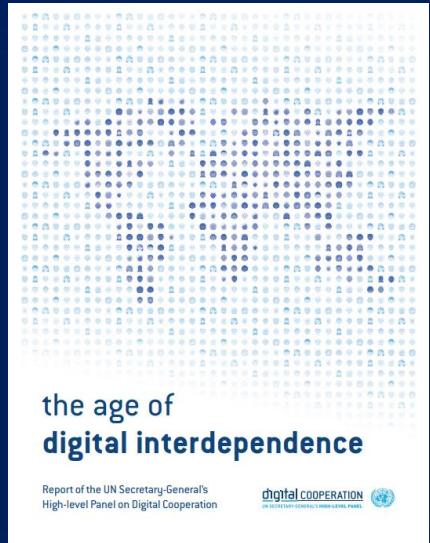




聚变： 数字时代的安全产业变革

吴云坤
奇安信集团总裁



数字技术正在迅速改变社会和经济，也带来前所未有的深刻挑战。

数字时代，国家、经济、社会与网络空间深度融合



智慧地球与数字中国



数字经济与实体经济



智慧社会与数字生活

网络空间安全直接影响国家安全、经济安全和社会安全



网络攻击致使基础
设施停止运行



网络攻击导致银行
资金被窃取



勒索攻击让城市
市政系统瘫痪

俄罗斯储蓄银行发布报告称，2018年因网络犯罪导致世界经济损失1.5万亿美元，2019年预计该损失将达到2.5万亿美元，增长60%。

今天中国的网络安全产业能否支撑数字时代的保障和防护？



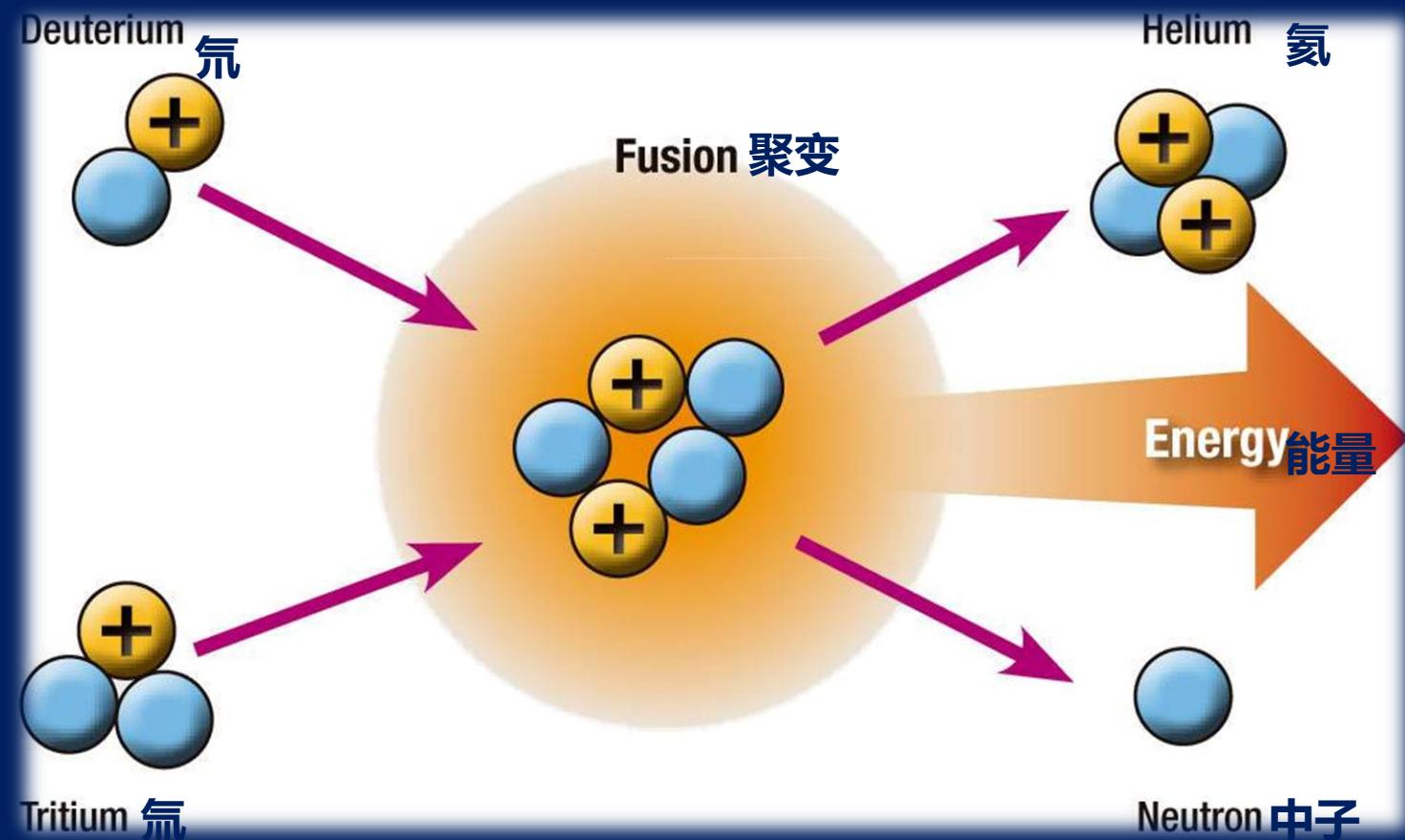
36万亿
中国数字经济规模

2.17万亿
中国ICT支出

487亿元
中国网络安全投入

亟待聚变

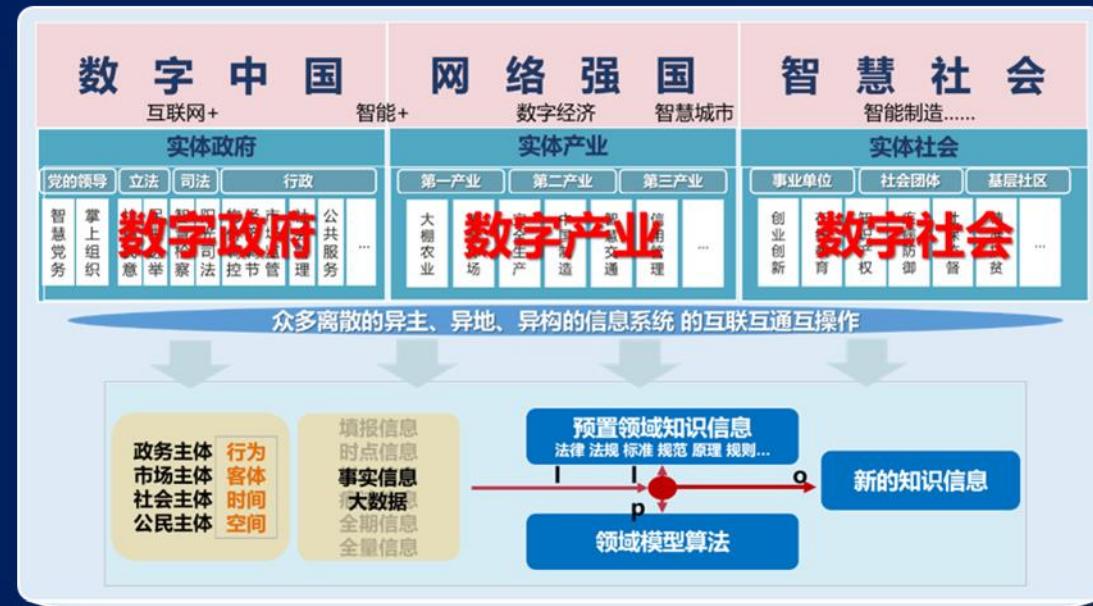
聚变是各要素聚合后的价值乘法倍增，不是简单的要素加减聚集。



聚变之一

信息化与安全的“聚与变”

信息化的变：云大物移人等信息技术的应用，推动了以云和大数据为基础设施的新一代信息化和业务系统建设



威胁的变：商业利益诉求和恐怖破坏目的交织，高智商利用高技术集团化、组织化对抗，“组织化”的网络攻击成为形成常态化



国家级黑客



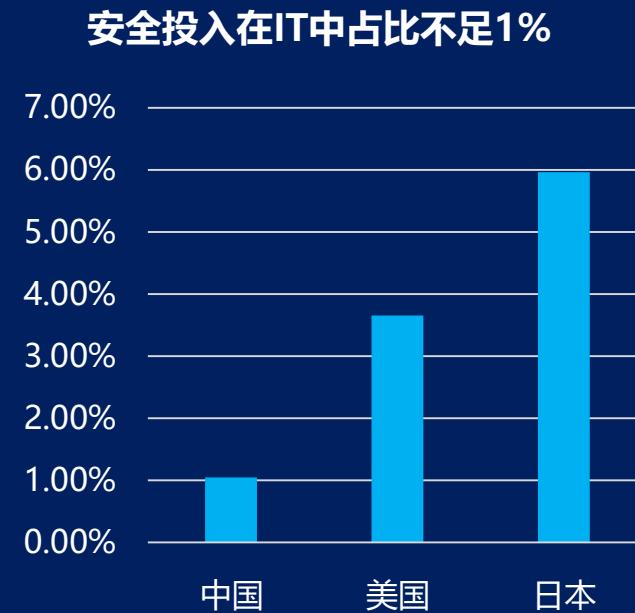
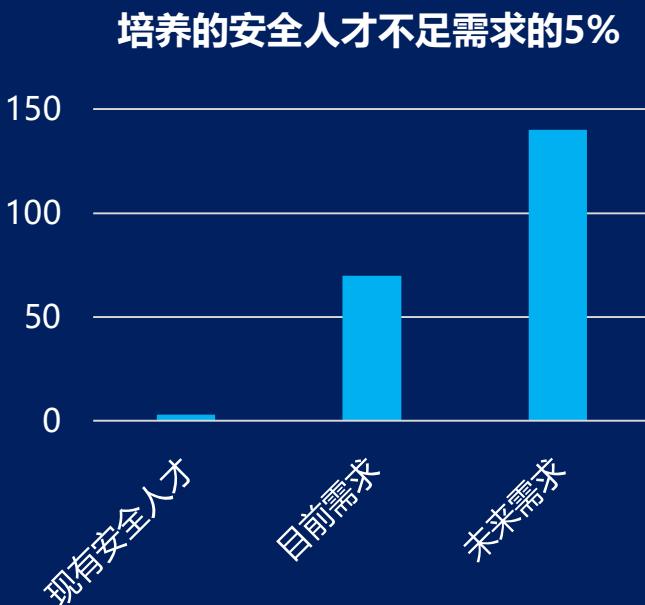
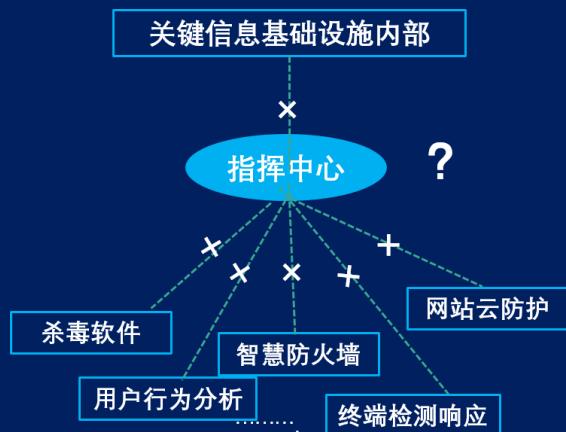
黑产组织



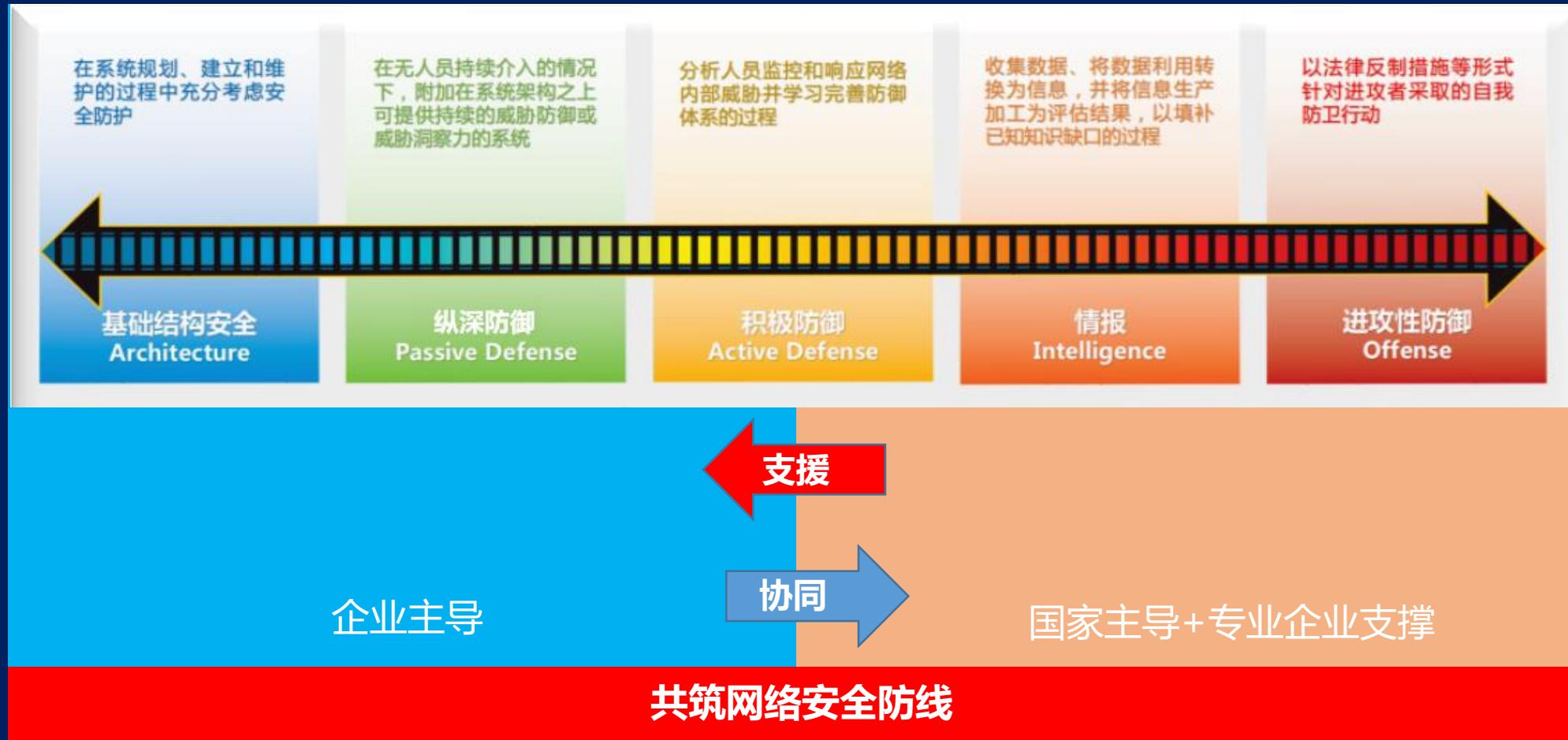
涉网犯罪分子

过去的坑：长期以来，由于网络安全的建设模式不合理、投入严重不足，导致安全防护与运行体系留下了很多“坑”……

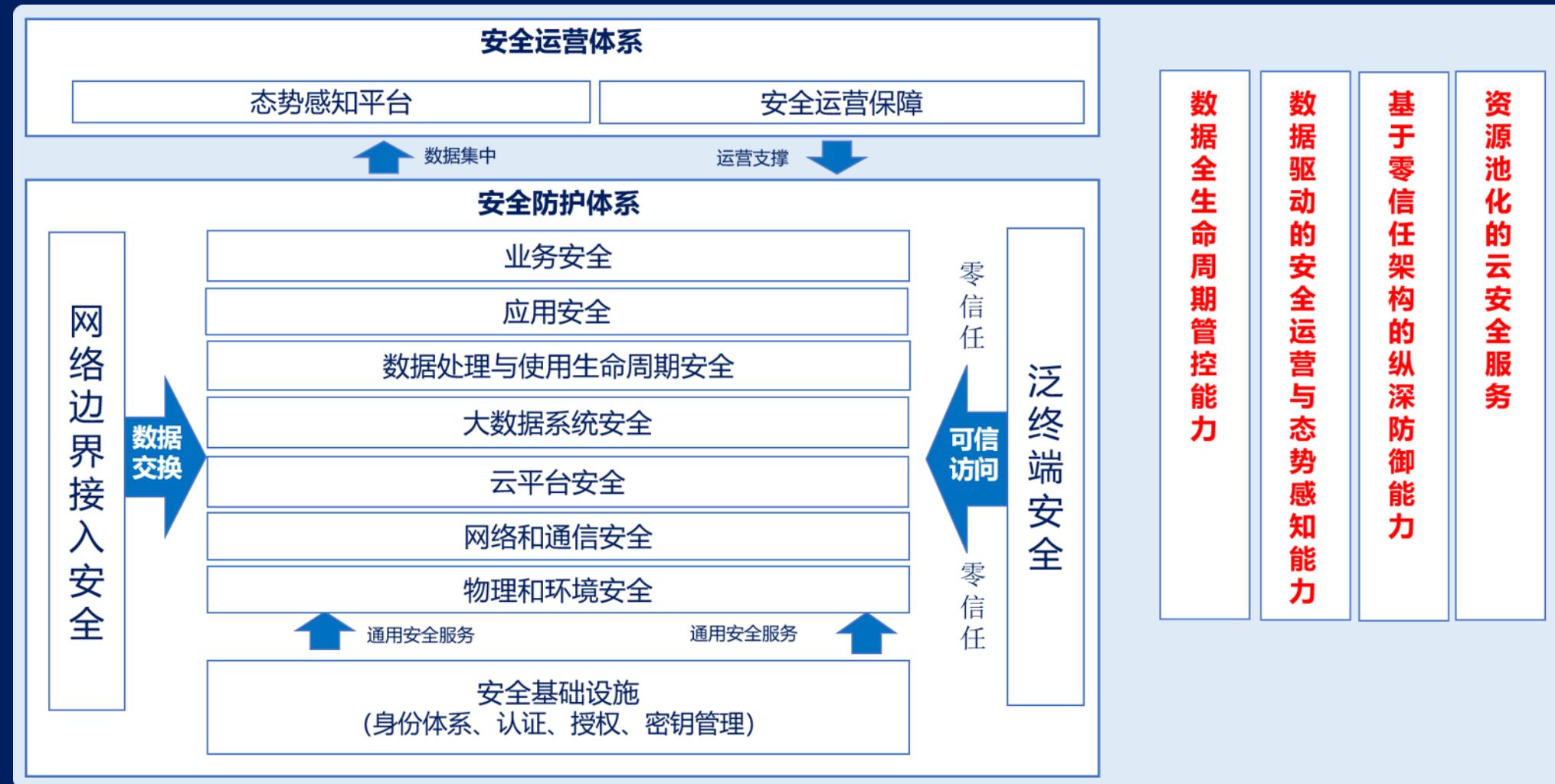
“创可贴”式的建设导致产品堆砌、防护失衡，手段“碎片化”



需要从应对特定威胁和合规点的建设模式，走向能力导向的建设模式



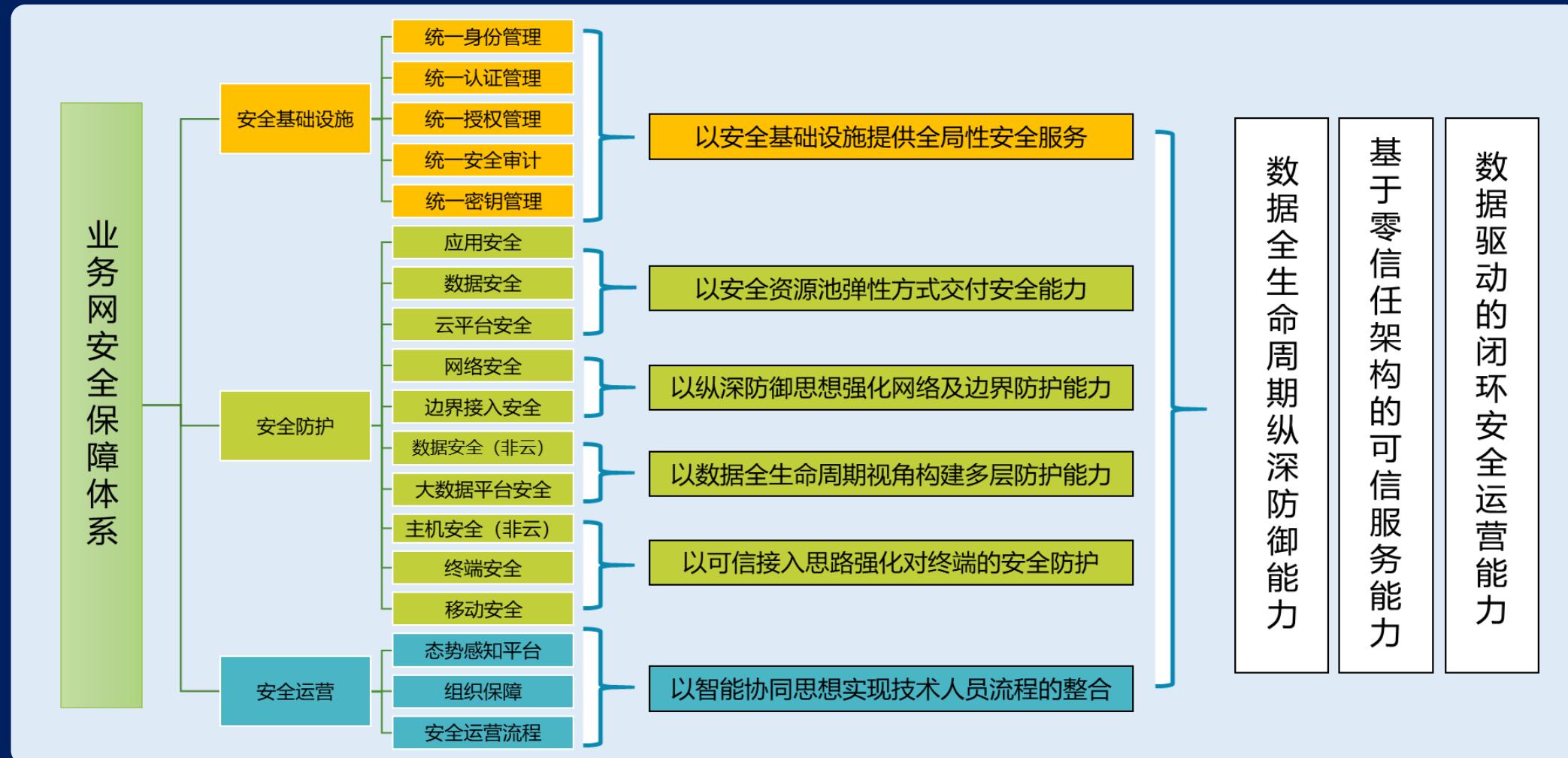
能力导向的安全防护体系建设强调“关口前移”，与信息化同步规划、同步建设安全体系



实践：某部委大数据项目中规划和建设中，与系统同步规划和建设安全体系。



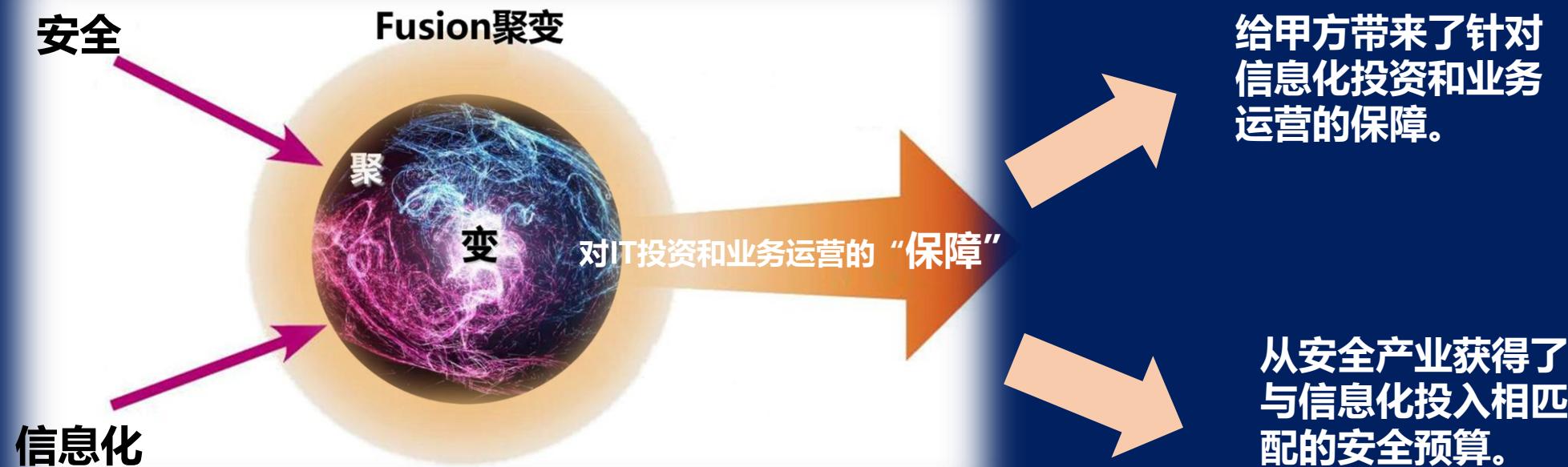
实践：某国有大型银行十三五信息化规划项目，同步规划安全体系。



实践：某能源央企衔接传统与新信息系统安全，全面覆盖云、大数据、移动、物联网和工控安全。



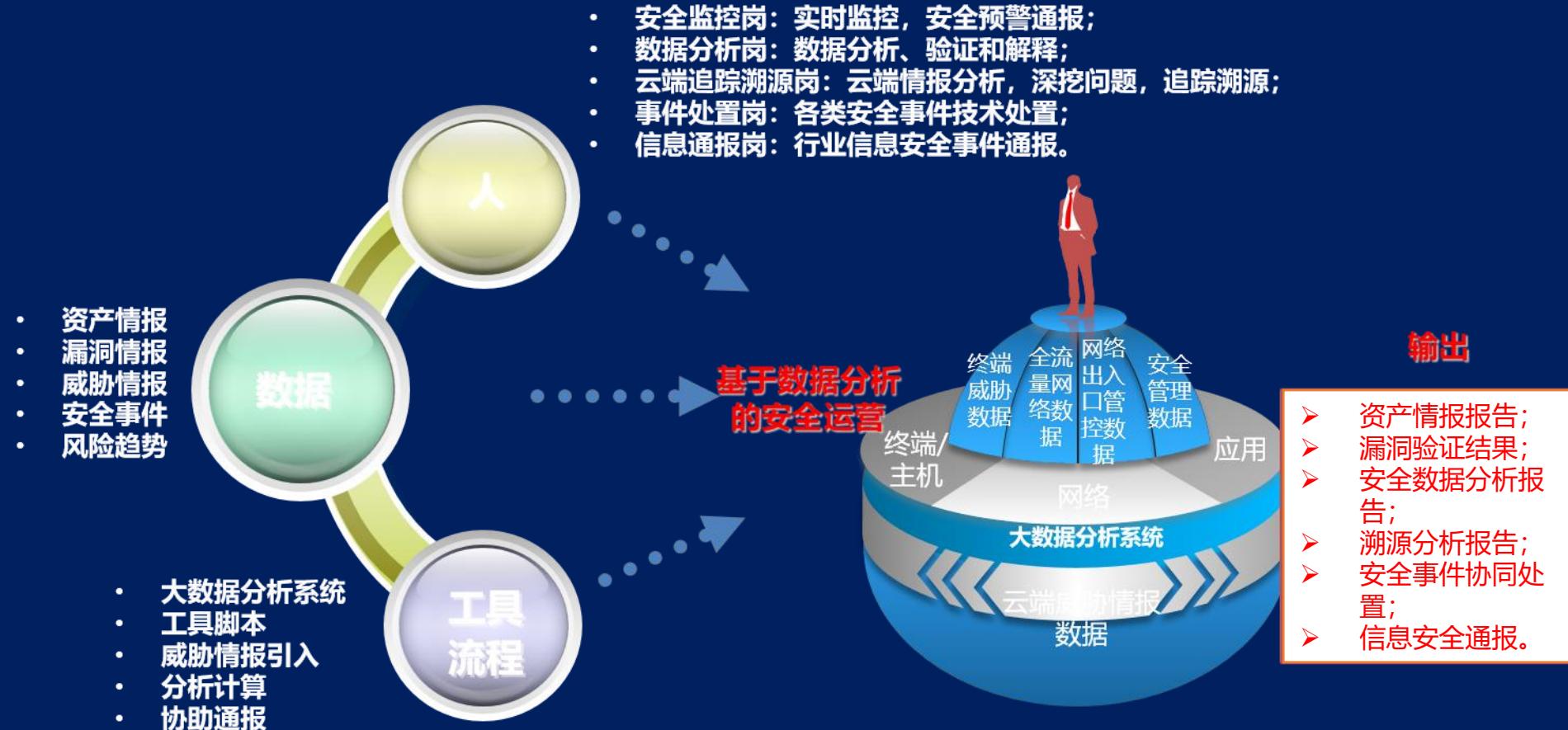
安全与信息化的聚，实现对信息化投资和业务运营的真正保障。



聚变之二

安全运行与IT建设/运维 “聚与变”

实战化的安全体系需要管理、技术与运行一体化



实践：结合客户业务需求的终端安全运行体系



| 2019年1月 | 至2019年6月 | 至2019年8月初 |
|-------------|---------------------------------|---|
| 安装率：约 70% | 安装率：约 85% ($\uparrow 15\%$) | 安装率：94.81% (\uparrow 年初 $\uparrow 24.81\%$) |
| 实名率：约 60% | 实名率：约 75% ($\uparrow 15\%$) | 实名率：94.81% (\uparrow 年初 $\uparrow 34.81\%$) |
| 正常率：约 45% | 正常率：约 70% ($\uparrow 25\%$) | 正常率：90.48% (\uparrow 年初 $\uparrow 49.81\%$) |
| 基线合规率：约 35% | 基线合规率：约 65% ($\uparrow 35\%$) | 基线合规率：91.87% (\uparrow 年初 $\uparrow 57.87\%$) |

实践：某机构护网内部攻防演练中的实战化运行

01

通过态势感知和安全运营平台实时对攻击行为进行监控，识别可疑攻击。

安全监测

02

对攻击行为进行分析判断，给出处置意见，进行攻击溯源，编制分析报告。

安全分析

03

对攻击成功事件进行阻断、隔离、断网，并进行全面排查、处置、恢复，编制处置报告。

事件处置

04

编制事件上报报告，上报护网工作组，编制每日日报和通报。

事件上报

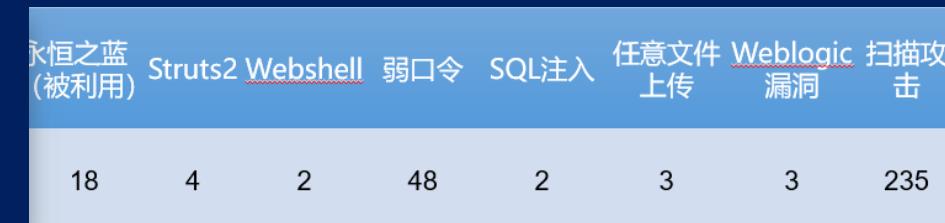
05

对上报信息进行现场判断决策，对入侵成功事件进行核实，适时向护网指挥部报告。

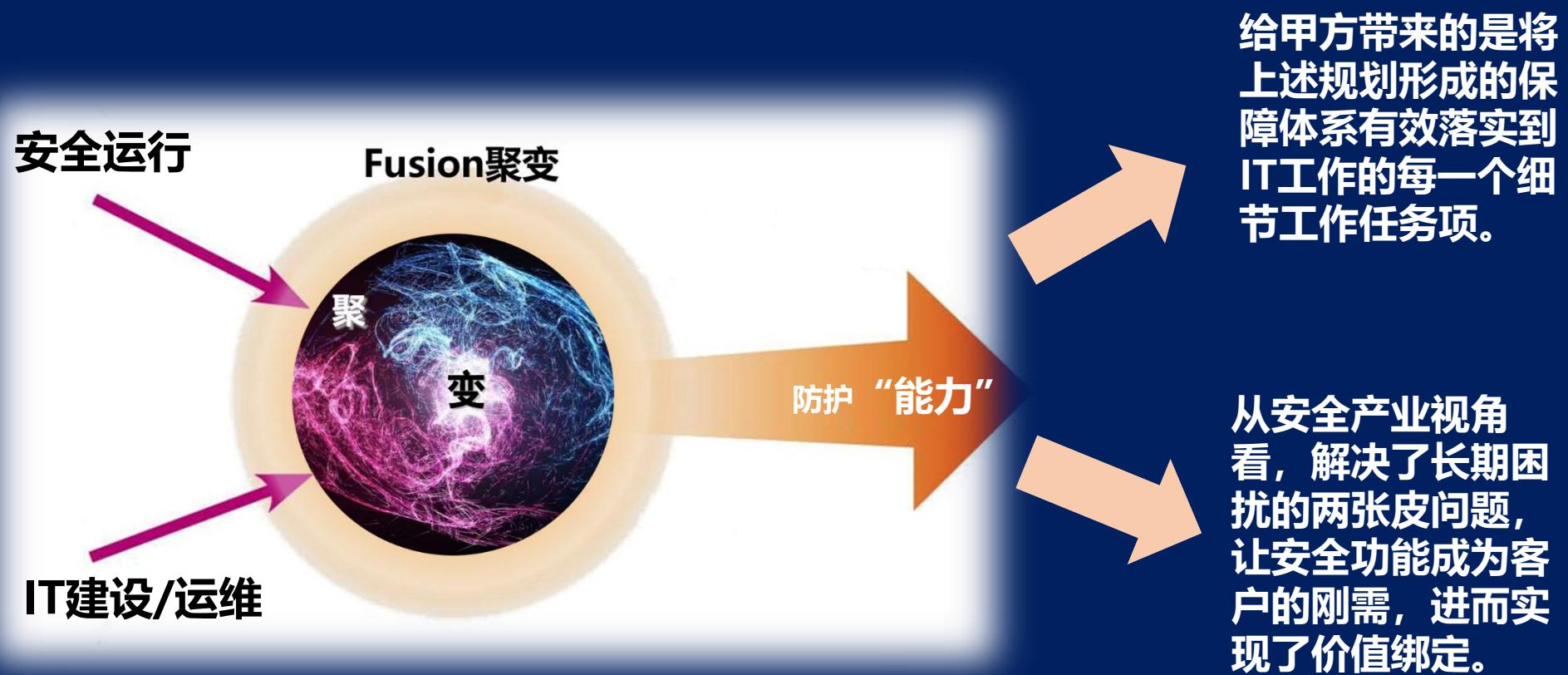
综合协调组



| 事件级别 | 三级事件 | 四级事件 | 五级事件 |
|------|------|------|------|
| 数量 | 4 | 72 | 235 |



安全运行与IT建设/运维的聚，建立了真正有效的防护能力。



聚变之三

人员组织与技术平台的 “聚与变”

实战化运行中人员组织与技术平台的协同是关键

实战化
安全运行

信息化变化驱动

基础结构安全



ARCHITECTURE

解决环境变化、
资产变化、产品
变化、配置变化
和漏洞出现

产品变化驱动

纵深防御



PASSIVE DEFENSE

满足安全防护
产品的建设部
署、运行维护
和适应调整

威胁变化驱动

积极防御



ACTIVE DEFENSE

实现对威胁的
猎杀、事件监
测与响应、取
证、欺骗操控

情报变化驱动

威胁情报



INTELLIGENCE

情报数据的收
集、整理、分
析、关联、溯
源、研判等

监管变化驱动

反制进攻



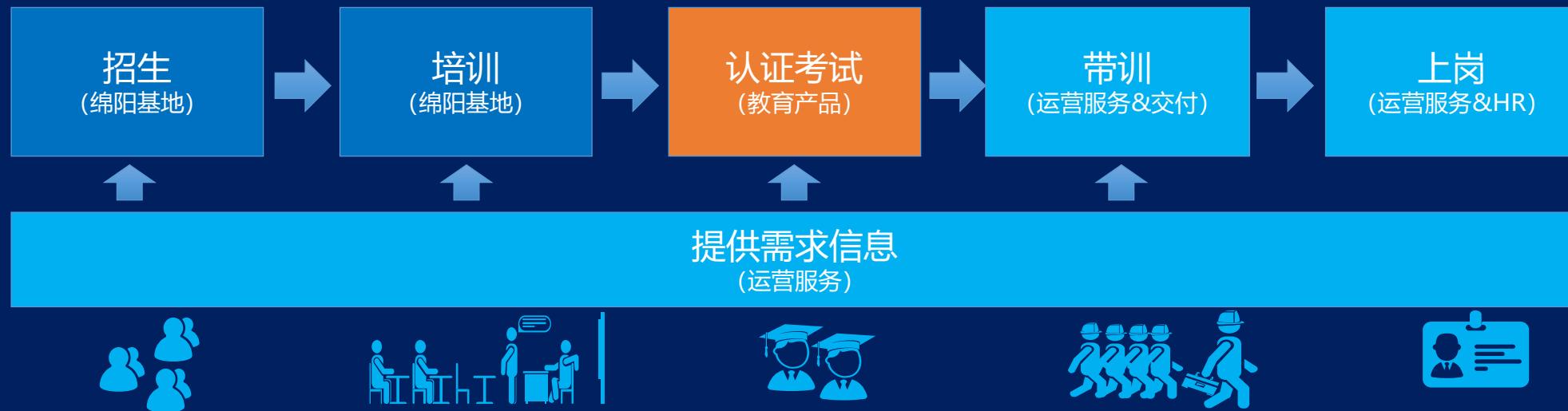
OFFENSE

常态化的开展
红蓝对抗、安
全众测、实网
攻防演习

不同的场景需要不同技能的安全人员参与



实践：绵阳安全运营人才实训基地培养安全运营人才。



- 已完成招生642人，培养389人，完成认证工程师144人，具备300人并行实训能力。
- 蜂巢计划启动，安运总控中心启动，210名安运工程师服务于120多个客户。

实践：DATACON大数据安全分析比赛培养安全分析人员。



- 线上积分赛：来自全球多个国家和地区的**551支战队、3000多名选手参赛**，美国Northeastern University、卡塔尔Hamad Bin Khalifa University、香港大学等都有团队报名参加比赛。
- 线下决赛：9支决赛团队，1支企业团队；湖南大学等多个高校将此次比赛纳入了计算机相关课程学分考核体系。
- 奇安信与清华、北大、中科大等30多所知名高校联合举办。
- **15家五百强企业直通就业**。
- 构建大数据资源池，模拟DNS攻击流量检测、恶意代码检测、攻击源与攻击者分析大数据实战场景，**培养选拔大数据安全分析人才**！

实践：安全训练营培养攻防渗透人才。

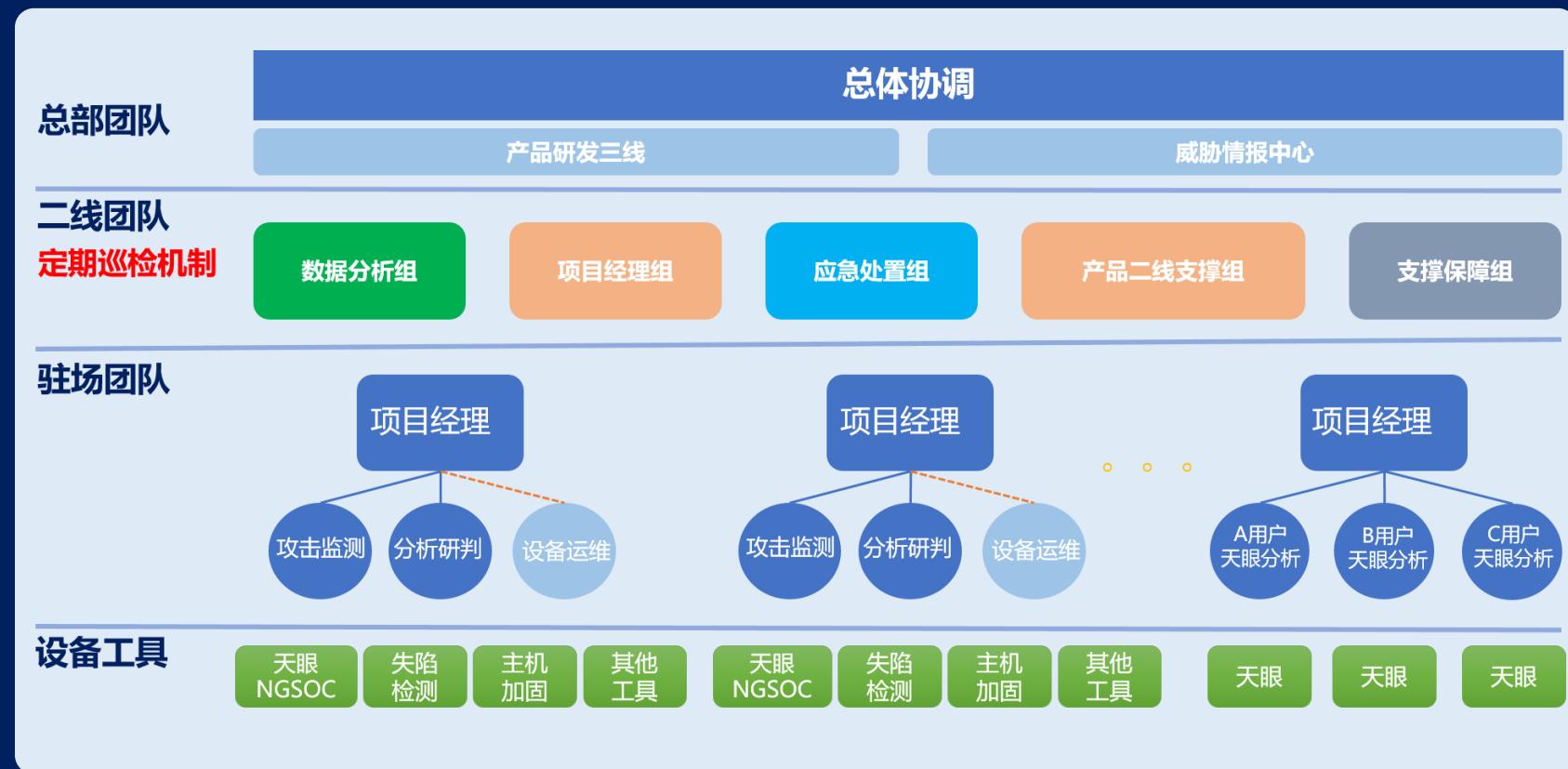


- **来自全球知名黑客团队讲师**，盘古团队、独角兽团队、伏尔甘团队、奇安信威胁情报中心、代码卫士团队、蓝莲花团队、长亭科技、中国信息安全测评中心、荷兰生物黑客大神Patrick Paumen、DEF CON生物黑客Village的负责人Nina Alli、全球知名黑客本杰明等国内外知名安全团队、黑客专家。
- **累计开发60门培训课程**，课程覆盖大数据、APT、威胁情报、云、人工智能、芯片安全、渗透测试、漏洞挖掘、移动安全、应急响应、无线安全、工控、web安全、生物黑客等领域。
- **累计培训2000多名学员**，覆盖政府、医疗、能源制造、教育、军工、运营商、金融、交通运输等行业领域安全从业者人员，有效提升从业者安全能力，挖掘培养安全人才。

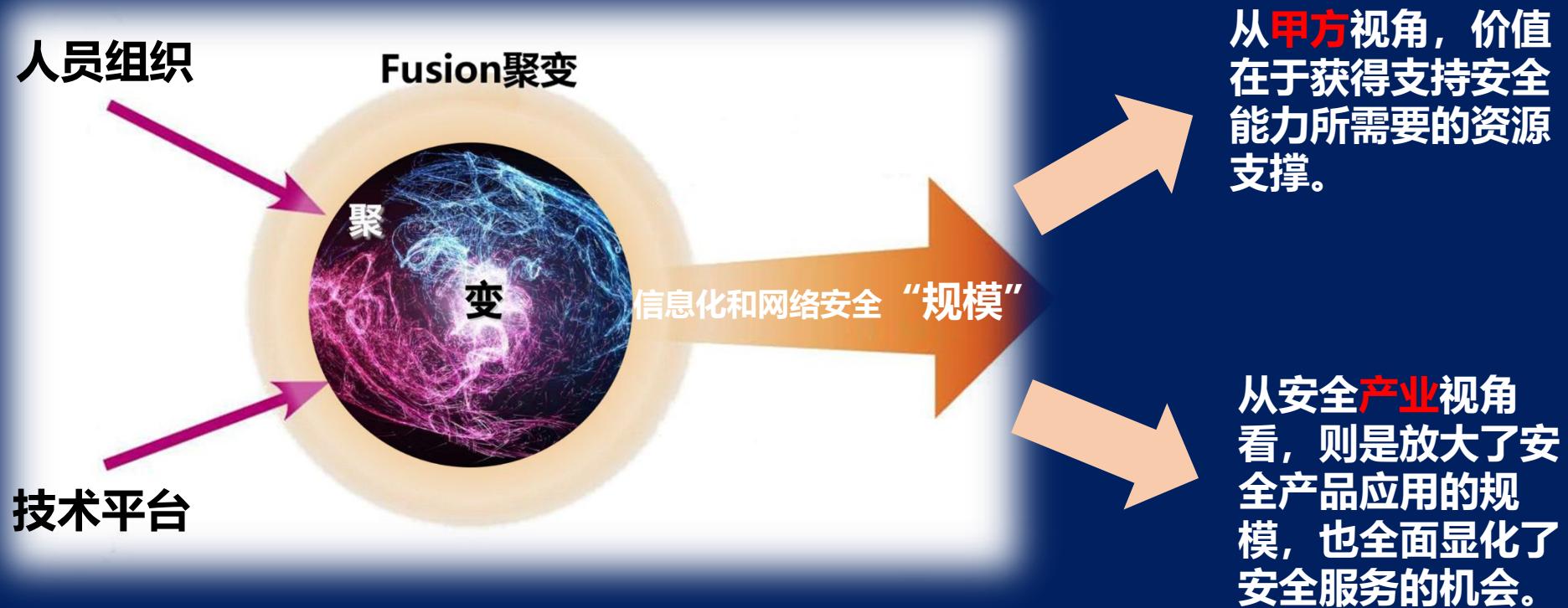


实践：规模化、体系化投入攻防演习的攻击和防守。

- 2019年前5个月奇安信集团共参与50场实战攻防演习，**最高峰每周参加12场攻防演习。**
- 准备了攻击队68支，攻击人员224人。
- 500+安运工程师（不包括后台支撑人员）7*24小时防护值守。
- 为参与演习的头部客户65家提供防护，约占HW目标单位总数的60%；涉及到金融、央企、政府部委、传媒、运营商等行业及二级单位近200家单位。



人员组织与技术平台的聚，扩大了信息化和网络安全规模。



聚变之四

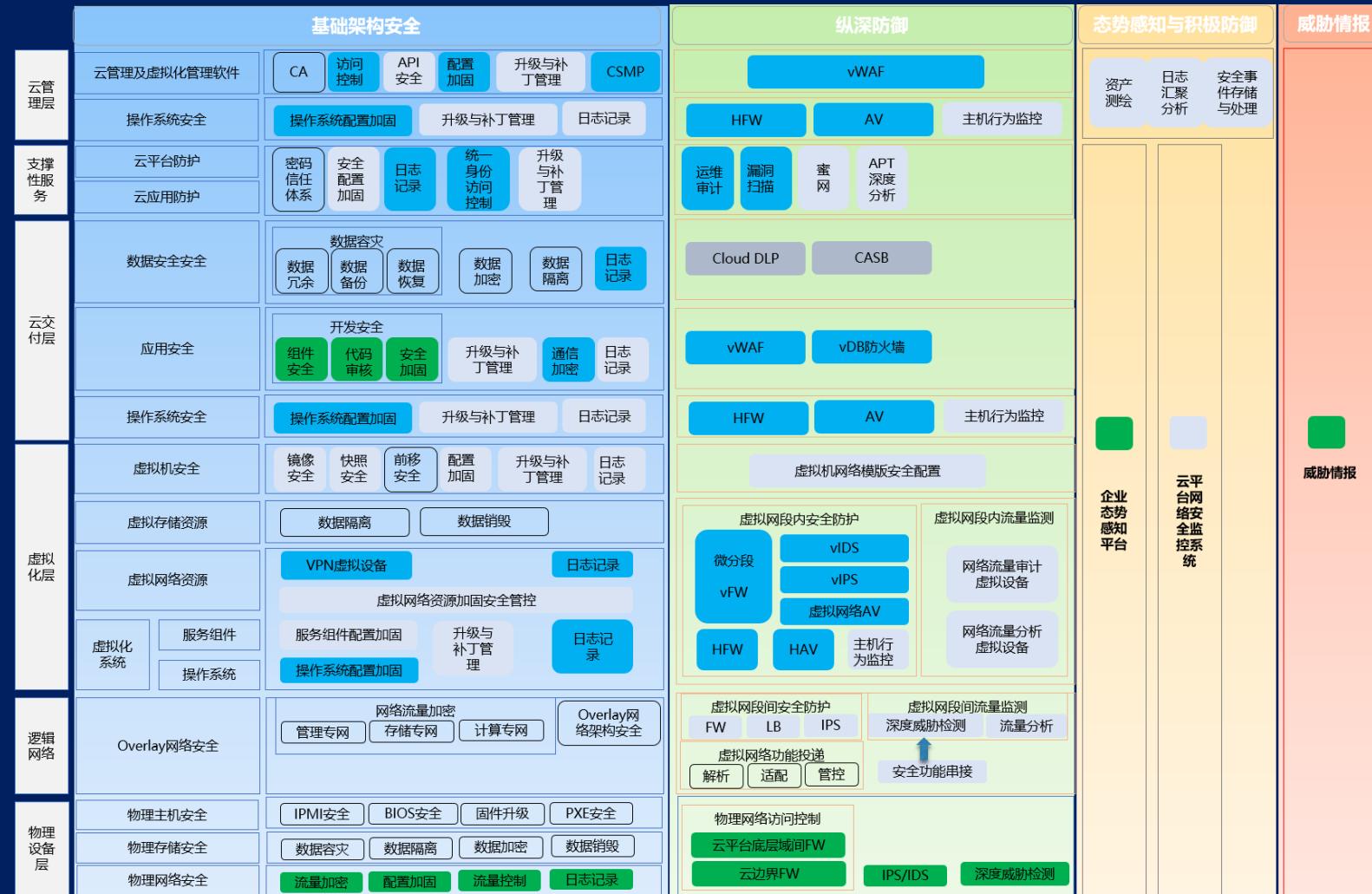
不同厂商产品与服务能力的“聚与变”

能力导向的防护体系建设是叠加演进，而不是淘汰演进



数据驱动安全

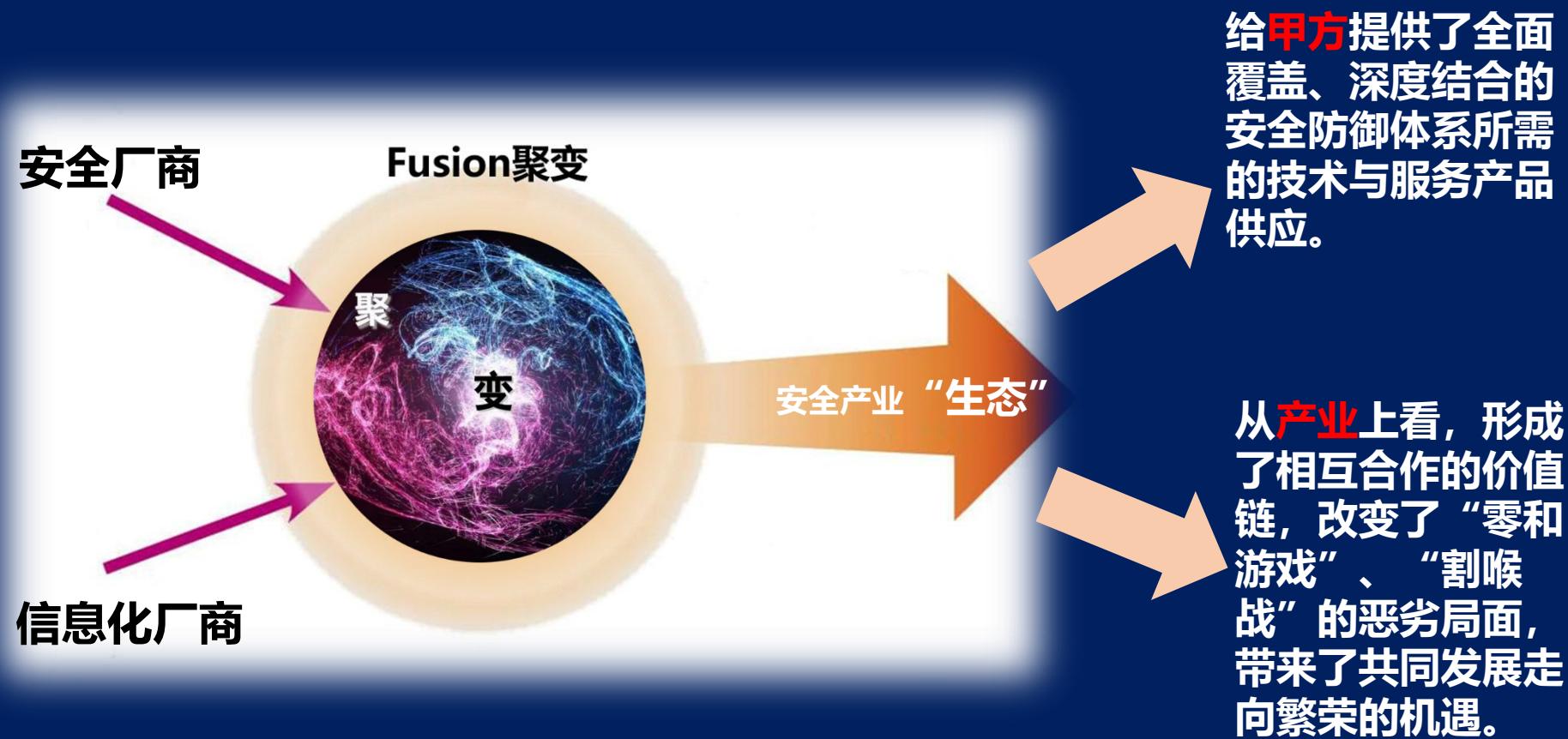
安全与信息化的深度结合和全面覆盖是一个体系，需要协同多家厂商的多样化能力



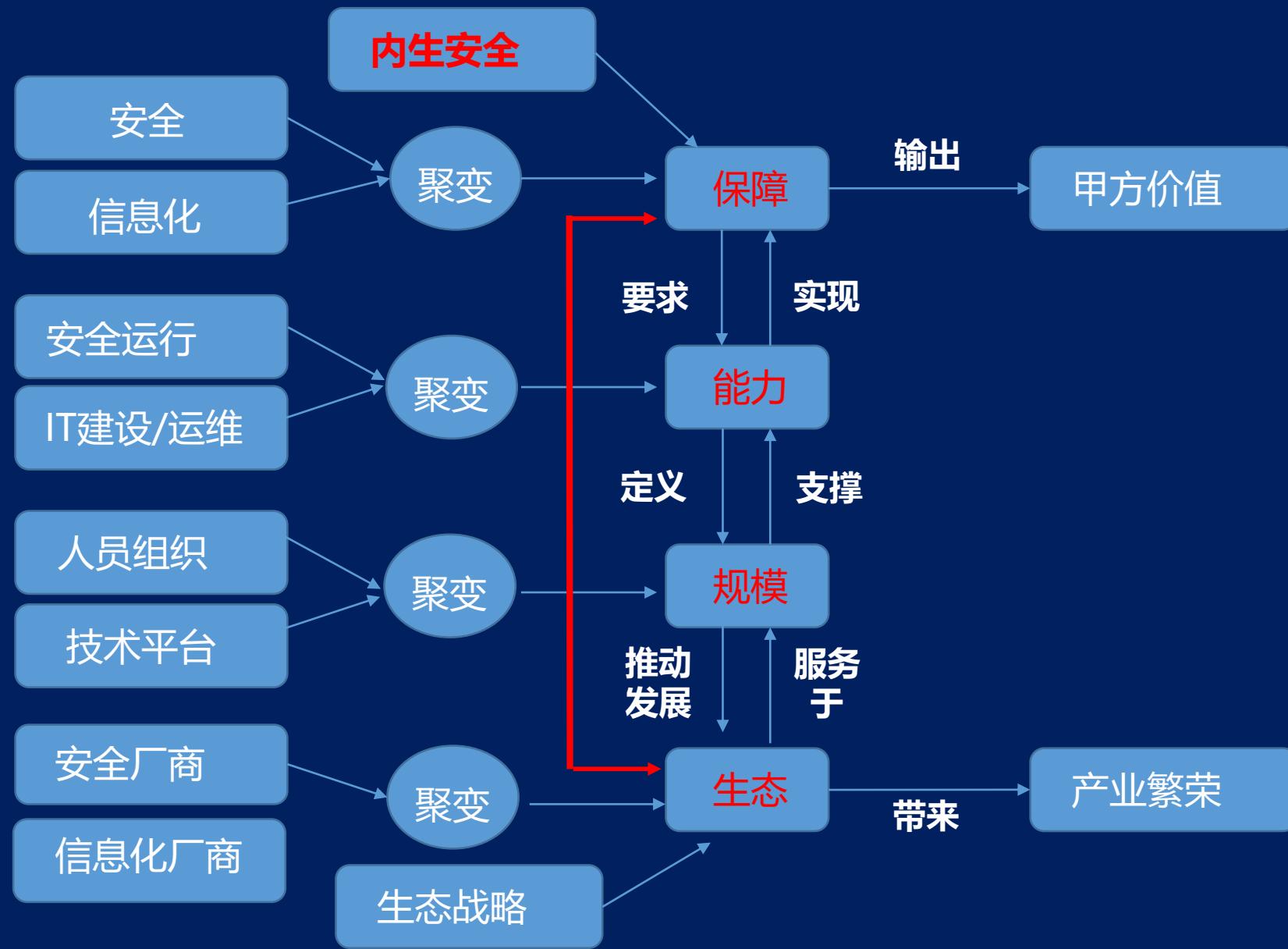
实践：奇安信以规划和集成，聚合了众多细分领域专注公司的能力。



不同安全与信息化厂商在技术与服务产品的聚，产生了网安产业生态。



四个聚变的关系。



全球数字化背景之下，网络强国的建设需要中国特色的信息化之路，更需要围绕安全可控的技术路线，实现对信息化投资和业务运营的有效保障，本质安全与过程安全的聚合，是上述四个聚合的实践，也是最终达到内生安全的必由之路。

内生安全

面向自主可控信息化系统的内生安全体系

— 过程安全

面向攻防的安全运营及服务

(安全咨询、安全运维、网络对抗、安全评估、应急响应、新技术服务等)

面向攻防的安全防护系统

(网络安全、终端安全、数据安全、安全管理、安全大数据、可信计算、身份与访问管理、业务安全、安全支撑工具等)

+ 本质安全

整机

(PC、服务器、网络设备、PLC)

PaaS平台

核心软件

数据库(关系型、实时型) 中间件(领域中间件) 工具软件(办公套件)

核心芯片

(网络交换芯片、存储控制器芯片、安全密码芯片、可信芯片、FPGA、MCU、IGBT、高端模拟芯片)

PK体系 (CPU+OS)

安全防护体系

安全的信息系统

呼吁：

不论正在进行的数字化转型，还是安全可控的信息化特色之路，都需要把握住即将到来的十四五规划机遇期，由领先的政企单位推动，综合性的大型安全企业担当，聚合所有细分领域安全企业的能力，一起构建跟信息化深度结合的融合安全生态，为信息化投资和数字业务提供有效保障，为国家、经济、社会转型升级保驾护航！

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE