



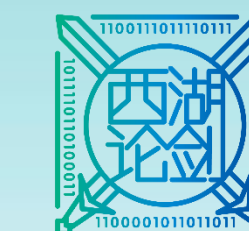
2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

平安集团企业信息安全治理与实践

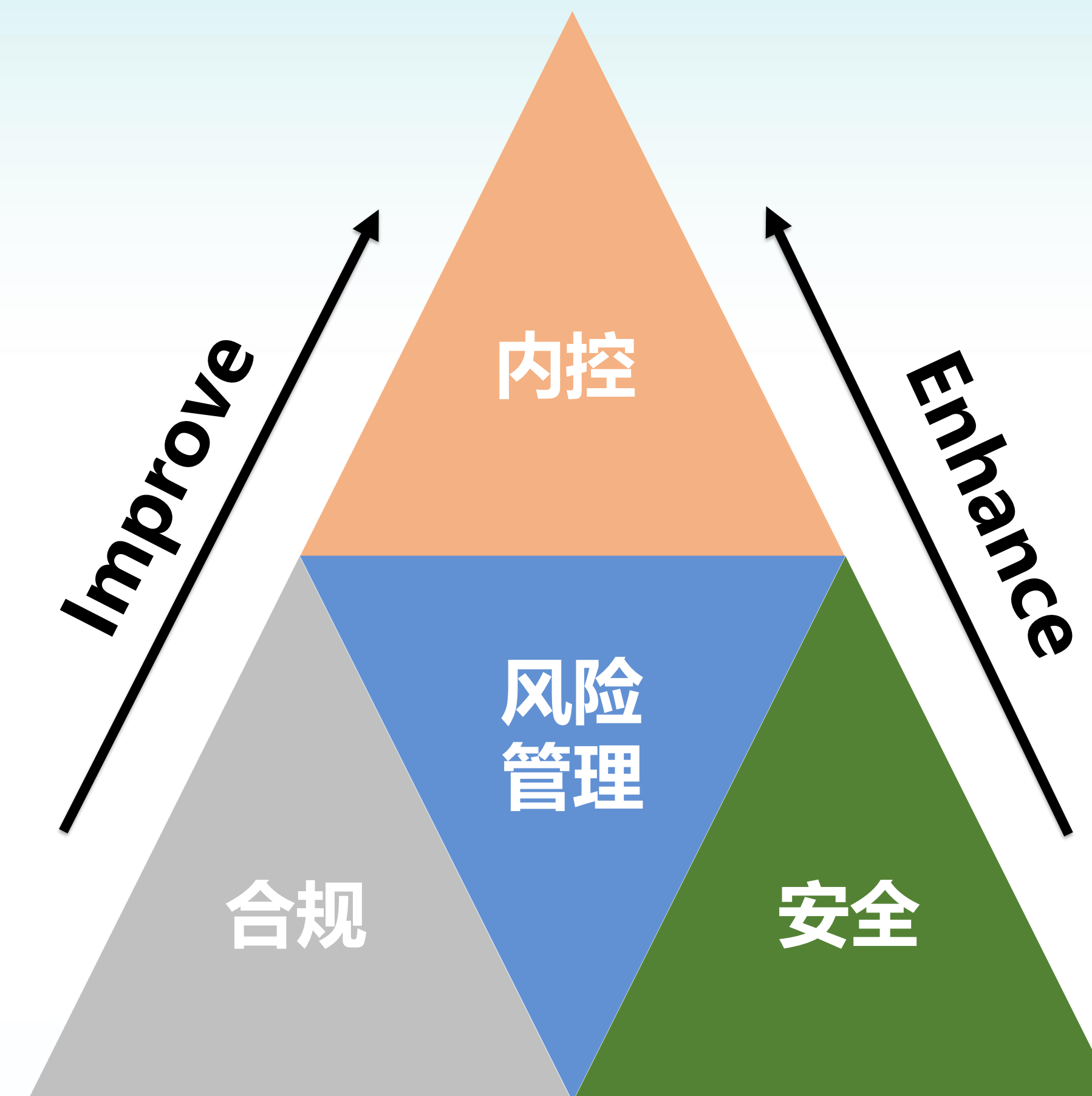
数据赋能 生态共荣

平安集团 CISO 陈建

平安集团信息安全关注点



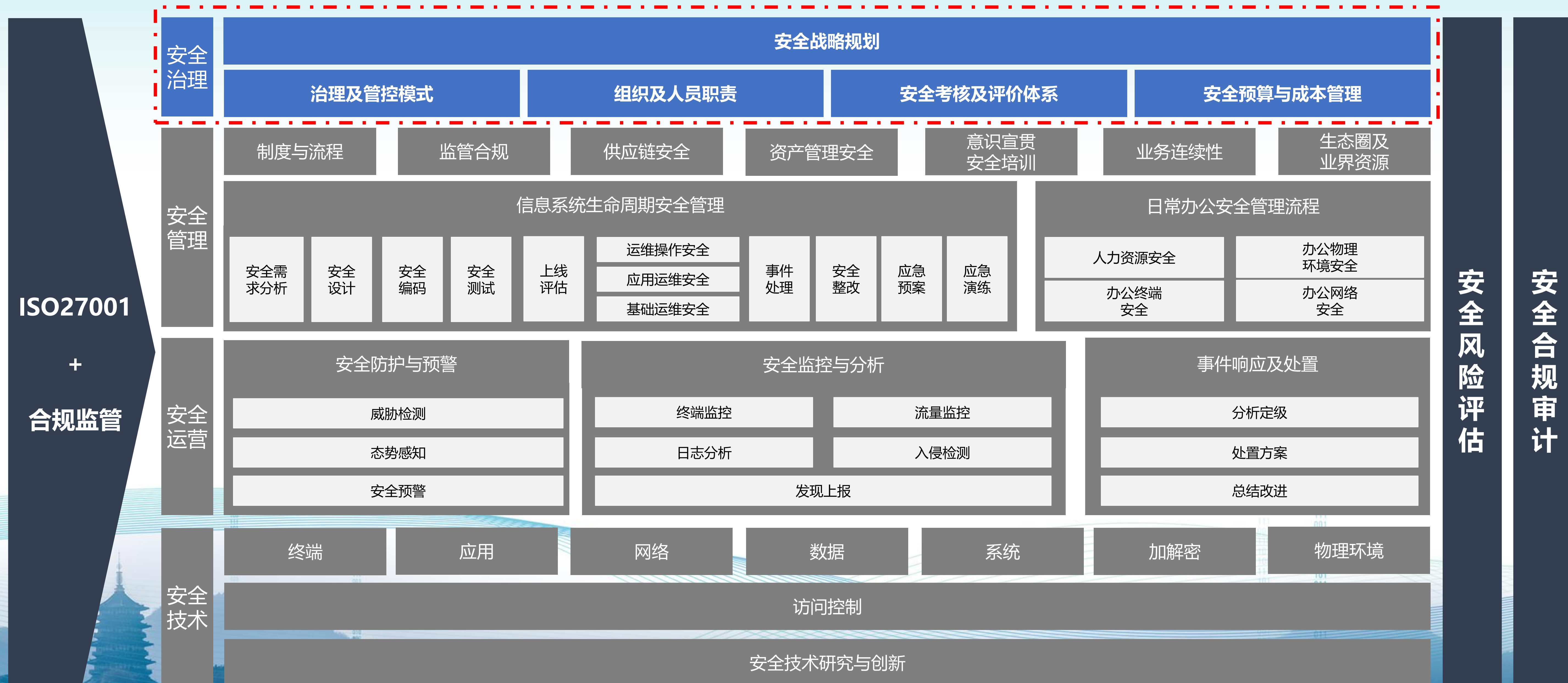
2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE



Motivate



平安集团信息安全治理结构





平安集团安全治理模式

安全战略规划

信息安全目标

组织架构设计

安全人才需求

安全技术方案

安全技术路线

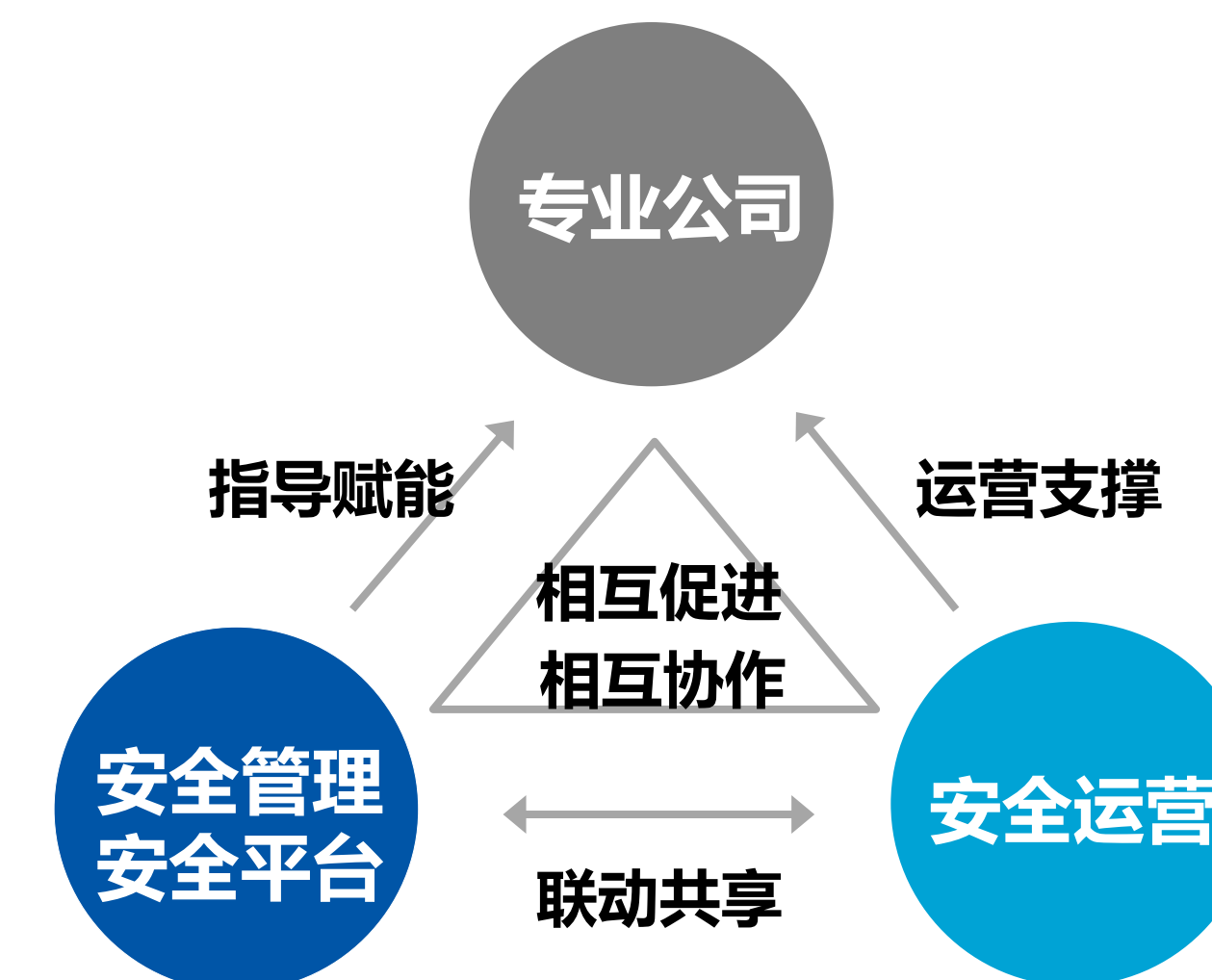
安全产品路线

安全管控模式

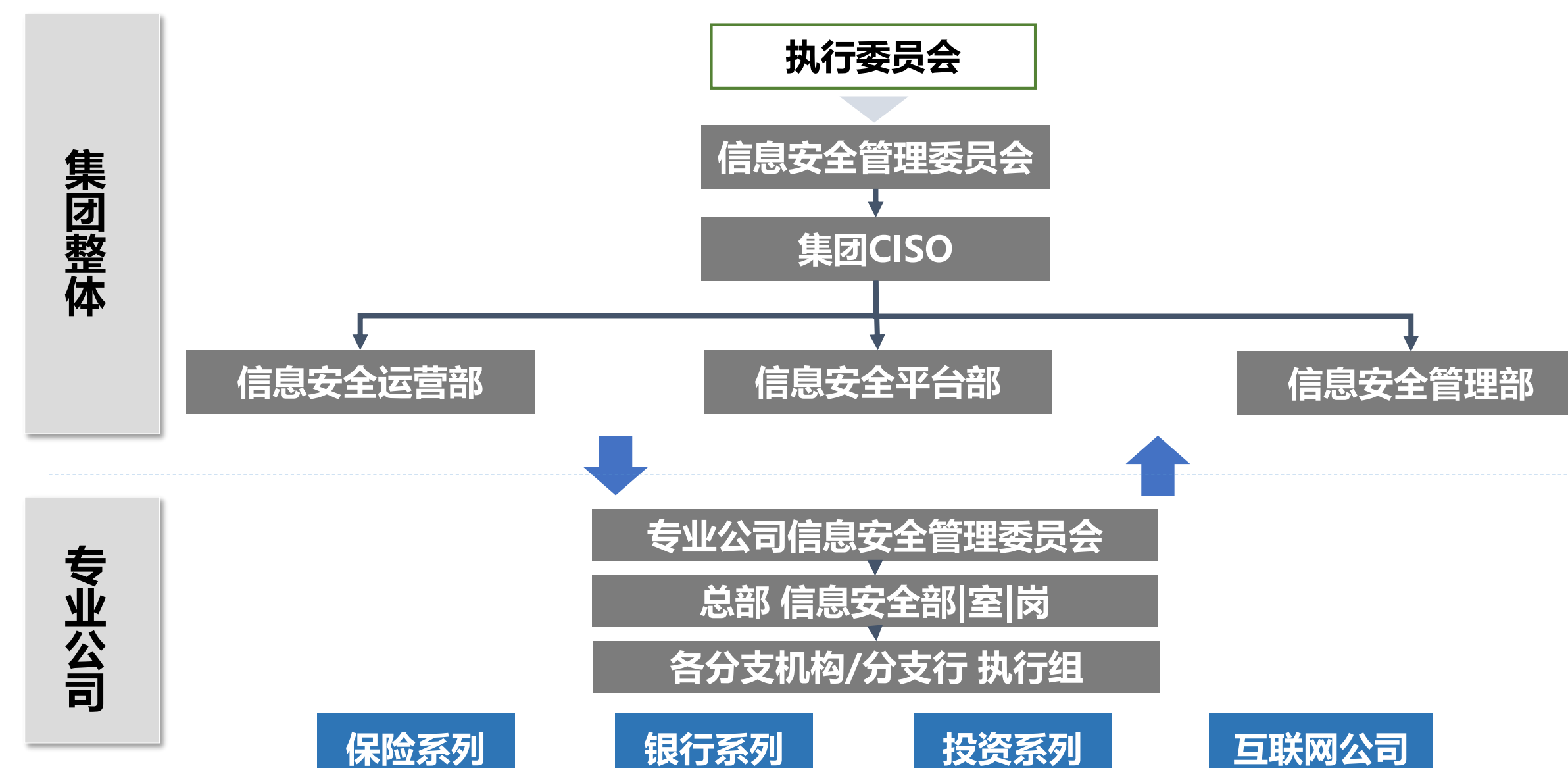
指导

+

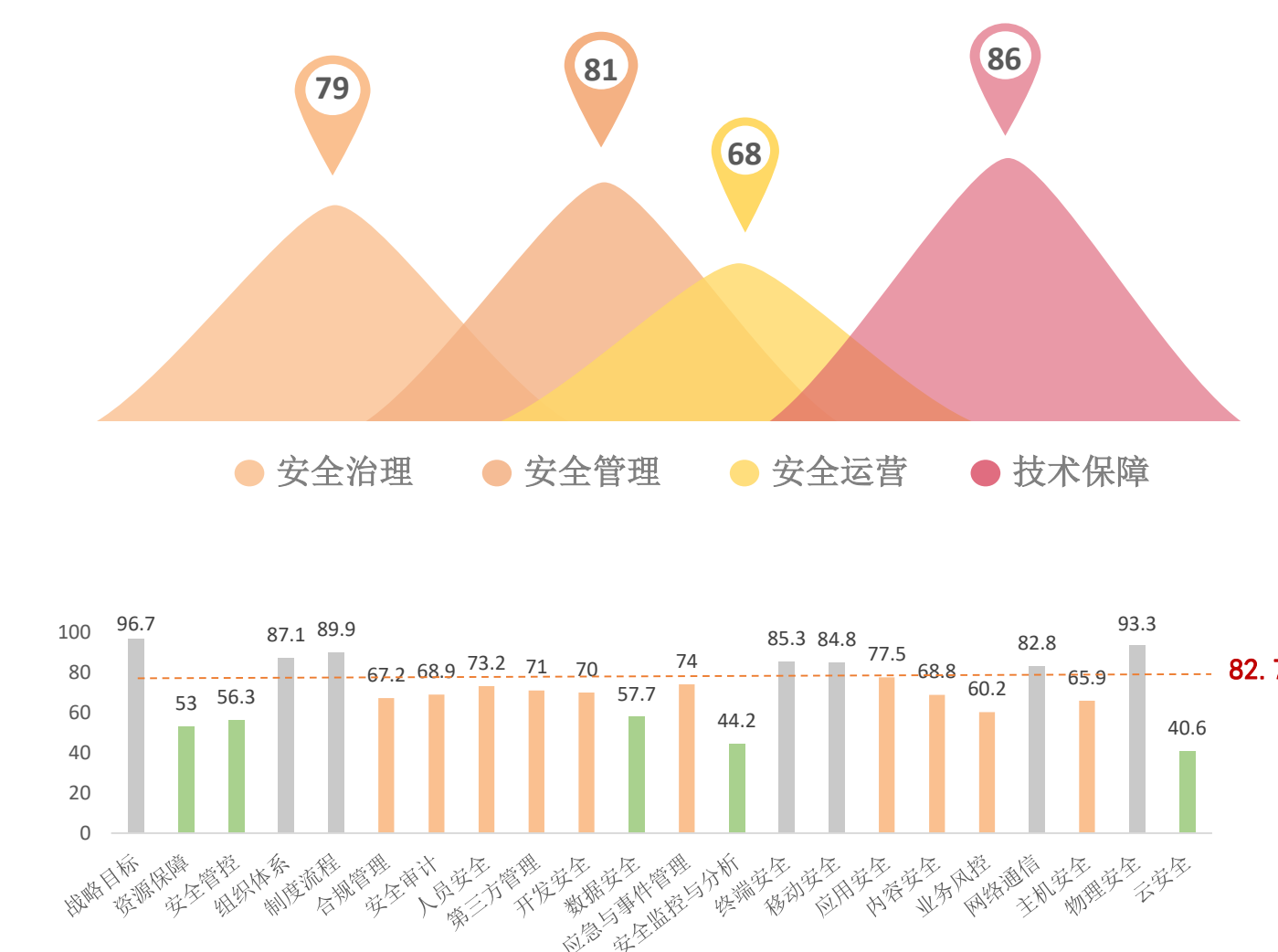
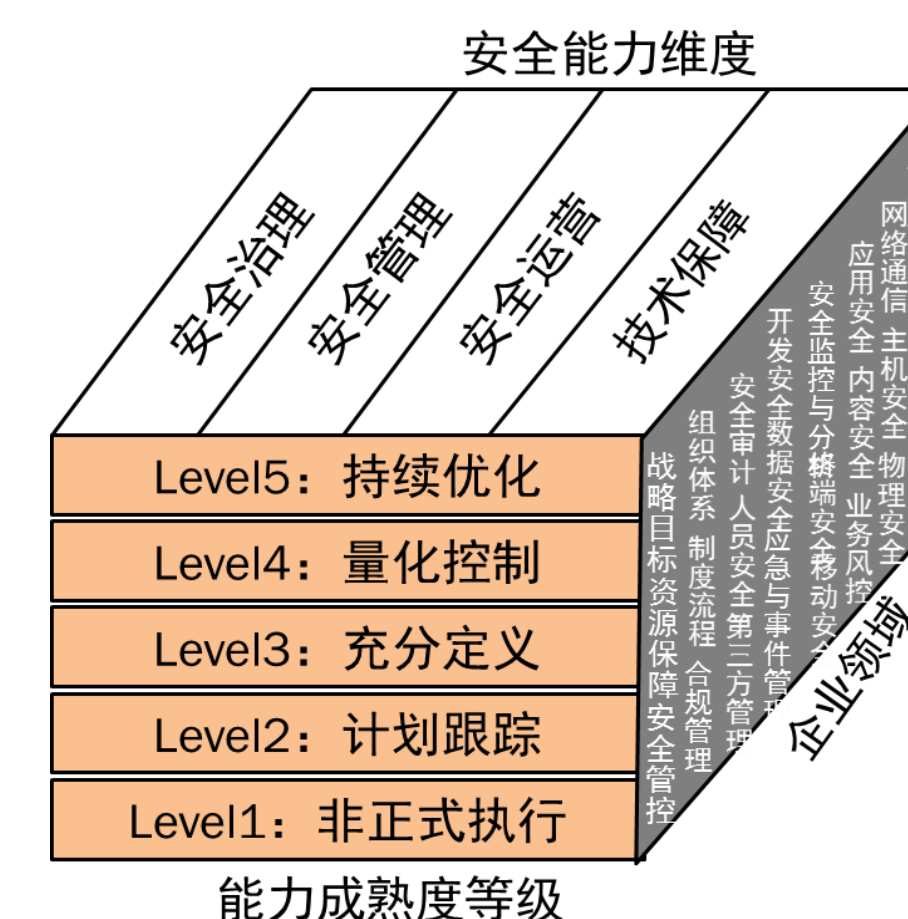
赋能



安全组织架构



安全成熟度评价

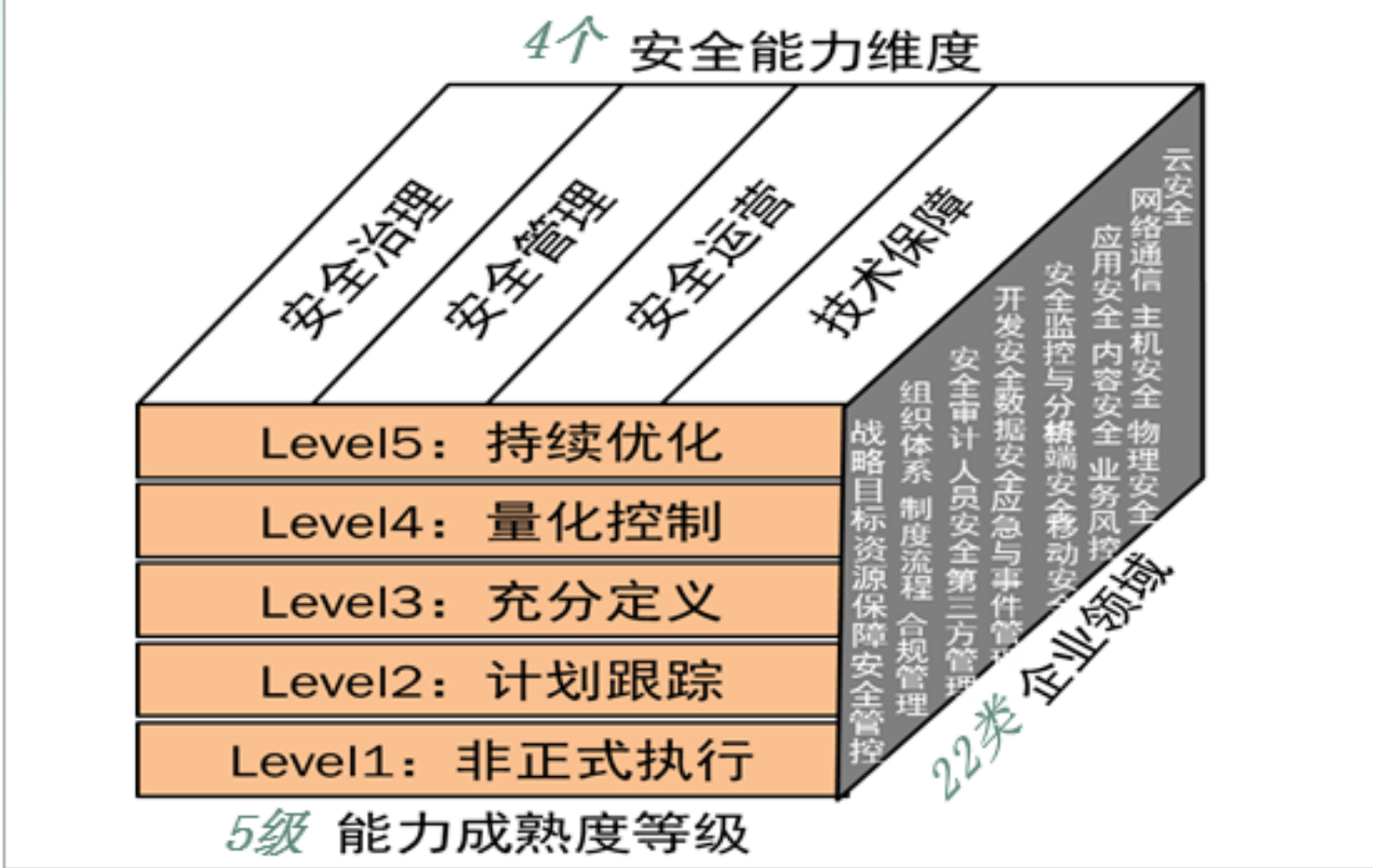


平安集团信息安全成熟度评价体系

成熟度评估体系要素



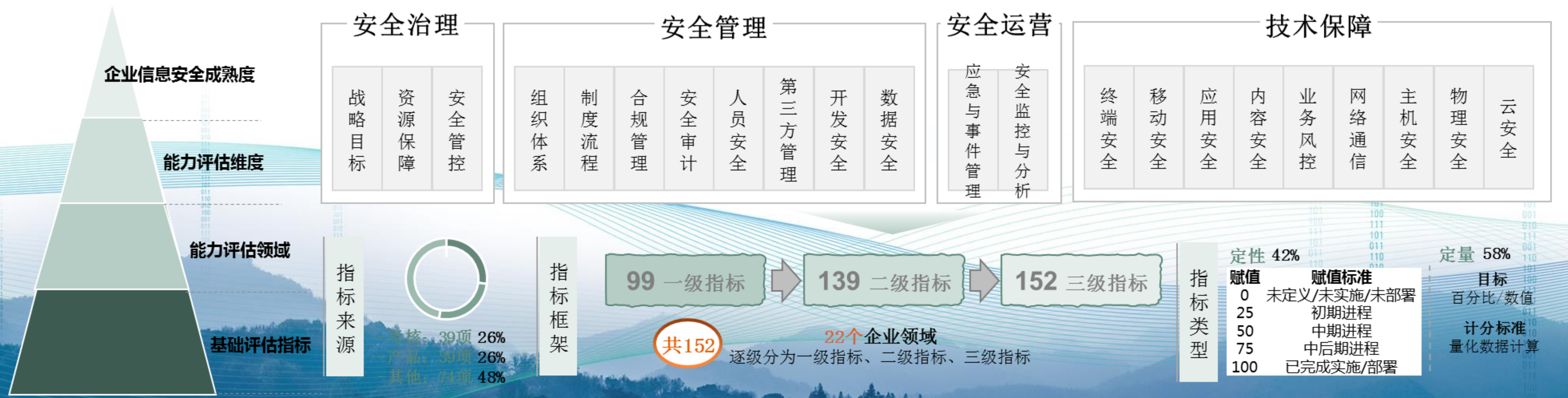
成熟度评估框架模型



能力成熟度等级

成熟度等级	分值范围	阶段特征
Level5：持续优化	(90-100)	安全过程自适应、持续优化改进能力。
Level4：量化控制	(80-90)	安全过程可量化、具备数据采集和分析监控能力
Level3：充分定义	(70-80)	规范的安全过程、采用流程控制、符合强制法规
Level2：计划跟踪	(60-70)	已定义、文档化
Level1：非正式执行	(<60)	无定义的过程

信息安全成熟度评估指标结构





数据驱动信息安全水平提升

集团信息安全治理



- 智慧管控
- 明确职责
- 业务驱动
- 数据赋能
- 资源共享
- 共同提升

平安集团的企业安全技术框架



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

安全管理

SOC/NGSOC

威胁管理

资产管理

日志管理

安全审计

安全合规（GRC）

配置检查

安全智能

行为分析（UEBA）

网络流量分析

威胁智能分析

APT检测

取证溯源

蜜网

云安全

云服务监控

云抗DDoS

云WAF

云访问安全代理

云数据安全

云身份管理

云基础架构安全

应用安全

代码安全

漏洞扫描

Web应用安全扫描

网页防篡改

应用防火墙

内容安全

舆情监控

登录验证

不良信息监测

邮件安全

反钓鱼

终端安全

终端防护

终端检测

防病毒

IM监控

移动安全

APP安全

移动业务安全

移动终端安全

业务安全

反欺诈

工控安全

数据安全

数据脱敏

HDLP

文档加密

加密机

数据库安全

硬盘加密

密钥管理

VPN

身份与访问管理

身份认证

数字证书

堡垒机

基础设施安全

NGFW&防火墙

入侵检测/防御

网络准入

上网行为管理

主机自适应防御

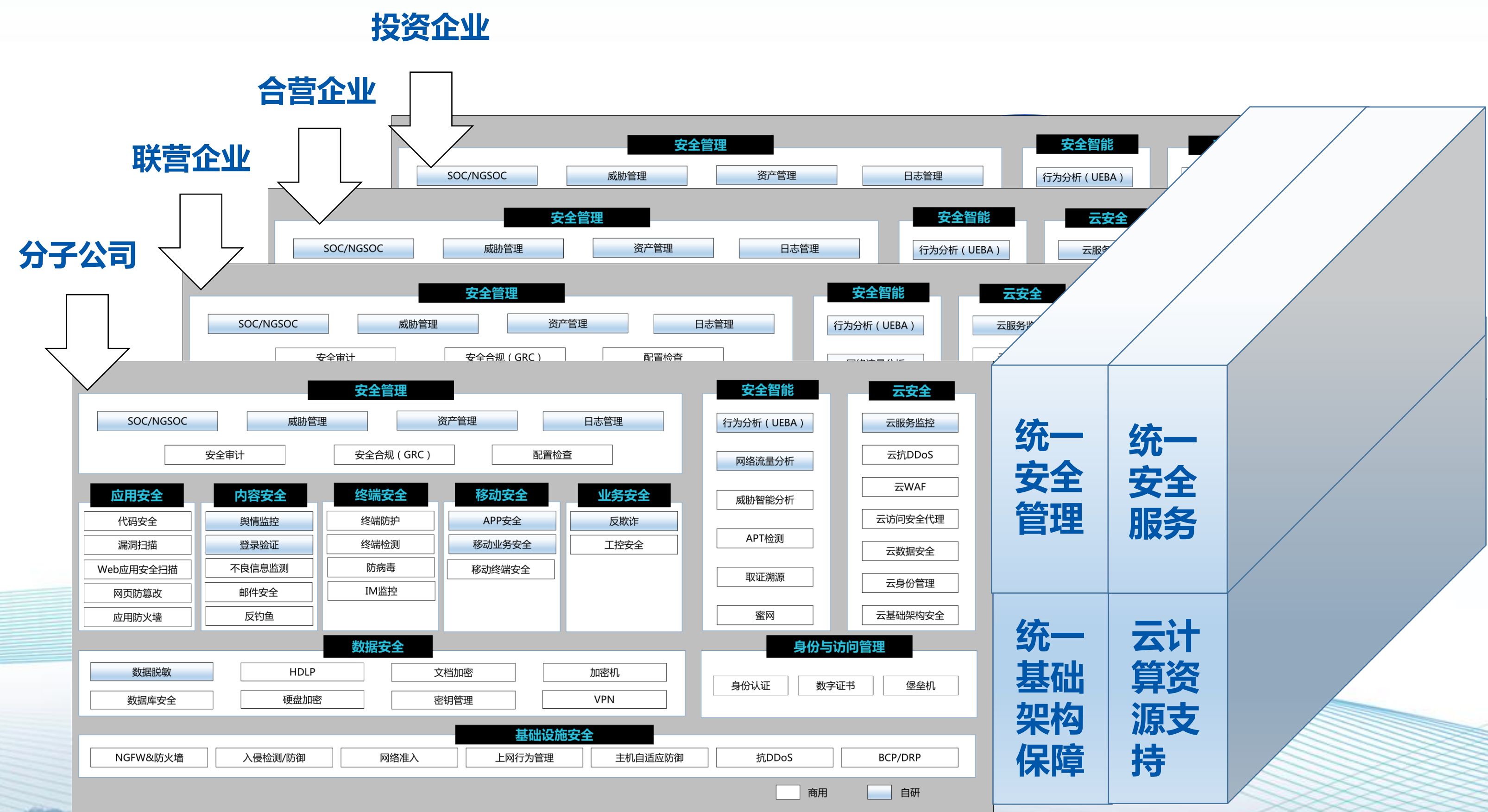
抗DDoS

BCP/DRP

商用 自研

打造开放安全中后台，构建安全新生态

- 打造企业安全中后台，确定规范、联动各方、汇聚能力，服务业务；
- 以数据、场景、业务为链条，串接前后台，反哺业务、赋能企业；
- 鼓励标准化封装应用API，向合作伙伴、第三方供应商提供安全、稳定、简洁的安全接入服务；
- 带动社会开发力量，吸引广泛资源进行应用混聚，构建用户、合作伙伴、安全供应商互利共赢的“安全生态圈”。



基于企业中台的开放安全新格局

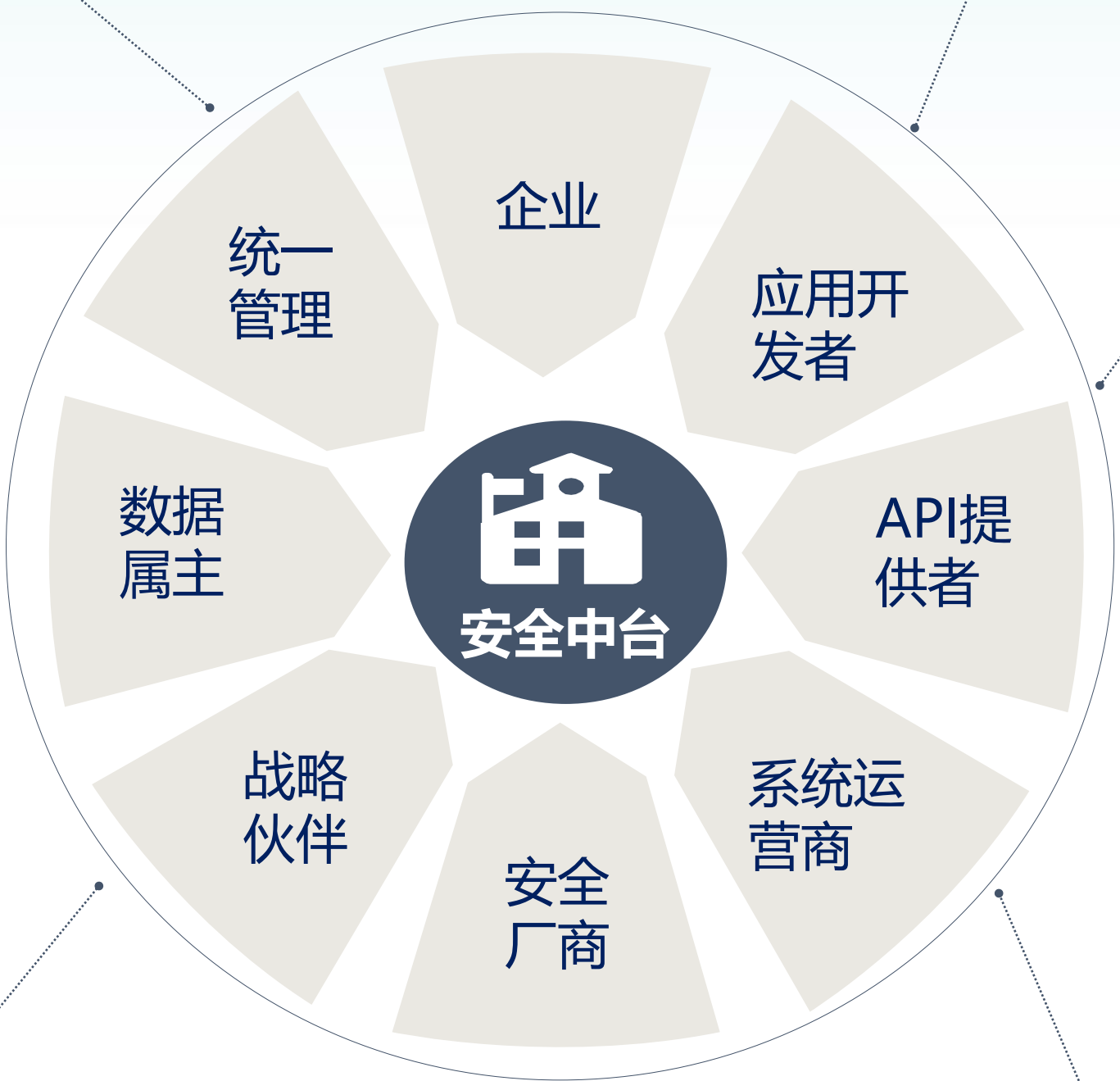


2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

基于API的安全生态逐渐呈现，通过安全产品API化来适应云环境，吸引更多使用者。同时具有选择API的自由，避免被绑定特定产品厂商的风险。

利用现有的资源和服务快速构建针对应用的安全保护，降低成本并大大缩短部署周期；将不同API的能力进行融合，推动业务模型发展，提升整体的安全防护能力。

通过开放的平台，可以将企业的业务资产，（如数据、职能或计算资源）、服务活动、应用系统、安全产品融合起来统一适配，同样是对企业数字化转型的助力。

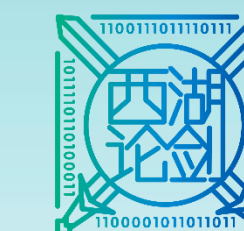


应用API用来重构客户安全管控体验，适应移动、云、社交平台等全新应用环境。安全真正成为保驾护航的要素，而不是对业务的阻碍。

从不能独自扩展到的市场或客户群，进化到更容易找到合作伙伴，帮助初创安全团队更容易获取新客户并提高收入。从而促进安全行业创新

连接业务前端和API服务后端，既懂安全又懂业务，可以协助后台获取使用情况，进行持续的按业务需求改进，将API作为数字产品进行产品管理。

企业中台+开放API带来的创新与价值



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

- 企业中台+开放API可以促进行业的安全生态合作发展。
- 打破壁垒，企业优势在于场景、数据与用户；安全厂商优势在于技术能力、优秀产品力。
- 优势叠加，促使传统产品赋能企业向模式赋能行业转变。

开拓新的商业模式

借助API生态系统，对于行业用户，可以接触、吸引和扩大更多新客户群。

融合第三方API，形成不同安全产品组合架构，适应移动、社交、物联网等新趋势，也给安全厂商带来新的业务机会和业务模式。

创新业务

加快API构建新服务

针对不同终端的业务功能，可以直接API聚合，从而形成应用系统和安全系统间的无缝衔接。

传统安全产品产销模式被API共享经济打破，与第三方合作越发广泛，创新产品推出时间缩短。

创新产品快速入市

改变业务服务方式

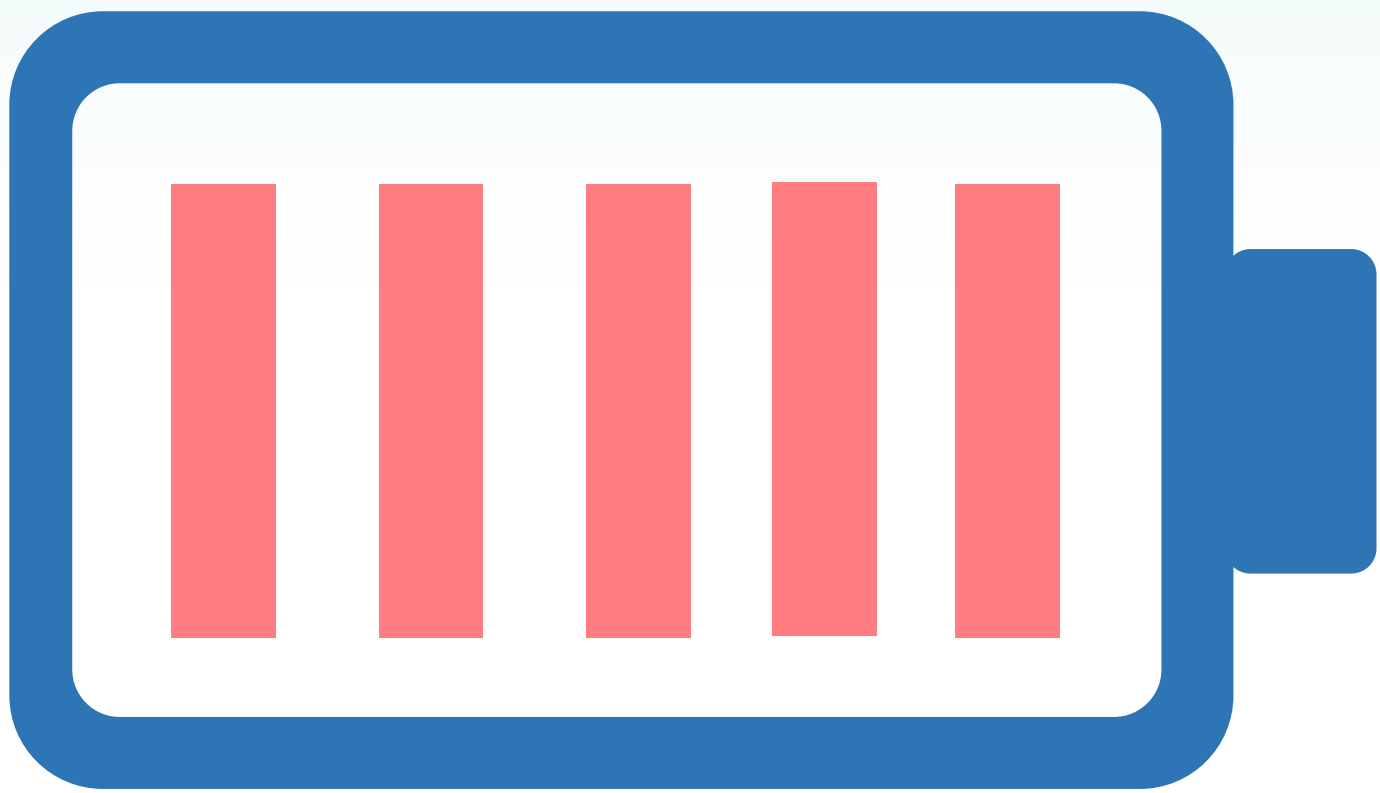
利用API+云，能够在社交化、物联网化、移动化的环境中，快速集成API服务，通过单一API构建新服务。从安全产品服务，发展为安全即服务的交付模式。

各方携手促进新模式安全生态赋能行业



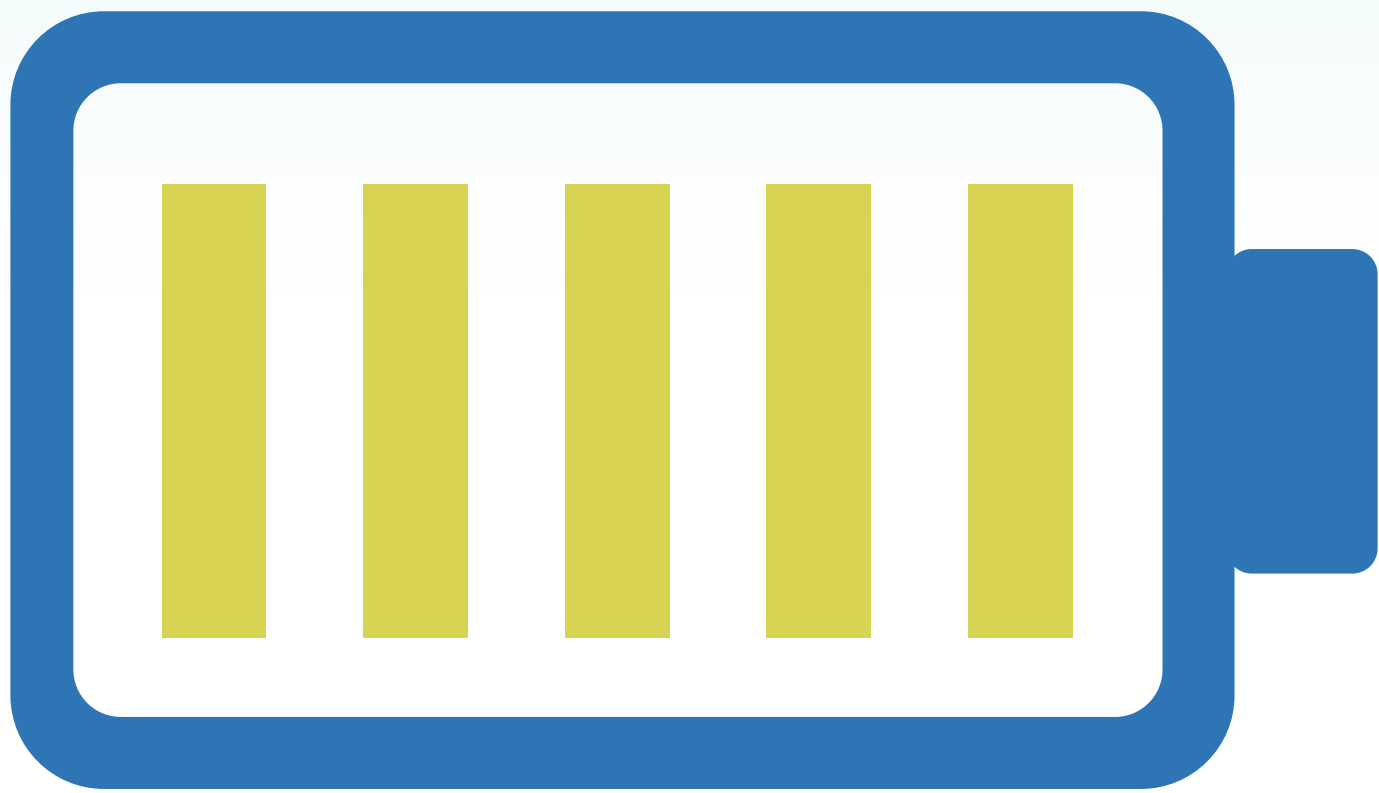
后台安全厂商

- 专注自身拳头产品
- 打造差异化竞争爆点
- 在优势领域持续深挖
- 保持自信开放心态



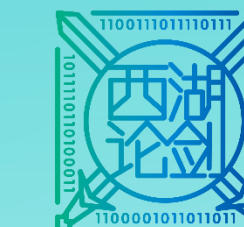
企业安全中台

- 提炼场景、数据、用户行为
- 整合商业产品能力
- 总揽企业全局安全特性
- 聚合各方力量



企业前台用户

- 业务引导安全发展方向
- 数据反哺安全能力提升
- 探索最贴合业务需求的安全模式
- 提供有价值的最佳实践



2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

THANK YOU

谢 谢 观 看