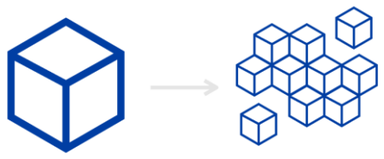
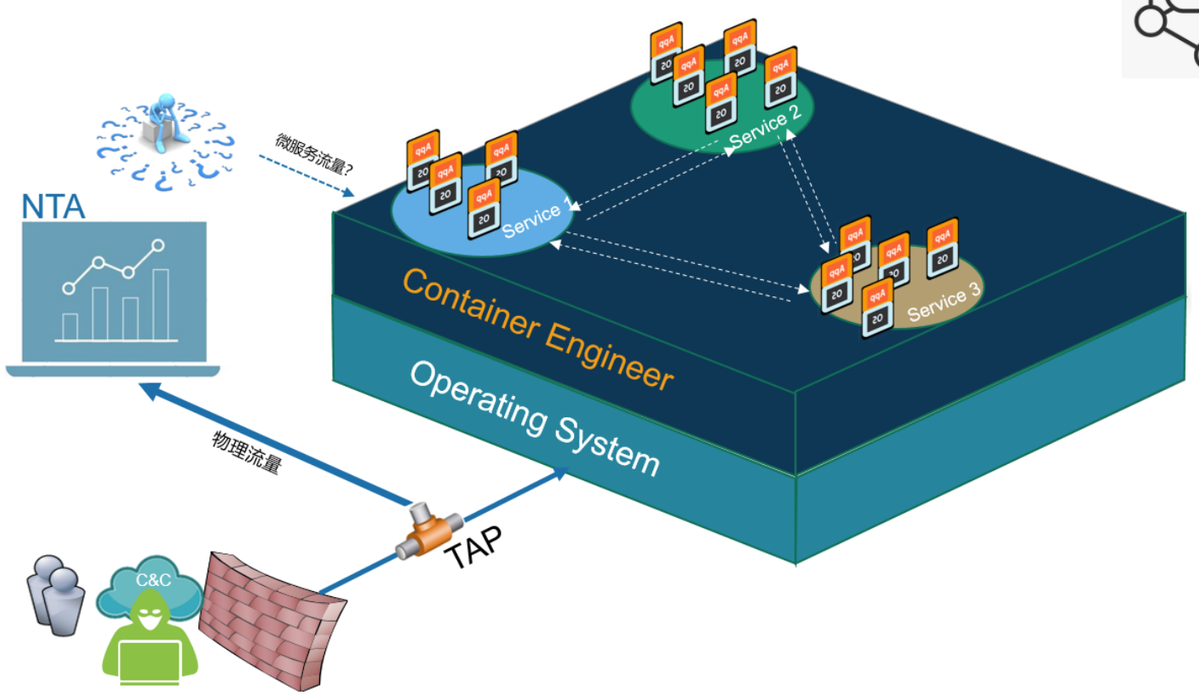
# 雅客云vTap

## 微服务东西向流量成为安全盲区

微服务架构的兴起，导致业务间产生了大量东西向流量，这些流量规避了传统物理网络安全设备的监控，对微服务的网络侧监测及拦截能力提出严峻的挑战，如何把物理网络上不可视的东西向非法流量提取出来是其中一个技术的关键难题，并且传统的流量提取技术只能够追朔到非法流量的源地址，也即源IP地址，但是在容器环境里IP地址是动态变化的，只提取出有问题的IP地址对查找问题源头没有实际意义，如何在提取非法流量的同时追踪到问题的源头才是问题的关键（进程，镜像，开发者等）。



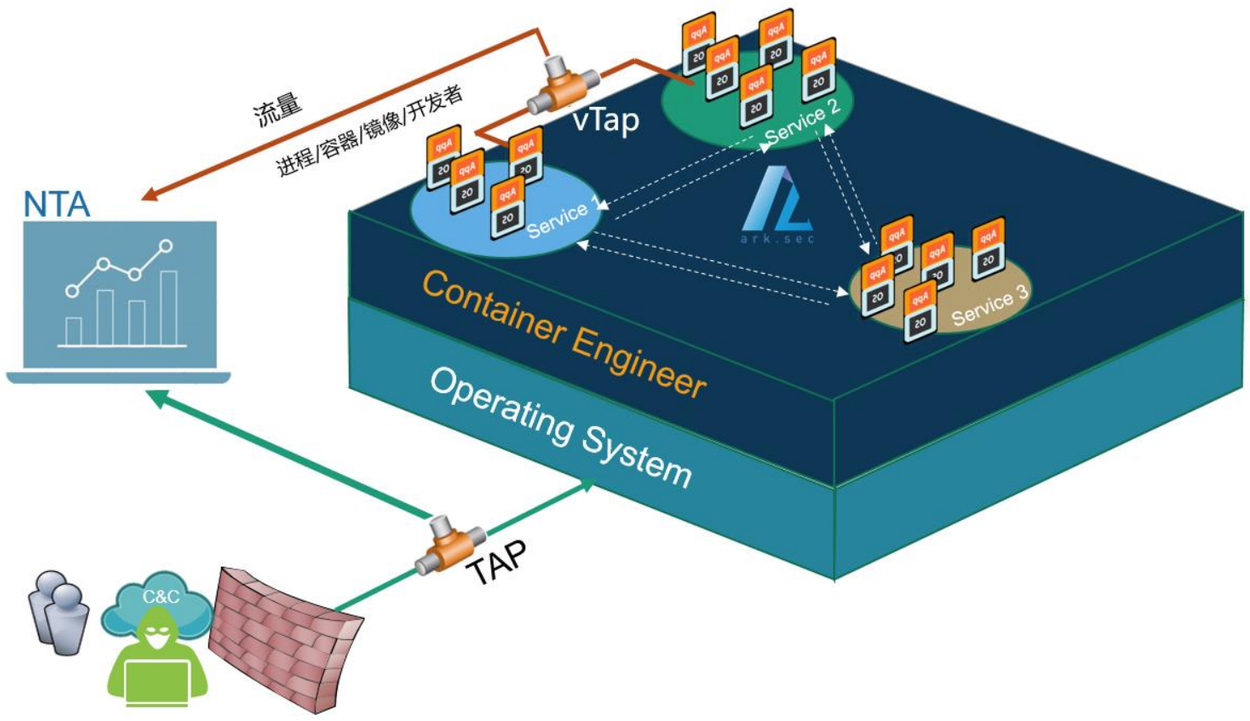



## 传统NTA在云原生环境下的痛点

目前网络流量分析解决方案的流量信息收集主要集中在用户到数据中心的数据通道上，比如在WOC设备，门户网关，负载均衡器，NGNIX，第三方防火墙或者应用防火墙WAF等设备上收集数据流量及日志信息。 而此类日志主要集中在南北流向和Web流量中。对于数据中心内部的东西向流量，以及K8S集群内部微服务之间交互的东西向流量可能成为解决方案的盲点。同时，对于一些K8S集群内加密流量的处理可能会有一定可视性问题。

## 雅客云vTap解决方案

借助于雅客云赤岩石vTap，可以为网络流量分析解决方案(NTA)解决微服务东西向流量可视性的问题，并且借助安全模块对主机系统及K8S上下文的感知能力，为网络流量分析解决方案提供更细粒度的信息：



# 雅客云vTap

1

## 为NTA提供集群内精细粒度的源数据

容器、K8s节点间的流量，也可以镜像到流量分析系统中，同时提供基于容器和K8s的流量上下文（例如目标流量的容器信息，比如容器内进程、容器镜像、开发者等等）

## 支持服务网格

对于实现了Service Mesh层的容器， 我们的收集系统可以镜像解密后流量，给流量分析系统提供明文数据增加可视性。

2

3

## 可配合云原生容器沙箱

若结合K8节点部署我们的云原生容器沙箱，把我们自己的分析（僵木蠕，病毒文件，攻击等）日志也同时吐给流量分析系统参考，提供更丰富的安全报告，用户对自己的资产有更细致得风险评估依据。

## API接口

我们的云原生网络方案，支持链接级的流量强制能力，包括阻断、转发和镜像禁用等操作。 对此类操作可以提供标准API操作。 对于流量分析系统的分析结果，用户可以下发通过分析结果所产生的流量强制和控制策略。

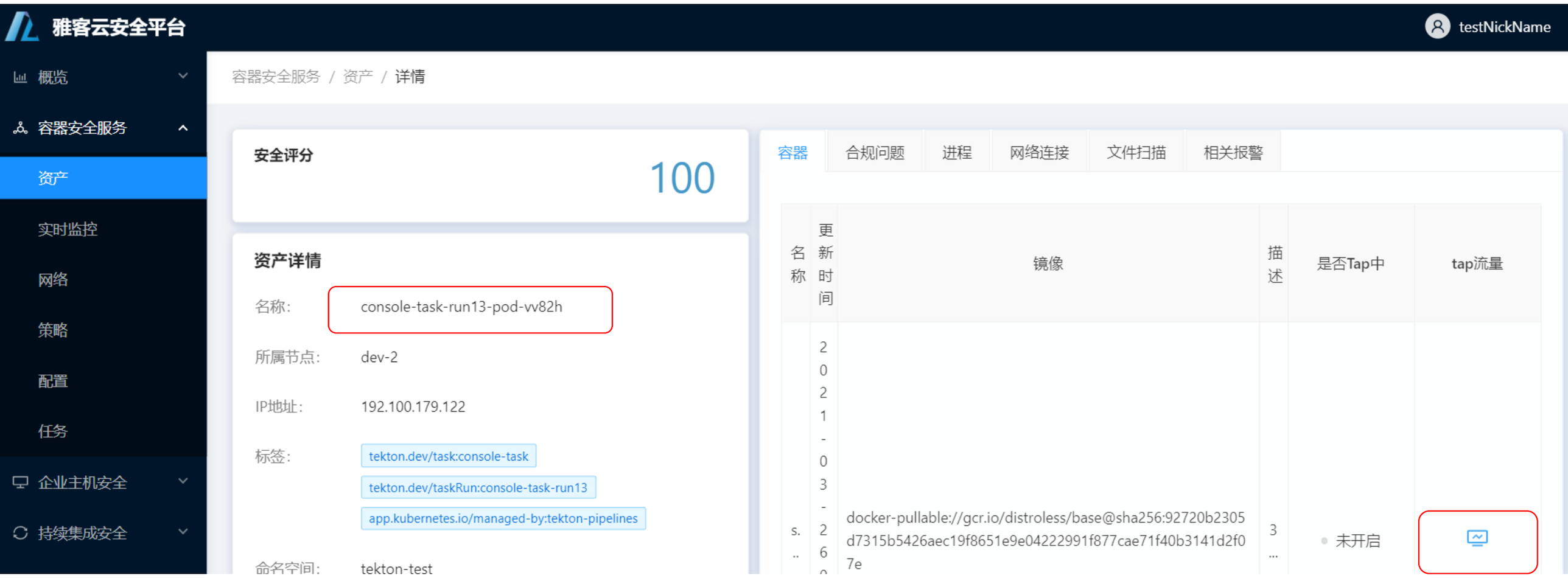
4



- 加载网络策略
- 隔离POD
- 停用POD
- 对镜像告警
- ETC

5

## 选择性采集微服务流量，针对目标POD打上vTap




# 关于雅客云

北京雅客云安全科技有限公司（ArkSec）是由硅谷领先网络安全公司资深技术专家、以色列领先网络安全公司高管团队成立的以基于云原生安全产品和服务为主的技术驱动型高新技术企业。公司开发了国内自主知识产权的赤岩石云原生安全全生命周期防护产品，为云原生安全平台打下基础，是中国首家将预测、防御、监控和响应能力融为一体，提供云原生安全防护平台并覆盖到边缘云的整体解决方案的公司（www.arksec.cn)。