AnaTraf 网络流量分析仪

全流量回溯分析

云争 YUNZHENG TECH

为什么需要全流量分析?

1. 信息安全保障
2. 满足合规要求
3. 事件调查取证

全流量

---网络所有原始流量的存储、分析

- **再高级的威胁、攻击都会产生流量**
- **网络安全等级保护2.0要求部署全流量回溯**
- **还原过程，责任界定**

全方向

---网络出口 & 内网核心

传统手段 vs 全流量回溯分析

传统手段

- Ping、tracert 等工具专业性强，故障分析周期长。
- 现有的工具受限，有的问题无法分析。比如部分设备无电口无法抓包分析。
- 现有的分析工具只能事后分析故障，无法对故障进行预警以及重现历史故障。

全流量回溯分析

- 图形界面，全面可视化网络。简单、高效、快速定位故障。
- 支持串联、TAP、镜像端口方式采集数据，适用范围广。
- 7×24持续采集、分析网络流量，随时可回溯，重现历史问题。细粒度，检索快。

传统手段弊端

问题难复现、难定位

过一会自己又好了...

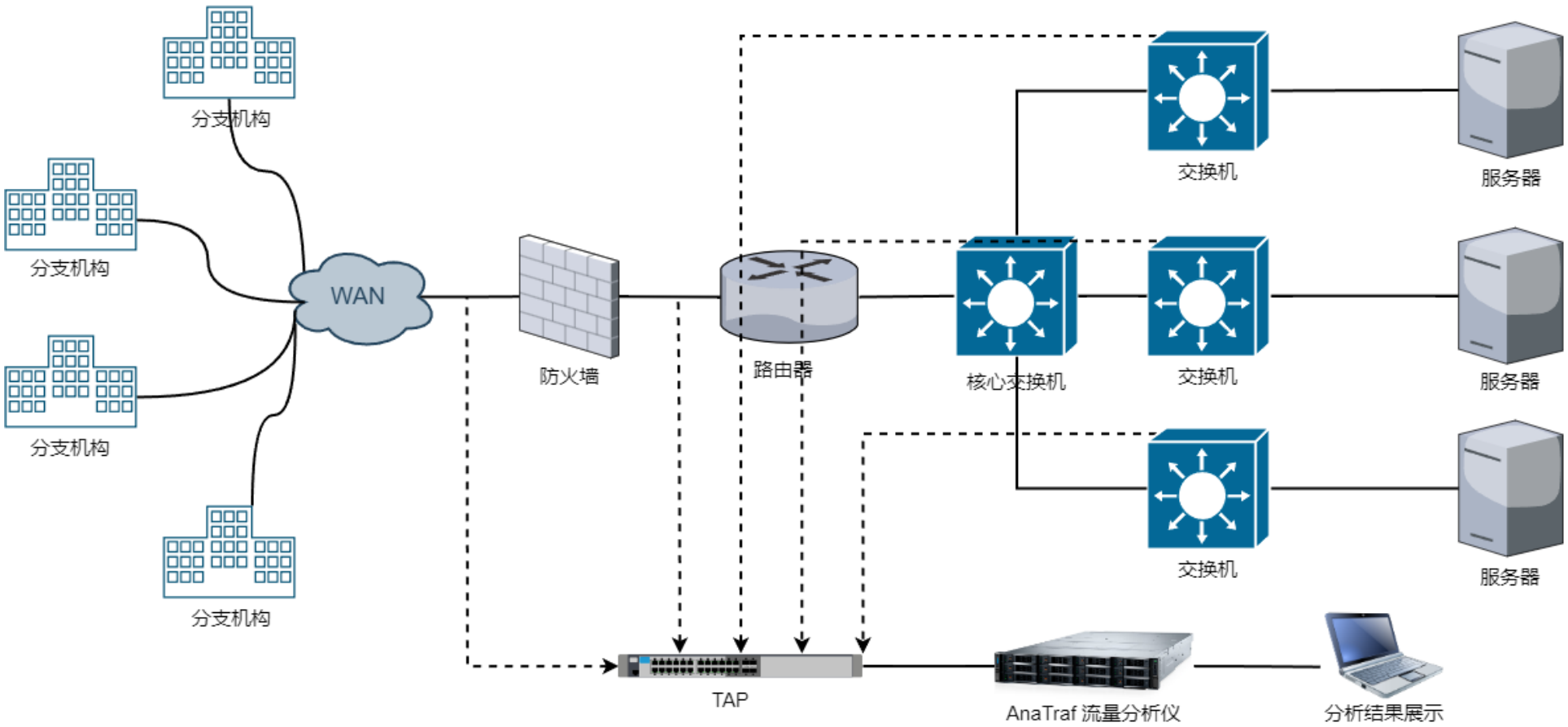
告警太多难以分析

粒度粗，检索慢，缺乏原始场景的数据，效率低，最后也懒得看

安全问题难以追溯

只有日志信息，无法做到对攻击的完整取证和溯源

典型部署



主要功能

所有型号的设备具有相同的流量分析功能，不同型号之间只有性能的差异。

流量可视化

- 用户流量可视化
- 应用流量可视化
- 服务器流量可视化
- 在线解码

分析并关联OSI 2-7层所有元数据

全流量回溯

- 全流量存储
- 全流量回溯
- 溯源取证

实时分析并长期存储流量，提供任意时间点的回溯分析能力

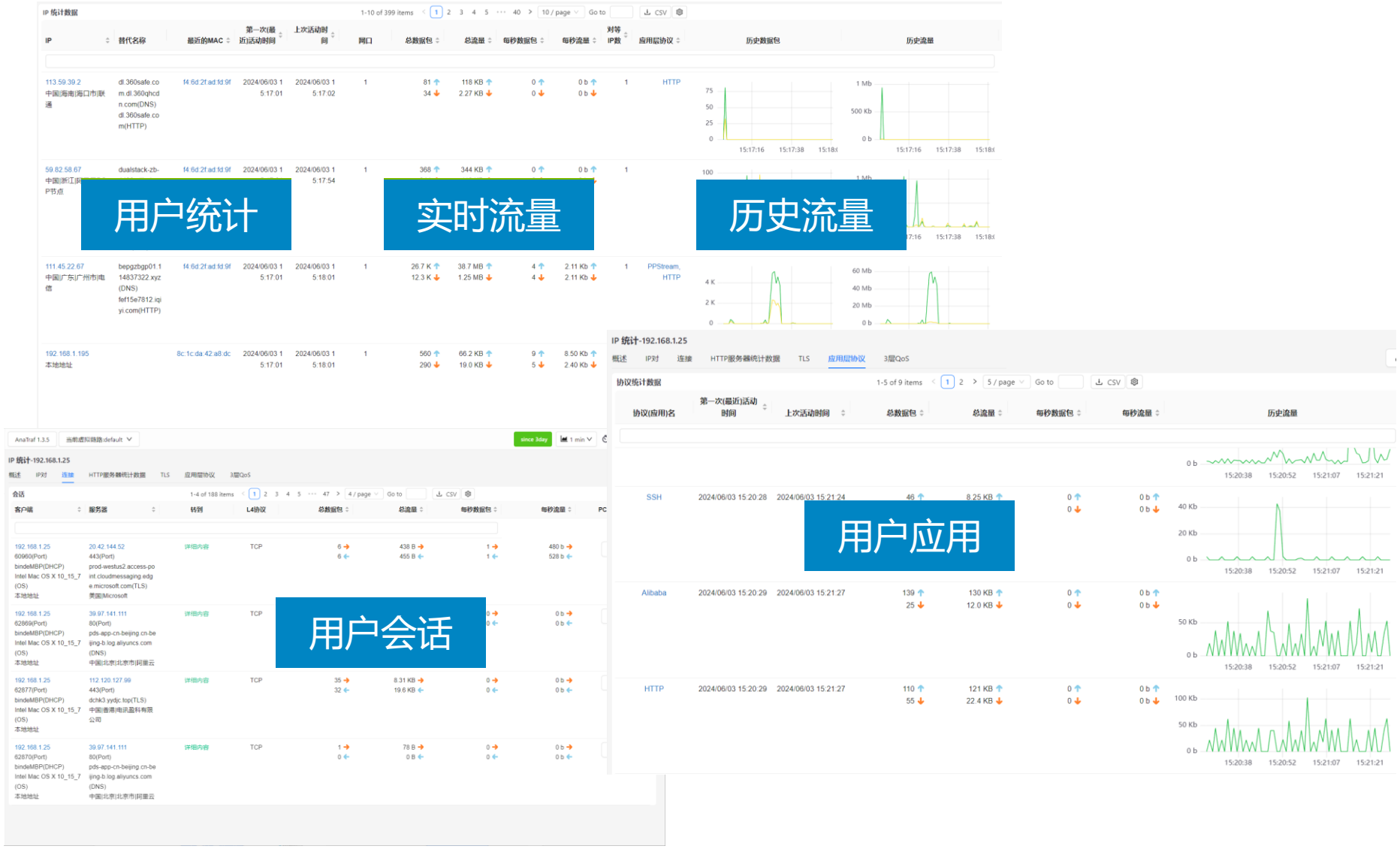
主要功能

1

流量可视化

- **用户流量可视化**
- 应用流量可视化
- 服务器流量可视化
- 在线解码

分析并关联OSI 2-7层
所有元数据



YUNZHENG TECH

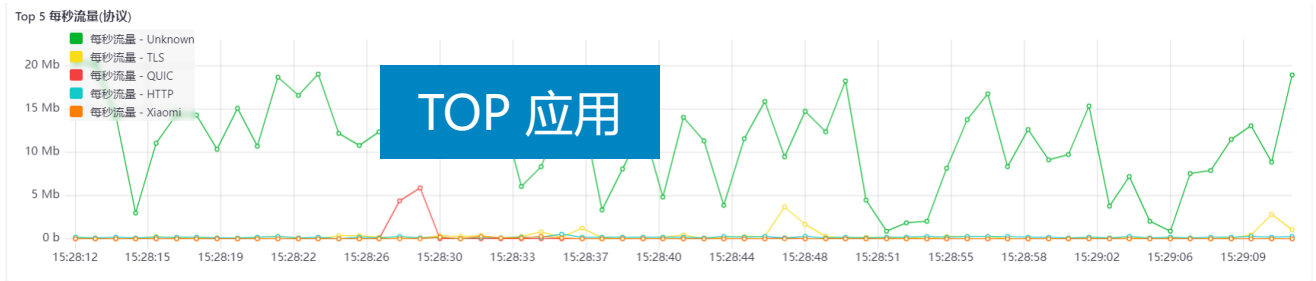
主要功能

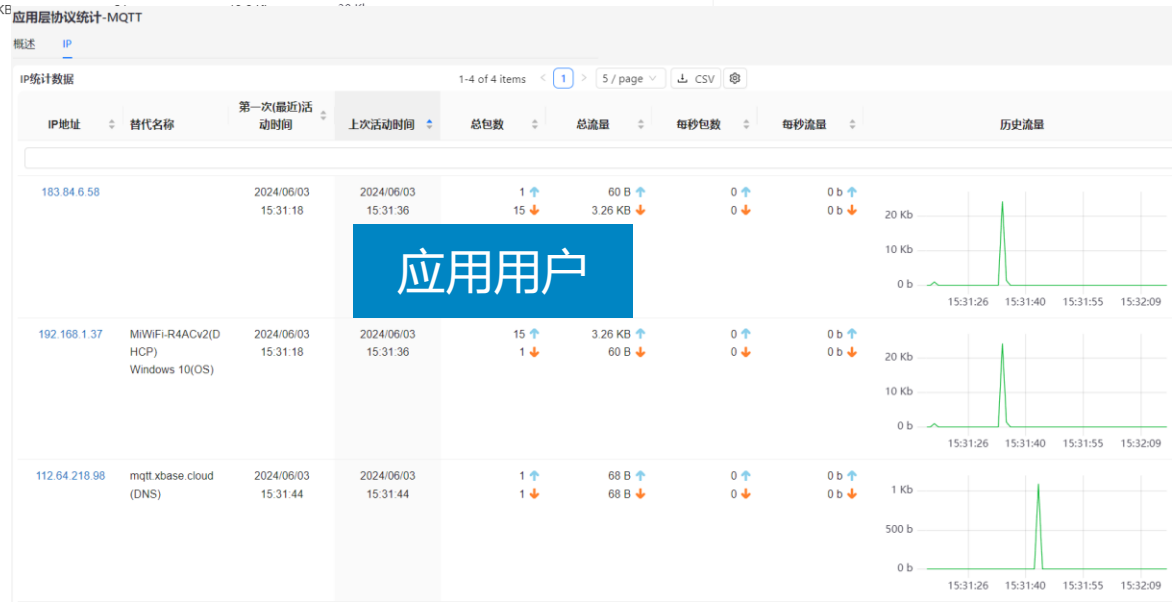
2

流量可视化

- 用户流量可视化
- **应用流量可视化**
- 服务器流量可视化
- 在线解码

分析并关联OSI 2-7层
所有元数据





YUNZHENG TECH

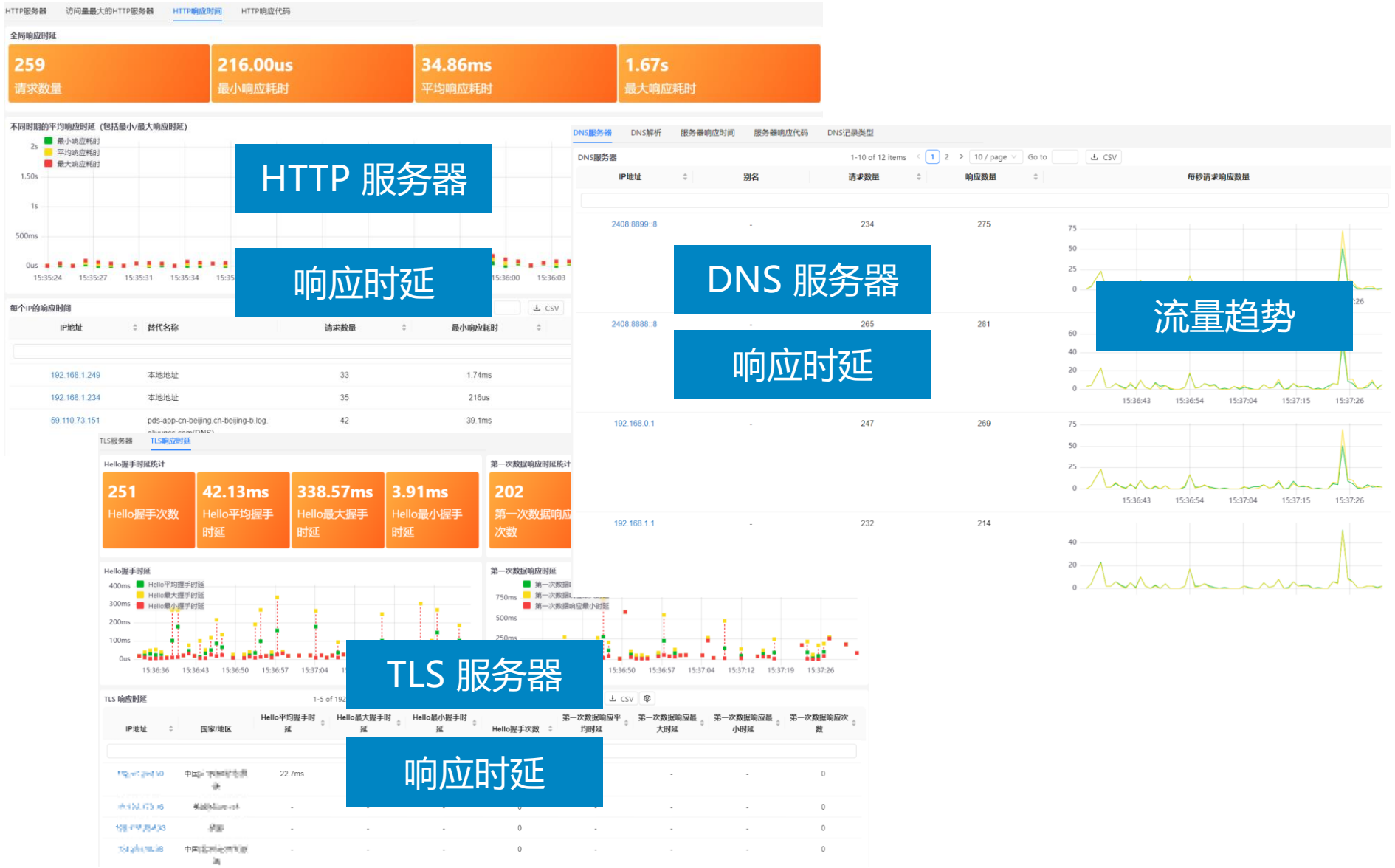
主要功能

3

流量可视化

- 用户流量可视化
- 应用流量可视化
- **服务器流量可视化**
- 在线解码

分析并关联OSI 2-7层
所有元数据



主要功能

4

流量可视化

- 用户流量可视化
- 应用流量可视化
- 服务器流量可视化
- **在线解码**

分析并关联OSI 2-7层
所有元数据

数据包在线解码分析

在线预览

时序图

流重组

YUNZHENG TECH

主要功能

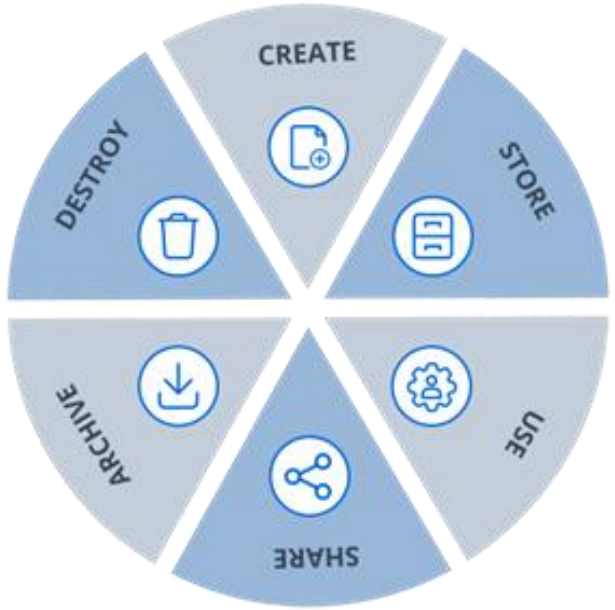
1

全流量回溯

- **全流量存储**
- 全流量回溯
- 溯源取证

实时分析并长期存储流量，提供任意时间点的回溯分析能力

大容量数据存储与检索



高速捕获

一体化设备，支持旁路、桥接部署。覆盖1G-100G网络。

大容量存储

单设备提供数百TB级原始流量存储。分布式、集群部署提供PB级存储。满足数月以至更长时间的存储需求。

流量回放

支持倍速、过滤、无损回放历史数据包，进行回溯分析。

高效检索

自研高性能内存数据库，数据秒级检索。支持基于网口、VLAN等方式配置虚拟链路接口，每条虚拟链路所有统计数据都是严格区分。

溯源分析

支持数百种协议识别。根据时间、GeoIP、连接等信息快速检索并导出原始报文，提供给安全产品。

主要功能

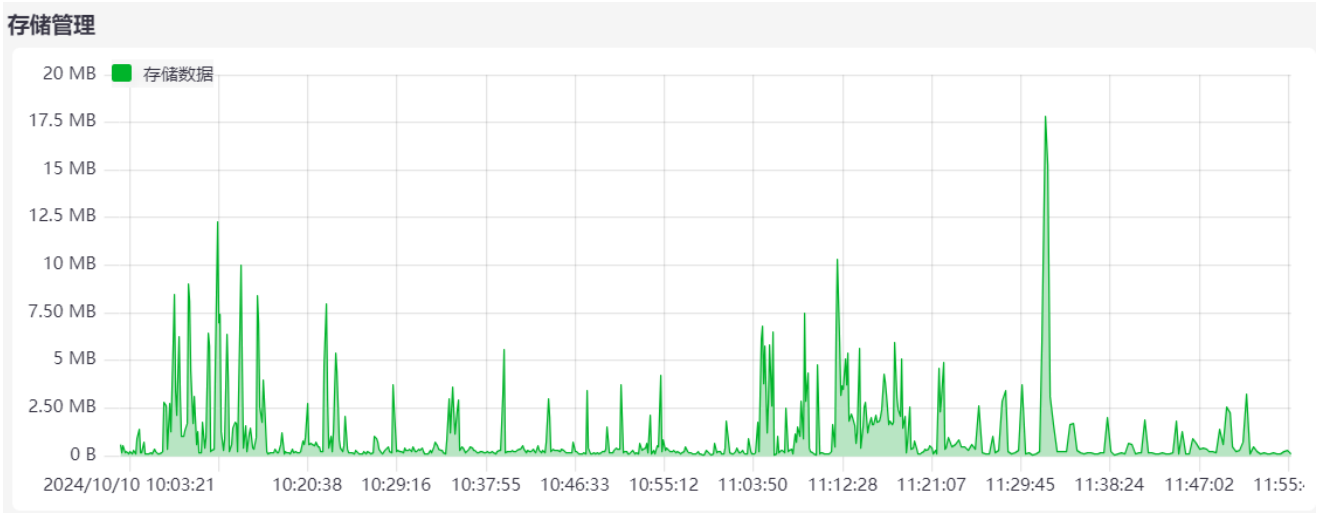
1

全流量回溯

- **全流量存储**
- 全流量回溯
- 溯源取证

实时分析并长期存储流量，提供任意时间点的回溯分析能力

满足等保测评180天流量回溯分析要求



- 在网络安全等级要求较高的网络中，需要长时间至少180天时间保存原始流量与日志信息。
- 支持长期的全流量、统计信息存储（配置足够的存储空间），满足检索、回溯分析的需求。
- 支持数据包过滤，数据包循环、滚动存储，以及数据包截断存储，节省硬盘空间。

主要功能

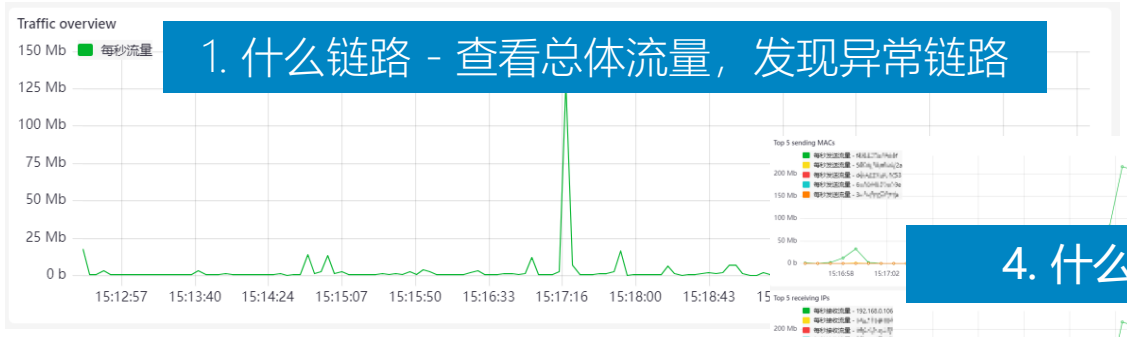
2

全流量回溯

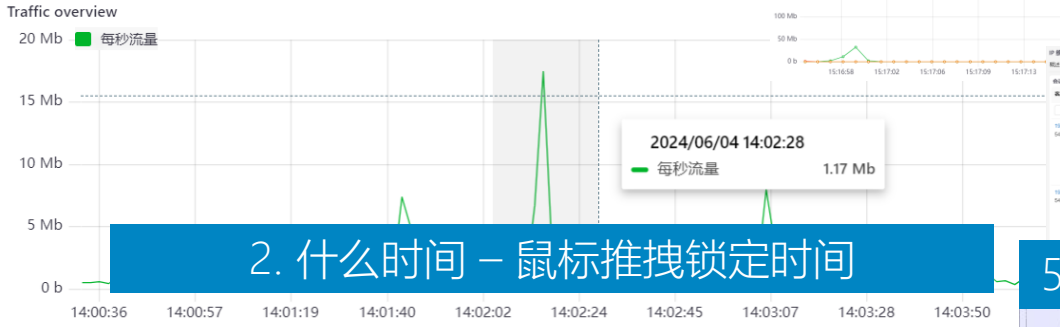
- 全流量存储
- **全流量回溯**
- 溯源取证

实时分析并长期存储流量，提供任意时间点的回溯分析能力

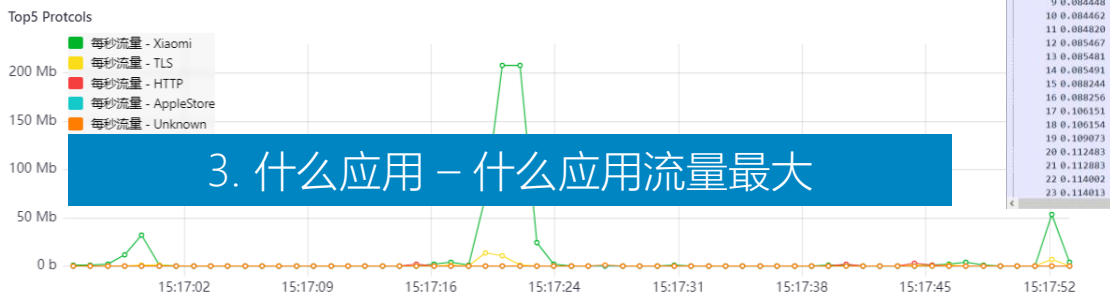
会话级流量回溯



1. 什么链路 - 查看总体流量，发现异常链路

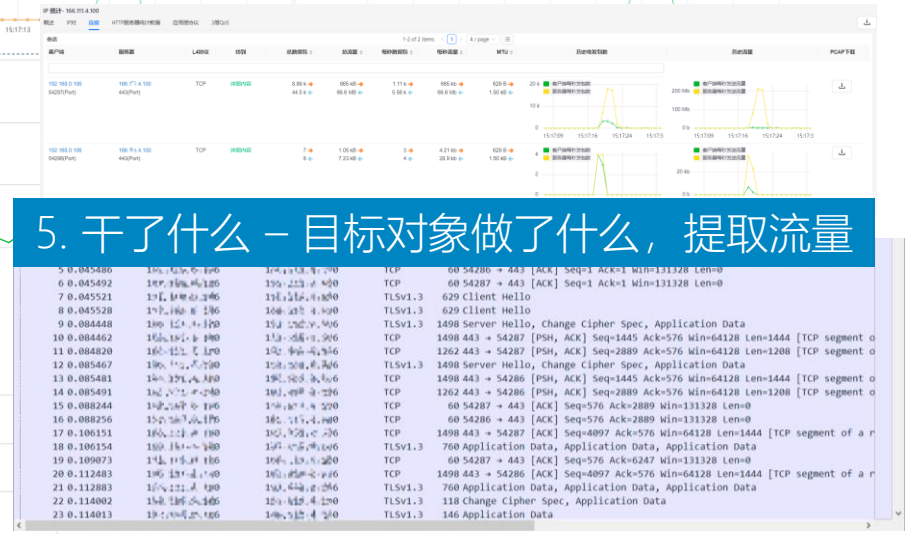


2. 什么时间 – 鼠标推拽锁定时间



3. 什么应用 – 什么应用流量最大

4. 什么人 – 谁在大量产生该应用流量



5. 干了什么 – 目标对象做了什么，提取流量

主要功能

全流量回溯

- 全流量存储
- 全流量回溯
- **溯源取证**

实时分析并长期存储流量，提供任意时间点的回溯分析能力

3

典型溯源取证方式

1	时间段+五元组等条件检索	1. 已知攻击者或被攻击者IP等线索 2. 溯源每条行为记录和攻击行为
2	检索溯源取证导出证据	1. 已知攻击者或被攻击者IP等线索 2. 对攻击行为取证，导出pcap文件
3	元数据溯源取证	1. 已知协议（HTTP、DNS等） 2. 已知攻击特征（URL、域名等） 3. 通过元数据检索取证
4	数据回放检测取证	1. 0day攻击溯源取证 2. 对历史数据进行二次检测 3. 研究攻击手法


云争
YUNZHENG TECH