GOPS2016
Beijing

2016 全球运维大会 北京站

DevOps 2.0：重塑运维价值

会议时间：12月16日 - 12月17日

会议地点：北京国际会议中心

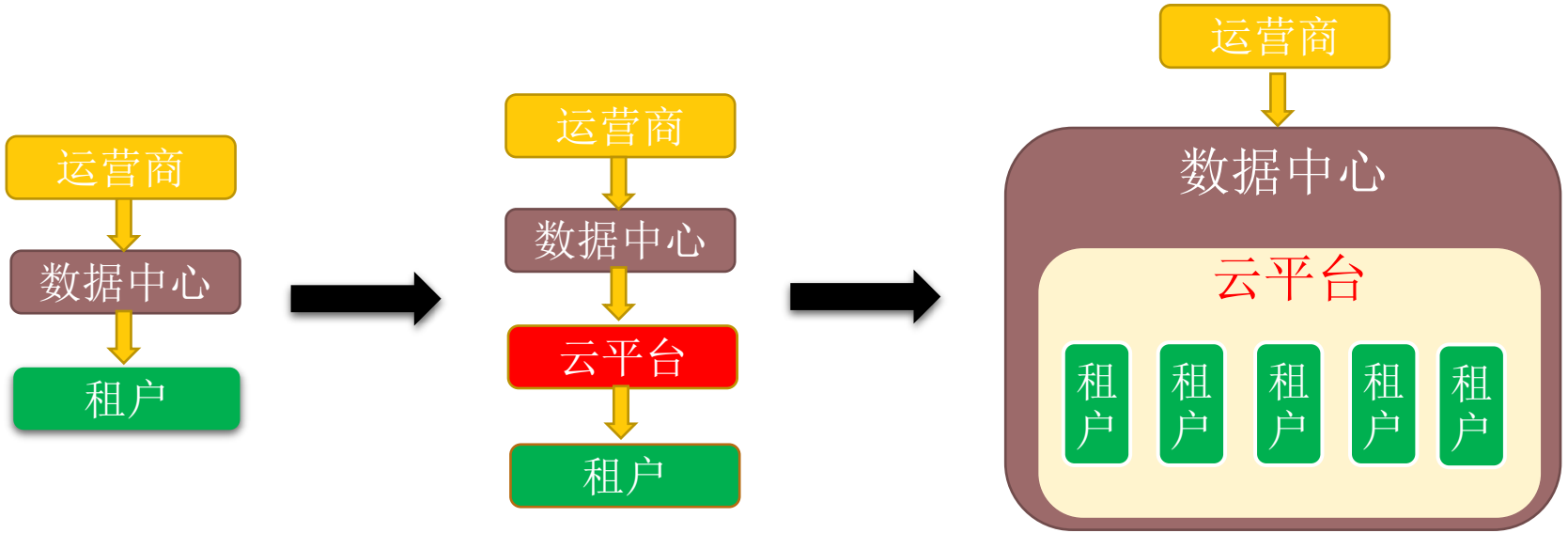
主办单位：

云网络数据分析及应用

张天鹏　CTO@云杉网络

目录

云网络差异

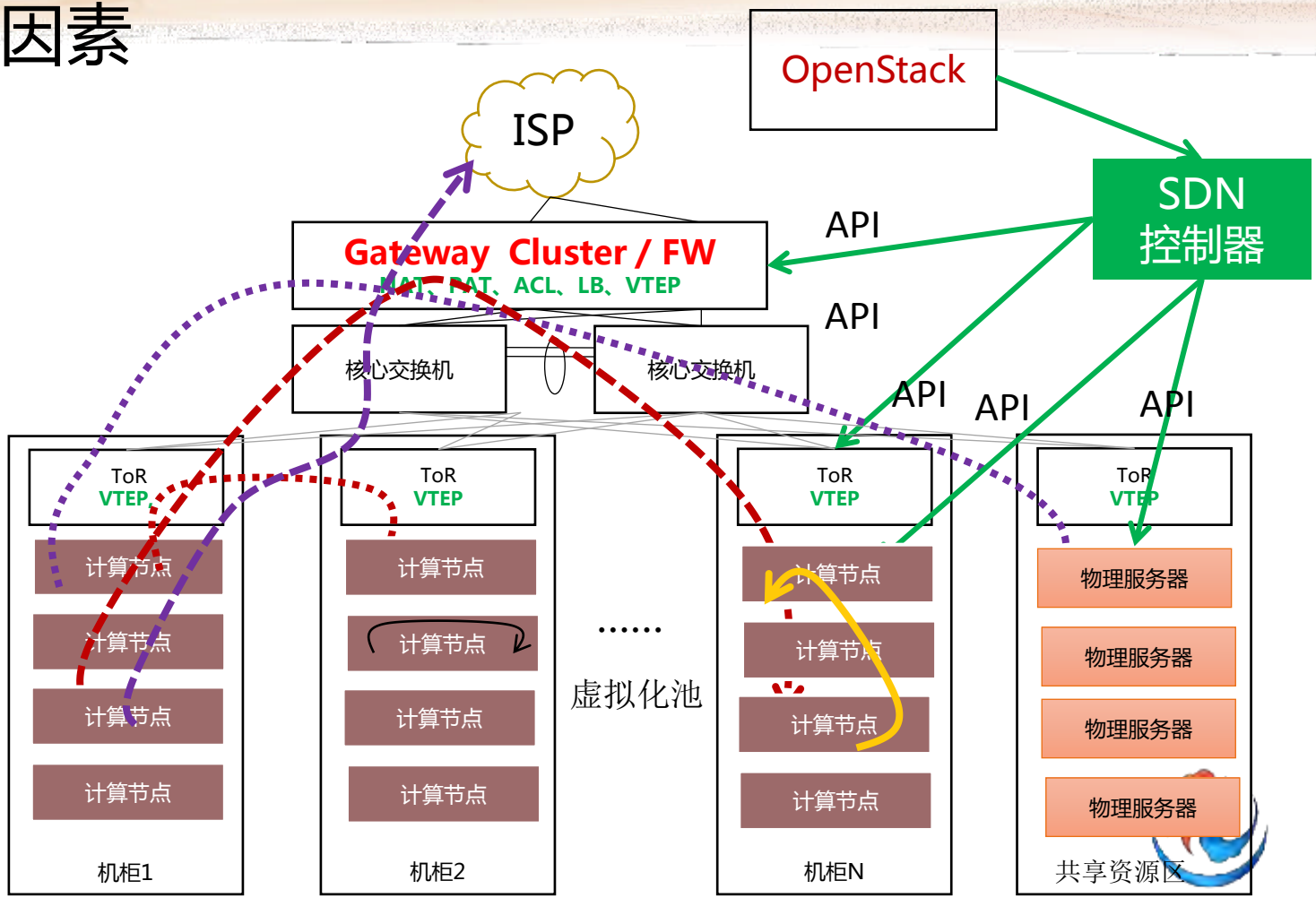


SDN关键因素

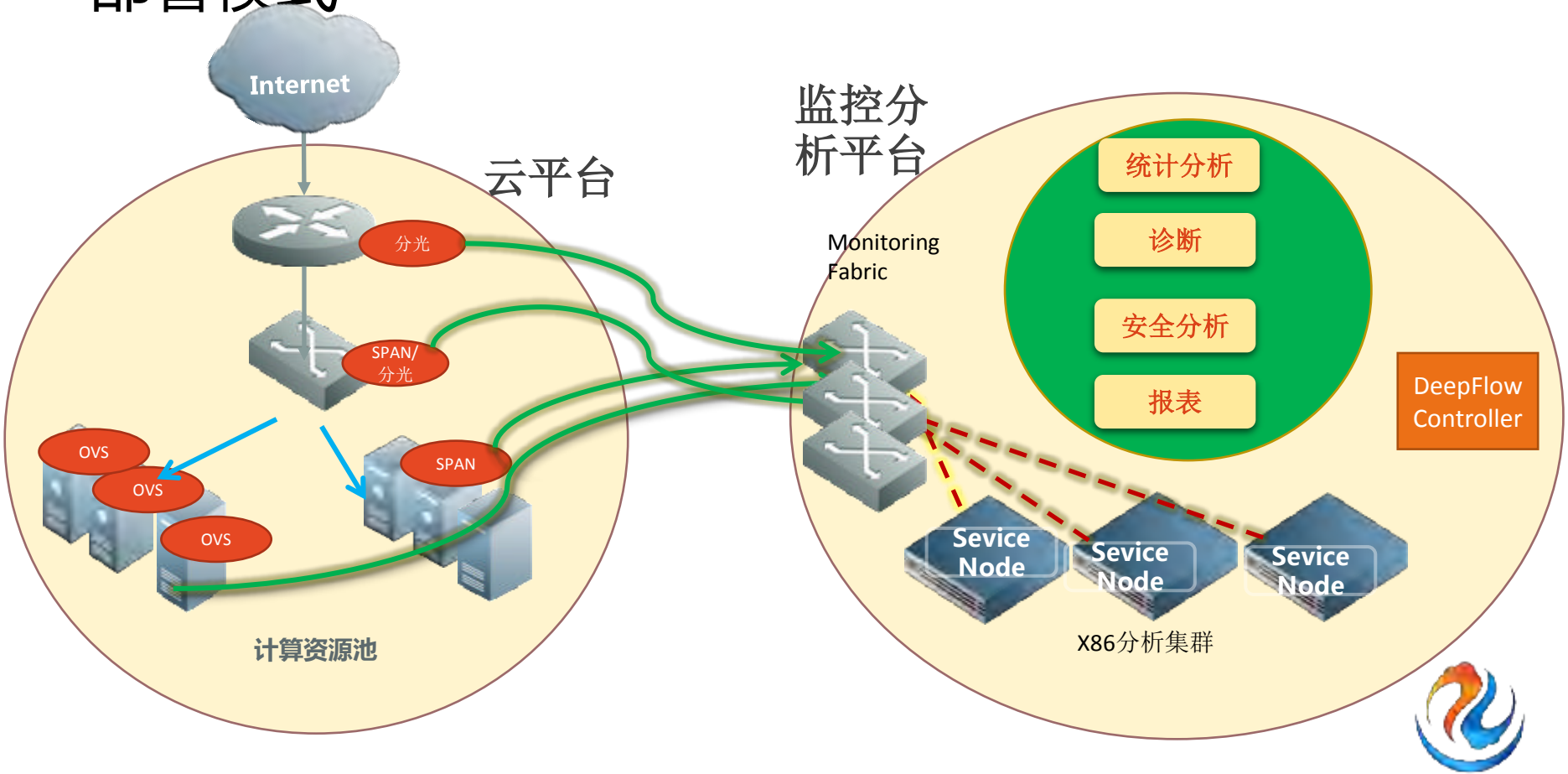
Scale问题

VTEP终结点

流量模型



部署模式


Internet
云平台
分光
SPAN/
分光
OVS
OVS
OVS
SPAN
计算资源池
监控分
析平台
Monitoring
Fabric
统计分析
诊断
安全分析
报表
DeepFlow
Controller
Sevice
Node
Sevice
Node
Sevice
Node
X86分析集群

目录

基于Flow的网络分析

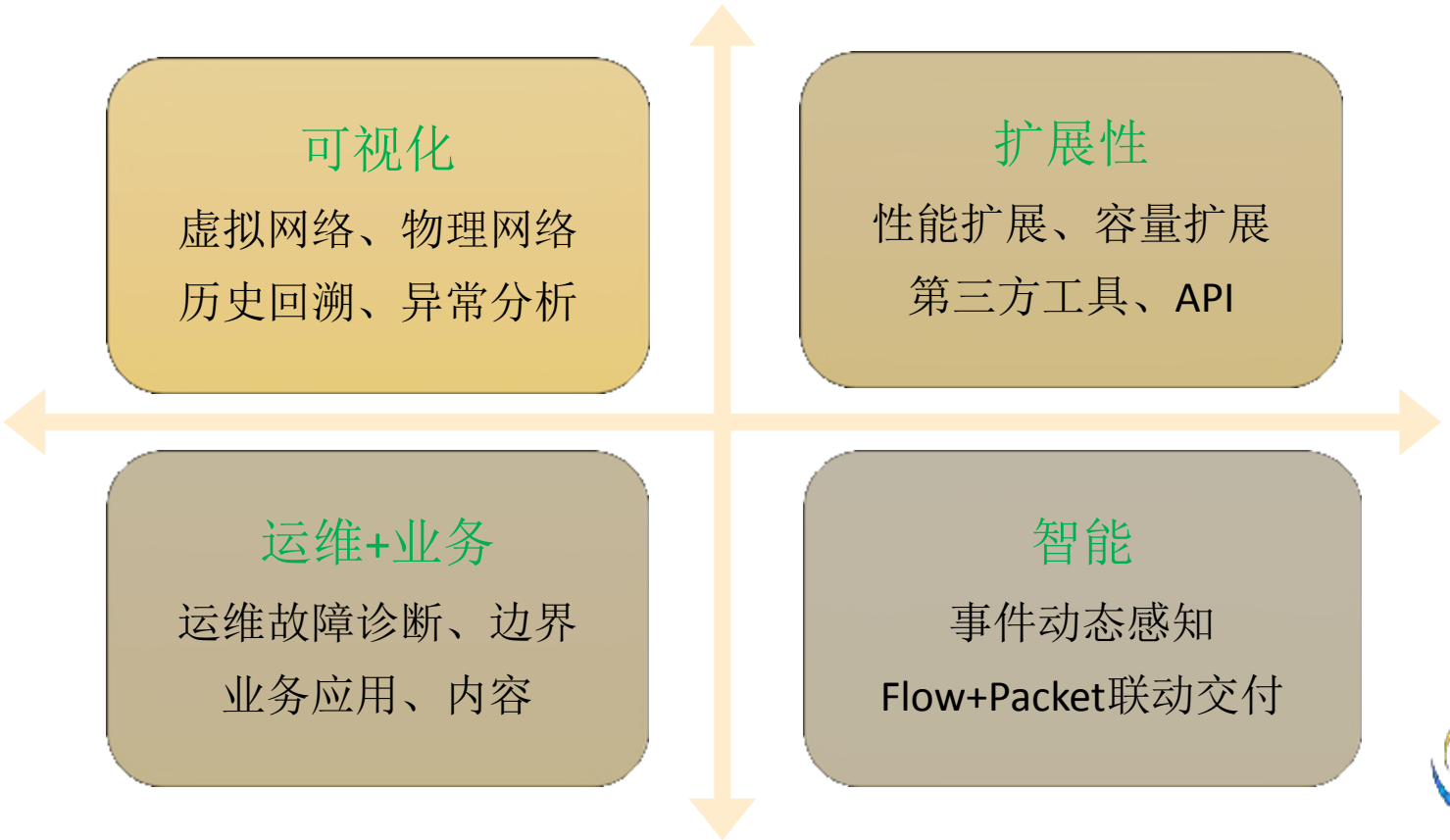
➢ **云网络监控困难**

- SFlow、Netflow/IPFIX、分光、镜像
- 数据存储，如何支持海量数据？
- 分析工具如何感知云？虚拟网络流量（东西流量）如何获取？
- 如何同时支持多个分析工具？

➢ **Flow的价值**

- 描述连接信息，五元组、连接状态、字节数、握手关闭状态，连接时间等，自动关联云平台信息
- 轻量级，存储数据量小，时间长
- 适合行为分析，按需与DPI结合，大大提高效率
- 无需看用户数据

云网分析需求

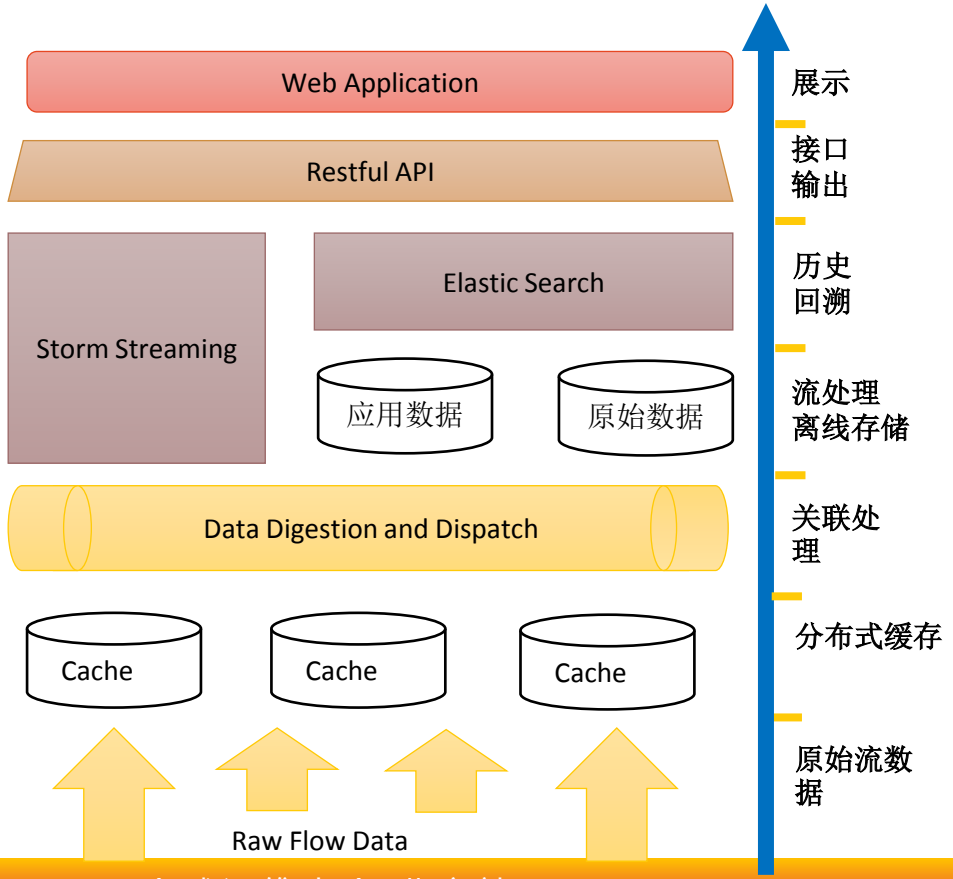

可视化
虚拟网络、物理网络
历史回溯、异常分析
扩展性
性能扩展、容量扩展
第三方工具、API
运维+业务
运维故障诊断、边界
业务应用、内容
智能
事件动态感知
Flow+Packet联动交付

软件定义探针

- **SDN + Flow + DPI+ Traffic Intelligence + Cloud**

- SDN：利用SDN优势，提供高效灵活的控制管理
- Flow：全时、全网，为网络行为分析提供依据
- Packet：DPI应用，内容深度检测
- Traffic Intelligence：包截断，流截断，内容隐藏，包头改写等
- Cloud Adapter：学习云的资源、配置、状态等信息

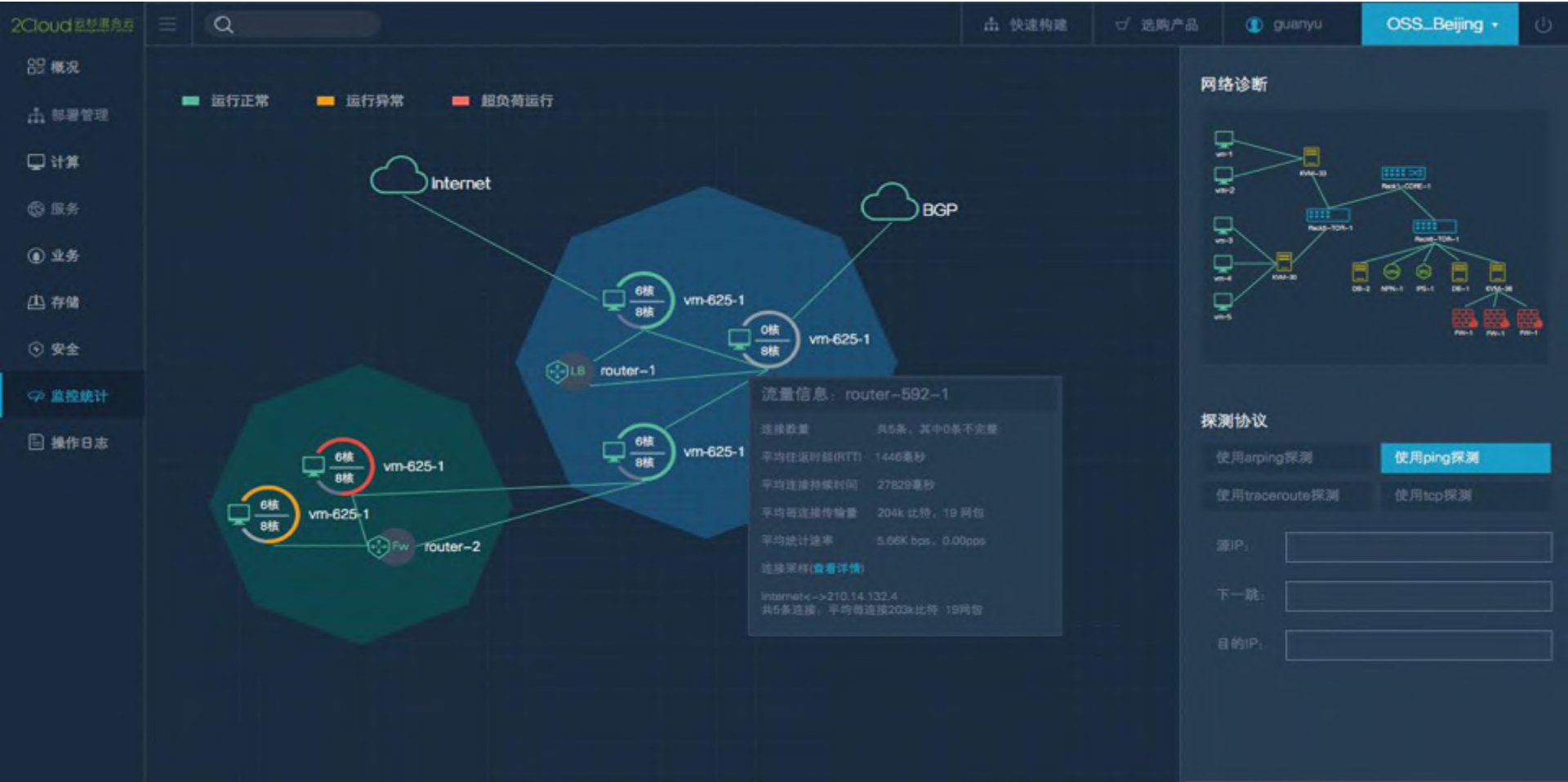
软件架构


Web Application
Restful API
Storm Streaming
Elastic Search
应用数据
原始数据
Data Digestion and Dispatch
Cache
Cache
Cache
Raw Flow Data
展示
接口输出
历史回溯
流处理离线存储
关联处理
分布式缓存
原始流数据


异常检测
网络可视化
监控诊断
动态学习

目录

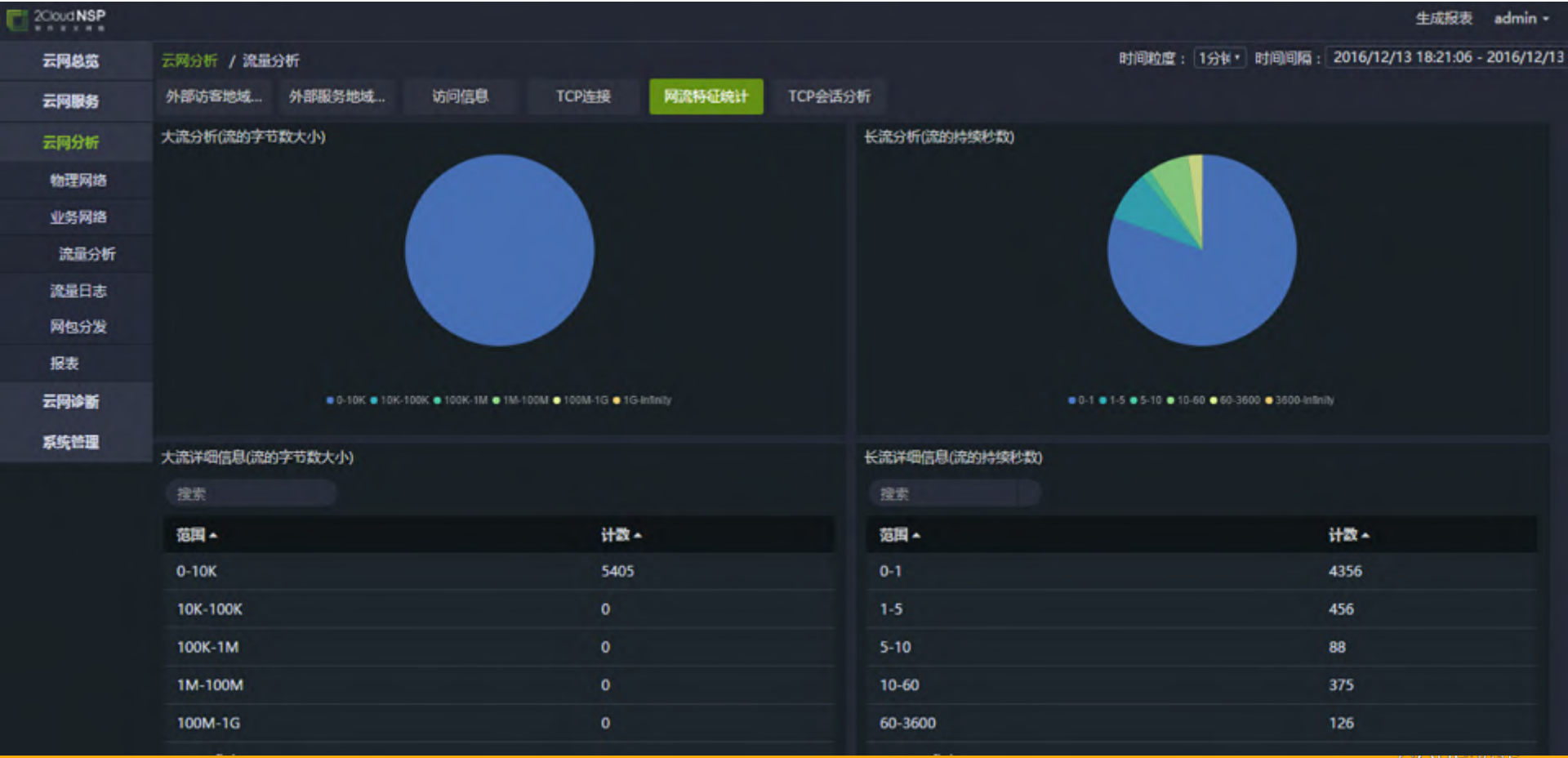
资源、位置、流量关联分析


2Cloud
快速构建
选购产品
guanyu
OSS_Beijing
概况
部署管理
计算
服务
业务
存储
安全
监控统计
操作日志
运行正常
运行异常
超负荷运行
Internet
BGP
6核
8核
vm-625-1
0核
8核
vm-625-1
LB
router-1
6核
8核
vm-625-1
6核
8核
vm-625-1
Fw
router-2
流量信息：router-592-1
连接数量
平均往返时延(RTT)
1446毫秒
平均连接持续时间
27829毫秒
平均每连接传输量
204k 比特，19 网包
平均统计速率
5.66K bps，0.00pps
连接采样(查看详情)
网络诊断
探测协议
使用arping探测
使用ping探测
使用traceroute探测
使用tcp探测
源IP：
下一跳：
目的IP：

自定义分析内容


2Cloud NSP
生成报表
admin
云网总览
云网服务
云网分析
物理网络
业务网络
流量分析
流量日志
网包分发
报表
云网诊断
系统管理
云网分析 / 业务网络 / 公网统计
时间粒度： 1分钟
时间间隔： 2016/12/13 14:37:54 - 2016/12/13 15:37:54
公网统计
私网统计
分类：
整体
自定义IP
增加标签
条件： 所有的ip均已选中
公网流量统计概况
流量速率峰值图
比特数 / 秒
2.5M
2M
1.5M
1M
500K
0
14:38
14:53
15:08
15:23
15:37
出口峰值
入口峰值
流量速率均值图
2M
1.6M
1.2M
800K
400K
出口均值
入口均值
报文速率均值和流数量均值图
包数量 / 秒
流数量 / 秒
500
400
300
200
100
4.3
3.4
2.5
1.6
0.7
网络协议占比排名
IP占比排名

网络行为统计


2Cloud NSP
生成报表
admin
云网总览
云网服务
云网分析
物理网络
业务网络
流量分析
流量日志
网包分发
报表
云网诊断
系统管理
云网分析 / 流量分析
时间粒度：1分钟
时间间隔：2016/12/13 18:21:06 - 2016/12/13
外部访客地域...
外部服务地域...
访问信息
TCP连接
网流特征统计
TCP会话分析
大流分析(流的字节数大小)
0-10K 10K-100K 100K-1M 1M-100M 100M-1G 1G-Infinity
长流分析(流的持续秒数)
0-1 1-5 5-10 10-60 60-3600 3600-Infinity
大流详细信息(流的字节数大小)
搜索
范围
计数
0-10K 5405
10K-100K 0
100K-1M 0
1M-100M 0
100M-1G 0
长流详细信息(流的持续秒数)
搜索
范围
计数
0-1 4356
1-5 456
5-10 88
10-60 375
60-3600 126

Flow & Machine Learning（内网）

source ip

Table | Request | Response | Statistics

src_ip: Descending	Count
10.10.2.102	21
10.10.2.2	312,300
10.10.1.103	53,146
10.10.1.102	146,719

dest ip

Table | Request | Response | Statistics

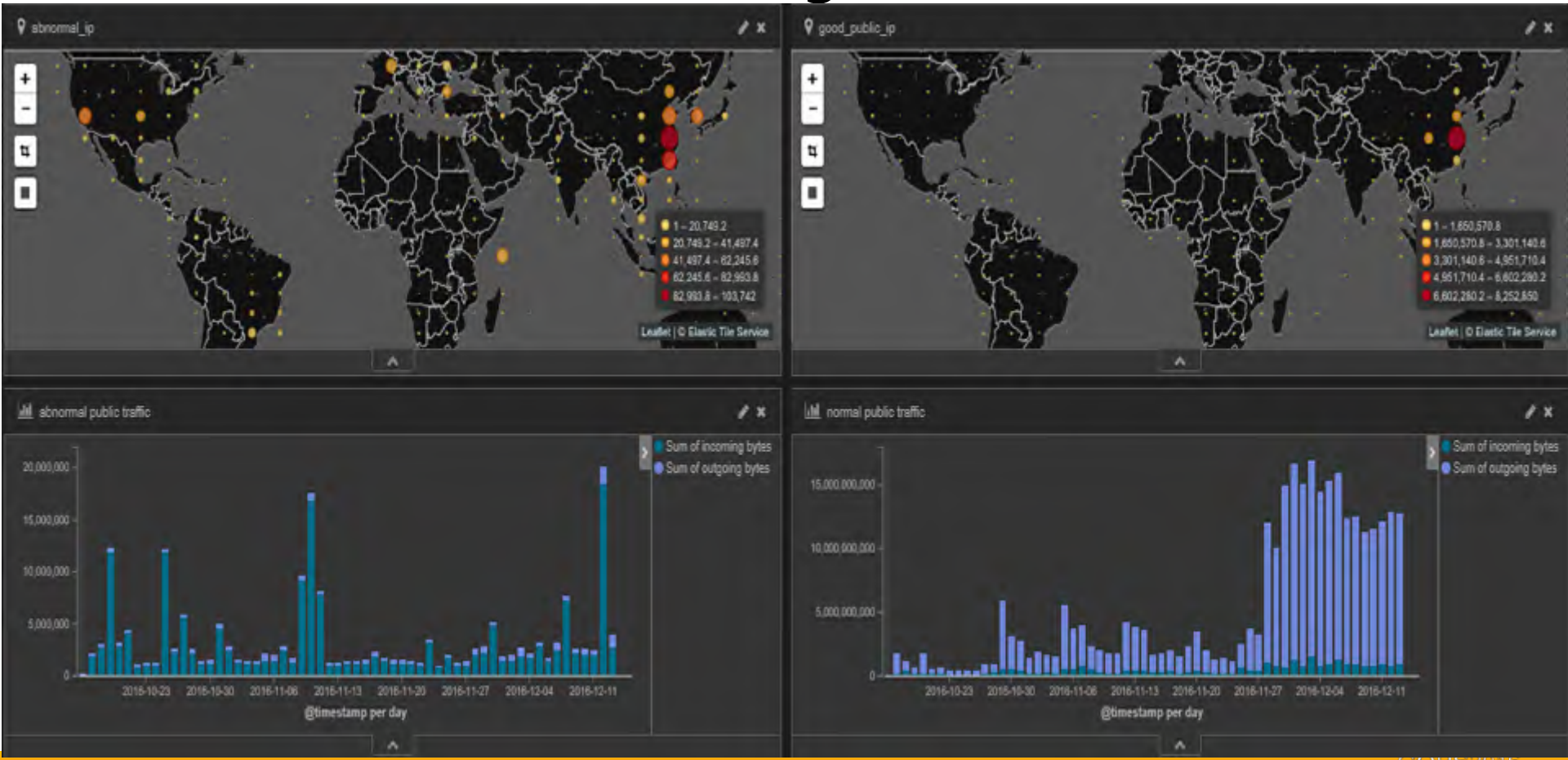
dst_ip: Descending	Count
192.168.250.101	890
192.168.250.100	889
172.16.64.38	3,120
10.10.2.102	199,865

scan port

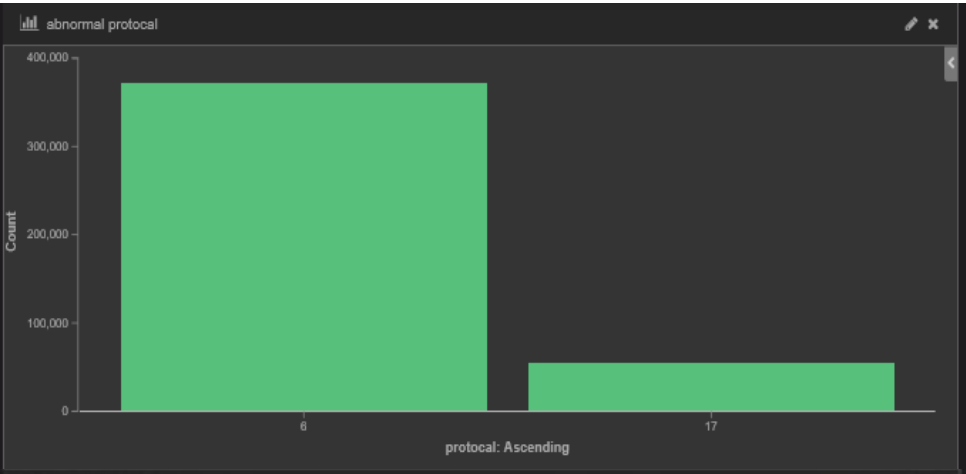
Table | Request | Response | Statistics

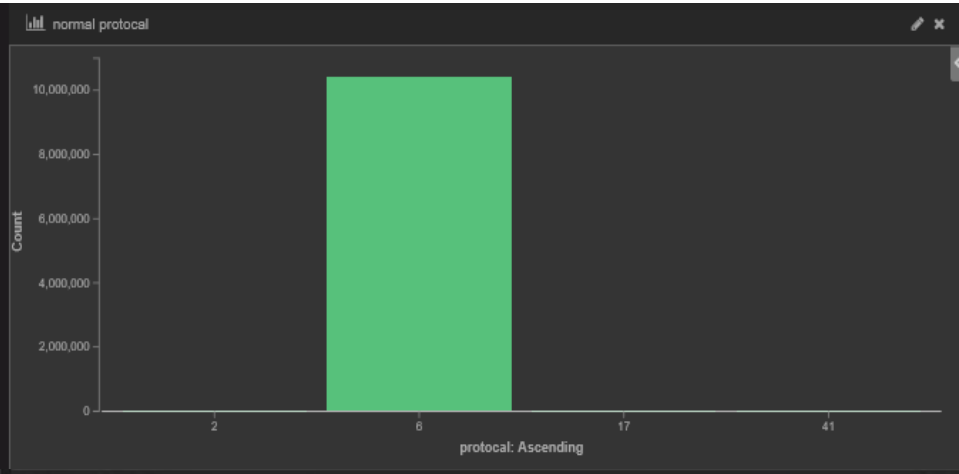
dst_port: Ascending	Count
1,433	154

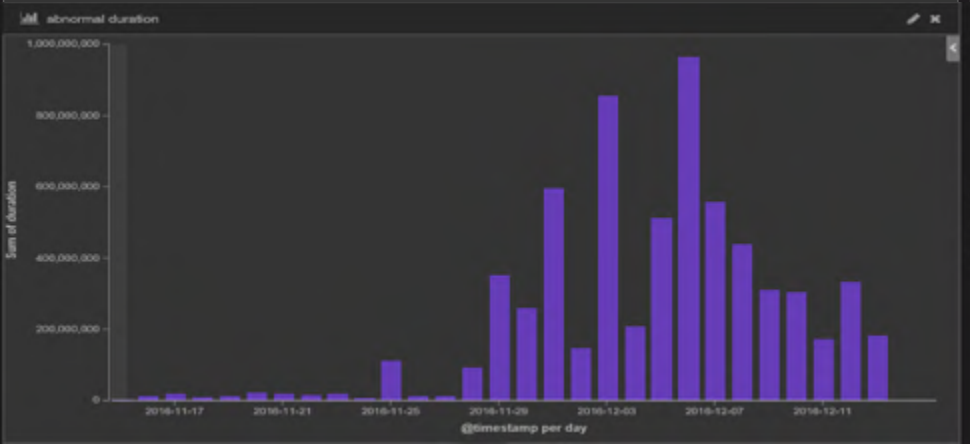
Flow & Machine Learning（公网）

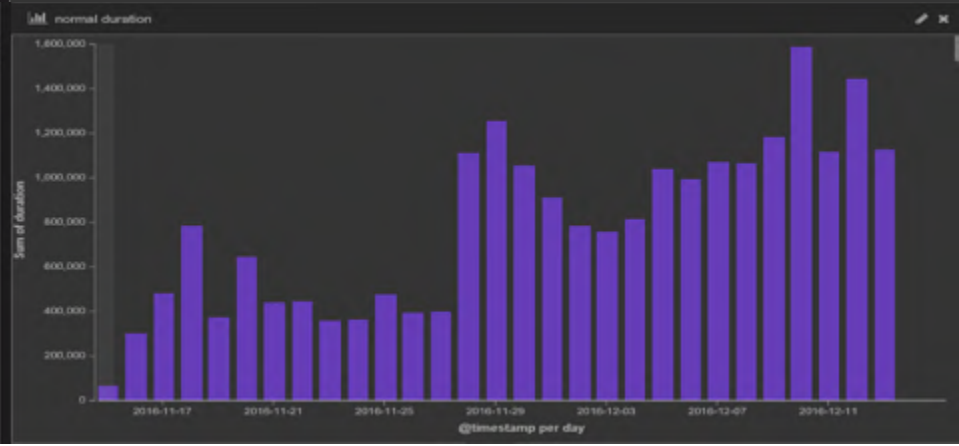


Flow & Machine Learning（公网）









第三方服务集成（绿盟）

历史溯源	APT攻击	内部攻击	网络可视化
• 大规模存储 • 快速检索 • Root cause	• 异常行为发现 • 非signature检测	• 内部网络行为违规 • 内部异常行为检测	• 直观态势 • 应急响应速度

DevOpsDays 即将首次登陆中国

DevOps 之父 Patrick Debois 与您相约

DevOpsDays 北京站 2017年3月18日

门票早鸟价仅限前100名，请从速哟

http://2017-beijing.devopsdayschina.org/

想第一时间看到
高效运维社区公众号
的好文章吗？

请打开高效运维社区公众号，点击右上角小人，如右侧所示设置就好

Thanks

高效运维社区

开放运维联盟

荣誉出品