

因唯安全
所以信赖
唯与同行,智御未来

千寻位置 Qianxun SI 傅奎

2018 唯品会第三届互联网电商安全峰会
2018 vip.com third Internet ecommerce Security Summit
2018-5-5 上海

中小企业
云上安全技术实践

我要我的云安全



我要我的云安全

中小企业

云上安全技术实践

向先行者致敬

我要我的云安全——

但，

从来就没有什么银弹，

有的只是

血泪教训

和惨淡的经验……

云计算和企业上云是大势所趋

上了云就更安全了吗？

不存在的！

安全产品 · 云盾

DDoS高防IP

Web应用防火墙

游戏盾

安骑士

态势感知

CA证书服务

内容安全

安全管家

堡垒机

加密服务

数据库审计

云防火墙

实人认证

安全加速 SCDN

混合云

网络漏洞扫描系统 NEW

安全解决方案

等保合规安全解决方案

政务云安全解决方案

新零售安全解决方案

混合云态势感知解决方案

互联网金融安全解决方案

游戏安全解决方案

社交/媒体spam解决方案

移动App推广欺诈解决方案

企业预防勒索解决方案

安全服务 · 先知

安全众测

等保测评

应急响应

漏洞扫描服务

安全培训

安全评估

代码审计

网站安全监测服务

安全加固

安全保障服务

现场值守服务

安全通告服务

安全应急演练服务

PCI DSS合规咨询

安全公益

产业安全扶助计划

安全

BGP 高防（网络安全）

网站管家 WAF（网络安全）

云镜（主机安全）

Web 漏洞扫描（网络安全） NEW

活动防刷（业务安全）

登录保护（业务安全）

验证码（业务安全）

内容安全（业务安全）

应用安全（移动安全）

手游反作弊（移动安全）

专家服务

态势感知

数据加密服务

案例一：防 DDoS，稳稳的黑洞

2017年，某个深夜。

服务器被黑洞，而我们还在沉睡……

案例一：防 DDoS，稳稳的黑洞

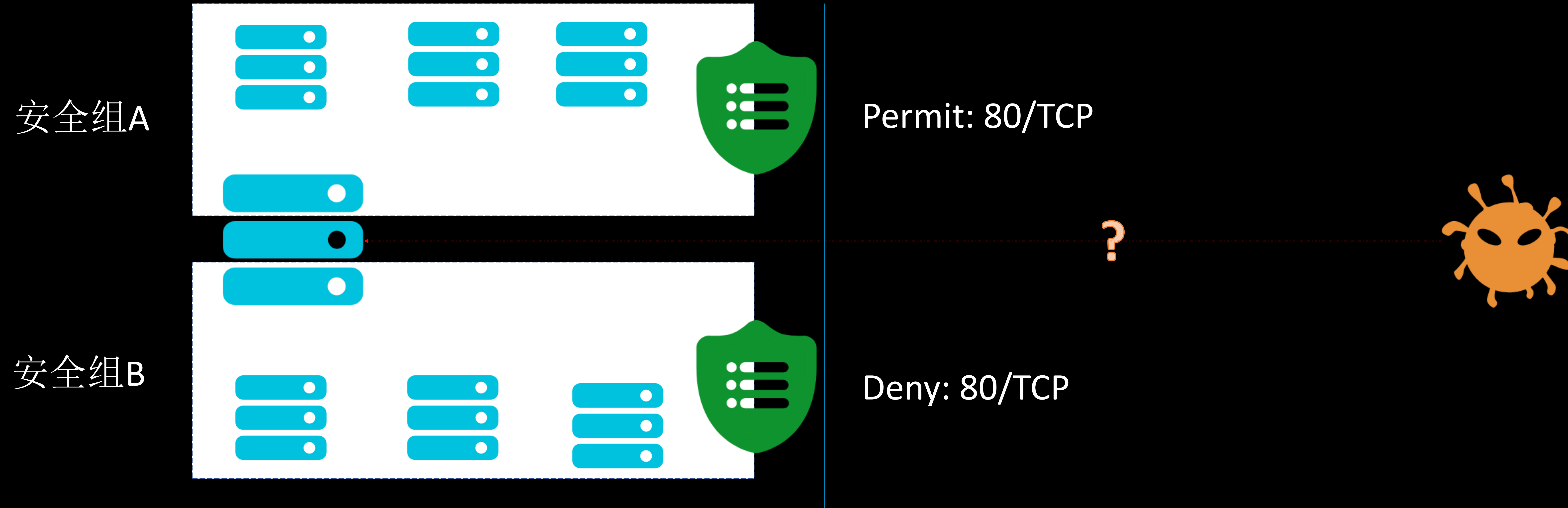
事件类型：DDoS	受影响资产：(ECS)
事件描述：遭受峰值流量为3319M的DDoS攻击，持续时间30分钟	被攻击资产：(ECS)
开始时间：2017-06-24 22:21:37	结束时间：2017-06-24 22:51:41
攻击响应状态：清洗	防护建议： 购买，可有效防护DDoS流量攻击

案例二：薛定谔的安全组

“安全组” “不安全”

访问控制策略既是关闭的，也是开放的……

案例二：“薛定谔”的安全组



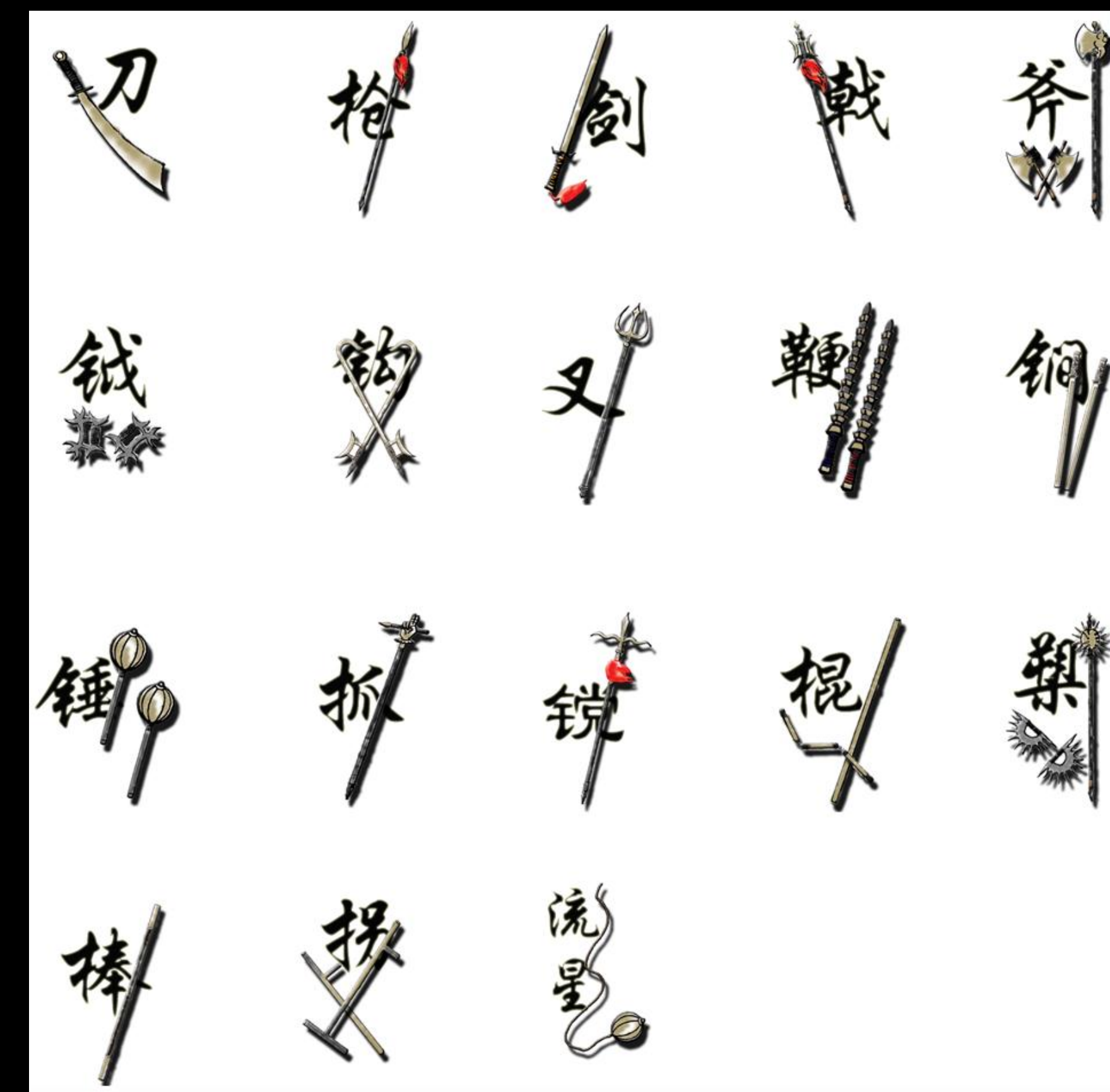
案例三：DPI了解一下？

“我也想做流量分析，问题是数据包在哪？”

“只有南北，无问西东？”

不要试图在云平台上自建 IDC.....

十八般武器都玩不转了？



云平台不是万能的，怎么办？

上了“贼船”你还能怎么样？



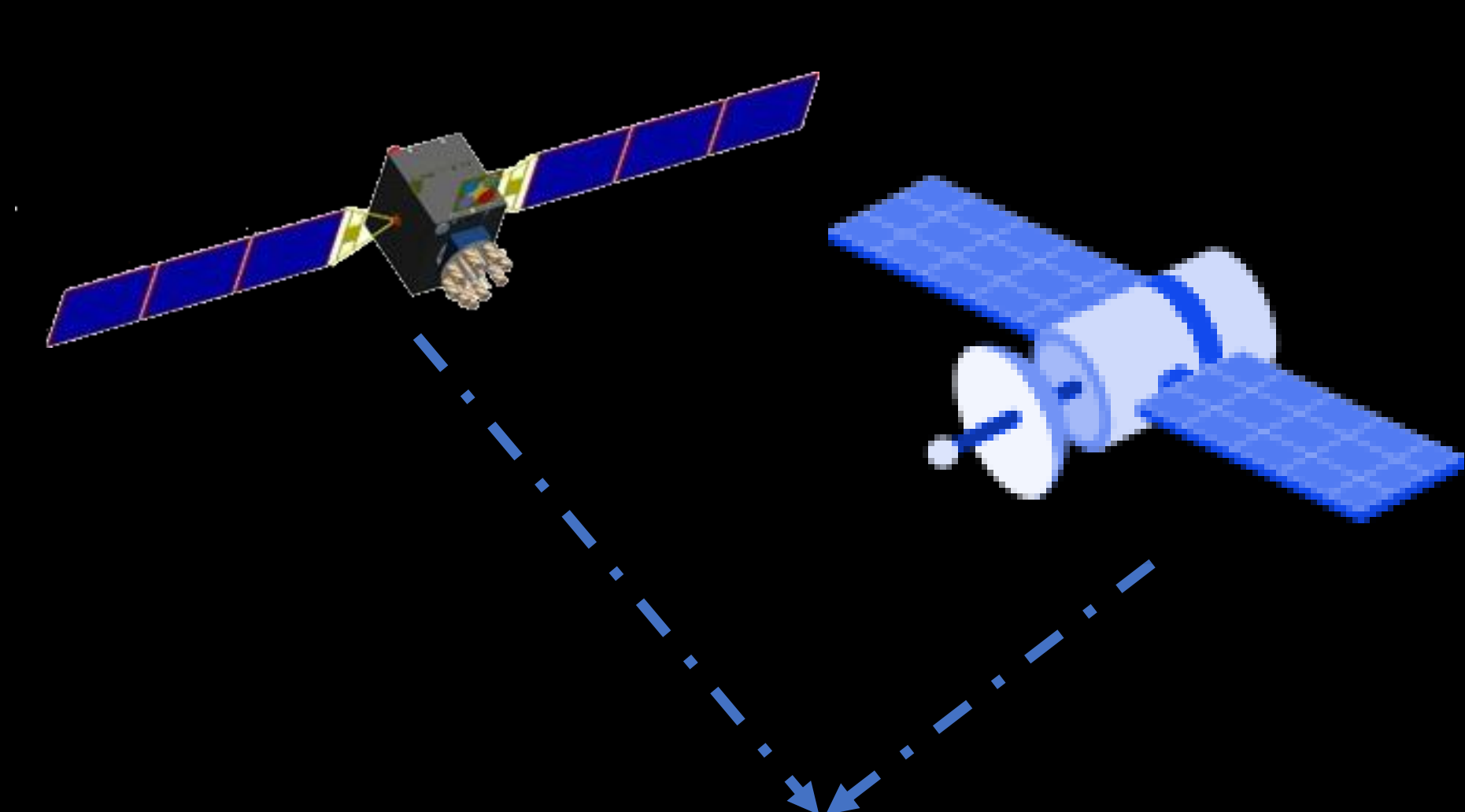
运行环境发生变化，

安全工作也要与时俱进



高精度位置服务在公有云上的安全防护实践

（基于阿里云）



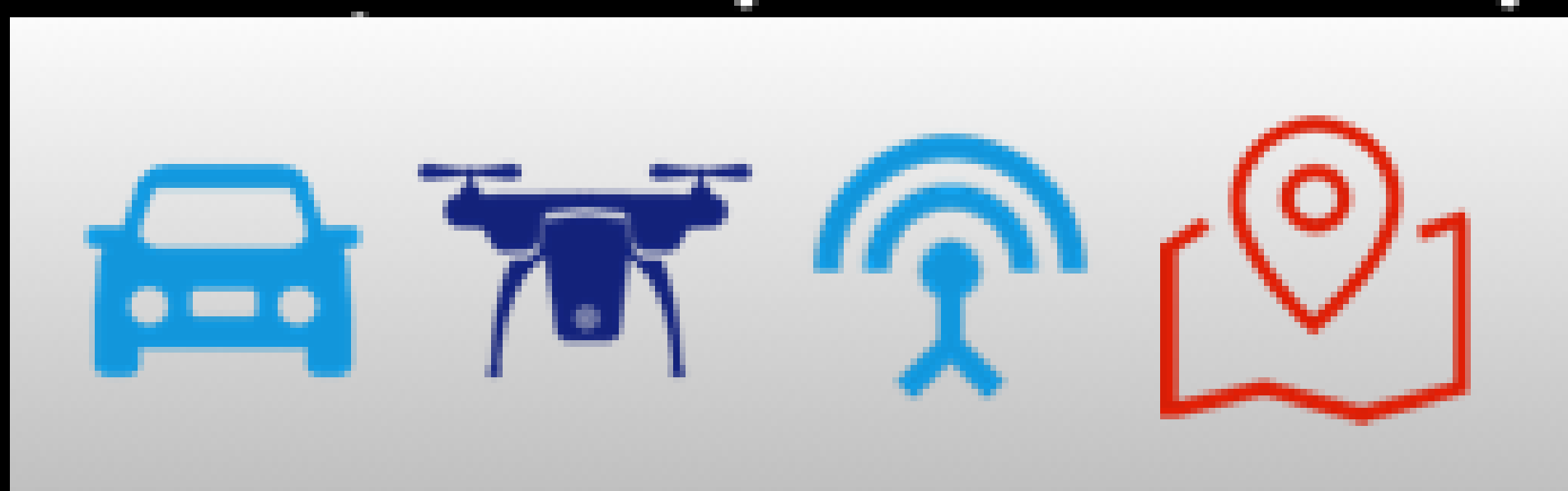


坐标解算



网络播发

利用云平台、大数据的能力为万物互联时代提供高精度位置服务



SDK客户端



浏览器



全球服务

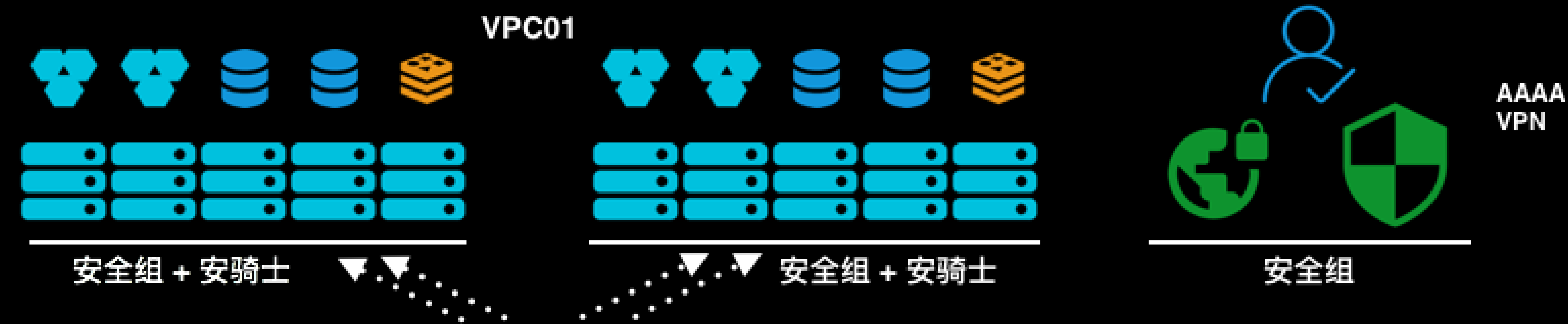
亿级用户

实时动态厘米级

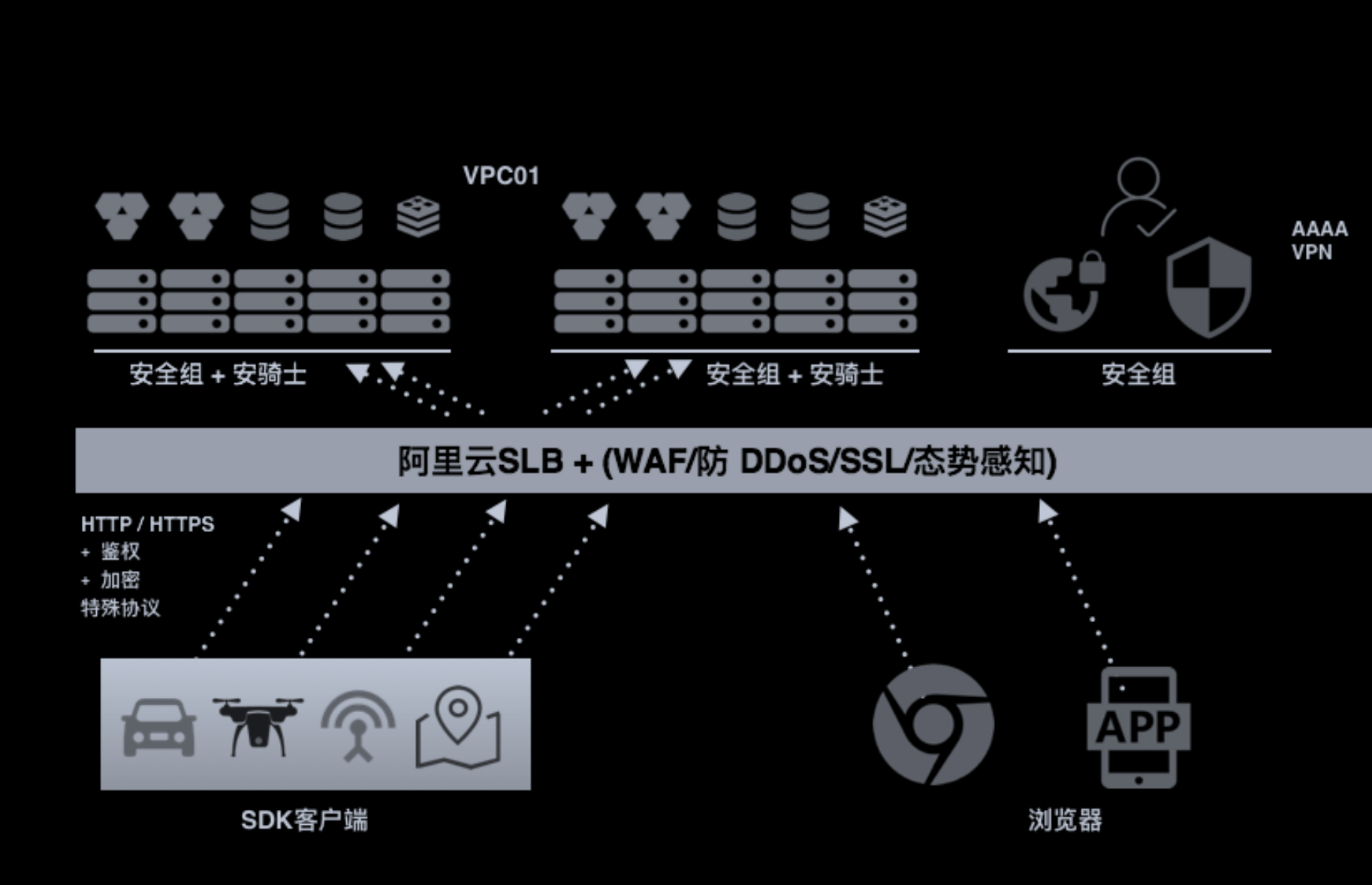
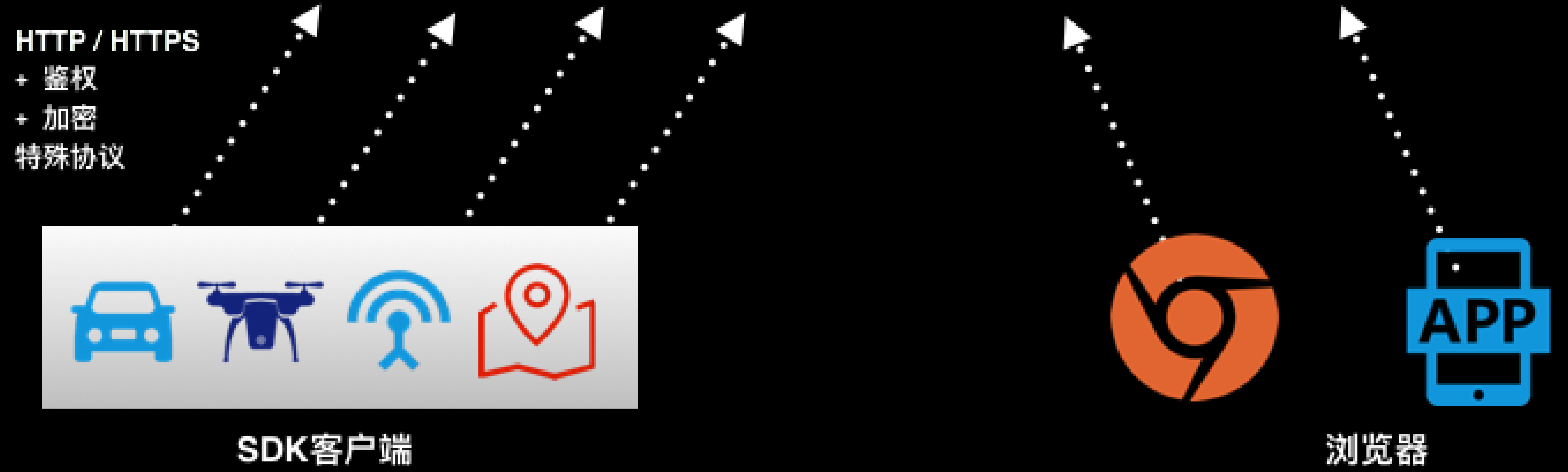
静态后处理毫米级

1) 基础安全防护:

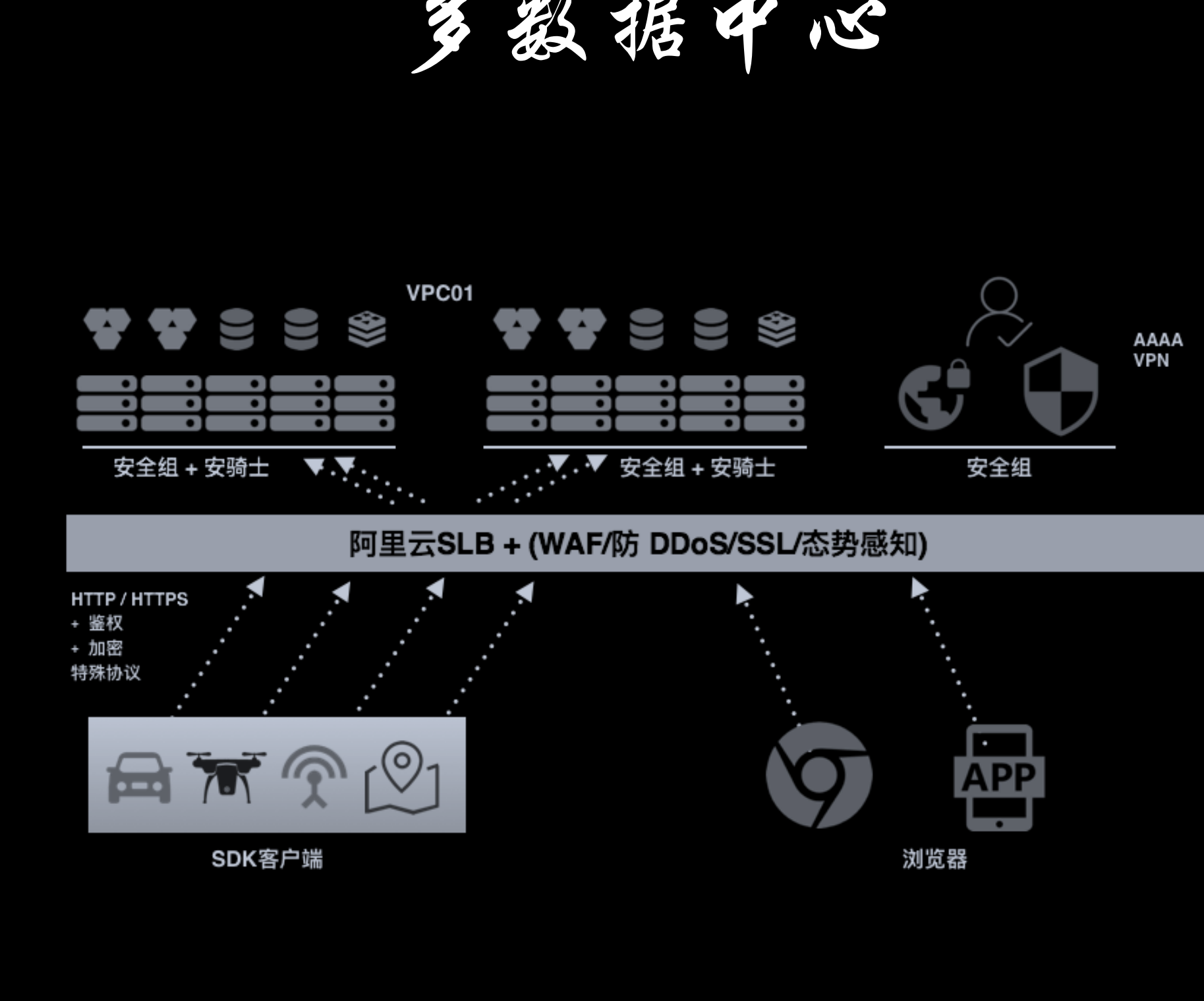
用好云平台基础产品，
识边界，扎篱笆。



阿里云SLB + (WAF/防 DDoS/SSL/态势感知)



多数据中心

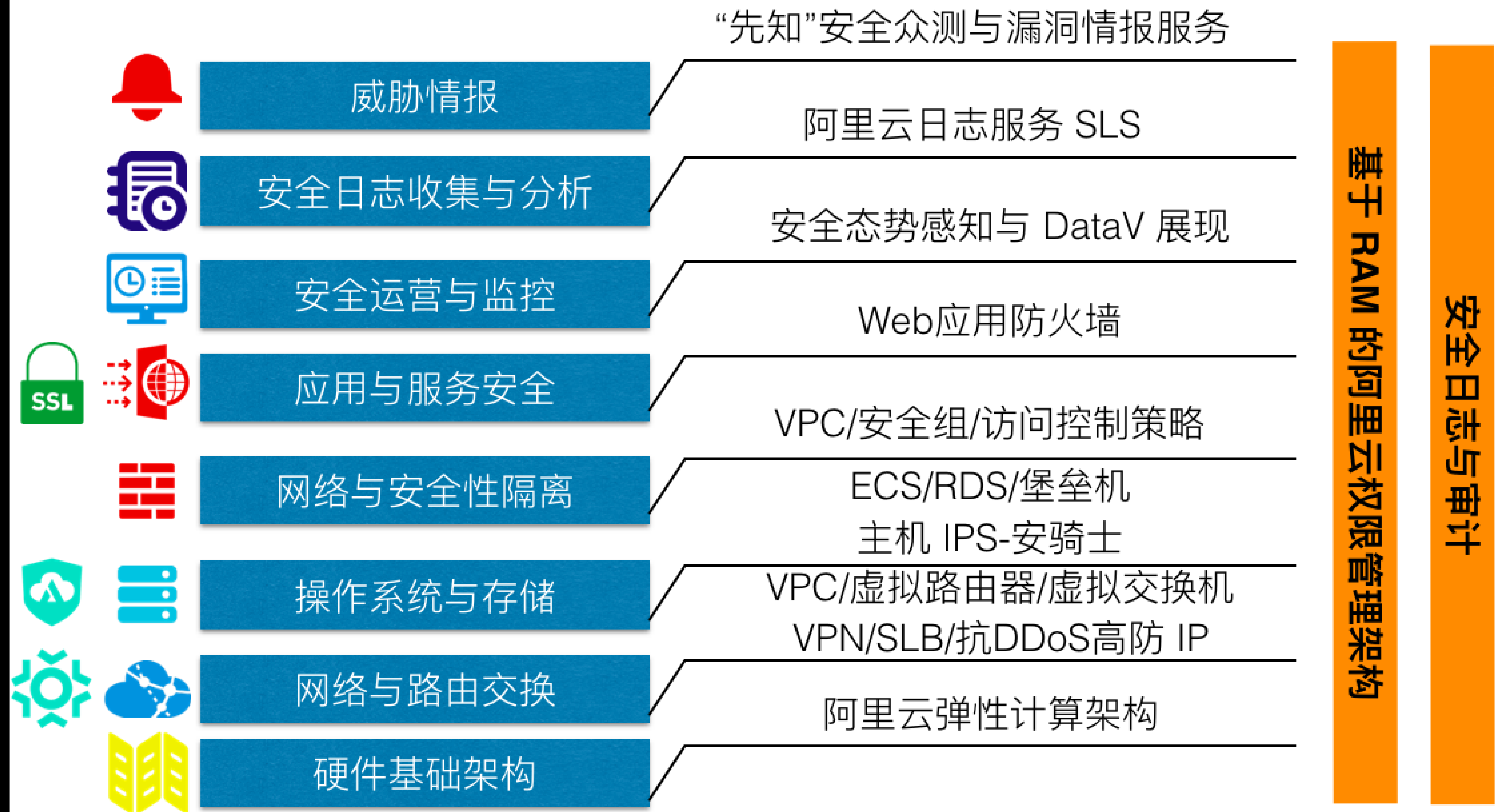


2) 科学搭建云上安全防护框架:

深入理解云产品是前提,

不仅仅是安全产品。

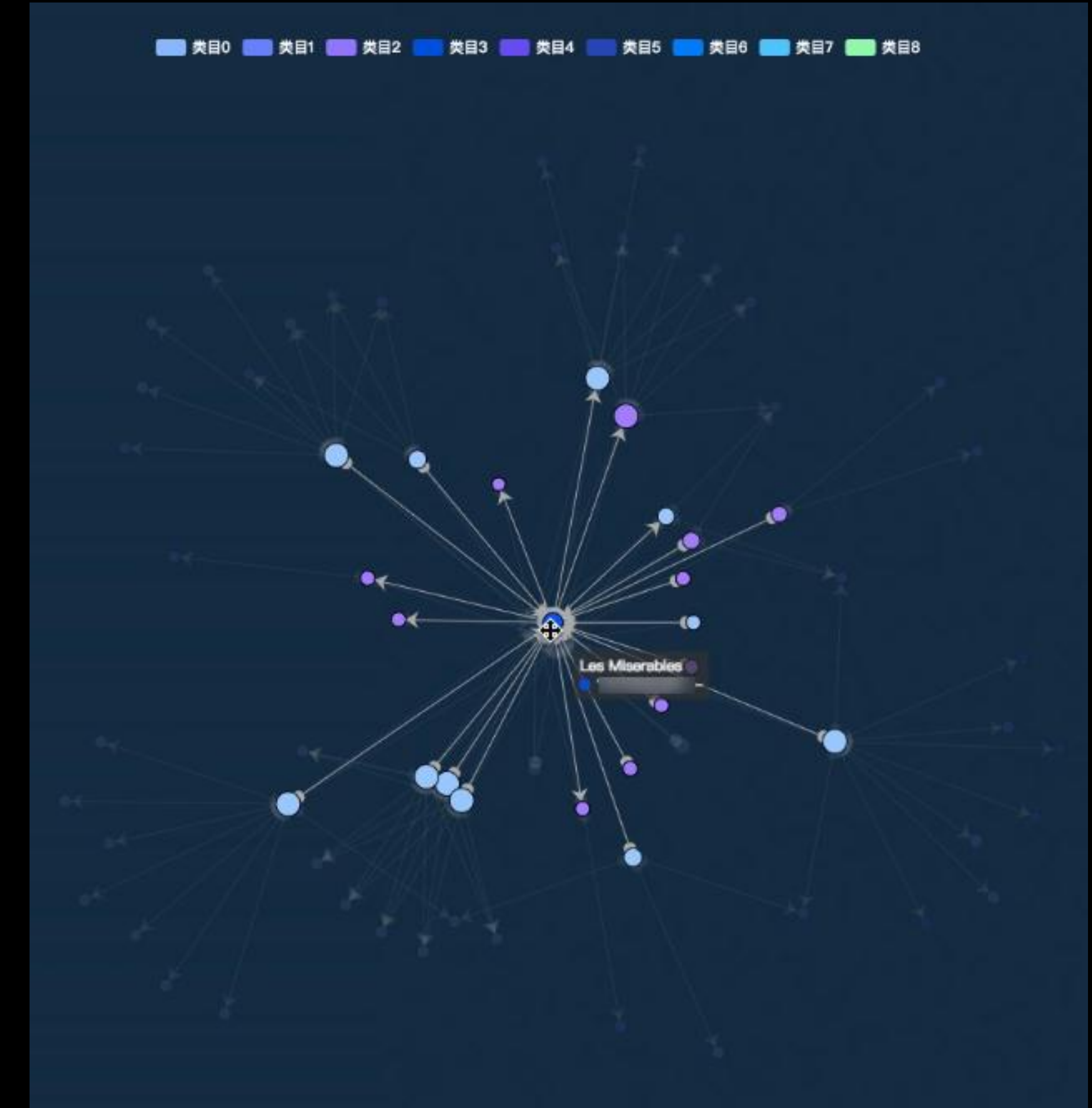
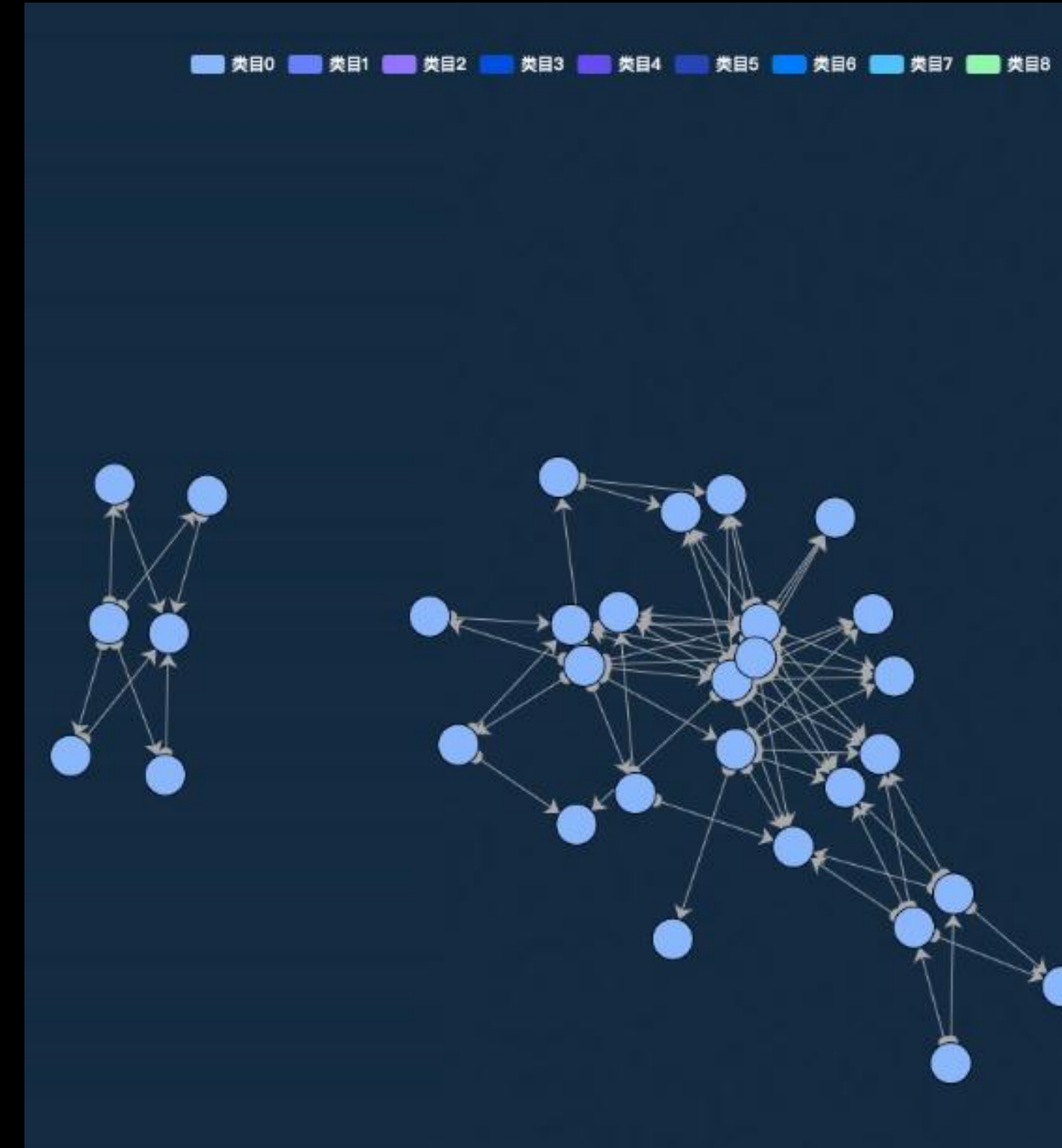
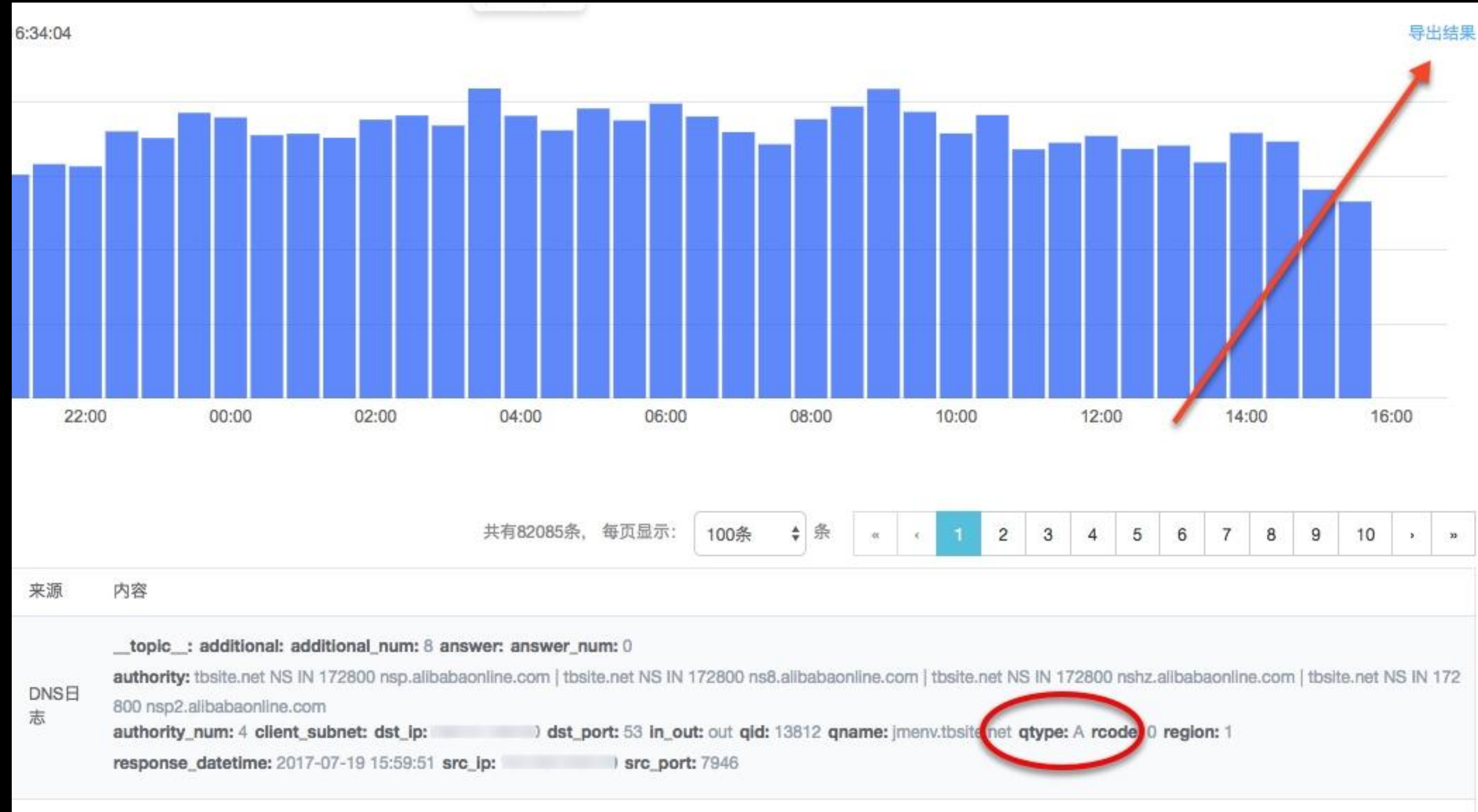
云上企业网络安全架构（基于阿里云）



3) 榨干云安全产品功能:

穷，就得物尽其用……

应用实践：态势感知DNS 日志分析



应用实践：网络会话日志分析

云盾 • 态势感知

总览
资产列表
安全告警
漏洞管理
基线配置核查
设置
更多功能

日志 [返回](#) (((🔔))) 3 [日志投递](#)

日志功能暂属于Beta测试阶段，当前企业版客户可进行体验，欢迎使用！

搜索条件 ?

not

网络连接

dst_port (目标端口)

等于

3389

+

-

not

网络连接

src_ip (源IP)

等于

152.31

+

-

not

网络连接

src_ip (源IP)

等于

64.11

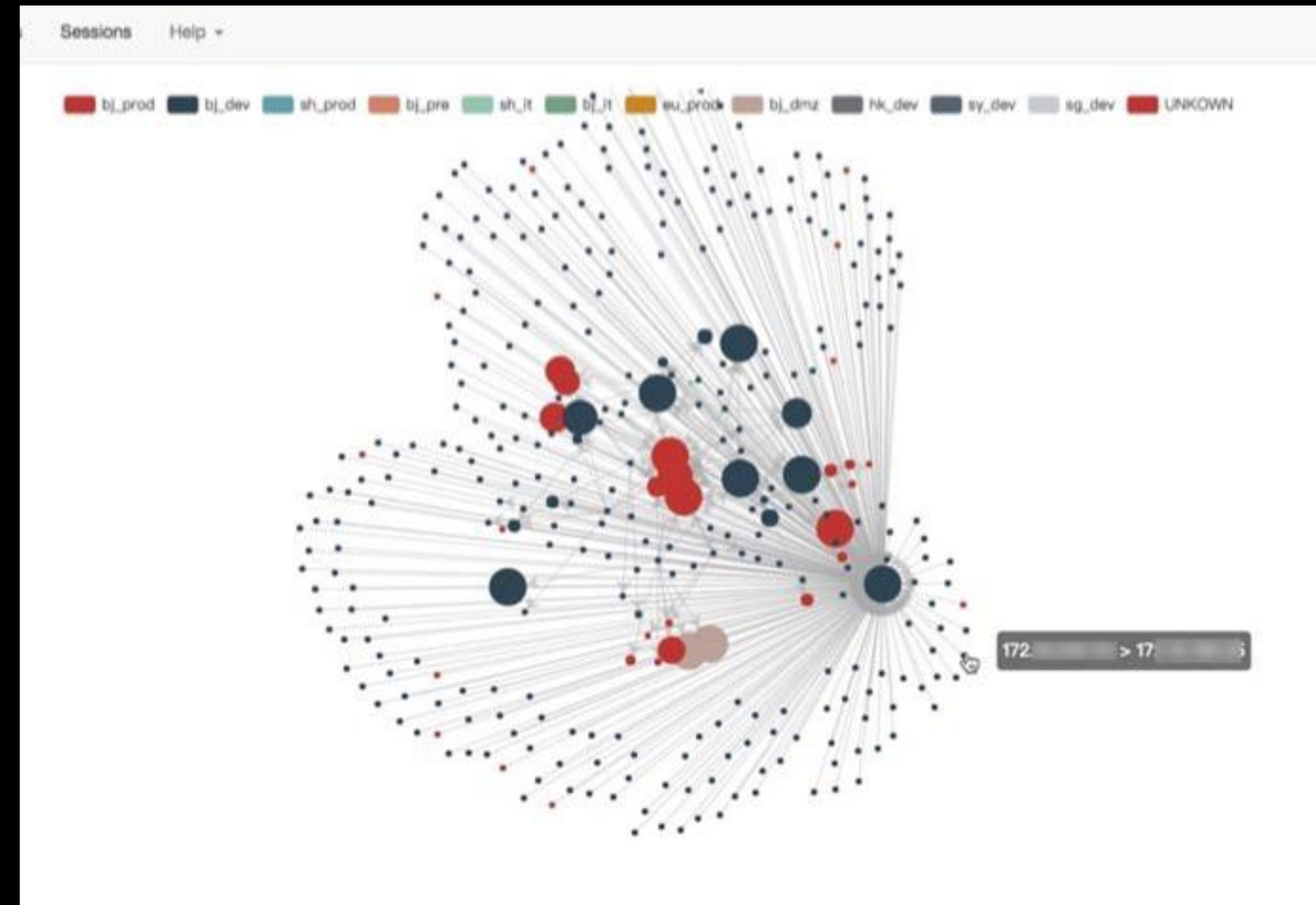
+

-

[+ 增加一组](#)

时间范围: 7天内

应用实践：网络会话日志分析



应用实践：换一种姿势检测“挖矿”行为

搜索重置保存搜索逻辑 | 已保存的搜索

默认事件 | 标记为误报 | 查看

共 45 条记录, 2018-03-02 20:34:00 至 2018-03-03 20:34:00

导出结果

共有45条, 每页显示: 100条 条<1>>

缺省	时间	来源	内容
<input checked="" type="checkbox"/> 时间 <input type="checkbox"/> src_ip <input type="checkbox"/> src_port	2018-03-03 18:44:32	DNS日志	<div>__topic__: additional: additional_num: answer: answer_num: authority: authority_num: client_subnet: dst_ip: 1[REDACTED] dst_port: 53 in_out: in qid: 53716 qname: pool.xxxxxmr.com qtype: A rcode: region: 3 src_ip: 1[REDACTED] src_port: 56778</div>

应用实践：借助 WAF 实现虚拟补丁

公司最后一名 PHP 工程师离职，

“0day”来了……

应用实践：借助 WAF 实现虚拟补丁

精准访问控制

CC攻击自定义规则

数据风控

网站防篡改

防信息泄漏

域名: bbs.example.com 返回

注意：当前每一条规则中最多允许三个条件组合，并且条件之间是"与"的逻辑关系（即必须三个条件同时满足才算匹配中规则）。匹配中规则后的动作有三种：阻断、放行（可选择后续是否继续进行Web攻击拦截或CC攻击）、告警（只记录不阻断）。规则之间是有先后匹配顺序的，可点击规则排序达到最优的防护效果。

精准访问控制

您还可以添加 99 条 新增规则 规则排序

规则名称	规则条件	动作	后续安全策略	操作
Web漏洞虚拟补丁	请求URL 包含 plugin.php	阻断		编辑 删除
	请求Params 包含 H_gate=vendor			
默认规则	所有未命中以上规则的请求	放行	Web通用防护 <input checked="" type="checkbox"/> CC防护 <input checked="" type="checkbox"/> 地区封禁 <input checked="" type="checkbox"/> 数据风控 <input checked="" type="checkbox"/>	编辑

共有2条， 每页显示：10条

http://bbs.example.com/plugin.php?H_gate=vendor

405

很抱歉，由于您访问的URL有可能对网站造成安全威胁，您的访问被拒绝。

访问者

存在攻击行为

应用防火墙

4) 运营好云上安全产品:

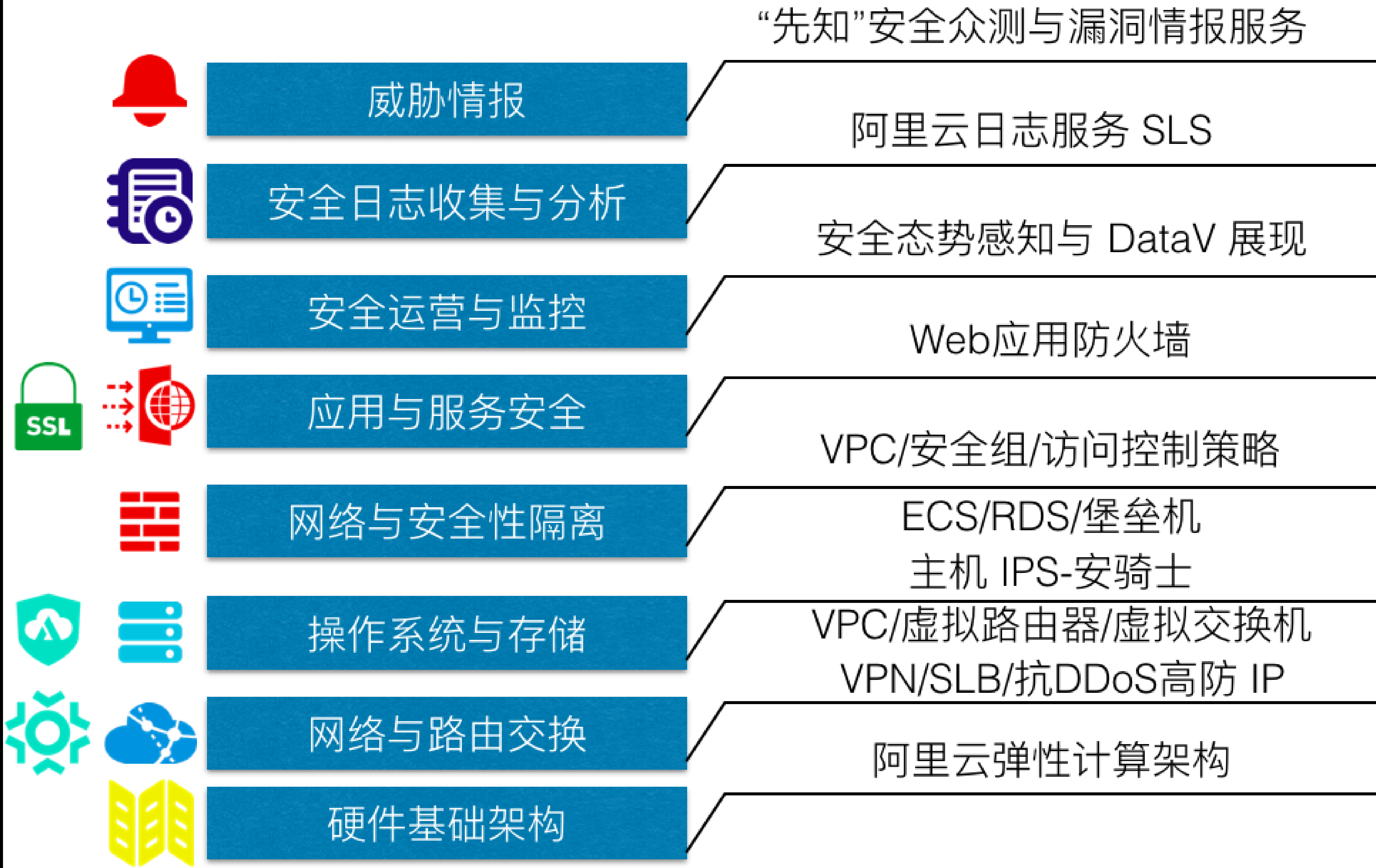
自己动手，弥补平台产品的不足

外网开放端口监测

Github 敏感信息监控

Gitlab 访问行为审计

云上企业网络安全架构（基于阿里云）



基于 RAM 的阿里云权限管理架构

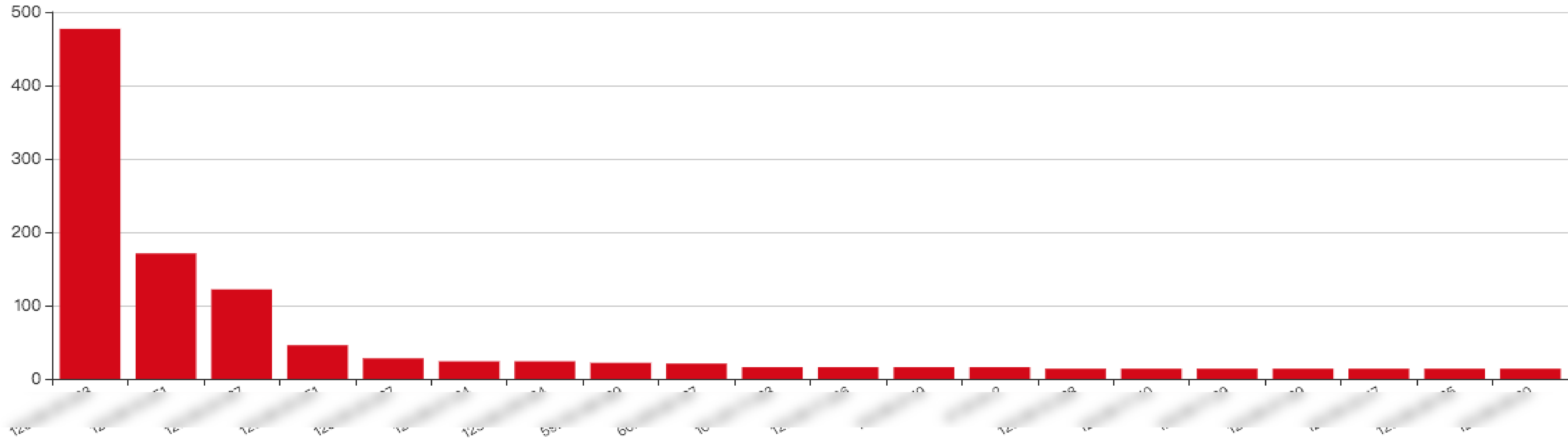
安全日志与审计

深度挖掘安全日志

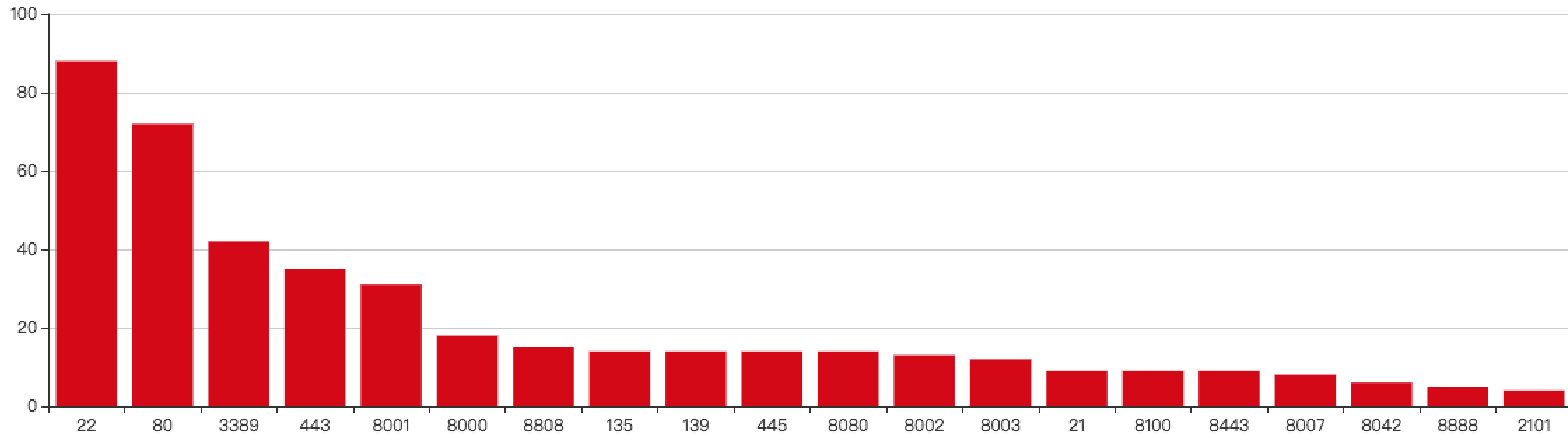
长期积累历史数据

反向推动架构演进

基于IP的端口开放统计



外网端口开放统计



安全概览

阿里云

端口监控

Github

内网安全

Gitlab日志

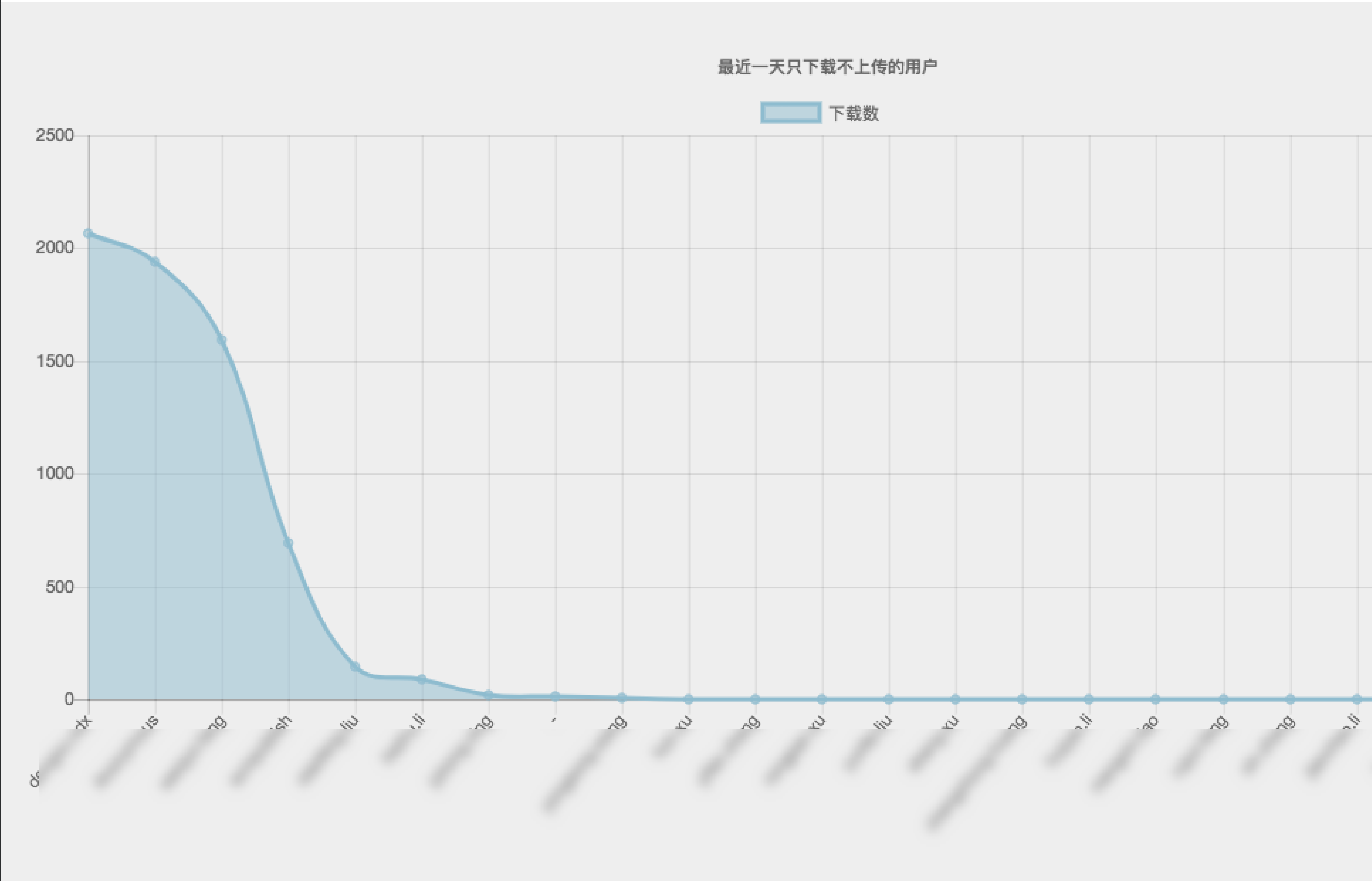
报表

查询

异常连接

规则中心

告警中心



安全告警

内部

PortScanner

机器人

Github 高危员工: [redacted],更新了仓库, 请关注,url: [https://github.com/users\[redacted\]:created_commits?from=2018-04-27&to=2018-04-27](https://github.com/users/[redacted]:created_commits?from=2018-04-27&to=2018-04-27)

4月27日 12:30

PortScanner

机器人

Github 高危员工: [redacted] 更新了仓库, 请关注,url: [https://github.com/users\[redacted\]:created_commits?from=2018-04-27&to=2018-04-27](https://github.com/users[redacted]:created_commits?from=2018-04-27&to=2018-04-27)

4月28日 18:43

PortScanner

机器人

4月28日 18:43

Found new open port: [http://4\[redacted\]:5:443](http://4[redacted]:5:443) / tcp|http|nginx 1.13.7|cn-[redacted]

Found new open port: [http://4\[redacted\]:5:80](http://4[redacted]:5:80) / tcp|http|nginx 1.13.7|cn-[redacted]

5) 构建良好的问题沟通机制:

云上安全的运营也是
企业与云平台共同协作关系的运营

5) 构建良好的问题沟通机制：

- 关注平台技术演进和发展方向
- 与云平台建立良好的沟通机制
 - 合作交流群
 - 聆听平台
 - ACE 活动
 - MVP 渠道
 - 云栖社区

已提交

预审通过

已采纳

【功能建议】通过钉钉机器人接口发送阿里云重要通知

钉钉告警短信消息通知

傅奎

MVP

发布于：2017-11-06 09:45:47

【问题描述】：

阿里云后台的各类消息通知，目前只能通过邮件和短信方式推送给用户，不支持更更高效的

半夜了，公司被 DDoS 攻击，阿里云发来一条短信/邮件，完全无感知。如果通过钉钉机器人，

【建议方案】：

建议，后台增加钉钉机器人接口的方式进行推送，几个好处：

1、钉钉是即时通工具，可以在群里快速通知，特别是重大系统故障、严重网络攻击行为等

2、有利于钉钉产品的推广

3、弥补微信之外即时通讯工具的空白

4、节约短信费用，解决发送账户的限制

编辑

阿里云社区

仙游 管理员 2018-01-18 10:26:04

感谢您的反馈，您的建议产品团队已经优化上线解决，请您登录产品关联平台进行验证，若使用中还存在其它建议与体验，可在此平台进行反馈，我们收到后会尽快处理。

回复

管理员将 状态 修改为 已实现 2018-01-18 10:26:01

获得了 50 积分奖励 2018-01-16 13:58:12

方淼 管理员 2018-01-16 13:58:00

您好，钉钉机器人的功能我们已经在开发中，开发周期比较长，目前安全消息已经支持语音通知，您可以进入消息中心-语音通知中进行设置

回复

管理员将 状态 修改为 已采纳 2017-11-13 12:27:02

辛苑 管理员 2017-11-06 13:51:48

非常感谢您的反馈，您的建议我们已经收到，并已提交至关联产品团队进行评估，产品经理会在10个工作日内完成对建议是否采纳的评估并给您答复，请您持续关注聆听平台，了解建议进一步处理结果，感谢您的建议！

回复

管理员将 状态 修改为 预审通过 2017-11-06 13:51:43

总结：云上安全成功运营的关键：

深入理解
平台架构

灵活运用
平台产品

持续运营
不断进步

关键时刻还得靠平台……

最后：一些感悟和观点

观点：

■ 没有百分之百的云

■ 太阳耀斑爆发影响GPS定位

■ 俄罗斯“福布斯”号飞船在太平洋坠毁

■ 日本“希望”号太空舱发射失败

■ 俄罗斯“福布斯”号飞船在太平洋坠毁

■ 俄罗斯“福布斯”号飞船在太平洋坠毁

观点：

■ 没有百分之百的云

■ 上云就是自废武功

■ 云计算是IT技术大跃进

■ 云计算是IT技术革命

■ 云计算是IT技术革命

■ 云计算是IT技术革命

观点：

- 没有百分之百的云
- 上云就是自废武功
- 云厂商自己要先上云
- 云厂商要成为基础设施
- 云厂商要成为应用
- 云厂商要成为生态

观点：

- 没有百分之百的云
- 上云就是自废武功
- 云厂商自己要先上云
- 与平台共同进步
- 云厂商要成为平台
- 云厂商要上云

观点：

■ 没有百分之百的云

■ 上云就是自废武功

■ 云厂商自己要先上云

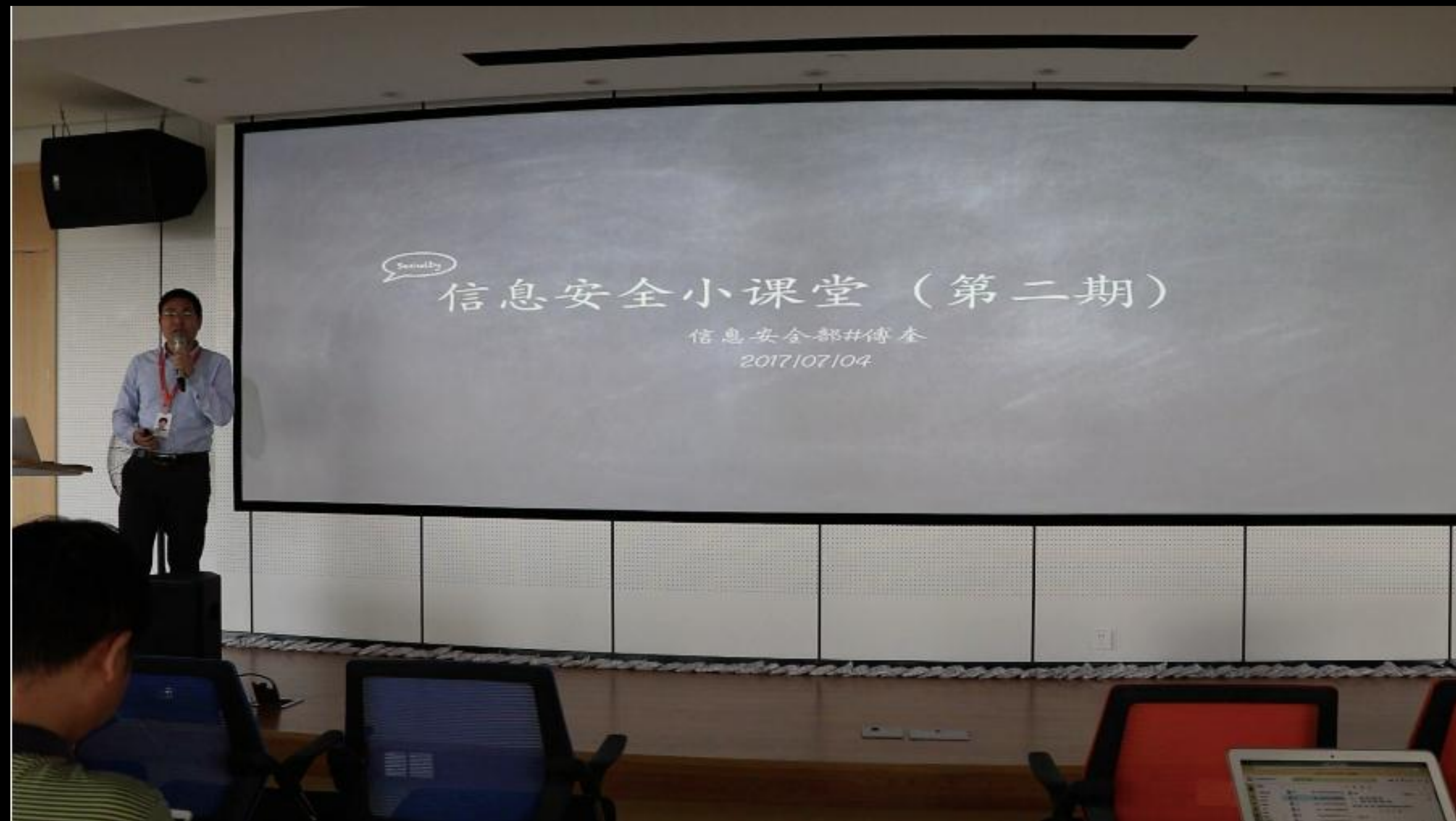
■ 与平台共同进步

■ 安全厂商正被挑战

■ 网络安全上云

观点：

- 没有百分之百的云
- 上云就是自废武功
- 云厂商自己要先上云
- 与平台共同进步
- 安全厂商正被挑战
- 死都死在密码上



专项安全开发培训



距离卓越开发者还有最后一公里



信息安全部



定目标

组团队

识边界

扎篱笆

上规范

走流程

多监控

少干预

收日志

！做审计

出数据

！做反馈

斗产品

练开发

调测试

撩运维

靠平台

入联盟

摸石头

勤复盘

云计算

更安全

上云就上阿里云

共同捍卫企业云安全

谢谢！

