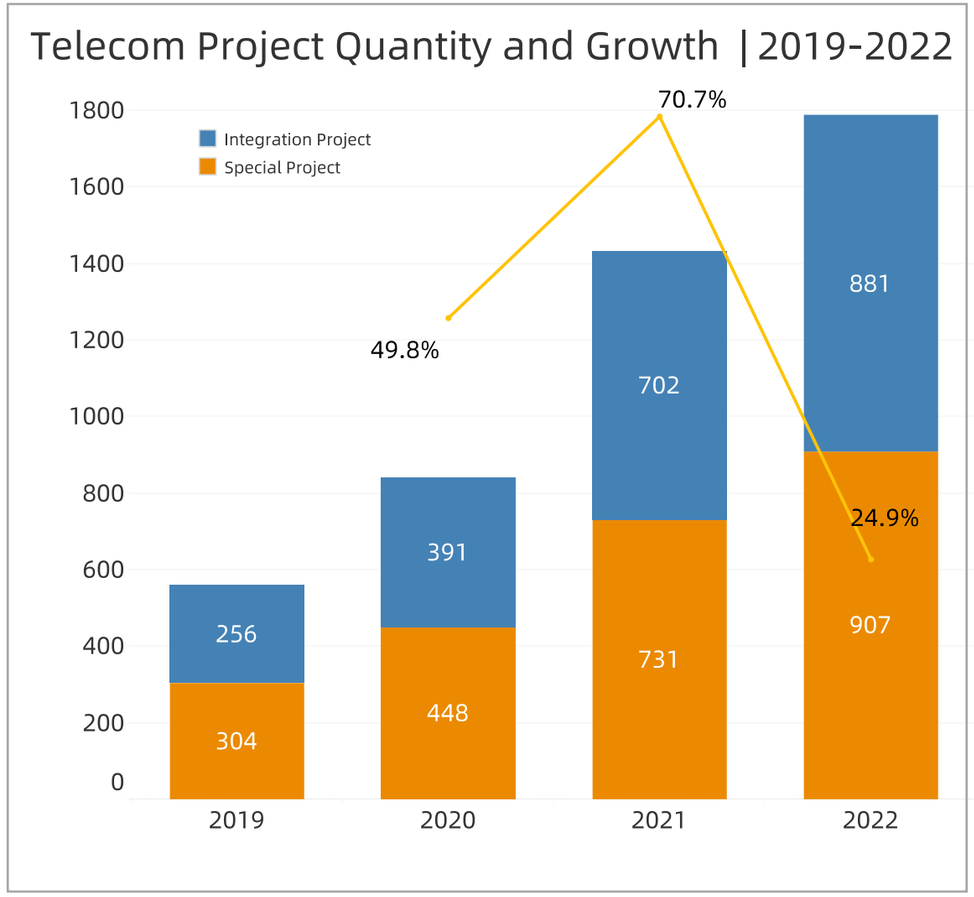


Data Security is still Fragmented

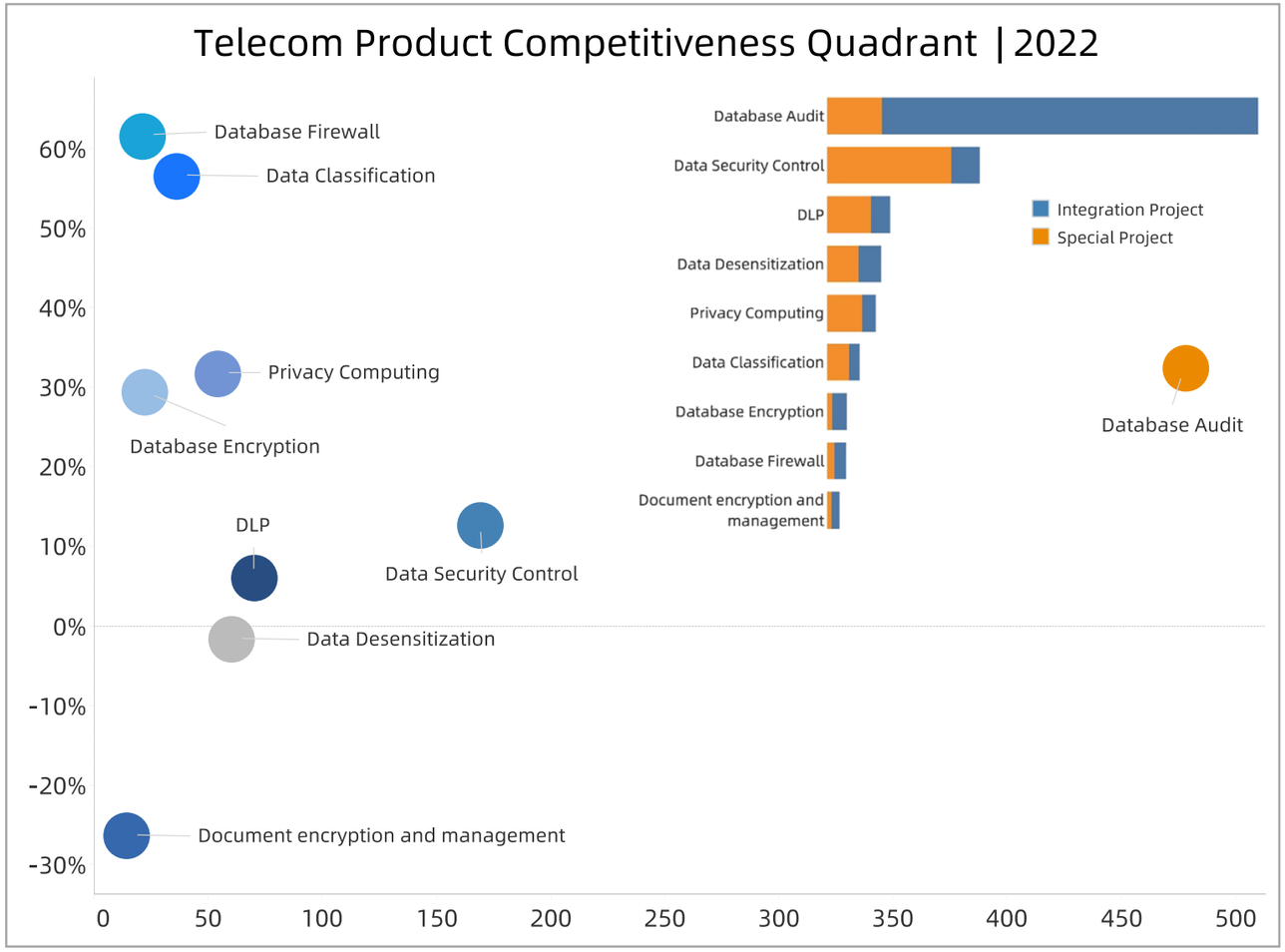


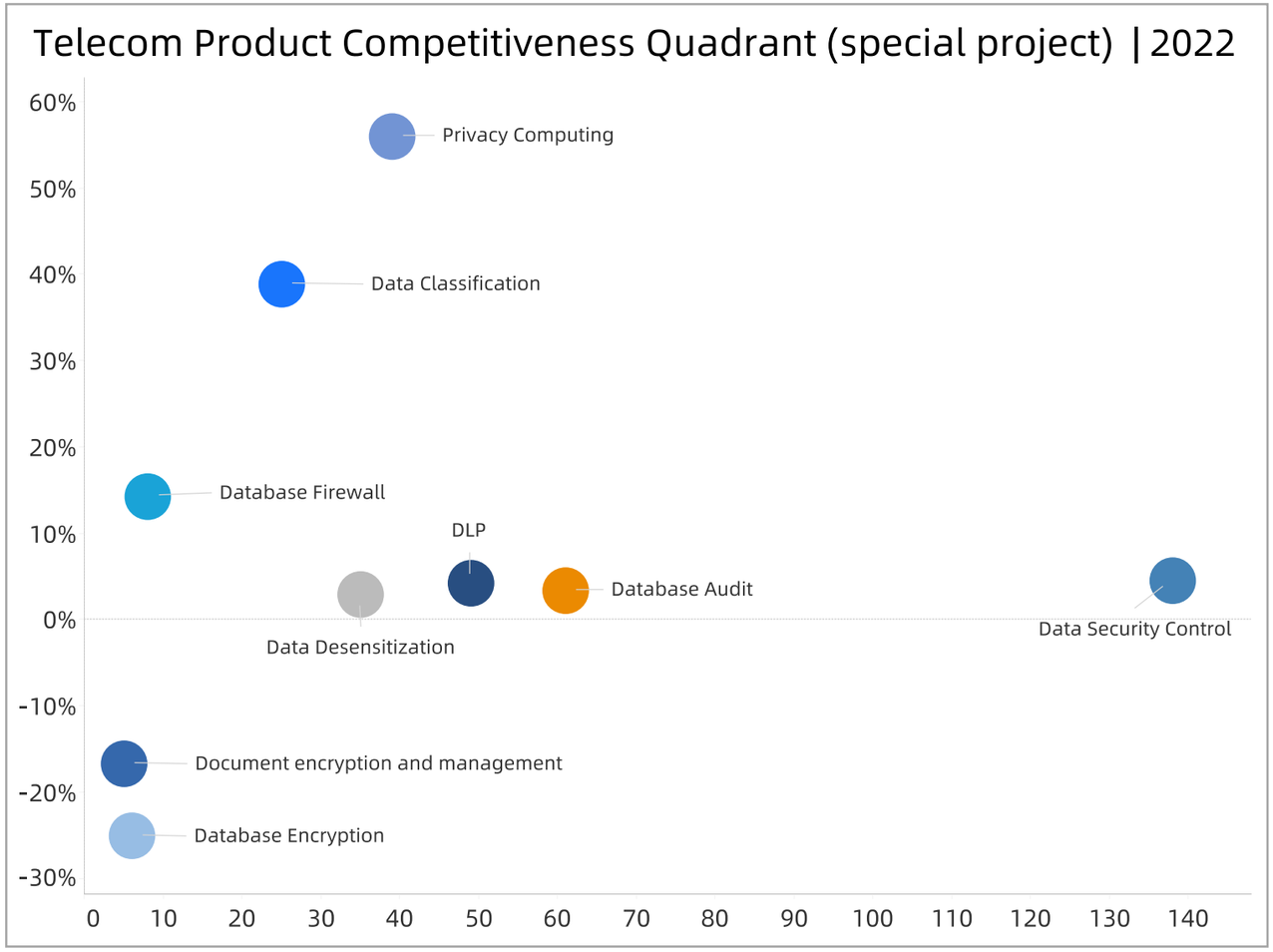
Telecom Carriers: Data Security is High Priority





Telecom Carriers: What’ s hot about Data Security

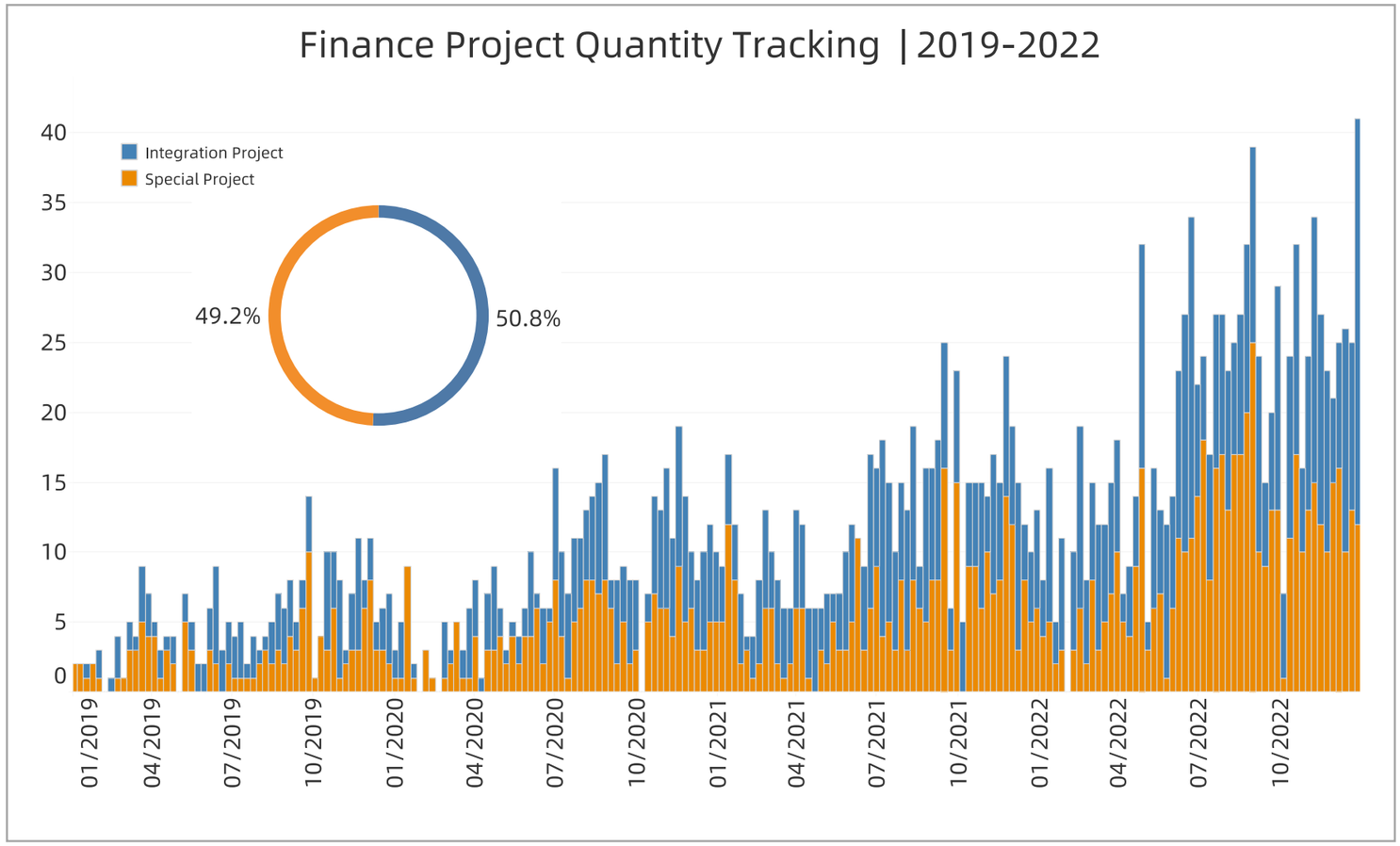


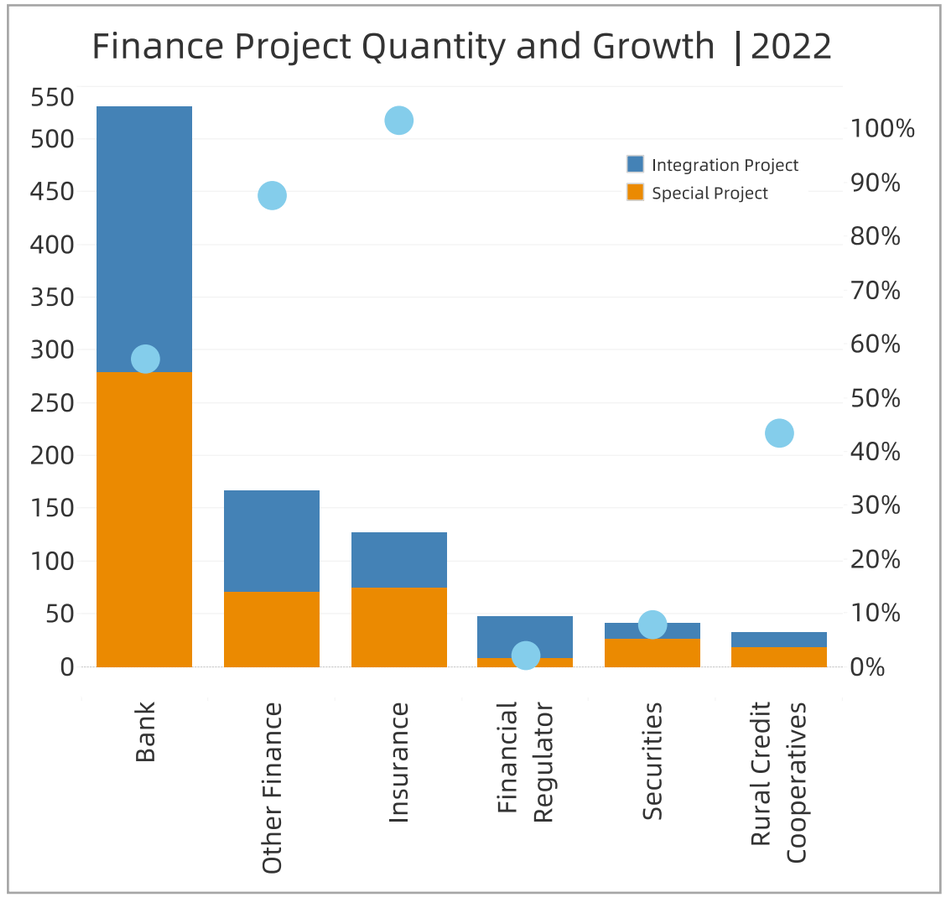


Financial Industry：Banking is the focus

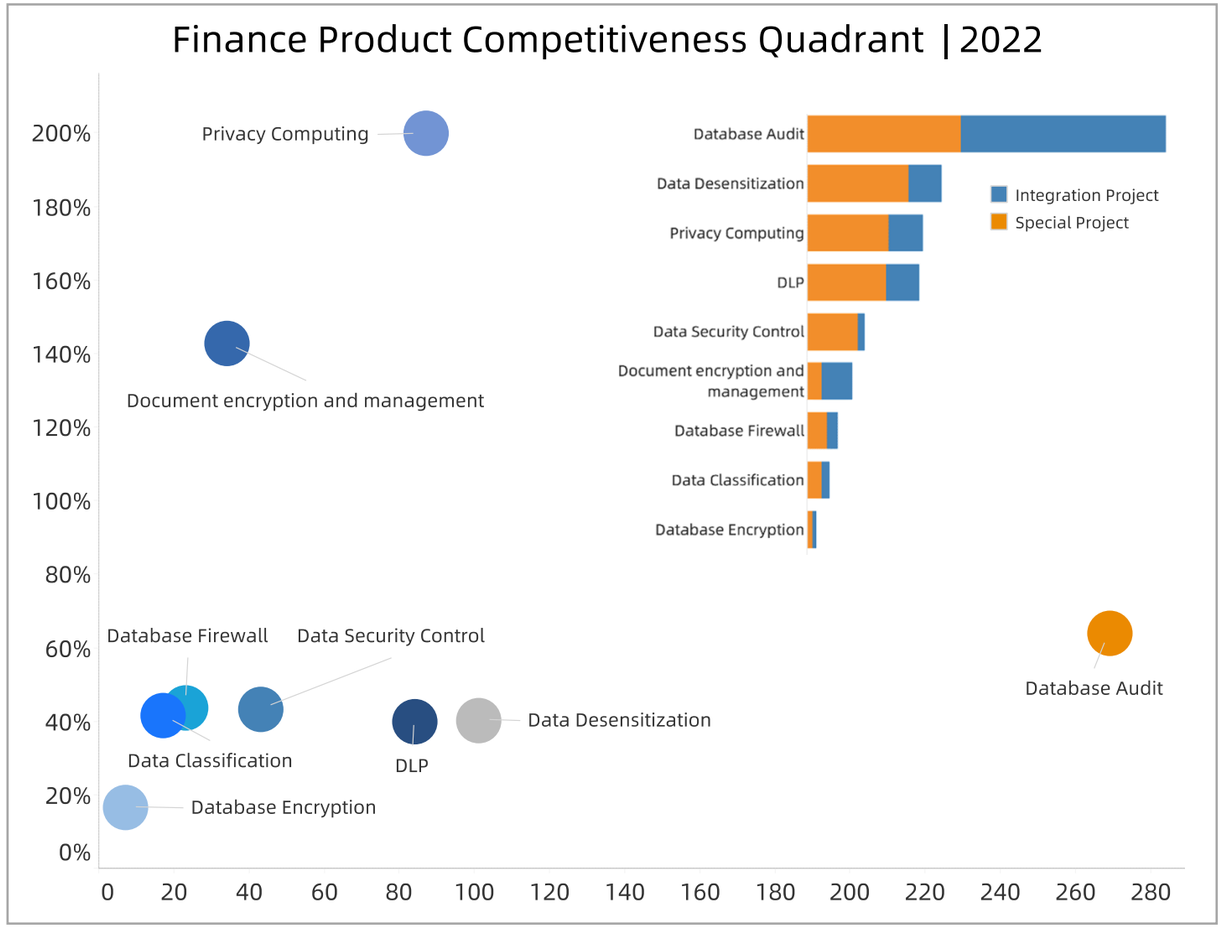
Released Time	Released by	Name	Major Content
Feb 13th 2020	People's Bank of China	Personal Financial Information Protection Technical Specifications	Divide personal financial information into three categories from C3 to C1 from high to low sensitivity, and implement different levels of protection; from two aspects of security technology and security management, put forward normative requirements for the protection of personal financial information
Sep 23rd 2020	People's Bank of China	Financial Data Security Classification Guide	The objectives, principles and scope of financial data security grading are given, as well as the elements, rules and grading process of data security grading
Jan 15th 2021	China Banking and Insurance Regulatory Commission	China Banking and Insurance Regulatory Commission Regulatory Data Security Management Measures (Trial)	Clarify the responsible department, and formulate regulatory data security work rules and management procedures, technical protection measures, evaluation and supervision and inspection systems, etc
Apr 8th 2021	People's Bank of China	Financial data security data life cycle security specification	It stipulates the security principles, protection requirements, organizational security requirements and information system operation and maintenance security requirements of financial data, and establishes a security framework covering data collection, transmission, storage, use, deletion and destruction
Dec 3rd 2021	People's Bank of China	Financial Data Security Assessment Specification (Draft for Comment)	It stipulates the triggering conditions, principles, participants, content, process and methods of financial data security assessment, and clarifies the three main assessment domains of data security management, data security protection, and data security operation and maintenance, as well as the main contents and methods of security assessment

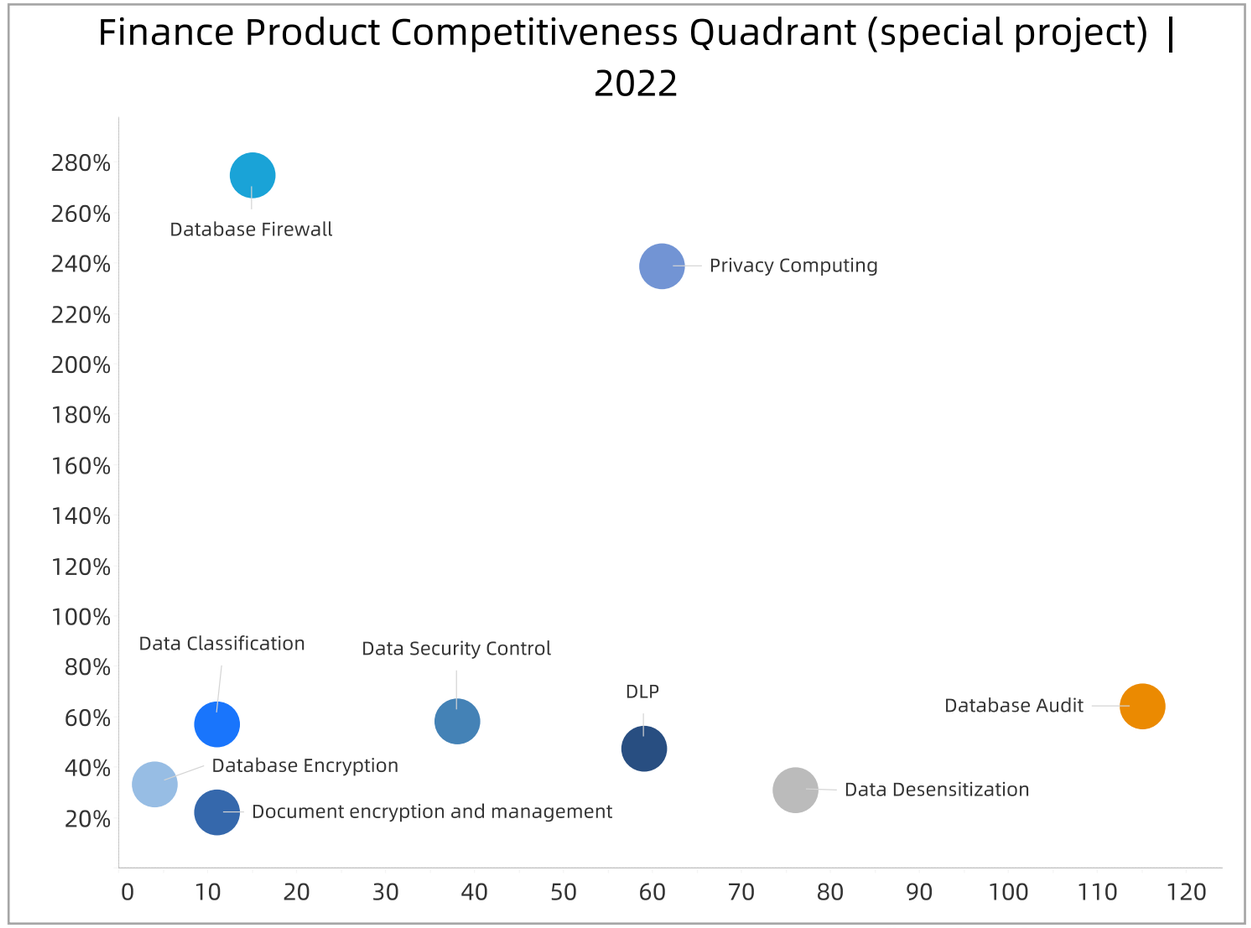
Financial industry: Speeding up Data Security Construction of Banks and Financial Investment Companies



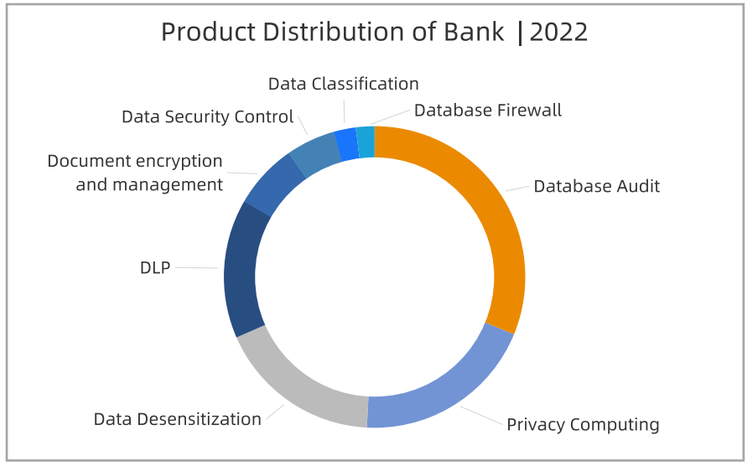


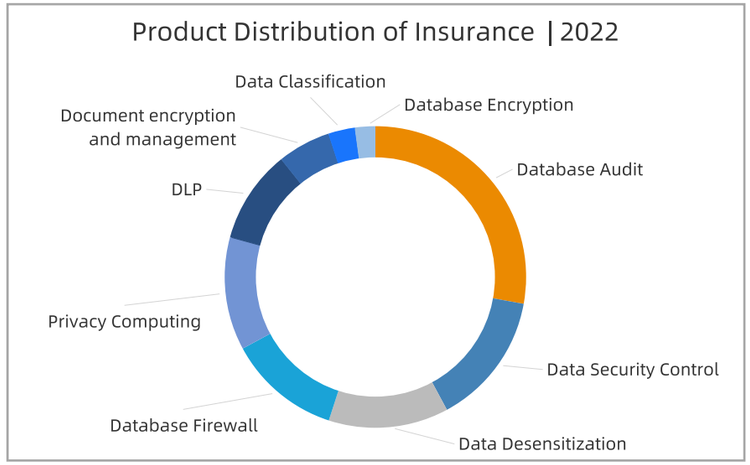
Financial Industry - Data Security has Entered the Preliminary Construction Stage

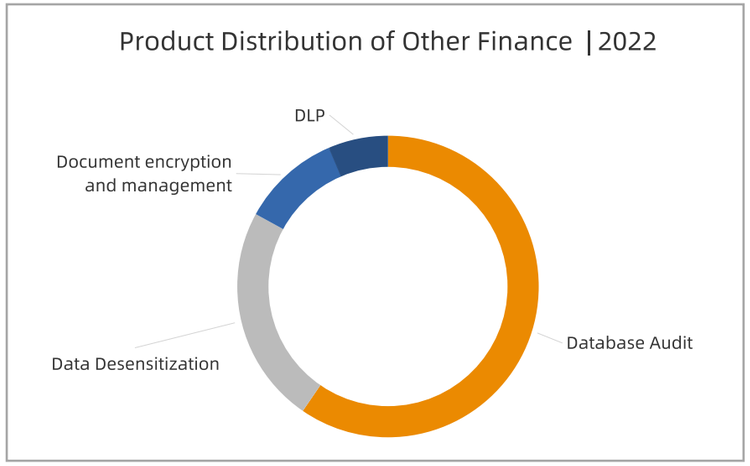


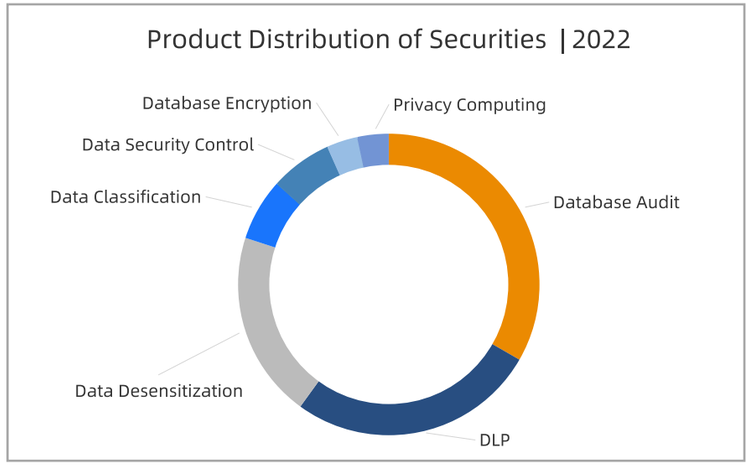


Financial Industry - Data Security Construction of Various Sub-Sectors is Uneven

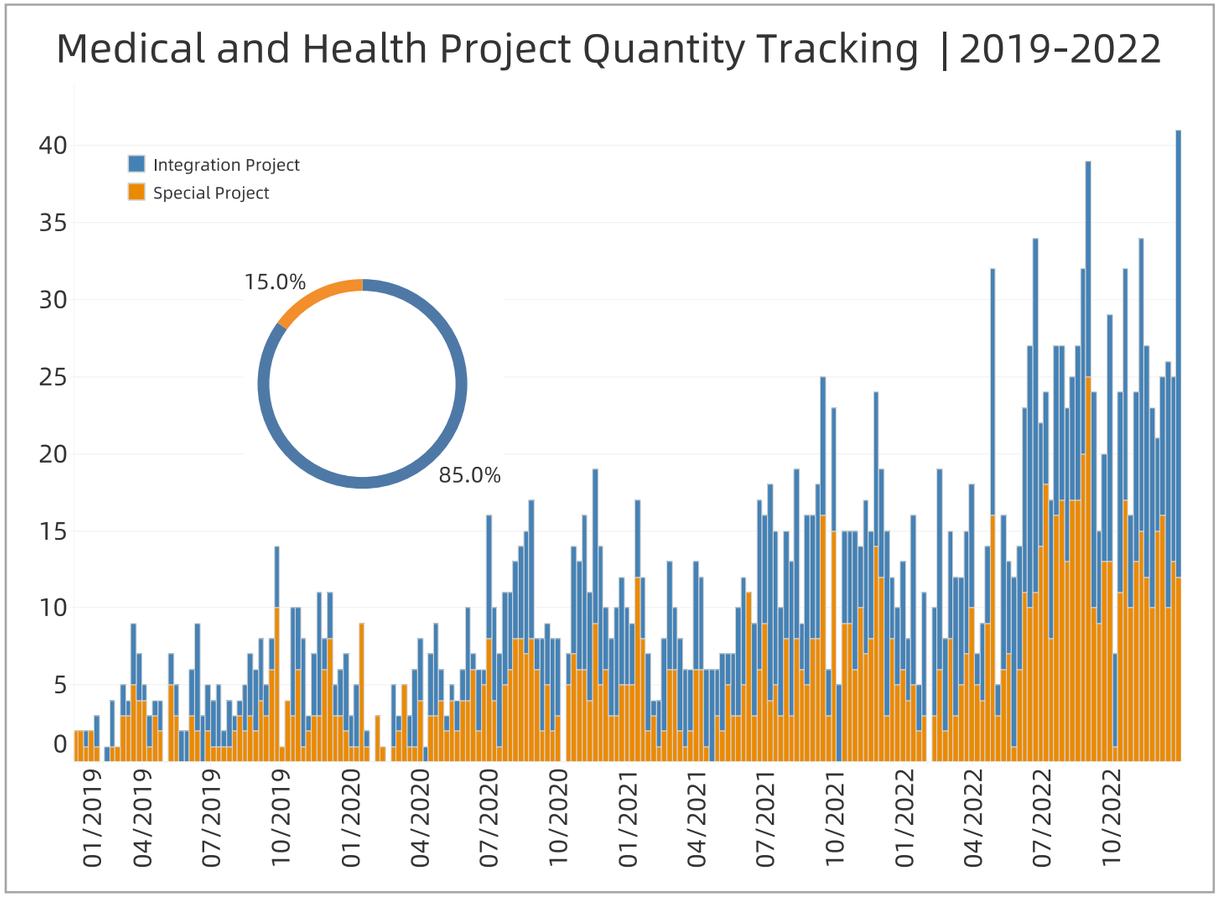


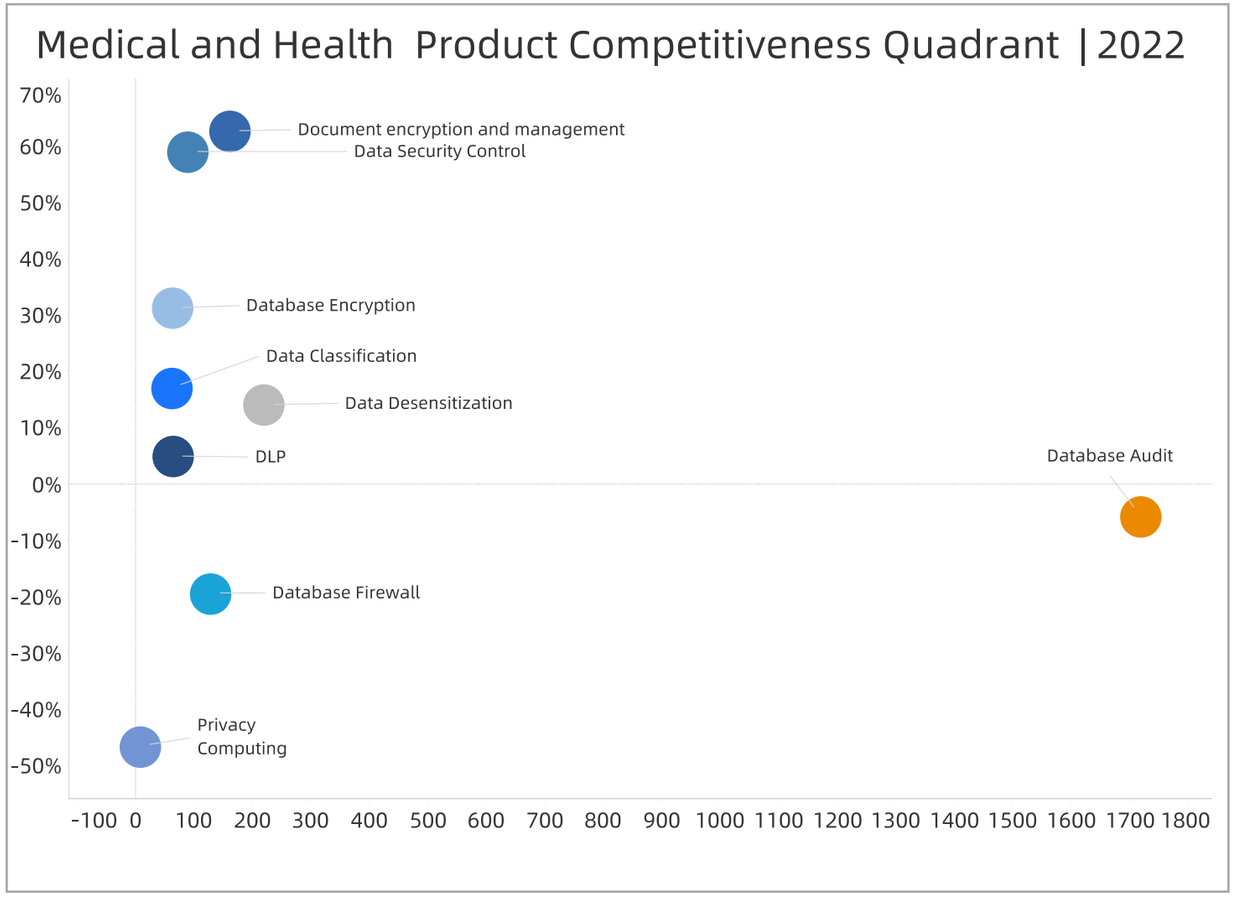




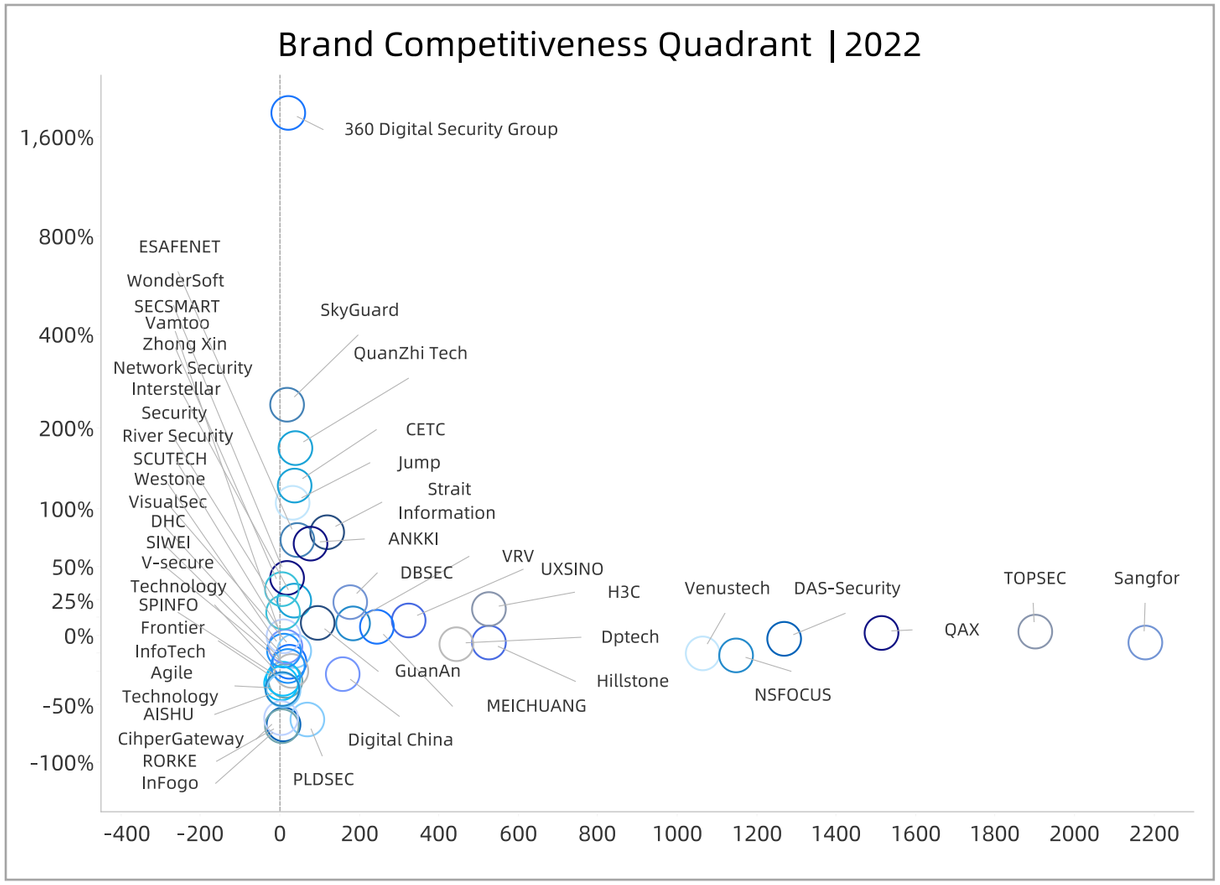


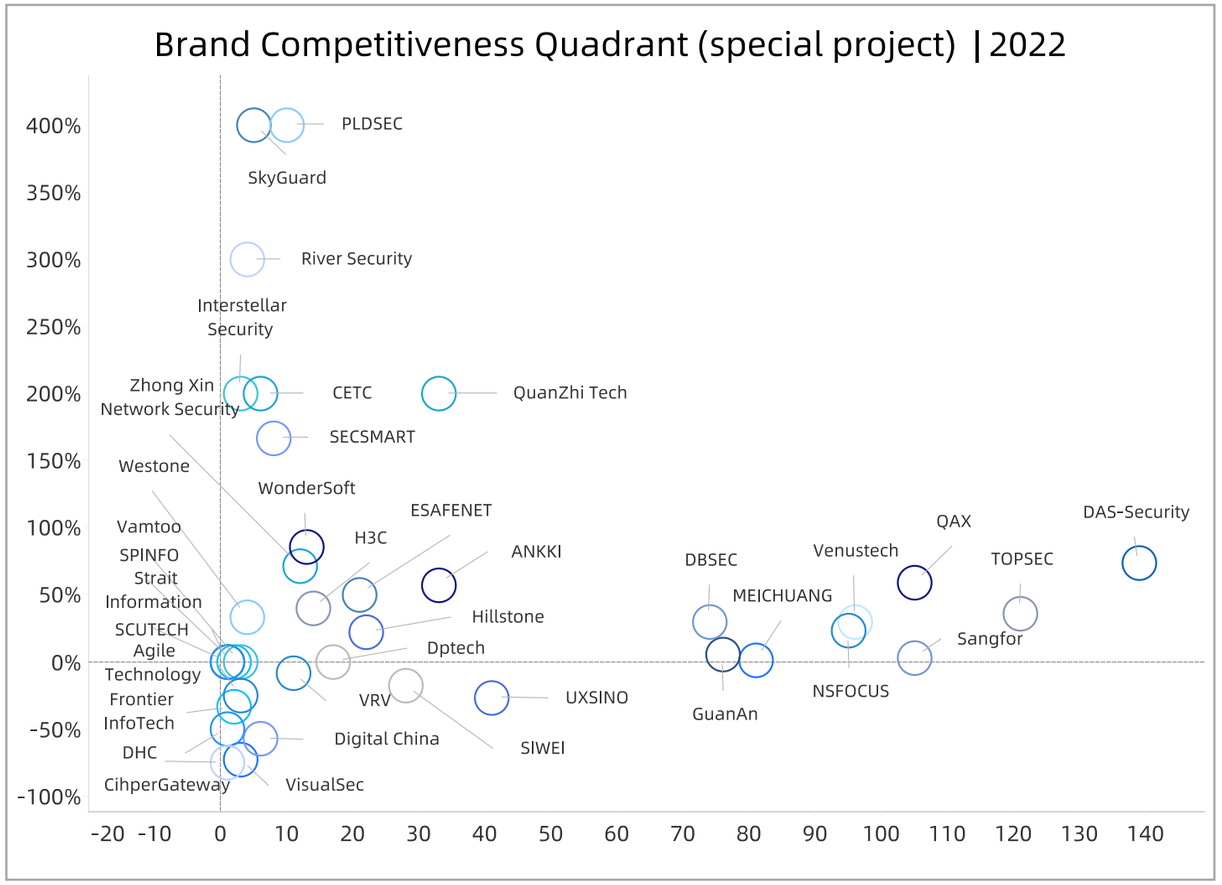
Healthcare – The Healthcare Security Administration takes the lead



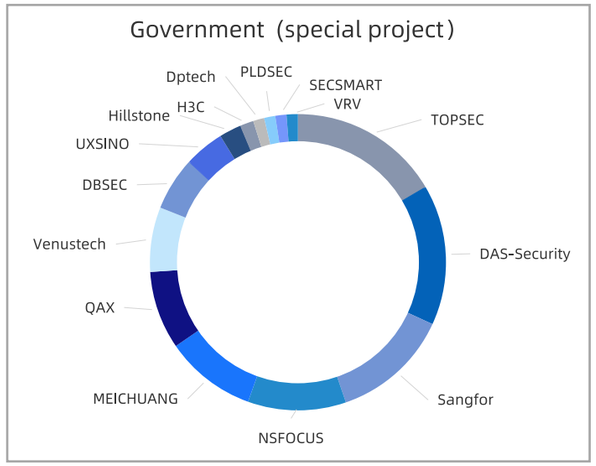


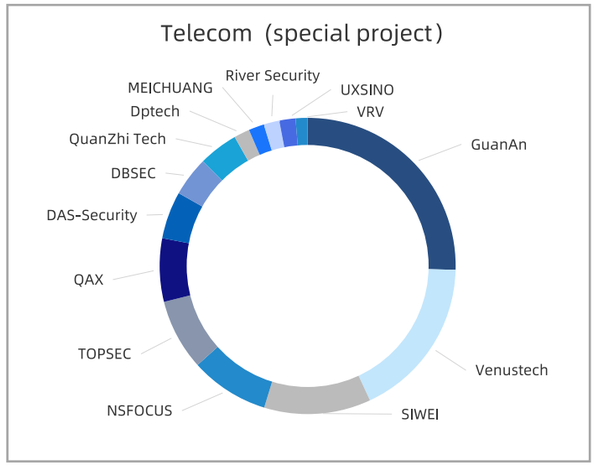
Data Security Brand Popularity of China in 2022

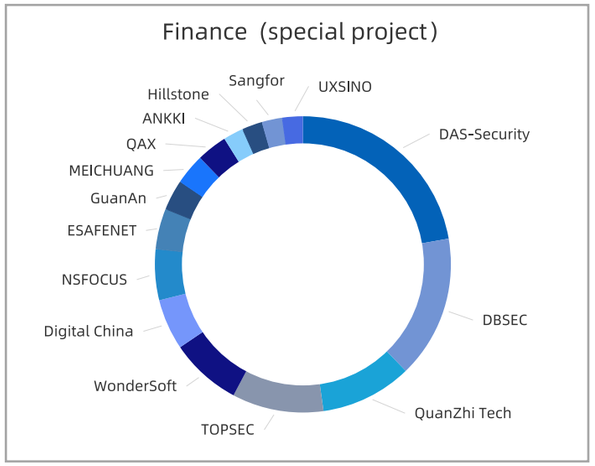


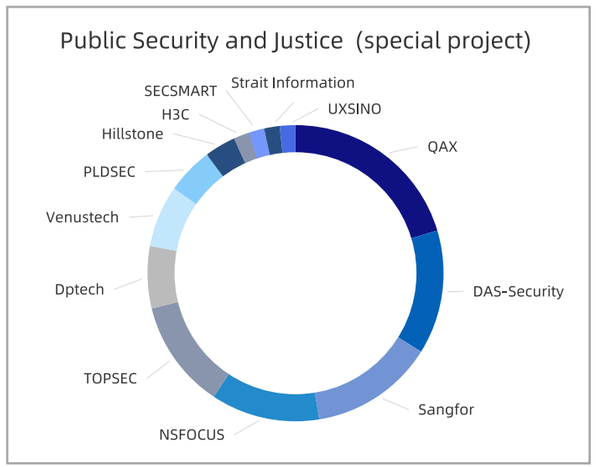


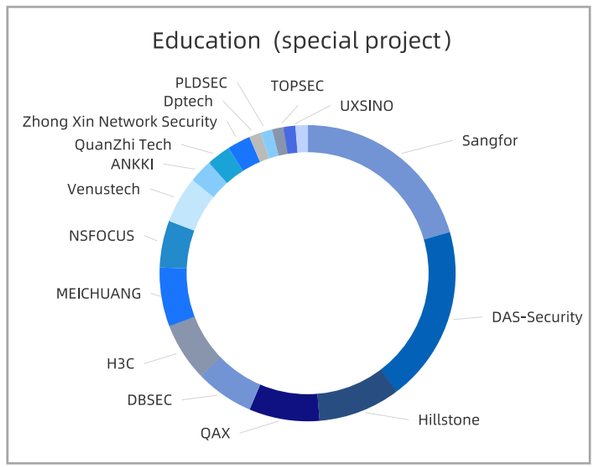
Industry Distribution of Data Security Brand Popularity of China in 2022

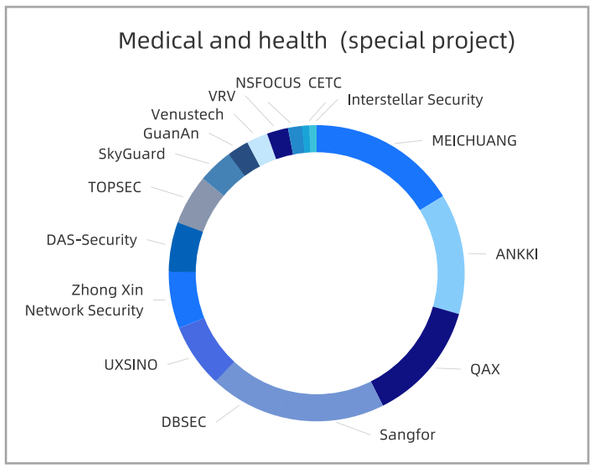






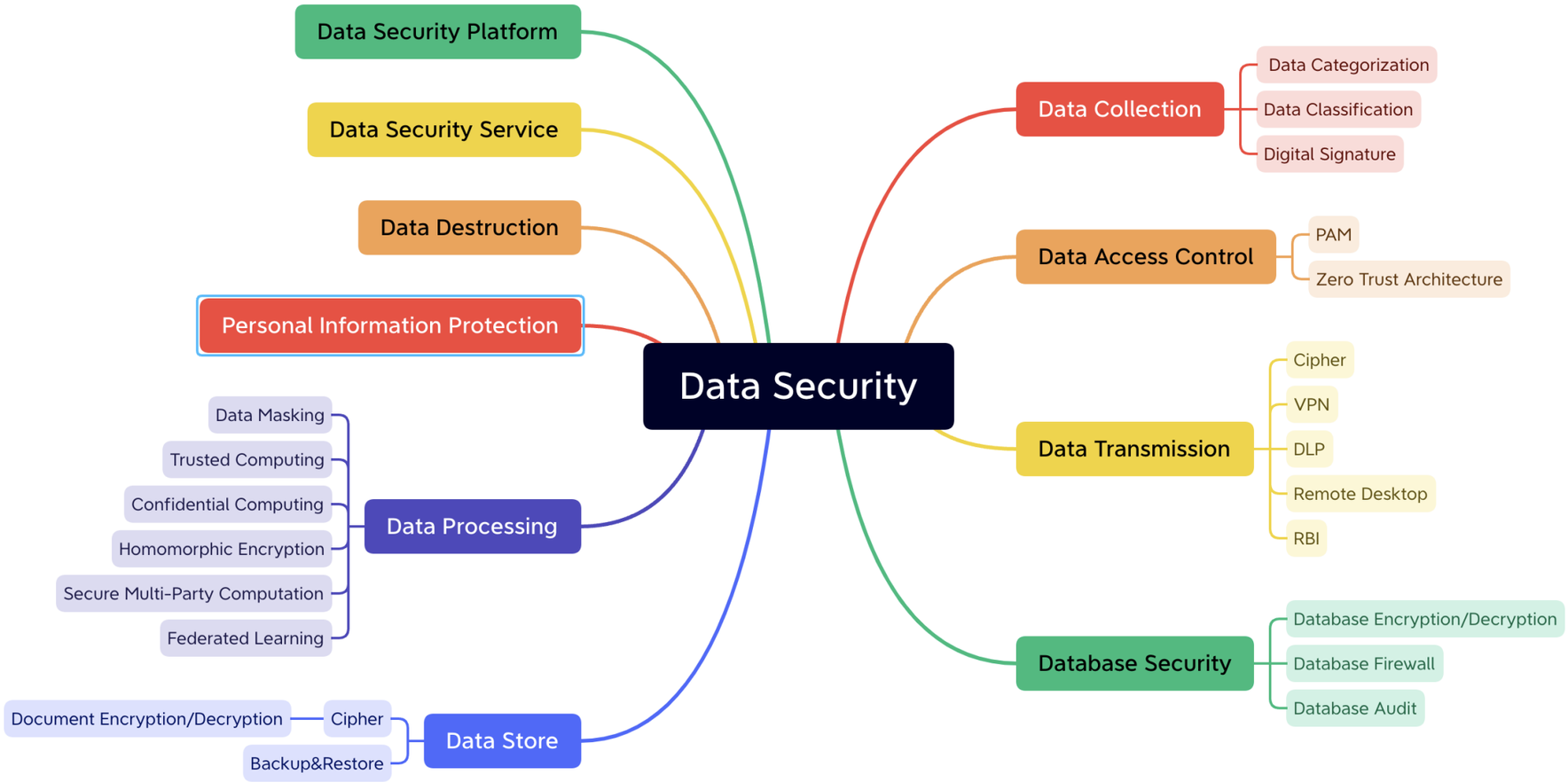




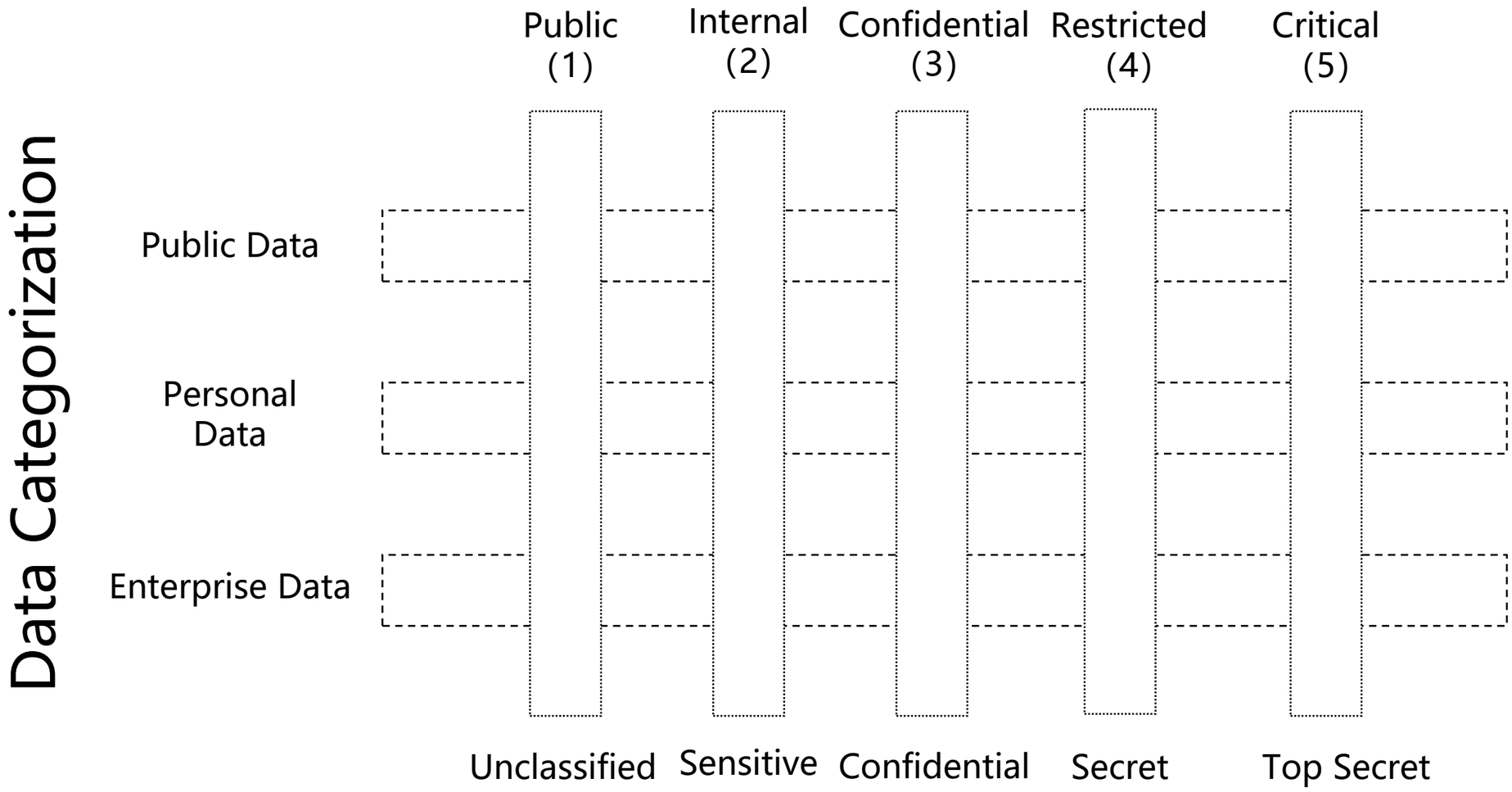


Technology, Product and Service

Data Security Technology/Product/Solution/Service Landscape



Data Classification

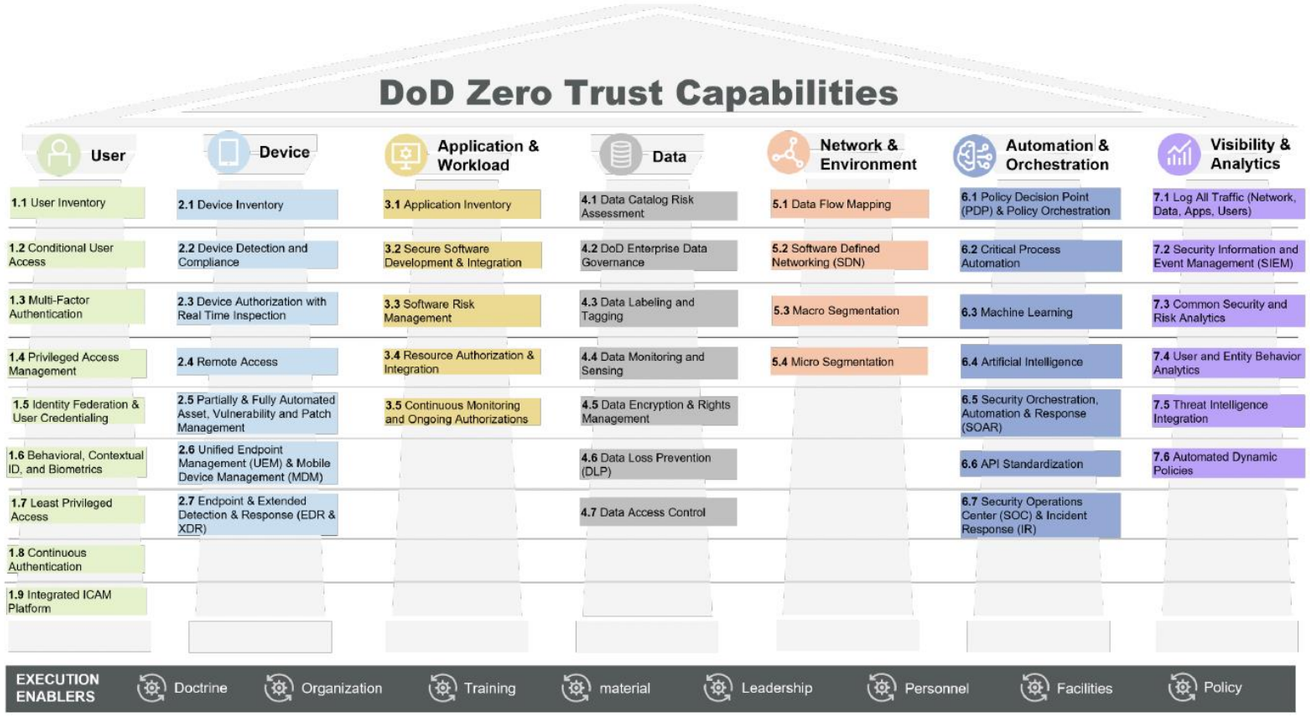


Challenges

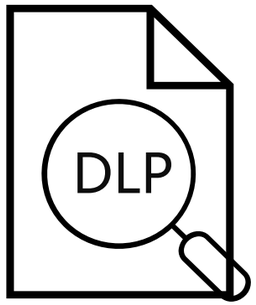
- Just a few industries (include Financial and Telecom) released their standard for data categorization and classification
- Not fully automated, a lot of human efforts
- The accuracy is a potential problem
- Tag are not used in the further data processing

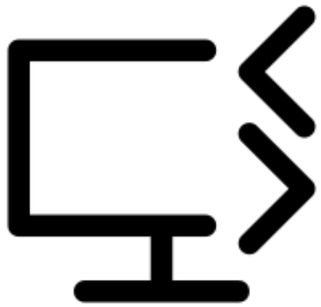
Access Control

- Distributed into different IT systems
- ZTA adoption just begins
- From IBAC,RBAC to ABAC, TBAC,PBAC



Data Transmission





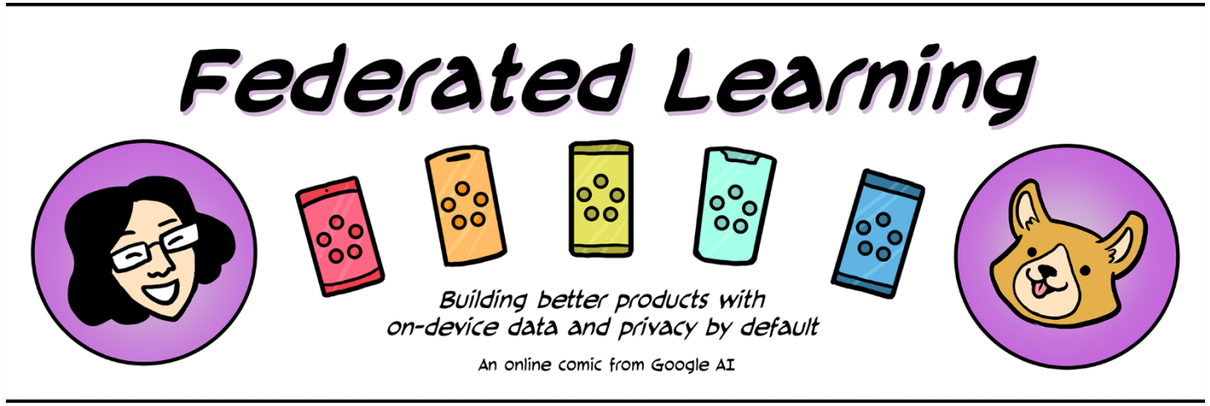
Data Storage

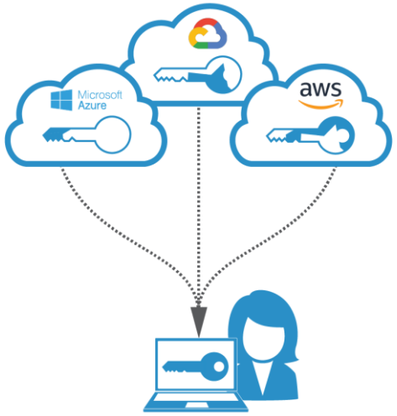
CASB

Database
Encryption/Decryption

Document
Encryption/Decryption

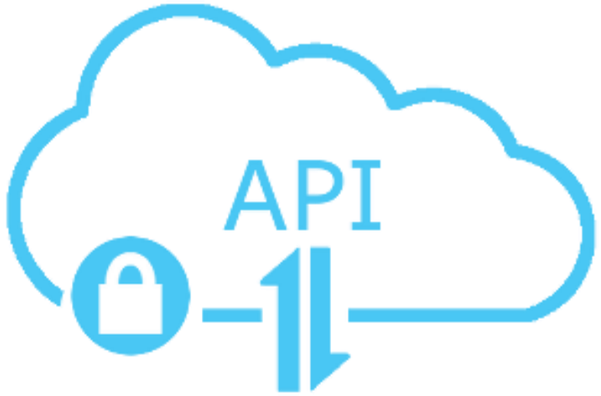
Data Exchange





Secure Multi Party Computing

Homomorphic Encryption



API monitoring based flowing data security

Data Masking

Innovations

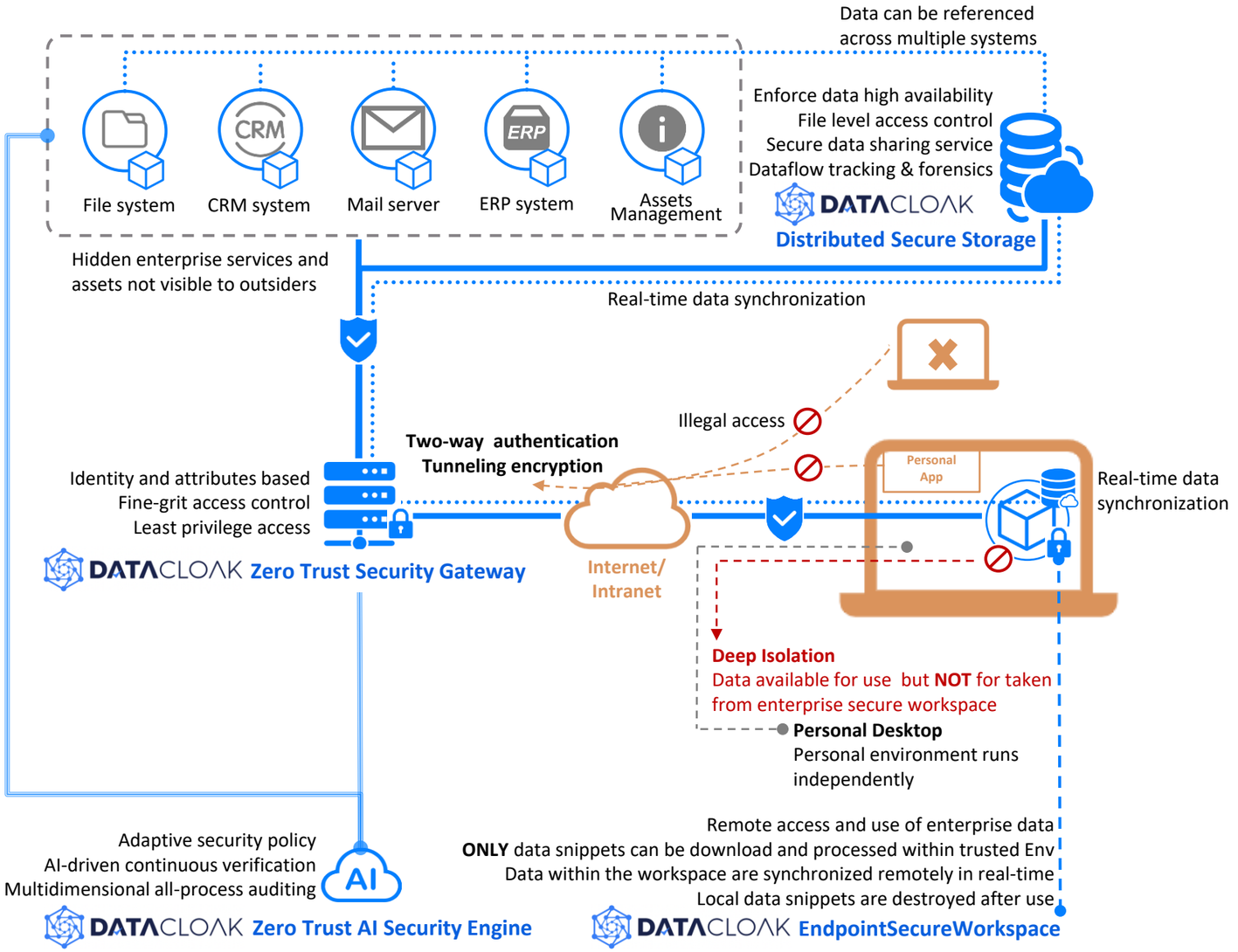
Unleashing local computing power to protect data remotely – A Zero trust data security solution

Engine
- **Zero Trust Policy Engine** — Dataflow tracking and forensics; Remote credibility and continuous verification
- **Access Control Engine** — Attributes based risk coordinated closed-loop control with dynamic strategy

Network
- **Trusted Tunnel** — Two-way authentication & tunneling encryption
- **Trusted Application Gateway** — Fine-grit access control & privilege management

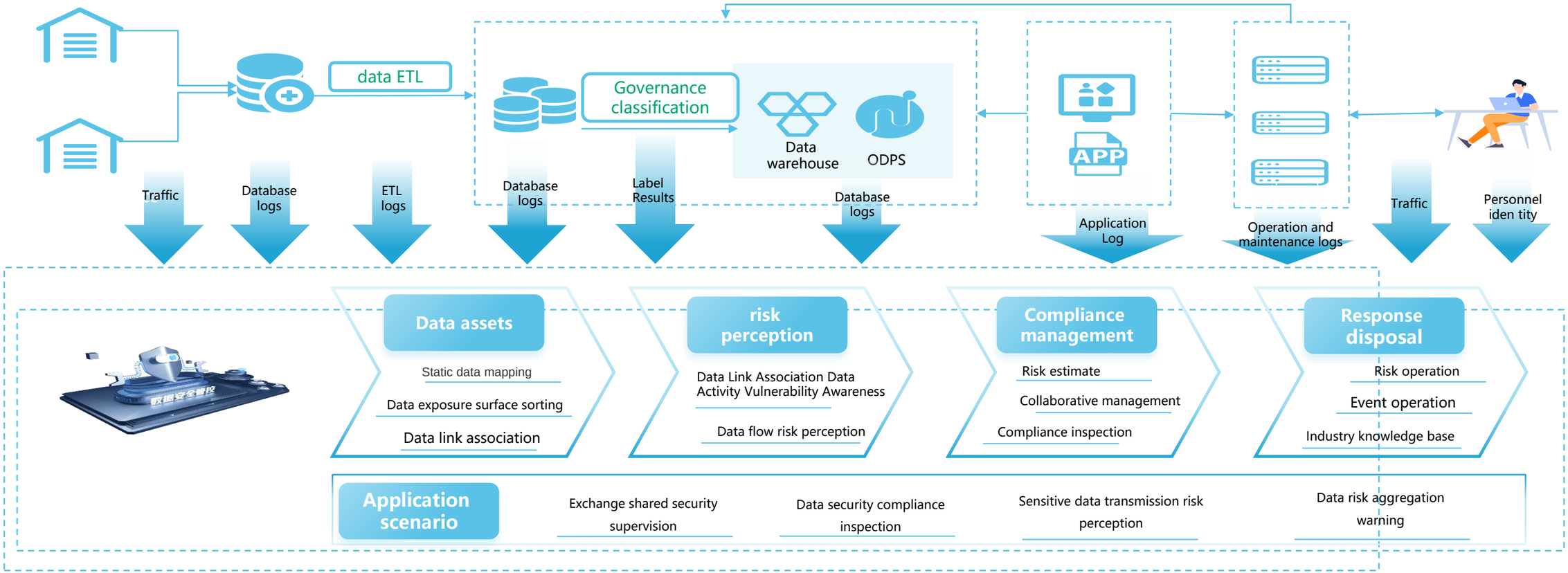
Storage
- **Transparent Encryption & Decryption** — High performance local secure storage
- **Encrypted File System** — Data secure synchronization & sharing; Distributed secure storage

Computing
- **Trusted Sandbox / Container** — Windows; MacOS
- **Trusted Computing Environment** — Linux; IOS/Android



Full link data secutrity situational awareness platform

The full link data secutrity situational awareness platform is a data basin wide security management and control plan launched to address the data security risks generated during the aggregation, flow, and exchange of big data from government and enterprise enterprises. It establishes a rule model from the perspectives of data, interface, and personnel, and conducts comprehensive governance and compliance supervision of data risks in scenarios of data collection, processing, sharing, and exchange. The situational awareness platform is used as the basic tool, Establish a data security supervision and control loop from **Asset Management → Risk Perception → Compliance Management → Response and Disposal at the data level.**



Contribute by: QuanZhi Tech（全知科技）

Dataflow Full Chain Observation Supports Data Privacy Compliance & Risk Management

Data Compliance

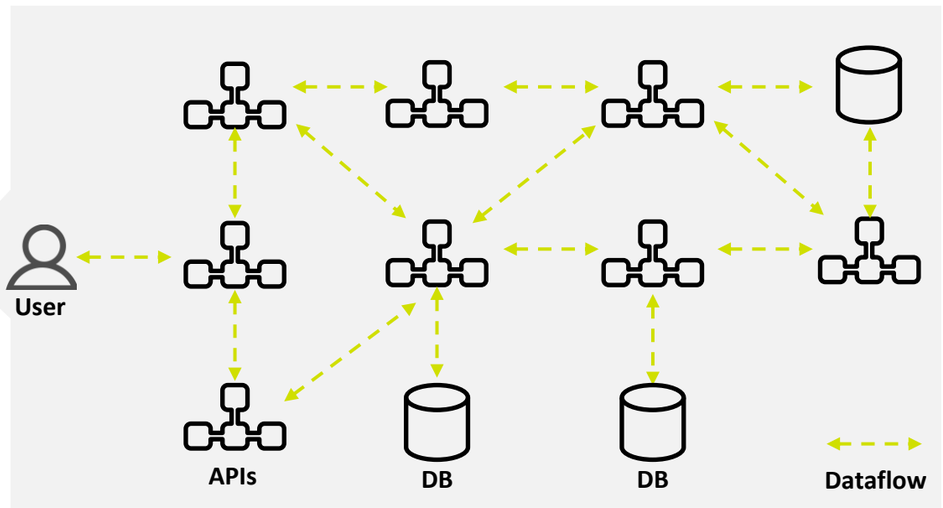
- Data Asset Catalog
- Outbound Data Transfer
- Data Subject Request
- Records of Processing Activities
- …

Risk Management

Event Traceability

Data Classification (Personal and Business Data)

API based, Dataflow Full Chain Observation Platform

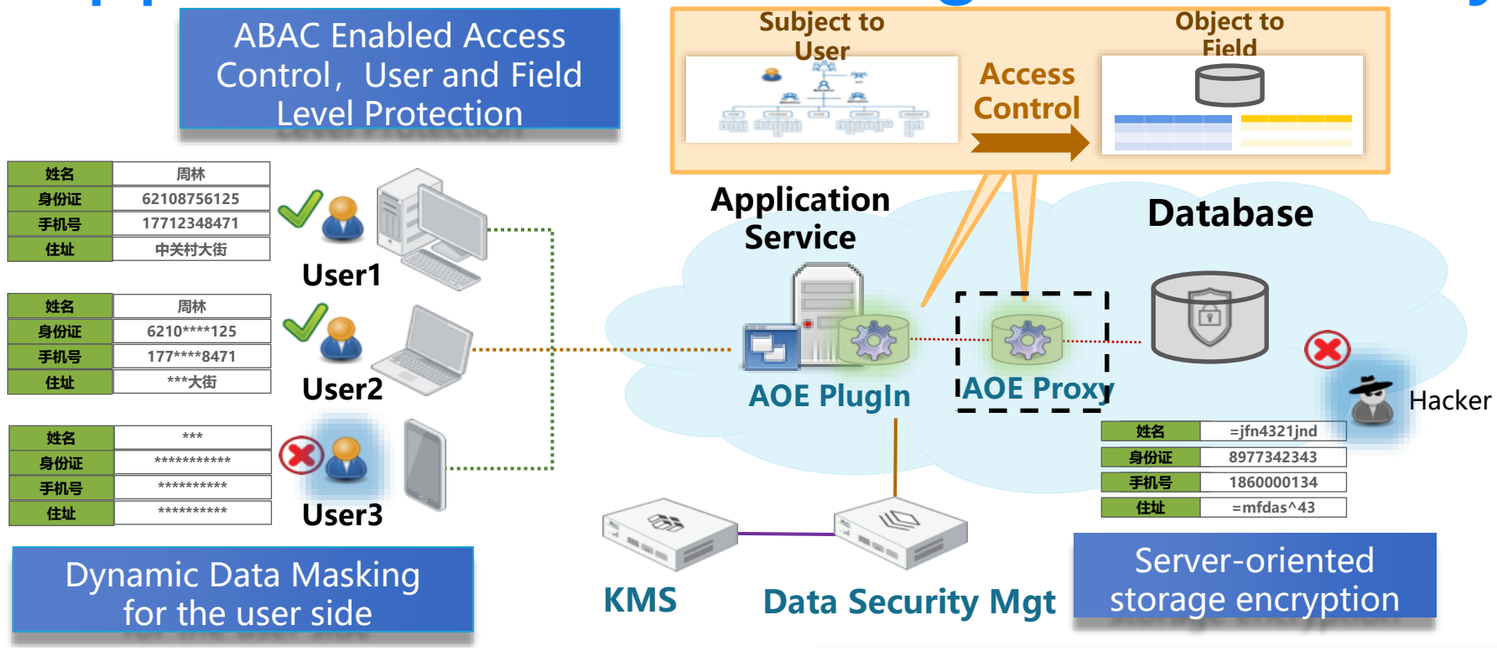


- Automatic
- Multiple IT/App architectures
- Account-APIs-DB-Data, Four Asset Associations

Contribute by: HongTu Tech（红途科技）

Application Zero Change Data Encryption

ABAC Enabled Access Control，User and Field Level Protection



Dynamic Data Masking for the user side

Server-oriented storage encryption

Defending outside and inside threats

- **OPS**：**Data access outside application**
  - **Data Encryption**：DBA，Outsource Worker，Hacker
- **User**：**In application threats**
  - **Dynamic Data Masking**
  - **Risk Monitoring**
  - **Auditing**

No Impact to OPS

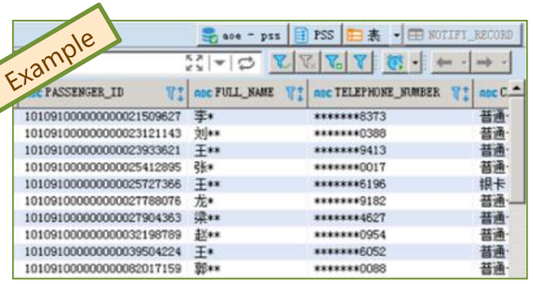
Example

Application：Data Masking Viewer

Example

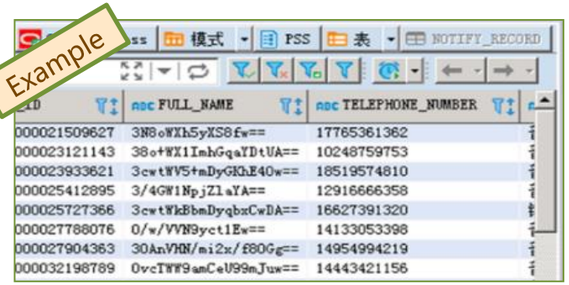
Application：Encrypted Data Viewer

Example



DBA Tools: Data Masking Viewer

Example



DBA Tools: Encrypted Data Viewer

DTTACK FRAMEWORK

Tactics

I: Identify

技术： 数据源发现
网络流量分析
应用接口探测
- 端口扫描
- 网络爬虫
- 数据同步

业务锚点监测

技术： 数据资产识别
关键词提取
- 基于统计特征的关键词提取算法
- 基于词图模型的关键词抽取算法
- 基于主题模型的关键词抽取

正则表达式
- 普通字符
- 非打印字符
- 特殊字符
- 限定符
- 定位符
- 选择
- 反向引用

基于文件属性识别
- 聚类识别
- 文件相似度
- 文件精确指纹识别
- 文件 DNA 识别
- 支持多属性条件过滤

精确数据比对
指纹文档比对
向量分类比对

技术： 数据资产处理（分析）
数据内容识别
- 文字识别
- 图片识别
- 语音识别

合规性分析
- 采集环节合规处理
- 传输环节合规处理
- 存储环节合规处理
- 密评工具箱

安全性分析
- 数据沙盒技术

重要性 （敏感性） 分析
- 基于元数据的敏感数据识别（敏感词库 + 关键词匹配）
- 基于数据内容的敏感数据识别 （正则表达式）
- 基于自然语言处理技术的中文模糊识别（敏感词库 + 分词 + 相似度计算）

技术： 数据分类分级
- 内容感知分类技术
- 情境感知分类技术
- 根据分类分级规则

自动化工具
- 自动化数据分类分级平台
- 自动化数据分类分级打标

人工辅助

技术： 数据资产打标
标记字段法
元数据映射表法
数字水印法
- 灰度值加密
- 位置加密
- 双因子加密

P: Protect

技术： 数据加密技术
存储加密
- DLP 终端加密
- CASB 代理网关
- 应用内数据加密（集成密码 SDK）
- 应用内加密（AOE 面向切面加密）
- 数据库加密网关
- 数据库外挂加密
- TDE 透明数据加密
- UDF 用户自定义函数加密
- 传输加密文件系统加密
- 磁盘加密
- 可互操作存储加密

传输加密
- 网线通信消息传输加密
- 在线通信消息传输加密
- 可感知窃听的专线通信传输加密技术
- 代理重加密受控分发消息传输加密技术

使用加密
- FHE 全同态加密
- MPC 多方安全计算
- ZKP 零知识证明
- 可验证计算
- 可信执行环境

技术： 数据脱敏技术
动态脱敏技术
静态脱敏技术
动态双因子可逆脱敏
隐私保护技术
- 匿名化技术
- 假名化技术
- 去标识化技术

技术： 隐私计算技术
可信计算
- 信任根
- 可信平台模块
- 信任链传递技术
- 可信 BIOS 技术
- 可信计算软件栈技术
- 可信网络连接技术

密码学应用
- 安全多方计算
- 同态加密
- 信任链传递技术
- 零知识证明
- 联邦学习
- 隐私求交
- 不经意传输

差分隐私

技术： 身份认证技术
口令认证技术
- 静态口令认证
- 一次性口令认证
- 双因素动态口令认证

无口令认证
生物特征认证
- 人脸识别技术
- 指纹识别技术
- 虹膜识别技术
- 掌静脉识别技术
- 声纹识别技术

令牌
- X.509 证书管理
- PKI 技术
- RFIS 身份认证

机器 ID 管理
去中心化身份 （DID）

技术： 访问控制技术
网络访问控制
- 入网访问控制
- 网络权限控制
- 自主级安全控制
- 属性安全控制
- 服务器安全控制

权限管理控制
- DAC
- MAC
- RBAC
- ABAC

风险操作控制
- 系统和设备指令级
- 应用和业务级

数据访问控制
- 存储介质访问控制
- 网间数据摆渡

技术： 数字签名技术
数字证书
签名验签
电子签章

技术： DLP 技术
终端 DLP
- 办公设备 DLP
- 移动设备 DLP

网络 DLP
端点 DLP
邮件 DLP
DLP 集成
- 企业 DLP 套件

数据交换 DLP
- 行为追溯
- 业务分析

CASB DLP
云原生 DLP

技术： 数据销毁技术
硬销毁
- 消磁
- 物理破坏
- 化学腐蚀

软销毁
- 格式化
- 磁盘分区
- 数据覆写
- 文件粉碎软件
- 云资源再分配

销毁审计

技术： 云数据保护技术
云密码服务
- 密钥管理（KMaaS，Key Management-as-a-Service）
- 加密即服务（EaaS，Encryption-as-a-Service）
- 基础设施即服务（IaaS）容器加密

云身份鉴别服务
云身份管理和访问控制技术
- 特权访问管理（PAM，Privileged access management）

技术： 大数据保护技术
- 数据隔离
- 数据分层访问
- 列级数据授权
- 批量授权

D : Detect

技术： 威胁检测
APT 检测
欺诈检测

技术： 流量监测
网络流量分析
- DPI 深度包检测
- DFI 深度动态流检测

高级安全分析
文件分析
TLS 流量解密

技术： 数据访问治理
UEBA 用户实体行为分析
业务风控
动态风险评估
安全影响评估

技术： 安全审计
主机安全审计
网络安全审计
数据库安全审计
业务安全审计
数据流转审计
- 异常访问监测
- DFI 深度动态流检测

技术： 共享监控
风险操作监测
交换策略监测
接口访问预警

R : Respond

技术： 事件发现
内 / 外部情报技术
互联网监测技术
安全预警分析
系统快照

技术： 事件处置
“一键” 通报机制
事件还原技术

技术： 应急响应
应急响应工具包
应急响应案例库

技术： 事件溯源
攻击源捕获
溯源定位手段

R : Recover

技术： 灾难恢复
数据备份
- 硬件实现
- 软件实现
- 云服务实现

容侵技术
容错技术
容灾技术
- 云灾备

技术： 数据迁移技术（分层存储管理）
- 数据迁移的实现可以分为 3 个阶段：数据迁移前的准备、数据迁移的实施和数据迁移后的校验。

技术： 集群技术
- 负载均衡集群
- 高可用集群

技术： 远程异地容灾
- 远程容灾系统一般由生产系统（即数据中心）、可接替运行的备份中心、数据复制系统、通信线路等部分组成。在正常生产和数据备份状态下，生产系统向备份系统传送需备份的数据。灾难发生后，当系统处于灾难恢复状态时，备份系统将接替生产系统继续运行。

C : Counter

技术： 水印技术
图像水印
多媒体水印
数据库水印
屏幕水印
- 文本水印
- 点阵水印
- 二维码水印

技术： 溯源技术
权限流转
权限迁移
签名验证

技术： 版权管理技术
验证授权
- 产品密钥
- 激活限制
- 在线 DRM

使用限制
- 复制限制
- 运行限制
- 地域限制
- 环境限制

侵权追溯
- 数字水印技术
- 元数据标注
- 安全容器技术
- 移动代理技术

内容保护
- 加密技术
- 数字证书技术
- 数字对象唯一标识符，（Digital Object Unique Identifier，DOI）

G : Governance

技术： 数据价值
信息经济学
信息估值
数据库价值管理
- 数据资产价值评估
- 数据资产定价

个人信息价值评估

技术： 数据安全策略
数据安全原则
数据安全隐私管理
- 设计隐私保护
- 设计和默认的数据保护
- 隐私数据安全策略清单
- 《工业和信息化领域数据安全管理办法（试行）》征求意见稿
- 《人类遗传资源管理暂行办法》
- PCIDSS 安全策略

技术： 数据安全模型
DSG 模型
CARTA 模型
DGPC 框架
- 人员
- 流程
- 技术

FinDRA 模型

技术： 数据安全管理
数据安全评估
隐私影响评估
个人信息安全影响评估
数据安全能力平台
- 数据安全管控平台
- 数据安全治理系统
- SaaS 平台安全管理
- 工业安全智能监管平台
- 容器安全管理系统
- 云安全资源池

数据安全能力评价

技术： 数据安全运营
DataOps
- 云架构
- 容器
- 时和流处理
- 多分析引擎
- 集成的应用程序和数据管理
- 多租户和安全性
- DevOps 工具

DevOps
供应链安全

技术： 意识与教育
- 通过安全意识动画、安全意识画册、安全意识海报、安全意识屏保、安全意识电子期刊等提升数据安全意识；通过理论知识和管理方法论学习，夯实数据安全理论知识；通过案例讲演、攻防实操，提升员工数据安全操作能力。

技术： 数字道德
- AvanadeTrendlines：数字道德
- Gartner：数字道德与隐私

Techniques

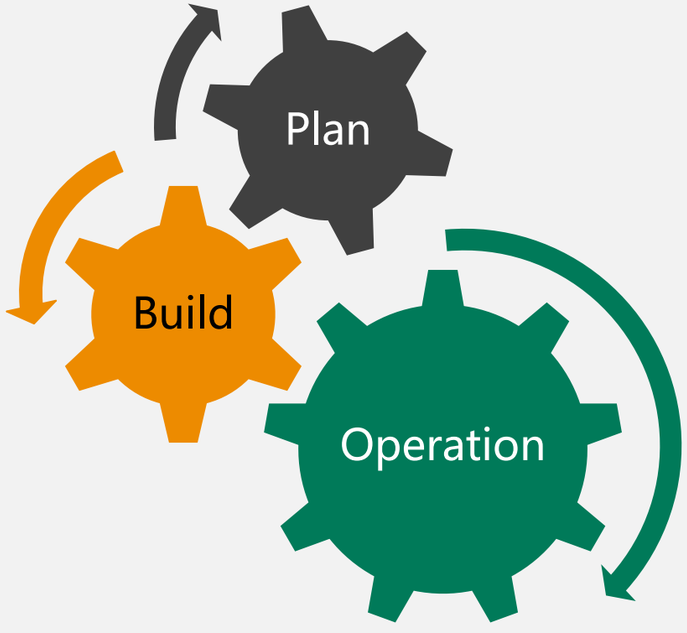
Sub-Techniques

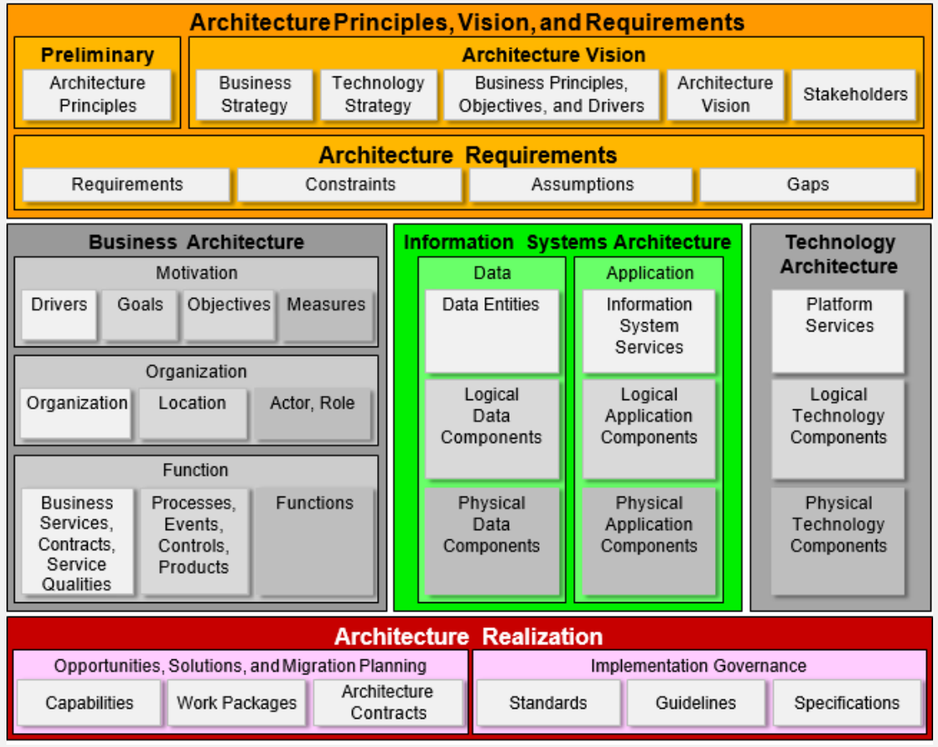
Method

7 Tactics, 38 Techniques, 110 Sub-Techniques, 161 Methods

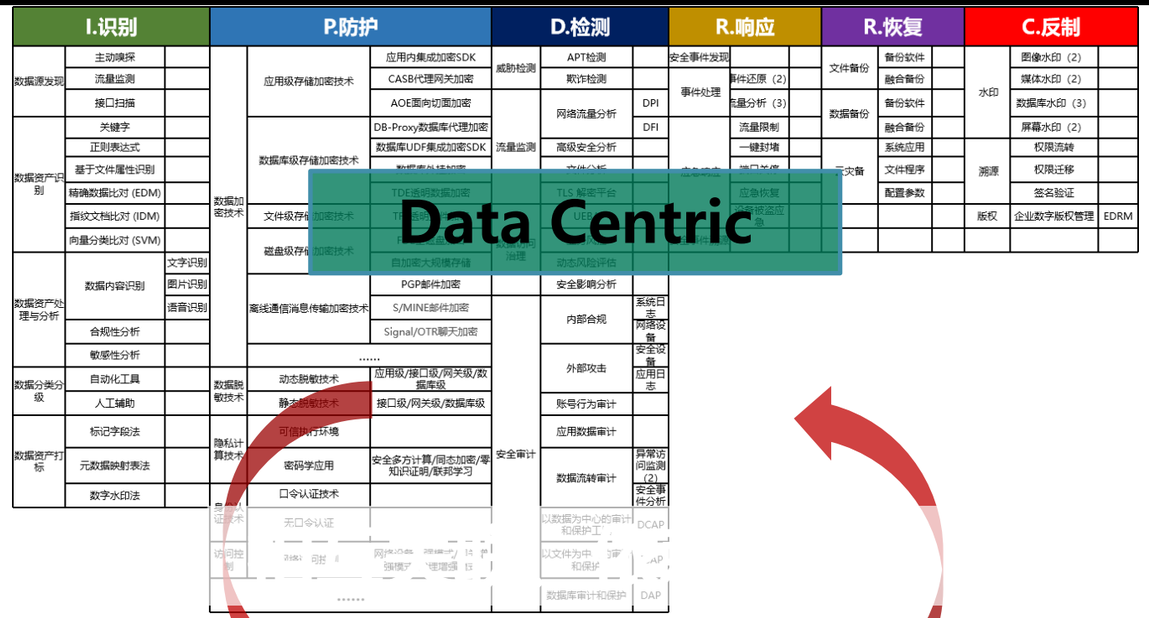
Contribute by: CihperGateway（炼石网络）

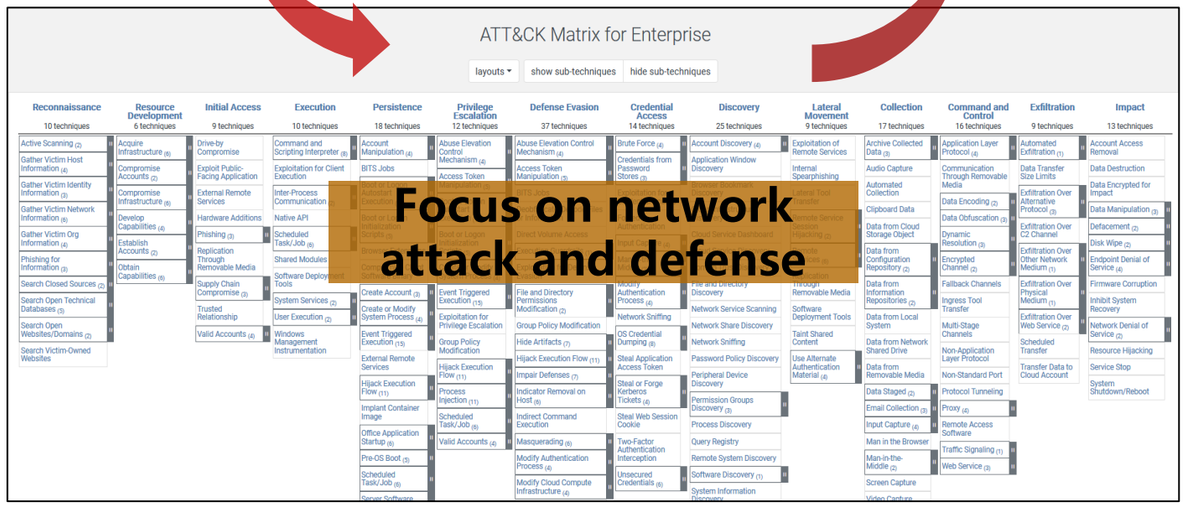
- DTTACK：Data-centric Tactics, Techniques And Common Knowledge
- DTTACK is not a security model for networks, servers or applications, but a security model that emphasizes the security of the data itself
- The DTTACK model can provide data security capability reference for information construction and enterprise business architecture design, and can create data security solutions based on DTTACK

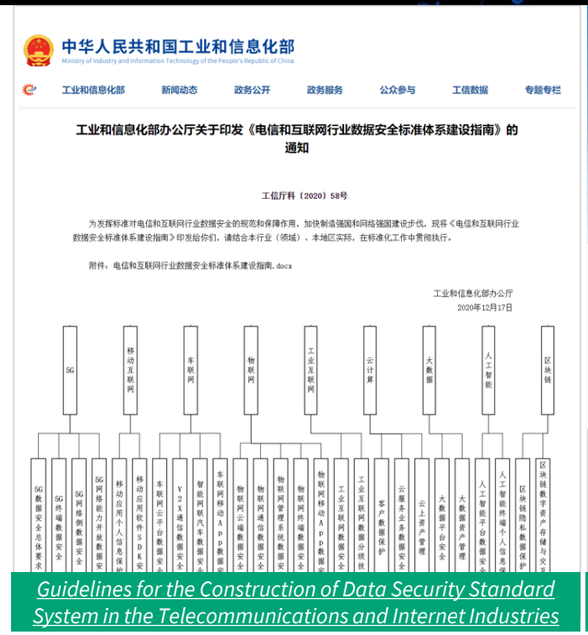




Contribute by: CihperGateway（炼石网络）







Guidelines for the Construction of Data Security Standard System in the Telecommunications and Internet Industries

Measures on Regulatory Data Security Management (Trial) 2020

- 《民用航空旅客服务信息系统信息安全保护 规范》《交通运输行业网络安全等级保护基本要求》……
- 《国家健康医疗大数据标准、安全和服务管理办法（试行）》《关于印发全国医院信息化建设标准与规范（试行）的通知》……
- 《工业控制系统安全检查指南》《工业控制系统安全管理基本要求》《工业控制系统信息安全分级规范》……

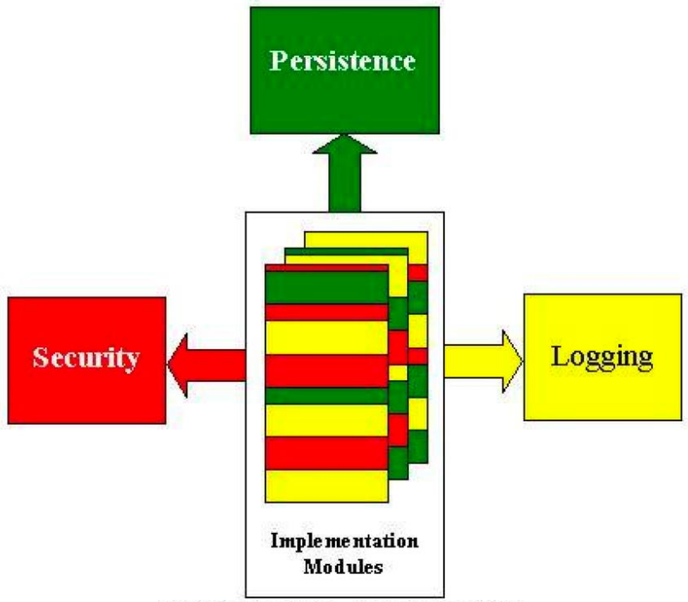
DoD Cloud Strategy

Shift its security focus from perimeter defense to securing data and services

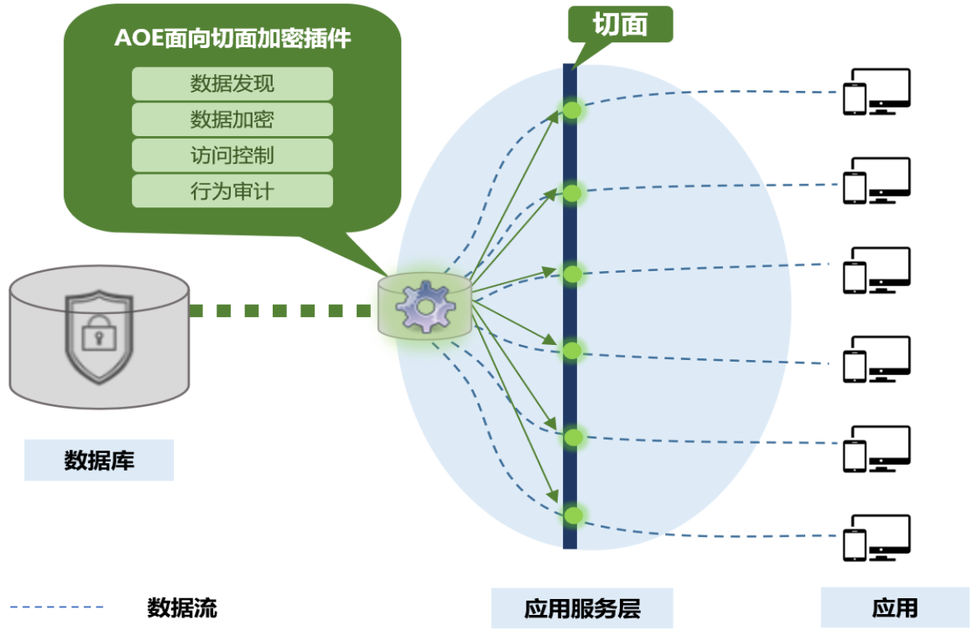
Feb 4th 2019

AOE oriented Data Security

Reference Spring:
From coupled programming to AOP decoupled programming



Aspect security: rebuild security rules on the aspect of data flow,
Realize the technical decoupling and capability integration of security and business



Contribute by: CihperGateway（炼石网络）

> A core technology for implementing security parallel aspects is AOP (Aspect Oriented Programming), that is, aspect-oriented programming or aspect-oriented programming. It was proposed by researchers at Xerox Palo Alto Research Center (Xerox PARC) in the 1990s. A new programming paradigm.

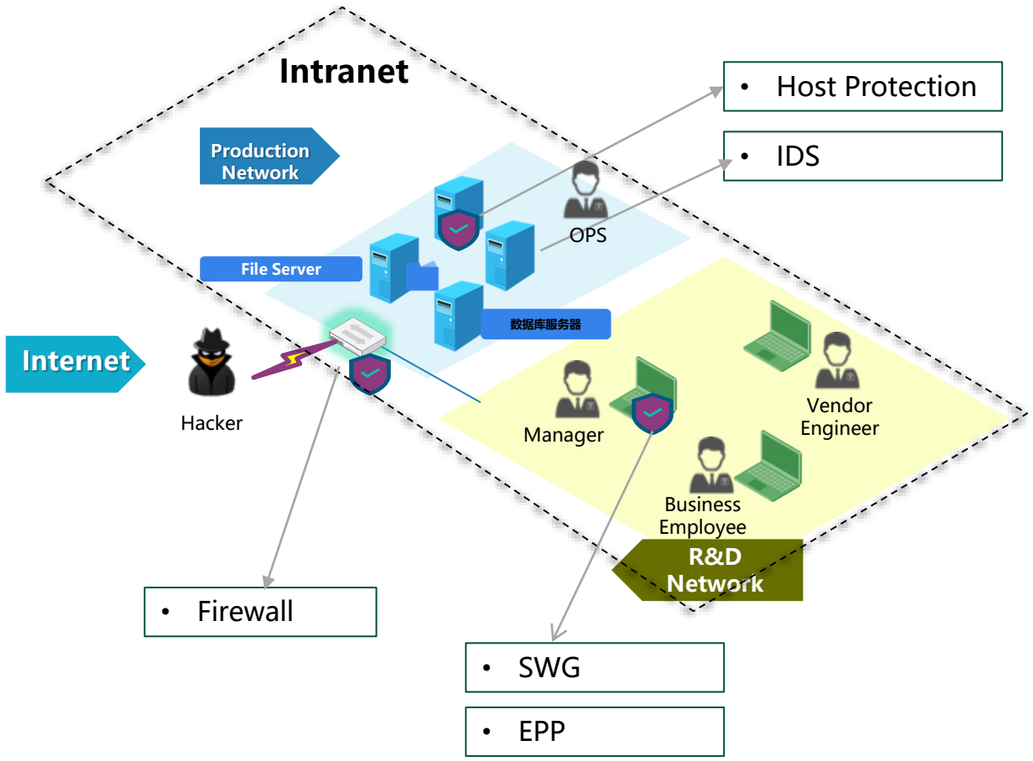
Security Parallel Aspect Definition

By embedding various layers of cut-off points in mobile APP, cloud application, operating system and other applications and infrastructure, a three-dimensional security protection system of device-pipe-cloud is formed, and security management and control are decoupled from business logic, and security is provided through standardized interfaces. The business provides internal vision and intervention capabilities, so as to achieve micro- and macro-perception coverage of network security and data security, and realize security attack and defense and security governance such as emergency response, loophole hemostasis, data security, and privacy protection.

Contribute by: Ant Group

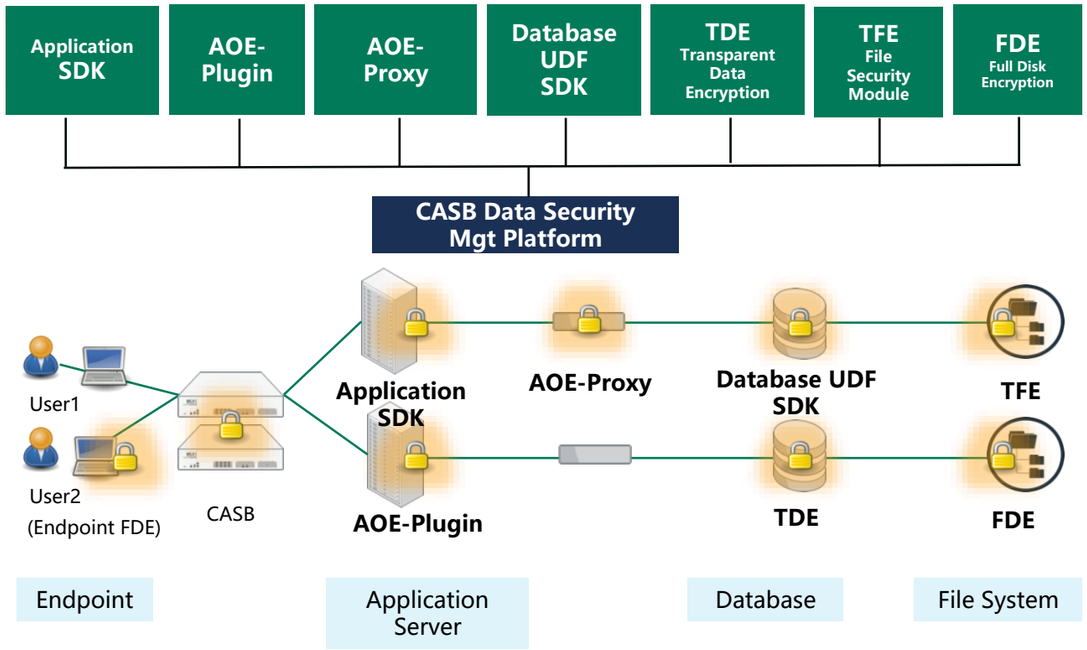
Network security "plug-in"

Block attacks and fix vulnerabilities for network tuples and content at endpoints and gateways

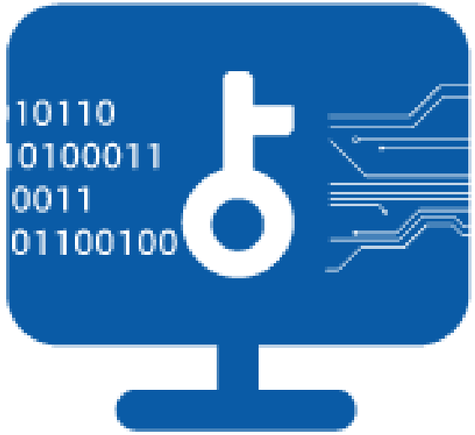


Data Security-Built In

At the control point of the application, security rules are rebuilt for flow-oriented full lifecycle data security



Looking into the future



Technology

Infrastructure
Architecture

Tools

Data Security
Operation

- Data Security will be a large industry that could compare with Cyber Security
- There are a lot of issues that should be addressed, from Academy, Industry to Government
- That will take at lease 5 to 10 years
- AI might help
- Big challenges and opportunities to the industry

Thank you!