



# 多态云安全治理方案

聂晓磊@盛邦安全  
产品总监



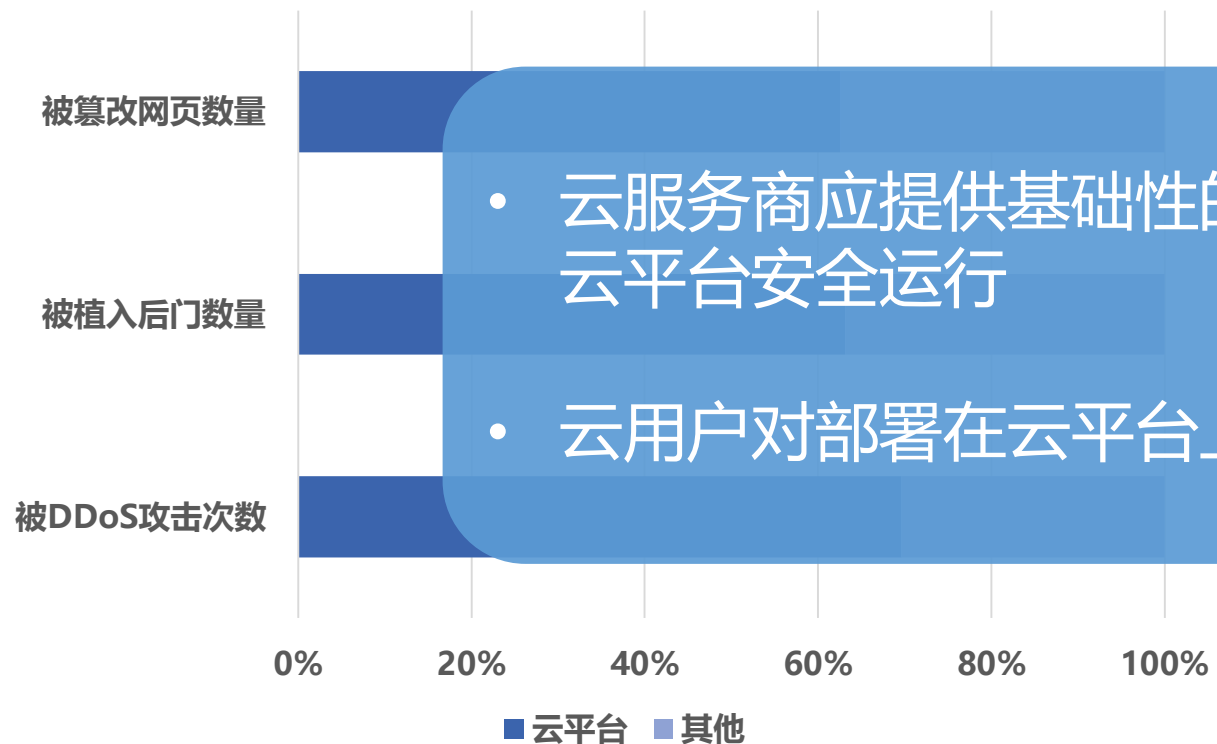
# 目录

## 现有安全方案的整理与反思

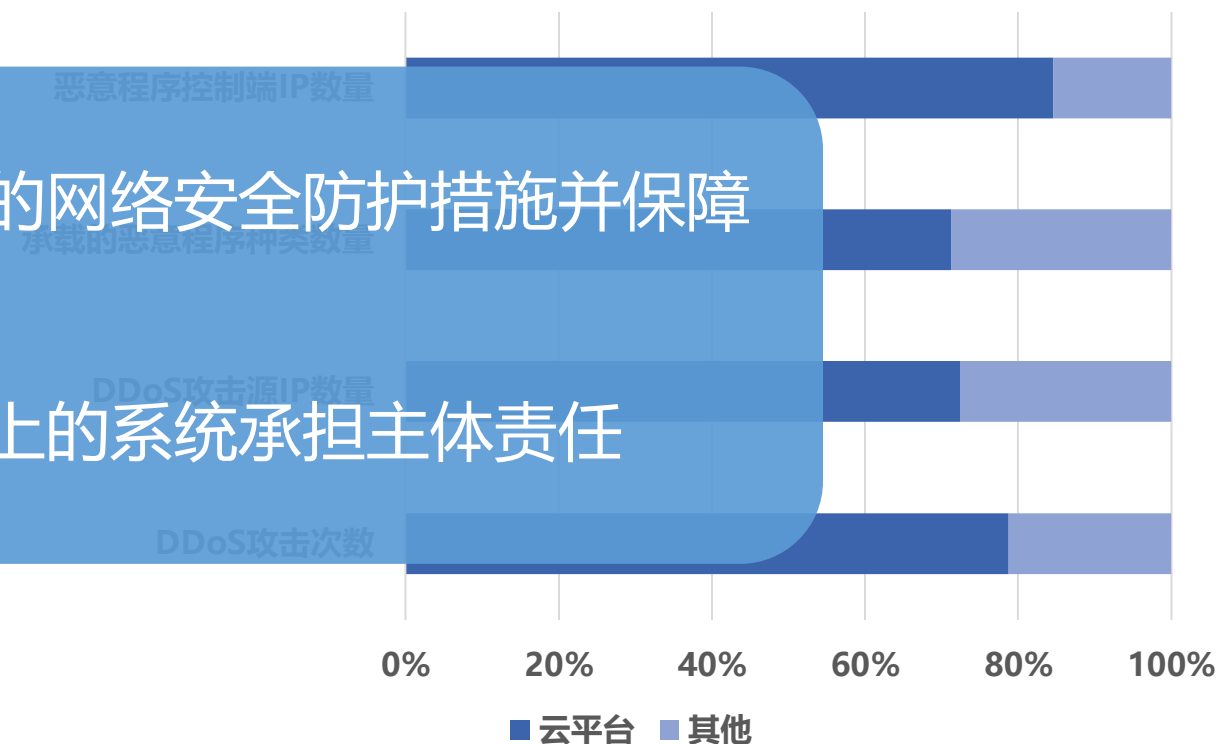
多态云安全治理方案

云安全治理带来的新思路

## 2019年上半年云上业务安全事件统计



## 2019年上半年云平台被利用安全事件统计



- 云服务商应提供基础性的网络安全防护措施并保障云平台安全运行
- 云用户对部署在云平台上的系统承担主体责任

数据来源于CNCERT 《2019年上半年我国互联网网络安全态势》

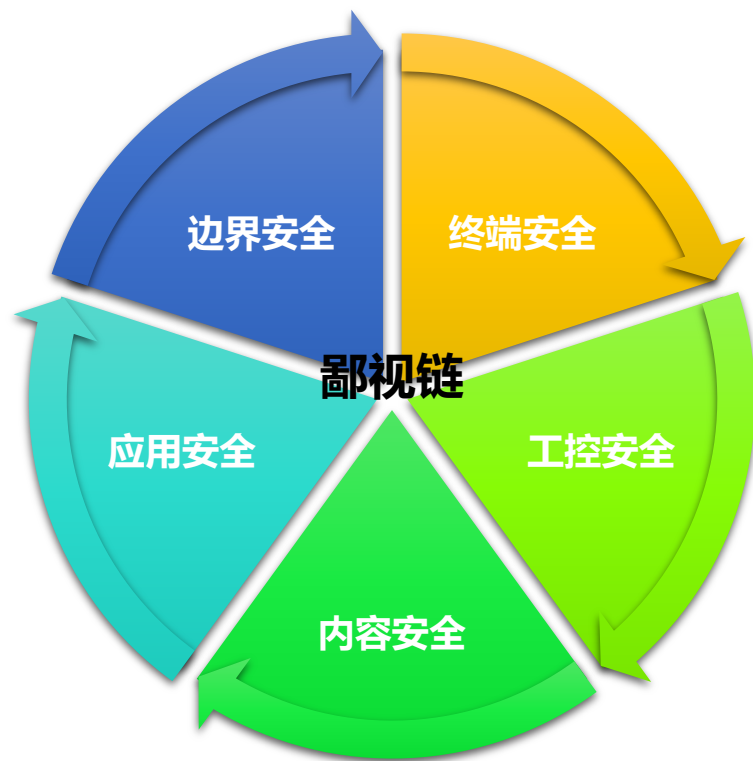


## 云服务方

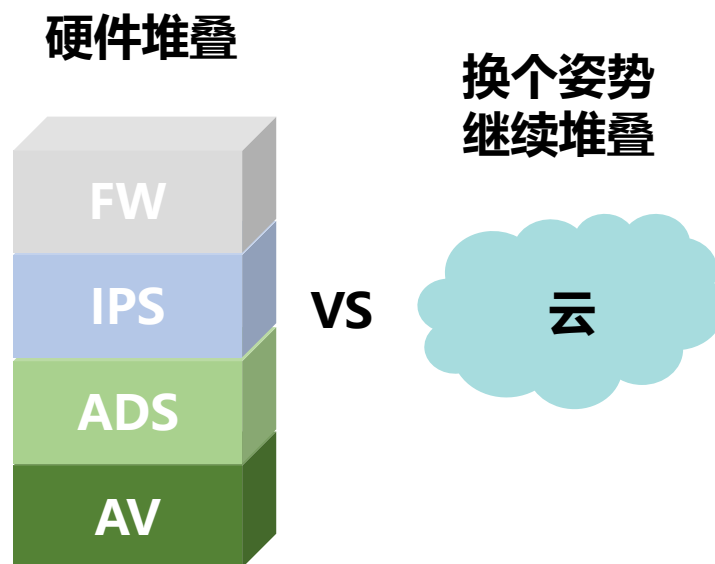
- SaaS: 硬件、虚拟机监视器、操作系统、中间件和应用等
- PaaS: 硬件、虚拟机监视器、操作系统和中间件等
- IaaS: 虚拟机监视器和硬件等

## 云租户

- SaaS: 部分应用职责及用户使用职责
- PaaS: 应用等
- IaaS: 操作系统、中间件和应用等



单一解决方案难以覆盖全部场景



传统解决方案容易造成资源浪费



安全建设与管理思路通常有偏差



安全边界模糊

按边界划分安全  
域思路不再适用



资产宿主和运营分离

宿主和运营分离  
隐藏的管理风险



安全审查乏力

云上资产形式多  
变且属性不明确

云环境下的资产  
多变、属性繁  
杂，宿主与运营  
分离，安全面临  
新挑战

## 业务需求

- 资产清晰。租户与运营方都应明确知晓被托管资产的属性及安全状态
- 全面覆盖。既要满足南北向安全，又要保证东西向安全
- 生态性。内部数据需要共享，外部数据也需要联动

## 管理需求

- 用户管理。需要满足最终用户自助管理安全服务的需求
- 运维管理。需要具备统一集中的管理运维方式
- 责权清晰。管理边界需要清晰，保护资产需要多重备案

## 部署需求

- 半即插即用部署，按需动态扩容
- 丰富的兼容特性，具备冗余可靠性

## 合规需求

- 满足网络安全法要求
- 符合等保2.0基本要求及云计算安全扩展要求，符合云计算服务网络安全审查要求

## 个性需求

- 场景化。需满足不同场景的个性化需求
- 行业性。需适应不同行业的定制化需求

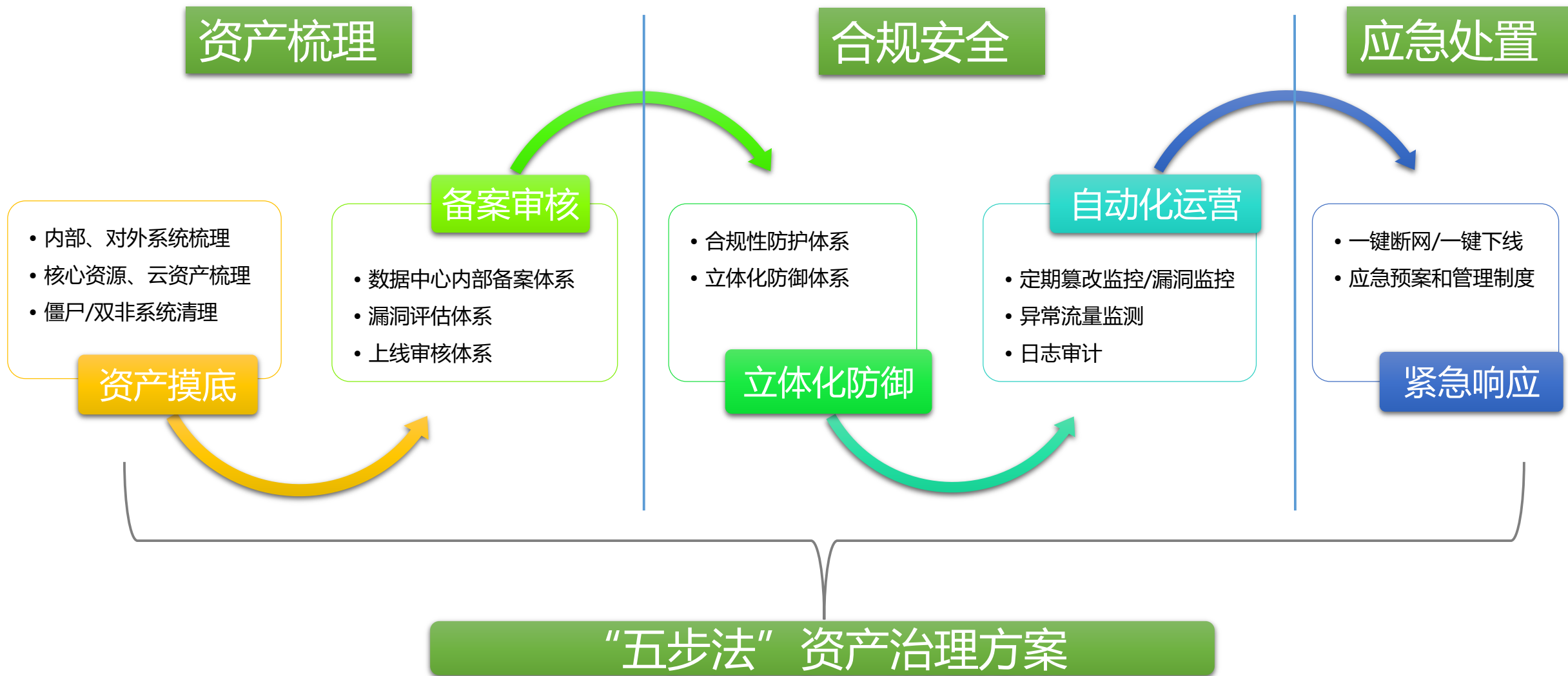
# 目录

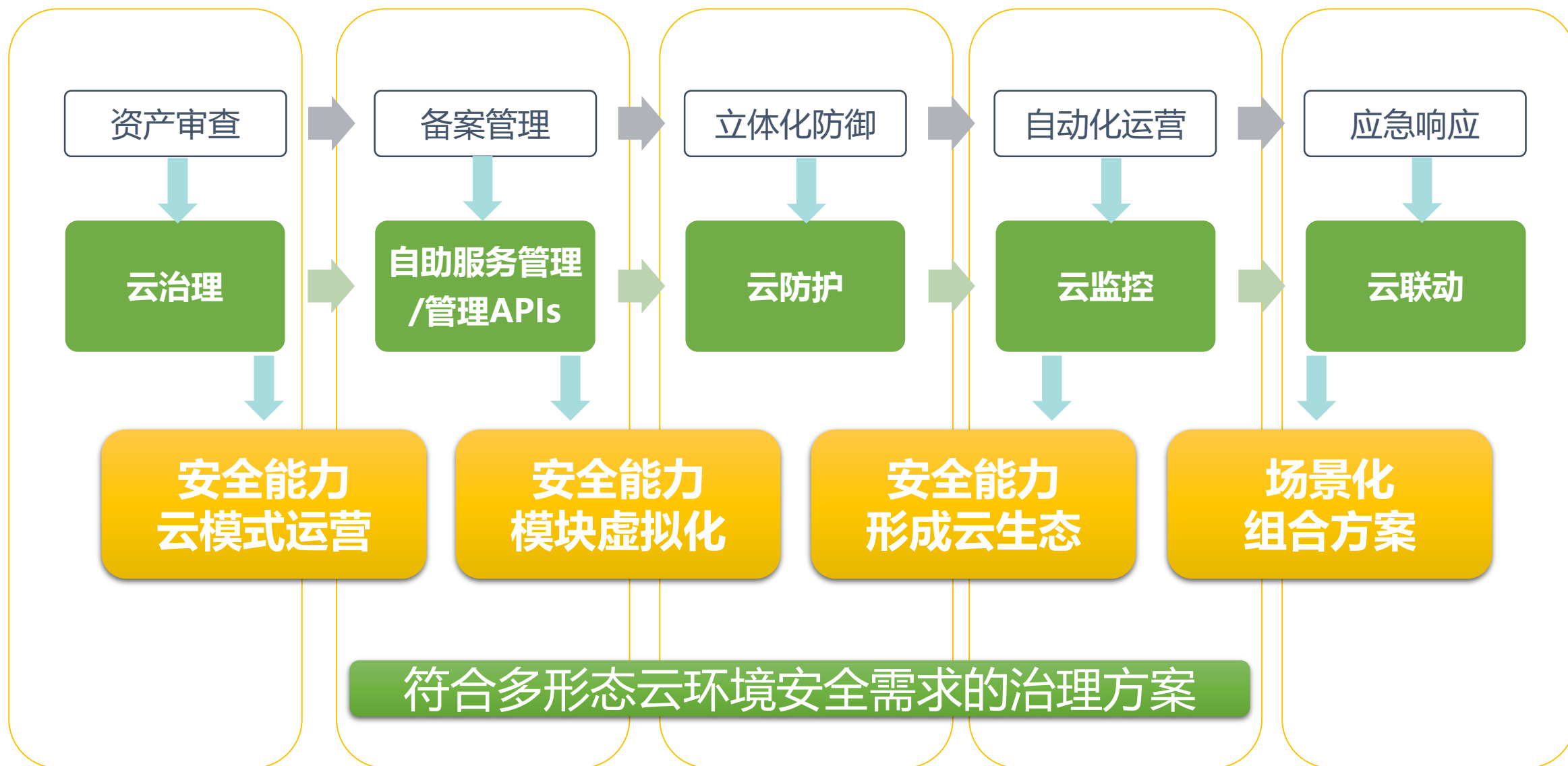
现有安全方案的整理与反思

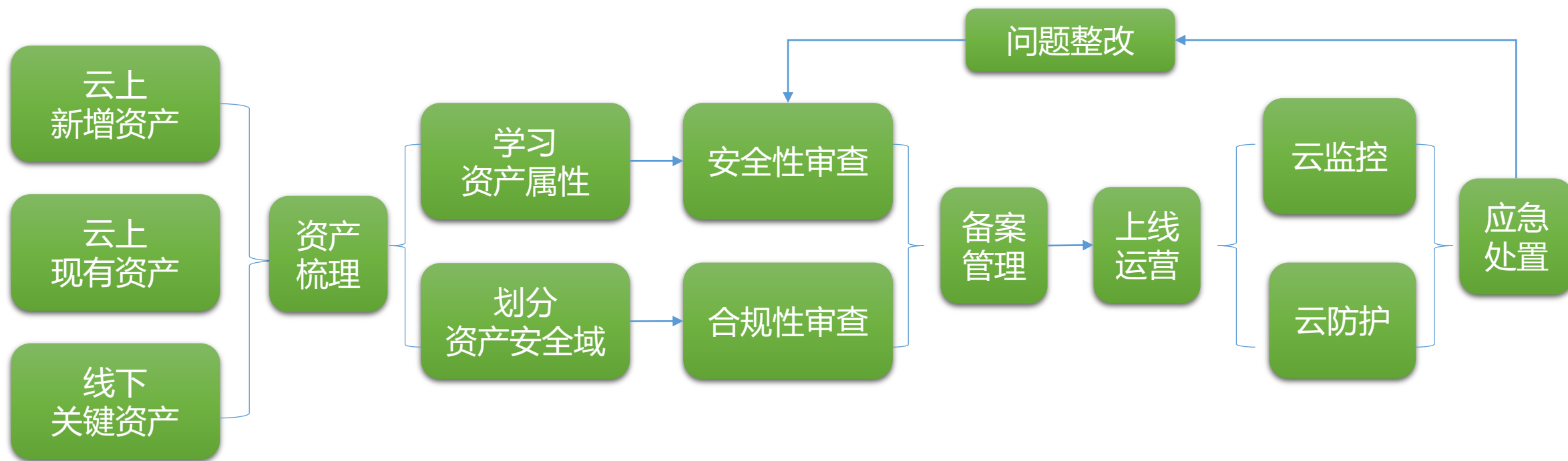
## 多态云安全治理方案

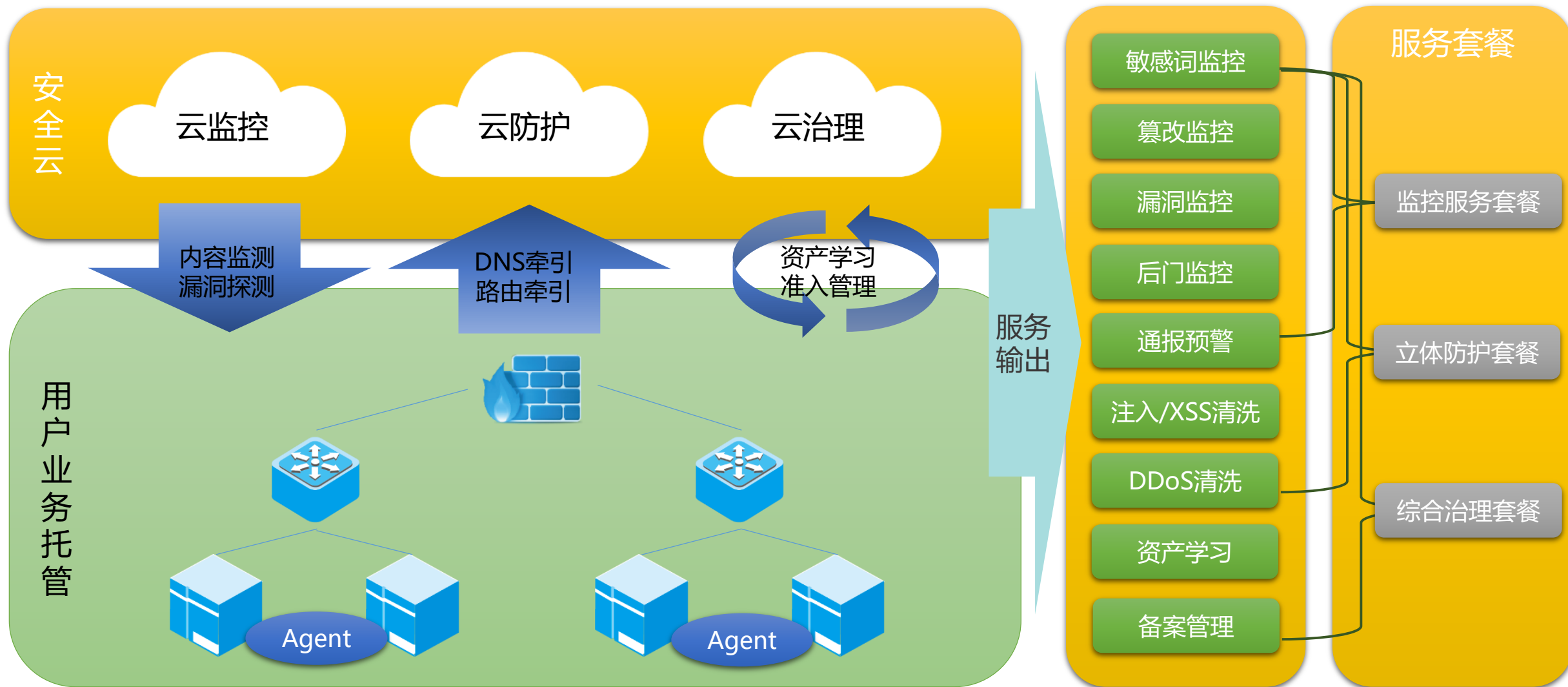
云安全治理带来的新思路















## 垂直监管

- 云平台提供了分层级的管理员配置，可满足垂直机构安全监管需求

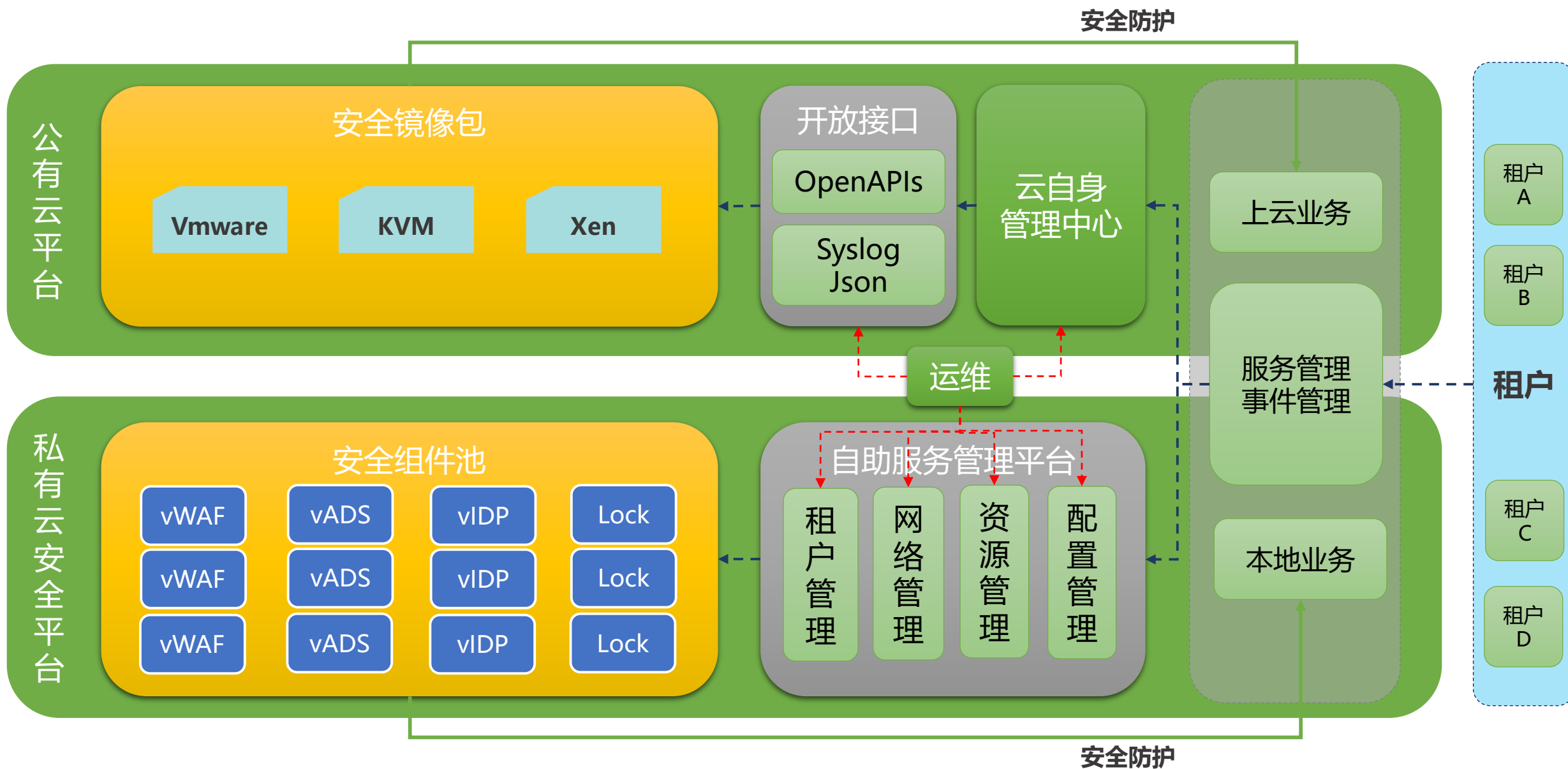
## 场景化分配

- 云平台输出的服务可根据不同安全需求自由组合搭配，适应各种场景

## 靶向服务

- 云平台可利用策略路由、BGP路由以及DNS牵引等技术方式，接受细粒度的业务托管，提供靶向服务

用户将业务托管至云监控、云防御以及云治理平台，按照需求选择搭配安全服务组合套餐



WebRAY  
盛邦安全

+ 攻击态势

系统信息

服务器管理

网络管理

设备管理

攻击日志

账户管理

服务器

+ 服务器

增加 +

刷新

导入

每页显示 15

服务器检索

域名检索

IP检索

全部用户

<input type="checkbox"/>	服务器名称	IP地址	端口	主机	防护策略	清洗选项	所属租户	所属设备	创建时间
<input type="checkbox"/>	 [redacted]	[redacted]	55.34	80	w [redacted] du	普通策略	<input checked="" type="checkbox"/> 启用	[redacted]	[redacted]
<input type="checkbox"/>	 [redacted]	[redacted]	1.149	80	lil [redacted]	禁用	<input type="checkbox"/> 禁用	[redacted]	[redacted]
<input type="checkbox"/>	 [redacted]	[redacted]	1.171	80	2 [redacted]	普通策略	<input type="checkbox"/> 禁用	[redacted]	[redacted]
<input type="checkbox"/>	 [redacted]	[redacted]	1.11	80	o [redacted]	增强策略	<input type="checkbox"/> 禁用	[redacted]	[redacted]
<input type="checkbox"/>	 [redacted]	[redacted]	1.167	80	j [redacted] n	专家策略	<input type="checkbox"/> 禁用	[redacted]	[redacted]
<input type="checkbox"/>	 [redacted]	[redacted]			监控策略	<input type="checkbox"/> 禁用	[redacted]	[redacted]	[redacted]

运维人员可进行复杂的系统管理、网络管理、组件管理；租户可自助进行服务搭配、策略选择及事件审计





运维人员可进行复杂的系统管理、网络管理、组件管理；租户可自助进行服务搭配、策略选择及事件审计



## 部署方便

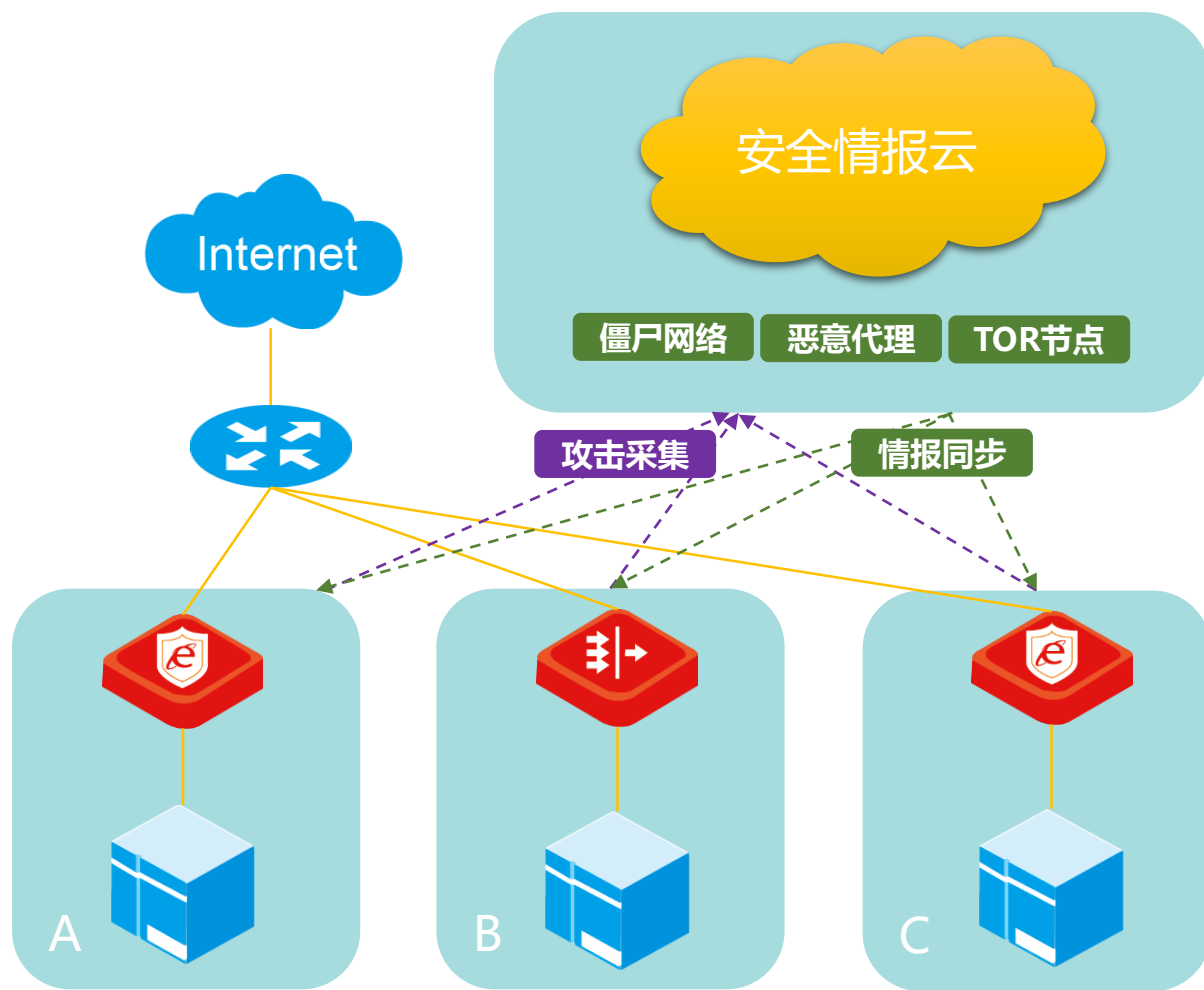
- 镜像+API的交付方式，兼容性开发工作量小
- 系统资源可动态扩展，满足弹性配置需求

## 管理便捷

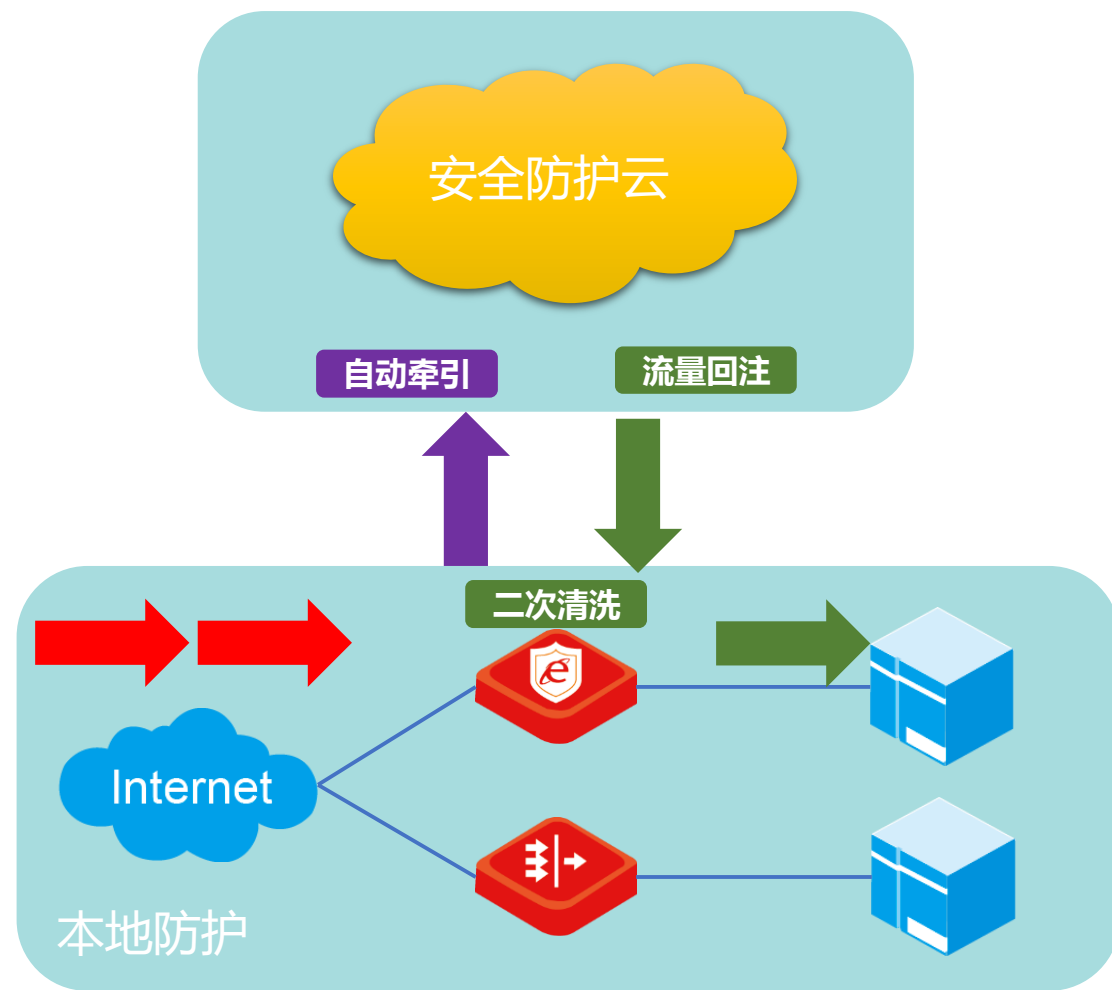
- 松耦合的管理方式，租户进行简单的自助管理，运维负责复杂的专业管理，边界清晰

## 覆盖面广

- 既拥有关键数据的本地私有云安全方案，也满足公有云业务的东西向安全方案



云情报联动



云防护联动

## + 安全情报中心配置

启用 ☒ 高级 ☒

威胁情报源 1 (厂商)  源地址  更新时间  (秒)

情报源类型 ☒ FTP ☐ API

FTP登录名

FTP密码

威胁情报源 2 (厂商)  源地址  更新时间  (秒)

情报源类型 ☒ FTP ☐ API

FTP登录名

FTP密码

### 生态合作

- 通过开放的生态，传统安全厂商与云安全厂商可以形成深度合作，为用户提供组合方案

### 协同防护

- 通过开放的API，传统产品与云产品可以实现能力互补，将南北向安全与东西向安全合理结合，同时扩展各自的能力范围

### 信息共享

- 通过信息共享，实现产品与产品间不同类型数据的同步，构建在态势分析、攻击取证等环节的完整链条

**独立产品与云产品互通API，通过本地集成管理接口，实现统一管理，形成协同联动生态体系**

# 目录

现有安全方案的整理与反思

多态云安全治理方案

云安全治理带来的新思路



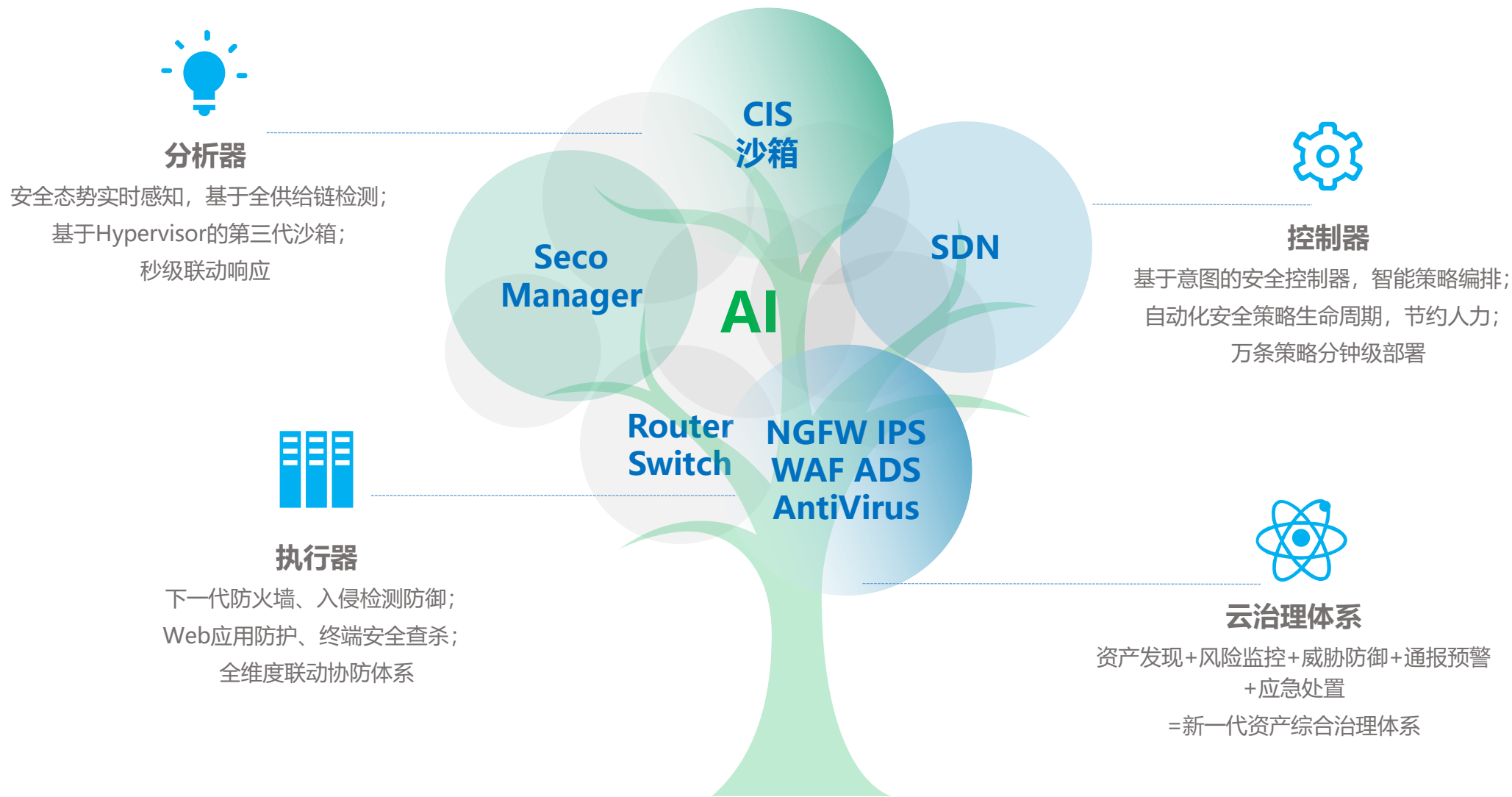
在等级保护与行业安全规范的大框架下，运用云计算的思想集约调度资源，以资产为最小安全域构建有针对性的解决方案，基于“五步法”安全保障体系建设，整合多种形态的云安全能力，形成全生命周期治理方案

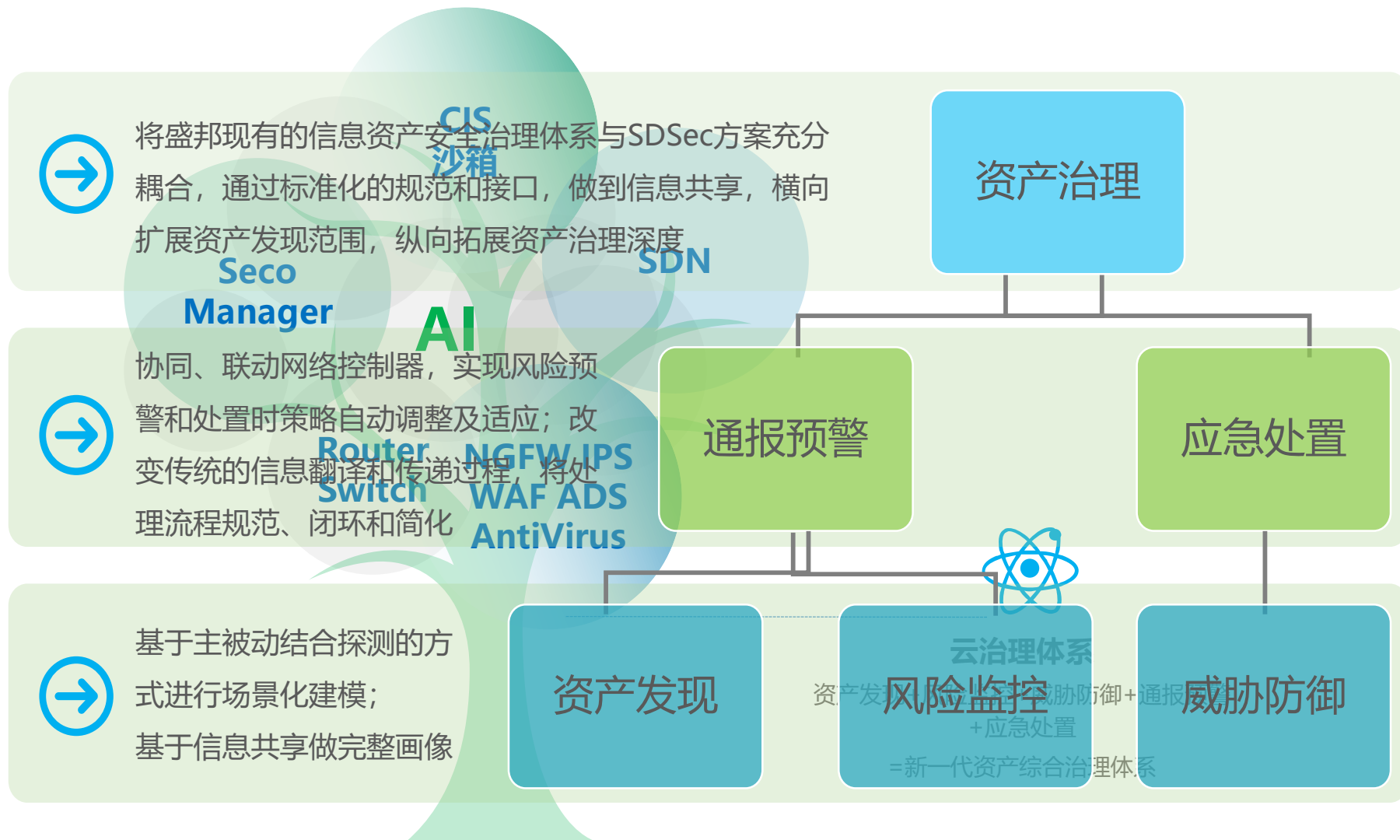
公安部等级保护标准




行业信息安全规范规范

基于以资产为核心的“五步法”资产治理体系







The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid-like structure, possibly representing a network or data flow. The pattern is more dense in some areas and more sparse in others, creating a sense of depth and movement.

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE