钛石网络安全流量监测分析系统

2020

产品介绍

深圳市智博通电子有限公司

目 录

1

产 品 概 述

复杂环境下对于安全运维管理的期许

1.1趋势背景

01 Gartner的定义

网络流量分析（Network Traffic Analysis）NTA，以网络流量为基础，应用人工智能、大数据处理等先进技术，基于流量行为的实时分析，展示网络性能、异常事件的客观事实。

NTA 技术入选《Gartner：2017年11大顶尖信息安全技术》

02 等保2.0需求

应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的监测和分析，安全管理要求必须对受到的攻击进行回溯分析。

1.2 政策要求

7 第二级安全要求

7.1.3.3 入侵防范

应在关键网络节点处监视网络攻击行为。

7.1.3.5 安全审计

本项要求包括：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

8 第三级安全要求

8.1.3 安全区域边界

8.1.3.3 入侵防范

本项要求包括：

a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；

c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；

d) 当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

8.1.3.5 安全审计

本项要求包括：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

d) 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

表 2：新增产品和新增要求项一一对应

	新增要求项	对应产品
入侵防范	应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为	防火墙、IDS、IPS
入侵防范	应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析	流量回溯、APT
恶意代码防范	应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新	邮件防护
集中管控	应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理	VPN
集中管控	应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测	堡垒机
集中管控	应对分散在各个设备上的审计数据进行收集汇总和集中分析	日志审计
集中管控	应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理	终端安全软件
集中管控	应能对网络中发生的各类安全事件进行识别、报警和分析	SOC/态势感知
安全审计	应确保审计记录的留存时间符合法律法规要	日志审计

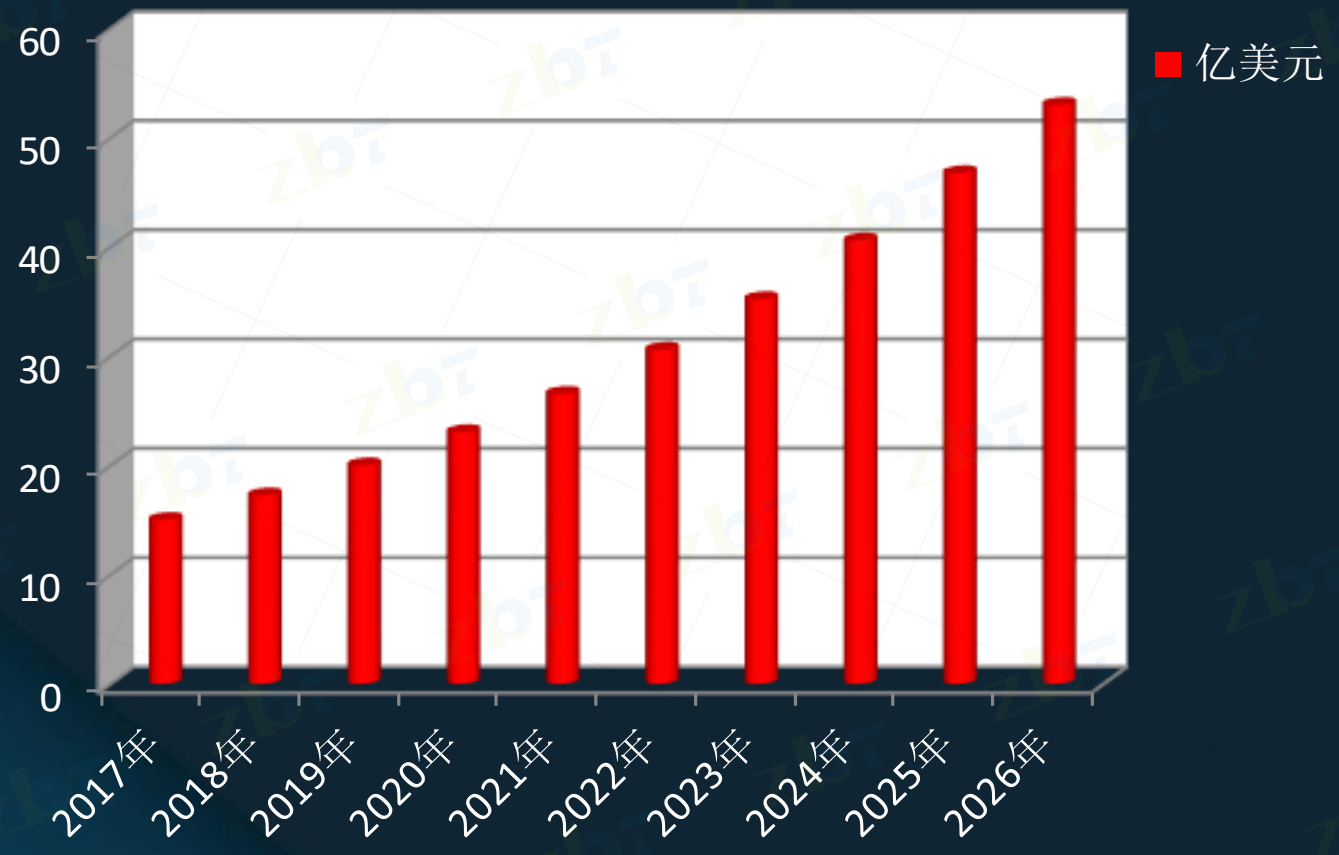
表 3：新增产品和服务市场空间超过 200 亿元

产品/服务	单价（万元）	新增数量（万）	新增市场空间（亿元）
APT	20	1.8	36
流量回溯	15	2	30
堡垒机	13	1	13
数据库审计	12	2	24
集中日志审计	20	2	40
态势感知平台	500	0.10	50
二级等保咨询服务	5	10	50
三级等保咨询服务	9	1	

数据来源：国泰君安证券研究

1.3市场预测

美国**透明市场研究公司**(Transparency Market Research)针对**2018-2026年内**的**全球**网络流量分析（NTA）市场进行了调研和展望，如下图所示：



全球现状

2017年，全球范围内的网络流量分析解决方案整体价值约为**15亿美元左右。**

发展情况

根据推测，在接下来直到2026年，其每年的增长率将高达**15.2%。**

未来产值

全球市场：

- 到2026年左右，规模将接近**53亿美元**左右。

国内市场：

- 科来18年9千万，2019年12月初1.3亿全年1.8亿，2020年计划2.5亿。
- 启明19年销售200万左右。

1.4 用户需求

溯源取证

缺乏对网络原始数据的保存与检索分析能力，缺乏内外网交互数据的关联能力，不能很好的对故障及安全事故进行溯源查证。

网络可用性

网络、业务性能健康度分析涉及应用、网络传输、端点设备等多方面，诊断难度大

攻击多样性

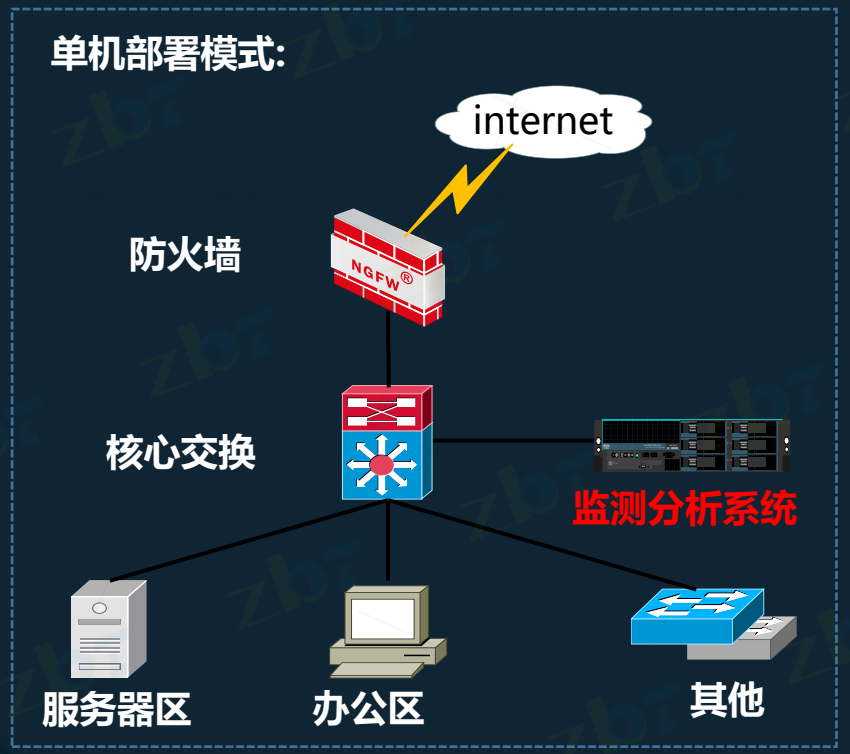
以勒索、挖矿病毒等高级持续性威胁为代表的新型攻击手段，绕过了传统边界防护设备。

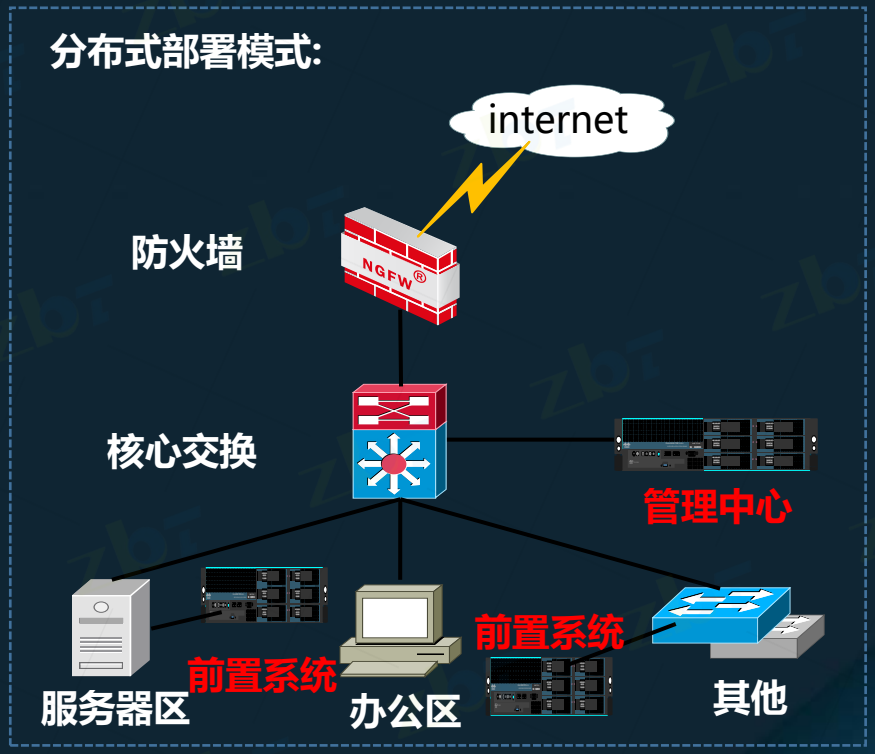
数据割裂

安全防护、流量检测、运维管理等产品的多样性，导致各类型数据割裂，无法形成立体的分析价值。

1.5 产品简介

一款全流量的深度数据包检测设备，2至7层用户通信数据报文还原分析，呈现**态势感知、流量透视、回溯分析、性能监控、安全检测、资产管理、漏洞扫描、病毒检测**八大主体功能，通过设备联动与功能扩展，还可实现拓扑管理、专题分析、机器学习建模分析、攻击反制，无损探测、异常文件识别和还原、攻击链还原、主动测量、工控网络监控等功能，打造一体化网络综合、智能化监测分析解决方案。





产品资质：已经通过GBT 20945-2013 信息安全技术 信息系统安全审计产品技术要求和测试

1.6 产品型态

产品型号配置参考（服务器平台）					
型号	吞吐	机型	固态硬盘	硬盘	接口(1个接口接一条镜像链路)
NAT-500	500M	2U	256G	4*2T （SATA）	4个千兆电口，含raid卡
NAT-2000	2G	2U	256G	8*2T （SATA）	4个千兆电口，4个千兆光口，含raid卡
NAT-5000	5G	2U	256G	8*4T （SATA）	4个千兆电口，4个千兆光口，含raid卡
NAT-10000	10G	2U	256G	8*6T （SATA）	4个千兆电口，4个万兆光口，含raid卡

其他支持：40G网络流量场景，100G网络流量场景，国产化场景等。

已经完成海光CPU适配认证的硬件平台

1. 网络流量分析与异常检测能力
2. APM应用性能分析能力
3. 主动协同测量能力
4. 智能边缘网络探测能力
5. 大数据存储与分析能力
6. 第三方接口管理及数据处理能力
7. 网络流量回溯分析能力
8 资产发现及管理能力
9 大屏数据展示能力
10. 异构数据处理与分析
11. 专题分析能力
12. 远程升级管理能力
13. 分权分域分布式部署能力
14. 物联网：隐私保护
15. 加密网络行为分析
16. 流量分层透视
17. 应用协议识别
18. 资产识别和漏洞扫描
19. 安全情报引擎
20. 基于DNS的受控主机发现
21. 未知威胁检测
22. 摄像头等物联网设备发现和防护
23. 在线病毒传播和阻断
24. 应用、用户、网元分析
25. 安全态势
26. 工控协议识别和解析
27. 业务系统分析

1、产品支持软件部署模块化，动态加载、按需部署；

2、支持硬件载体多样化，标准X86服务器、工控机、网关设备、AP设备等；

3、依据不同的网络环境，不同的用户需求，将不同模块部署在各类别硬件载体上，实现用户所期待的产品价值与能力输出。

模块化，轻量化，场景化！

1.7 核心功能组成

01 流量分析

流量轨迹分析，上网行为分析，
异常流量检测。

02 安全检测

病毒检测、漏洞检测、攻击检测等安全事件分析。

04 性能分析

网络性能分析，业务性能分析，
业务系统可用性分析；
设备、链路管理分析。

03 溯源取证

原始数据报文解码分析，安全事件数据取证分析，
会话日志回溯分析。

1.8 产品优势

集中性

- 集中数据关联：支持网络流量数据与业务性能、安全事件及资产的集中关联分析，多角度下钻分析与定位；
- 集中资产管理：链路、设备资产、业务系统统一平台的综合分析。
- 集中态势感知：流量态势、安全态势、性能态势、资产态势、威胁态势全局掌控。

专业性

- 深度分析：最细粒度的全流量、性能、安全监测分析，全网拓扑管理；
- 自有技术：实现端到端测量、数据包处理、硬件加速、精确业务识别、网络行为建模、安全事件关联分析；
- 核心引擎：拥有各类独立的应用识别特征库、安全规则数据库、地址库、URL库、终端库等。

适应性

- 本地业务：支持超过30种以上自定义业务识别引擎，监控单位内部自有业务；
- 多样环境：支持不同速率的以太/PoS/ATM等网络环境；可根据客户需求灵活部署，适应不同规模的云平台、企事业单位、多分支机构及全国性大网；开放共享：提供开放、通用、透明的数据查询分析接口，和第三方系统融合。

扩展性

- 多元化数据来源，主被动联合监测：镜像流量，主动测量，snmp网管，资产发现等，日志采集等；
- 虚拟化探针与云端部署，独立/分布式部署，支持SDN/NFV；
- 支持扩展工控监测、流量控制、攻击溯源反制、威胁文件还原等功能；

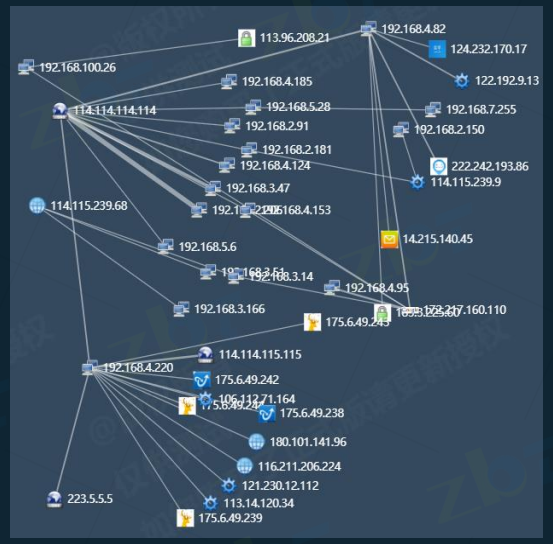
2

功 能 介 绍

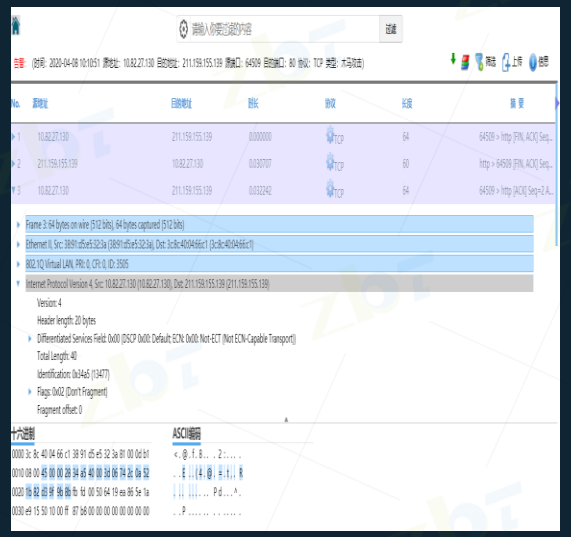
以问题为导向，以场景为目标

2.1 流量分析

IP资产



会话记录



报文解码

应用访问

2.2 安全监测

漏洞扫描（5W+）

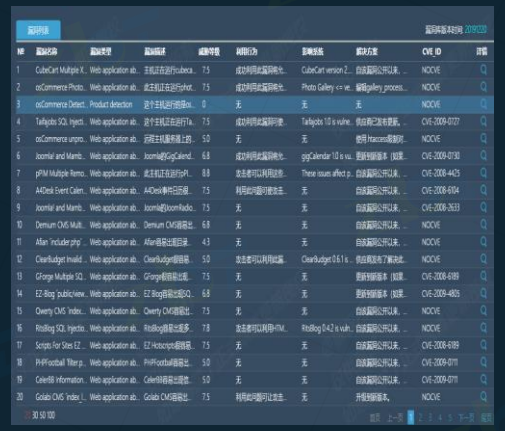
可检测缓存溢出、ROP、堆喷射等漏洞利用行为的检测。

异常分析（协议识别2400+）

结合流量、性能、资产等数据信息检测网络环境中出现偏离阈值或正常模型的异常流量、异常用户行为、异常资产事件。

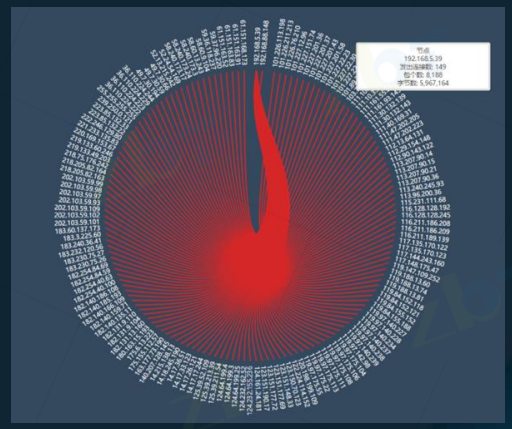
攻击检测（5W+）

包含勒索病毒、挖矿木马、蠕虫攻击、暴力破解、远控木马、恶意软件等。



病毒检测（800W+）

实时检测网络中传输（下载/上传）的木马、病毒和恶意软件。。



协议库、安全规则库、漏洞库、病毒库均支持每周在线更新，针对内网环境支持离线升级。保证规则的实时性与有效性！！

2.3 性能分析

服务健康度评分

设备、链路管理分析

应用价值：
门户网站等web系统分析；
网络卡顿分析；
网络行为分析；
安全事件分析；
资产状态分析；
……

网络状态分析

主流应用访问记录分析

2.4 回溯分析

会话记录分析

保存2-4层所有数据并图表化呈现，
易于用户查询与分析。

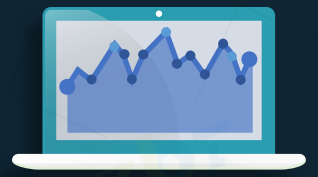
应用记录分析

保存所有主机的对外访问的主流应用记录，
实现用户行为的精准溯源。

原始报文

保存所有风险主机的风险报文，
在进行安全事件总结分析时提供
完整的证据链。

2.5 资产中心



流量分析

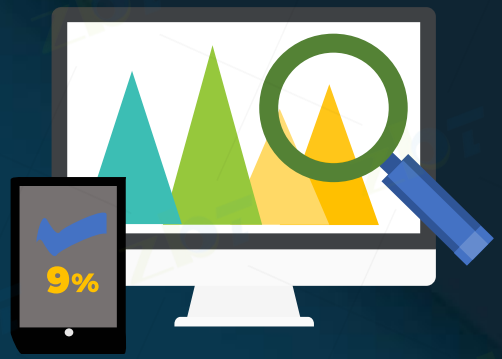
1、流量轨迹分析;
2、网络行为分析;
3、数据回溯分析;

安全检测

1、攻击检测分析;
2、漏洞扫描分析;
3、病毒检测分析;
4、异常流量分析;

性能监控

1、网络性能分析;
2、业务性能分析;
3、基于SNMP设备管理;
4、服务健康度综合分析;



资产为核心实现多维分析管理。性能、流量、安全构建三角分析模型，综合评估资产风险状态的同时呈现流量维度分层流量、用户数、老化流、新增流、并发流异常分析，性能维度时延、丢包率、拥塞率、http响应成功率、dns请求成功率、sip通话数、Oracle/mysql/pop3登录成功率异常分析，安全维度IDS攻击方与被攻击方场景分析、漏洞扫描与指纹特征分析、病毒及威胁文件还原分析的多层评测。

2.6 案例之内网主机非法外联

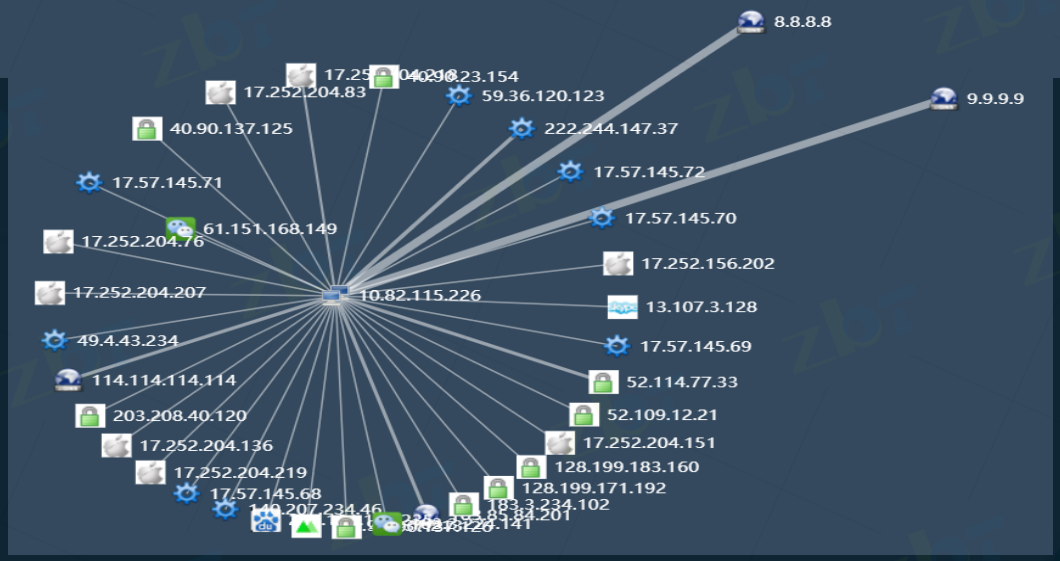
筛选工具 | 10.82.115.226 | 36.110.147.35 | 所有告警 | 所有级别 | 高级选项 | 自定义时间

用时0.124秒，约1条记录 导出

时间段：2020-04-01 08:30:00 ~ 2020-04-01 11:30:00

№	记录时间	源地址	目的地址	源端口	目的端口	协议	处理方法	告警信息	告警类型	告警级别	数据包	白名单
1	2020-04-01 09:11:16	10.82.115.226	36.110.147.35	1194	80	TCP	allowed	疑似伪装成搜狗的特洛伊木马	木马攻击	严重		

尾页



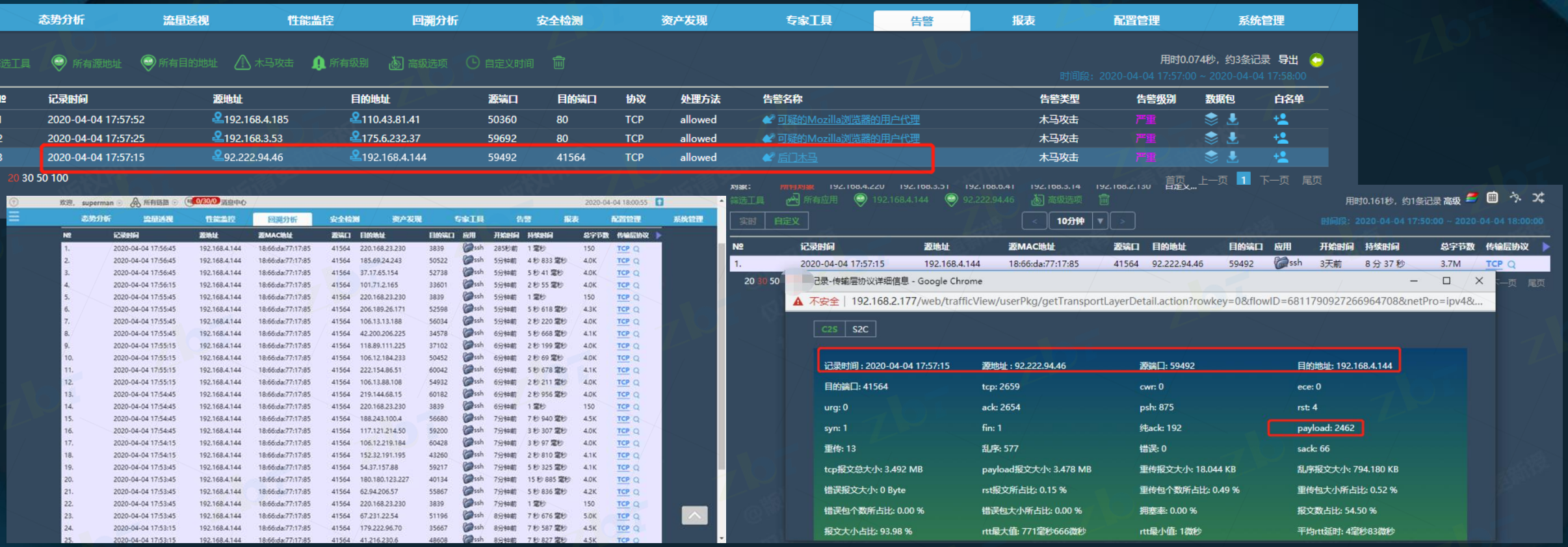
某政务网络安全问题分析

1、在核心接入所有汇聚的镜像点资源。

2、客户的公网IP被被通报有非法连接的行为，通知告知了目的IP、端口与时间。但是客户没办法溯源到具体的用户并进行分析？？

3、通过我们的设备直接定位到了内网的用户IP，同时提供溯源取证分析的数据支撑。

2.7 案例之SSH暴力破解

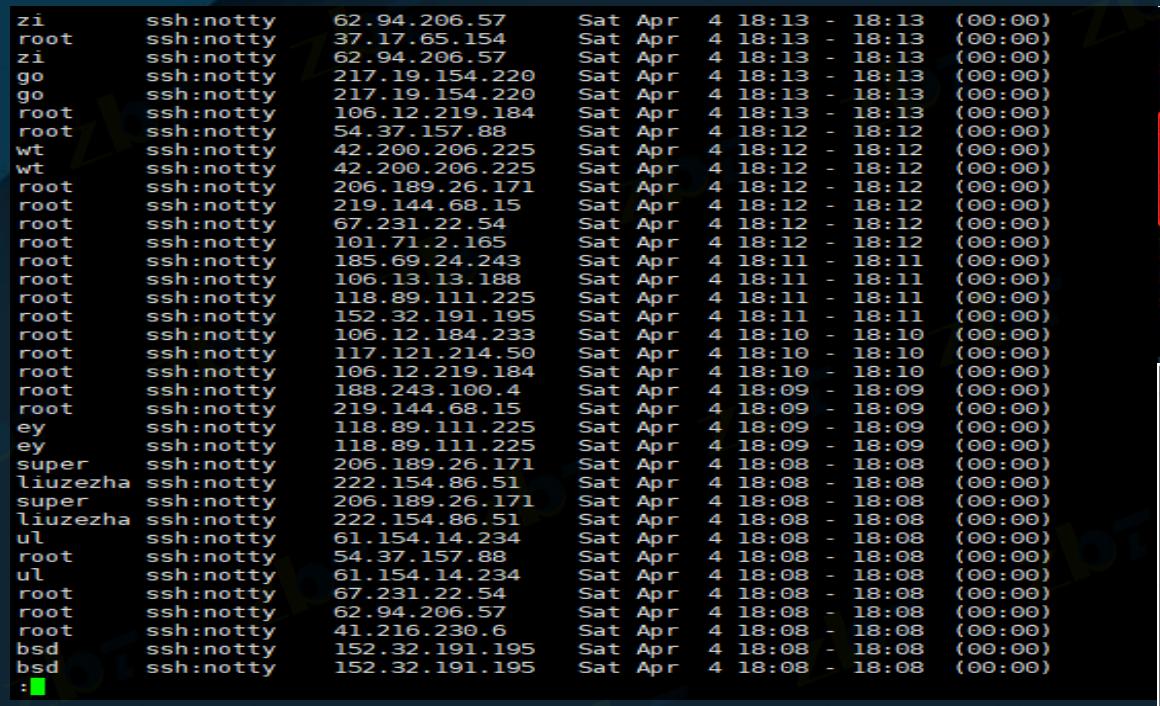


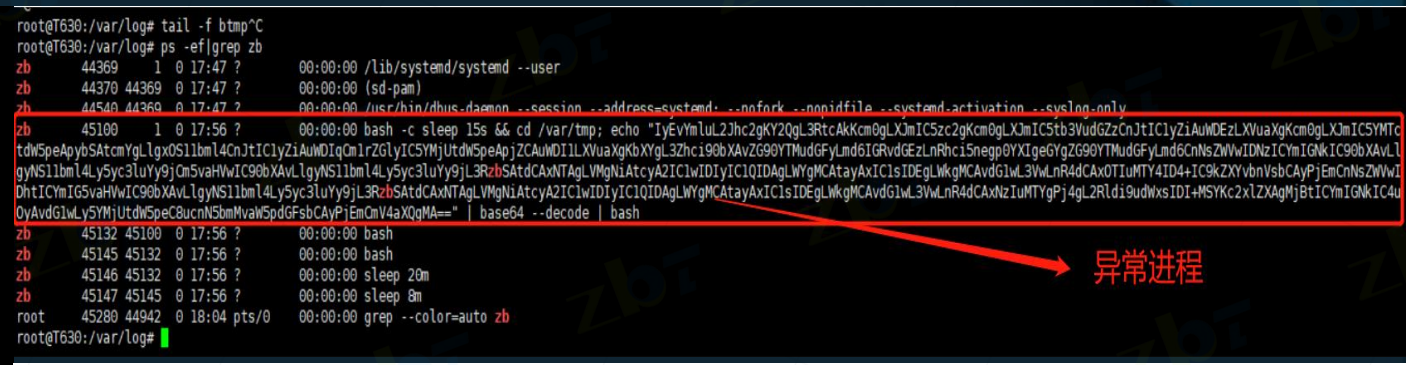
某企业安全事件分析

1、在核心接入所有汇聚的镜像点资源。

2、192.168.4.144为客户一台重要的服务器，邮件通知木马攻击，攻击IP为92.222.94.46，为法国的IP；

3、通过当时的系统数据分析，非法用户登录系统的SSH连接并成功，发现payload大小有3M多，推测在传输后台木马的文件到入侵了的服务器；





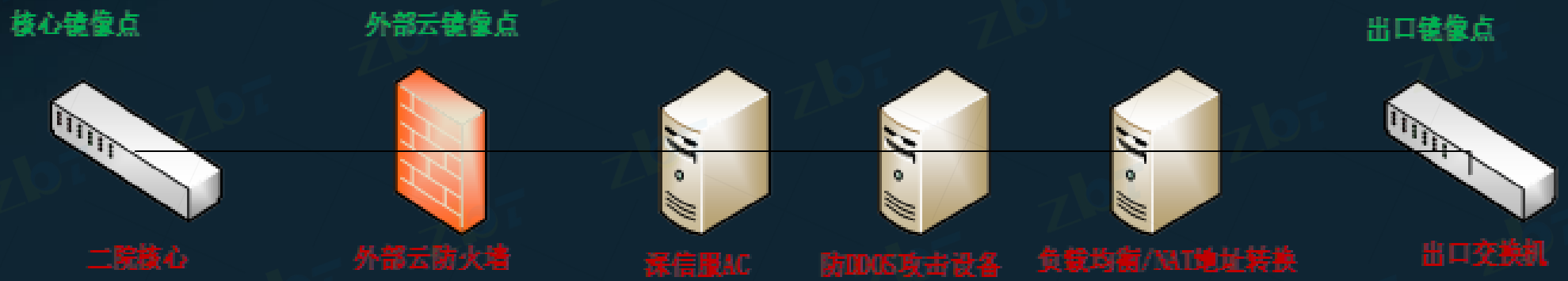
4、登录被入侵服务器查看，发现已经有很多国外IP在尝试登录这台机器的ssh，且登录失败。当时应该是在暴力破解；

5、系统中有一个zb用户使用的是弱密码，我们首先判断zb用户被暴力破解，使用zb用户登录发现了异常进程，该账号被破解成功；

6、通过排查发现，在服务器的zb用户的家目录 /home/zb/.ssh/authorized_keys这个文件里面被添加了公钥，留了后门，这种情况下，以后黑客就可以实现免密码登录我们的服务器；

7、通过对整个事件的分析，在杜绝后续隐患的同时也使客户对安全管理有了更深刻的理解。

2.8 案例之业务偶现断连分析



某局网络长连接业务偶现掉线网络问题分析

1、在核心、防火墙、出口接入三个镜像点资源；

2、当出现问题后，我们通过回溯TCP指标的连接数据，发现在出口侧数据与防火墙、核心侧数据差异很大，出口侧有收到服务端的报文，到防火墙、核心侧时该报文却丢失了导致客户侧发起重传；

3、发现主要原因就在于客户端或服务端连续两次及两次以上发包均没有收到服务端或用户端的回复，从而触发重传模式，因为中间网络存在丢包的现象，导致客户端依旧没有收到服务器端的回复最后执行RST操作，从而导致业务掉线；

4、通过网络性能路径指标分析，找出问题主要在负载均衡。

2.9 竞争力分析

25%

基于flow的流量产品

1、数据来源简单

2、无性能分析，安全能力非常弱

50%

基于DPI的流量产品

1、有流量，有安全，有资产

2、有流量、有性能

3、有流量、有回溯

75%

方案级解决方案

1、多产品联合

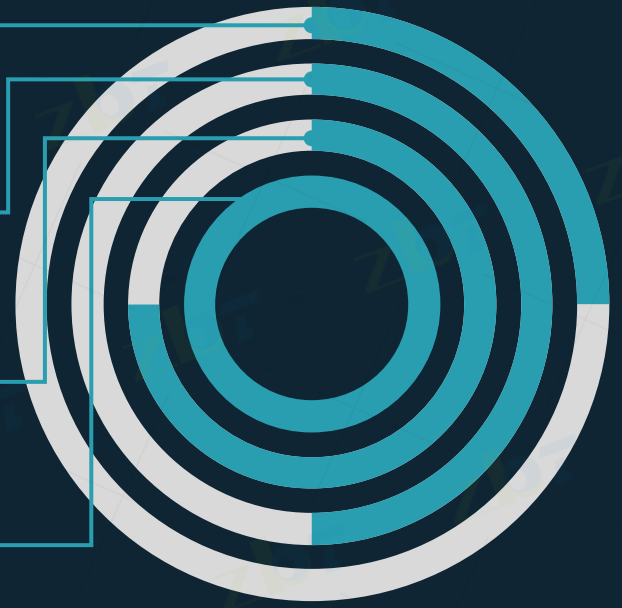
2、缺乏集中管理概念，综合分析能力较弱。

100%

全方位驱动型产品

1、多维数据来源，主动、被动……

2、有核心概念，建立综合数据分析模型。



2.10 友商产品分析

我方核心优势

多样化数据来源。如镜像流量、主动探测、网管数据等，综合安全分析模块、性能分析模块、流量分析模块，建立深度的数据分析模型。最终实现数据的场景化分析目标，做有效的数据呈现。

01

成都科*类似产品

1、产品体系涵盖回溯、性能、安全三个方面，数据解码呈现能力比较强；

2、在易用性、完整性上有一定的欠缺；

3、没有资产属性分析概念，没有主动数据来源；

02

深圳深**类似产品

1、在界面呈现、威胁情报联动、深度检测能力比较突出；

2、基于回溯、性能、运维管理等综合监测偏弱；

03

北京奇**类似产品

1、产品主打资产与安全概念，所有产品主要在安全方向；

2、没有结合业务关系做全局分析，缺乏业务层面信息呈现；

04

北京东*软件类似产品

1、基于flow数据采集分析不精细；

2、流量、安全分析粗放，无性能与资产属性分析；

2.11 控标策略

回溯分析系统、流量分析系统

1、使用流量分析、数据包解码、网络性能分析、原始报文保存指标应标；

2、资产综合分析、资产指纹特征、漏扫指标控标；

APM、NPM系统

1、使用网络性能分析、业务性能分析、业务系统健康度评估、链路指标关联分析、数据包解码功能应标；

2、资产综合分析、资产指纹特征、安全指标控标；

威胁态势感知、全流量安全分析系统

1、使用病毒检测、漏洞扫描、攻击检测、异常流量分析、数据包解码、资产综合分析应标；

2、业务健康度分析、网络性能分析、业务性能分析关联资产分析控标。

3

行 业 案 例

突出的行业应用效果

3.1 护网行动

在实际护网工作中，安全事件的处理一般分为以上五个部分。

1、多个厂家，不同类型产品，多重异构的数据分析。

2、最终通过收敛攻击面、漏洞补丁修补、建立纵深防御体系、回溯分析等手段解决分析问题。

流量分析系统可以从第一步骤开始参与直至整个攻击事件的总结分析完成，伴随护网工作全阶段需求的实现！

3.2 电力行业

- **项目背景**

规模：**省级调度数据网分为核心层（中调主、中调备）、汇聚层（地调主、地调备）和接入层（各变电站和用户站）各层通过两台路由器虚拟化冗余组网，实现省、市、县三级区域网络的全覆盖。**网络实时性要求较高：**调度数据网传输的是调度自动化核心业务数据，如何提供有保障的端到端延时，保障电网调度系统安全、可靠、稳定运行是客户关注的重点。

- **解决方案 （综合管理平台+10G高端设备+拨测探针）**

1、分布式部署：采用端口旁路镜像方式将**流量采集探针**连接至省中调和省备调的两台调度数据网业务接入路由器上，实现对调度数据网业务流量的监控;

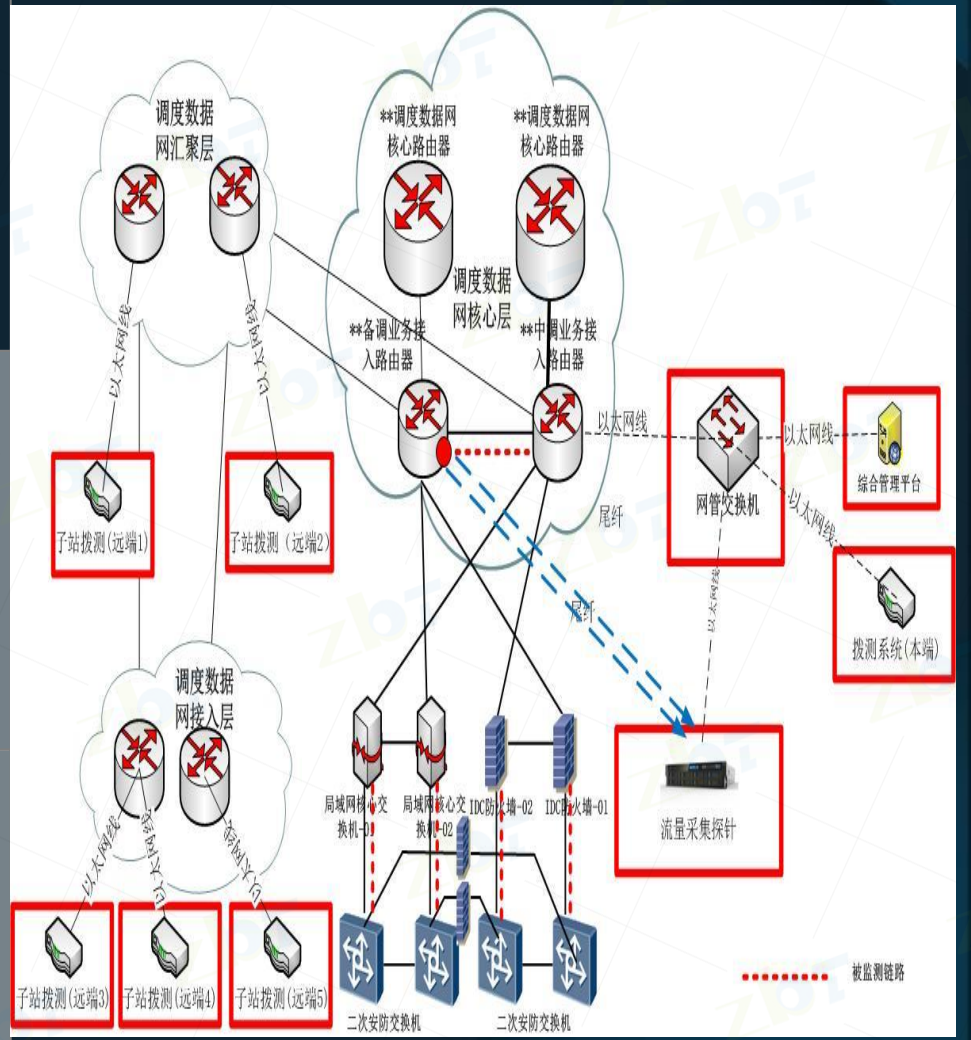
2、在中调配置统一的**综合管理平台**，负责**流量采集探针**和**拨测探针**的管理，在本端中调和备调核心位置、在远端接入层通信机房220KV长流站汇聚等位置分别部署拨测探针实现7X24小时端到端网络性能分析。

- **客户收益**

1、对各节点与链路的实时在线监测，实现网络故障的秒级响应；

2、主被动监测的结合，当出现问题时拨测探针能直接定位到故障点，流量分析探针数据报文的解析定位故障原因，快速解决问题；

3、提升工作效率，减轻运维成本。



3.3 高校行业

- **项目背景**

1、流量大：出口上网流量平均2G,学生上网人生较多;

2、架构复杂：学校网络架构复杂，大二层架构和三层架构共用，故障定位困难;

3、上网慢：学校老师和学生经常反应上网慢，无法打开网页。

- **解决方案 （5G中端设备）**

1、单机部署：在校园网核心、出口各取一个镜像点资源，核心采集下行口数据，出口采集上行出口数据;

2、设定出口流量阀值，设定出口流量预警，根据网段设定群组，识别特定流量;

3、对全网性能进行监控，开启安全检测模块，保存所有数据7天;

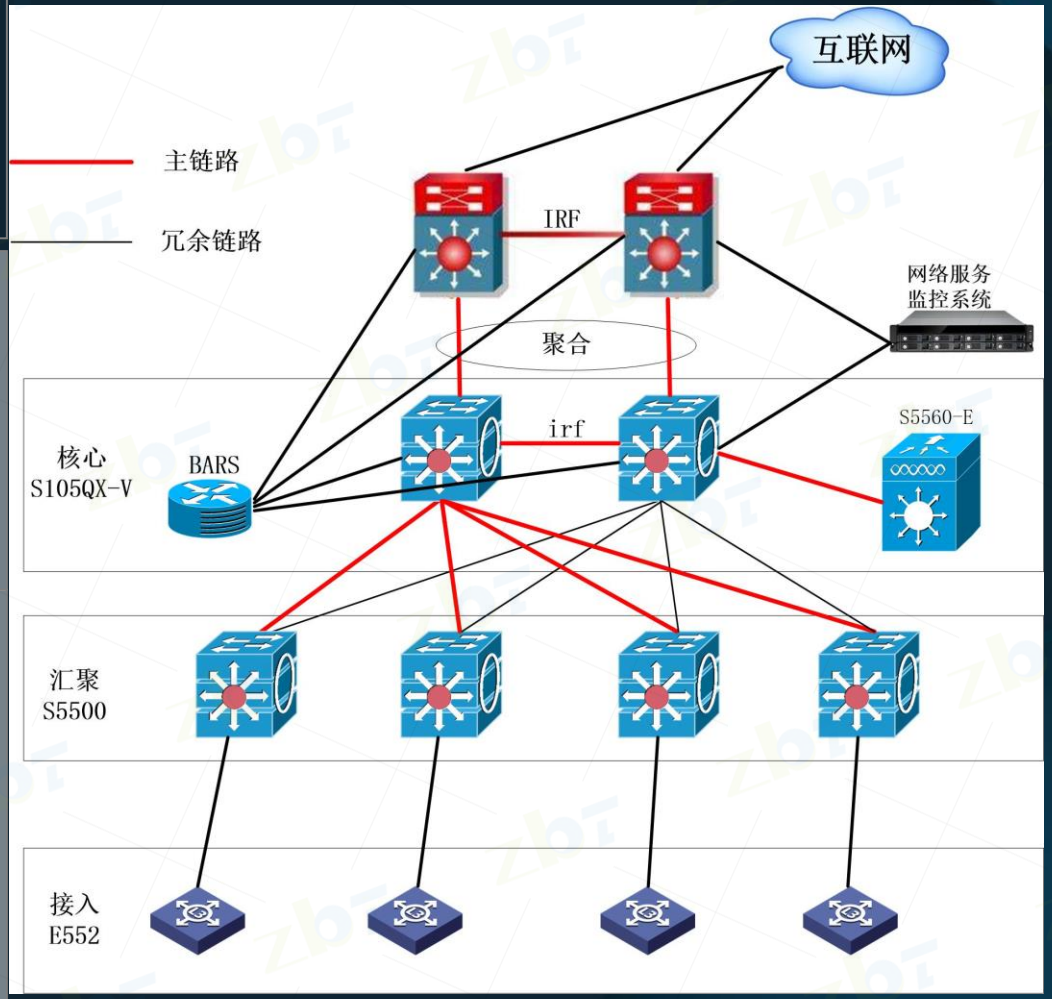
- **客户收益**

1、梳理学校出口带宽资源，科学规划带宽容量，杜绝资源浪费;

2、多节点数据采集，快速定位用户上网故障原因，有效减少故障响应处理时间，降低运维成本，提升用户满意度;

3、针对出口，核心所有交互数据进行深度的安全检测，保障内网信息安全，当有问题时能及时推送告警信息，提高响应效率;

4、提供详细的流量、性能、安全报表科学评价校园网络健康程度，有效提升信息化建设管理水平。



3.4 政府行业

- **项目背景**

1、规模大：作为从事政府网络（电子政务）建设和提供综合信息服务工作的省人民政府直属正厅级事业单位，其网络架构复杂，规模庞大，省直单位用户和外网用户众多，提供应用服务复杂；

2、流量大：两个机房总出口流量达4G，并发数130W，对内提供省直单位出局上网服务，对外提供省政府门户网站、相关应用系统查询访问等服务。

- **解决方案 （2台10G高端设备）**

1、集中部署：二院部署一台设备，在总出口、总核心、外部核心三个位置镜像流量；

2、IDC机房部署一台，在外部核心、外部出口、内部核心三个位置镜像流量；

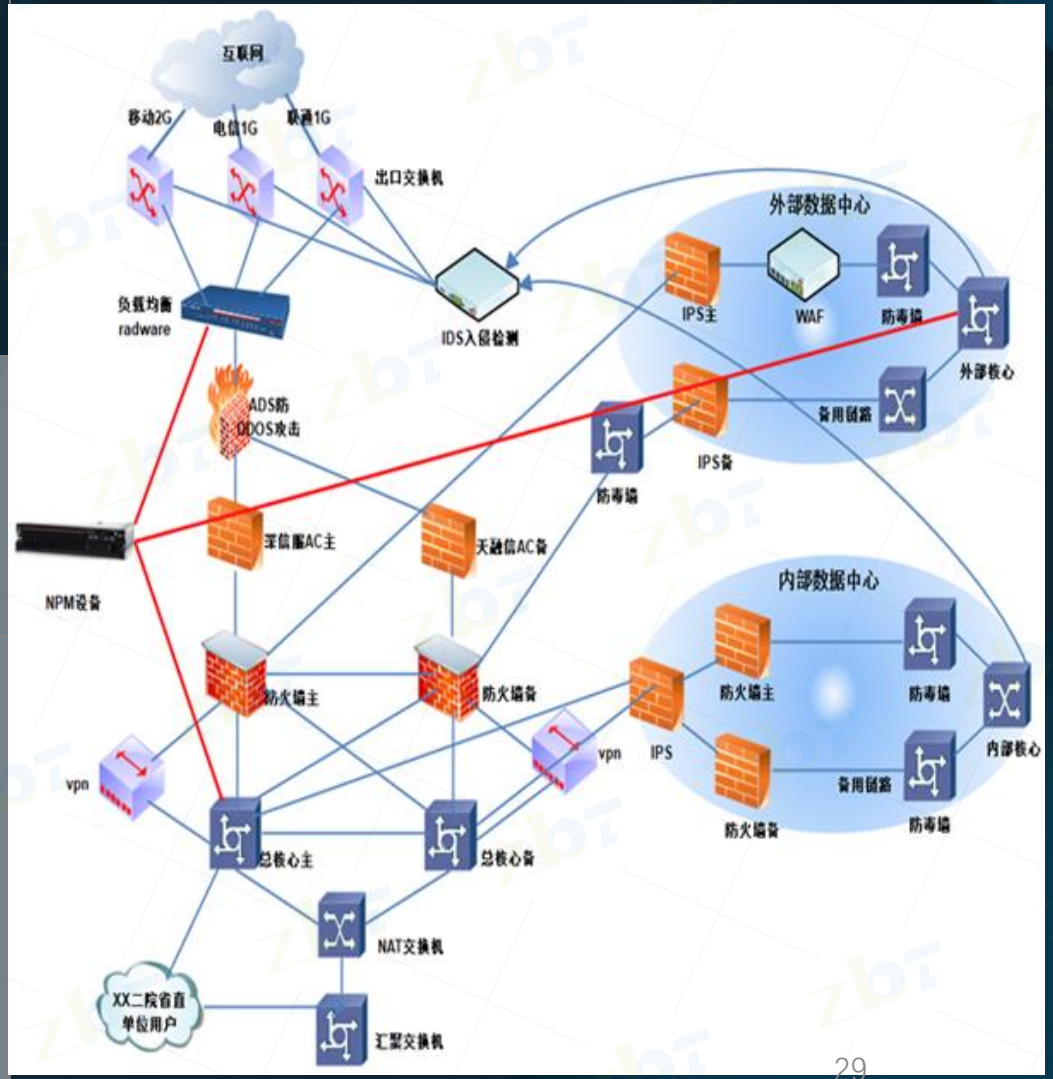
3、主要使用性能分析模块，保存所有数据7天；

- **客户收益**

1、全面监控溯源所有省直单位用户上网体验情况，根据网络性能指标科学评价用户网络性能状态；

2、多节点数据采集实现性能路径分析，根据各节点网络性能指标有效区分网络故障责任边界；

3、提升运维人员应对网络故障处理能力；



3.5 其他

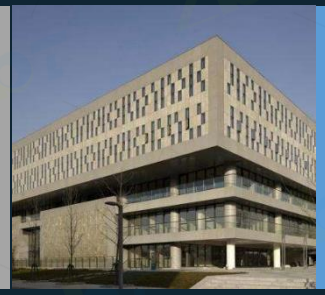
场景一：政府机关类

省高级人民法院、省政府、水利部**委、海关总署、**省电子政务中心、**武警总队、**公共资源中心、**省环保厅、**铁路运输法院、**省卫生防疫等

场景二：高校/科研院所

•*华大学、*南大学、东*大学、**理工大、GL电子科大等

•中国科学院、深圳**实验室项目、数据所、中国**技术研究院、中国**科技集团等



场景三：金融行业

YG保险集团、大同**、**银联、**银联、广西**、**信诺、**邮政、**农商银行、**浦发银行

场景二：医院医疗

武汉**医院、
**人民医院、
**医学院附属医院、
阳江**医院、
**省肿瘤医院

场景四：电力行业

国家电网公司（11省）
南方电网（5省）
**调度数据网
**综合数据网
**电科院

场景六：军队

*****基地
******军种
*******军事院校
******战区

场景七：运营商

NMG移动、
HB市电信、
HHHT市移动、
SY市移动、
AM电信

场景八：企业

•南京JX、XY集团、*车网、**国银、南方航空公司、YX集团、建信资管、**租赁、*众网、深圳市*道科技、*美达科技、广西*源行电子信息股份有限公司

场景九：其他

中石油**油田
**电子集团
**铁路集团公司
**

4 等 保 应 用

等保利器！

4.1 等级保护基本要求


网络安全等级保护基本要求
(安全通用要求)
技术要求
管理要求
安全物理环境
安全通信网络
安全区域边界
安全计算环境
安全管理中心
安全管理制度
安全管理机构
安全管理人员
安全建设管理
安全运维管理
物理位置选择
物理访问控制
防盗窃和防破坏
防雷击
防火
防水和防潮
防静电
温湿度控制
电力供应
电磁防护
网络架构
通信传输
可信验证
边界防护
访问控制
入侵防范
恶意代码和垃圾邮件防范
安全审计
可信验证
身份鉴别
访问控制
安全审计
入侵防范
恶意代码防范
可信验证
数据完整性
数据保密性
数据备份恢复
剩余信息保护
个人信息安全
系统管理
审计管理
安全管理
集中管控
安全策略
管理制度
制定发布
评审和修订
岗位设置
人员配置
授权和审批
沟通和合作
审核和检查
人员录用
人员离岗
安全意识教育和培训
外部人员访问管理
定级和备案
安全方案设计
产品采购和使用
自行软件开发
外包软件开发
工程实施
测试验收
系统交付
等级测评
服务供应商选择
环境管理
资产管理
介质管理
设备维护管理
漏洞和风险管理
网络和系统安全管理
恶意代码防范管理
配置管理
密码管理
变更管理
备份与恢复管理
安全事件处置
应急预案管理
外包运维管理

4.2 产品应用


运营商1
运营商2
Internet
Internet
内网服务器区域
外网区
情报防护
DMZ服务器区域
可信接入
子系统
应用服务器
接入交换机
Web防护
子系统
DDoS防护
子系统
路由器
情报中心
应用区域
汇聚交换机
Web防护
子系统
DB服务·器区域
入侵防护
子系统
内网办公区
接入交换机
防火墙
数据库备份系统
数据库服务器
数据库审计
子系统
行为管理
汇聚交换机
用户接入
可信接入
子系统
核心交换区
核心交换机
运维管理区
安全监控区
流量及性能分析
子系统
资产探测
子系统
回溯分析
子系统
日志审计
子系统
威胁态势感知
漏洞评估
子系统
病毒检测
子系统
APT威胁检测
子系统
综合监测平台
安全管理平台

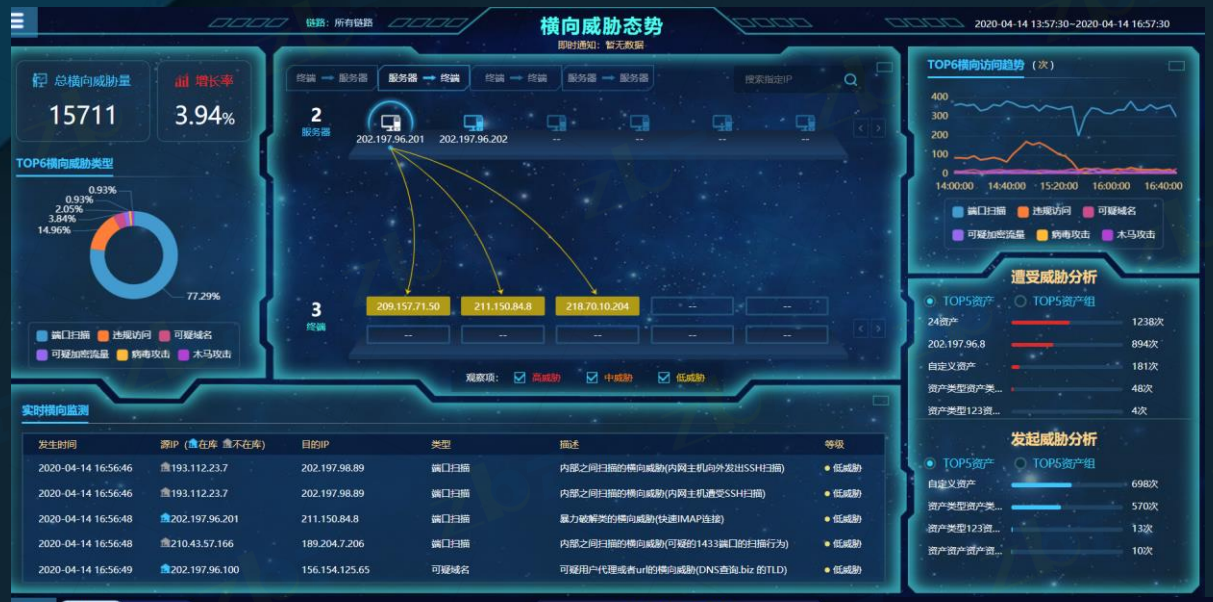
4.3 系统呈现（资产态势）

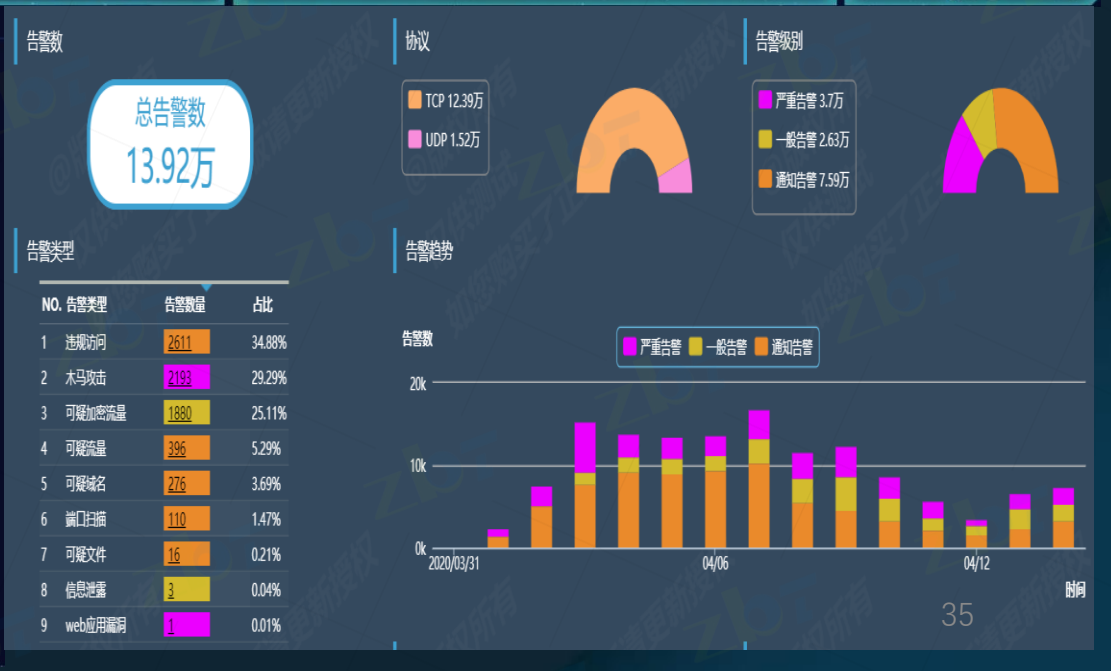

资产态势
[专用分组交换机] 202.197.96.100处于失陷状态，需及时处理
2020-04-14 14:05:30~2020-04-14 17:05:30
总资产量
20
总异常资产
3
资产发现
发现时间 识别方式 在线数量 离线数量
2020-04-14 14:19:32 手动操作 11 9
2020-04-14 14:01:45 手动操作 无变化 1
2020-04-14 13:54:08 手动操作 1 1
2020-04-14 13:54:01 手动操作 1 无变化
2020-04-14 11:32:04 手动操作 无变化 1
TOP10资产类型
7.14%
28.57%
14.29%
终端 移动电话 打印服务器 无线接入设备
通用设备 掌上电脑 专用分组交换机 网桥
防火墙 VoIP适配器
低危
失陷 3
高危 0
中危 3
低危 0
TOP 1
TOP 2
TOP 3
TOP 4
TOP 5
TOP 6
TOP 7
TOP 8
最近变动资产
IP 资产名称 资产类型 资产所属分组 状态 变更时间
58.20.127.170 58.20.127.170 移动电话 58_123abc 在线 2020-04-14 14:19:32
8.8.8.8 8.8.8.8 掌上电脑 其他 在线 2020-04-14 14:19:32
202.197.98.24 24资产 路由器 202资产分组98 离线 2020-04-14 14:19:32
资产安全
告警趋势图
严重 一般 通知
TOP 10 遭受攻击
TOP 5 漏洞排行
暂无漏洞信息


资产概况
资产概括
20
在库资产
16
资产类型
终端 4
终端服... 0
交换机 0
安全装... 1
虚拟机 0
路由器 1
打印服... 1
打印机 1
移动电... 2
专用分... 1
防火墙 1
宽带路... 1
资产安全 [全部类型]
总体状态
低危
分数: 76
当前所监测的资产整体安全评级低危，各个状态等级所对应的资产数如下:
失陷状态的资产共3台，高危状态的资产共0台，
中危状态的资产共3台，低危状态的资产共0台，
良好状态的资产共14台
2020-03-14 17:09--2020-04-14 17:09
导出
TOP变更类型统计
(次)
100
80
60
40
20
0
在线状态
开放端口
操作系统
资产类型
MAC地址
厂商


资产列表 [全部类型]
所有资产类型
所有分组
所有安全状态
高级选项
搜索资产名称或IP
资产导入 资产导出 合法配置 资产添加 核心切换 批量删除
序号 IP (•手动 •扫描) Mac地址 资产类型 核心 在线状态 最近发现时间 资产分组 漏洞数量 安全状态 操作 详情
1 新 8.8.8.8 掌上电脑 在线 2020-04-14 16:21:15 其他 无 良好
2 新 202.197.96.100 00:00:00:00:00:00 专用分组交换机 在线 2020-04-14 15:41:34 类型可以_自定义... 无 失陷
3 新 94.141.48.123 宽带路由器 在线 2020-04-14 14:19:32 其他 无 良好
4 新 58.20.127.170 移动电话 在线 2020-04-14 14:19:32 58_123abc 无 中危
5 新 202.197.98.24 路由器 离线 2020-04-14 14:19:32 202资产分组98 无 中危
6 新 202.197.97.1 移动电话 离线 2020-04-14 14:19:32 202资产分组202... 无 良好
7 新 202.197.96.8 防火墙 离线 2020-04-14 14:19:32 202资产分组123 无 中危
8 新 202.197.96.201 终端 在线 2020-04-14 14:19:32 类型可以_自定义... 无 失陷
9 新 202.197.96.1 网桥 在线 2020-04-14 14:19:32 202资产分组123 无 失陷
10 新 202.197.120.28 00:00:00:00:00:00 通用设备 在线 2020-04-14 14:19:32 其他 无 良好
10 30 50 100
总计20条记录 首页 上一页 1 2 下一页 尾页

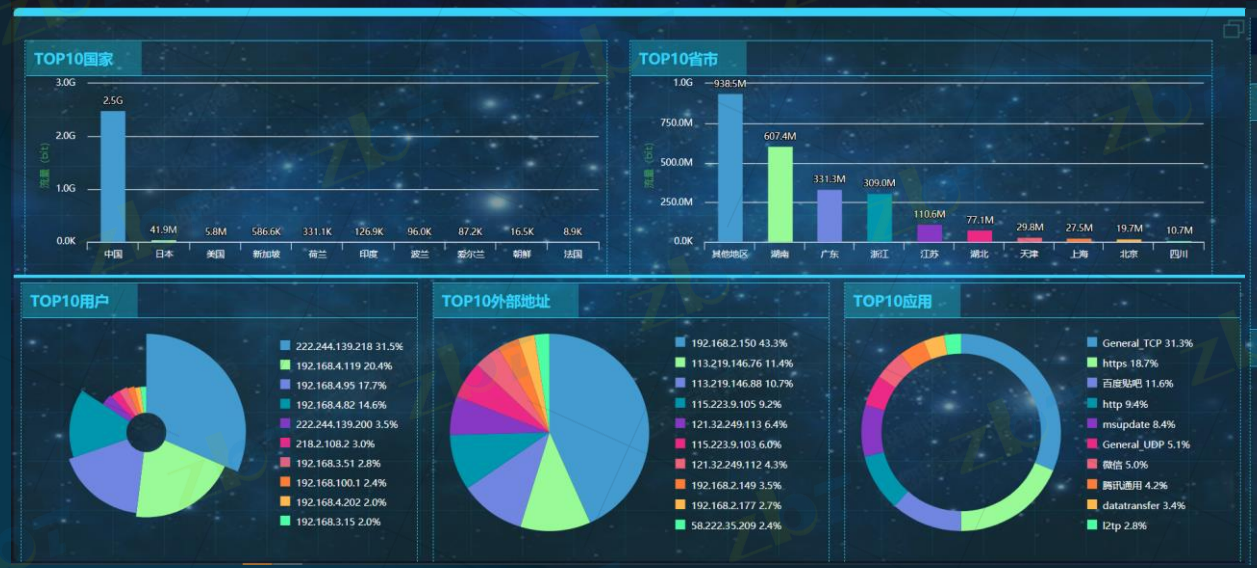
4.4 系统呈现（安全态势）





NO.	告警类型	告警数量	占比
1	违规访问	2611	34.88%
2	木马攻击	2193	29.29%
3	可疑加密流量	1880	25.11%
4	可疑流量	396	5.29%
5	可疑域名	276	3.69%
6	端口扫描	110	1.47%
7	可疑文件	16	0.21%
8	信息泄露	3	0.04%
9	web应用漏洞	1	0.01%

4.5 系统呈现（流量性能态势）



2020

请大家批评指正！