安全之痛：创业初期如何应对黑产威胁

阿里云安全

2016年3月

版本：v 1.7

阿里云. 安全

- 互联网安全威胁
- 云盾安全方案
- 云盾客户案例

01 互联网安全威胁

Hacking Team被黑事件

2015年7月5日，有“**互联网军火库**”之称的意大利监控软件厂商**Hacking Team**被黑客攻击，400GB内部数据泄露，包括Hacking Team掌握的大量漏洞和攻击工具，这些工具目前已经在互联网公开下载和传播。

Hacking Team开发的软件**可以监听几乎所有的桌面计算机和智能手机**，包括Windows、Linux、Mac OS、iOS 、Android、Blackberry、Symbian等，还提供能够协助偷偷安装监听程序的未公开漏洞(0day)。

@赵武在路上: 2011年的时候，HBGray被黑，很多人没有意识到意味着什么，因为跟国家安全相关。这两天Hacking team被黑，大家也没有意识到意味着什么。这次包括了客户清单和0day，但我更关注的是RCS的代码，以前行业内都是粗糙到不行的demo，工程化公开的很少，**这次会让行业内的技术往前推进几年，尤其是黑产。**

]HackedTeam[

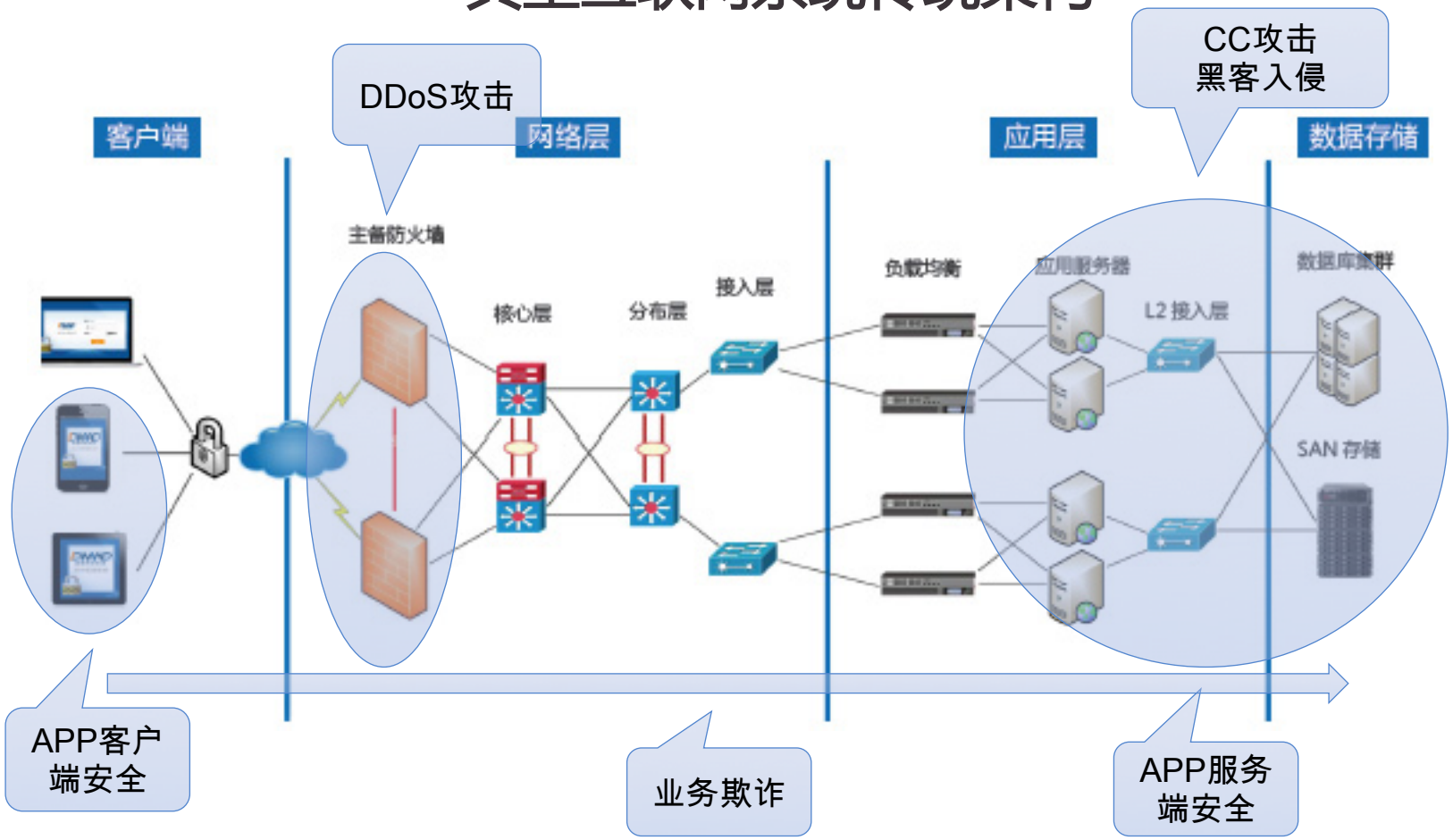
]HT[

互联网行业安全威胁

安全威胁

- DDoS/CC攻击
- 黑客入侵
- APP安全
- 业务欺诈

典型互联网系统传统架构



安全问题——DDoS攻击
攻击层出不穷，行业常态

行业现状

- 游戏、软件&科技、互联网&通信和医疗行业名列DDoS攻击频率前四位
- 2014年12月，阿里云上某游戏客户遭遇全球最大453GDDoS攻击

攻击成本低廉

- 打1小时1G的流量到一个网站，网上报价只需50块钱
- DNS/NTP/SNMP/BT等新型反射攻击可将流量放大100倍以上

防御困难

- 攻击方式复杂多变，SYN/UDP Flood，CC
- 受到IDC清洗能力限制，一旦超过IDC能承受的攻击流量（一般远小于20G），会强制将机器下线

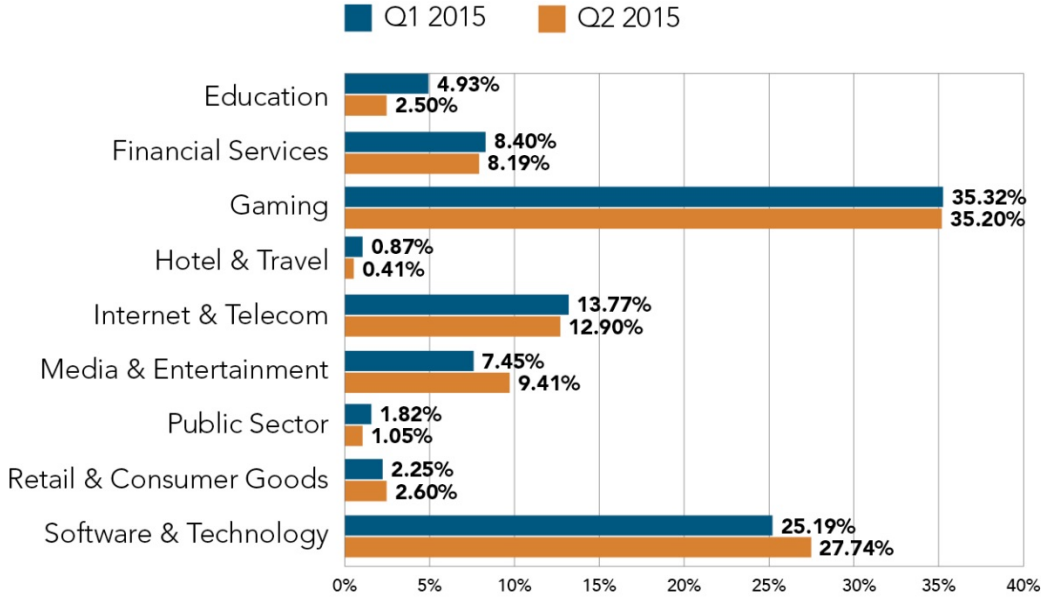


Figure 1-8: The gaming industry remains a top target for malicious actors

Akamai FASTER FORWARD
www.stateoftheinternet.com

安全问题——数据泄露
安全，事关平台生存

安全漏洞普遍存在

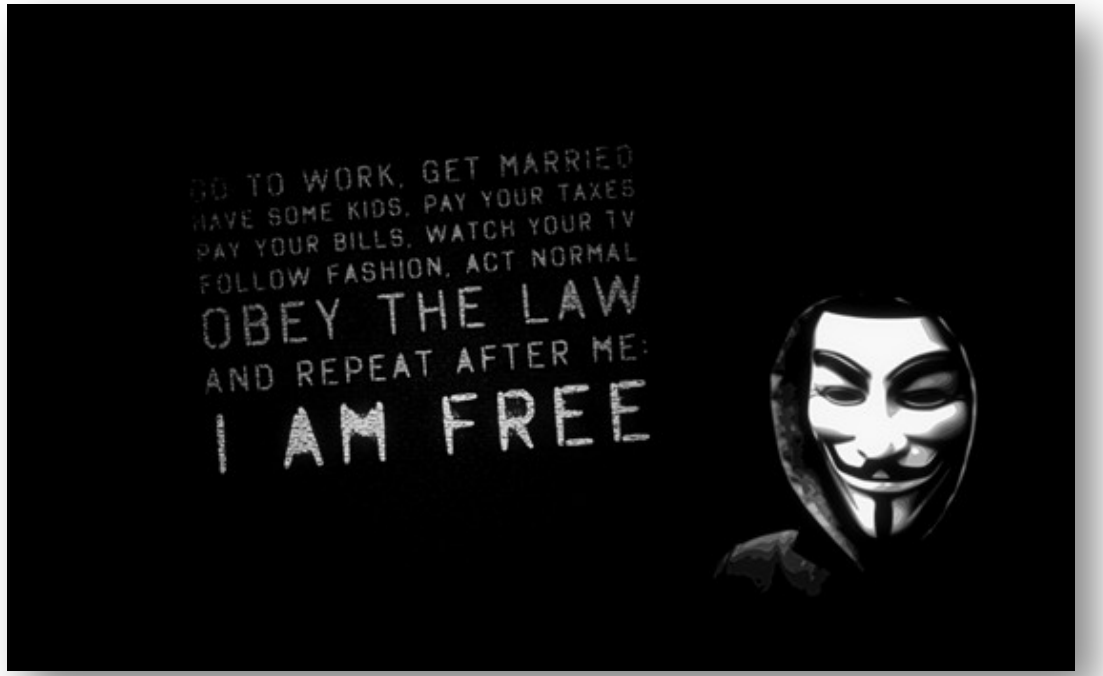
- 2014年，第三方安全机构对400家互联网金融平台进行安全检测评估，其中65%存在安全漏洞，其中35%有严重高危漏洞

平台漏洞，损失巨大

- 2014年7~8月，深圳某软件公司服务的一百多家P2P公司集中遭到了黑客的攻击，导致很大一部分损失惨重，20多家P2P平台跑路

黑客入侵导致被“拖库”

- 2015年4月9日，某P2P平台遭遇数据库泄露，网站的用户姓名、身份证号、手机号、银行卡号等大量敏感内容曝露

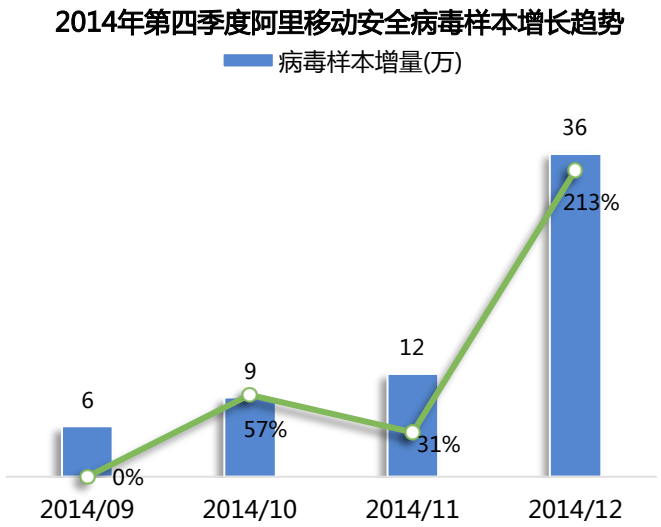


安全问题——APP安全
移动APP，漏洞层出不穷

病毒木马

100%

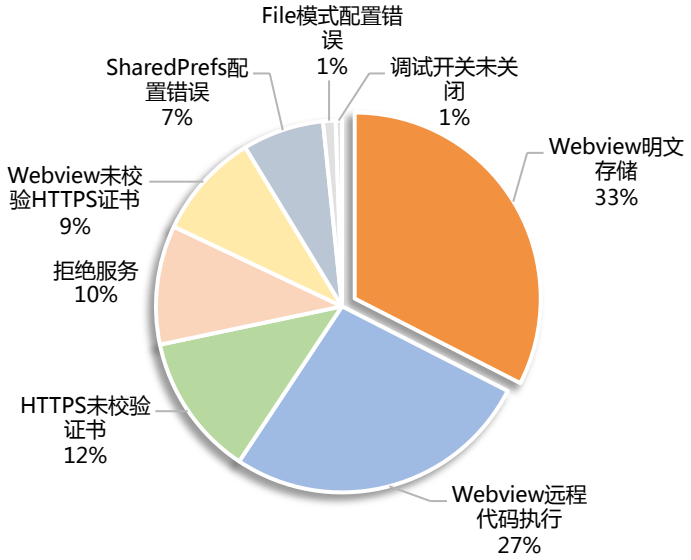
病毒木马的月均增长比例超过100%，严重威胁移动互联网的安全



应用漏洞

86%

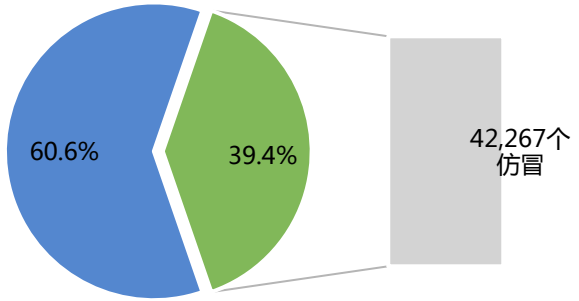
超过86%的应用存在漏洞，而开发者却没有足够的重视



仿冒应用

40%

近40%的应用存在仿冒应用，热门的应用被仿冒几率越高



安全问题——业务欺诈
垃圾注册，营销作弊

活动很快开始，最近作弊注册一堆号的黑客多了好多，一个地址一千单，我们的技术也很头疼，我们做福利是为了把东西给聚美粉丝，黑客爷们儿们别来凑热闹，干坏事会找不到女朋友的

@聚美陈欧

已经确定，黑客攻击，大家稍安勿躁，黑客也别用抢购机抢了，抢了我们也会审单剁掉，另外，小心法律制裁

8月7日 10:28 来自 iPhone 6 Plus

收藏 | 转发 3719 | 评论 91175 | 55193

8月6日

又宕机了别拦我，我去体检。。

@聚美陈欧

听说裸奔就有妹纸要联系方式，程序员们都奔起来了。。

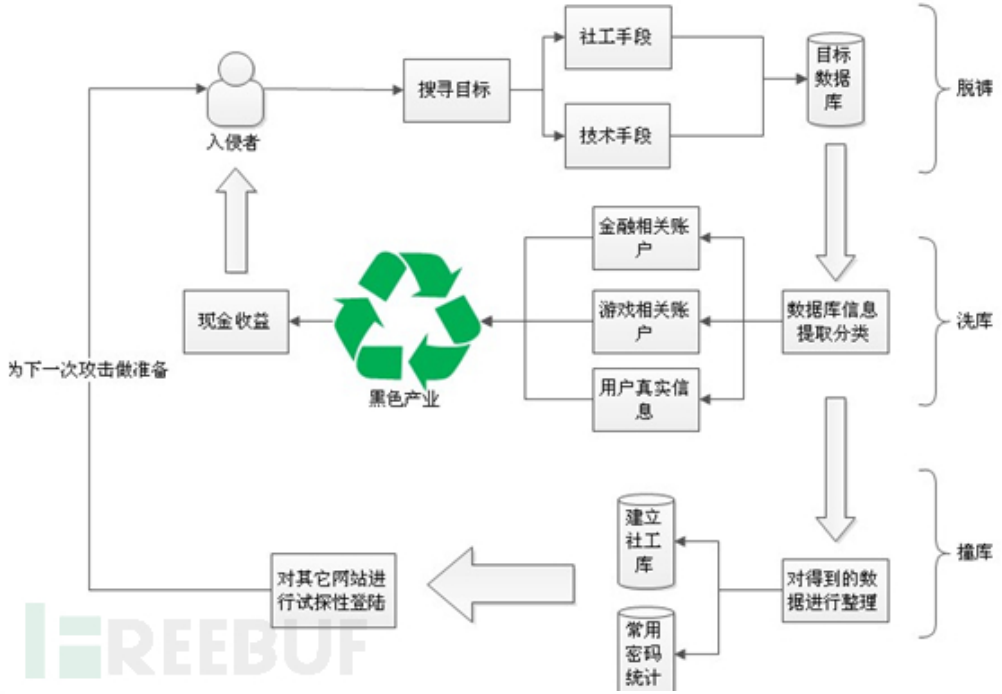
7月31日 23:27 来自 iPhone 6 Plus 转发 2335 | 评论 17288 | 38665

8月7日 10:04 来自 iPhone 6 Plus

8月7日 09:

那些曾经脱过的“裤”

天涯社区 www.tianya.cn



02 云盾安全方案

阿里云-世界级安全能力

世界级安全能力 World-Class Security Service

AliCloud provides a high level of data security for 30% of the websites across China.
Each day, it fends off more than 200 million web attacks and over 1,000 DDoS (Distributed Denial of Service) attacks, with peaks reaching 453.8 gigabytes per second.

当前阿里云保护30%中国网站安全

30%

每天防御超过

2亿次

暴力破解攻击

每天抵御1,000次以上DDoS攻击

1,000次

DDoS

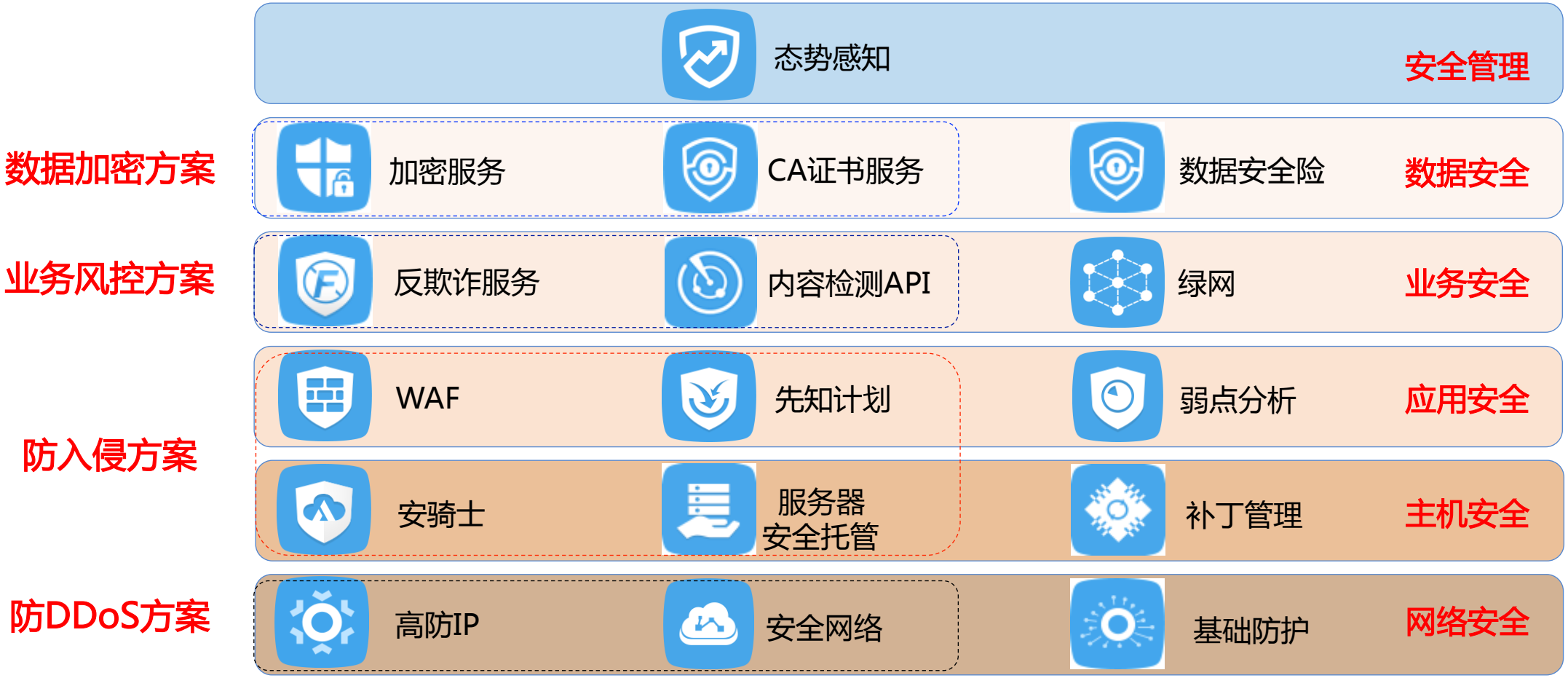
453.8 G

云盾
十年攻防，一朝成盾


护航集团业务
阿里安全团队护航阿里巴巴集团内部
所有业务系统的信息安全
云盾 v 0.6
网络流量监控
DDoS防护
主机入侵防护
Web弱点分析
云盾 v 1.6
云平台整体防护
云盾 v 3.0
云盾专有云版
态势感知
安全大数据分析
APT防护
HISTORY
2005 …… 2011
2012
2013
2014
2015
云盾 v 1.0
云平台恶意主机检测
云盾 v 2.0
云平台恶意软件查杀
云平台漏洞快速修复
云平台内容安全

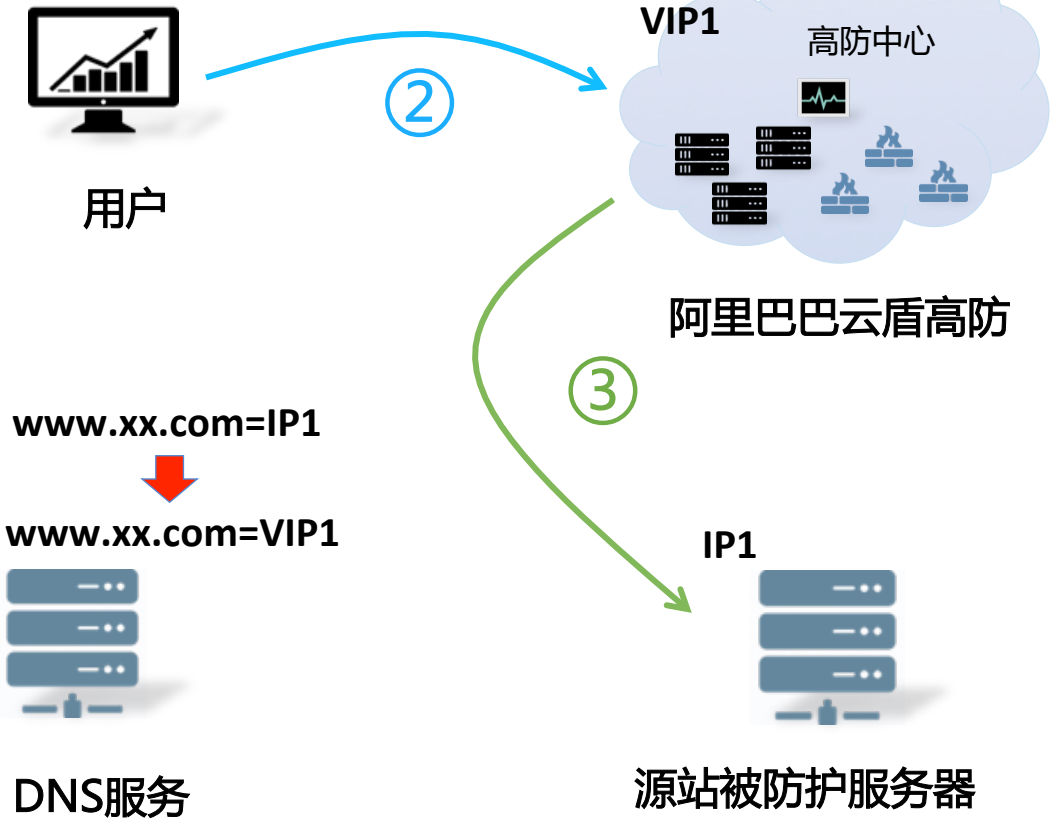
云盾产品与服务Family

十年攻防，一朝成盾



DDoS高防IP服务

接入高防



1.DNS服务器更换对外服务IP

2.流量切入高防IP

3.正常用户流量回源

特点：

- 300G攻击防护
- 按天付费
- 多线路接入
- HTTPS七层防护

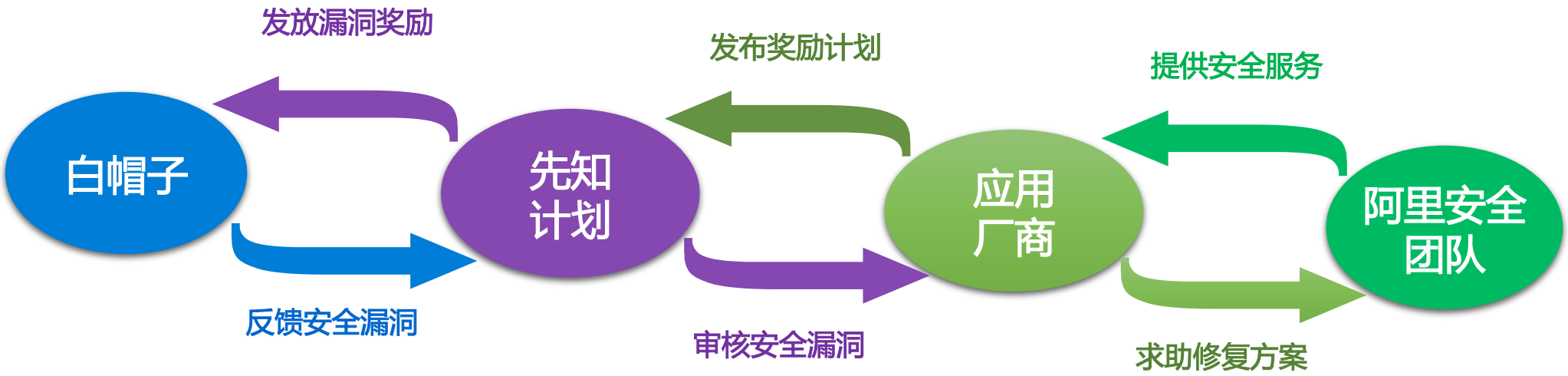
攻击防御能力全覆盖

攻击防御类型

- Malformed Packets — 有效阻断畸形单包类攻击
- Large Traffic Attacks — 轻松应对流量拥塞型攻击
- Web Application Attacks — 识别阻断WEB应用攻击
- DNS Attacks — 保护DNS服务器
- Connection Exhaustion Attacks — 精确识别连接耗尽型、慢速攻击
- WAF — SQL注入、XSS、代码执行、WEBSHELL、CRLF、CSRF
- Other — 自适应最新攻击类型

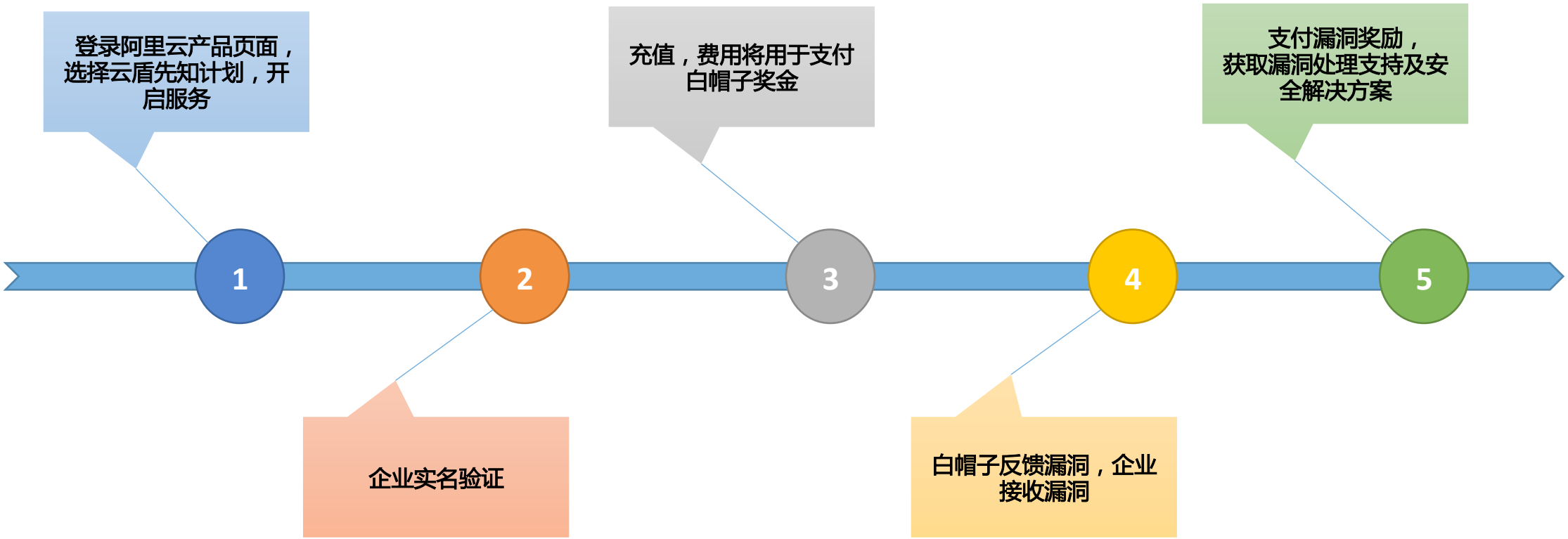
先知计划

先知计划是一个帮助企业建立私有应急响应中心的平台（帮助企业收集漏洞信息）。企业加入先知计划后，可自主发布奖励计划，激励先知平台的安全专家来测试和提交企业自身网站或业务系统的漏洞，保证安全风险可以快速进行响应和修复，防止造成更大的安全损失。



发现、响应、修复、改进，形成闭环！

先知计划-服务流程


登录阿里云产品页面，选择云盾先知计划，开启服务
1
企业实名验证
2
充值，费用将用于支付白帽子奖金
3
白帽子反馈漏洞，企业接收漏洞
4
支付漏洞奖励，获取漏洞处理支持及安全解决方案
5

先知计划-服务优势

私有的安全中心

- ✓ 不公开漏洞标题细节
- ✓ 不进行漏洞负面炒作
- ✓ 漏洞奖励金额自定义

可靠的安全专家

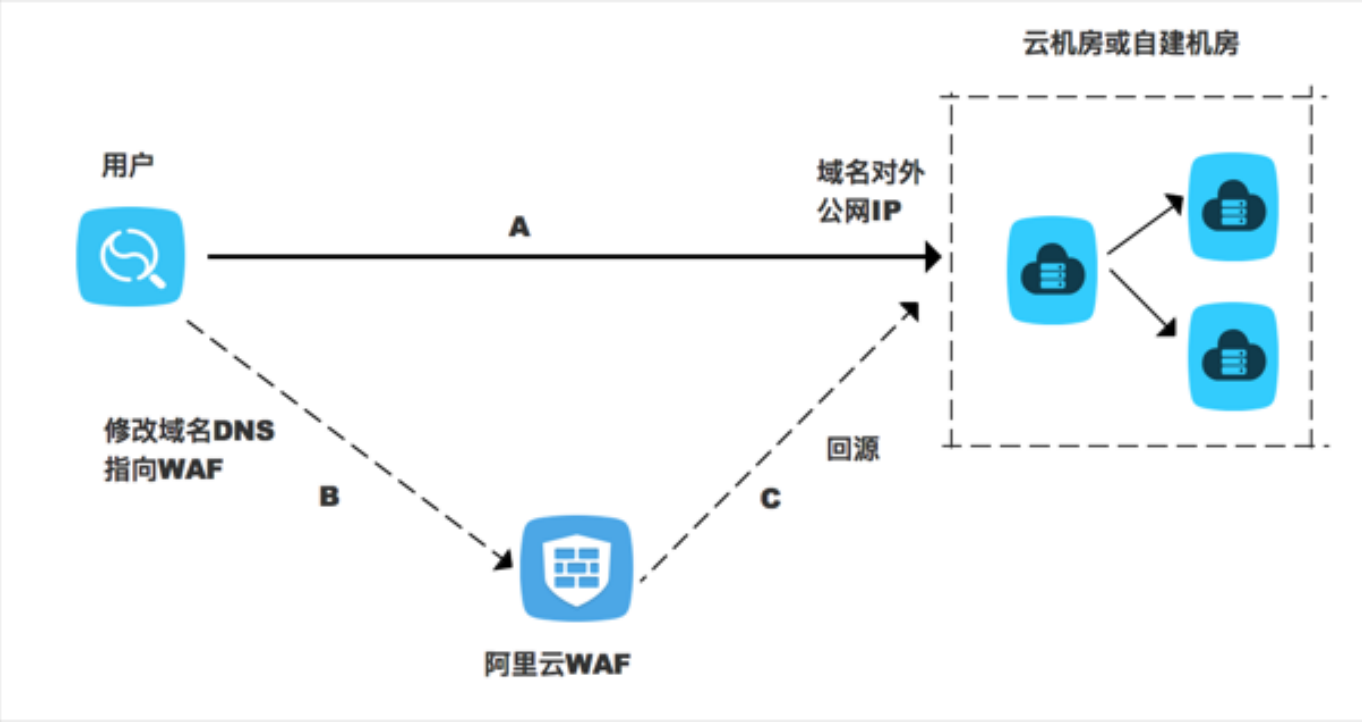
- ✓ 共享ASRC白帽子资源
- ✓ 100%支付宝实名认证
- ✓ 签署平台用户保密协议

完整的漏洞闭环

- ✓ 专业漏洞运营团队
- ✓ 引入安全服务厂商
- ✓ 可执行的修复方案

云盾WAF

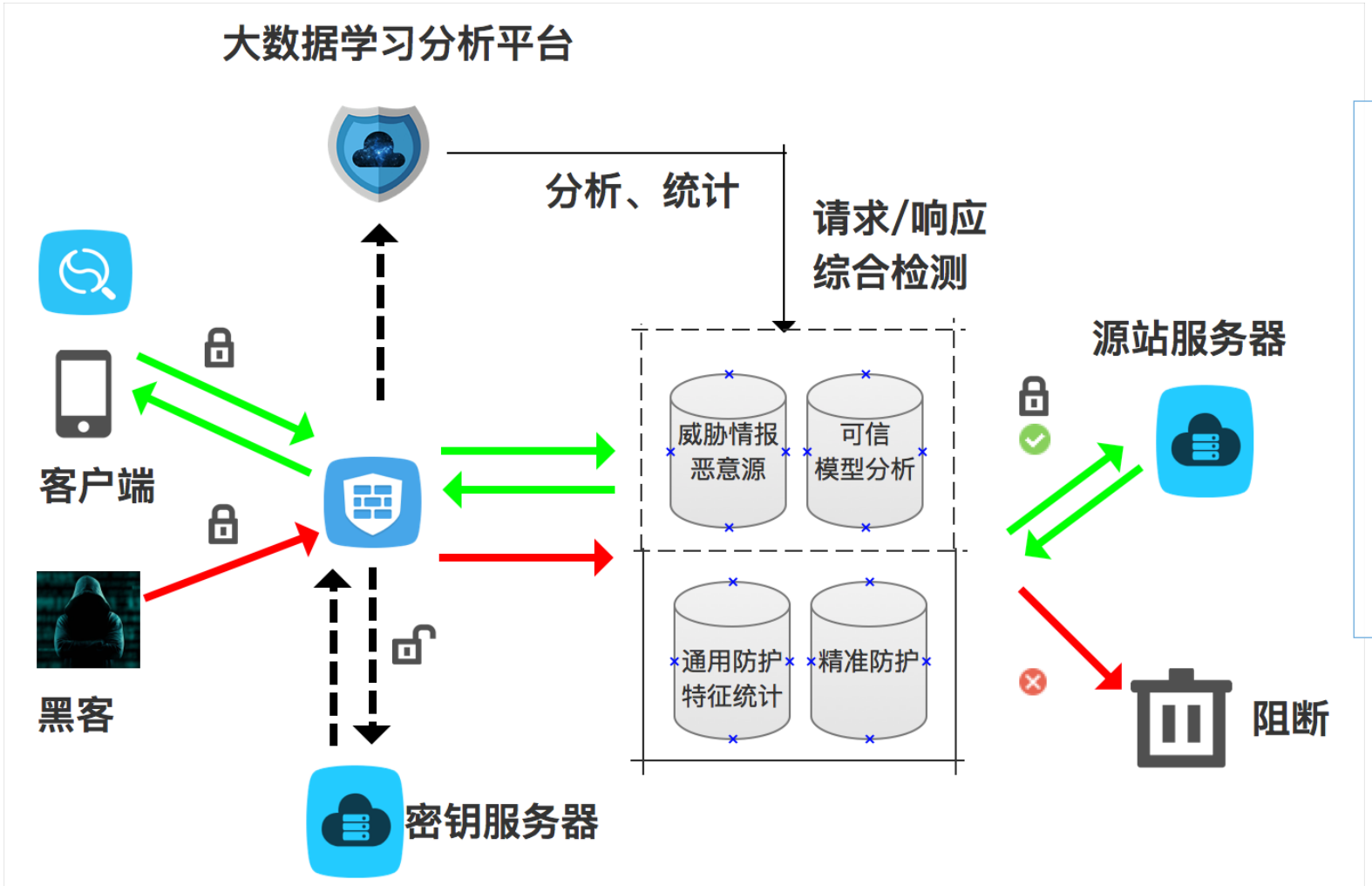
云盾WAF是一种基于云安全技术的WAF服务，它能够快速部署，实时升级，用户每时每刻都享有最新的防御策略和防护效果。



产品功能

- 通用攻击防护：SQL注入，XSS跨站脚本，Webshell上传等
- CC攻击防护：Cookie重定向，访问频率限制，威胁情报
- 精准防护：盗链防护，网站管理后台保护，自定义防护

云盾WAF产品体系架构



产品优势

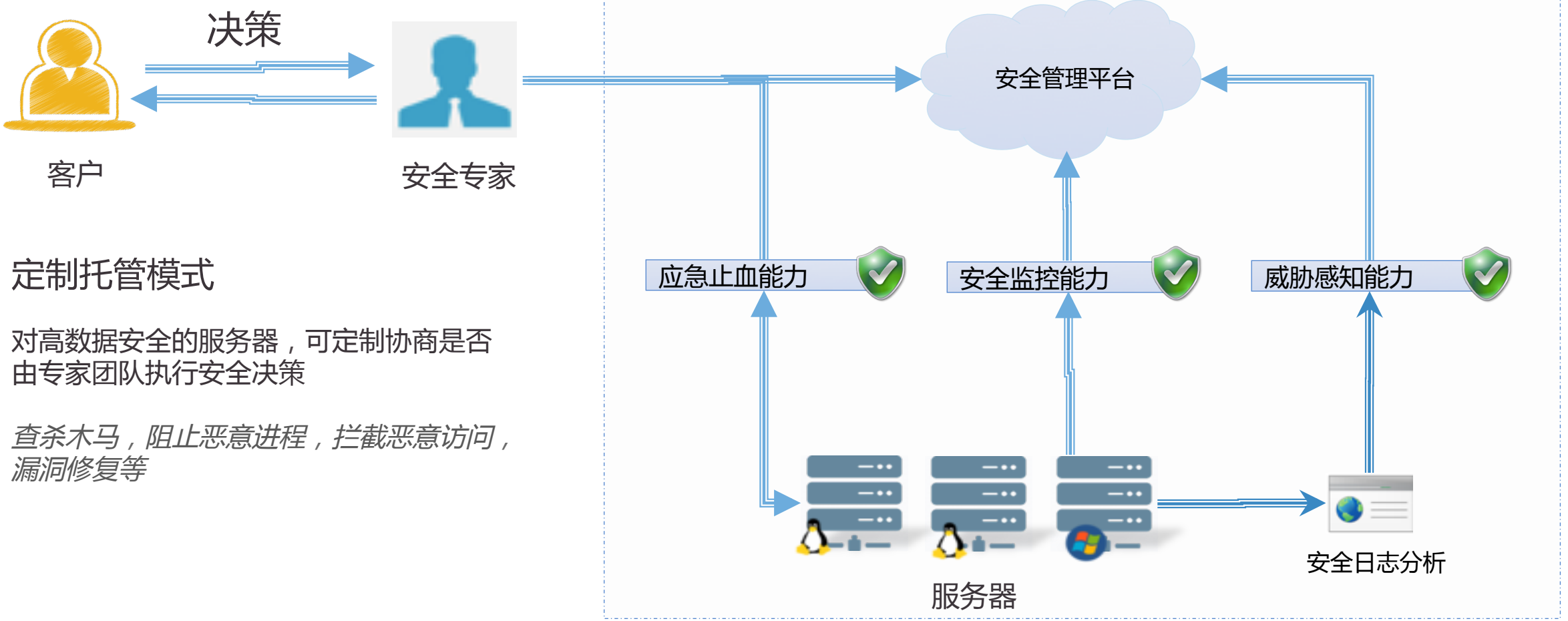
- 支持HTTPS和自定义防护策略
- 防护规则与阿里巴巴集团同步更新，检测性能与稳定性成功经受海量流量考验
- 7*24小时专家运维和监控，形成安全闭环
- 集成强大的安全大数据分析能力、共享集团全网威胁情报源和可信分析模型

服务器安全托管服务

服务器安全托管服务是一种安全专家服务，为云服务器提供定制化的安全策略防护、木马文件检测和高危漏洞检测与修复工作。当发生安全事件时，云盾安全团队提供安全事件响应、分析，并进行系统防护策略的优化。

项目	具体内容
安全评估	对托管的服务器进行整体安全评估，出具安全评估报告（包含修复建议）
漏洞管理	共享阿里巴巴漏洞情报，为客户提供漏洞监控、漏洞预警、漏洞修复的服务
基线加固	定期对服务器的安全配置进行优化，定制调整安全防护策略，提升服务器的安全防御基线
威胁分析	通过云平台整体威胁建模，分析客户安全日志，输出真实黑客攻击，保护重点资产和数据
应急响应	黑客入侵后，快速响应并阻断攻击和异常行为，避免损失扩大。同时还原攻击路径，追溯攻击源
安全咨询	提供专业级别安全咨询，帮助客户建立完善的安全体系

服务器安全托管服务

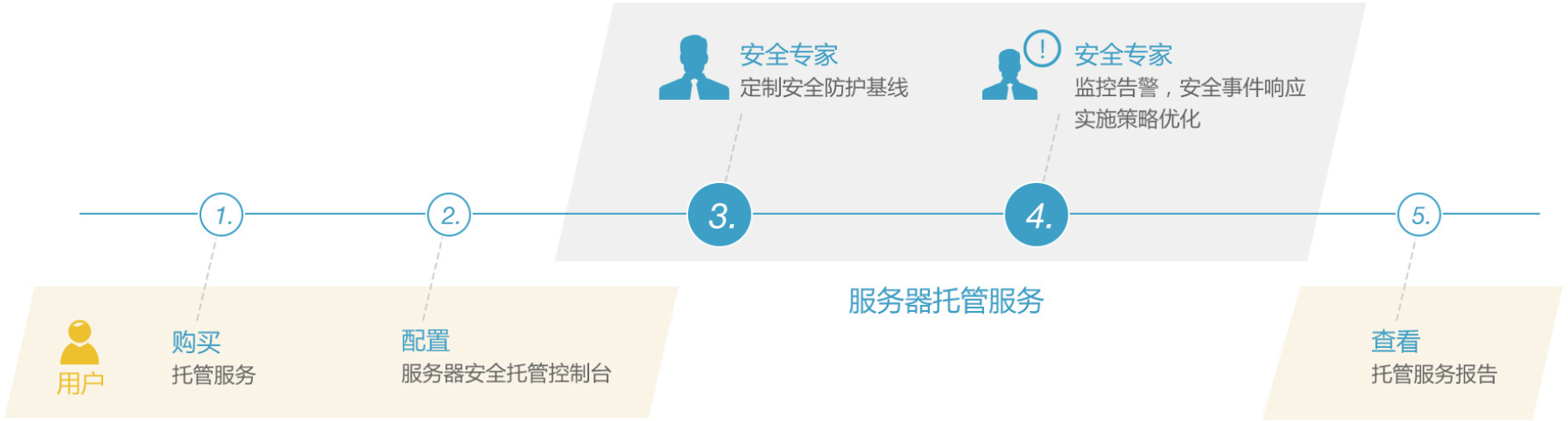


定制托管模式

对高数据安全的服务器，可定制协商是否由专家团队执行安全决策

查杀木马，阻止恶意进程，拦截恶意访问，漏洞修复等

服务流程与价值

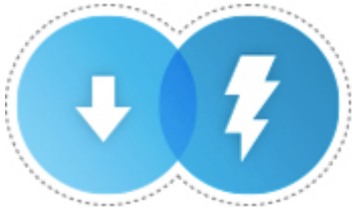


提升安全等级

云盾拥有全网最大的威胁源，
实时阻断最新安全威胁

节约成本

可节约一半以上的安全
管理成本



降低风险

阿里云安全团队实施
有SLA保证的可靠安全服务

移动安全服务

检测

木马扫描
- 快速检测恶意代码，外包APP安全性检测
- 第三方SDK安全性检测

漏洞扫描
- 业界最全的自动化漏扫引擎
- 发现应用自身安全风险，并提供分级机制与修复建议

安全评估服务
- 业界顶尖安全专家团队评估
- 深度渗透移动应用及相关业务，发掘安全隐患

防护

安全组件
- 快速组件化接入
- 业界独创的端安全能力
- 亿级应用久经攻防考验

应用加固
- 提供了快速加固，多渠道加固以及自定义加固
- 实战验证高兼容性、高稳定性、高性能

情报

安全告警
- 业界漏洞、安全风险第一时间通报
- 规避或解决方案的建议

仿冒监测
- 大数据监测全网活跃应用,关注论坛，网盘等高风险渠道
- 多维度仿冒检测能力

应用风险感知
- 运行环境监测（Root / JB / 模拟器）
- 攻击行为监测（注入 / 篡改 / 调试）
- 业务风险

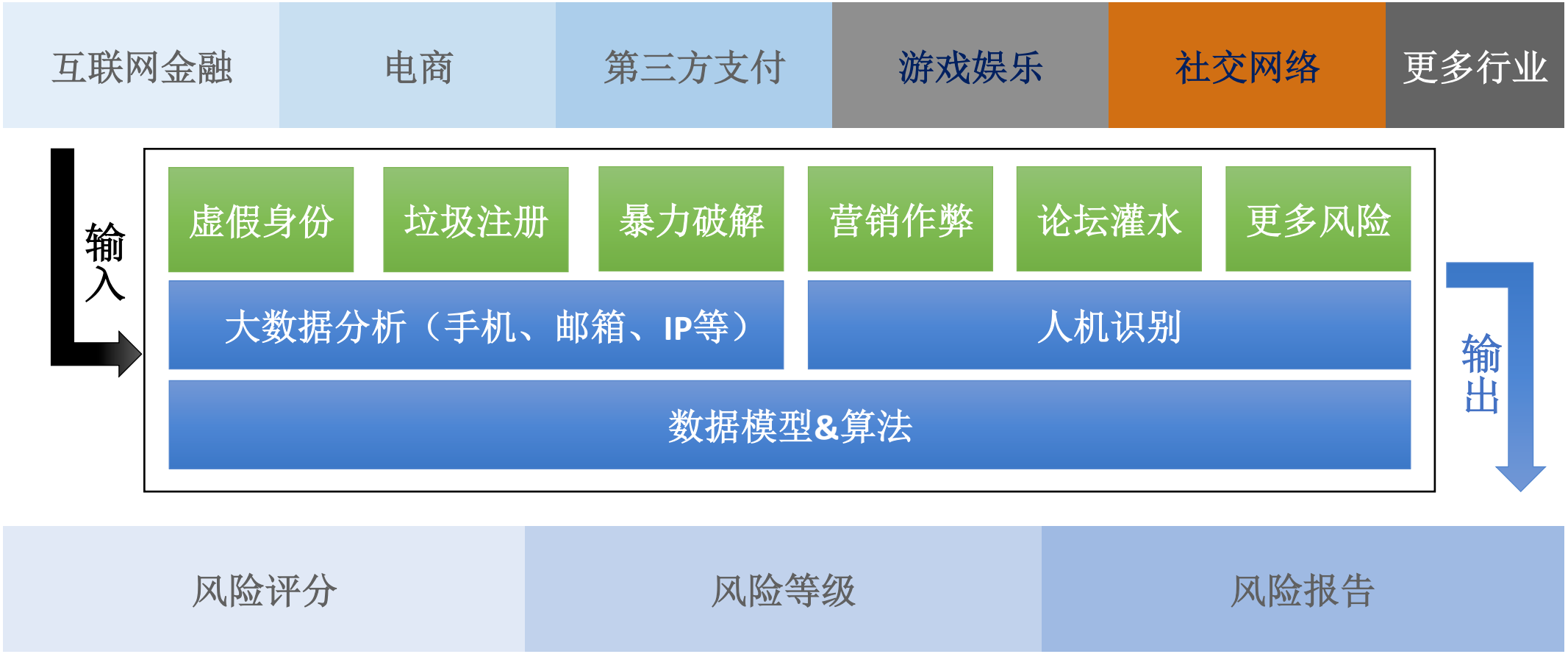
咨询

安全流程咨询
- 设计、开发、测试、上线、运营全流程安全咨询
- 上线安全标准与规范培训

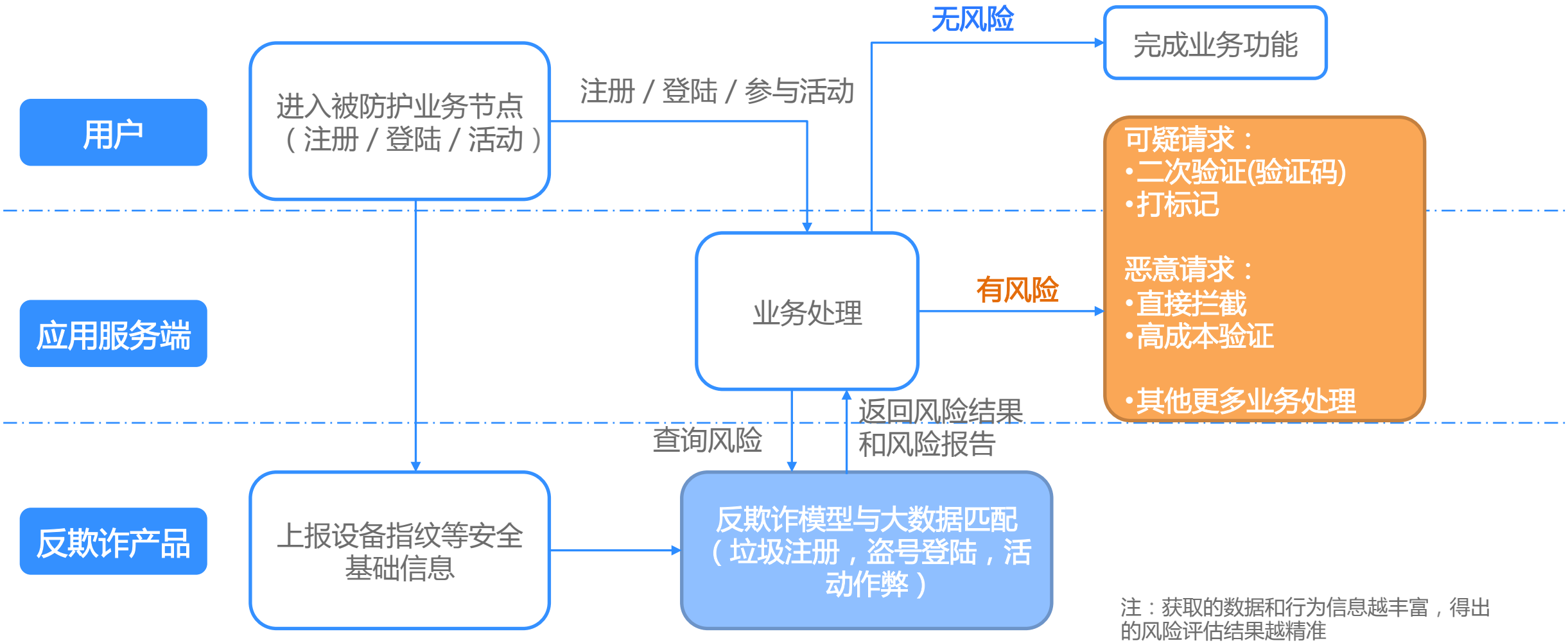
应急响应
- 公关事件应急响应
- 活动护航

反欺诈服务

反欺诈服务是阿里大数据风控服务能力的对外输出，通过**整合**包含互联网金融、电商、第三方支付等**众多行业的数据**，配合领先的**行为收集技术**，经过**机器学习模型**、**大数据关联分析和指标计算**，**解决**账号、活动、交易等**关键业务环节**存在的欺诈威胁。



反欺诈防护流程示例

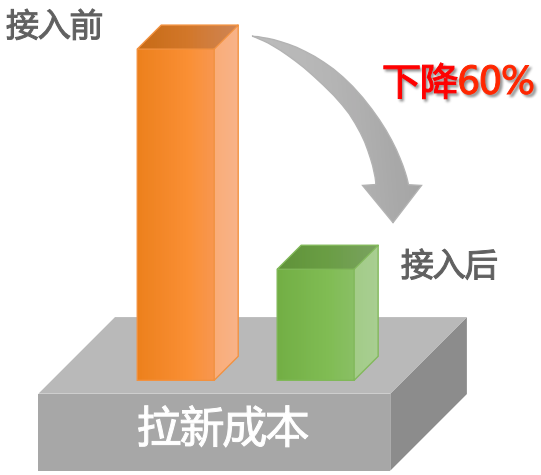


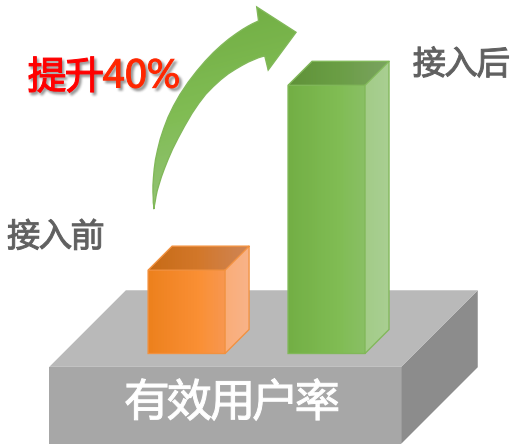
注：获取的数据和行为信息越丰富，得出的风险评估结果越精准

成功案例——某O2O应用

某O2O应用，处于推广阶段，进行了新注册用户返现的活动。此消息马上被互联网黑产团伙获悉，发起了大规模的垃圾注册。一时间系统压力陡增，市场经费也损失较大。

- **接入产品前，**恶意注册占比**30~70%**
- **接入产品后，**识别恶意领用**数万次**



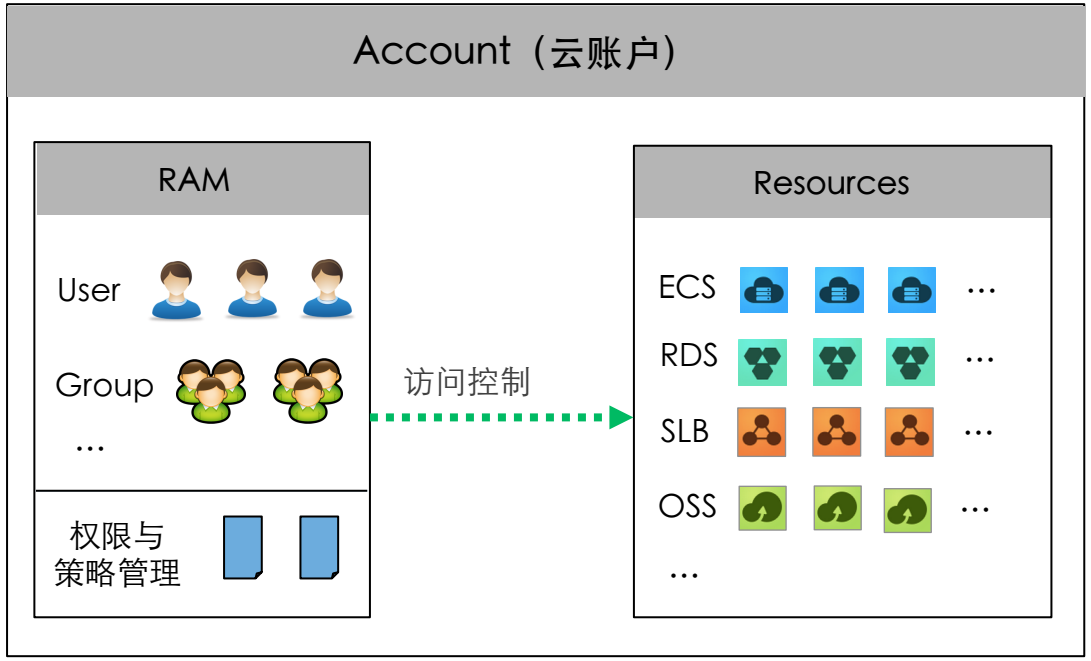


节约推广费用**近百万**

账户安全管理-RAM

阿里云资源访问管理服务（RAM）使得**一个阿里云账户（主账户）可拥有多个子账户**，支持**分组授权**、**双因素认证**、强密码策略、控制台用户与API用户分离、**临时授权**、账户临时禁用等功能。授权可以细化到API粒度，**支持时间段、源IP地址、资源标签等条件。**

RAM**是阿里云账户安全管理和安全运维的基础。**通过RAM可以为每个子账户分配不同的密码或AK，**消除了云账户共享带来的风险**；同时可为不同的子账户分配不同的权限和细化条件，**大大降低了因账户权限过大带来的风险。**



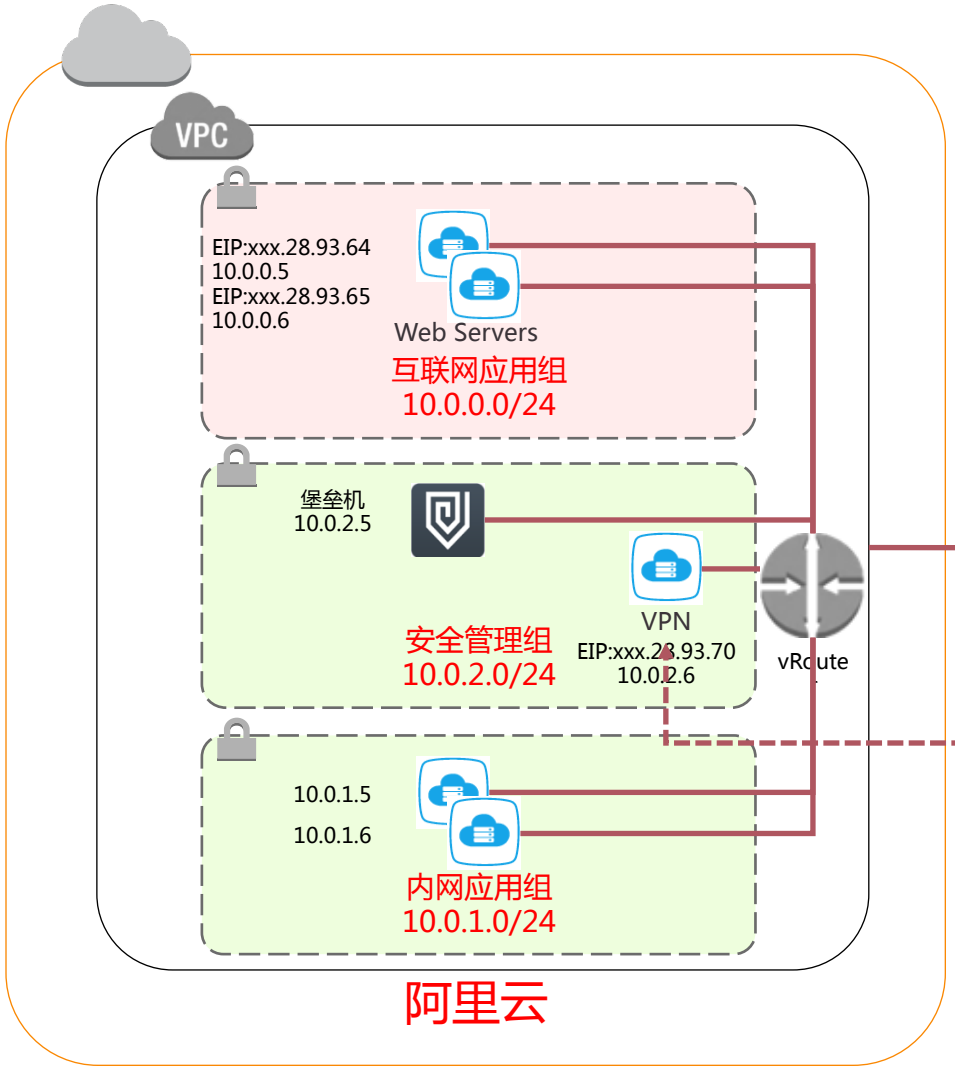
RAM功能

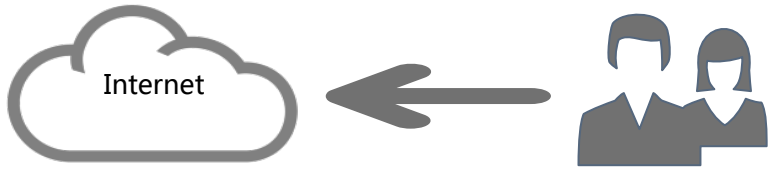
- 子账号和组
- 认证方式：
  - AccessKey ID/Secret
  - 用户名/密码
  - 双因素认证
- 细粒度授权策略
  - OpenAPI授权
  - 资源授权
- 临时授权
- 强密码策略
- 跨主账号授权

RAM优点

- 子账号对应到自然人，确保账号唯一
- 分组授权，实现权限分离
- 细粒度授权策略，实现最小授权
- 强密码、双因素、临时授权，保护账号
- 跨主账号授权实现跨公司、跨部门协作

云上安全接入与运维





1、登录VPN公网地址
2、登录堡垒机进行运维

云上运维安全问题：

- 需要开放所有ECS的互联网管理运维权限，或自行架设跳板机，但跳板机存在诸多不便，且无法进行有效权限控制；
- 操作日志没有记录，安全事件无法追溯；

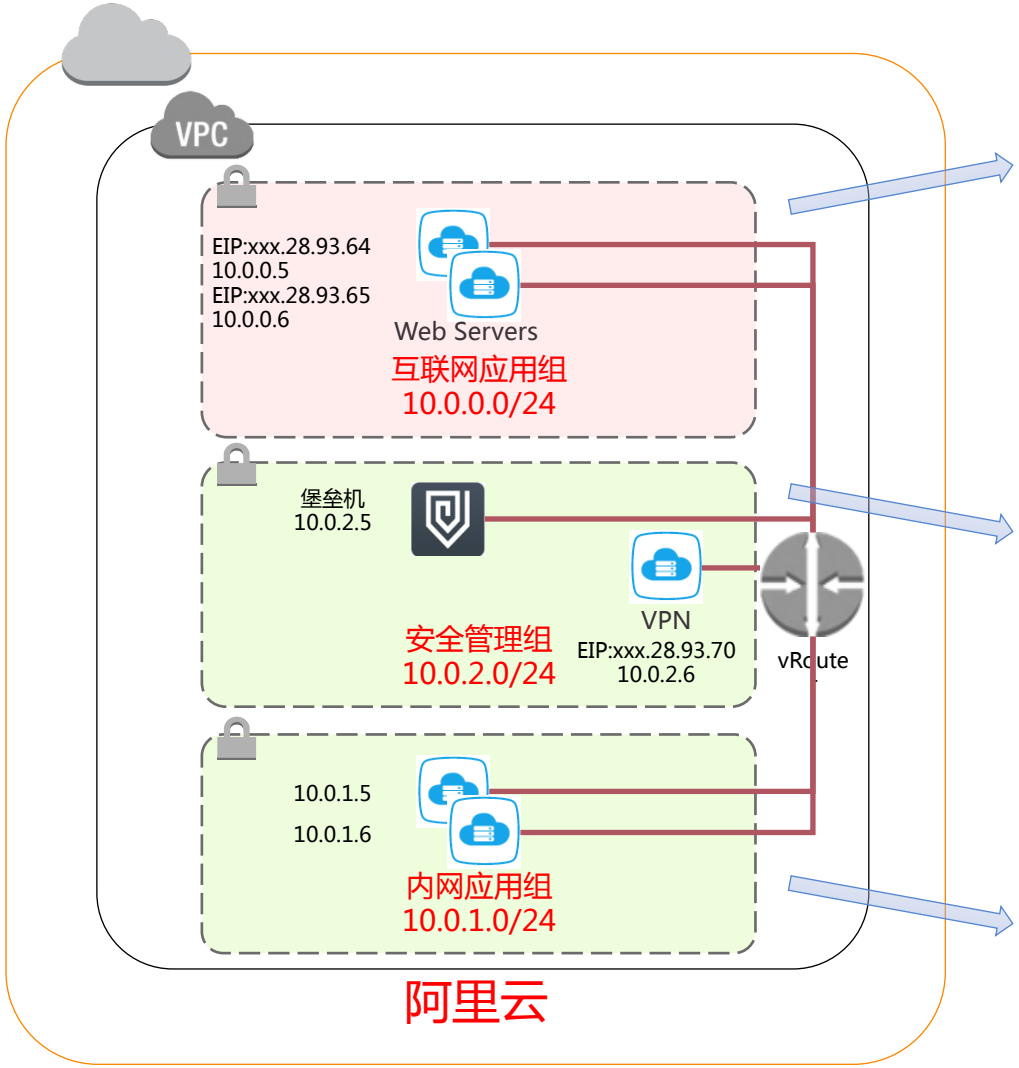
部署VPN和堡垒机产品（经典网络与VPC均适用）：

- 在云市场中购买第三方虚拟VPN和堡垒机产品；
- 在云上增加一个安全管理组，专门用于部署VPN和堡垒机等安全产品，并设置仅安全管理组IP可以访问其他ECS；

方案价值：

- VPN+堡垒机成为唯一的运维通道，ECS运维端口不必对外；
- 堡垒机实现运维实名制，所有操作可定位到人；
- 远程运维过程全审计，可实现实时监控、事后回放；
- 满足等级保护等法律法规要求；

云上安全访问控制



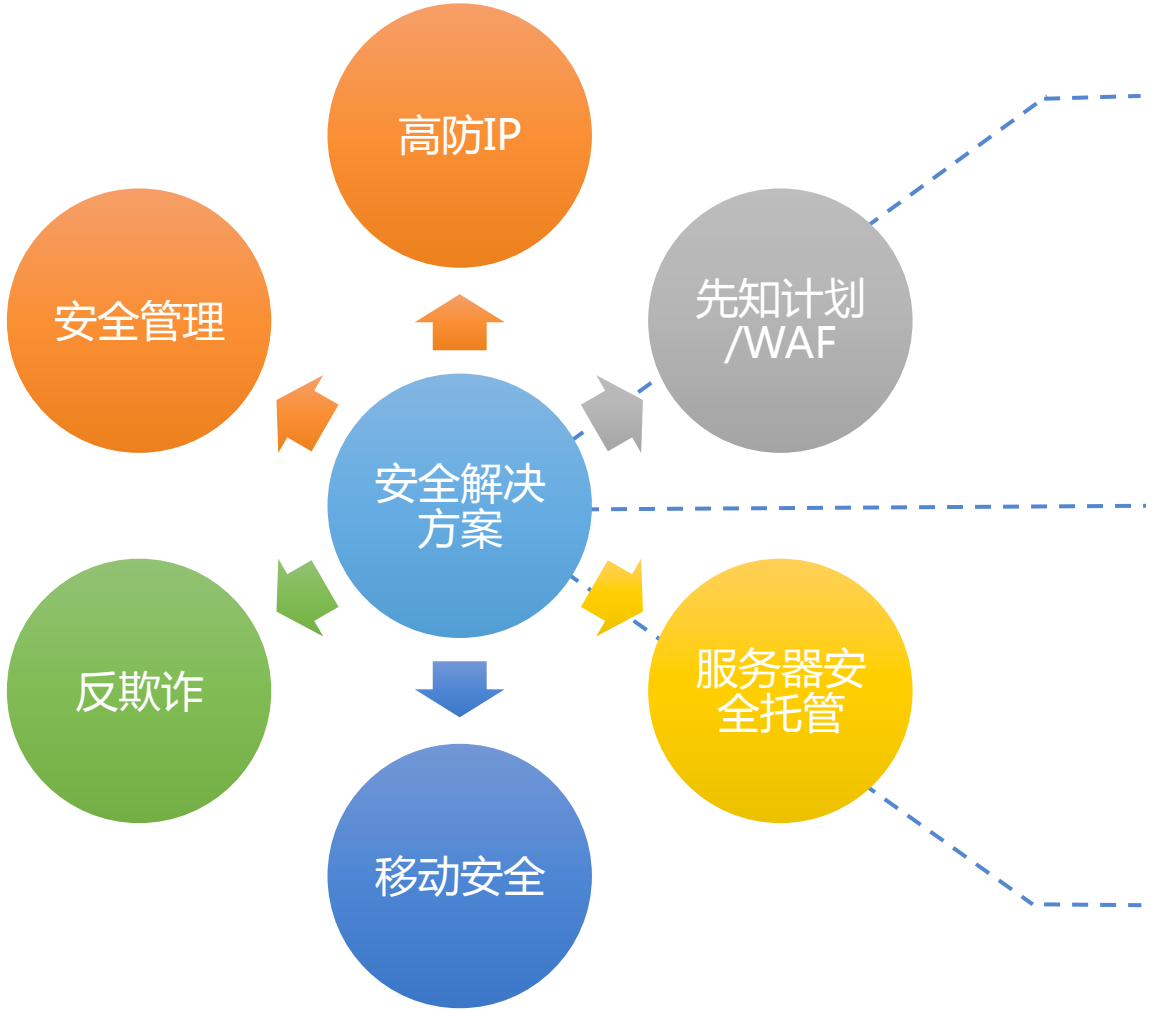
安全组防火墙策略示例：

授权访问源	方向	策略	网卡	协议	目的端口	备注
0.0.0.0/0	入方向	允许	外网	tcp	80	允许从任何地方对Web服务器进行入站HTTP访问
0.0.0.0/0	入方向	允许	外网	tcp	443	允许从任何地方对Web服务器进行入站HTTPS访问
安全管理组	入方向	允许	内网	tcp	22	Linux实例允许来自运维安全组的入站SSH访问
安全管理组	入方向	允许	内网	tcp	3389	Windows实例允许来自运维安全组的入站RDP访问

授权访问源	方向	策略	网卡	协议	目的端口	备注
0.0.0.0/0	入方向	允许	外网	tcp	443	允许从任何地方访问运维安全组的SSL VPN和堡垒机服务（也可限制为办公网IP）
0.0.0.0/0	入方向	允许	外网	gre	4430	SSL VPN需要允许从任何地方发起的VPN管理访问（配置完成以后此策略可以关闭）
0.0.0.0/0	入方向	允许	外网	udp	500	如果使用L2TP/IPSec VPN，则允许从任何地方访问运维安全组的IPSec IKE服务
0.0.0.0/0	入方向	允许	外网	udp	4500	如果使用L2TP/IPSec VPN，则允许从任何地方访问运维安全组的IPSec NAT-T服务
0.0.0.0/0	入方向	允许	外网	udp	1194	如果使用默认的OpenVPN协议和端口，则允许从任何地方访问运维安全组的OpenVPN服务

授权访问源	方向	策略	网卡	协议	目的端口	备注
互联网应用组	入方向	允许	内网	tcp	8080	允许安全组1访问安全组2的应用服务端口
安全管理组	入方向	允许	内网	tcp	22	Linux实例允许来自运维安全组的入站SSH访问
安全管理组	入方向	允许	内网	tcp	3389	Windows实例允许来自运维安全组的入站RDP访问

安全解决方案总结
十年攻防，一朝成盾



阿里云云盾高级服务

高防IP
- 防御DDoS、CC、Web漏洞攻击
- 高防：业务高可用性，全流量清洗，300G以上防御

先知计划
- 全球顶尖安全专家，丰富的行业经验
- 专业的安全服务报告

WAF
- 通用攻击防护
- CC攻击防护
- 精准防护

服务器安全托管
- 安全体检与系统加固
- 安全告警实时监控和处理，专家定制安全防护策略

反欺诈
- 反垃圾注册，反营销作弊
- 防暴力破解，防撞库

安全管理
- RAM主子账号功能，避免账户共享和权限过大
- VPN+堡垒机，安全接入，操作全记录
- 配置安全组防火墙策略，实施安全访问控制
- 态势感知服务（免费使用），云上安全管控中心

谢谢！

Let’s Talk