CAICT 中国信通院

中国通信标准化协会
China Communications Standards Association

China unicom中国联通

中国联通软件研究院
Chinaunicom Software

中国联通云平台安全实践

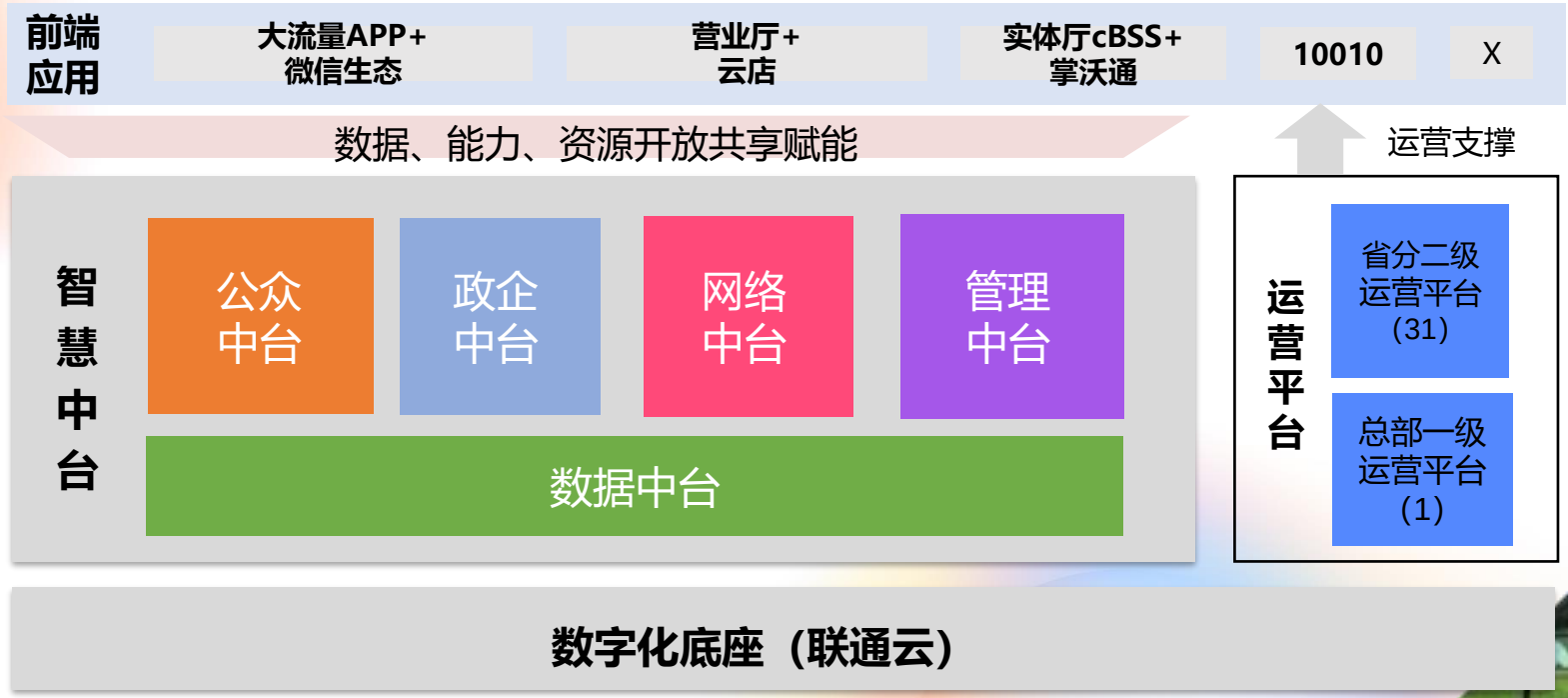
护航央企数字化转型
构建牢固集约化IT底座

中国联通软件研究院
张晶龙

2021 可信云大会
2021 TRUSTED CLOUD SUMMIT
数字裂变 可信发展

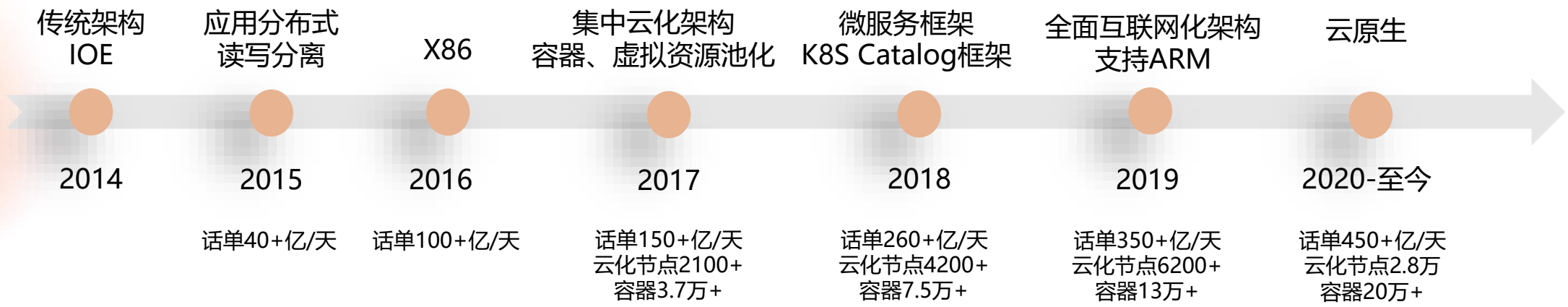
中国联通软件研究院简介

- 中国联通软件研究院是中国联通集团直属二级研发机构,成立于2015年7月1日，致力于科技自立自强、核心IT系统自主研发。本部位于北京，下设哈尔滨、济南、广州、西安、南京五个分院。
- 目前承担中国联通业务支撑域（BSS）、管理支撑域（MSS）、数据域（DSS），以及中国联通全集团IT技术中台的研发、生产和运营，全行业率先“去IOE”，是中国联通贯彻落实央企数字化转型，实现高质量发展的中坚力量



中国联通云平台发展历程

- **从2014年至2020年，公司IT技术架构逐渐从传统IOE架构演进为以联通云平台为载体。期间收敛技术栈，统一运营门户，统一监控平台，统一为集团提供数字化底座，护航IT集约化。**



天宫1.0
容器、虚机资源池化
基于mesos两级弹性调度

天宫2.0
多租户、微服务框架
Marathon+K8s容器双擎

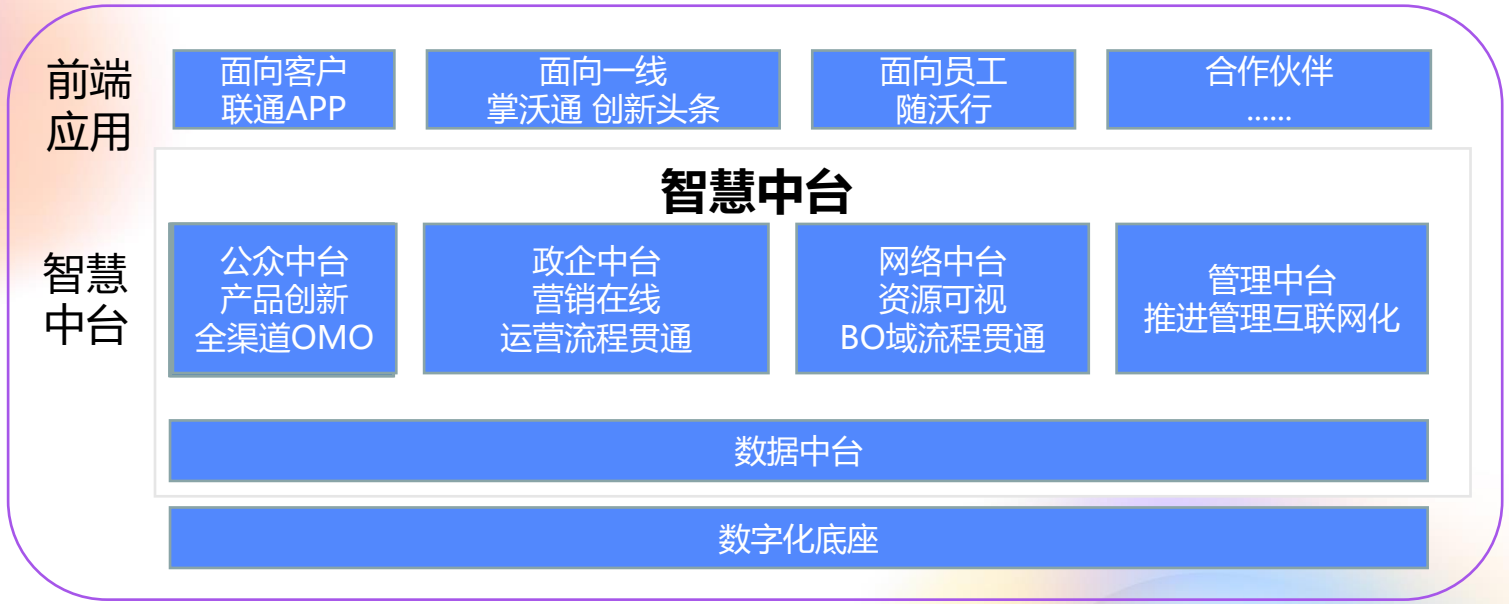
天宫3.0
率先全面支持ARM
新增CKE，通过CNCF认证

联通云
云原生架构
统一云资源运营

“平台+应用” 架构模式完成构建

- **经承载4亿用户，2万笔/秒实时并发等实战验证过的“共平台、共能力、共技术栈、共研发体系”的数字化架构体系，已成为构建联通智慧运营大脑的坚实基础**

联通数字化架构体系



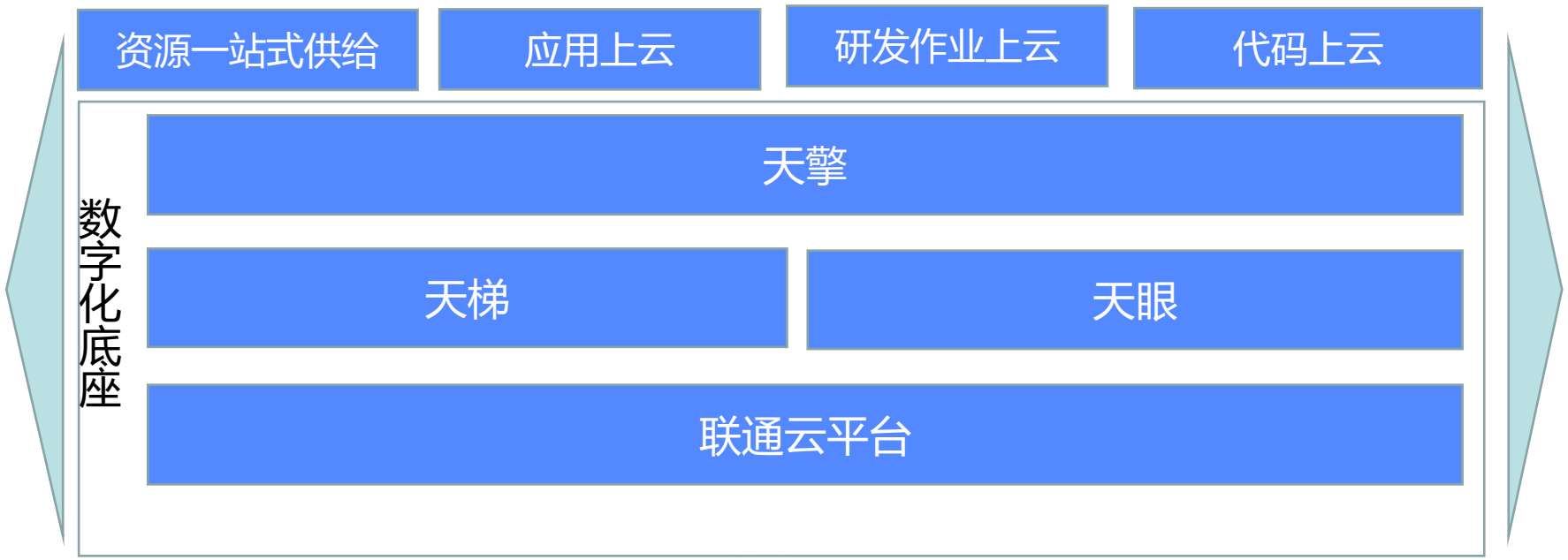
“平台+应用”架构优势

- 轻、薄、快个性的前端应用：实现服务全在线、多触点协同、基于同体验之上的千人千面
- 集约化核心能力：沉淀核心业务、核心数据、核心流程、核心能力，一点开放服务，全域共享
- DT能力：整合拉通前后端、内外部全域数据，驱动数据嵌入业务、嵌入场景、实时赋能，数据服务快速交付
- 统一底座：“共平台、共能力、共技术栈、共研发体系”基座底座，服务实例3.7万+，服务调用13亿+/天

数字化新IT敏捷底座

共平台、共能力、共技术栈、共研发体系、共治理体系

面向内部
赋能数字化新IT
加速全面转型



面向外部
数字化引领
央企最佳实践

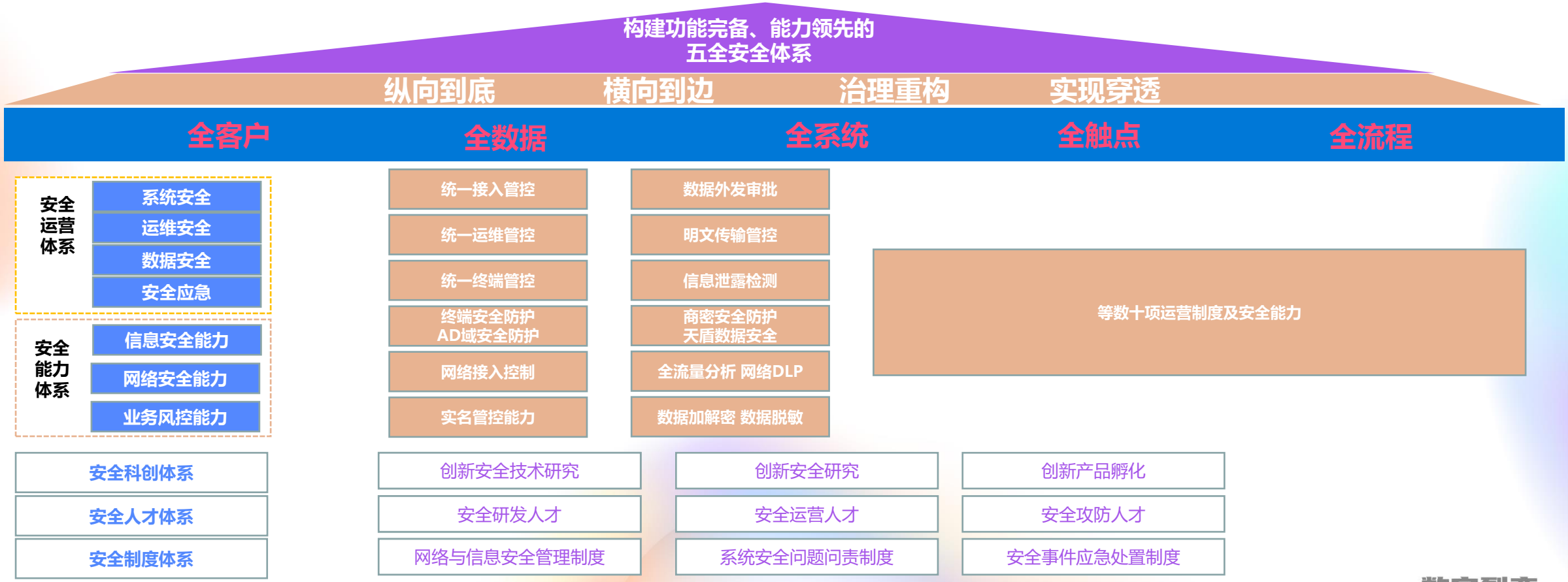
容器双擎、 虚裸双机
6大数据中心 3.0w+节点
三大架构、混合部署

容器实例22w+
日调用量 30亿+
存储320+PB

自研+开源+商业
8大产品家族180+组件
OLAP+OLTP全场景覆盖

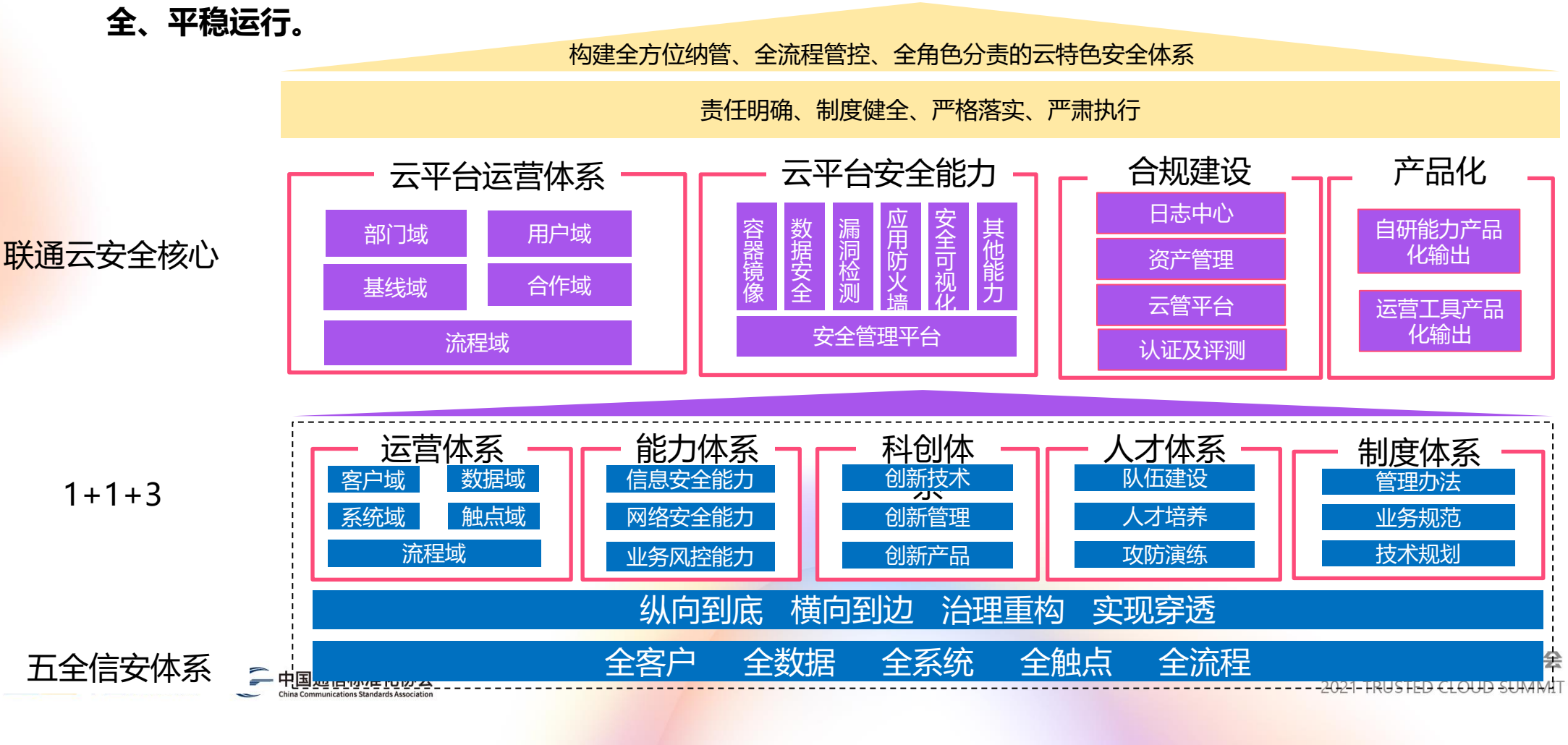
中国联通“五全”安全体系

- 落实“五全网络信息安全体系”要求，推进“1+1+3”体系建设，做好集中系统安全管理，加强等保、关保、双新评估等合规基线常态化运营，打造云防护、态势感知、安全攻防等能力，进一步整合安全队伍，打造自有“红客”团队，不断推进安全能力服务的产品化、方案化



最佳实践之云安全体系

- **联通云以私有云形式，面向全集团各分子公司提供企业级云计算解决方案，具有底层开放度高、参与角色众多、数据敏感度高、业务连续性强的安全特点；**
- **通过构建分层分责模型、全流程安全规约等管控办法，及容器防护、镜像扫描、安全可视化等安全能力，保障平台安全、平稳运行。**



最佳实践之Devops安全一天梯

通过规则定义及代码扫描，实现全面的代码质量管理，提升内建研发质量

01.精准定位缺陷

代码扫描全面覆盖，违规定位到人，从个人意识、技能方面提升研发团队开发质量

02.全面分析质量

大幅缩减扫描时间，降低版本交付成本，通过代码输出率、研发活跃度等指标综合分析，促进团队实现持续改进

03.代码健康度

利用动态权重公式，建立代码健康度模型

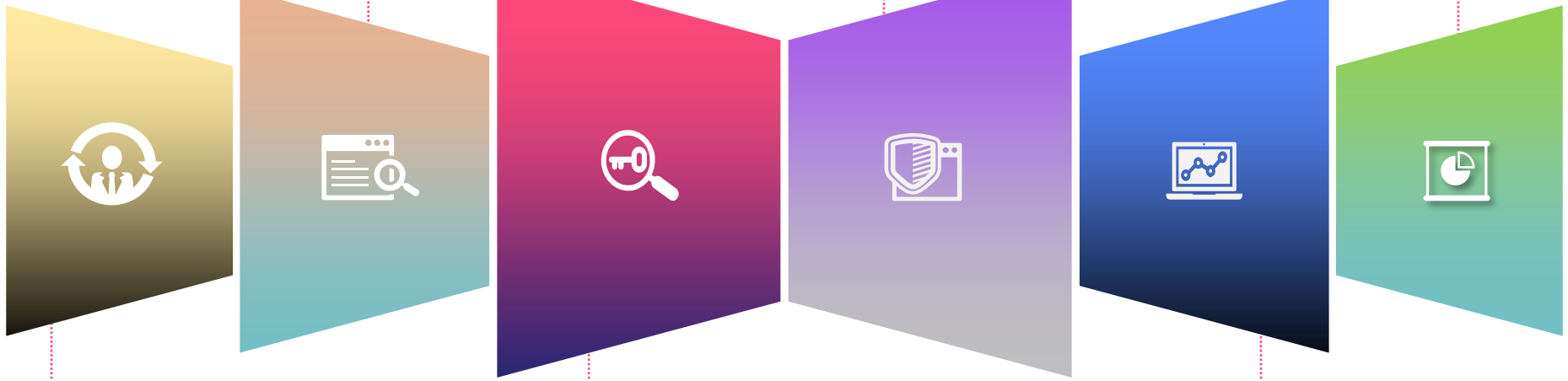
检查	跟踪	集成	反馈	度量
Code Quality	R&D Activities	With Devops	Quality Specification	Business Report
研发规范融入到代码检查	研发人员的输出与质量度量	无需植入被扫描系统	公司级代码质量规约	多层级数据钻取
自动代码扫描	记录研发活动轨迹	与DevOps工具链整合	根据业务需求定制	数据精细化
支持多语言质量规约	实时展示项目最新状态	阻断级缺陷拦截	与管理系统对接	运营分析数据
可集成多种代码扫描工具	缺陷情况定位到人	对外提供服务报表		
		项目自助安装		

最佳实践之能力治理安全—天擎

- 企业级能力开放治理平台，纳管1.7w+能力，780+能力提供方，日调用峰值13亿；
- 面临能力安全、可信调用、信道安全、数据安全等安全课题

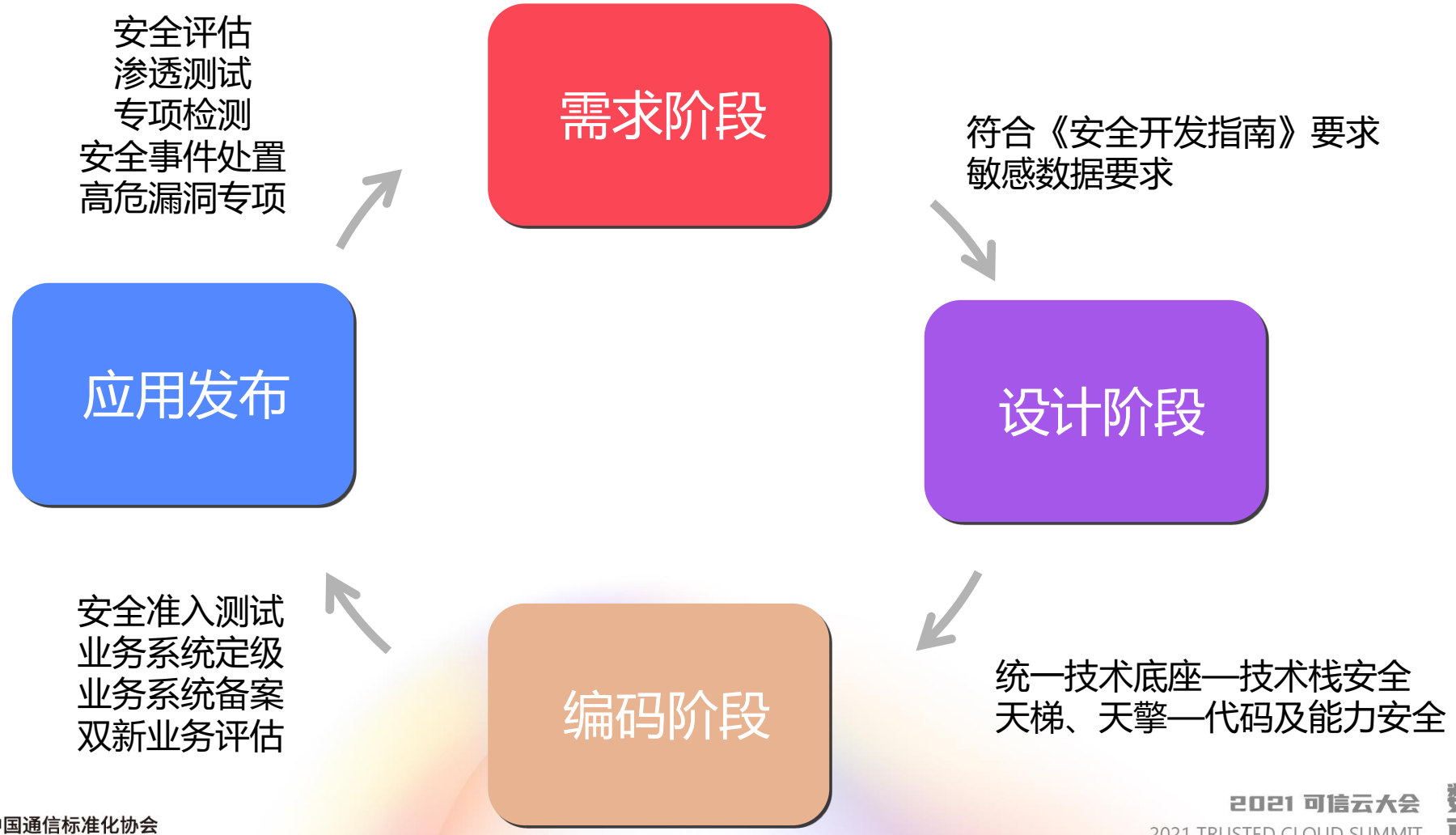
安全 / 环境	内安全机制	外安全机制
白名单		√
认证鉴权	√	√
非对称加密校验		√
时间偏移量校验	√	√
流量控制	√	√
熔断处理	√	√
能力分级	√	√

最佳实践之云安全治理



最佳实践之研发活动周期安全

- **软件开发生命周期遵循《安全开发指南》，系统上线、发布需要通过安全准入测试并定级备案**



THANKS!

2021
TRUSTED CLOUD
SUMMIT