奇安信
新一代网络安全领军者

基于“44333”思想构建现代政企网络安全防护体系

奇安信 陈志华

奇安信
新一代网络安全领军者

目　　录

Contents

奇安信
新一代网络安全领军者

01 关键信息基础设施面临的网络安全风险

新信息技术革命 | 数字化转型上升为国家战略

奇安信
新一代网络安全领军者

“加快传统产业数字化、智能化，做大做强数字经济，拓展经济发展新空间。”

习近平
2016年10月9日

“聚焦前沿，聚焦共赢，推动数字经济创新合作，共享发展机遇。”

李克强
2017年5月26日

中国十三五规划的6大举措都和数字化转型相关

数字经济规模迅速增长

奇安信
新一代网络安全领军者

至2018年底

网民规模：
8.29亿

互联网普及率：
59.6%

数字经济规模：
31.3万亿

占GDP比重：
34.8%

当前我国数字经济规模位居全球第二，数字经济与实体经济深度融合，有力促进供给侧结构性改革。

习近平指出：“安全是发展的前提，发展是安全的保障，安全和发展要同步推进。我们一定要认识到，古往今来，很多技术都是‘双刃剑’，一方面可以造福社会、造福人民，另一方面也可以被一些人用来损害社会公共利益和民众利益。”

数字化转型引发新安全威胁丨三大安全威胁

奇安信
新一代网络安全

网络犯罪

个人信息滥用，数据泄露、网络诈骗，数据窃取

关键信息基础设施攻击

勒索攻击、敏感数据窃取，直接威胁国家稳定和经济运行

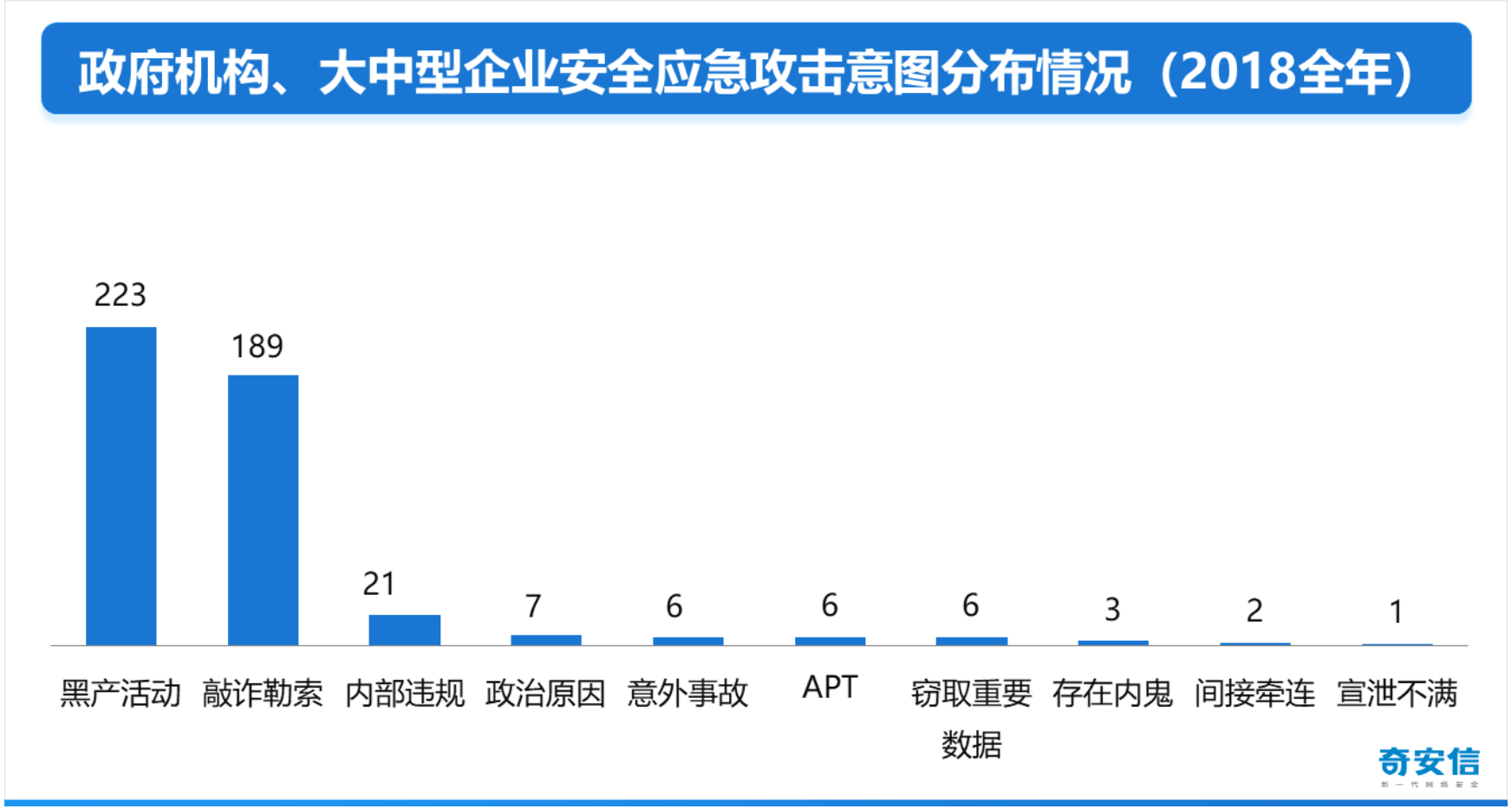
国家对抗和网络空间利益重新划分

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对抗升级

网络攻击意图分布情况

奇安信
新一代网络安全领军者

2018年奇安信集团安服团队共参与和处置了717起全国范围内的网络安全应急响应事件，从行业报告排名可知，攻击者的主要攻击对象为公检法、各级政府部门以及医疗卫生，其次为金融、教育培训、IT信息技术和事业单位，从中窃取数据、敲诈勒索。



面对的新型安全挑战相比还存在三大不足

奇安信
新一代网络安全领军者

我国成为APT攻击重灾区，但防护能力不足

根据奇安信威胁情报中心的数据，我国是APT攻击的主要受害国，仅在2015-2018年，奇安信天眼实验室和奇安信追日团队就发现了多达38个针对我国的网络攻击组织。这些针对我国政府部门、重要企事业和科研机构的攻击已经造成了大量数据泄露。

关键网站漏洞修复率不足半数

根据奇安信互联网安全中心发布的数据，通过对2016年补天平台的备案网站漏洞的抽样调查，我们发现，平均漏洞修复率仅为42.9%。即便是在能够修复漏洞的网站中，仍有近2/3的网站存在漏洞修复周期过长、修复很不及时（大于7天）的问题。

传统安全防护手段落后，彼此之间脱节

传统的安全产品以配置安全策略规则、碰撞防护的思路为主，由于安全产品类型、厂商、型号和策略众多，在遭受威胁和攻击时，它们相互之间的识别、防护、检测、预警、响应和处置的协调能力较差，不能形成完整的安全闭环体系。

关键信息基础设施面临的网络安全风险与挑战

奇安信
新一代网络安全领军者

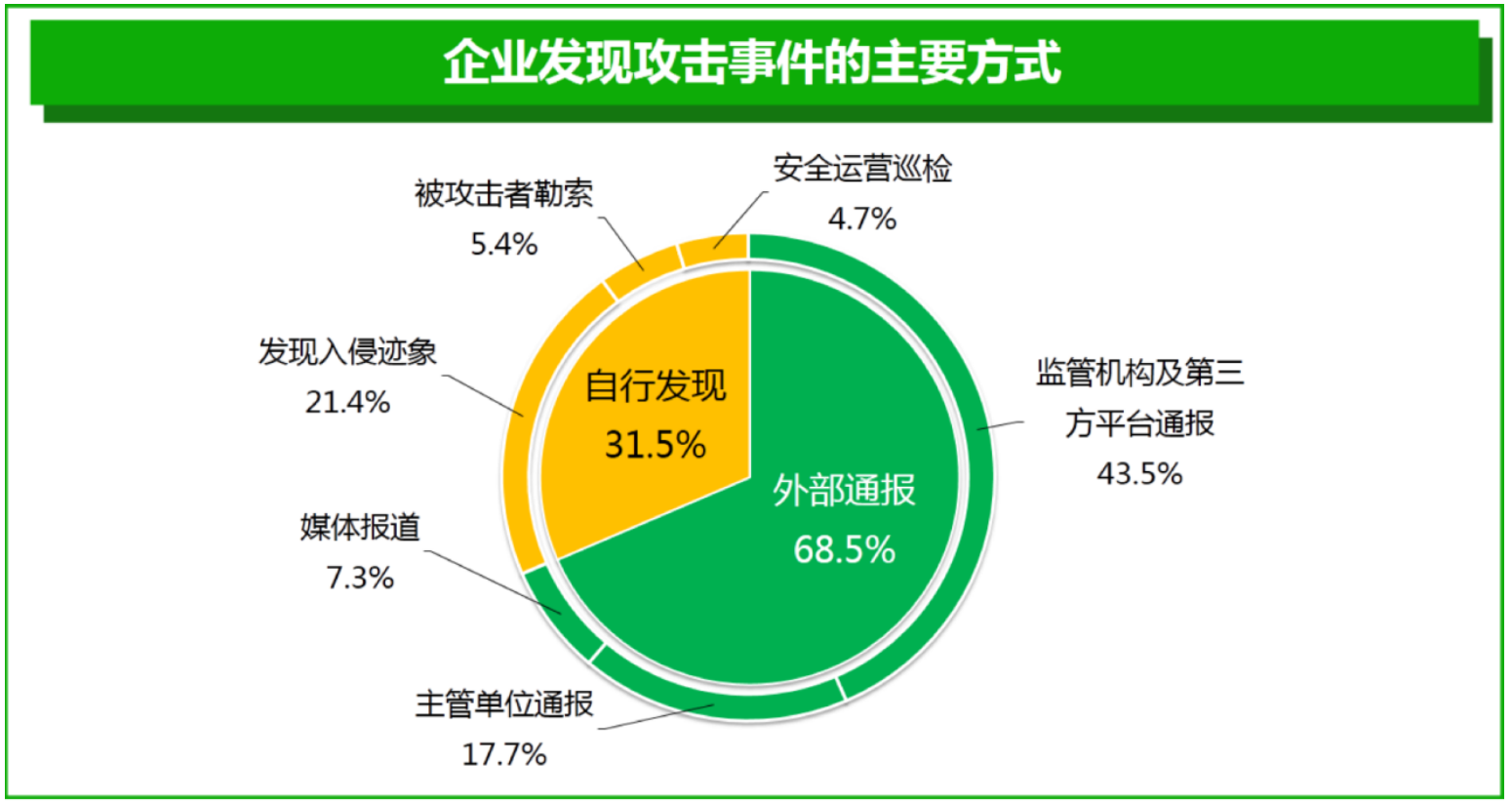
攻防能力不对称

漏洞是永远存在的！ → 没有攻不破的系统！

企业面临的网络安全风险与挑战

奇安信
新一代网络安全领军者

- 习主席:“谁进来了不知道、是敌是友不知道、干了什么不知道”



关键信息基础设施网络安全风险与挑战

奇安信
新一代网络安全领军者

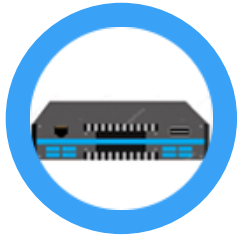
落后的安全防护体系Vs灵活多变的渗透技术

安全技术人才缺失Vs黑客团队军事化

一片祥和的监控页面Vs暗流涌动的隐蔽信道

设备不可靠

无法抵御各类新型网络攻击



人不可信

内鬼频发

未知的威胁

不确定也没法确定会面对何种攻击和人、设备、网络、系统、数据所遭受的风险。

奇安信
新一代网络安全领军者

02 | “44333”网络安全新思想

树立正确的现代网络安全观

阻碍政府部门、企业建立现代网络安全防御体系的首要障碍，既不是成本问题，也不是技术问题，而是观念问题。传统安全观主要立足于防护，尽可能地避免安全事件的发生，而不太重视应急响应机制的建设。

- 安全管理以免责为目标
- 害怕暴露问题，存在侥幸心理
- 关心自身损失，忽略社会责任
- 缺乏动态防御与应急响应意识

而新型的安全观认为，“防不住是一定的”，应当立足于一定防不住的假设来设计自己的防御、监控和运营系统。

基于“44333”建设综合防御能力体系

奇安信
新一代网络安全领军者

四个假设

系统一定有没被发现的漏洞

系统一定有没打补丁的已知漏洞

系统已经被黑

一定有内鬼，边界已被突破

四新战略

新战具：第三代网络安全技术

新战力：数据驱动安全

新战术：零信任架构

新战法：人+机器的安全运营

三位一体

高位能力

中位能力

低位能力

三同步

同步规划

同步建设

同步运营

三方制衡

用户

云服务商

安全公司

四个假设

奇安信
新一代网络安全领军者

假设一	• 系统一定有还没被发现的漏洞
假设二	• 系统一定没打补丁的已知的漏洞
假设三	• 系统已经被黑
假设四	• 一定有“内鬼”，且传统边界已被突破

四新战略

奇安信
新一代网络安全领军者

新战具

第三代网络安全技术
“查行为”

新战力

数据驱动安全

新战术

“零信任”
动态认证与
访问授权

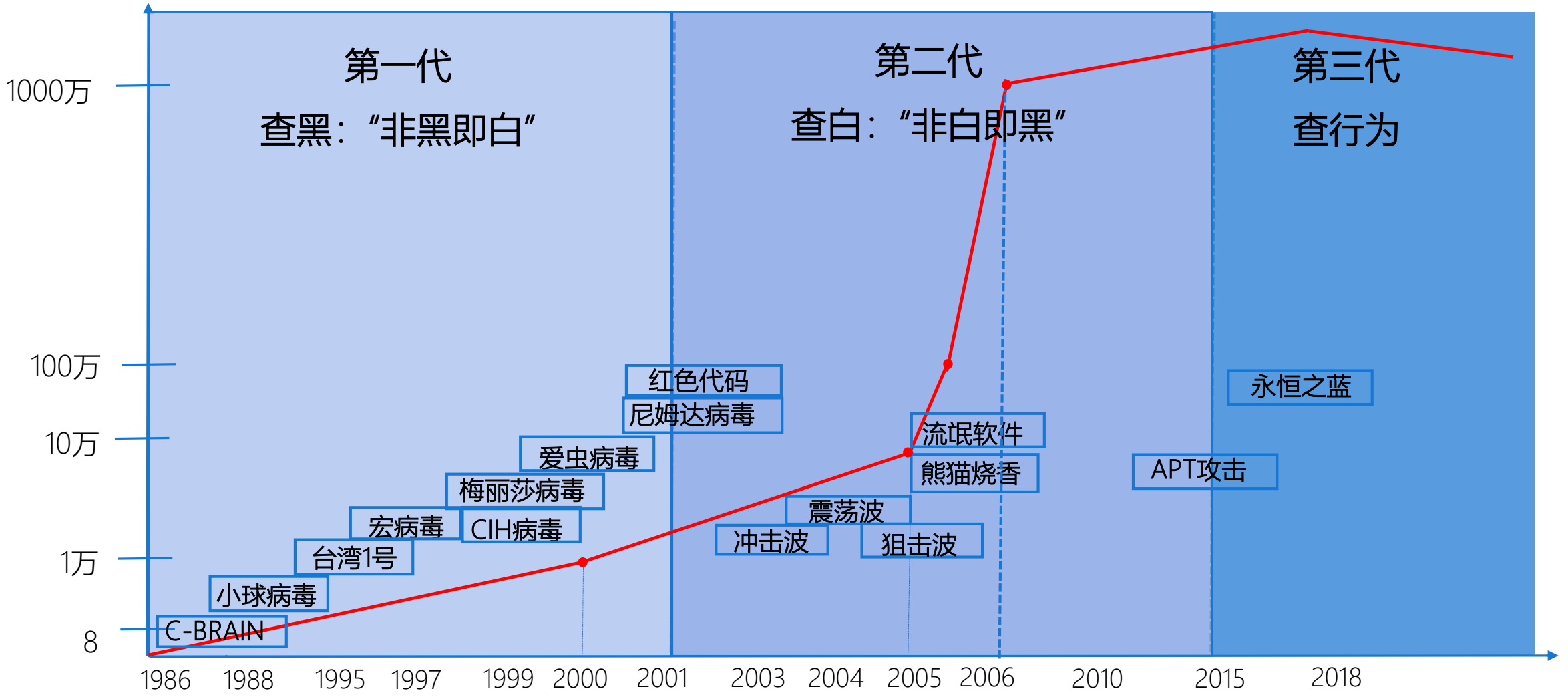
新战法

“人+机器”
新运营体系

四新战略—新战具：第三代网络安全技术

奇安信 新一代网络安全领军者

➢ 网络安全发生了质的变化，必须采用新技术，做到**不依赖黑名单、不信任白名单、不放过可疑行为**



四新战略—新战力：数据驱动安全

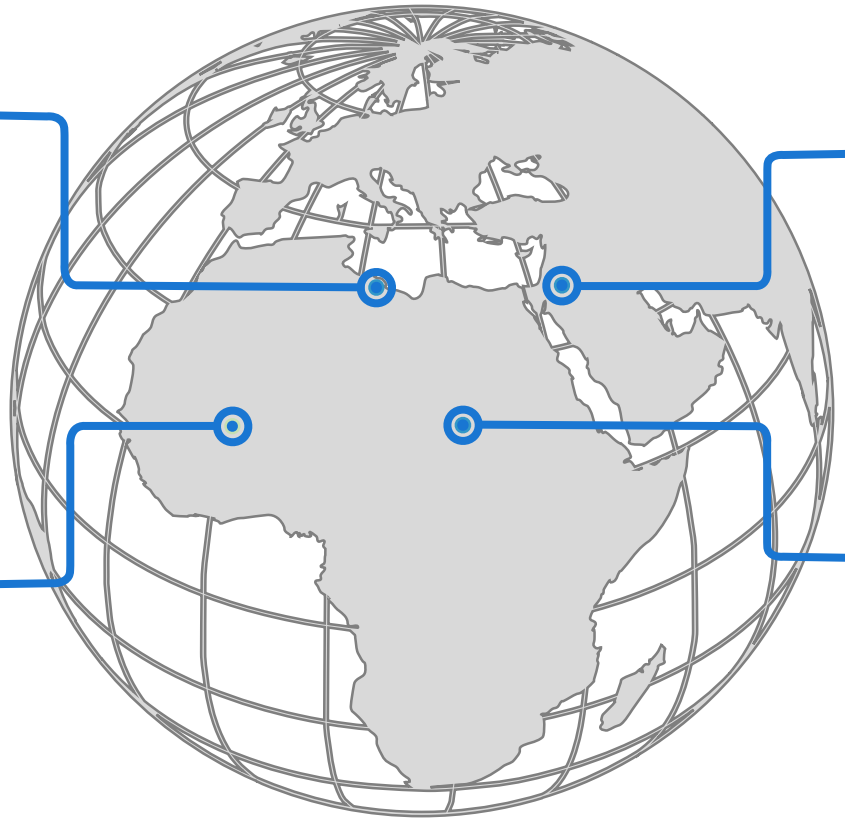
奇安信
新一代网络安全领军者

- 通过对各类网络行为数据的记录、存储和分析，从更高的视野、更广的角度发现异常、捕获威胁
- 实现威胁与入侵的快速监测、快速发现和快速响应，更好地应对不断变化、日益增长的安全威胁

四新战略—新战术：动态认证与访问授权

奇安信
新一代网络安全领军者

- 几乎所有的网络安全事件都和账号、密码、电脑、手机、服务器、路由器等被监控有关
- **信任根据任务访问动态建立，默认不信任任何设备、任何IP、任何身份、任何账号……**



全面身份化

建设统一身份源，实现全网用户、设备、应用、API接口的统一身份化，实现统一权限梳理。

风险度量化

采用大数据分析技术，基于人和设备的环境数据、访问行为数据，进行风险建模，度量潜在的安全风险。

授权动态化

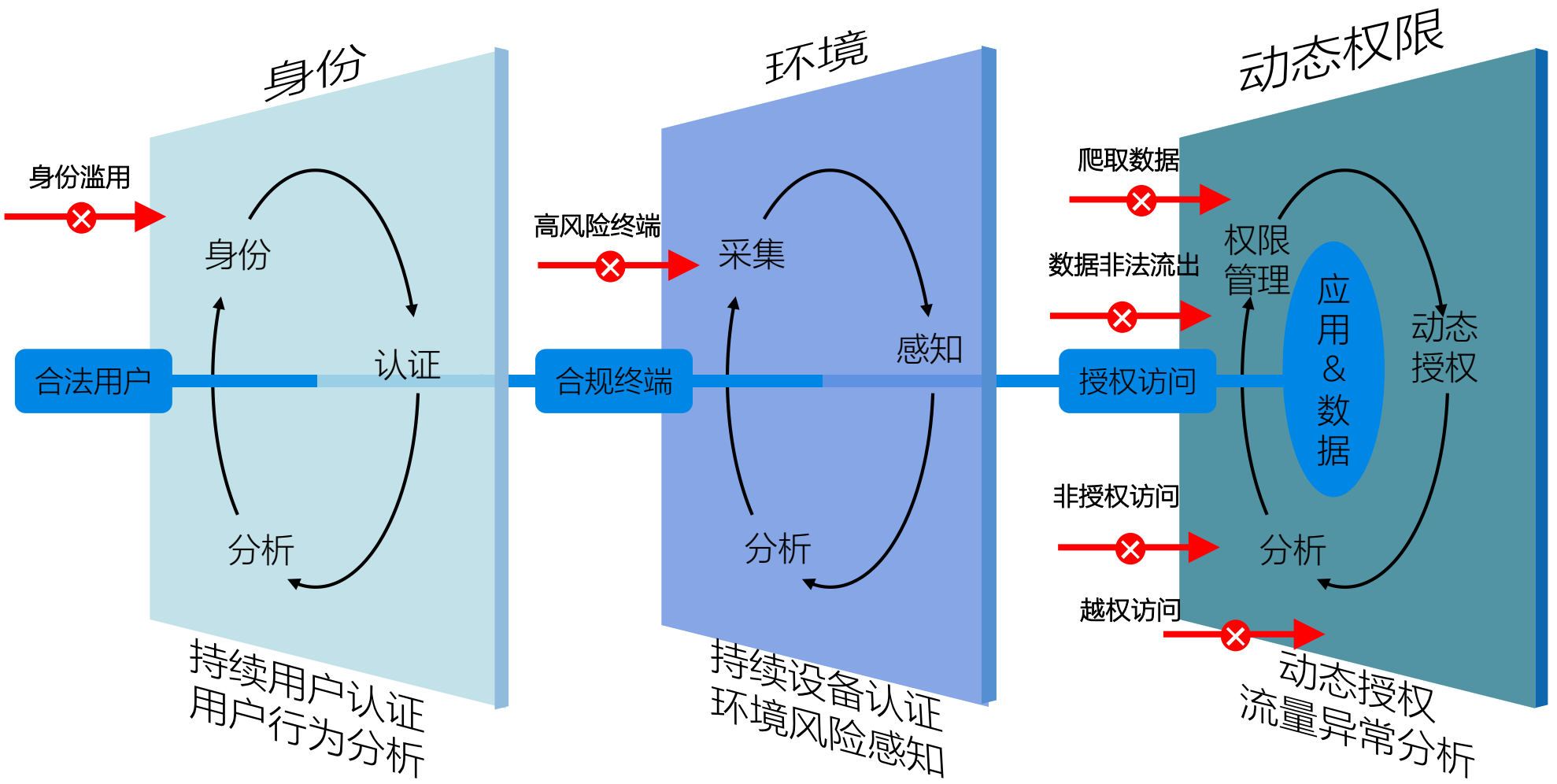
访问控制进行细粒度授权，基于风险的度量和信任评估，动态调整授权，实现自适应访问控制。

管理自动化

采用机器学习算法，基于高级身份分析技术和工作流引擎，实现身份与访问管理的自动化。

四新战略—新战术：动态认证与访问授权

奇安信
新一代网络安全领军者



四新战略—新战法：“人+机器”的新运营体系

奇安信
新一代网络安全领军者

- 智能化时代，网络安全的本质是人与人的对抗、人与机器的对抗、人工智能的对抗
- 机器不能取代网络安全工程师，“人+机器”协同作战，能极大提升战斗力

- 态势感知
- 资产告警
- 网站监测
- 威胁情报监测

- 终端安全
- 边界安全
- 安全域
- 服务器安全
- 云安全
- 工控安全
- 重要时期安全保障

- 安全事件响应处置
- 追踪溯源
- 运营保障

- 风险评估
- 代码检测
- 渗透测试
- Web失陷检测
- 全流量威胁分析
- 对抗式演习

三位一体

奇安信
新一代网络安全领军者

高位、中位、低位立体联动的一体化体系

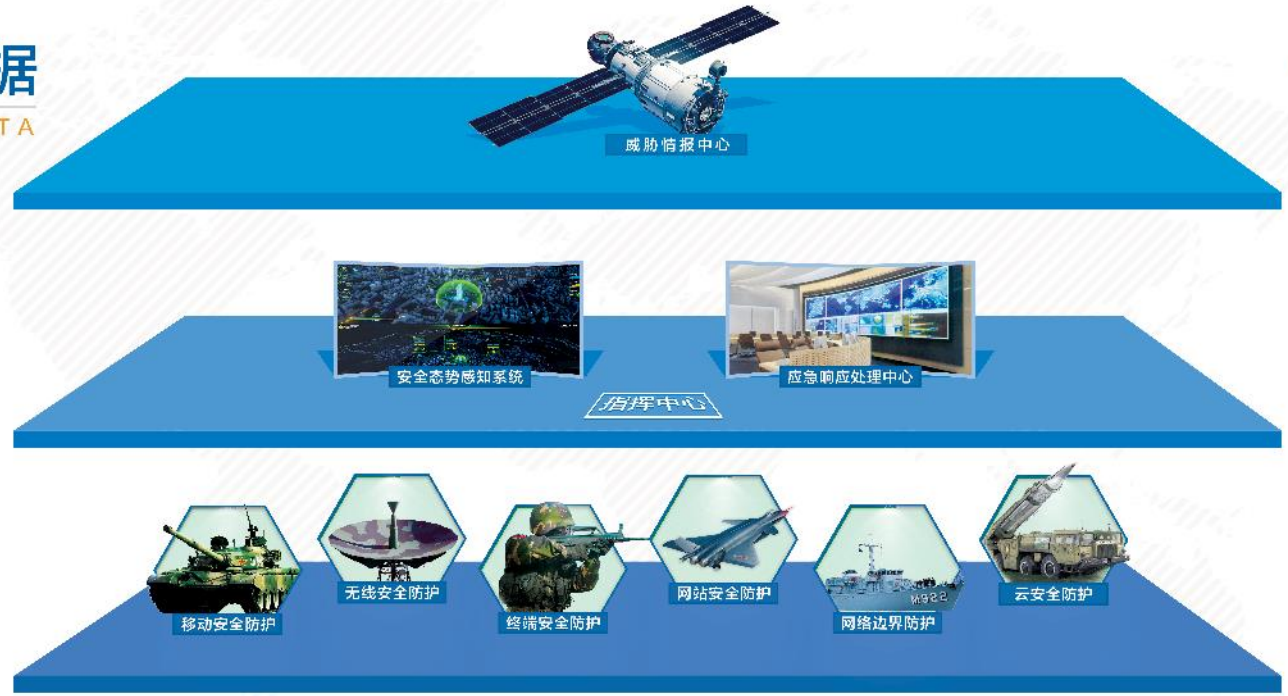
实现从低到高的数据传送、从高到低的情报指令

高位能力
“外脑”

中位能力
“指挥中心”

低位能力
“一线作战部队”

数据驱动安全

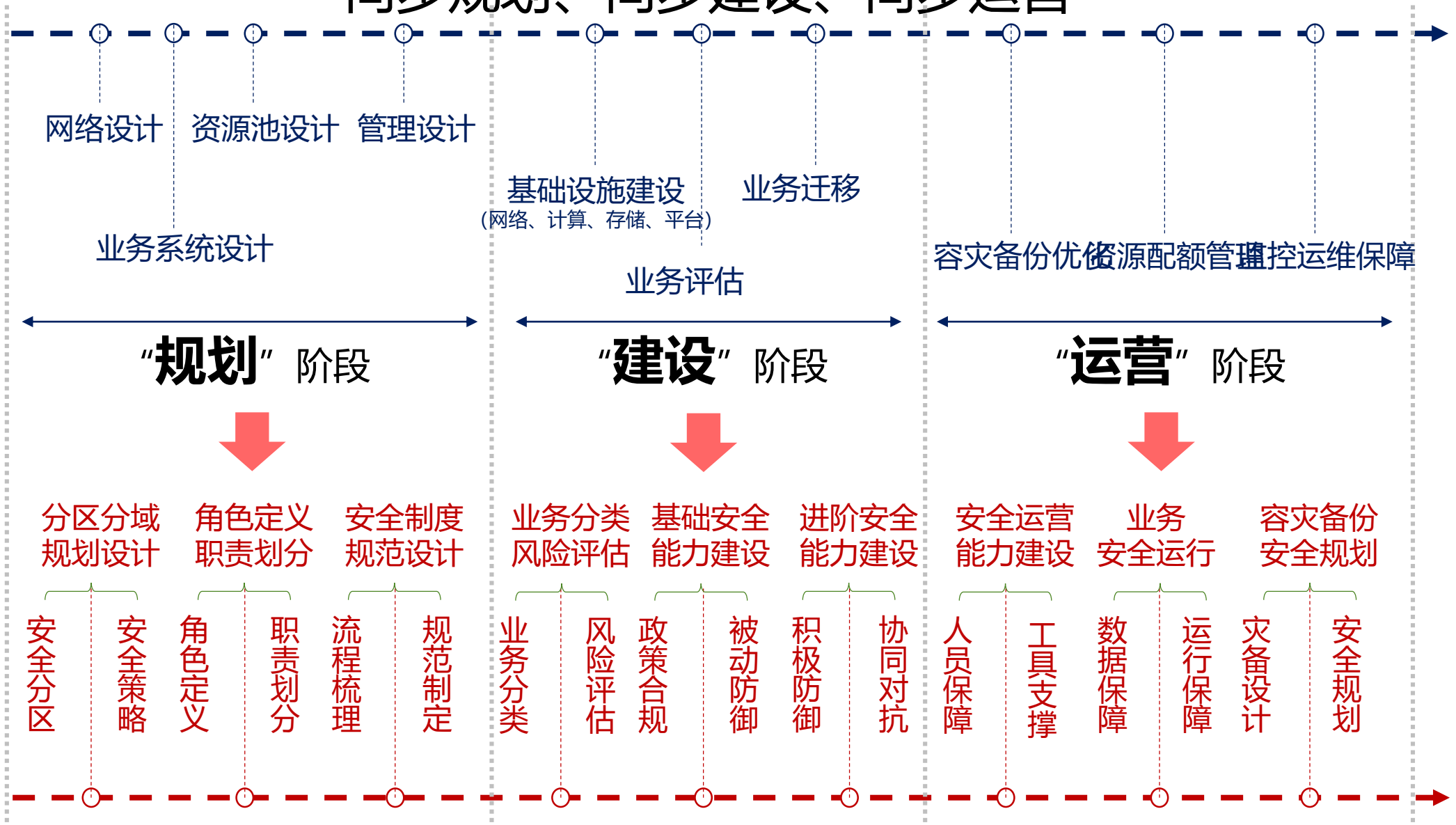


协同联动防御

三同步

奇安信 新一代网络安全领军者

同步规划、同步建设、同步运营

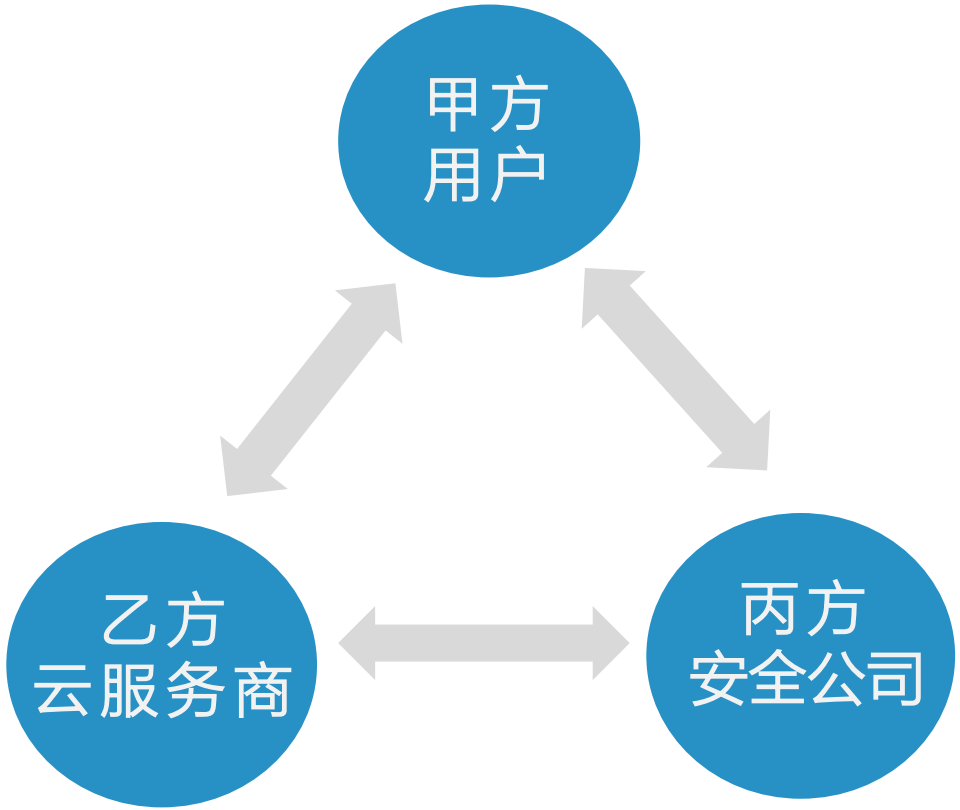


三方制衡

奇安信
新一代网络安全领军者

云和大数据平台存储的都是数字化信息，像安全“黑洞”

引入第三方的安全公司，对云服务商形成有力制衡，真正对用户安全负责



- 甲方用户**严格要求**
- 乙方云服务商**提高标准**
- 丙方安全公司**查漏补缺**
- 三方互相制衡，才能从最大程度上杜绝漏洞，长治久安。

奇安信
新一代网络安全领军者

03 | 建立现代政企网络安全防护体系

防御体系+响应体系

奇安信
新一代网络安全领军者

过去，传统的政府部门、企业的安全防御体系特点是：单点防御、各自为战。它们分别从不同的厂商采购各种各样的安全产品或服务，尽管表面上“设施齐全”，但实际上不同的安全产品之间却独立运行，无法全面地把控自身网络安全问题，对于自身安全状况也处于一种完全不自知的状态。同时还普遍存在“重防御，轻响应”的问题，一旦发生安全事件往往无所适从，从而产生了很多不必要的损失。

在网络安全等级保护不断升级、网络安全制度不断完善的前提下，我们的目标应该是搭建一个现代政企网络安全防护体系。

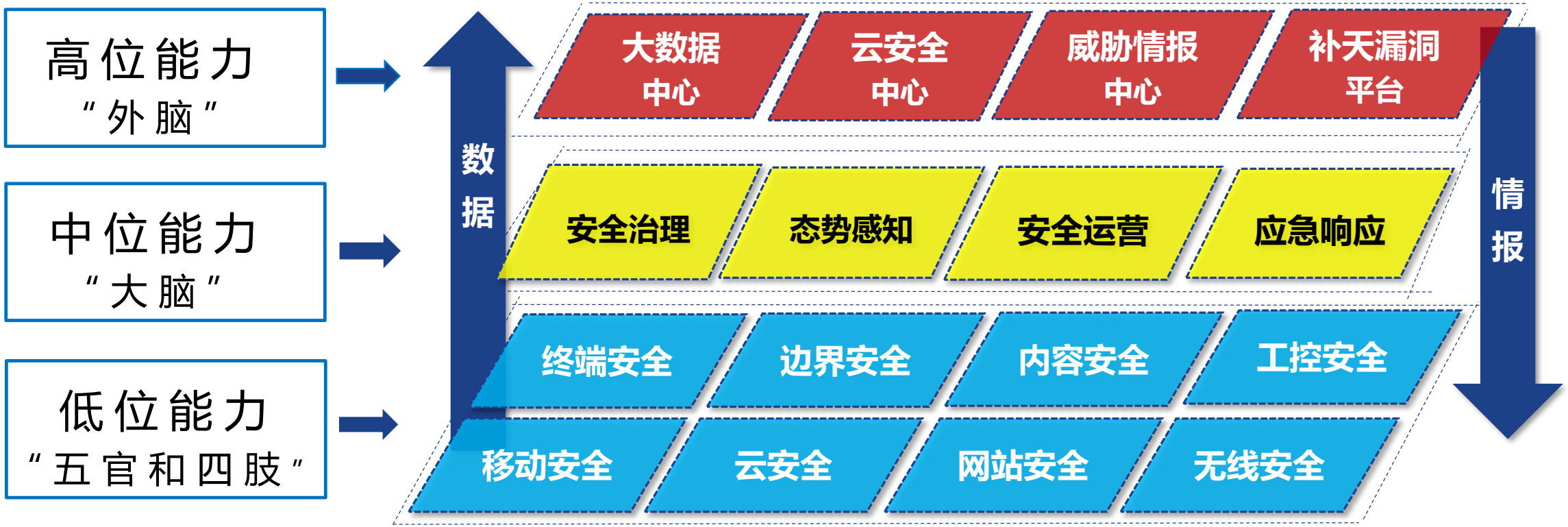
这个体系的核心思想是：建立数据驱动、协同联动、“云+端+边界”的立体纵深防御体系，以及迅捷有效的网络安全应急响应体系，及时应对各种突发的网络安全事件。

建立数据驱动的协同联动防御体系

奇安信
新一代网络安全领军者

高位、中位、低位立体联动的一体化体系

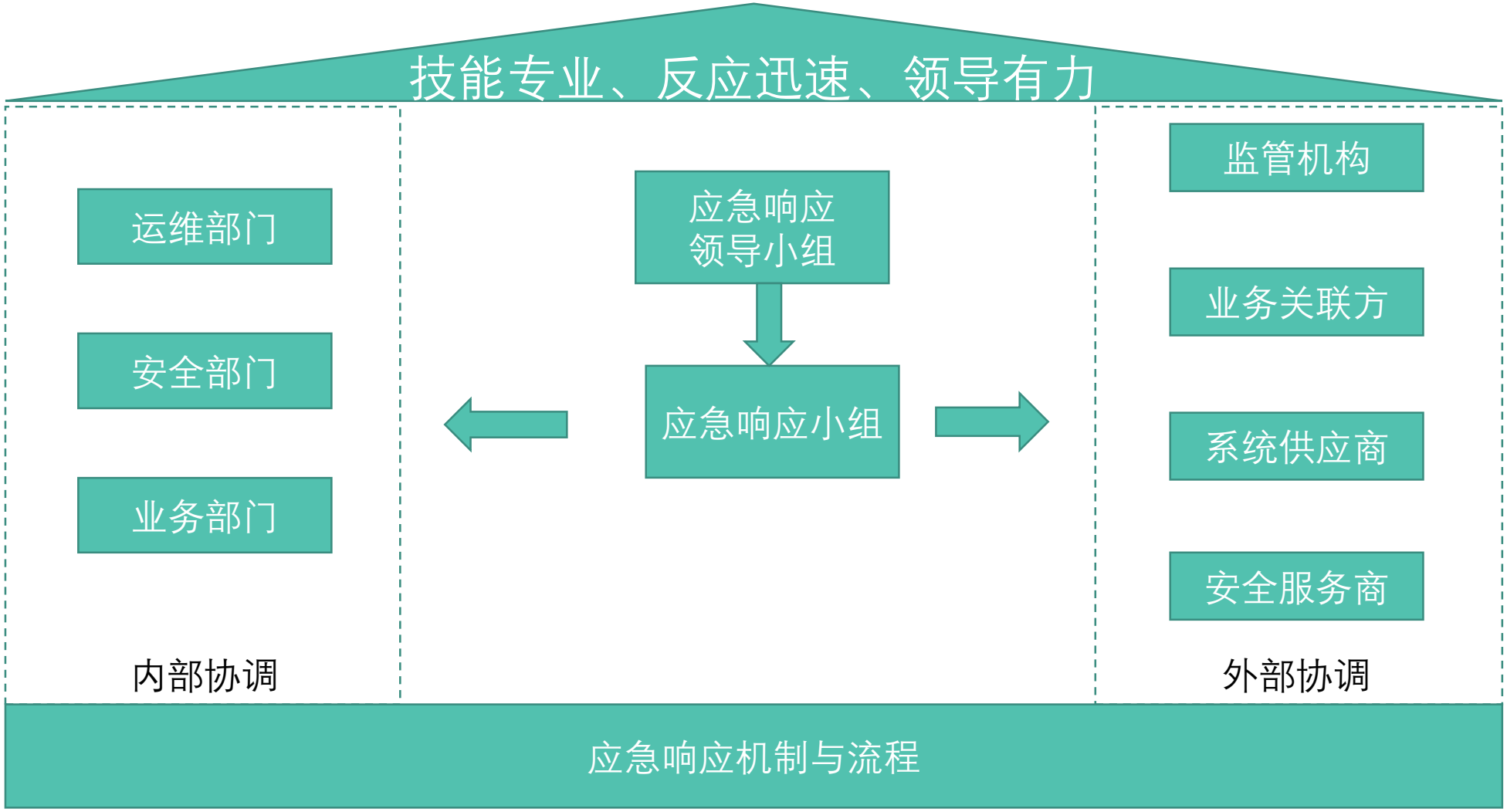
实现从低到高的数据传送、从高到低的情报指令



建立有效的网络安全应急响应体系

奇安信
新一代网络安全领军者

网络安全应急响应体系建设的不足，是现代政府部门、企业网络安全建设的主要缺陷之一。这主要是源于人们对“防不住是一定的”这一客观事实的认识不足。

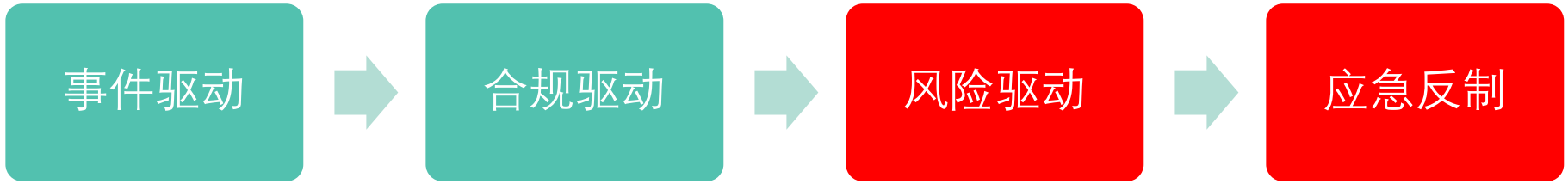


专业的安全服务是保障安全的关键

奇安信
新一代网络安全领军者

在国内政府部门、企业的安全采购过程中，他们往往能够接受为软硬件安全产品买单，却普遍不愿意为安全服务买单。甚至很多政府部门、企业认为，安全服务本应该就是安全产品的售后服务，应该是无偿的。但无论是从运营成本还是商业价值来看，安全服务都要比安全产品高得多。

这就好比是再豪华的汽车，如果没有司机开也不过是废铁一堆。由于安全人才全球性的极度短缺，在网络安全领域，好的司机比好的汽车难找得多，这也就使得安全服务的成本事实上要远大于安全产品的研发成本。对于政府部门、企业安全服务商来说，安全服务的质量和水平才是服务商实力差距和价值高低的根本体现。



信息安全建设发展阶段

奇安信
新一代网络安全领军者

Thank you!