



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

CSA Summit

云安全联盟峰会



数字新基建时代的云数一体化安全防护

演讲人：毛俐旻

Contents

01 安全防护新趋势

02 云数一体安全防护设计

03 航天科工安全中台实践

01

- 2018年8月，工信部《推动企业上云实施指南（2018-2020年）》：推动企业加快数字化、网络化、智能化转型。
- 2020年4月，国家发改委、中央网信办印发《关于推进“上云用数赋智”行动培育新经济发展实施方案》，提出以企业数字化转型为主线，加快推进数字产业化和产业数字化步伐。
- 2020年4月，国家发改委明确新型基础设施范围，提供数字转型、智能升级、融合创新等服务的基础设施体系。

02

- 2017年6月，《中华人民共和国网络安全法》正式实施，鼓励开发网络数据安全保护和利用技术。
- 2017年7月，国家互联网信息办公室发布《关键信息基础设施安全保护条例（征求意见稿）》
- 2019年10月，十三届全国人大常委会第十四次会议《中华人民共和国密码法》
- 2020年7月，第十三届全国人大常委会第二十次会议审议《中华人民共和国数据安全法（草案）》，坚持维护数据安全和促进数据开发利用并重。



数字新基建
安全新挑战

标准规范

- 美国国家标准与技术研究所NIST
2015 发布 SP 1500 《NIST 大数据互操作框架》系列标准,
2018 年 完成第二版编制工作, NIST SP 1500-4 《安全与隐私保护》
- ISO/IEC 大数据工作组 (WG9)
20547 《大数据参考框架》, 20547 -4 《安全与隐私保护》
- ITU-U 国际电信联盟
2018年, 《大数据安全与隐私过程》、《数据资产管理框架》、《大数据基础设施评测框架》正式立项



数据安全发展现状及趋势

● 2018 Gartner数据安全治理框架 (DSG)

从业务风险分析出发，对业务的各个数据集进行识别、分类和管理，并针对数据集的数据流和数据分析的机密性、完整性、可用性创建安全策略。

● 2018 Microsoft 数据治理框架 (DGPC)

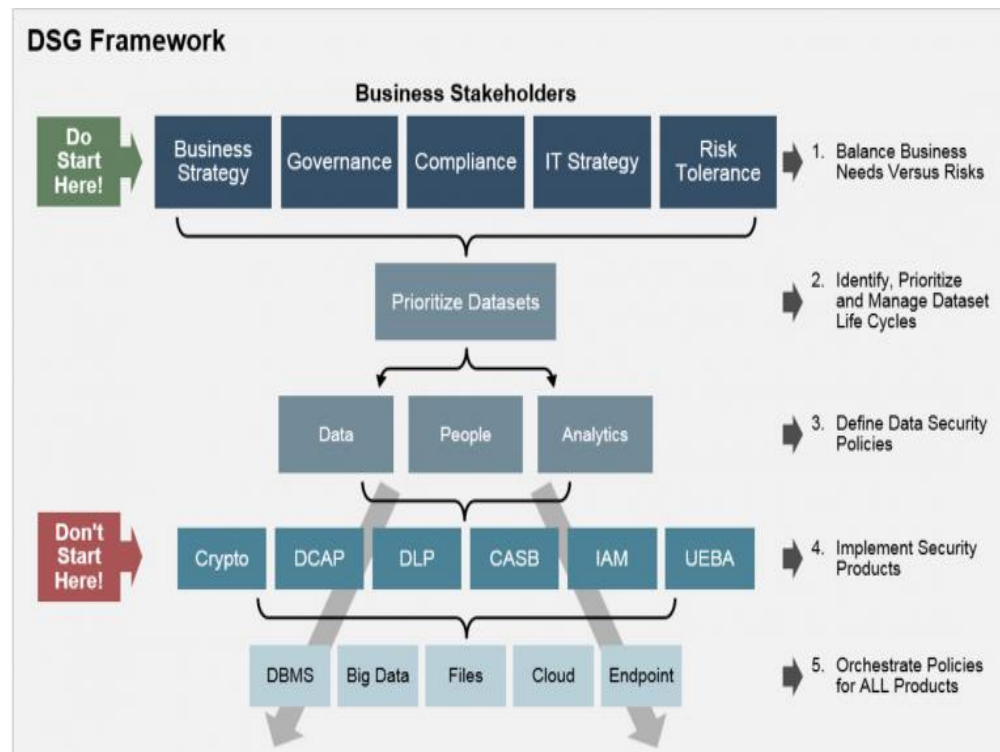
针对隐私、保密和合规性，从人员、流程、和技术三个角度出发，识别和管理与特定数据流相关的安全和隐私风险需要保护的信息。

● 2019 Gartner七大安全和风险趋势

领先的企业组织正在利用数据安全治理框架来确定数据安全投资的优先等级；
云已成为主流计算平台，领先的企业组织正在投资并完善其云安全能力；
持续自适应风险与信任评估 (CARTA) 的战略安全方法开始出现在传统网络安全市场
.....

● 2020 RASC

大会主题是“HUMAN ELEMENT(人为因素)”，趋势：产品设计、开发和运营安全，软件工程流程安全DevSecOps、合规与隐私、安全框架等

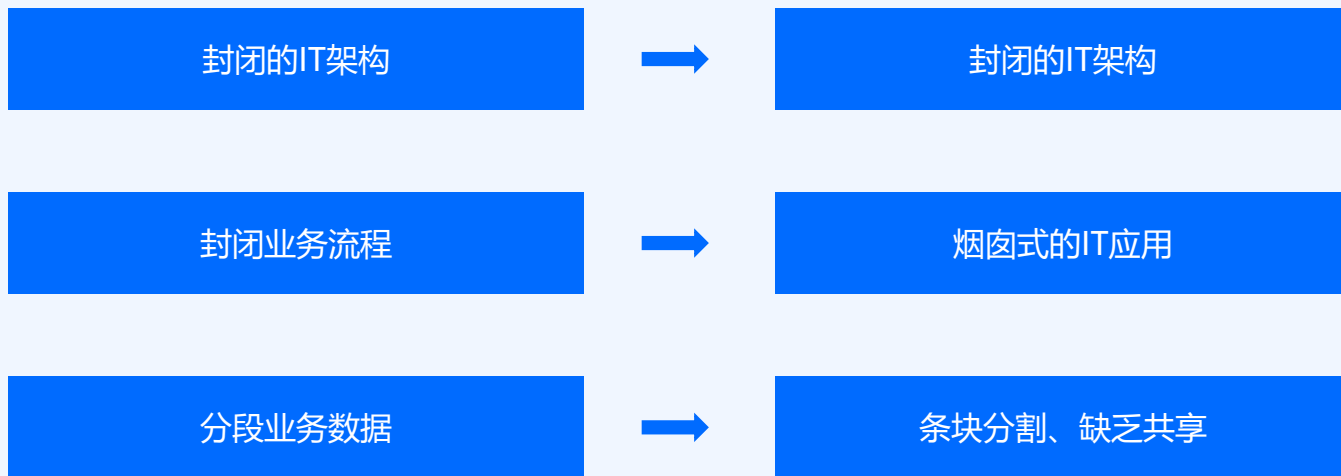


数字化转型：传统IT架构向云数一体架构转变

企业数字化转型的基石是技术架构变革,构建云+大数据的数字底盘,实现**平台赋能、资源共享、能力复用**

传统IT架构——“系统+系统”模式,

在原有业务系统的基础上,不断开发新的业务系统,导致“烟囱林立”、复杂臃肿、迭代缓慢、交付低效。

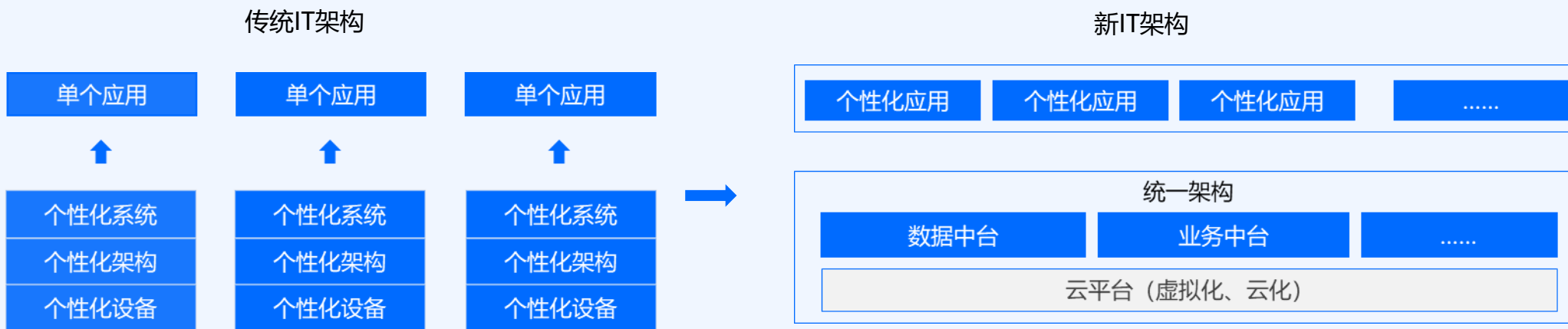


数字化转型：传统IT架构向云数一体架构转变

企业数字化转型的基石是技术架构变革，构建云+大数据的数字底盘，实现**平台赋能、资源共享、能力复用**

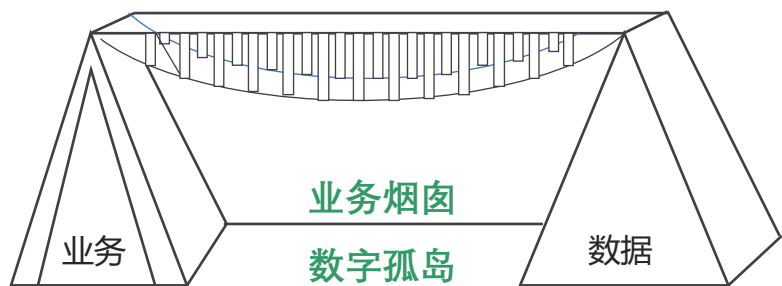
云数一体的新型IT架构 —— “系统之系统” 模式，

实现各业务系统和解决方案的云化迁移，实现敏捷开发、快速迭代、高效交付、及时响应。



新架构、新需求、新安全

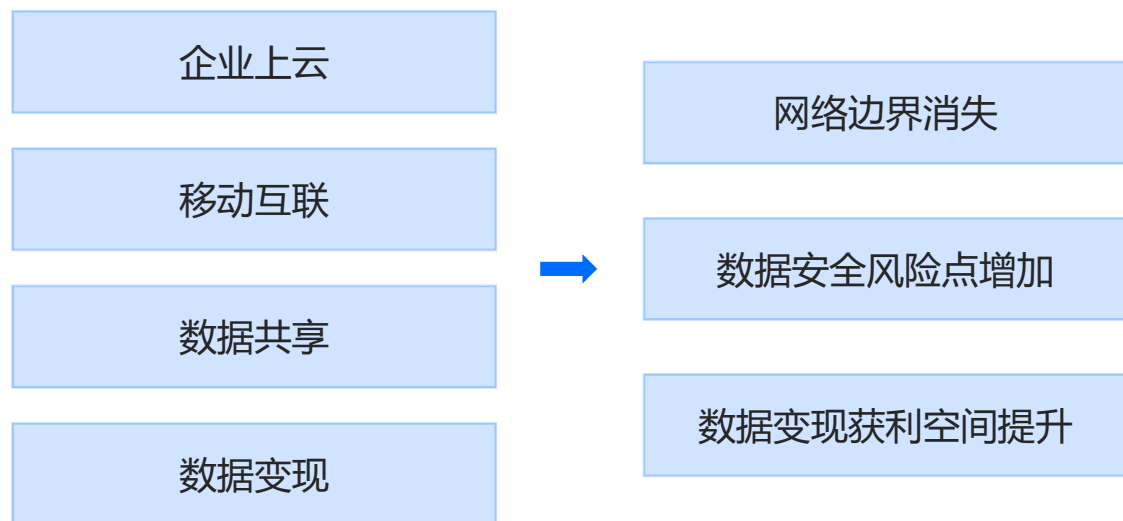
数字化转型：传统IT架构向云数一体架构转变




中台战略
→



新基建时代的数据安全 以数据为核心，云数一体



“

上市公司每起网络数据泄露事件的平均损失为
1.16亿美元
”

以数据为核心的云数一体化安全防护

安全中台 共性能力 要求

安全服务
标准化

安全能力
集成化

安全流程
规范化

安全防护
一体化

云数一体 安全防护 能力要求

基础软硬件
平台安全

安全服务
及数据
分级分类

数据声明
周期安全

云原生数
据安全

Contents

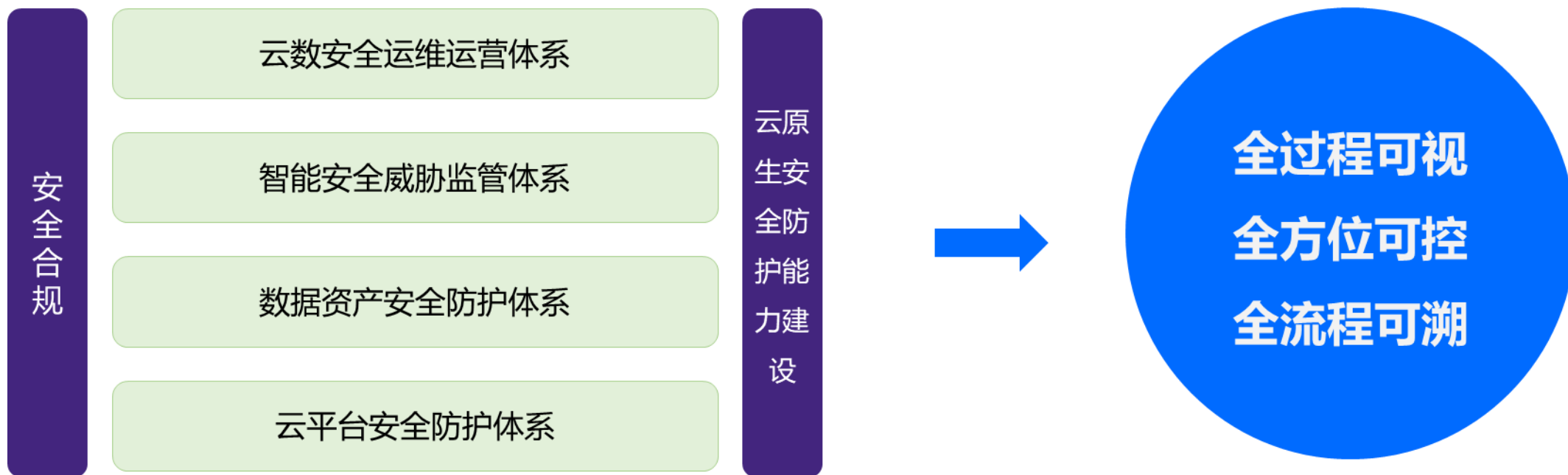
01 安全防护新趋势

02 云数一体安全防护设计

03 航天科工安全中台实践

以数据安全为核心的云数一体化安全防护

设计理念



云安全——软件定义、弹性扩展、安全合规



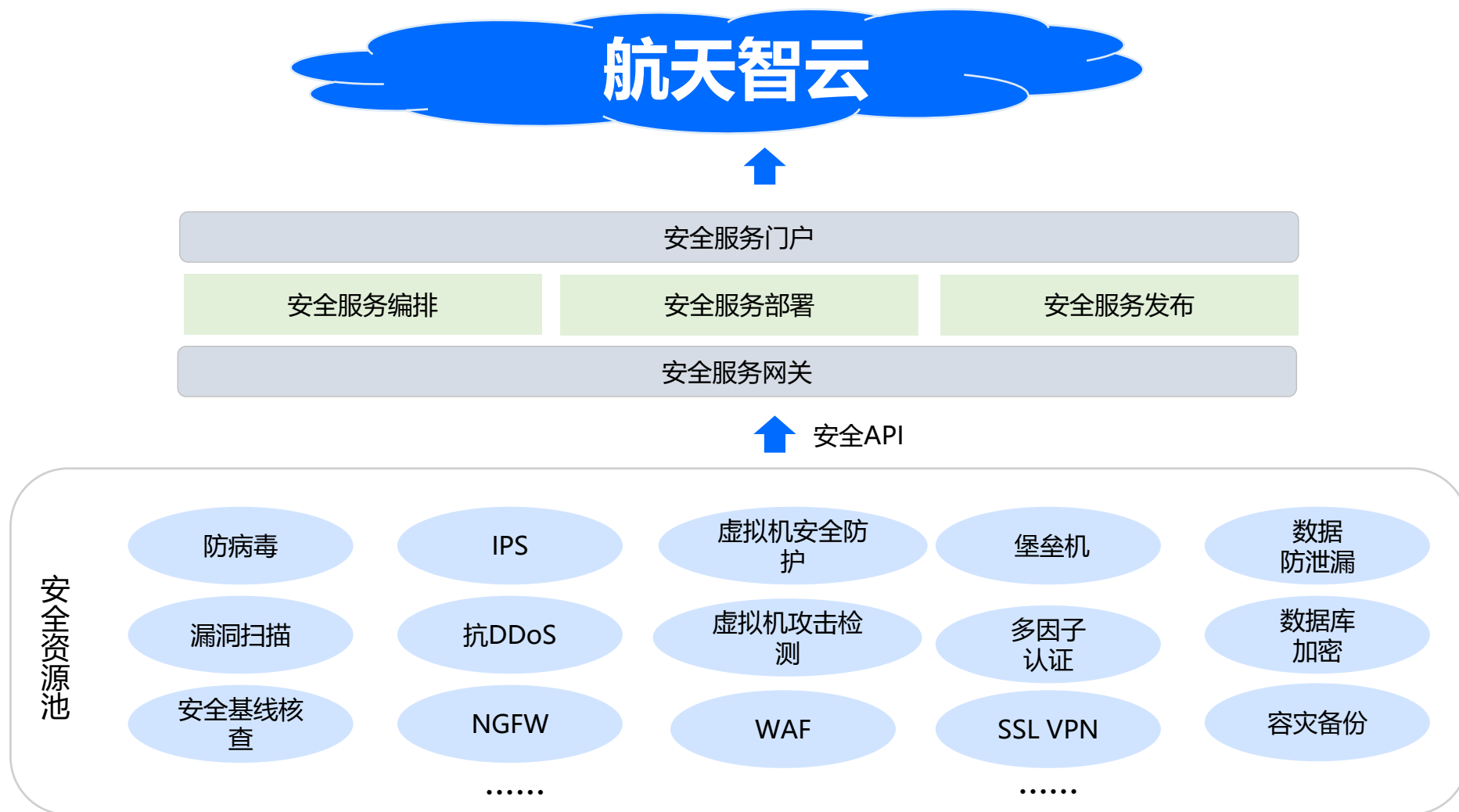
云安全——软件定义、弹性扩展、安全合规



安全服务 可编排可扩展

云安全服务管理平台

虚拟化安全资源池



- 保护国家数据资产
- 保护商业秘密
- 保护个人隐私

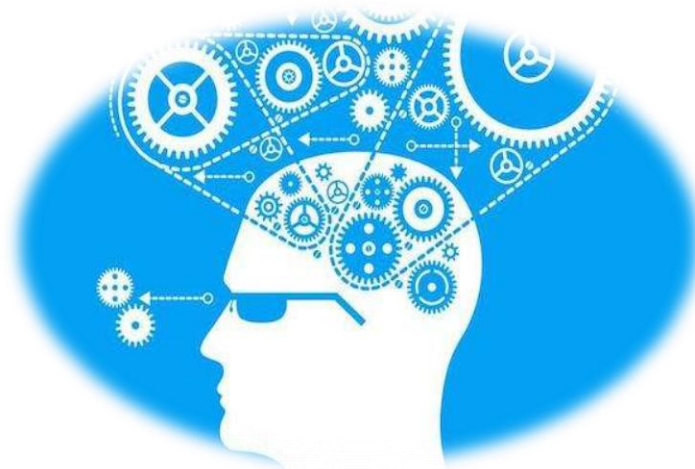


人工智能+大数据

- 分级分类安全管控
- 合理开放安全共享
- 跨网跨域安全交换
- 数据服务监测审计
- 数据销毁彻底清除

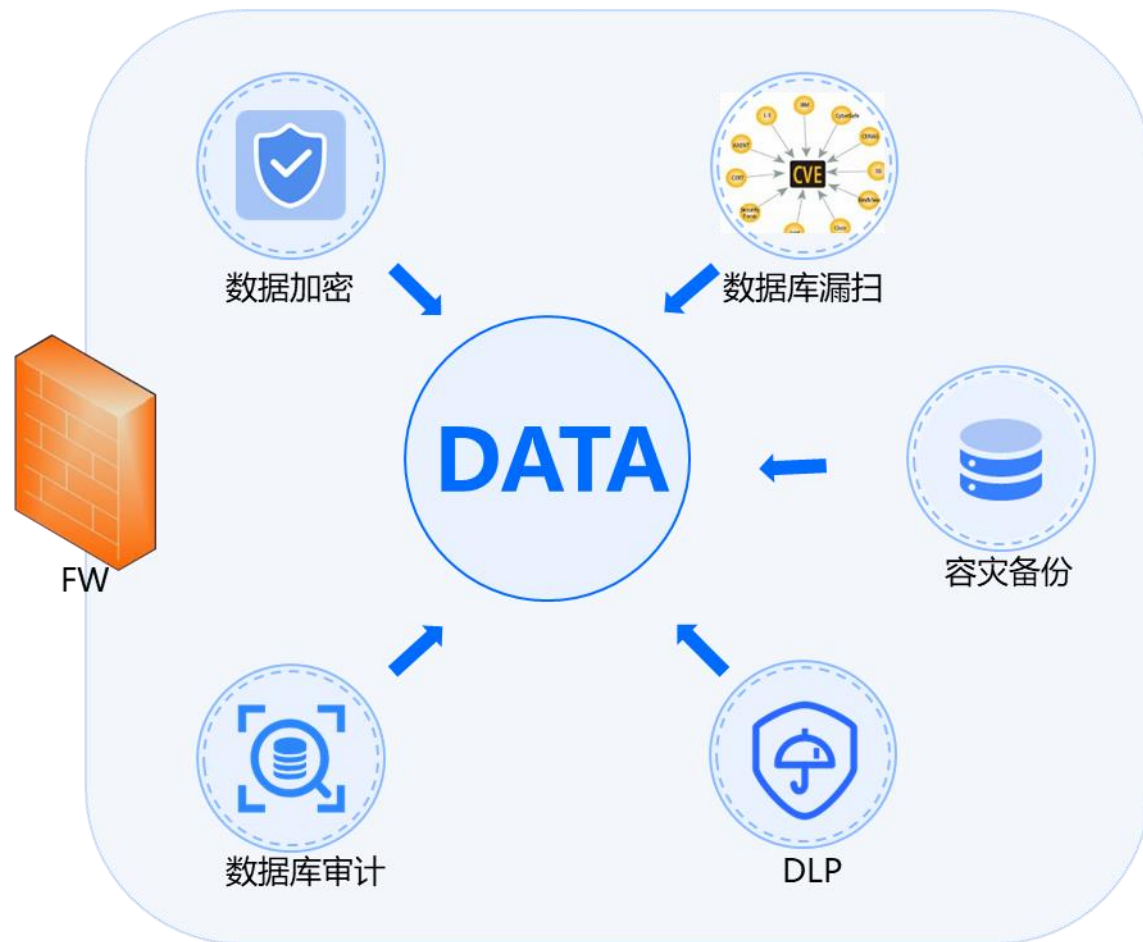
网络空间安全

数据全生命周期安全



传统数据安全 以DBMS为中心的防护

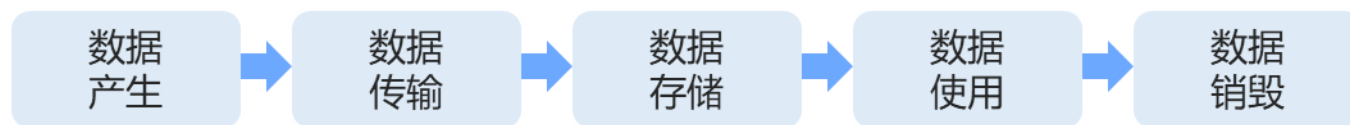
- **防护理念**: 传统网络安全防护理念, 边界防护、入侵防范
- **防护对象**: 重点针对静态数据 (data at rest), 以数据库为核心, 针对结构化数据的安全防护
- **防护模式**: 单点设备的集成



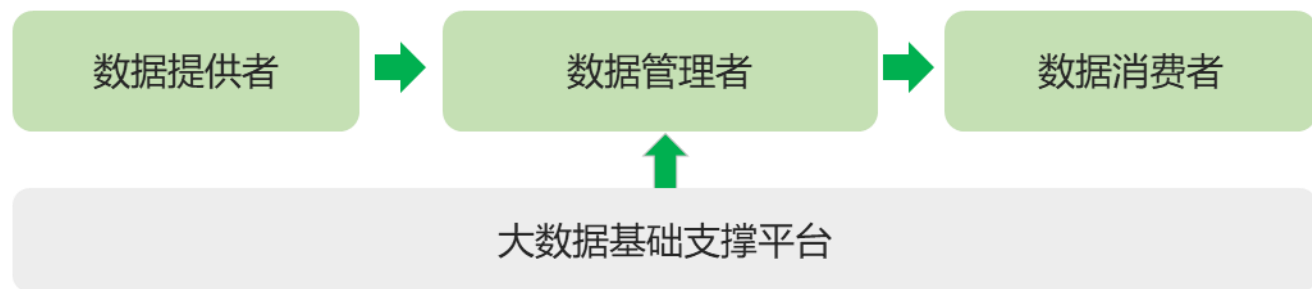
新基建时代的数据安全—— 数据生命周期动态安全防护

- 防护理念：一体化的动态防护
- 防护对象：动态数据（data in transit 数据频繁跨域流动）
- 防护模式：多维视角（主体、客体、场景） / 全生命周期过程

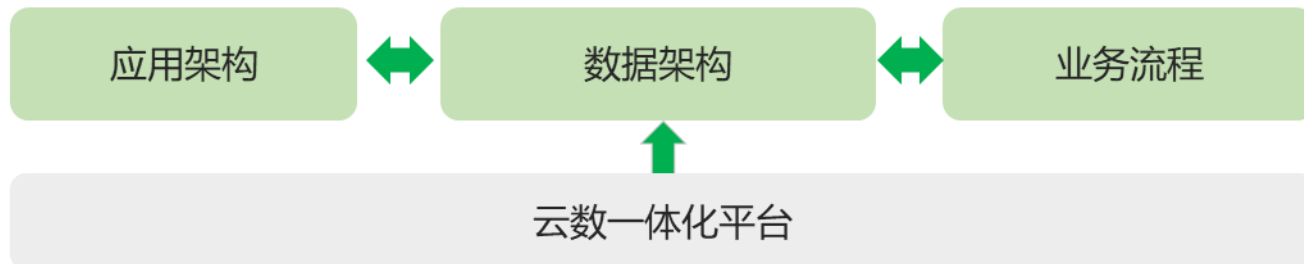
(1) 客体：数据——生命周期过程



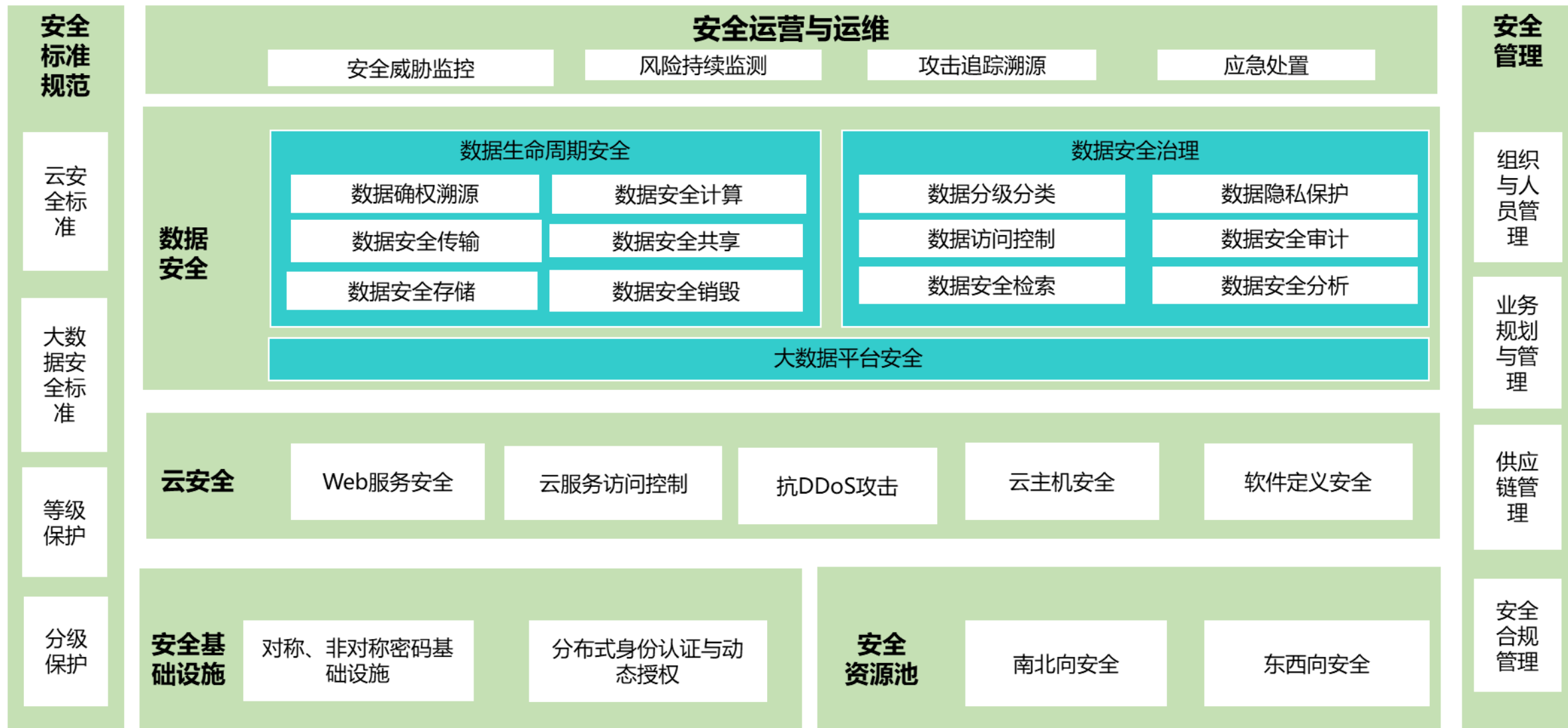
(2) 主体：人——数据生命周期过程参与者



(3) 场景：



云数一体化安全防护设计





平台等保合规

GB/T 22239-2019

信息安全技术 网络安全等级保护基本要求 云计算安全扩展要求 ——满足等级保护三级要求

- ◆ 安全物理环境
- ◆ 安全区域边界
- ◆ 安全管理中心
- ◆ 安全通信网络
- ◆ 安全计算环境



网络安全审查

“面向政府部门的云服务网络安全管理”标准 ——为政府领域的客户提供安全合规的云服务

Contents

01 安全防护新趋势

02 云数一体安全防护设计

03 航天科工安全中台实践

数字化转型——航天科工集团IT架构变革

航天科工集团IT架构整体设计 ——云五网N平台M应用

规范引领、领域创新平台赋能、共享复用

统一平台架构、支撑企业数字化转型：

· 基础云平台--航天智云平台：

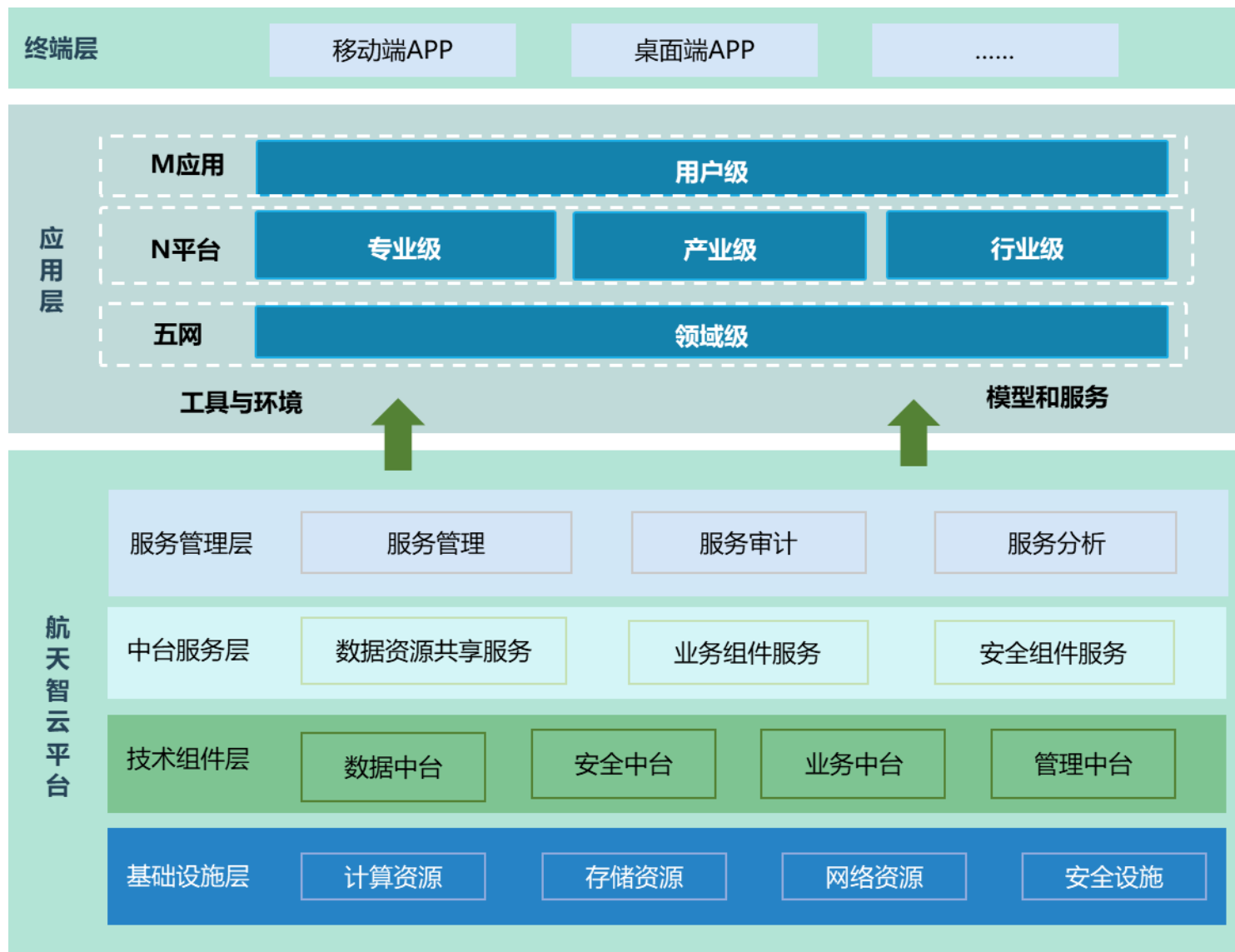
- 作为集团基础云平台，为“五网N平台M应用”的建设和运行提供开发工具、运行环境、业务模型及服务。

数据基础设施--数据资源共享服务平台：

- 为上层业务提供数据服务，实现数据共享交换和能力复用，使静态数据流动并鲜活起来。

安全中台：

- 提供动态安全服务，保障云安全、大数据平台安全、数据生命周期安全。



数字化转型——航天科工集团IT架构变革



航天智云平台

云数智一体化平台

数据中台:

数据全链路治理开发

业务中台:

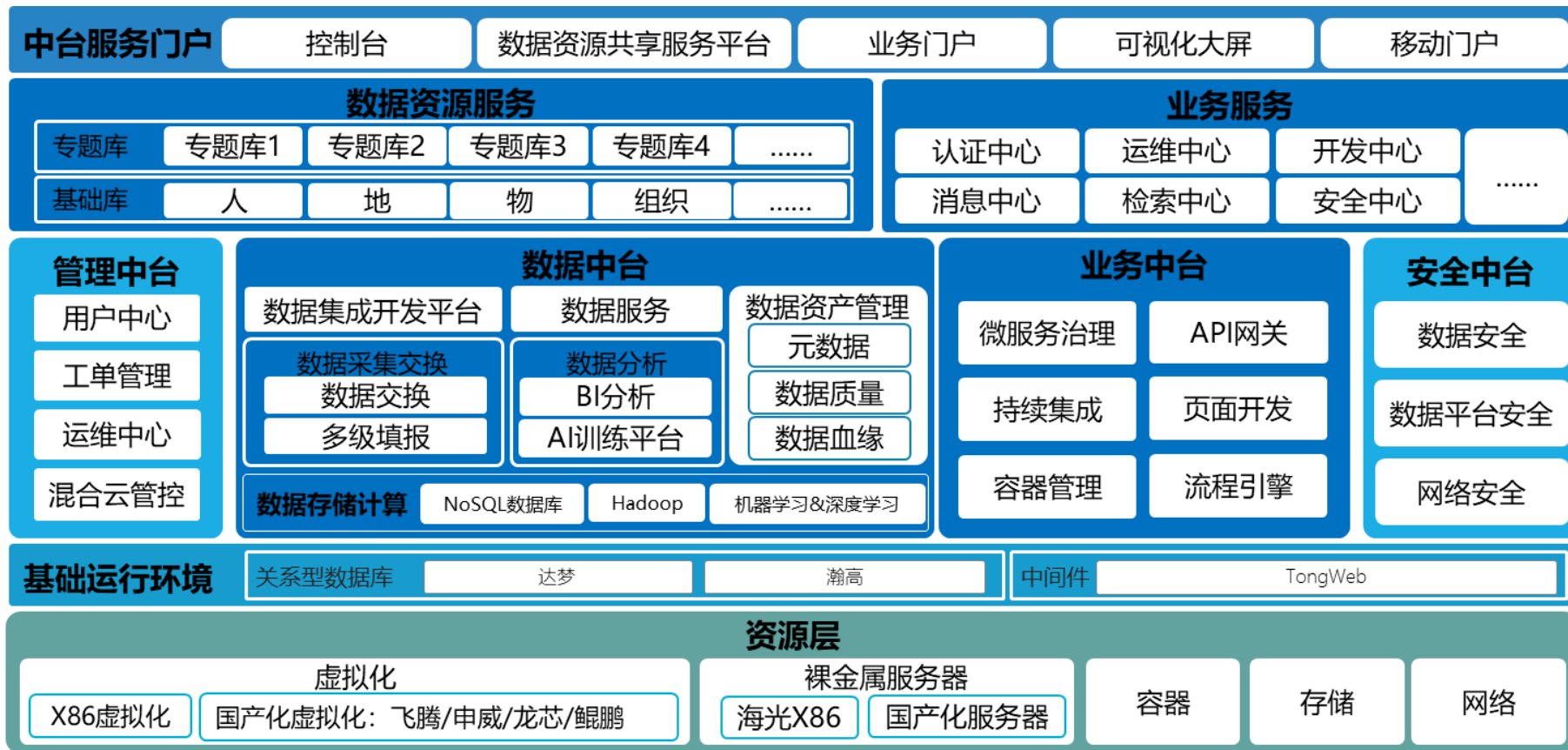
业务可视化敏捷构建

管理中台:

管理运维高效自动化

安全中台:

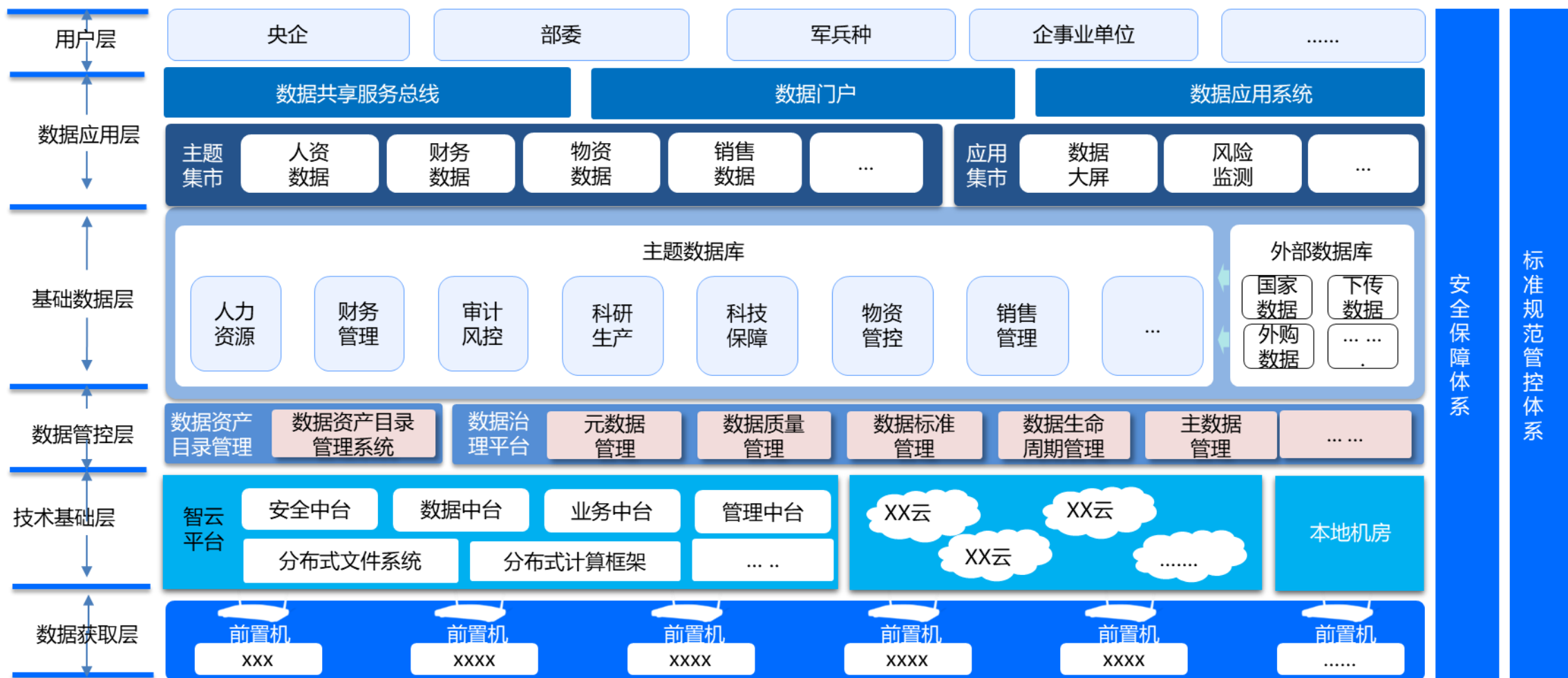
安全智能感知



云原生安全、自主可控

数字化转型——航天科工集团IT架构变革

数据中台--数据资源共享服务平台



数据中台--数据资源共享服务平台

清底数、立标准、建平台、构服务

- 数据资产盘点与规划：进行数据盘点，建立全局数据资源目录；
- 数据资产获取与存储：多渠道获取数据，进行数据标准化，实现数据集中管理；
- 数据服务与能力构建：以数据资产目录为核心，提供统一、标准、高质量的数据服务。

数据资源 “可知、可查、可管、可用”



数据中台——数据资源共享服务平台

数据资源目录设计

数据资源目录是实现数据资源安全合理共享、业务有效协同的基础。参考国家政务信息资源目录、国家电网、中石油、中石化等企业数据治理经验，开展数据资源目录设计和盘点，为数据安全治理提供支撑。

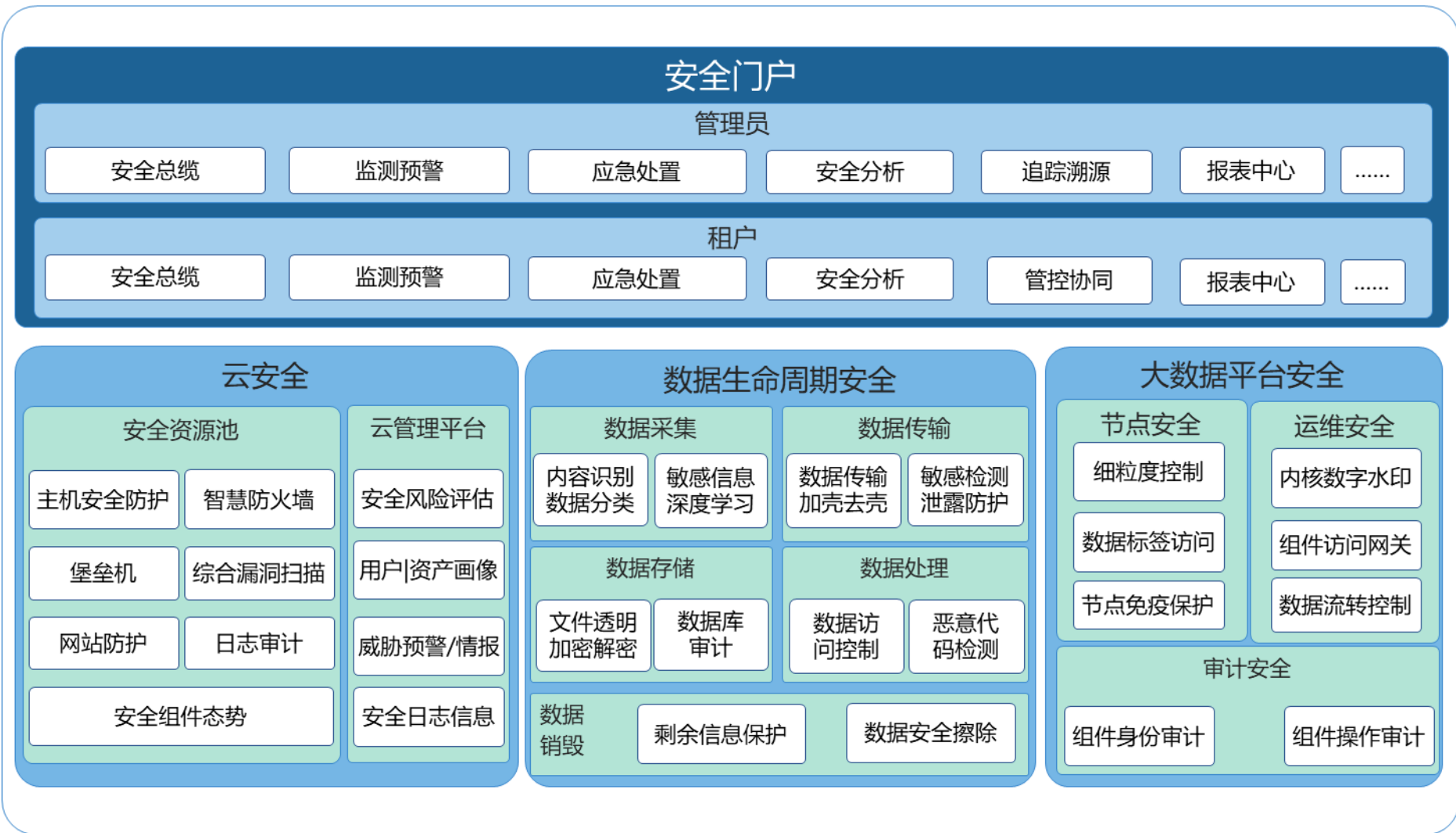
资源分类		资源分类扩展属性				数据资源管理属性						数据资源技术属性						数据资源开放共享属性				数据项技术信息			
一级分类	二级分类	所属业务域	所属业务组件	所属主题域	对应本期主题库	资源名称	资源描述	采集范围	提供方	归口部门	敏感级别	资源格式	资源状态	所在网络	来源系统	来源表	更新周期	共享级别	共享条件	共享方式	开放范围	数据项名称	数据类型	数据长度	是否脱敏
1		2				3						4						5				6			

安全中台 = 可信计算环境 + 云安全 + 数据安全

安全中台面向云平台管理员、租户，借助40余款（虚拟化）安全产品覆盖业务、运营、数据、网络、应用、主机、账号、虚拟化等8个维度，囊括了数据采集、传输、存储、使用、销毁的全生命周期。安全中台具备策略、服务编排能力，管理员/租户可以自主、灵活选择和配置适用于业务场景、数据场景的安全产品与服务。



数字化转型——航天科工集团IT架构变革



感: 资产感知、威胁感知

传: 全面采集、融合汇聚

智: 智能分析、研判预警

控: 全域管控、应急处置

对外提供定制化安全服务

对内提供整体安全防护

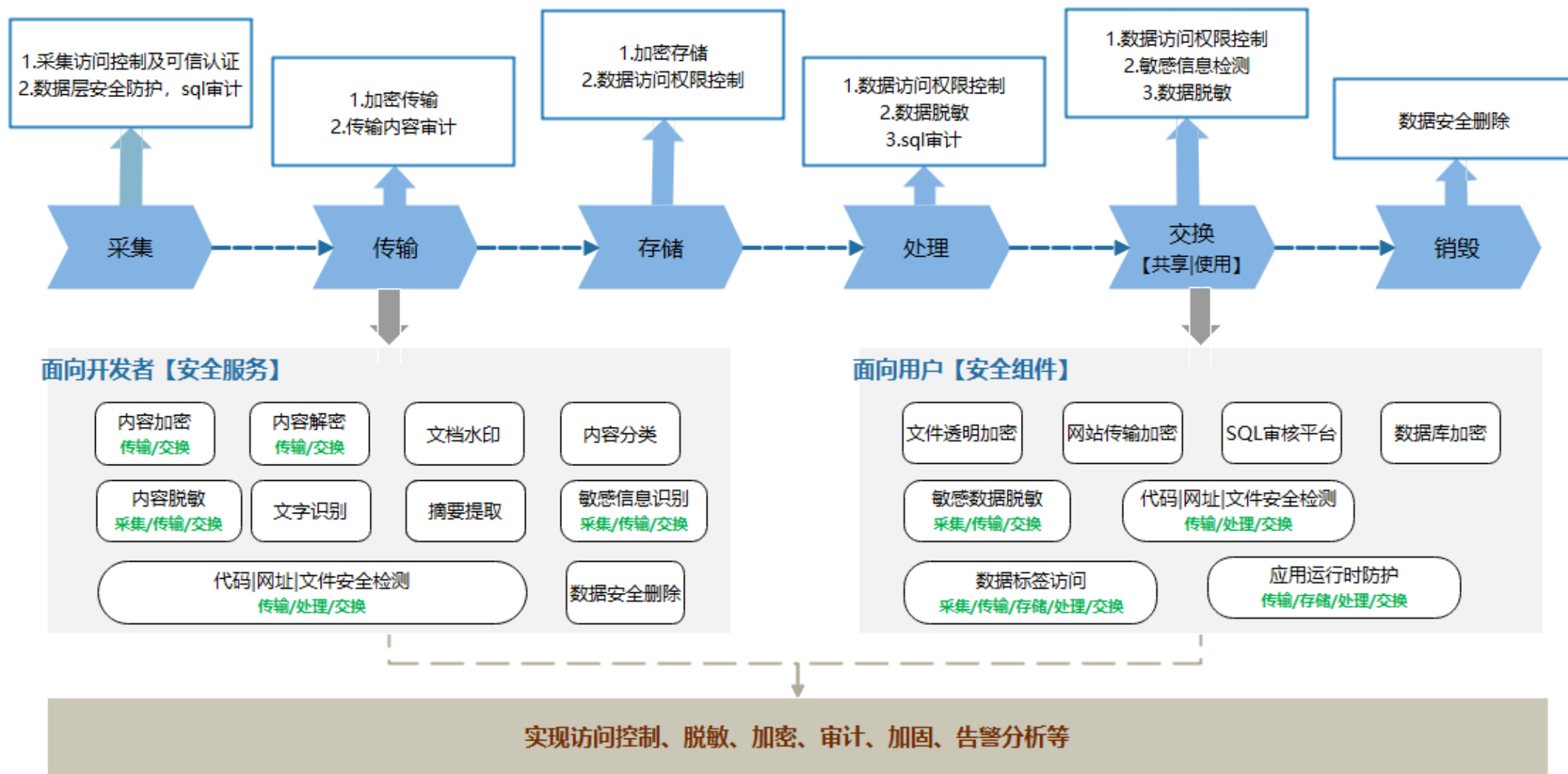
云数一体化安全防护服务——云安全服务

资源池化安全组件，实现按需使用及弹性伸缩【云化模式】

安全门户为租户提供基于云安全的自服务门户。租户可以通过自助门户快速便捷地进行安全组件的购买、续费、扩容、策略管理等功能，全面满足租户按需使用、快速部署、安全可靠、专业服务的安全需求。



云数一体化安全防护服务—数据生命周期安全服务



云数一体化安全防护服务—数据生命周期安全服务

大数据安全可视化平台



- 数据全生命周期风险展示
- 汇总各子系统数据安全风险数据，统一分析，动态生成安全策略

大数据交换安全防护系统



- 共享节点多因子认证，防止数据非法外流
- 基于流量、协议、应用、内容的多维分析，阻断高危会话
- 数据流实时风险展现，及时预警

大数据节点安全防护系统



- 数据节点透明加解密，窃取数据也无法使用
- 终身免疫勒索病毒，确保数据不被病毒损毁
- 防止合法或非法人人员违规访问大数据节点
- 防止合法或非法人人员“拖库”窃取数据
- 防止合法或非法人人员篡改、损毁数据

大数据审计安全防护系统



- Hive、Hbase等Hadoop核心组件全面审计
- Oracle、SQLServer、MySQL、人大金仓、达梦、神州通用等传统数据库审计
- 智能分析与高危操作阻断
- 敏感数据脱敏，保护用户隐私

大数据运维安全防护系统



- 多因子认证，禁止非法终端接入
- 拍屏/截屏/录屏泄密防护
- 数据文件落地加密，脱离安全环境无法使用
- 共享文件外发安全防护，防止数据非法扩散
- 非法工具窃取数据防护

云数一体化安全防护服务——数据安全态势监控服务

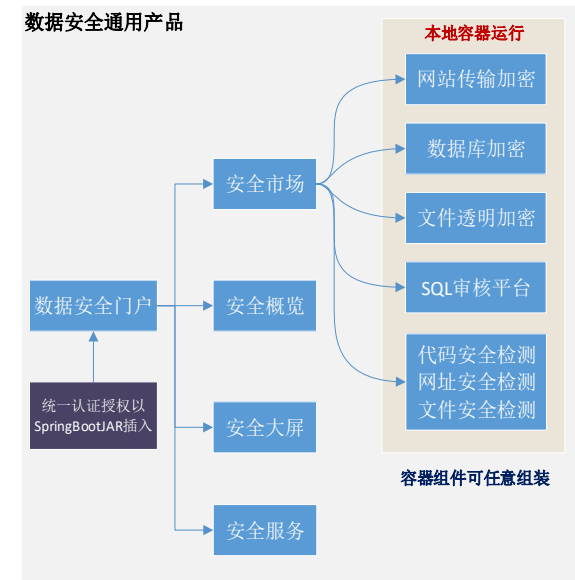
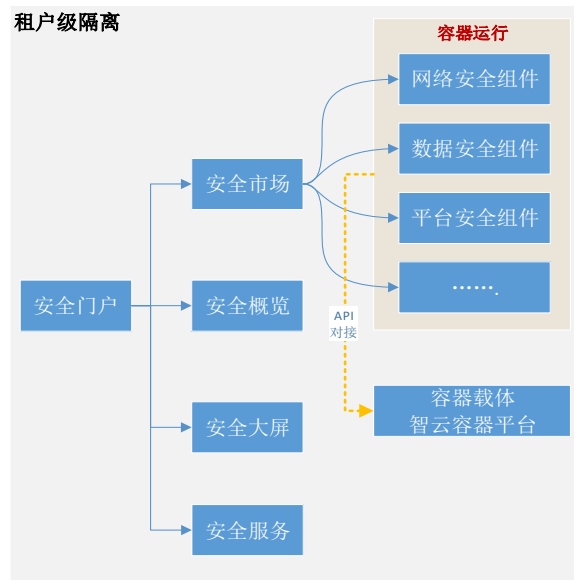


云数一体化安全防护服务模式

提供自服务门户 通过租户隔离提供基于云的安全服务

- **提供云平台整体安全防护**：支持公有云、私有云模式，提供从IaaS到PaaS到SaaS整体安全防护能力。
- **数据安全核心组件**：支持单线产品输出，或组合后以套装形式输出。
- **安全服务**：基于安全组件，将安全能力以RestfulAPI、SDK模式输出，覆盖离线模式和在线模式。
- **统一认证授权**：共性支撑，实现用户的统一管理、单点认证以及权限集中配置。

批量操作	全部	授权不足2月	请选择	请输入内容	搜索	导出			
<input type="checkbox"/>	组件名称	安全组件类型	规格	租户项目	端口	IP	到期时间	状态	操作
<input type="checkbox"/>	敏感数据脱敏检测	敏感数据脱敏	企业版	tenant01	10312	192.168.12.114	2021-02-03	正常运行	访问 更多
<input type="checkbox"/>	网站传输加密2	网站传输加密	标准版	tenant01	10285	192.168.12.114	2020-05-29	正常运行	关机 重启 扩容 授权延期
<input type="checkbox"/>	网址安全检测	网址安全检测	标准版	tenant01	10303	192.168.12.114	2020-04-29	正常运行	
<input type="checkbox"/>	数据库加密	数据库加解密	标准版	admin	10291	192.168.12.114	2020-09-07	正常运行	



助力云上合规 实现安全运营



安全产品服务化

合规高效

对标等保2.0标准和分级保护，确保**安全合规**。

通过安全功能虚拟化（SecFV），构建安全资源池，提供丰富的安全防护手段。



安全能力一体化

智慧易管

通过软件定义安全（SDS），实现安全能力**可编排、易管理**。

通过安全门户和安全市场，实现优势集成、**开放共享**。



安全运营自动化

增值共赢

通过订单、计费等体系，提供可配置的**自动化安全运营能力**。

通过安全市场，无缝接入第三方安全应用，构建**安全生态**。



2020 北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

CSA Summit

云安全联盟峰会



THANKS

智能协同 数智未来

毛俐旻 13810594511

航天科工网信公司



航天科工集团



航天网信公司