DOIS | 2018 · 深圳站

DevOps 落地，从这里开始

DevOps 国际峰会

暨 DevOps 金融峰会

指导单位：云计算开源产业联盟 OpenSource Cloud Alliance for Industry, OSCAR

主办单位：DevOps时代　高效运维社区 GreatOPS Community

时间：2018年11月2日-3日

地址：深圳市南山区圣淘沙大酒店（翡翠店）

DOIS

金融云业务网络智能采集与一体化分析实战

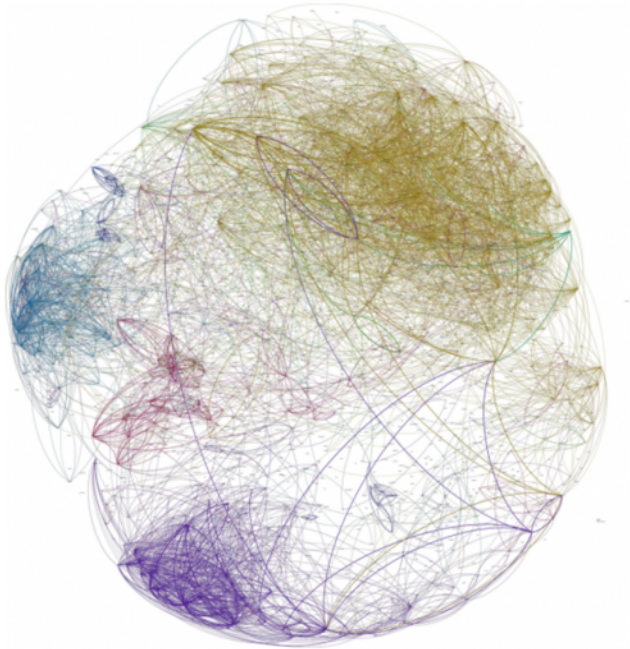
吴毓华 高级技术经理

DOIS

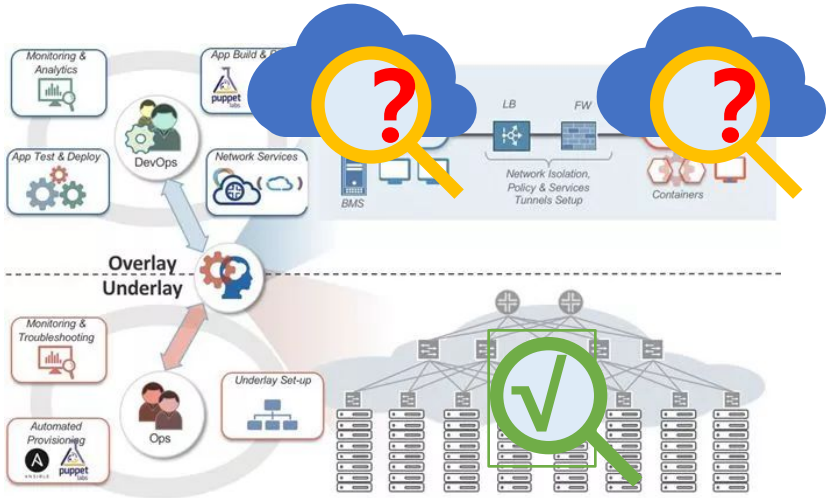
目录

网络变化趋势

DOIS

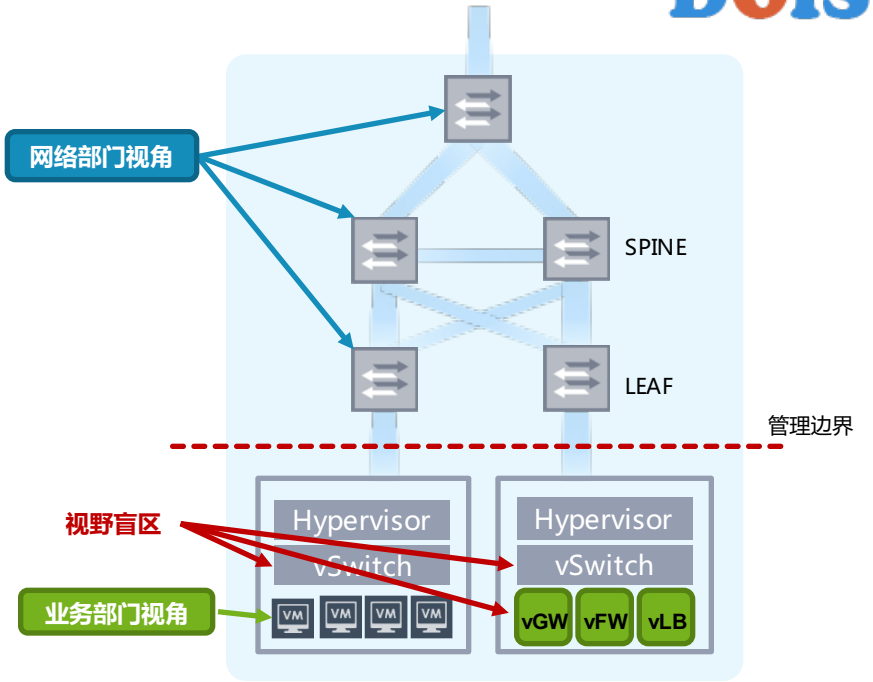


80%东西向流量



网络与业务的脱节

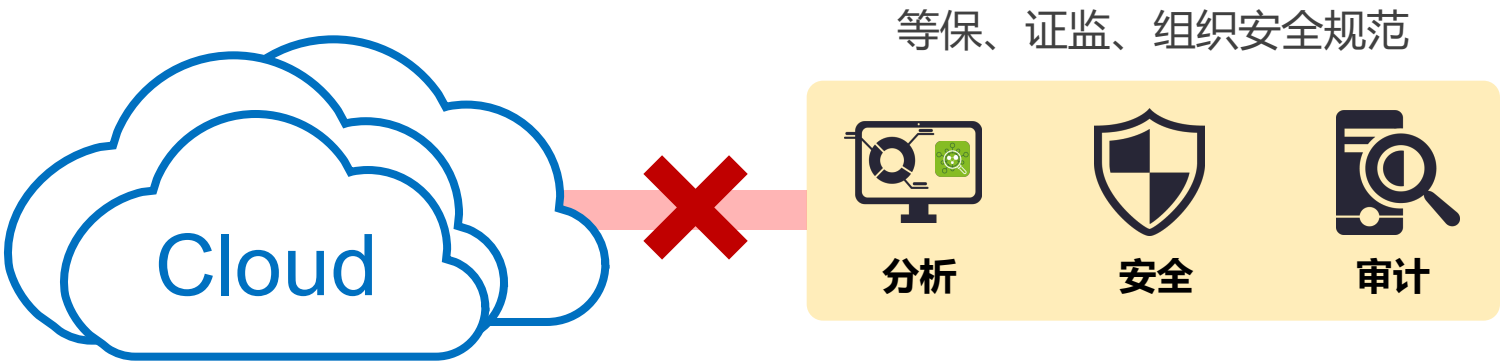
例子1



每天都在发生的争论

管理盲区

例子2

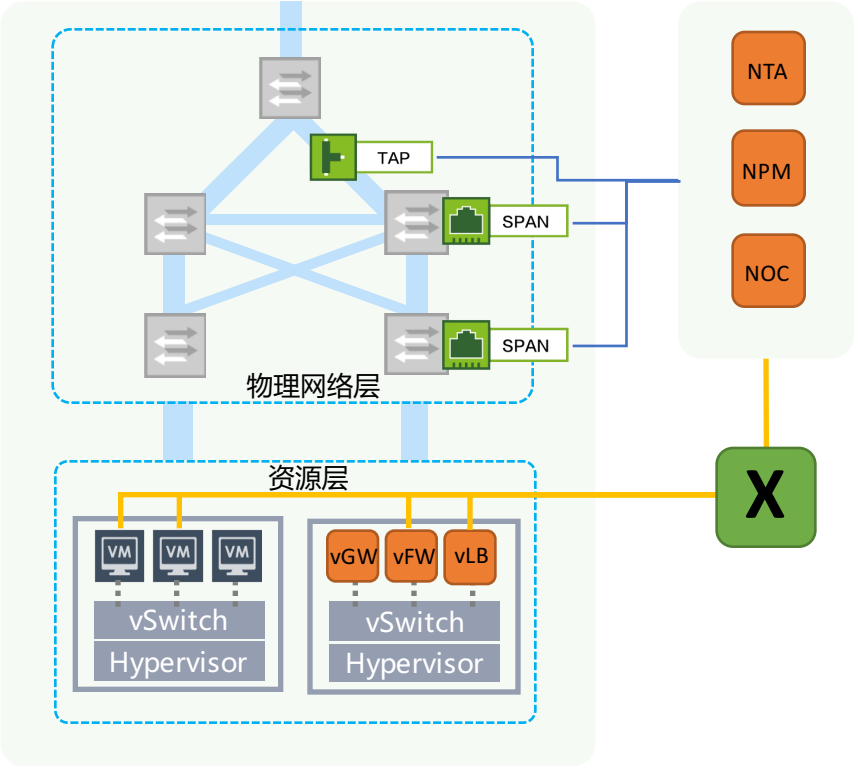


采集虚拟网络流量，必须安全、可靠。

总结

虚拟网络流量采集与分析

云时代网络的标配



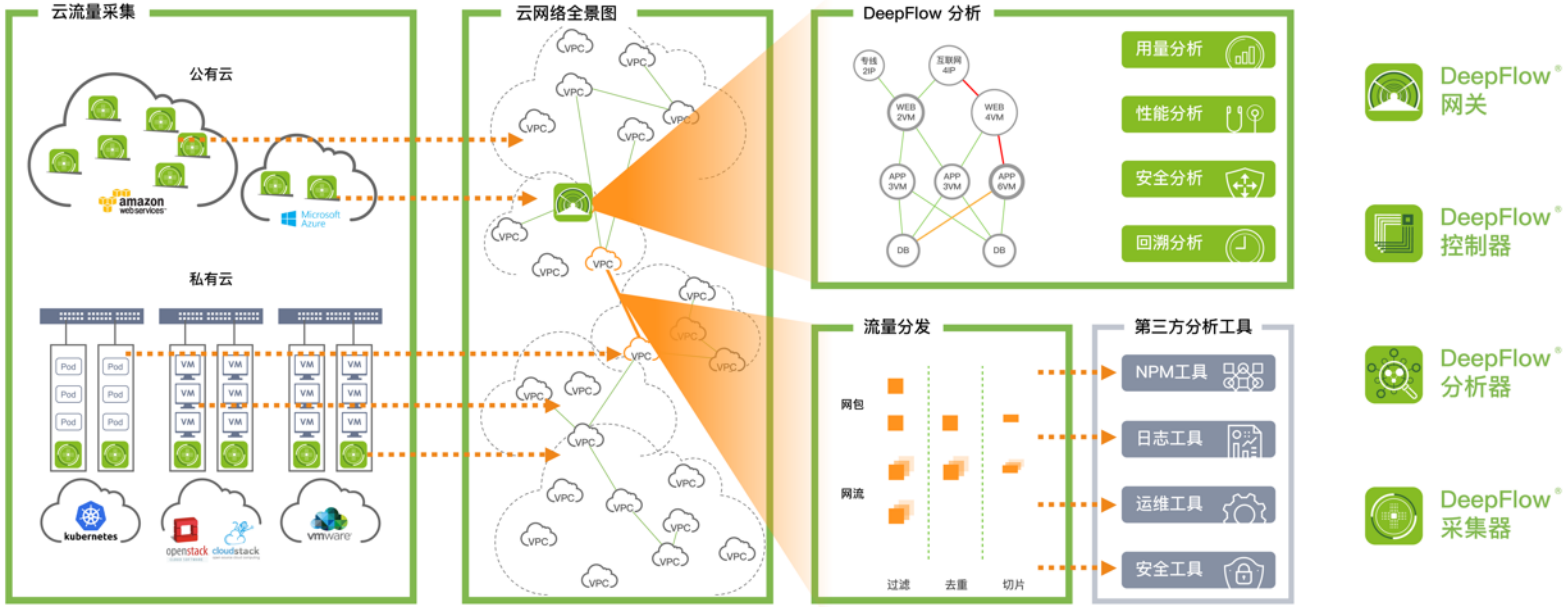
DOIS

目录

虚拟网络流量智能采集与一体化分发方案

DOIS

DeepFlow® 一体化的虚拟网络流量采集分析



适用于云环境的采集方式

DOIS

大规模

支持500个节点，满足单个数据中心Region规模；

安全可控

用户态，不影响内核功能；CPU、内存消耗可控，不影响生产；

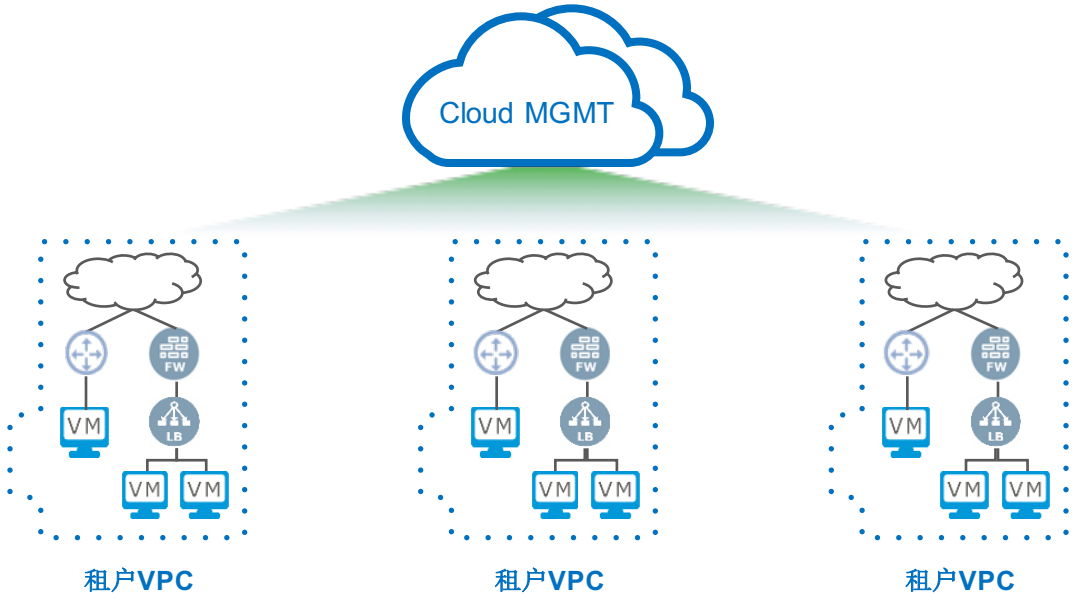
高性能

单节点支持10G虚拟机流量。

策略灵活

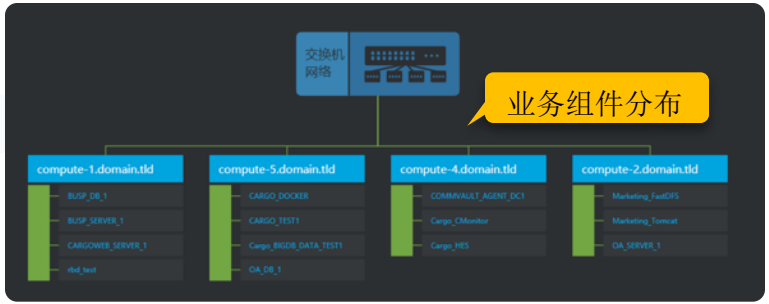
与云平台同步信息，策略自适应；支持多种过滤条件，适用于不同场景

业务网络自动学习



从云平台中自动学习业务信息，梳理主机、虚拟机、网络关系

网络全景展现

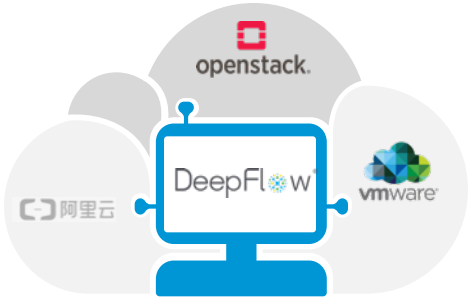


- 梳理项目、主机、虚拟机信息
- 根据网络流量绘制访问关系

方案优势及价值总结

DOIS

- **覆盖网络管理盲区，**做到有迹可循，提高运维效率；
- 有效分析虚拟网络流量，**满足安全合规要求；**
- **展示业务网络全景**，梳理业务调用关系，提高管理效率。



目录

定位问题

DOIS

1. 需求：

   - 从业务角度定位问题根因。

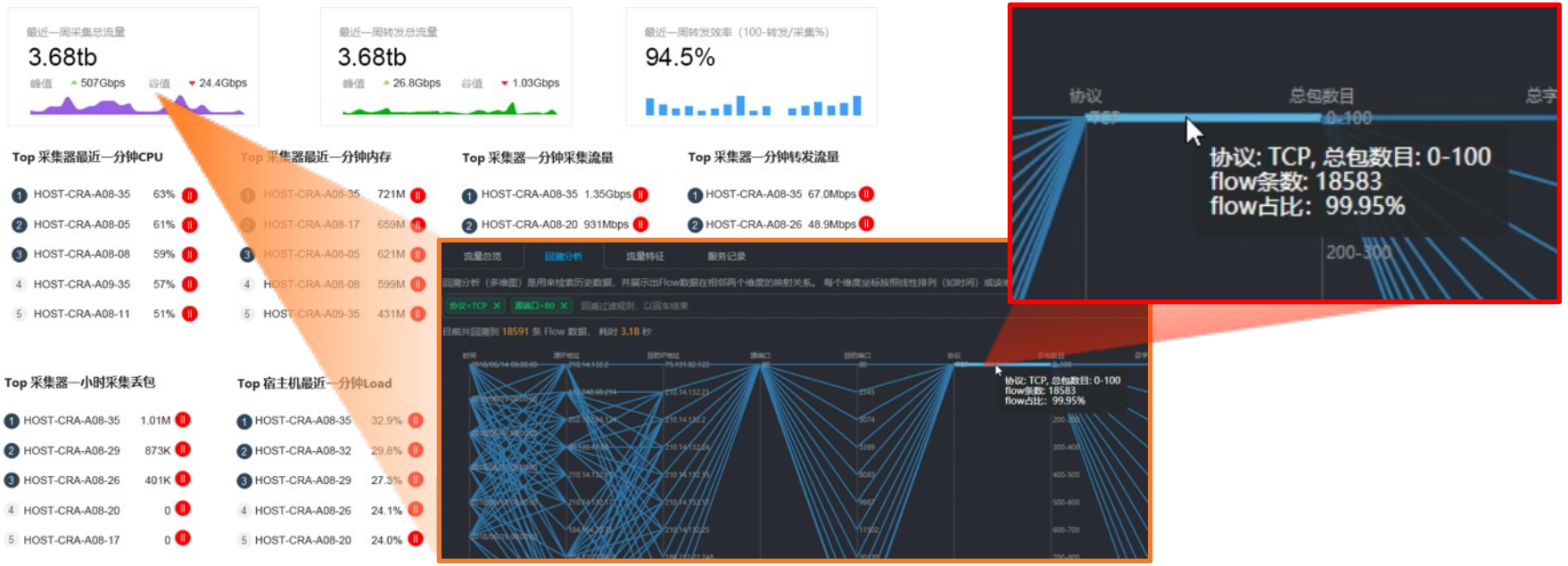
2. 解决方案：

采集	回溯	对比	钻取	“抓包”	回测	结论
采集业务对应虚拟机流量； 覆盖150个节点。	将时间倒退至事故发生时段，还原现场。	将问题虚拟机的网络流量与正常情况下的做对比； 发现有突发流量。	针对异常流量，分析其流量成分； 发现与某IP产生大量流量。	调取PCAP文件，分析“案发”过程； 发现单方向push大量数据。	基于异常特征，回测过往发生次数、频率； 发现每小时都有发生。	数据库备份系统策略异常。

定位问题

DOIS

采集 → 回溯 → 对比

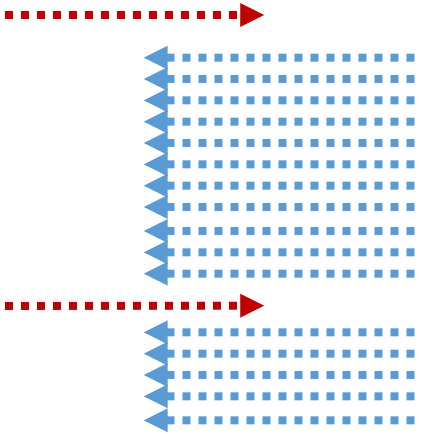


定位问题

DOIS

钻取 → “抓包” → 回测

针对异常流量，分析其流量成分；
发现与某IP产生大量流量。



调取PCAP文件，分析“案发”过程；
发现单方向push大量数据。

基于异常特征，回测过往发生次数、频率；
发现每小时都有发生。

定位问题

DOIS

问题结论：数据库备份系统策略异常。

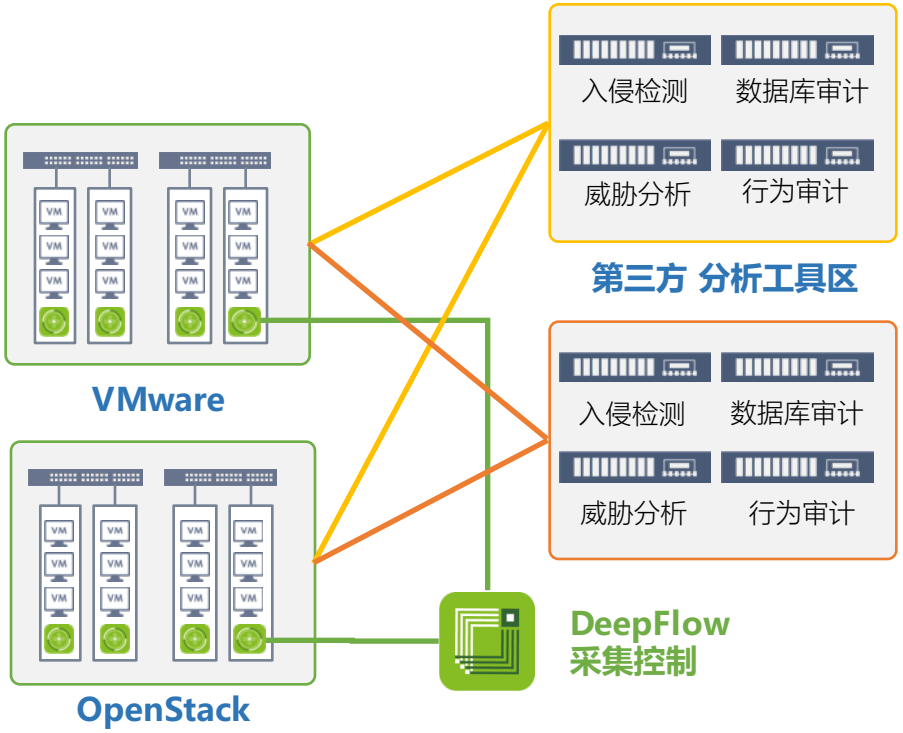
其他常见问题：

- SLB策略不当导致流量不均 或 特定流量被随机；
- 突发流量影响vGW；
- 数据库语句异常导致数据查询缓慢；
- ……

价值：从业务角度出发，帮助准确回溯定位问题，提高运维效率。

安全合规

1. 需求：
   - 获取虚拟网络流量，实现安全分析、审计，满足合规性要求。
2. 解决方案：
   - 同时采集VMware和OpenStack环境的东西向流量，按需分发给第三方工具。
3. **价值：**
   - **赋予虚拟网络流量分发能力，满足安全合规要求。**



目录

总结

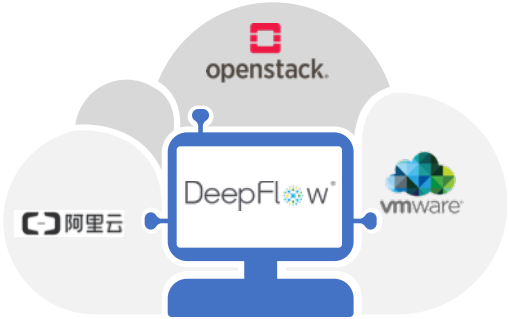
DOIS

零依赖、无侵扰

在Openstack环境中，不受OvS策略、软件版本的依赖限制。在VMWare环境中，通过SPAN进行流量获取。对现有生产网络无干扰。

高性能、微消耗

具有专利的高性能算法，实现了算子前置，从而大幅降低采集信息传输带宽（高达1：1000），同时支持用户自定义采集器的系统资源消耗。



为云而生

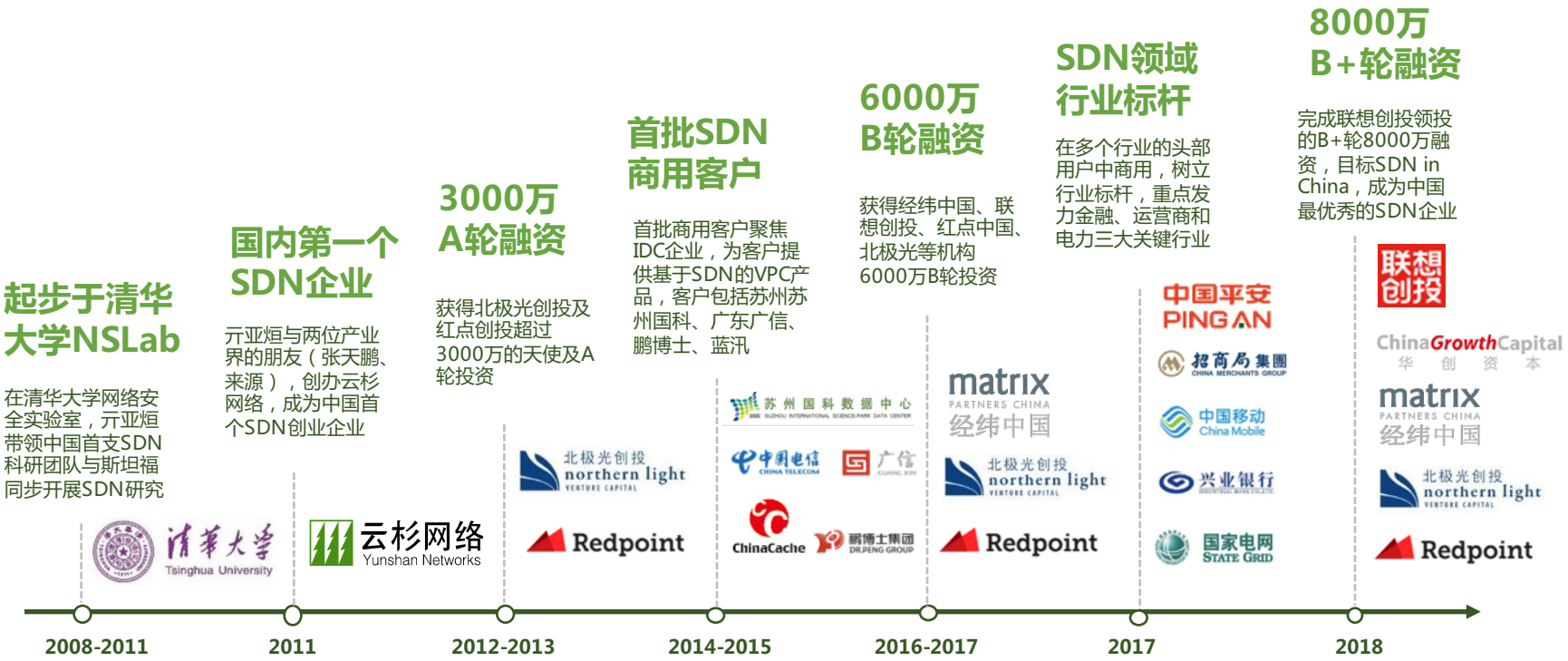
适配主流云平台。控制器统一配置分发目的、控制起停、设置截短策略、下发ACL策略、统一监控状态。

安全、可管理

不影响系统内核，不会引起系统宕机，内存泄漏等异常。采集器支持自定义策略，可秒级起停，安全可控。

关于云杉网络

DOIS


起步于清华大学NSLab
在清华大学网络安全实验室，亓亚烜带领中国首支SDN科研团队与斯坦福同步开展SDN研究
清华大学 Tsinghua University
2008-2011
国内第一个SDN企业
亓亚烜与两位产业界的朋友（张天鹏、来源），创办云杉网络，成为中国首个SDN创业企业
云杉网络 Yunshan Networks
2011
3000万A轮融资
获得北极光创投及红点创投超过3000万的天使及A轮投资
北极光创投 northern light VENTURE CAPITAL
Redpoint
2012-2013
首批SDN商用客户
首批商用客户聚焦IDC企业，为客户提供基于SDN的VPC产品，客户包括苏州苏州国科、广东广信、鹏博士、蓝汛
苏州国科数据中心
中国电信 CHINA TELECOM
广信
ChinaCache
鹏博士集团 DR.PENG GROUP
2014-2015
6000万B轮融资
获得经纬中国、联想创投、红点中国、北极光等机构6000万B轮投资
matrix PARTNERS CHINA 经纬中国
北极光创投 northern light VENTURE CAPITAL
Redpoint
2016-2017
SDN领域行业标杆
在多个行业的头部用户中商用，树立行业标杆，重点发力金融、运营商和电力三大关键行业
中国平安 PING AN
招商局集团 CHINA MERCHANTS GROUP
中国移动 China Mobile
兴业银行
国家电网 STATE GRID
2017
8000万B+轮融资
完成联想创投领投的B+轮8000万融资，目标SDN in China，成为中国最优秀的SDN企业
联想创投
ChinaGrowthCapital 华创资本
matrix PARTNERS CHINA 经纬中国
北极光创投 northern light VENTURE CAPITAL
Redpoint
2018

DOIS

Thanks

云杉网络 Yunshan Networks

荣誉出品

DOIS

欢迎加入技术交流群

【云杉网络】DevOps金融峰会2018

该二维码7天内(11月10日前)有效，重新进入将更新