# 基于数据中心的私有安全云

王刚

网神信息技术（北京）股份有限公司 副总裁

2014-09

# 新环境、老问题

- 病毒、木马、各种恶意软件
- 非授权访问、黑客攻击
- 系统、应用程序漏洞

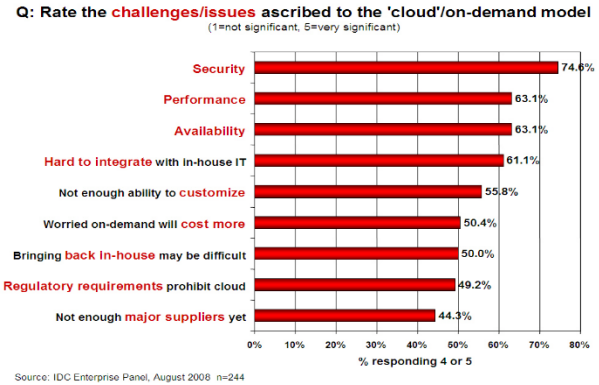
# 新环境、新问题

- 虚拟化、资源共享、动态分配
- 数据大集中、多租户
- 环境复杂、边界模糊
- 新的攻击手段、未知的威胁

# 云数据中心安全现状

理想，
很重视

现实，
很无奈




- 没有方案
- 仅在边界部署
- 有设备，无效果

# 云的问题云来解决

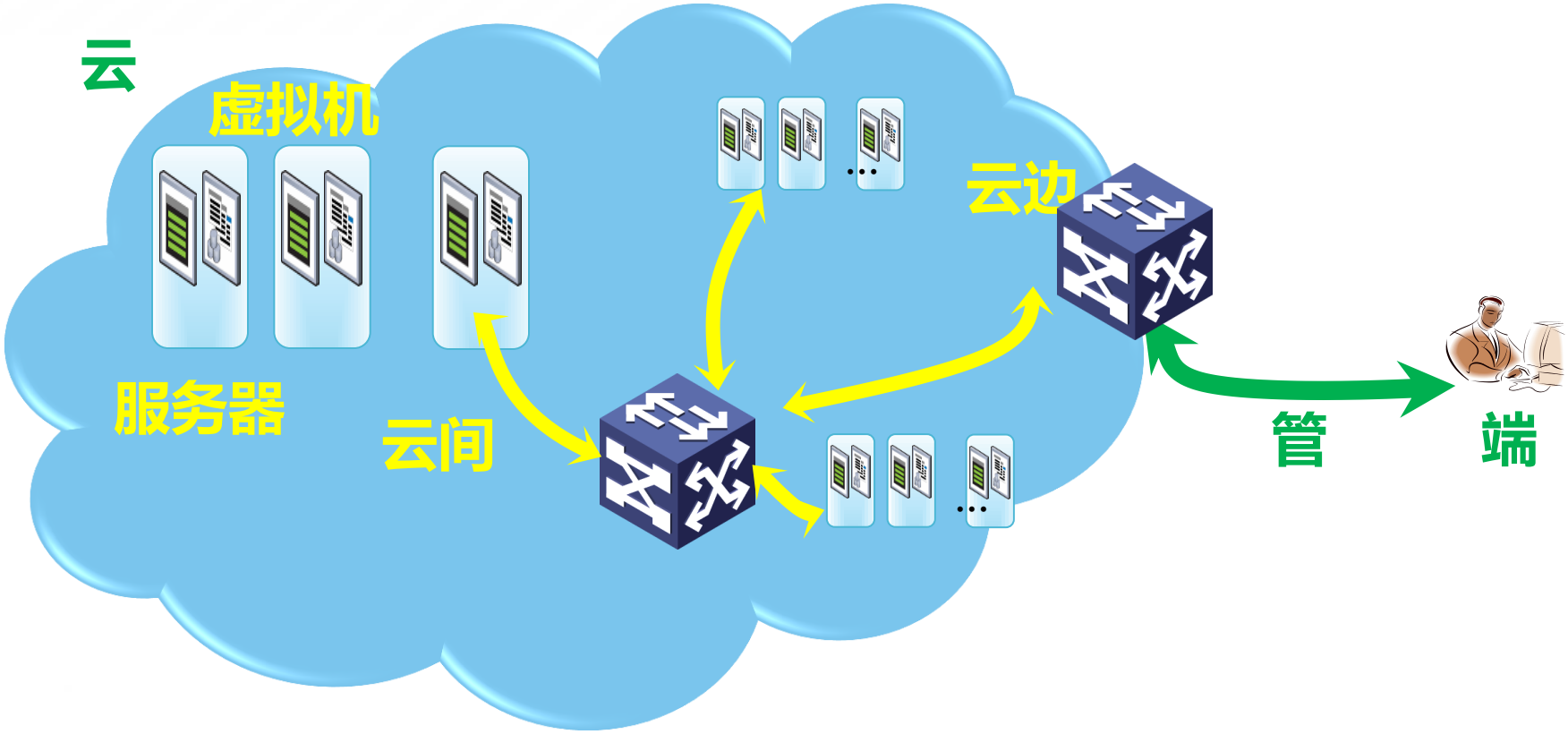
# 云的问题云来解决



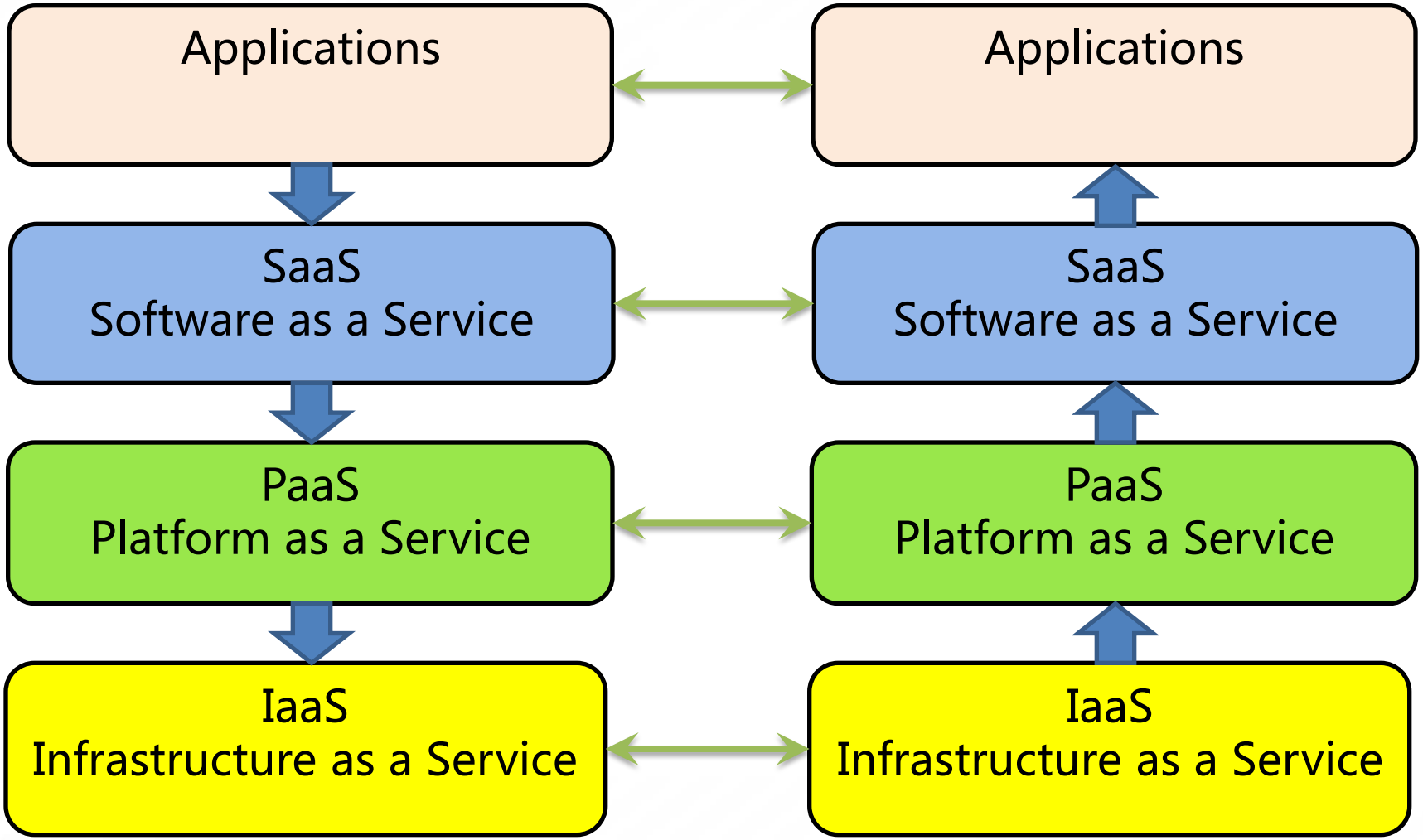
- 需求不一致
- 对数据的担忧
- 对服务的需求

- 包含行业云
- 优点：高度可控
- 缺点：与世隔绝

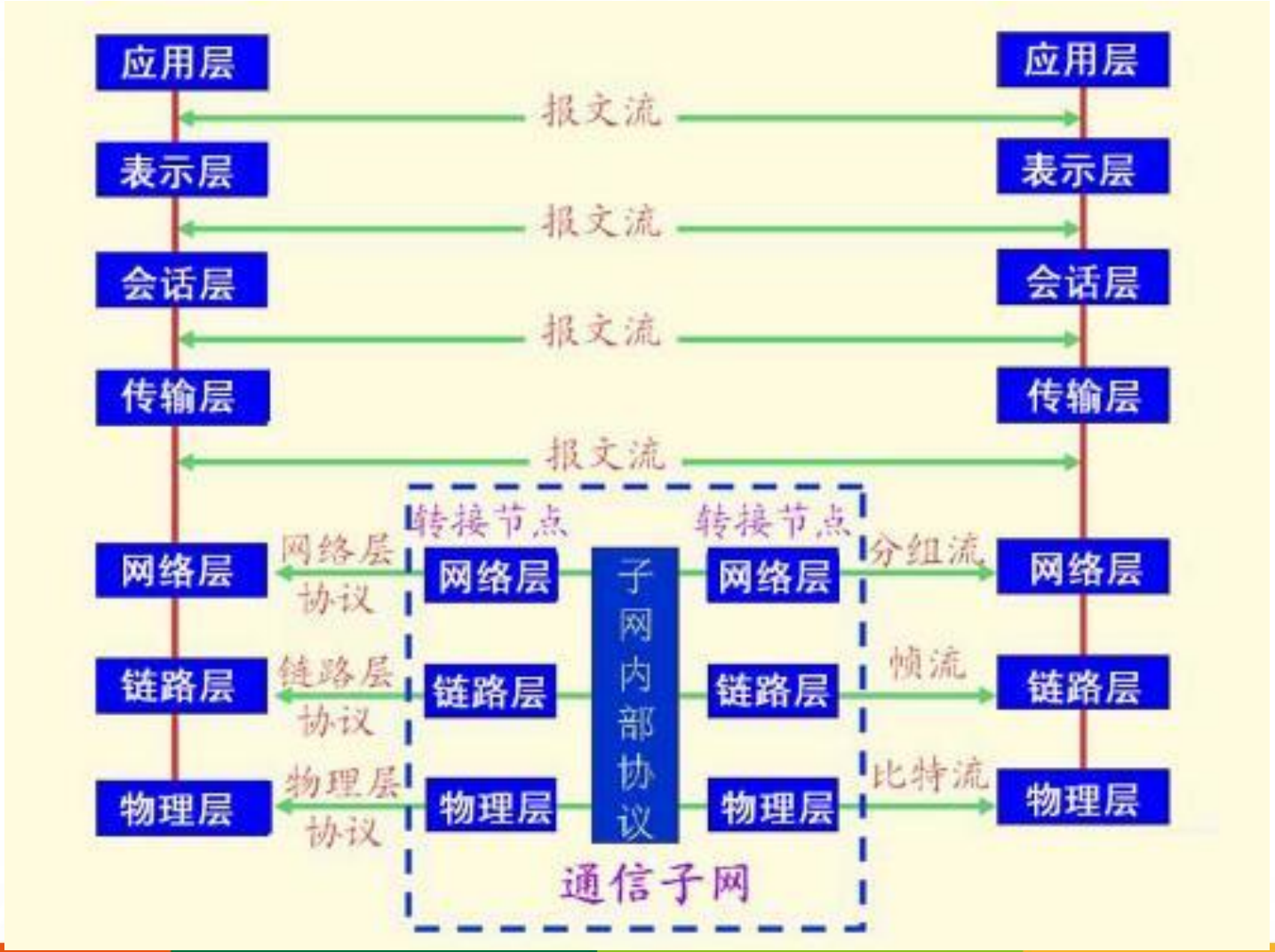
# 从三个维度来看云：物理维度



# 从三个维度来看云：逻辑维度



# 从三个维度来看云：逻辑维度



# 从三个维度来看云：攻击者视角

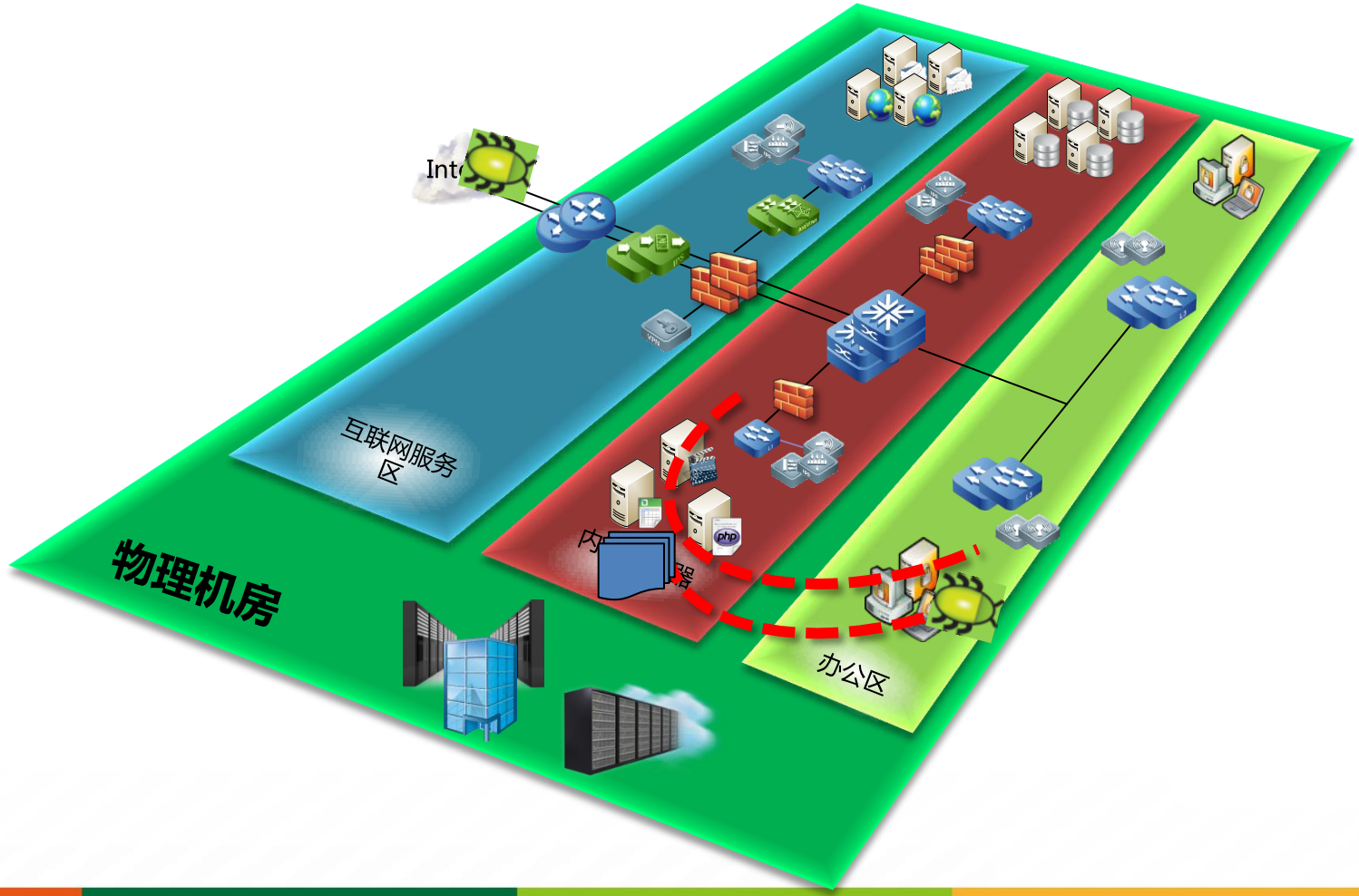
感知网络

发现漏洞

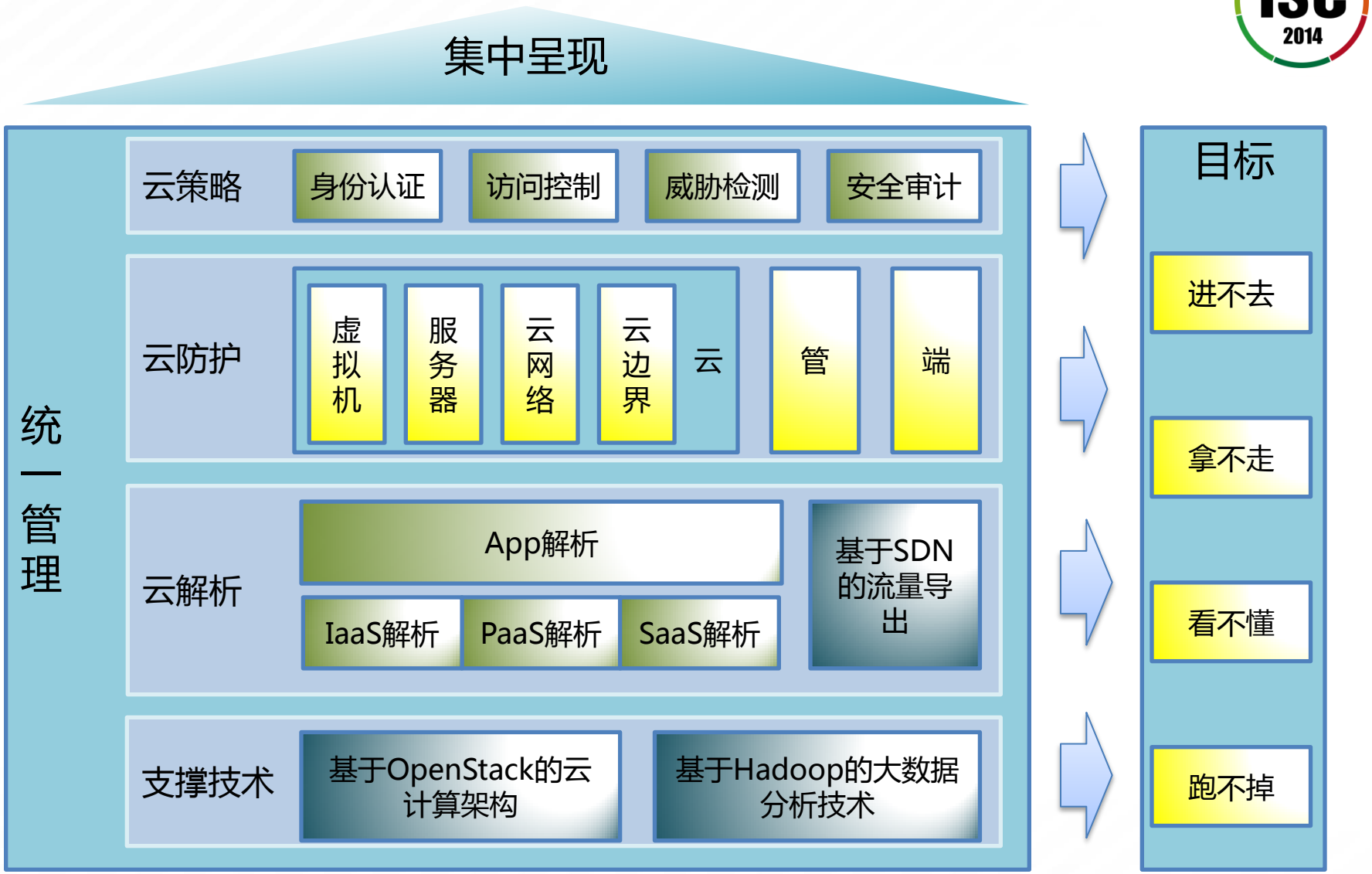
利用漏洞

发动攻击

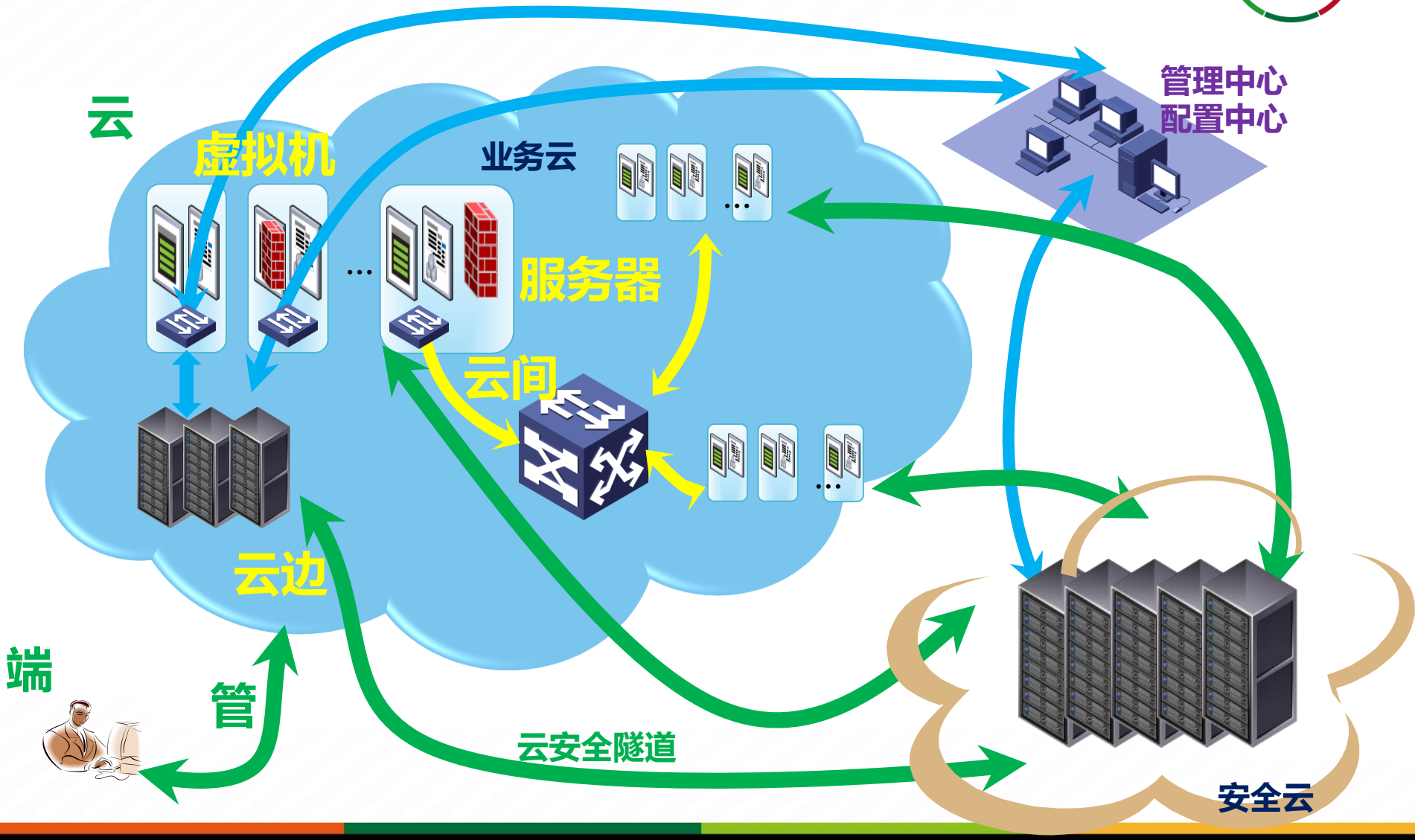
窃取数据



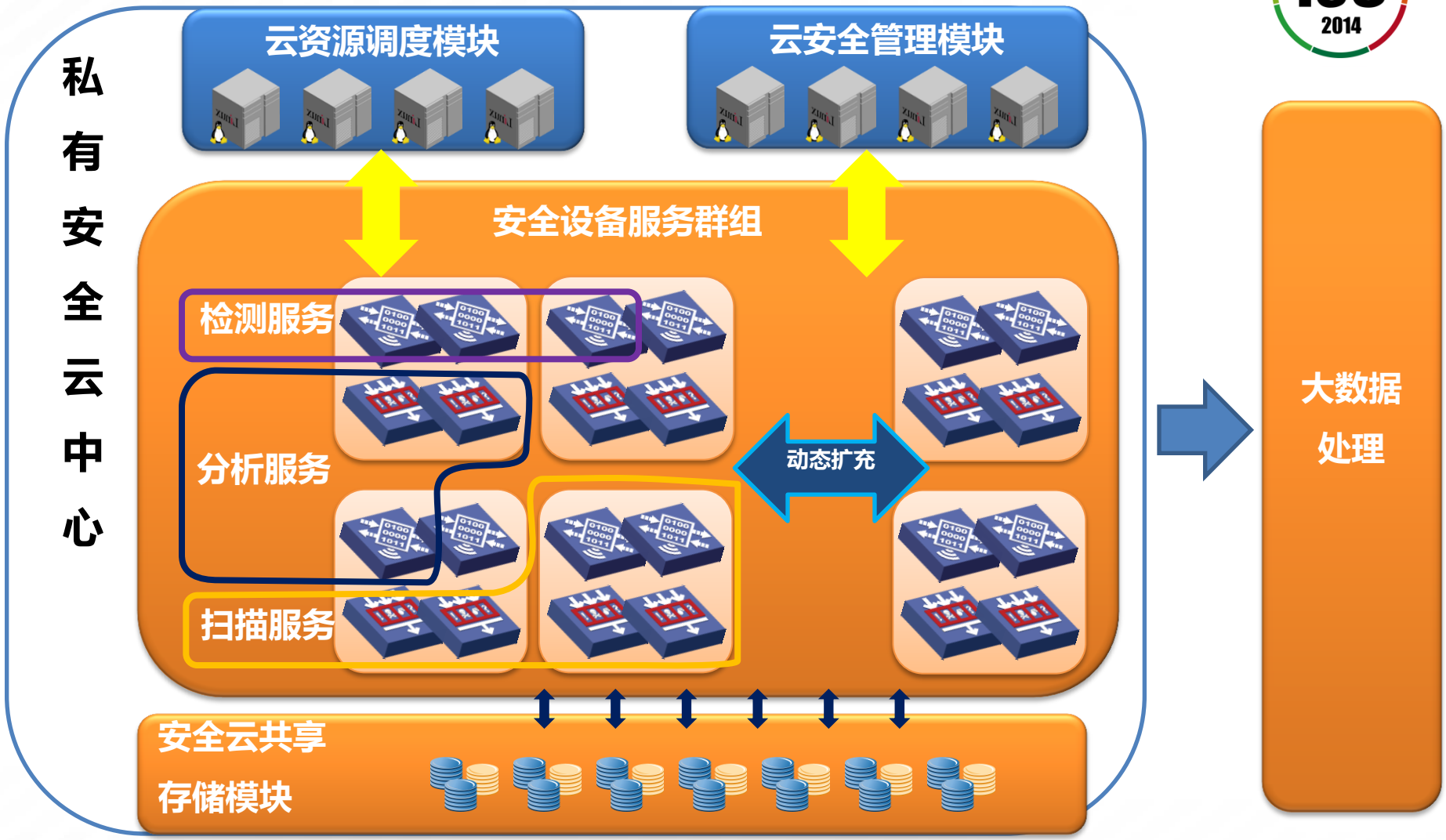
# 私有安全云防护体系


集中呈现
统一管理
云策略
身份认证
访问控制
威胁检测
安全审计
云防护
虚拟机
服务器
云网络
云边界
云
管
端
云解析
App解析
IaaS解析
PaaS解析
SaaS解析
基于SDN的流量导出
支撑技术
基于OpenStack的云计算架构
基于Hadoop的大数据分析技术
目标
进不去
拿不走
看不懂
跑不掉

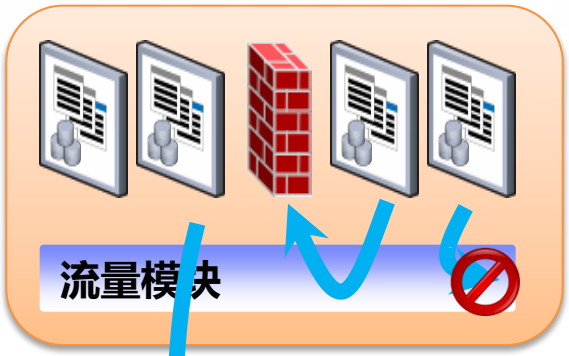
# 云防护体系：云计算架构

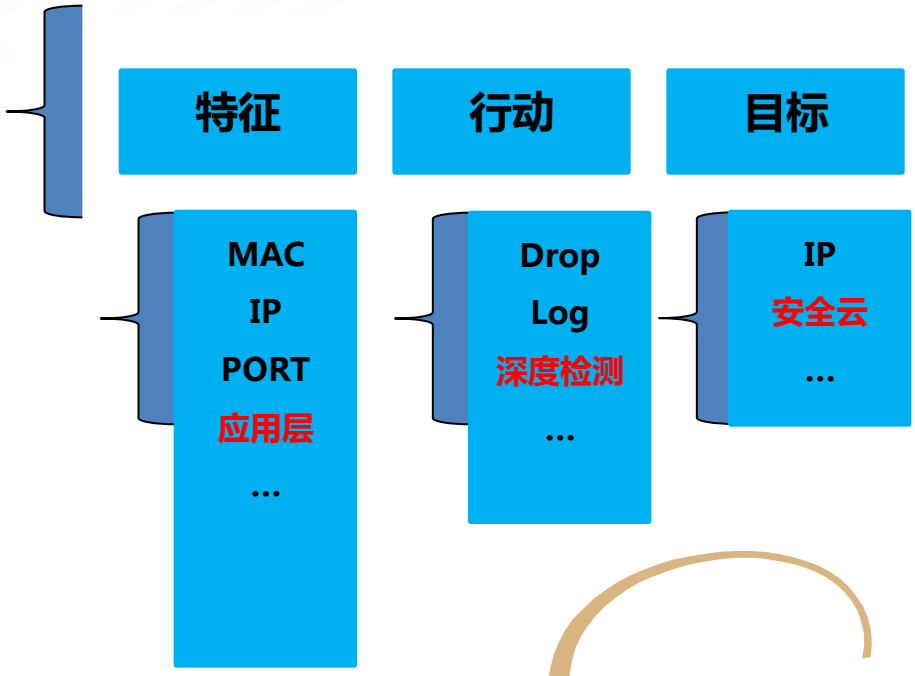


# 云防护体系：云计算架构

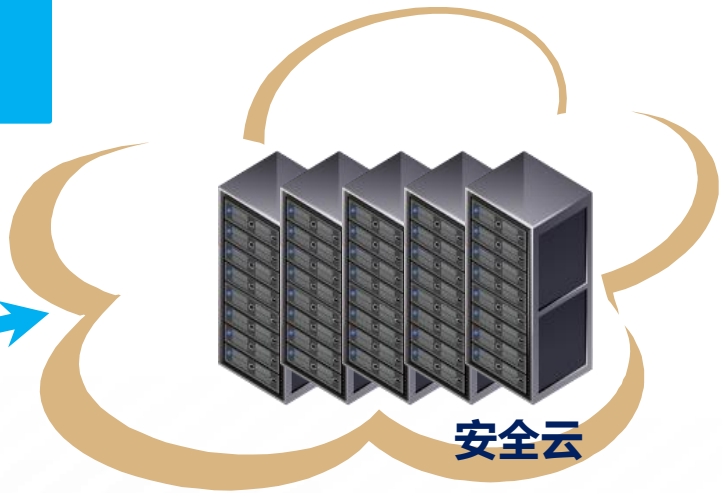

私有安全云中心
云资源调度模块
云安全管理模块
安全设备服务群组
检测服务
分析服务
扫描服务
动态扩充
安全云共享
存储模块
大数据
处理

# 云防护体系：流量导出

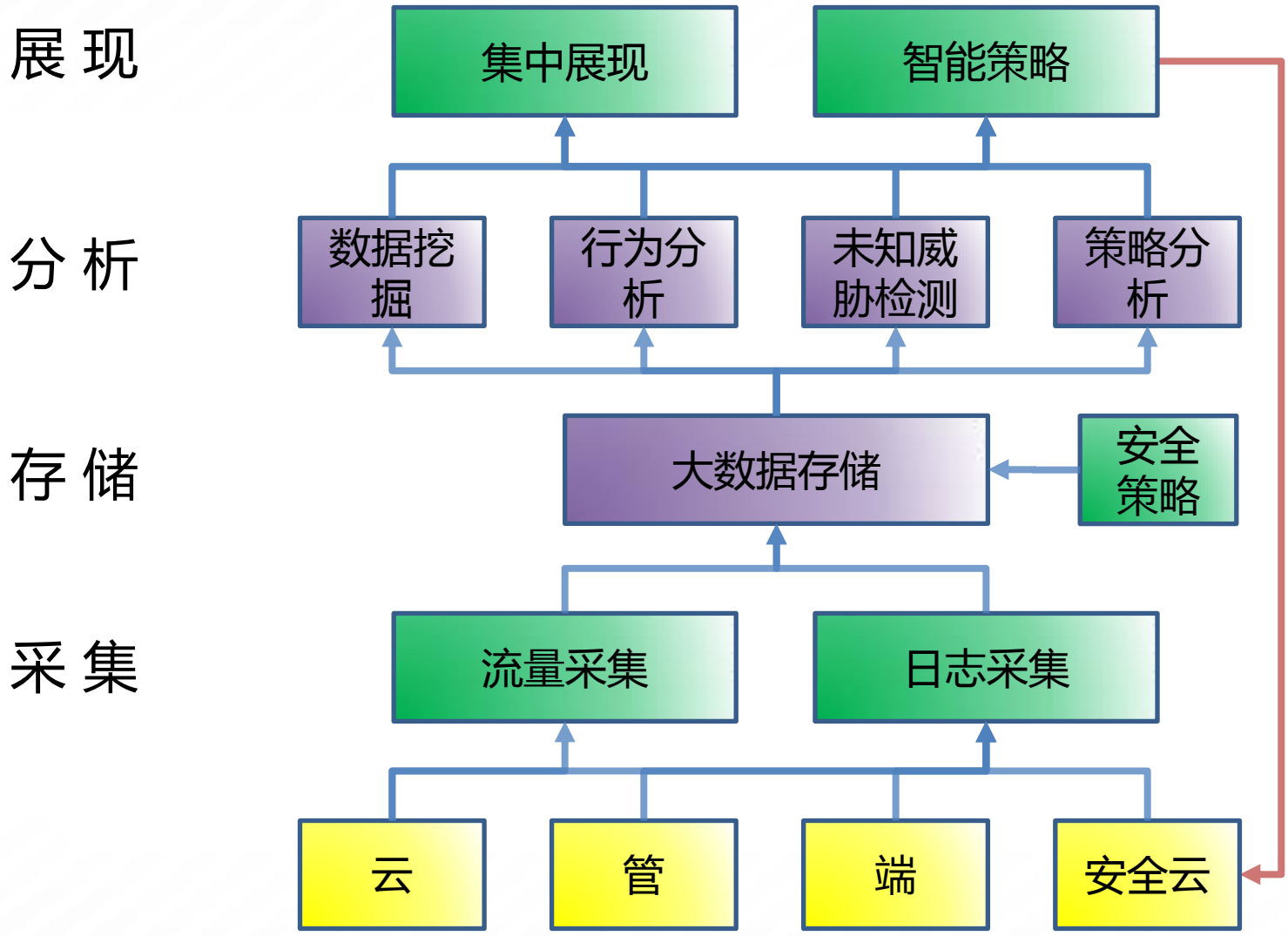


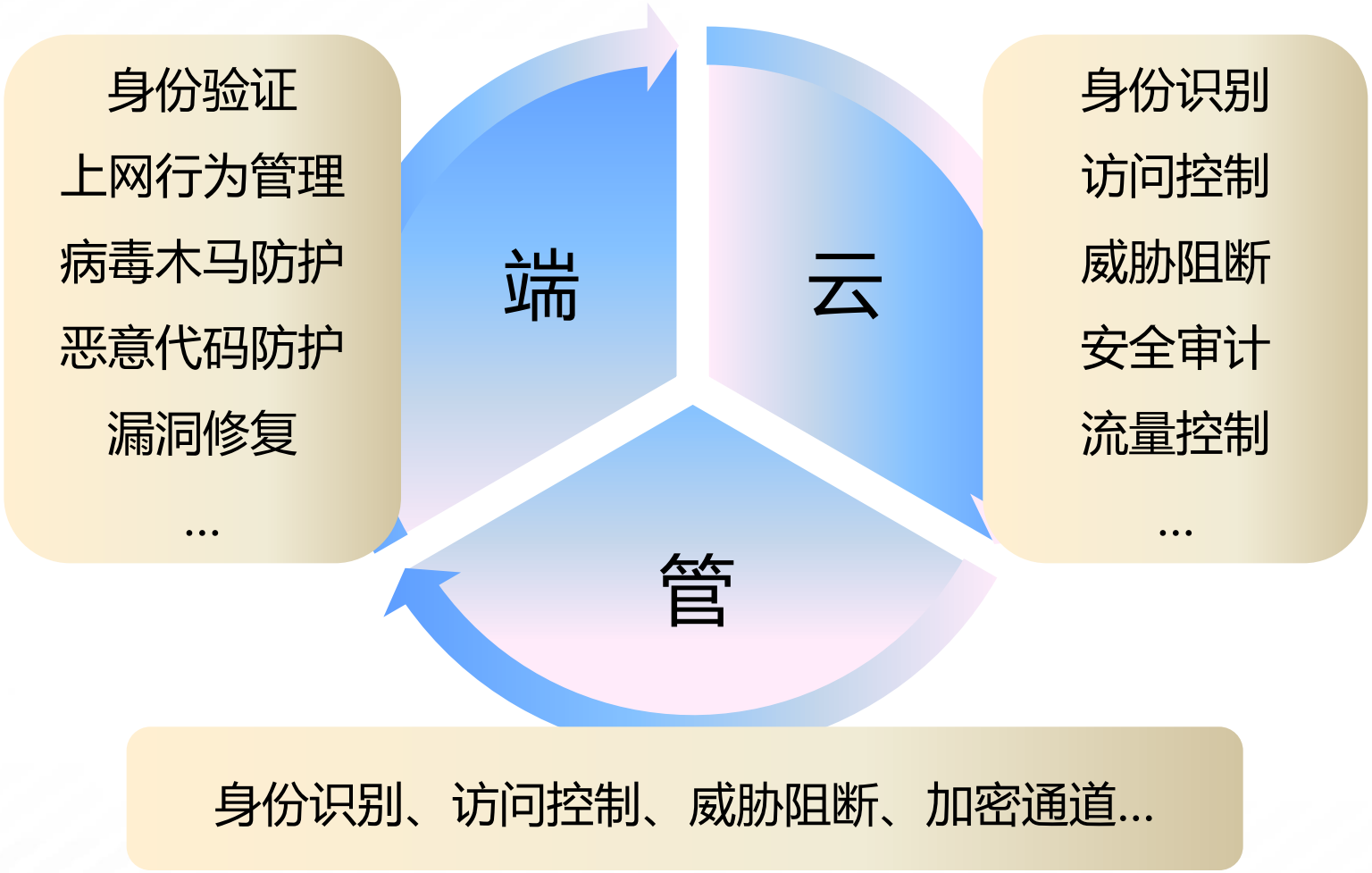

- 云端
  - 云检测
  - 云查杀
  - 云监控
  - 云审计
  - …



# 云防护体系：大数据架构


展 现
分 析
存 储
采 集
集中展现
智能策略
数据挖掘
行为分析
未知威胁检测
策略分析
大数据存储
安全策略
流量采集
日志采集
云
管
端
安全云

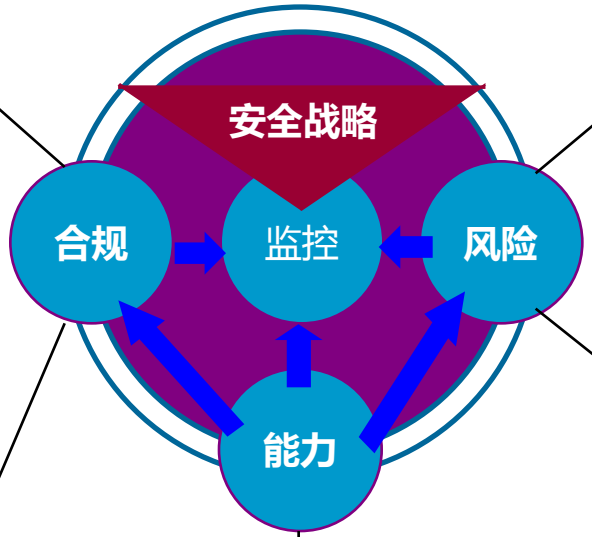
# 云防护体系：云策略


身份验证
上网行为管理
病毒木马防护
恶意代码防护
漏洞修复
...
端
云
管
身份识别
访问控制
威胁阻断
安全审计
流量控制
...
身份识别、访问控制、威胁阻断、加密通道...

# 云防护体系：统一管理

**信息安全战略**
- 安全保障业务
- 安全战略和政策

**安全风险管理**
- 安全对象
- 威胁&事件
- 脆弱性&预警
- 安全风险分析

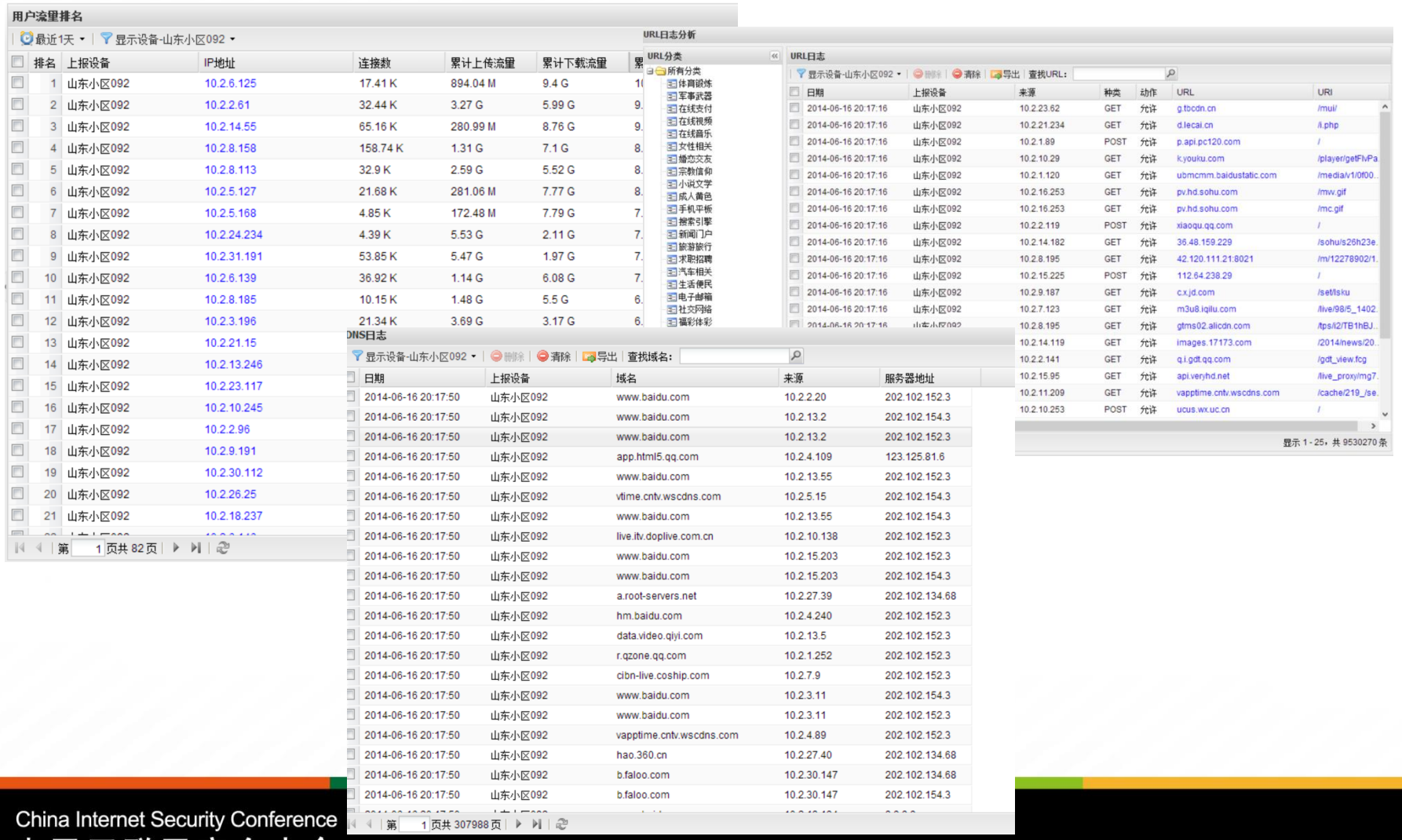



**安全合规管理**
- 国家政策要求
- 行业政策要求

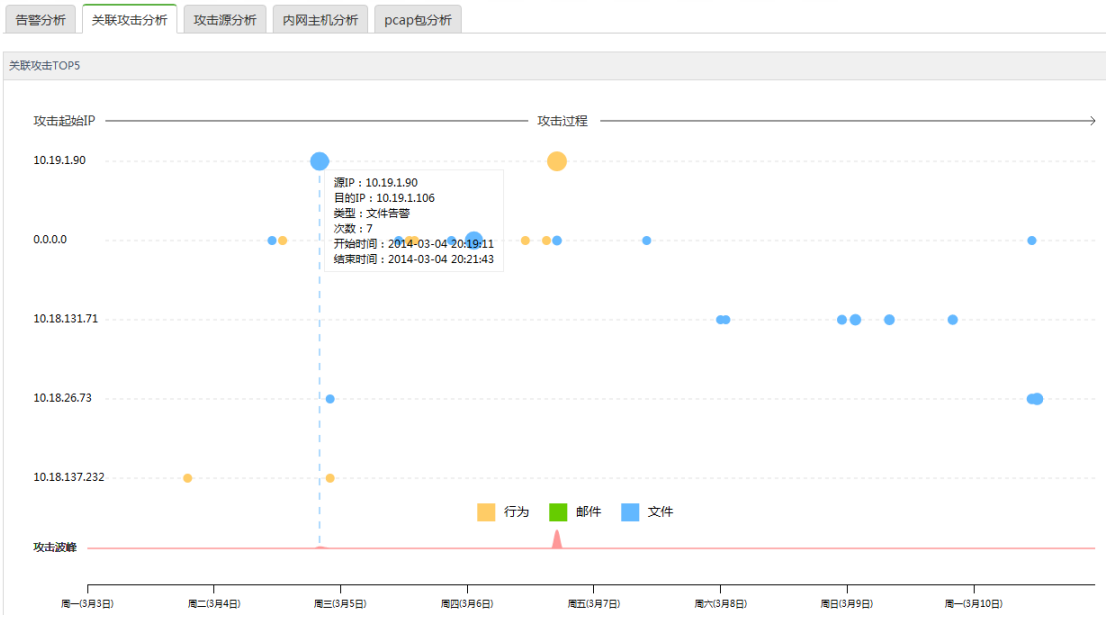
**安全运维监控**
- 数据访问和外传监控
- 数据完整性监控
- 网站安全性监控
- 防护体系有效性监控
- 安全事件关联分析
- 安全告警
- 安全应急响应
- 安全审计
- APT攻击检测分析

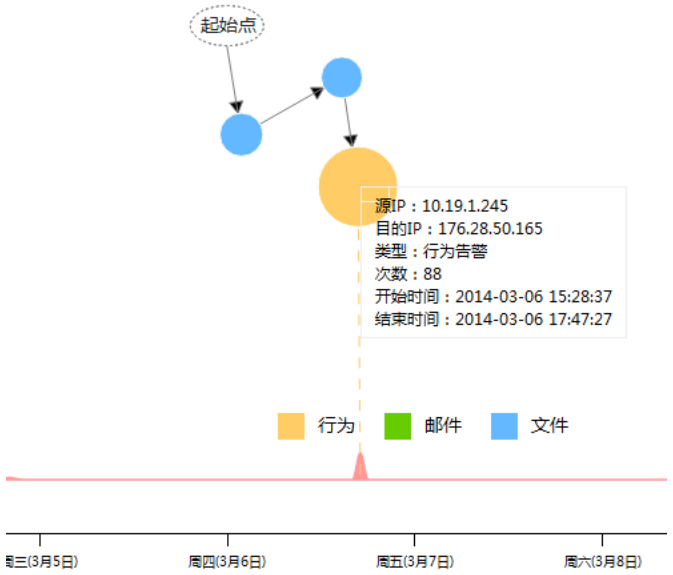
**安全能力管理**
- 安全组织、岗位责任
- 安全意识&培训
- 安全知识库

# 云防护体系：统一呈现


用户流量排名
最近1天
显示设备-山东小区092
排名 上报设备 IP地址 连接数 累计上传流量 累计下载流量
1 山东小区092 10.2.6.125 17.41 K 894.04 M 9.4 G
2 山东小区092 10.2.2.61 32.44 K 3.27 G 5.99 G
3 山东小区092 10.2.14.55 65.16 K 280.99 M 8.76 G
4 山东小区092 10.2.8.158 158.74 K 1.31 G 7.1 G
5 山东小区092 10.2.8.113 32.9 K 2.59 G 5.52 G
6 山东小区092 10.2.5.127 21.68 K 281.06 M 7.77 G
7 山东小区092 10.2.5.168 4.85 K 172.48 M 7.79 G
8 山东小区092 10.2.24.234 4.39 K 5.53 G 2.11 G
9 山东小区092 10.2.31.191 53.85 K 5.47 G 1.97 G
10 山东小区092 10.2.6.139 36.92 K 1.14 G 6.08 G
11 山东小区092 10.2.8.185 10.15 K 1.48 G 5.5 G
12 山东小区092 10.2.3.196 21.34 K 3.69 G 3.17 G
13 山东小区092 10.2.21.15
14 山东小区092 10.2.13.246
15 山东小区092 10.2.23.117
16 山东小区092 10.2.10.245
17 山东小区092 10.2.2.96
18 山东小区092 10.2.9.191
19 山东小区092 10.2.30.112
20 山东小区092 10.2.26.25
21 山东小区092 10.2.18.237
第 1 页共 82 页
URL日志分析
URL分类
所有分类
体育锻炼
军事武器
在线支付
在线视频
在线音乐
女性相关
婚恋交友
宗教信仰
小说文学
成人黄色
手机平板
搜索引擎
新闻门户
旅游旅行
求职招聘
汽车相关
生活便民
电子邮箱
社交网络
福彩炸彩
URL日志
显示设备-山东小区092
删除
清除
导出
查找URL:
日期 上报设备 来源 种类 动作 URL URI
2014-06-16 20:17:16 山东小区092 10.2.23.62 GET 允许 g.tbcdn.cn /mui/
2014-06-16 20:17:16 山东小区092 10.2.21.234 GET 允许 d.lecai.cn /i.php
2014-06-16 20:17:16 山东小区092 10.2.1.89 POST 允许 p.api.pc120.com /
2014-06-16 20:17:16 山东小区092 10.2.10.29 GET 允许 k.youku.com /player/getFlvPa
2014-06-16 20:17:16 山东小区092 10.2.1.120 GET 允许 ubmcmm.baidustatic.com /media/v1/0f00
2014-06-16 20:17:16 山东小区092 10.2.16.253 GET 允许 pv.hd.sohu.com /mv.gif
2014-06-16 20:17:16 山东小区092 10.2.16.253 GET 允许 pv.hd.sohu.com /mc.gif
2014-06-16 20:17:16 山东小区092 10.2.2.119 POST 允许 xiaoqu.qq.com /
2014-06-16 20:17:16 山东小区092 10.2.14.182 GET 允许 36.48.159.229 /sohu/s26h23e
2014-06-16 20:17:16 山东小区092 10.2.8.195 GET 允许 42.120.111.21:8021 /m/12278902/1
2014-06-16 20:17:16 山东小区092 10.2.15.225 POST 允许 112.64.238.29 /
2014-06-16 20:17:16 山东小区092 10.2.9.187 GET 允许 c.x.jd.com /set/isku
2014-06-16 20:17:16 山东小区092 10.2.7.123 GET 允许 m3u8.iqilu.com /live/98/5_1402
2014-06-16 20:17:16 山东小区092 10.2.8.195 GET 允许 gtms02.alicdn.com /tps/i2/TB1hBJ
10.2.14.119 GET 允许 images.17173.com /2014/news/20
10.2.2.141 GET 允许 q.i.gdt.qq.com /gdt_view.fcg
10.2.15.95 GET 允许 api.veryhd.net /live_proxy/mg7
10.2.11.209 GET 允许 vapptime.cntv.wscdns.com /cache/219_/se
10.2.10.253 POST 允许 ucus.wx.uc.cn /
显示 1 - 25，共 9530270 条
DNS日志
显示设备-山东小区092
删除
清除
导出
查找域名:
日期 上报设备 域名 来源 服务器地址
2014-06-16 20:17:50 山东小区092 www.baidu.com 10.2.2.20 202.102.152.3
2014-06-16 20:17:50 山东小区092 www.baidu.com 10.2.13.2 202.102.154.3
2014-06-16 20:17:50 山东小区092 www.baidu.com 10.2.13.2 202.102.152.3
2014-06-16 20:17:50 山东小区092 app.html5.qq.com 10.2.4.109 123.125.81.6
2014-06-16 20:17:50 山东小区092 www.baidu.com 10.2.13.55 202.102.152.3
2014-06-16 20:17:50 山东小区092 vtime.cntv.wscdns.com 10.2.5.15 202.102.154.3
2014-06-16 20:17:50 山东小区092 www.baidu.com 10.2.13.55 202.102.154.3
2014-06-16 20:17:50 山东小区092 live.itv.doplive.com.cn 10.2.10.138 202.102.152.3
2014-06-16 20:17:50 山东小区092 www.baidu.com 10.2.15.203 202.102.152.3
2014-06-16 20:17:50 山东小区092 www.baidu.com 10.2.15.203 202.102.154.3
2014-06-16 20:17:50 山东小区092 a.root-servers.net 10.2.27.39 202.102.134.68
2014-06-16 20:17:50 山东小区092 hm.baidu.com 10.2.4.240 202.102.152.3
2014-06-16 20:17:50 山东小区092 data.video.qiyi.com 10.2.13.5 202.102.152.3
2014-06-16 20:17:50 山东小区092 r.qzone.qq.com 10.2.1.252 202.102.152.3
2014-06-16 20:17:50 山东小区092 cibn-live.coship.com 10.2.7.9 202.102.152.3
2014-06-16 20:17:50 山东小区092 www.baidu.com 10.2.3.11 202.102.154.3
2014-06-16 20:17:50 山东小区092 www.baidu.com 10.2.3.11 202.102.152.3
2014-06-16 20:17:50 山东小区092 vapptime.cntv.wscdns.com 10.2.4.89 202.102.152.3
2014-06-16 20:17:50 山东小区092 hao.360.cn 10.2.27.40 202.102.134.68
2014-06-16 20:17:50 山东小区092 b.faloo.com 10.2.30.147 202.102.134.68
2014-06-16 20:17:50 山东小区092 b.faloo.com 10.2.30.147 202.102.154.3
第 1 页共 307988 页

# 云防护体系：统一呈现




| 源IP | 目的IP | 攻击类型 | 最近告警时间 | 告警次数 | 操作 |
|---|---|---|---|---|---|
| 10.19.1.90 | 10.19.1.106 | 文件告警- | 2014-03-04 20:21:43 | 7 | 查看本条详情 |
| 10.19.1.106 | 10.19.1.245 | 文件告警- | 2014-03-04 21:50:17 | 3 | 查看本条详情 |
| 10.19.1.245 | 176.28.50.165 | 行为告警-nessus扫描 | 2014-03-06 17:47:27 | 88 | 查看本条详情 |

# 需进一步研究的问题

- 如何利用公有云
  - U盘、光盘
  - 内网服务器
  - …
- 安全云与云安全基础架构共享、冲突、融合
  - 服务器
  - 管理中心
  - SDN
  - …

# Thanks!