2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

数据安全保障工程

主讲人：林明峰

CONTENTS
目 录

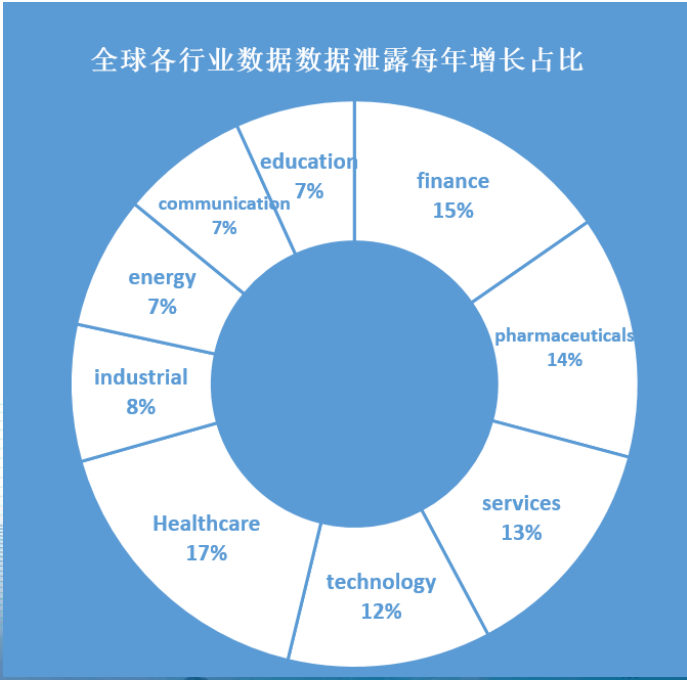
PART 01 数据安全保护面临的挑战
PART 02 数据安全保障工程建设框架
PART 03 数据安全治理体系架构设计
PART 04 数据数据安全工程建设解决方案
PART 05 数据安全保障工程建设蓝图

全球数据泄露事件案例

美国去年大概发生了1800起重大数据泄露事件，医疗行业成为重灾区，每条记录成本在408美元，其次是金融行业每条成本是206美元。

2018年12月17日，2万名FBI特工信息在网上泄露，英、美、法多国情报机构均受影响。

截止2019年1月统计的全球各行业数据泄露增长占比。由高到低依次是医疗、金融、药物、服务、技术。



全球数据安全保护现状

随着国家大数据战略的不断推动深化，大数据驱动的产业创新层出不穷，针对日趋严重的数据安全问题，**我国已经将数据安全纳入国家战略，保护国家数据主权。习近平总书记明确指出：“要依法加强对大数据的管理”**。2019年第十三届全国人大二次会议提出要尽快制定**《中华人民共和国数据安全法》**，明确数据安全法律责任，完善监管体系，保障国家安全、公民个人隐私权益和社会安全稳定。

欧盟《通用数据保护条例》（GDPR）

美国加利福尼亚州颁布了《2018年加州消费者隐私法案》

印度《2018个人数据保护法（草案）》

巴西《通用数据保护法》

法国《法国数据保护法》

俄罗斯《个人数据保护法》

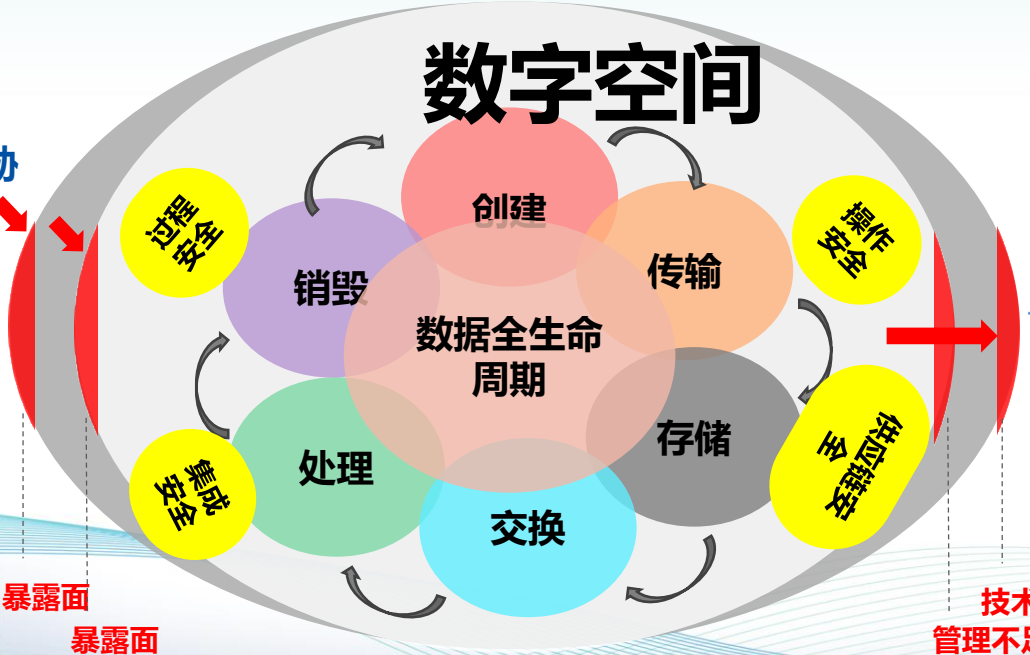
日本《个人信息保护法案》

风险语境下的数据安全治理

数据问题是数字时代的问题，数据安全是网络空间的安全！

国家级攻击
有组织攻击
经济利益组织
商业间谍
……

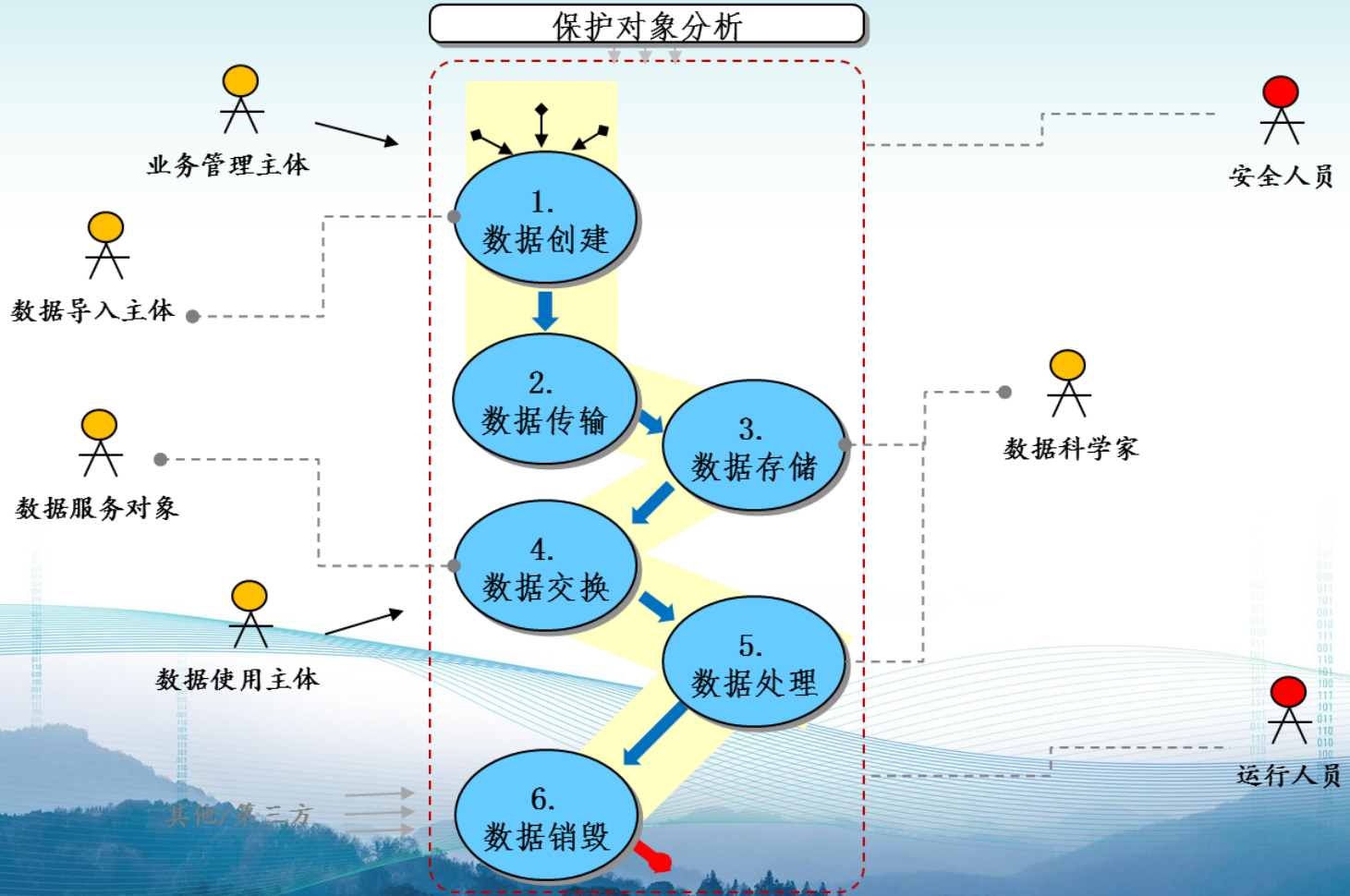
外部威胁



内部威胁

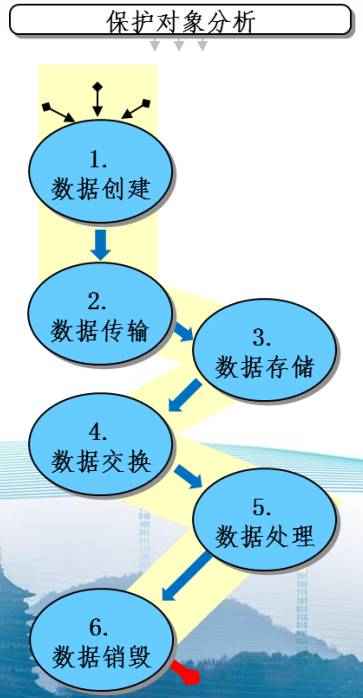
内部滥用
间谍活动
人为有意操作
人为无意操作
……

业务驱动的保护对象分析(1/4)

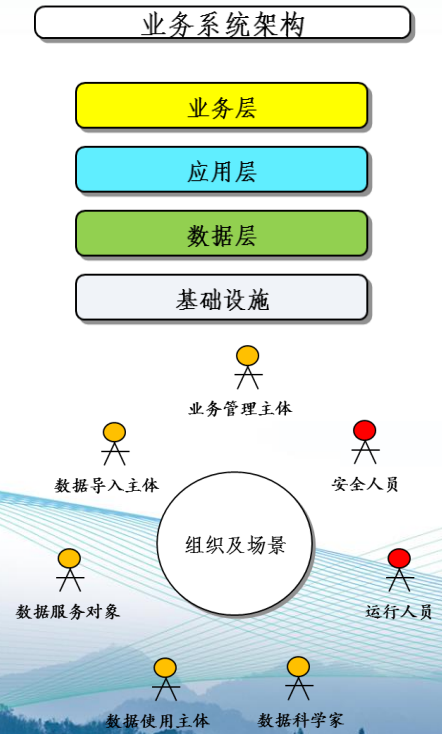


业务驱动的保护对象分析(2/4)

1.数据视角



2.业务视角



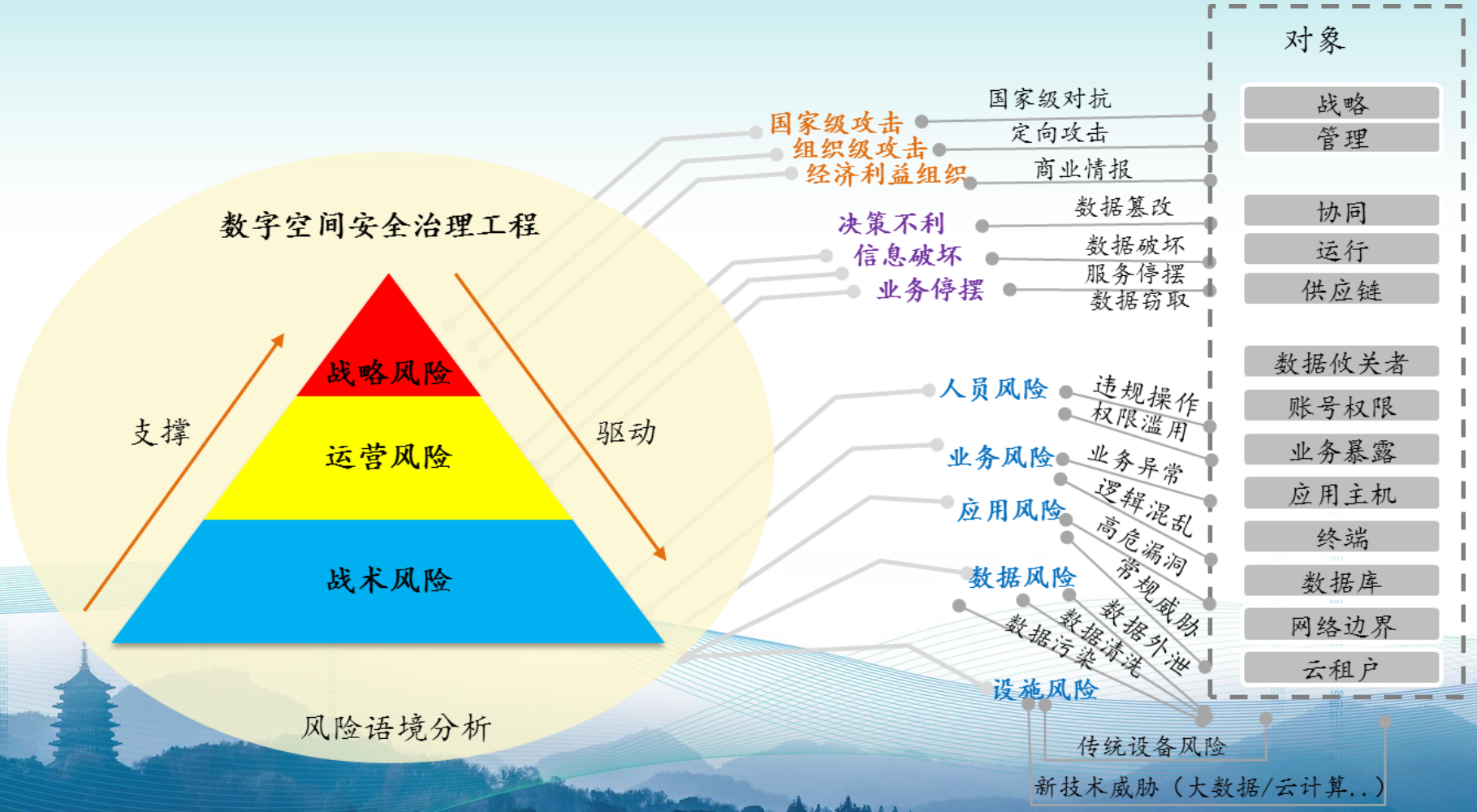
3.风险视角

业务驱动的保护对象分析(3/4)

4.合规视角

- 2014年4月15日习近平总书记在中央国家安全委员会第一次会议上正式提出“总体国家安全观”；
- 2016年11月7日全国人民代表大会常务委员会发布《中华人民共和国网络安全法》，2017年6月1日正式施行，落实国家总体安全观；
- 2017年8月，全国信息安全标准化技术委员会发布了《信息安全技术 个人信息去标识化指南（征求意见稿）》；
- 2018年5月1日，国家标准《信息安全技术 个人信息安全规范》实施；
- 2018年6月27日，公安部发布《网络安全等级保护条例（征求意见稿）》；
- 2018年11月30日，公安部网络安全保卫局发布《互联网个人信息安全保护指引（征求意见稿）》等。

业务驱动的保护对象分析(4/4)



CONTENTS
目 录

PART 01 数据安全保护面临的挑战
PART 02 **数据安全保障工程建设框架**
PART 03 数据安全治理体系架构设计
PART 04 数据数据安全工程建设解决方案
PART 05 数据安全保障工程建设蓝图

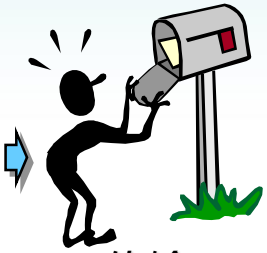
面向数据全生命周期的安全保障工程建设

采集

- 分类分级
- 秘密事项
- 秘密范围
- 密级标识
- ……

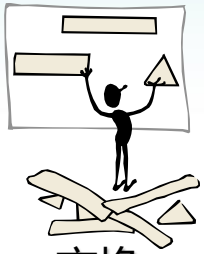
存 储

- 存储位置
- 存储/备份
- 保密期限
- 密源单位
- ……



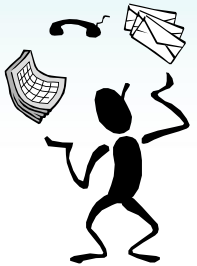
传输

- 知悉范围
- 授权/审批
- 网络/应用
- 介质/加密
- ……



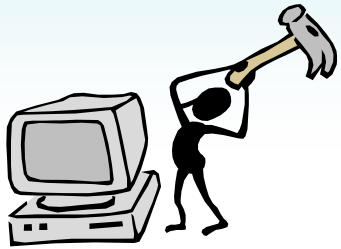
交换

- 知悉范围
- 授权/审批
- 密级修订
- 审核/备案
- ……



处理

- 知悉范围
- 身份/权限
- 操作
- 打印
- ……

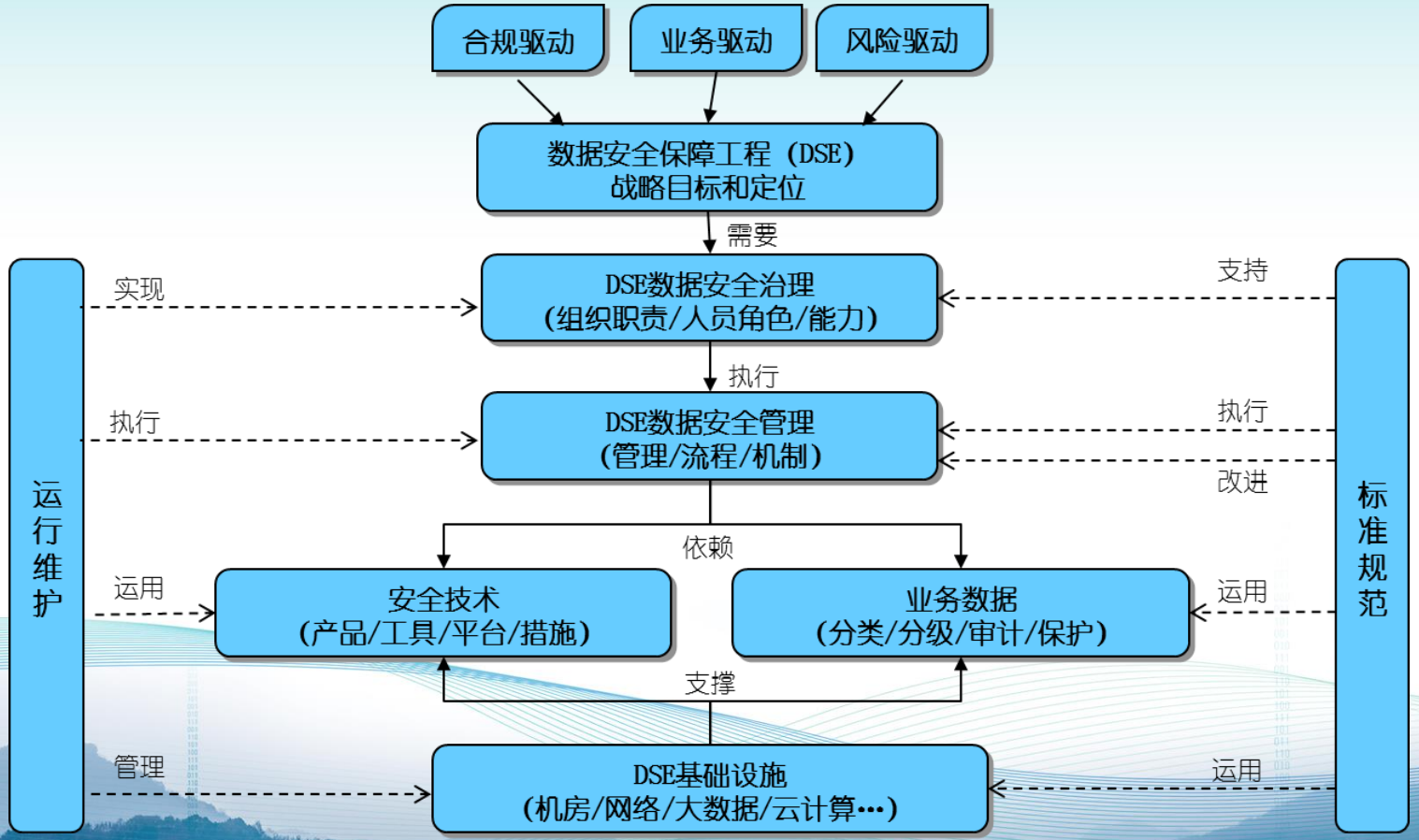


销毁

- 知悉范围
- 授权/审批
- 销毁方式
- 介质处置
- ……

数据安全保障工程建设

数据安全保障工程（DSE）框架

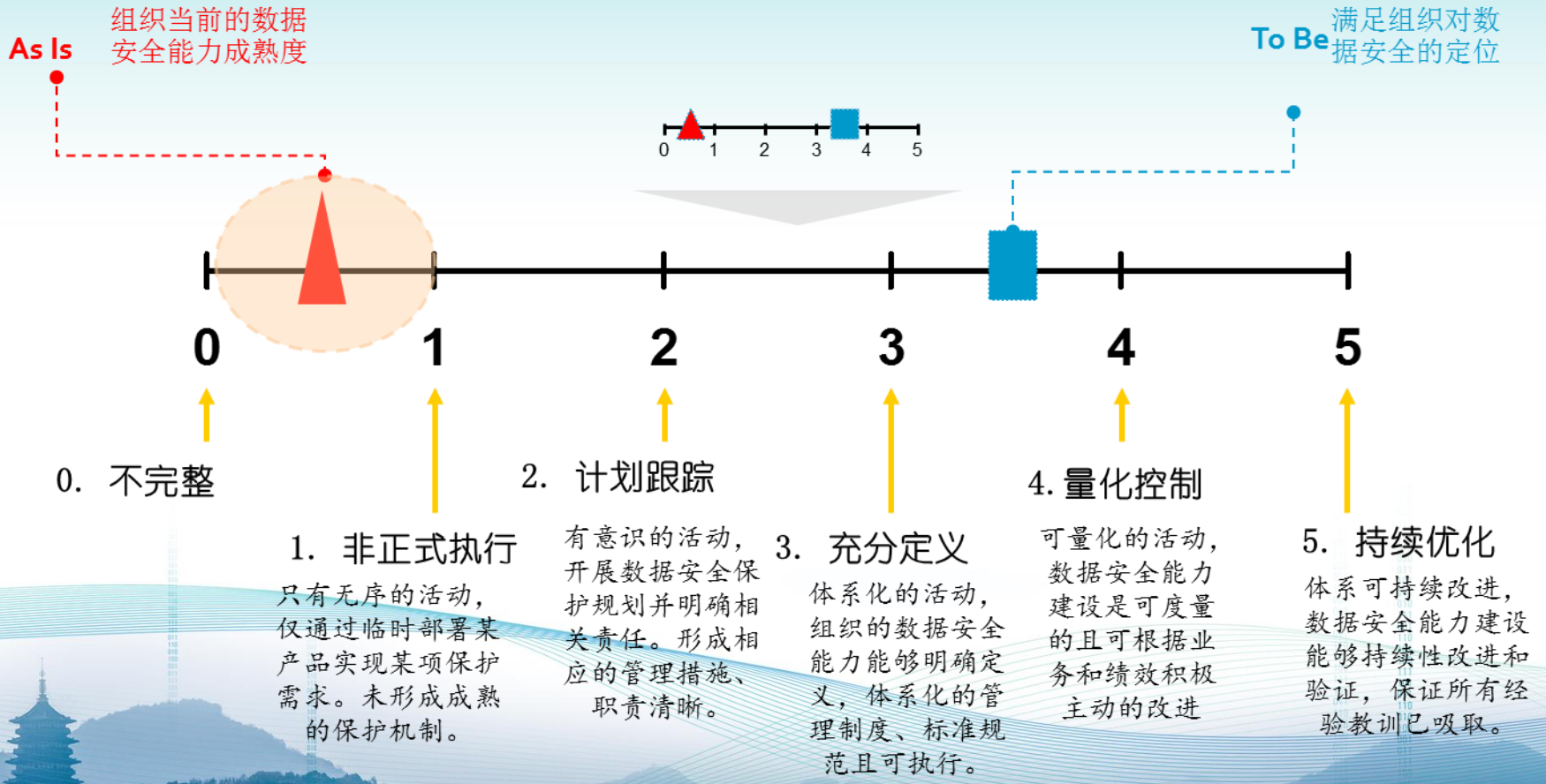


DSE能力成熟度模型，组织能力持续提升

数据安全工程能力成熟度模型
Data Security Engineering capability maturity model
（DSE-CMM）

组织（P）	过程（P）	技术（T）	数据（D）	智能（I）
数据治理组织 落实数据安全保护责任制	过程管理规范 管理过程制度和规范	安全技术措施 全面有效的保护措施	数据资产全貌 数据全生命周期	智能化处理 实现自动化处理
数据安全官 数据安全保护组织	过程管理体系 过程安全管理制度集	技术支持平台 3个”保障环”平台/系统/工具	业务数据管理 业务和数据风险并举	AI 植入人工智能基因

数据安全能力成熟度模型以及最佳实践

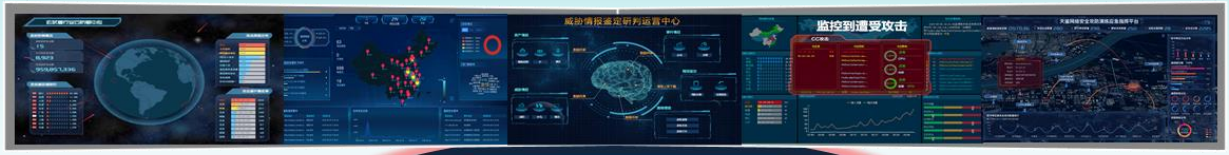


备注：参考《信息安全技术 数据安全能力成熟度模型》对级别的定义。

CONTENTS
目 录

PART 01 数据安全保护面临的挑战
PART 02 数据安全保障工程建设框架
PART 03 数据安全治理体系架构设计
PART 04 数据数据安全工程建设解决方案
PART 05 数据安全保障工程建设蓝图

数字空间大数据安全治理体系定位



数据空间：战略风险

网络空间：运营风险

物理空间：战术风险

数字空间安全态势感知中心
数据离境处理中心
大数据安全治理中心
国家数字空间大数据安全保障中心
P P T D I

政府 金融 企业 互联网 医疗 教育 能源 媒体
智慧城市“大数据安全保障中心”SaaS
行业大数据安全运营平台
大数据监测与管控平台
大数据资源池
智慧城市大数据安全保障中心

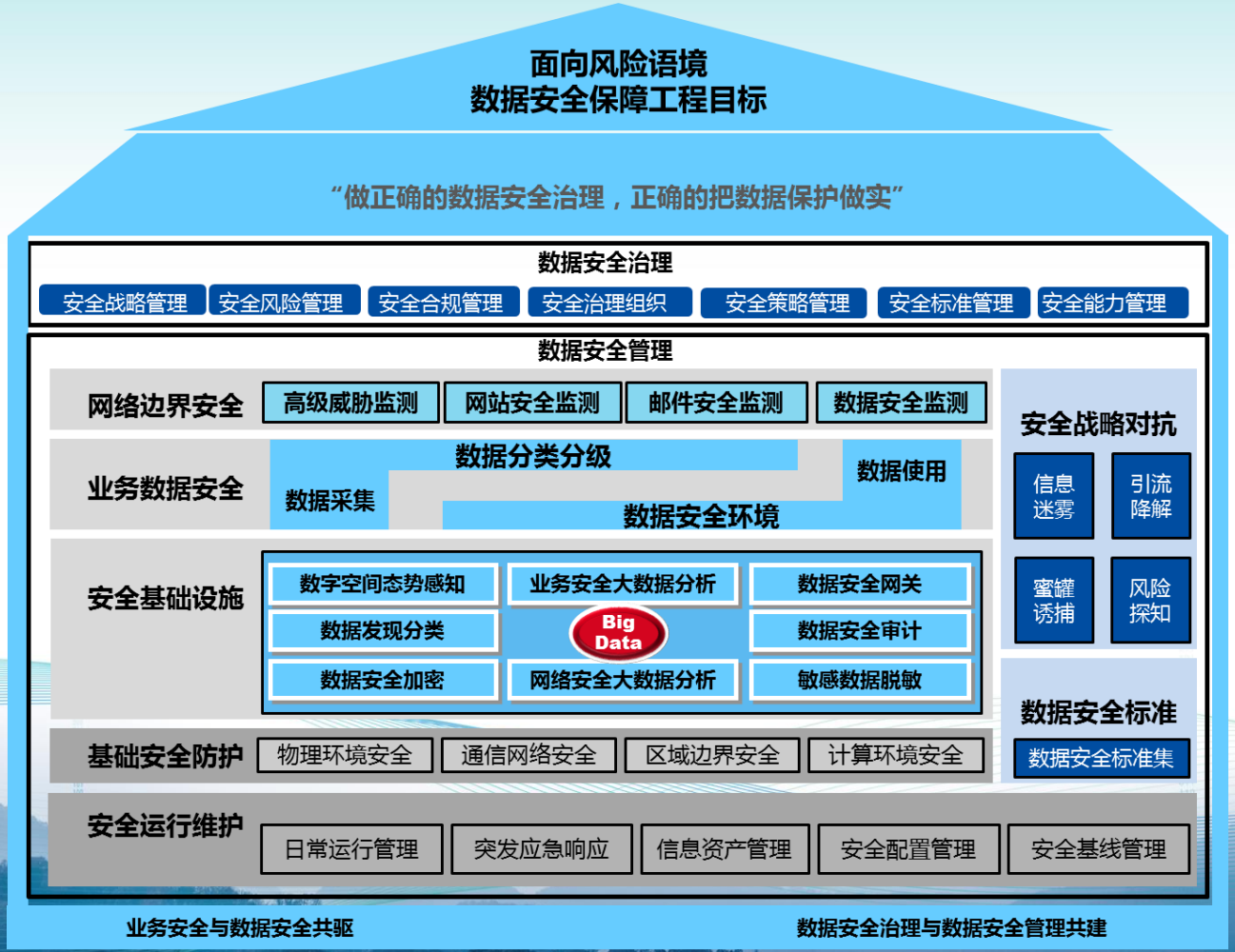
大数据安全保障能力建设
… 采集 存储 传输 交换 处理 销毁 …
基础大数据安全保障工程
政企大数据安全保障中心

境外攻击
战略对抗
数据治理
数据离境

智慧城市
重点行业
网络边界
业务数据
安全运营

安全能力
保障工程

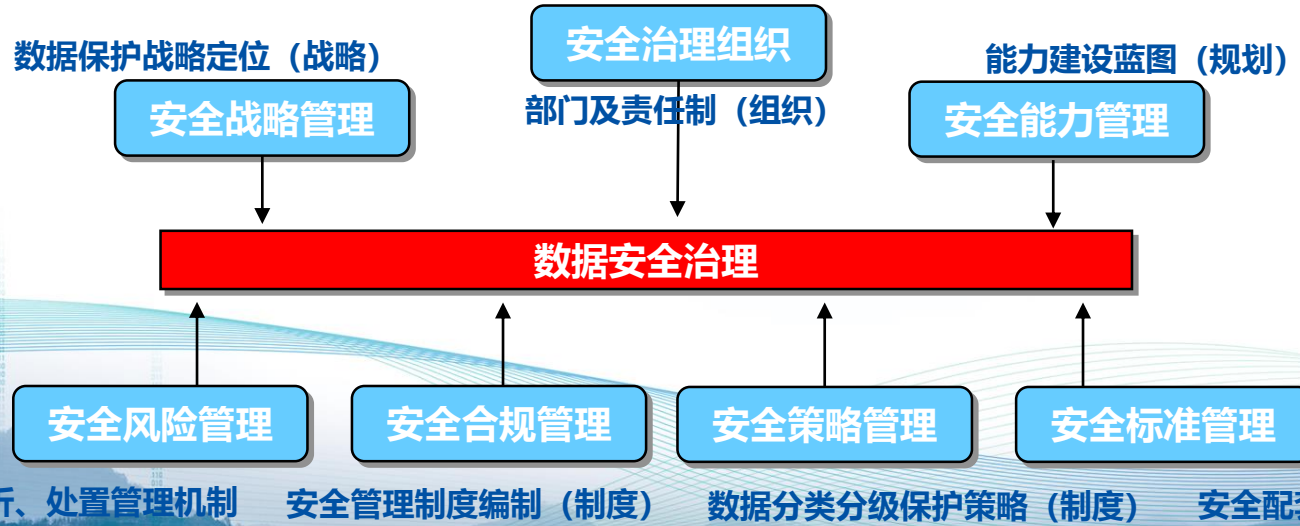
数据安全治理体系架构设计



数据安全治理

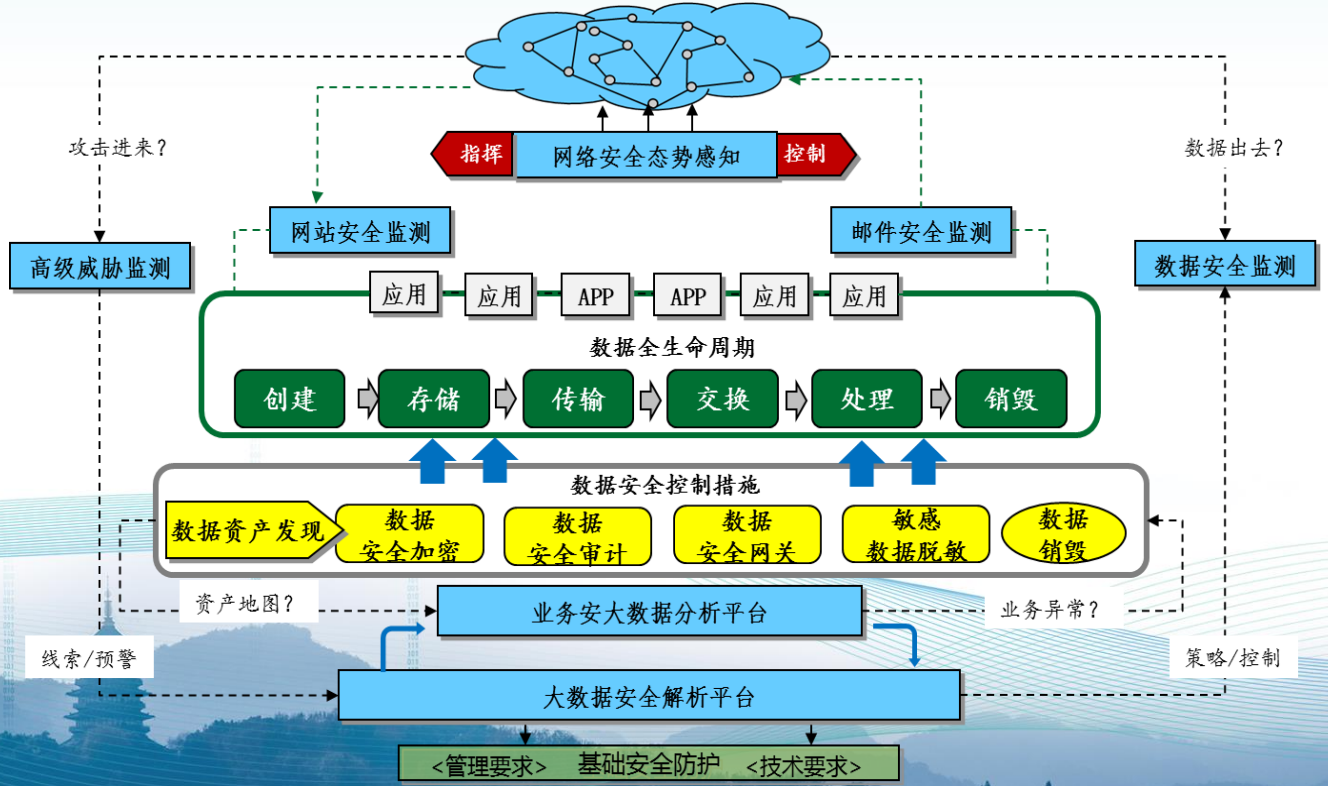
在风险语境下，“以业务安全为驱动，以数据安全为核心”，构建先进、科学、可行、合规的数据安全保障工程（Data Security Assurance Engineering，DSE）主要包括数据安全治理和数据安全管理。

数据安全治理：明确数据安全治理组织、职责并落实责任制，明确目标、内容、范围和策略。具体包括如下：安全治理组织、安全战略管理、安全风险管理、安全合规管理、安全策略管理、安全标准管理和安全能力管理。



数据安全管理体系

数据安全管理：核心是有效落实并实现组织（P）、过程（P）、技术（T）、数据（D）、智能（I）五大能力建设。具体包括如下：**安全战略对抗、业务数据安全、网络边界安全、安全基础设施、基础安全防护、数据安全标准及安全运行维护。**



“安全智能”
“协同防护”
“全局态势”
“主动防御”
“去灰色地带”
“管理能力提升”
“业务快速融合”

CONTENTS
目 录

PART 01 数据安全保护面临的挑战
PART 02 数据安全保障工程建设框架
PART 03 数据安全治理体系架构设计
PART 04 数据数据安全工程建设解决方案
PART 05 数据安全保障工程建设蓝图

建立数字空间保障环，应对战略风险

数字空间保障环

数据安全保障环

基础安全保障环

数据安全治理：

安全治理组织、安全战略管理、安全风险管理、安全合规管理、安全策略管理、安全标准管理、安全能力管理。

数据安全标准：

元数据管理、数据质量管理、数据安全管理、数据分类分级、数据共享、数据使用规范等。

安全战略对抗：

“主动防御和协同防御”技术，增强“扰乱、降解、欺骗”安全保障能力。蜜罐诱捕、信息迷雾、引流降解、风险探知。

建立数据安全保障环，应对运营风险

数字空间保障环

数据安全保障环

基础安全保障环

网络边界安全：

高级威胁监测、数据安全监测、网站安全监测、邮件安全监测。

业务数据安全：

数据分类分级基础之上，应用合理的数据安全措施，打造数据安全环境，才能保证获得数据安全可用的治理效果。

安全基础设施：

数据资产发现、数据安全网关、数据安全审计、敏感数据脱敏、业务大数据安全分析、网络安全大数据分析、数字空间态势感知。

建立基础安全保障环，应对战术风险

数字空间保障环

数据安全保障环

基础安全保障环

基础安全防护：

依据国家网络安全等级保护和关键信息基础设施安全保护，以及个人信息安全规范、个人隐私保护、数据出境、数据交易服务等安全要求，明确政企在数据安全的建设需求,结合政企信息安全现状，形成体系化的规划方案，从而构建基础安全保障技术框架。

安全运行维护：

由于数据安全保障工程（DSE）的复杂性、可行性和可维护性，DSE由规划建设，转为后期的安全运行维护均需要有较为专业的安全服务支持。重点从日常运行维护、突发应急响应、信息资产管理、安全配置管理、安全基线管理五个方面形成着力点。

CONTENTS
目 录

PART 01 数据安全保护面临的挑战
PART 02 数据安全保障工程建设框架
PART 03 数据安全治理体系架构设计
PART 04 数据数据安全工程建设解决方案
PART 05 数据安全保障工程建设蓝图

DSE解决方案视图

数据安全保障工程建设蓝图（DSE）

安恒信息 DAS-SECURITY 安全中国

DSE解决方案价值


目标
治理体系
数据安全
保障工程
落地
重点行业
智慧城市
国家安全
国家数字空间大数据安全保障中心
智慧城市大数据安全保障中心
政企大数据安全保障中心
大数据安全治理联盟

安恒信息解决方案优势

安恒信息
DAS-SECURITY 安全中国

你值得信赖的合作伙伴！

- 行业应用安全和数据安全领导者；
- 数据安全治理工程（DSE）提出者；
- 根据12年的应用和数据安全经验和案例保障DSE有效落地，保证政企数据安全。

- 全智能数据资产发现和分类，有效简化政企跨部门数据责权协调和管理复杂度；
- 复杂业务数据场景安全智能分析，快速发现业务异常行为和数据违规操作；
- 基于“零信任”的访问控制网关，保证数据“可用不可见、可控可追溯”；
- 全新打造“网络空间、数字空间、物理空间”三位一体的新一代安全保障体系。

数据安全展望

我们的使命：AI赋能安全，让安全无忧

- 能力覆盖
- 数据资产可视
- 数据隐私保护
- 数据交换管控
- 数据风险追溯

- 核心步骤
- 数据分级分类
- 数据动态鉴权
- 数据安全保护
- 数据应急处置

- 关键价值
- 资产梳理策略制定
- 过程控制
- 追溯溯源
- 持续优化

- 数据库安全
- 数据库审计
- 数据库安全网关
- 数据库加密

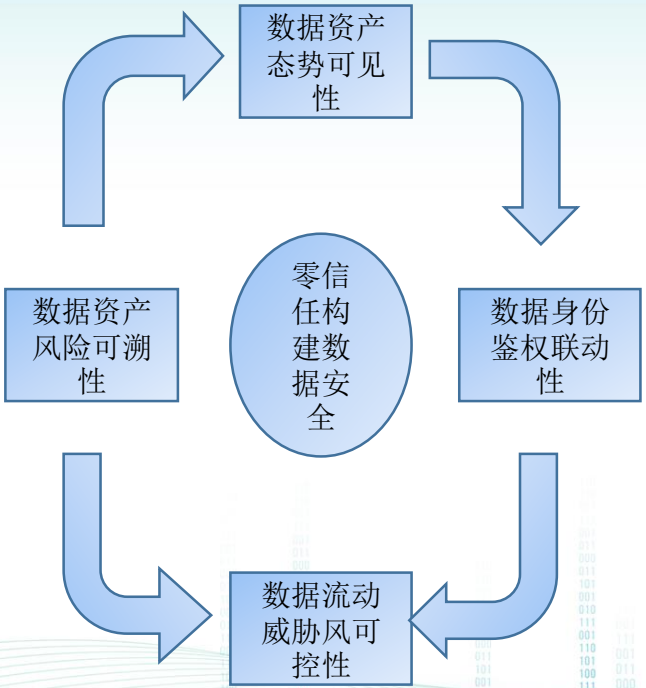
- 数据保护
- 数据动态鉴权
- 数据脱敏
- 数据水印

- 数据治理
- 数据资产梳理
- 数据分级分类
- 大数据监管平台
- 数据治理风险平台

有道可循，有依可循
UEBA落地数据安全场景

方法论

- 基于数据生命周期做数据治理
- 基于零信任做数据安全保护



数据安全治理目标

外部数据交换场景

数据操作审计

识别流动的敏感数据内容
识别敏感数据透出的应用和URL
识别获取&查看和操作数据的行为
关联使用的账号和IP

数据风险

谁获取了那些敏感数据
谁操作了那些关键标识的数据
高风险涉敏应用和URL
敏感数据流动量级和来源去向
可能高危的数据行为

数据管理

涉敏应用和透出面管理

行为监控

行为和敏感内容溯源

数据资产

数据库

大数据集群

可见：数据资产

可知：敏感数据

数据安全态势

数据安全全局态势地图

内部业务操作场景

资产梳理

数据服务&数据资源
账号&权限
数据操作权限

风险感知

可能高危的数据行为
谁操作和导出那些敏感数据

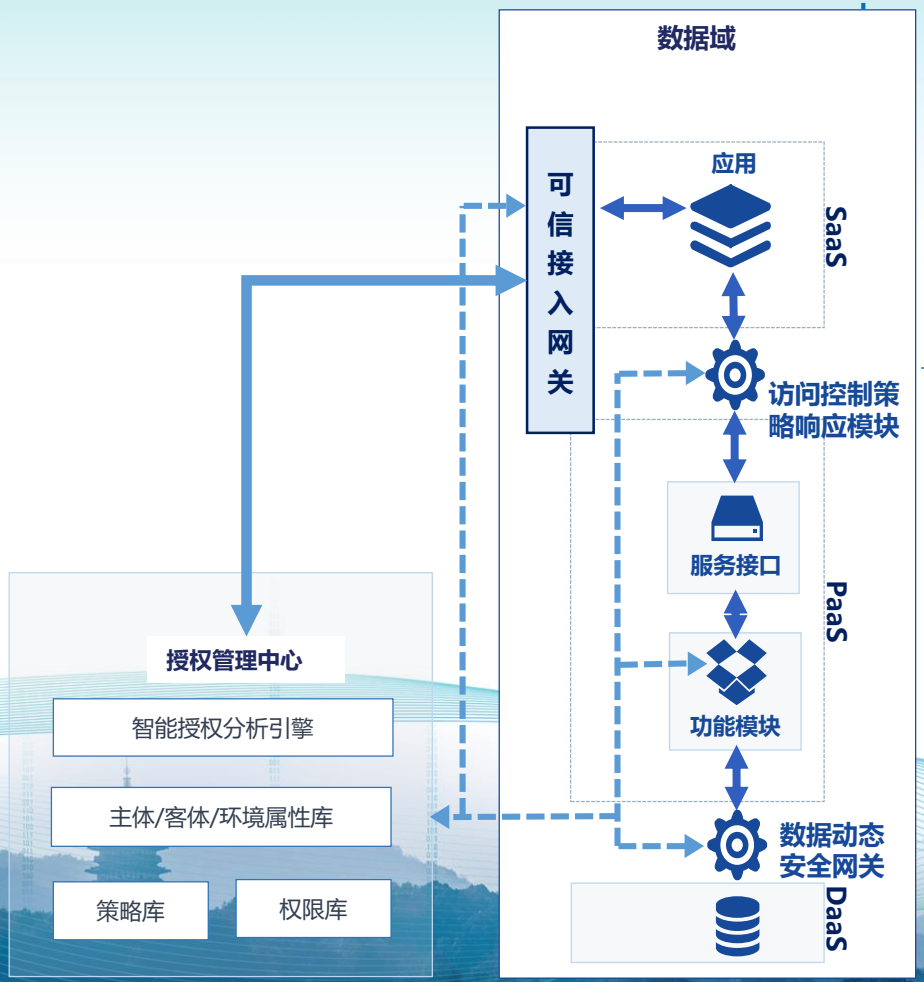
访问鉴权

统一服务&账号管理
基于资源细粒度权限分发管理

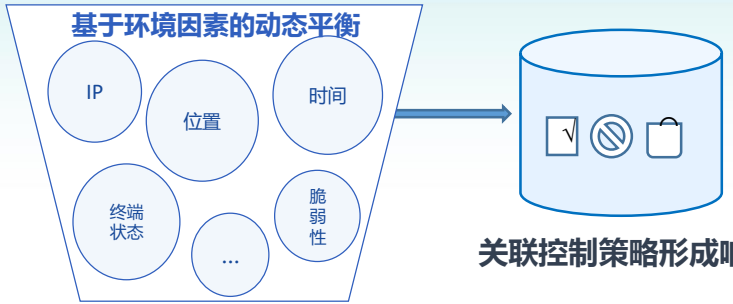
数据保护

动态行为控制策略
动态脱敏
行为和敏感内容溯源

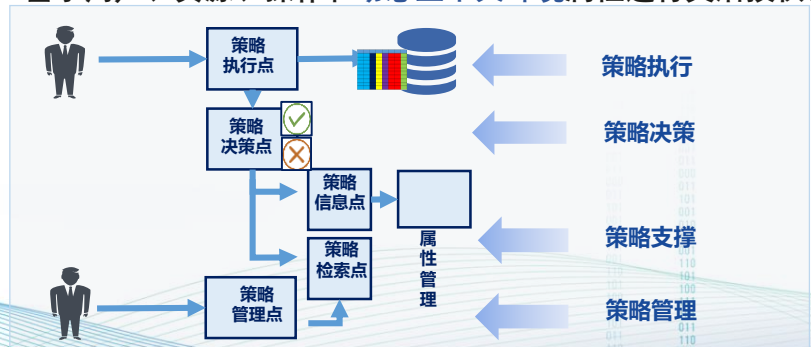
鉴权是数据交换的关键



基于属性的访问控制策略响应模块



ABAC（Attribution Based Access Control，基于属性的访问控制）：基于用户、资源、操作和动态上下文环境属性进行灵活授权。



主体属性：
- ❖身份
- ❖角色
- ❖职位
- ❖部门
- ... ...

客体属性：
- ❖分级标签
- ❖分类标签
- ❖行
- ❖列
- ... ...

动作属性：
- ❖允许(增删改查)
- ❖禁止(增删改查)
- ❖... ...

环境属性：
- ❖是否本人在终端前使用；
- ❖是否有人围观；
- ... ...

THANK YOU

谢　　谢　　观　　看