启明星辰抵抗网络安全熵增实践

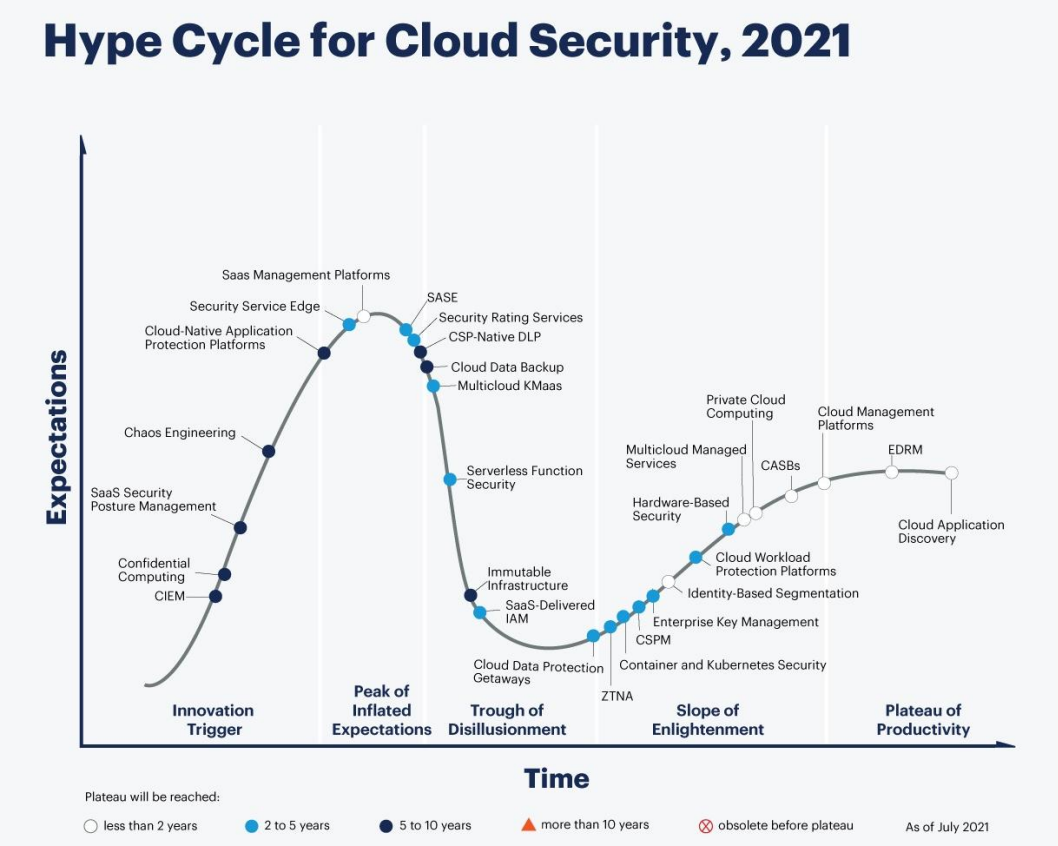
演讲人：胡毅勋　　单位名称：启明星辰信息技术集团股份有限公司

01 云安全技术现状与分析

02 思考、手段与成果

云安全技术发展现状与分析

研究机构眼中的网络安全



产品间能力重复现象明显

- SASE、SSE、ZTNA
- CNAPP、Container and Kubernetes Security、SSPM、CSPM、CWPP、Microsegmentaion
- …

随场景安全需求挖掘深入，安全产品细分种类越来越多，处理安全问题的核心能力可以抽象解耦纵向发展。

用户眼中的云安全

安全运维的效能困局

产业的发展促使安全产品细分种类激增，运维人员需要掌握大量不同厂商和不同类型的安全设备，安全运维难度极具增加。

安全孤岛的协同困局

为了形成行业竞争力，安全厂商和安全产品互相制造行业壁垒，在安全能力上构成了安全孤岛，在安全分析上构筑了数据孤岛。

安全产品的云化困局

云安全资源池成为我国云安全场景中特有的安全产品类型，堆砌的安全能力无法满足5G、AI、算力网络、云计算等新场景下真正的安全需求。

安全场景的落地困局

安全场景化已成为行业共识，实际上却大多停留在给用户的解决方案文档和口号中，真正实战化落地举步维艰。

网络安全系统中的熵增

网络安全系统熵增

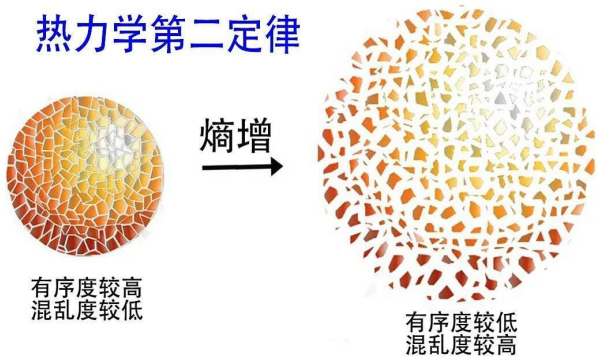
安全信息分布变广

信息不确定性增加

$$H[x] = -\sum_x p(x)\log_x p(x)$$

安全产业高速发展

热力学第二定律



安全进入细分领域竞争

- 安全牛第十一版全景图包含16项一级安全分类，108项二级安全分类
- 各安全产品之间具有很多相似的安全能力，整体防护体系存在大量冗余

安全厂商追求商业垄断

- 异构厂商互相堆砌壁垒在用户侧形成“安全孤岛”
- 大量的安全数据无法全局分析，形成“数据孤岛”

熵减的必要手段：开放平台、引入外力

熵增定律

在一个孤立系统里，如果没有外力做功，其总混乱度（熵）会不断增大。

开放平台

构建**开放式的云安全生态**，基于**标准化接口**全面支持第三方能力（安全、运营、工具等），从而提升系统安全能量。

引入外力

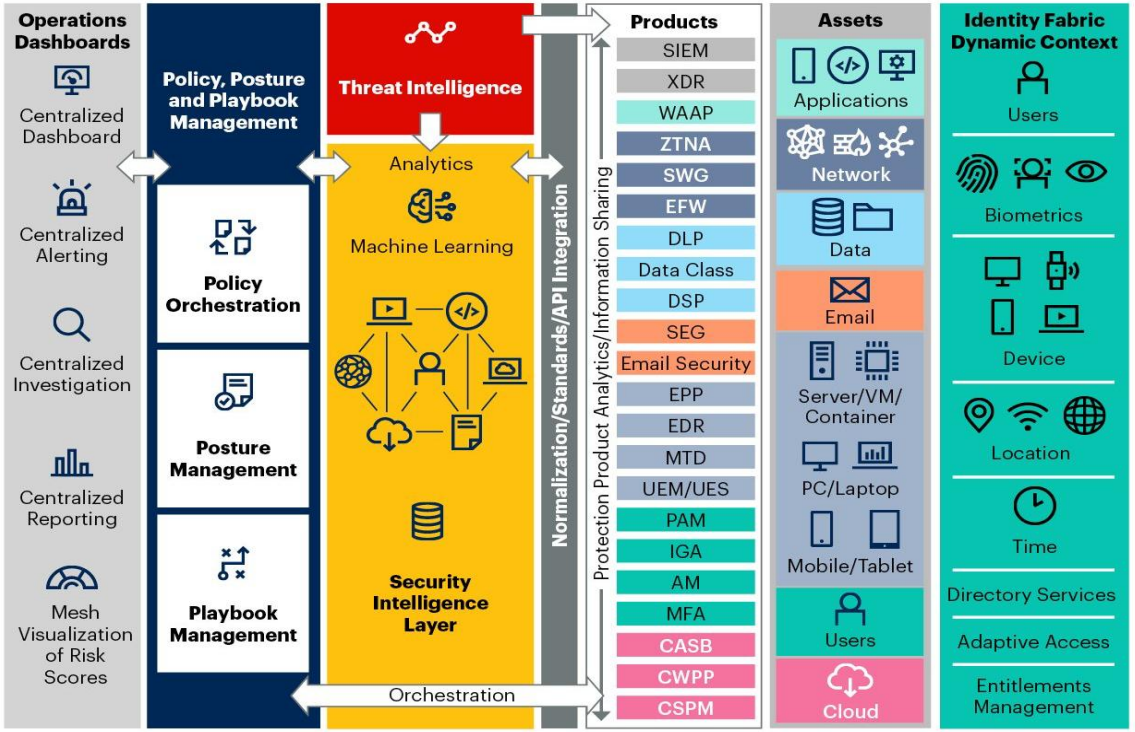
基于平台整合分散的安全能力，从而打破安全孤岛和数据孤岛，在用户侧按需构建和交付安全价值。

用秩序交付安全

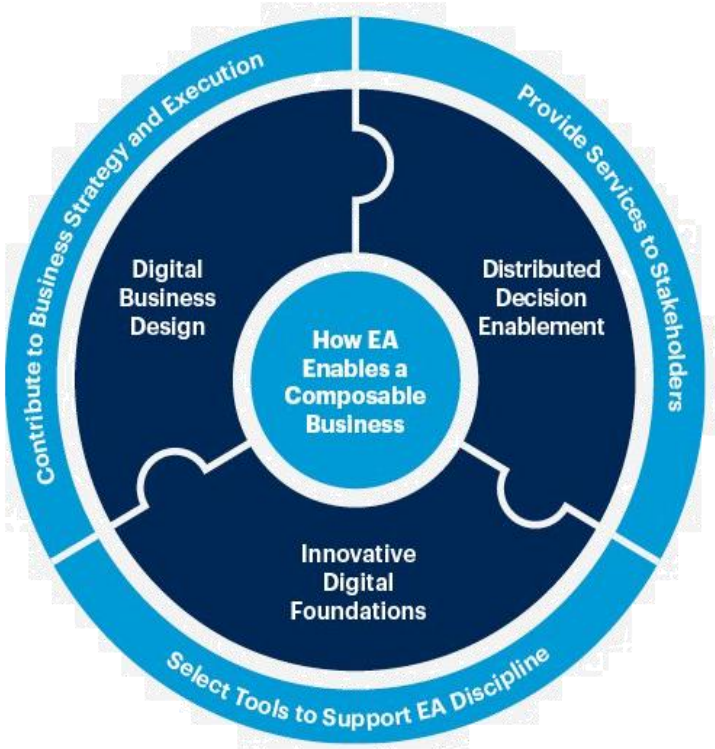
探索一种现代化的安全方法，能够在**需要的地方**部署**一致性的控制能力**，以一种紧密**集成、可扩展、高度灵活**，并富有弹性/韧性的方式，通过提供支持服务层（整合策略管理、控制台安全情报和身份矩阵）来让安全工具之间能够**协作而不是各自为战**。

思考、手段与成果

云安全新方向：网络安全网格架构+可组装业务开发



网络安全网格架构



可组装安全业务开发

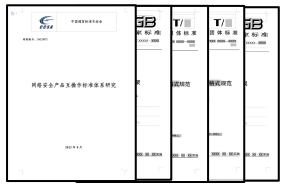
熵减手段：以顶层设计为抓手指导产品落地

- 依托平台构建协同防御安全体系，基于安全产品互联互通互操作打破安全孤岛，通过编排、智能和知识协助安全场景化高质量落地。

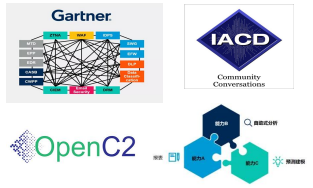
安全产品实践安全范式

顶层设计拓展安全产品成长格局

积极参与网络安全顶层设计，从产品互联互通、安全能力开放等方向，设计组装式网格化防御架构。



网络安全标准



前沿安全理念

输出产业需要的安全需求
设计产业前沿的产品架构

互联互通互操作

以平台驱动
以集成为手段

安全场景化落地

弹性动态的IT新架构
各具特色的垂直行业

技术平台支撑场景化产品落地

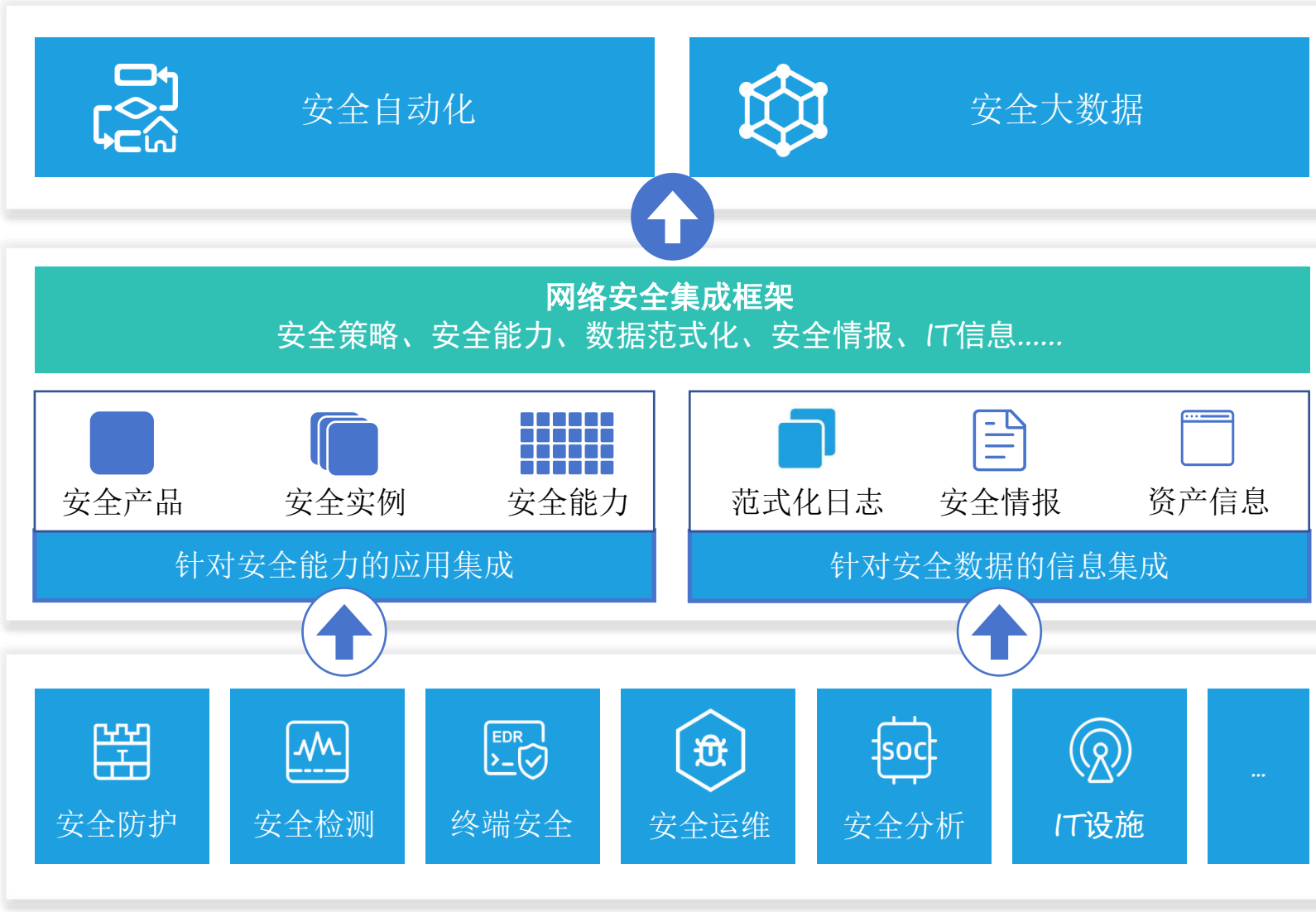
以行业场景实战化经验积累安全知识，基于可组装开发平台和网格化可编排安全能力构建安全平台。

运营商　金融　能源　政企

建设符合产业方向的安全平台

顶层设计指导安全产品

熵减手段：通过安全原子能力构建安全产品

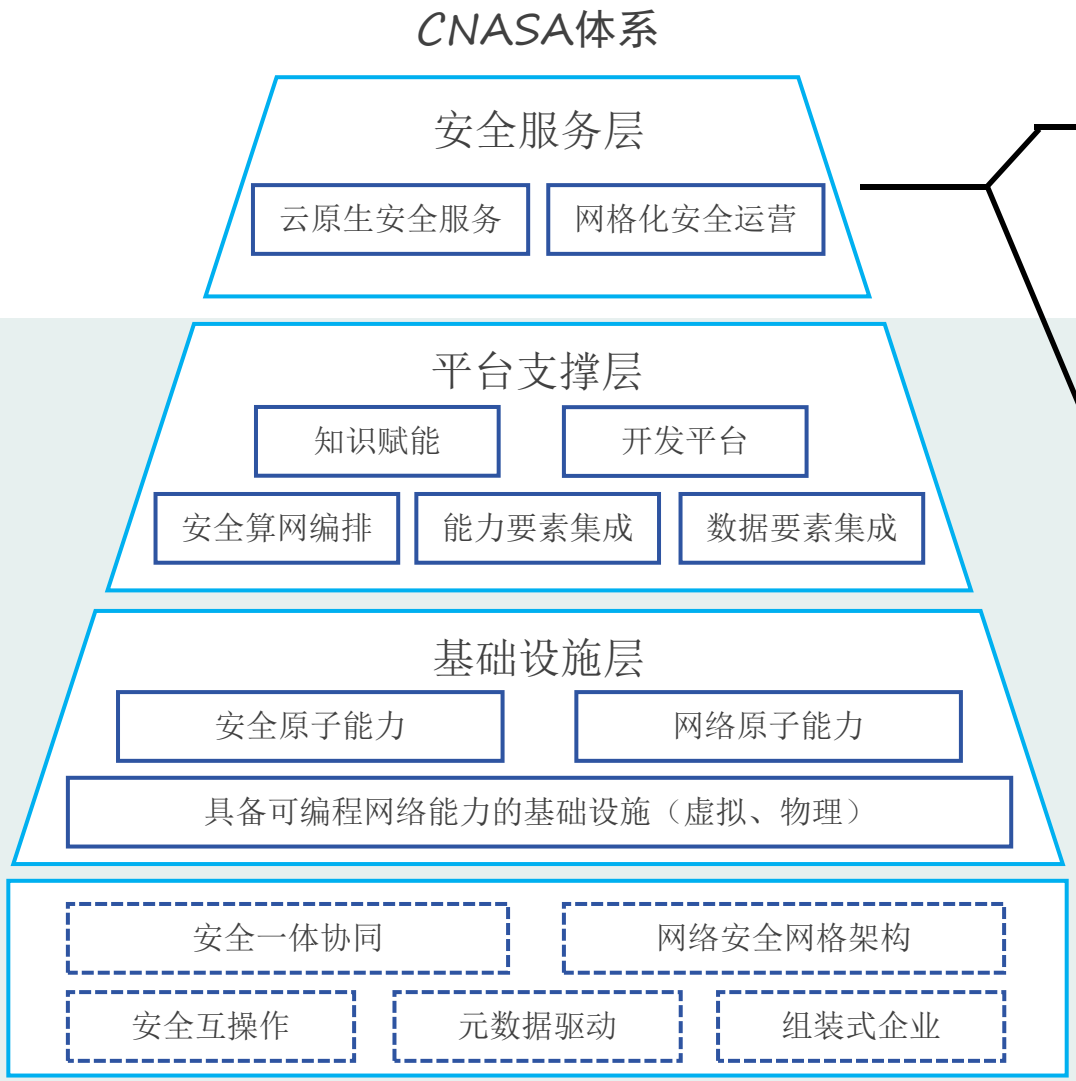


- **安全自动化**支撑安全循环
  安全大数据支撑安全分析
- **网络安全集成框架**集成异构安全策略和数据，打破孤岛
- **应用集成**集成异构安全能力和IT手段
- **信息集成**集成统一和规范的安全数据
- **安全产品**提供安全功能，执行安全策略，上报安全数据

熵减手段：平台化和组装式驱动云安全防护网格建设

一些成果：CNASA一体化云原生自适应体系

冰山层构建安全基础设施作为移动云安全底座，上层建设安全服务和运营。



云租户安全

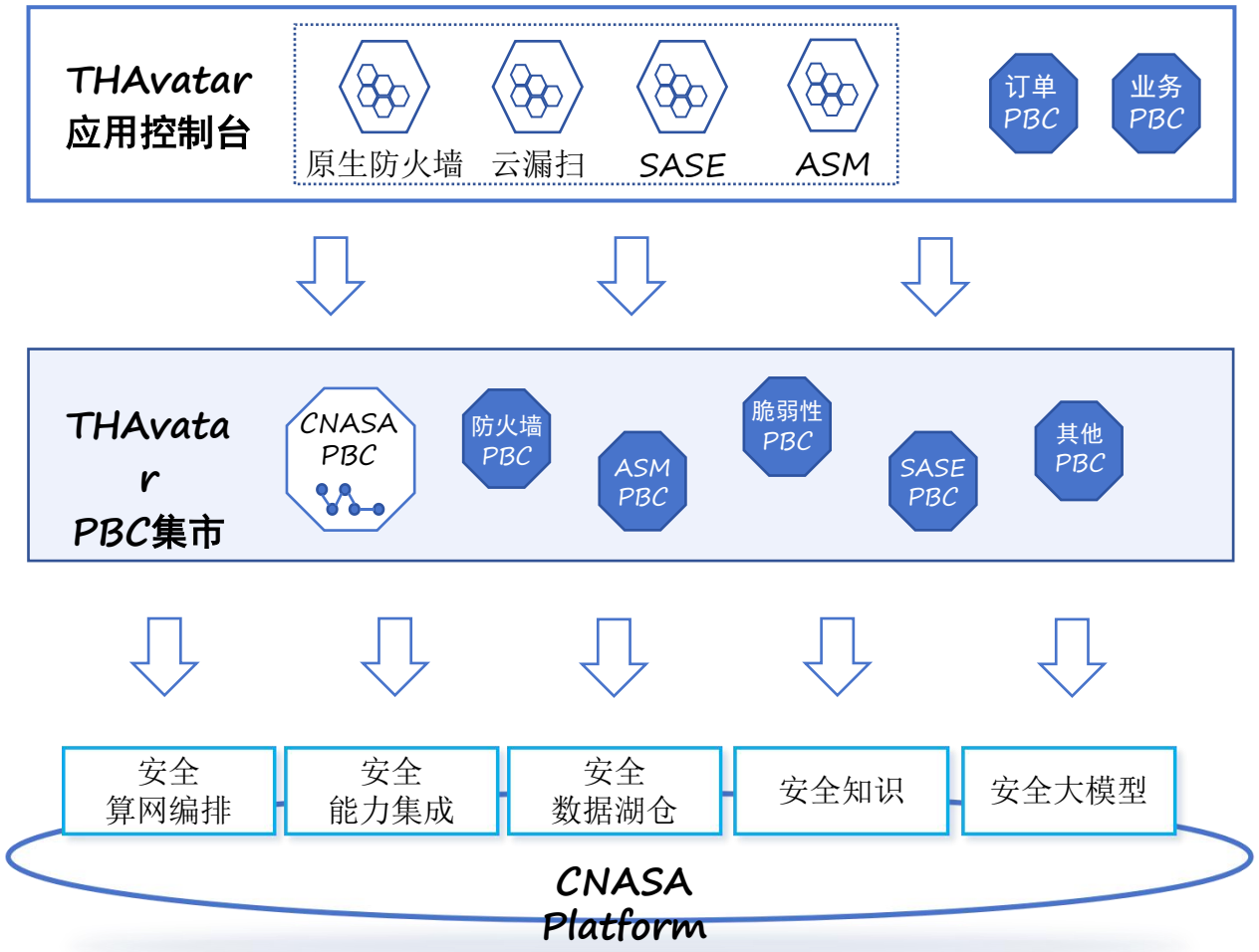
基于IPDRR安全过程构建面向于租户场景的安全服务

云平台安全

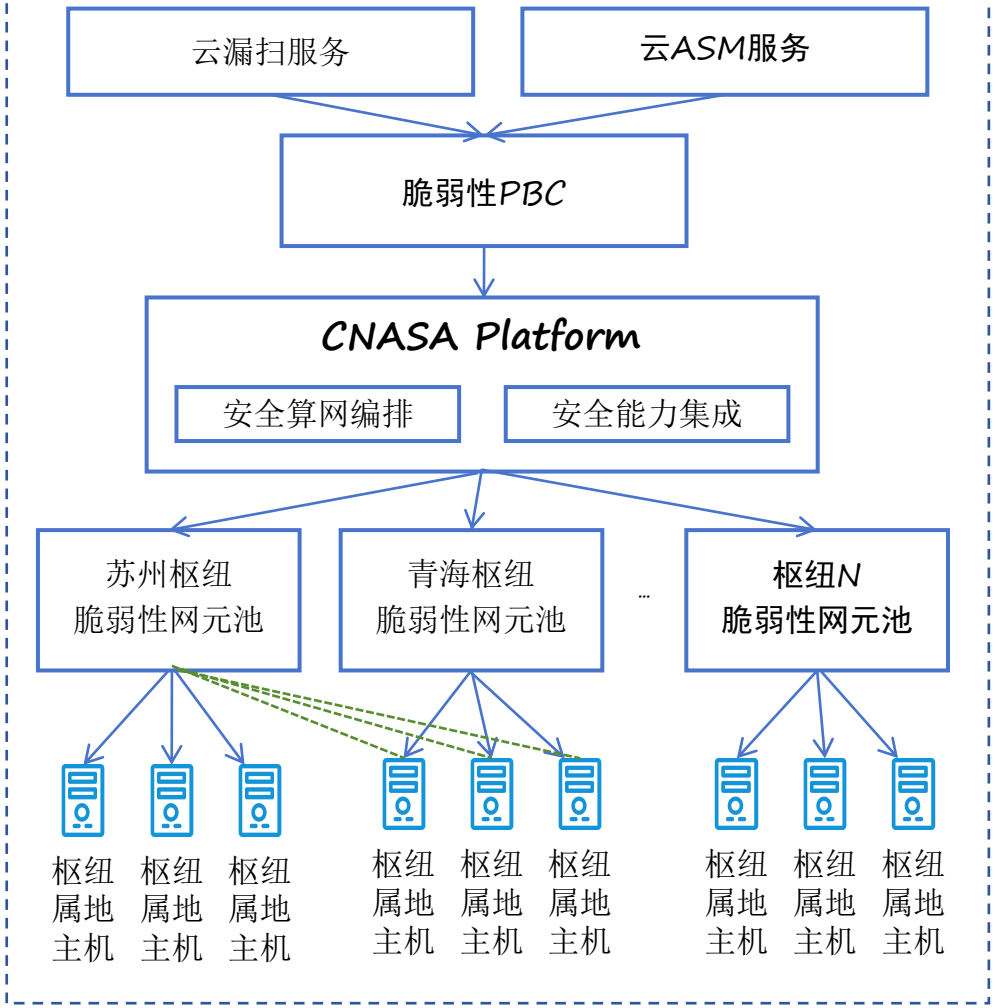
边界安全、身份安全、数据安全、应用安全、安全管理...

一些成果：CNASA体系上构建云安全服务

CNASA上的THAvatar云原生框架



漏扫和ASM的共性能力



一些成果：中国移动算网安全资源池

1个集团运营管理平台

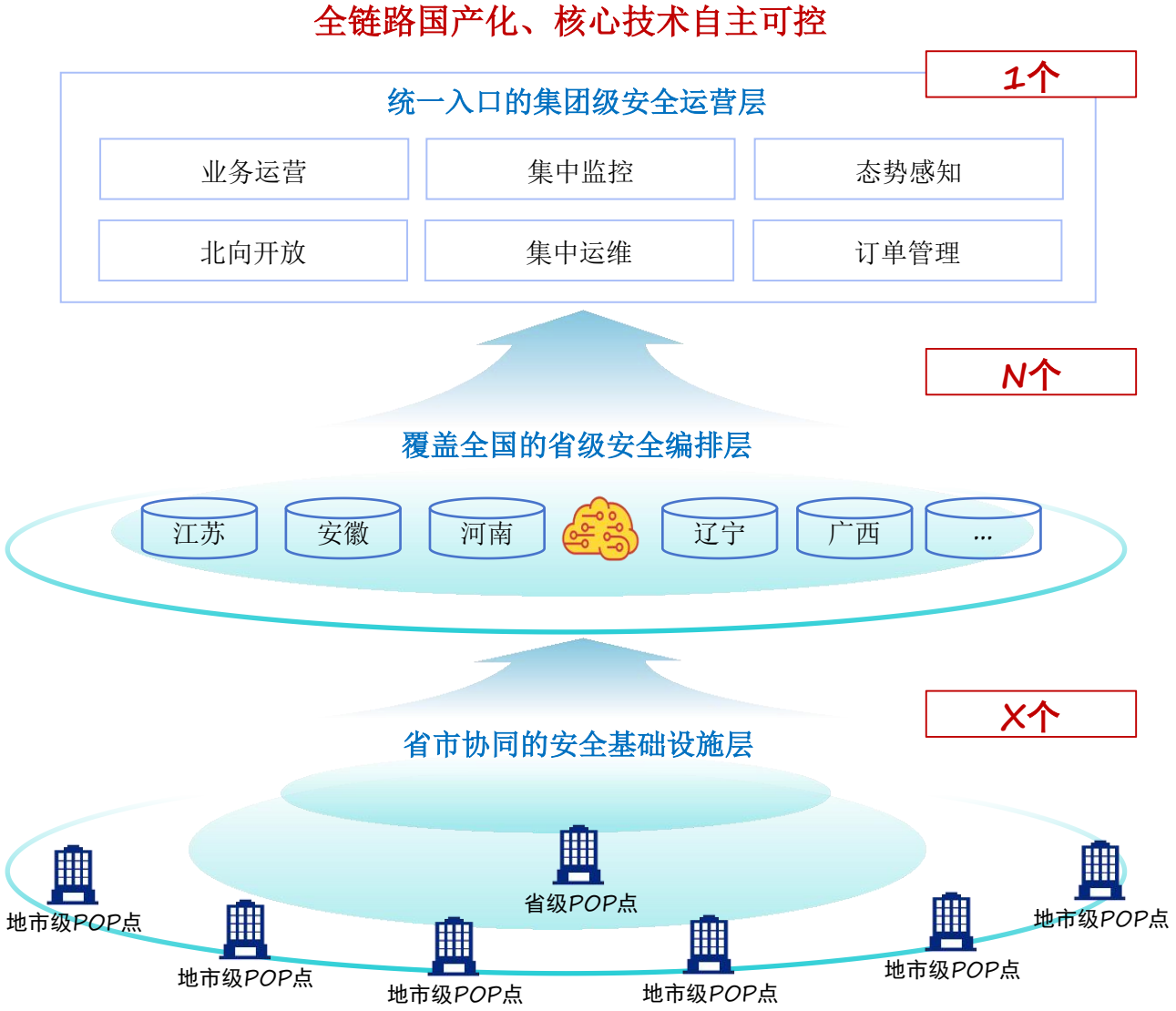
- 全国集中运维，对省级和近源安全资源池做集中运维，并具备业务运营、态势感知等功能，通过与移动云官网门户OP进行接口对接实现订购信息的同步

N个省级安全管理平台

- 实现全省统一运维、统筹管理，对省级安全资源池和近源安全资源池做集中运维，并具备业务运营功能。

X个安全PoP节点

- 省侧：供给全省覆盖的延时不敏感的运维和扫描类安全能力
- 地市侧：供给地市覆盖的延时敏感的近源流量类防护能力



等保合规型能力

- 下一代防火墙
- 入侵防御
- WEB应用隔离
- 数据库审计
- 终端安全EDR
- 网页防篡改
- 日志审计
- 堡垒机
- 漏洞扫描

数据安全型能力

- 数据脱敏
- 数据分类分级
- 数字水印
- 数据安全网关

增强安全型能力

- 资产测绘
- 网站安全监测

密码安全型能力

- 签名验签(时间戳)

THANK YOU!