



2022

畅享连世界

多分支网络的一体化安全溯源分析

01

遥测网络介绍

安全隐患

2022年09月XX日，15:50-16:30，有黑客从分行网络入侵，目前总行生产网业务受到严重影响，分行目前不具备安全防御与入侵检测能力，此事件难以回溯。

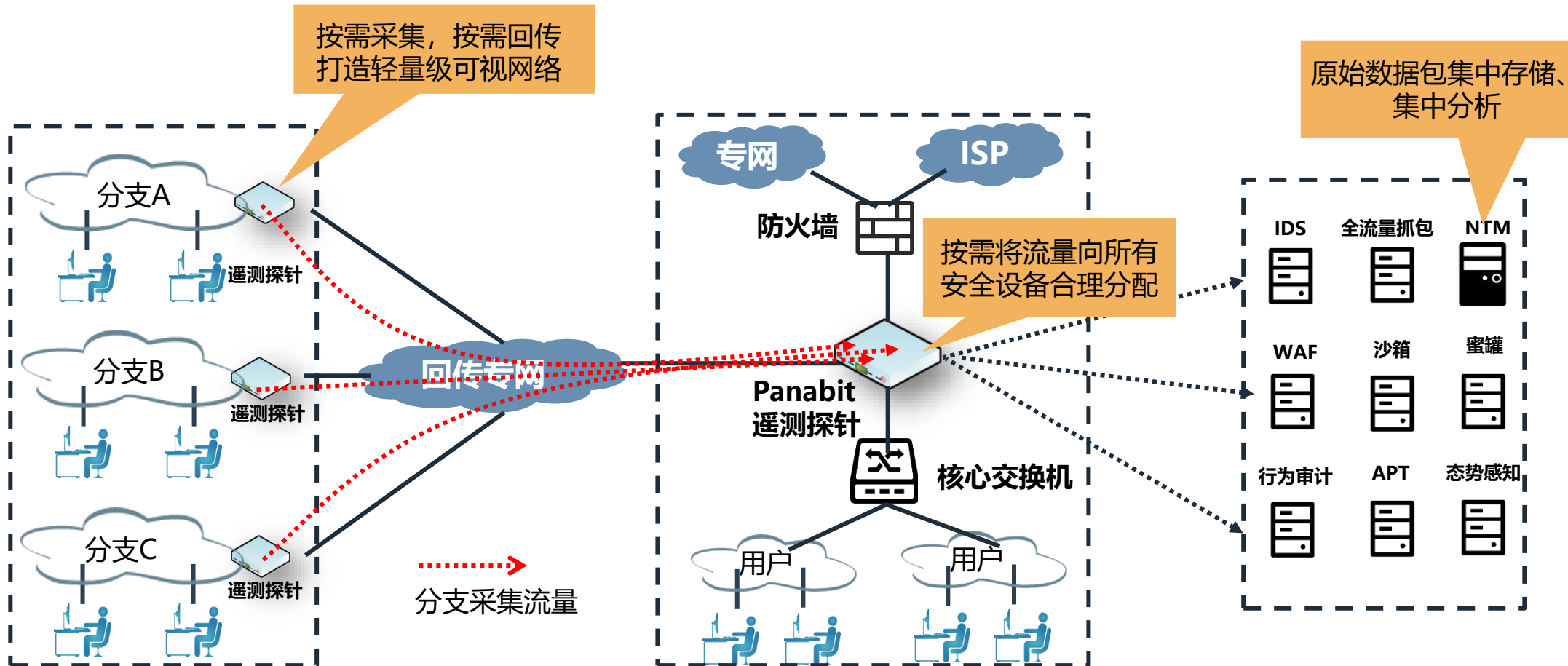
由重点突破总部安全防御边界，转为将重点攻击分支节点弱安全边界。

当网络安全建设达到一定程度时，针对网络安全管控范围，维护部门就会遇到如下三个难题：

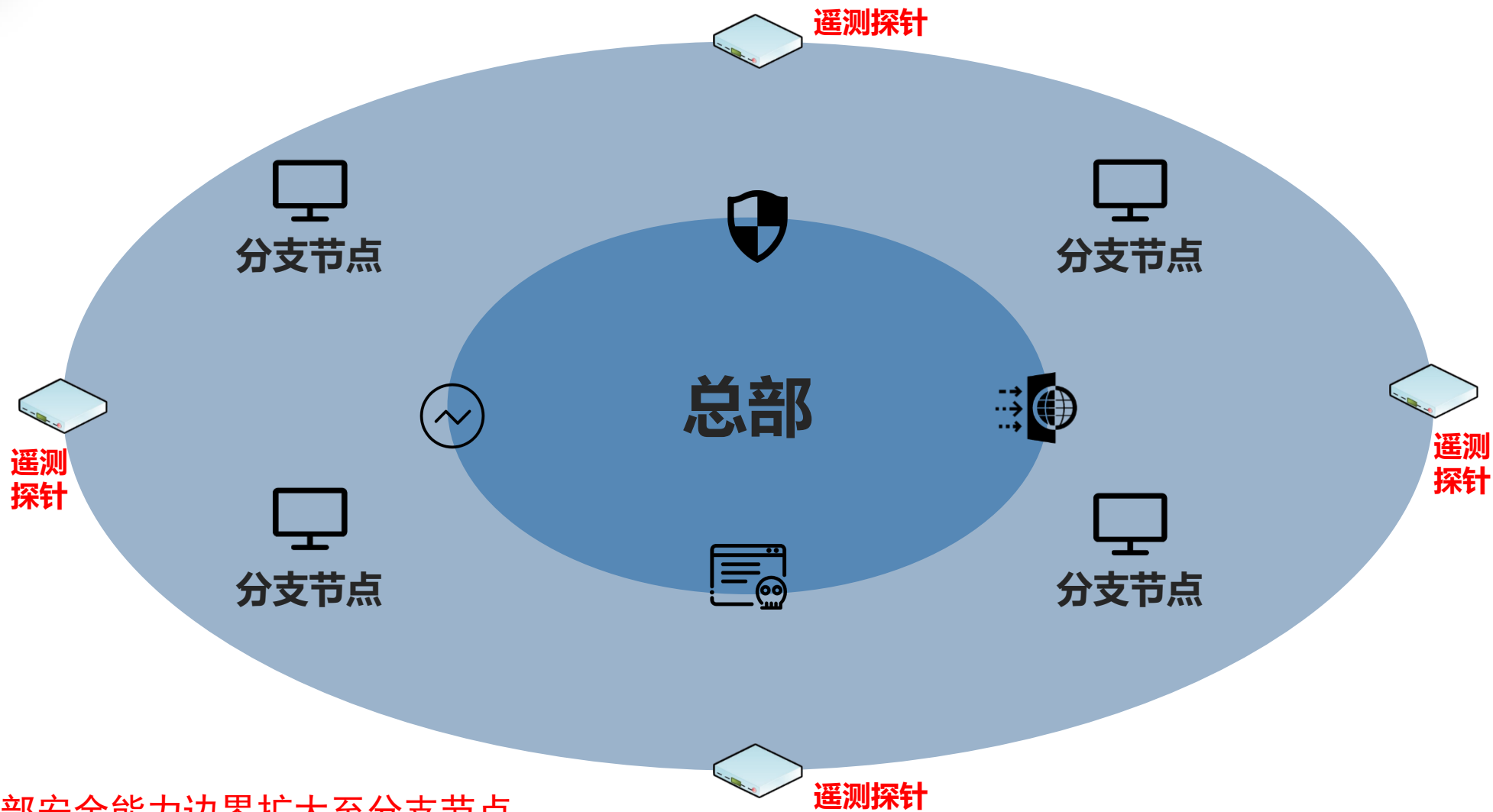
总部检测能力强，分支检测能力弱，远端看不到

出口检测能力强，接入检测能力弱，东西向看不到

云外检测能力强，云内检测能力弱，云里看不到

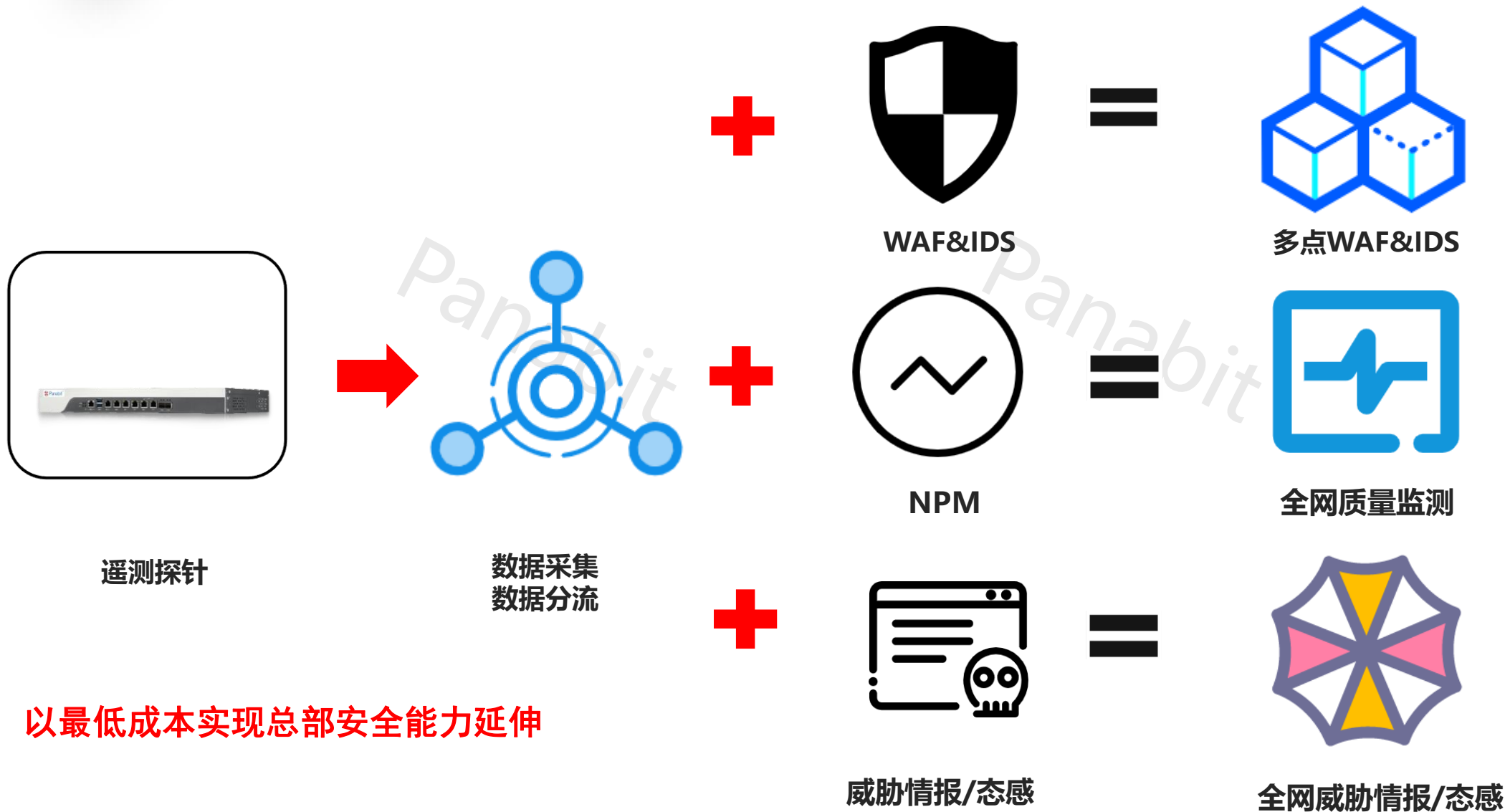


遥测加强了数据分析的空间范围

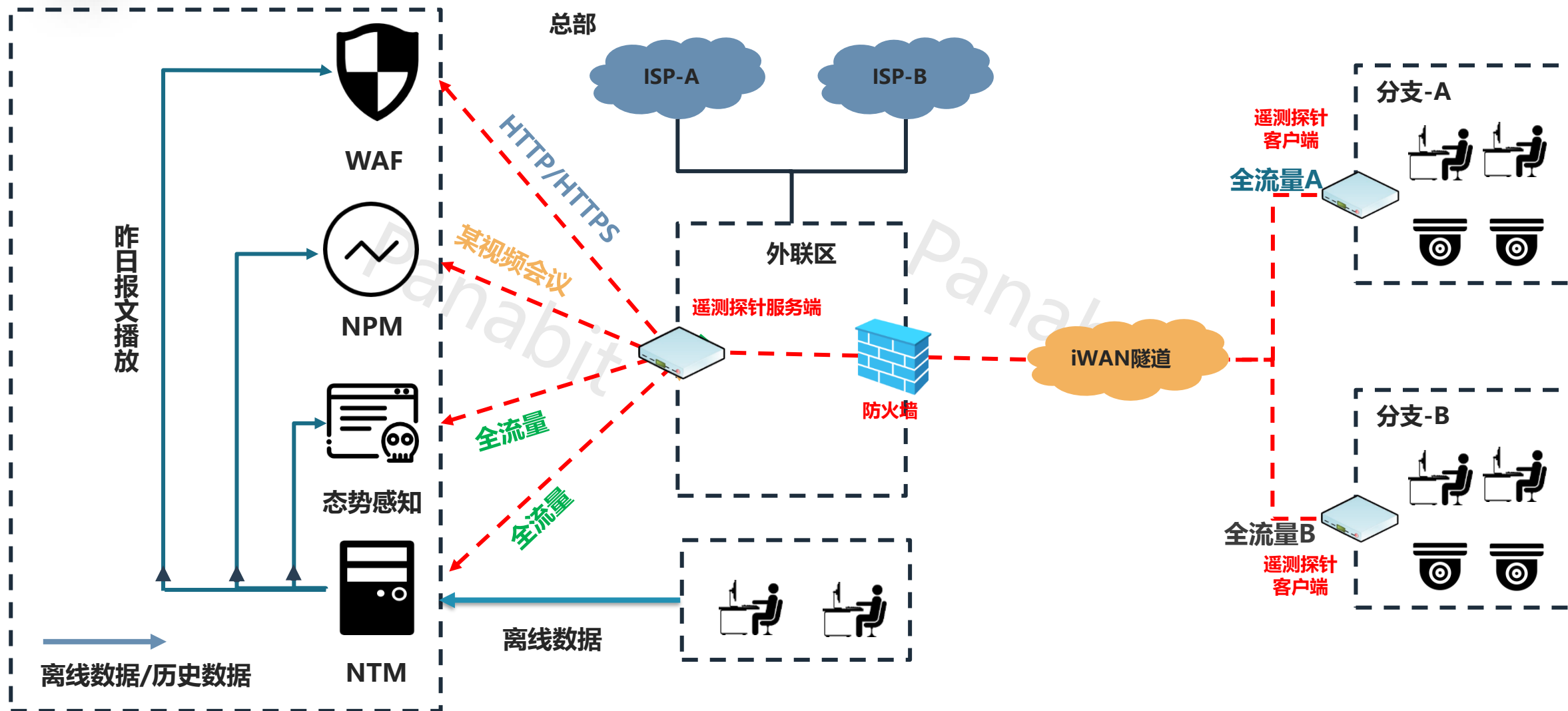


将总部安全能力边界扩大至分支节点

遥测加强了安全溯源的空间范围



遥测加NTM组网



遥测天生具备**原生分布式组网**及数据采集回传的能力

安全能力共享



通过采集分支节点流量回传至总部安全能力资源池的方式，实现总部安全能力共享给分支节点



一套遥测网络，代替所有分布式探针部署方案，降低探针网络重复部署成本和运维压力



代替探针网络

全网质量监测



通过NPM能力，完成全网应用级业务质量监测，实时掌握业务响应状态



支持统一设备管理，支持远程数据包采集，降低人员出差成本



远程运维管理

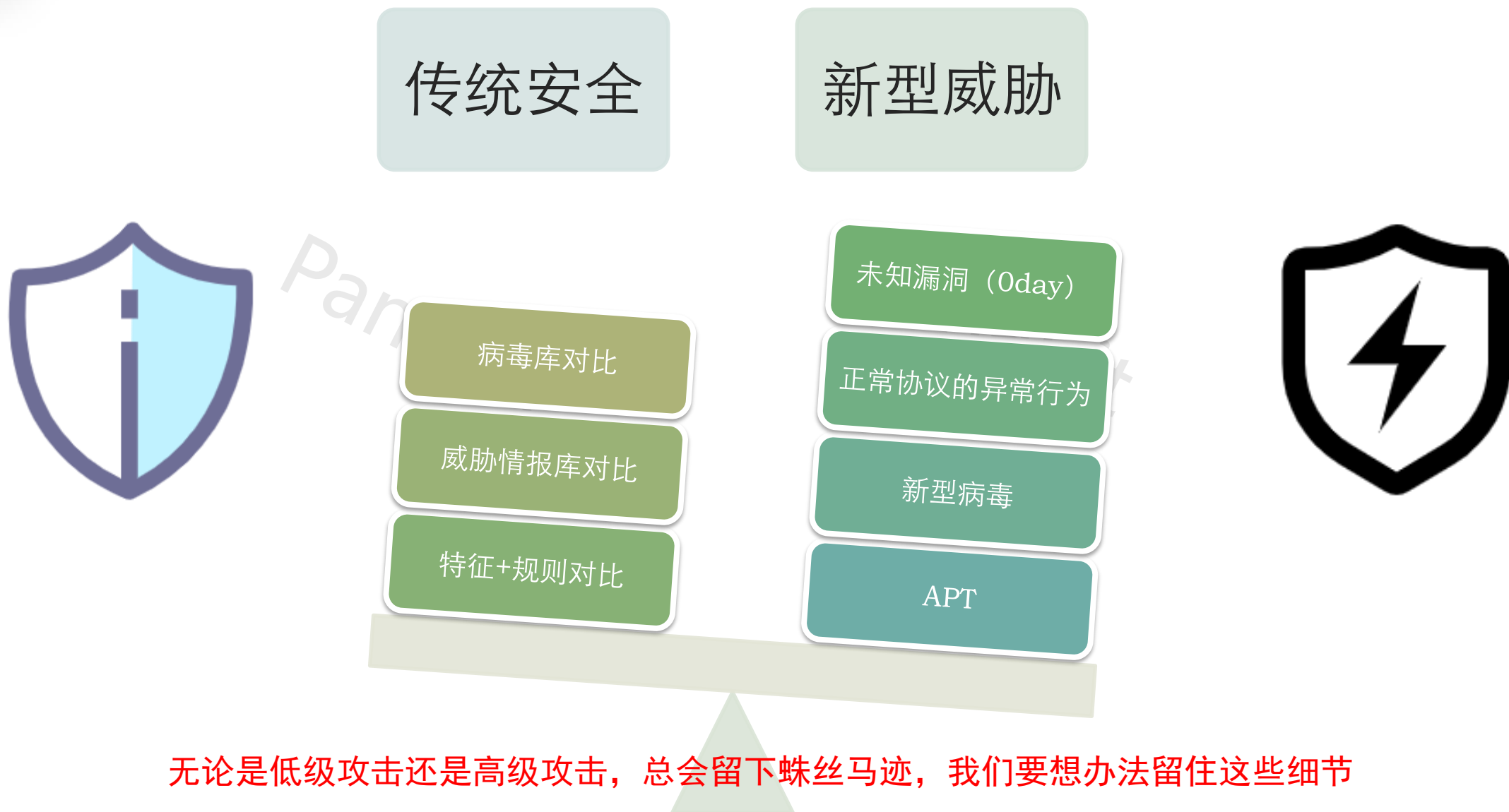
02

NTM介绍

暴力破解

2022年8月XX日13:24分，业务网某服务器受到未知安全攻击，网监要求提供溯源分析信息，确认是否存在数据泄露情况，及泄露数据流向。

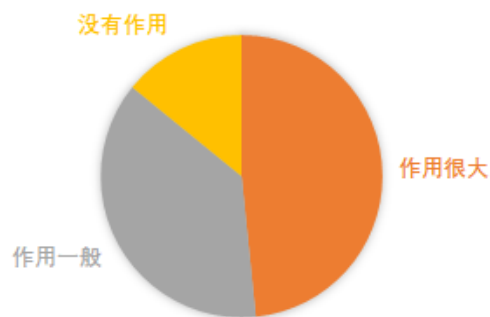
安全防御由传统黑名单被动防御方式，逐步发展为安全事件溯源分析。



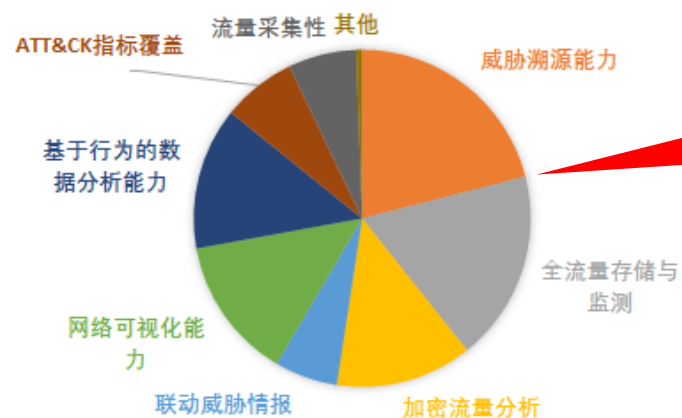
网络流量分析 (NTA) 解决方案监控网络流量、连接和对象，找出恶意的行为迹象。有些企业正在寻找基于网络的方法来识别绕过了周边安全性的攻击，这些企业应该考虑使用NTA来帮助识别、管理和分类这些事件。

——Gartner 《2017年11大顶尖信息安全技术》

已经部署的NTA/NDR产品在攻防演练中的作用



NTA/NDR产品在后续开发中需增强哪些能力



威胁溯源能力
全流量存储与检测
成为重点

《中国网络流量监测与分析产品研究报告》（2020年）



- g) 对外提供服务的大数据平台,平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理;
- h) 大数据平台应提供数据分类分级安全管理功能,供大数据应用针对不同类别级别的数据采取不同的安全保护措施;
- i) 大数据平台应提供设置数据安全标记功能,基于安全标记的授权和访问控制措施,满足细粒度授权访问控制管理能力要求;
- j) 大数据平台应在数据采集、存储、处理、分析等各个环节,支持对数据进行分类分级处置,并保证安全保护策略保持一致;
- k) 涉及重要数据接口,应实施访问控制,包括但不限于数据处理、使用、分析、导出、共享、交换等;
- l) 应在数据清洗和转换过程中对重要数据实施保护,以保证重要数据清洗和转换后的一致性,避免数据失真,并在产生问题时能有效还原和恢复;
- m) 应跟踪和记录数据采集、处理、分析和挖掘等过程,保证溯源数据能重现相应过程,溯源数据满足合规审计要求;
- n) 大数据平台应保证不同客户大数据应用的审计数据隔离存放,并提供不同客户审计数据收集汇总和集中分析的能力。

网络回溯

溯源

7.1.2.5.3 测评单元 (L3-NCS1-19)

a) 测评指标

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检测和分析;
(本条款引用自 GB/T 22239.1-20XX 7.1.2.5 c))

b) 测评对象

网络回溯和抗 APT 攻击等系统或设备。

c) 测评实施

- 1) 应核查是否部署网络回溯系统或抗 APT 攻击系统对新型网络攻击进行检测和分析;
- 2) 应测试验证是否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检测和分析。

d) 单元判定

如果 1) - 2) 均为肯定,则等级保护对象符合本测评单元指标要求,否则,等级保护对象不符合或部分符合本测评单元指标要求。

GBT28448-2019 《信息安全技术网络安全等级保护基本要求》

威胁情报助力已知安全隐患防控



内置16类威胁情报

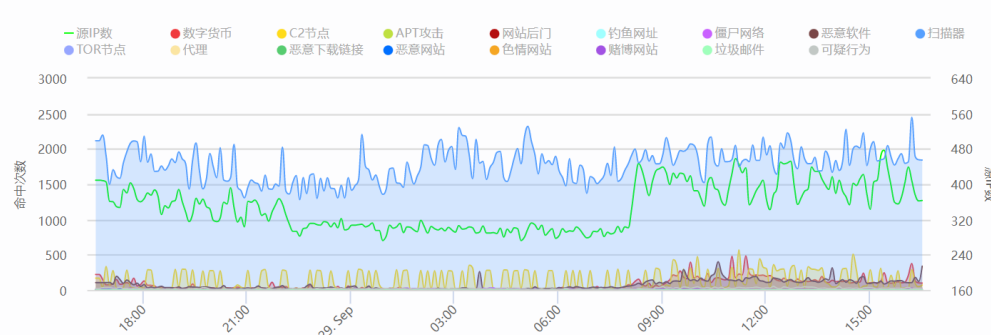
自动命中检测告警

60s 会话确认命中主机

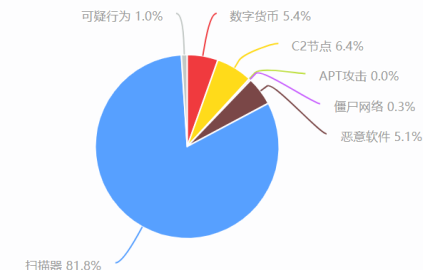
免费更新无忧保障

情报概况 情报诊断 命中会话 情报管理

情报命中趋势



情报类型命中分布



序号	源IP	命中次数	情报类型
5	10.4	1625	扫描器
6	20.117	1618	扫描器
7	124	649	扫描器
8	14.35	638	扫描器
9	225	615	扫描器
10	14.39	569	扫描器
11	20.176	512	扫描器
12	105.85	512	扫描器

< 1 2 3 ... 10 > 总共 991

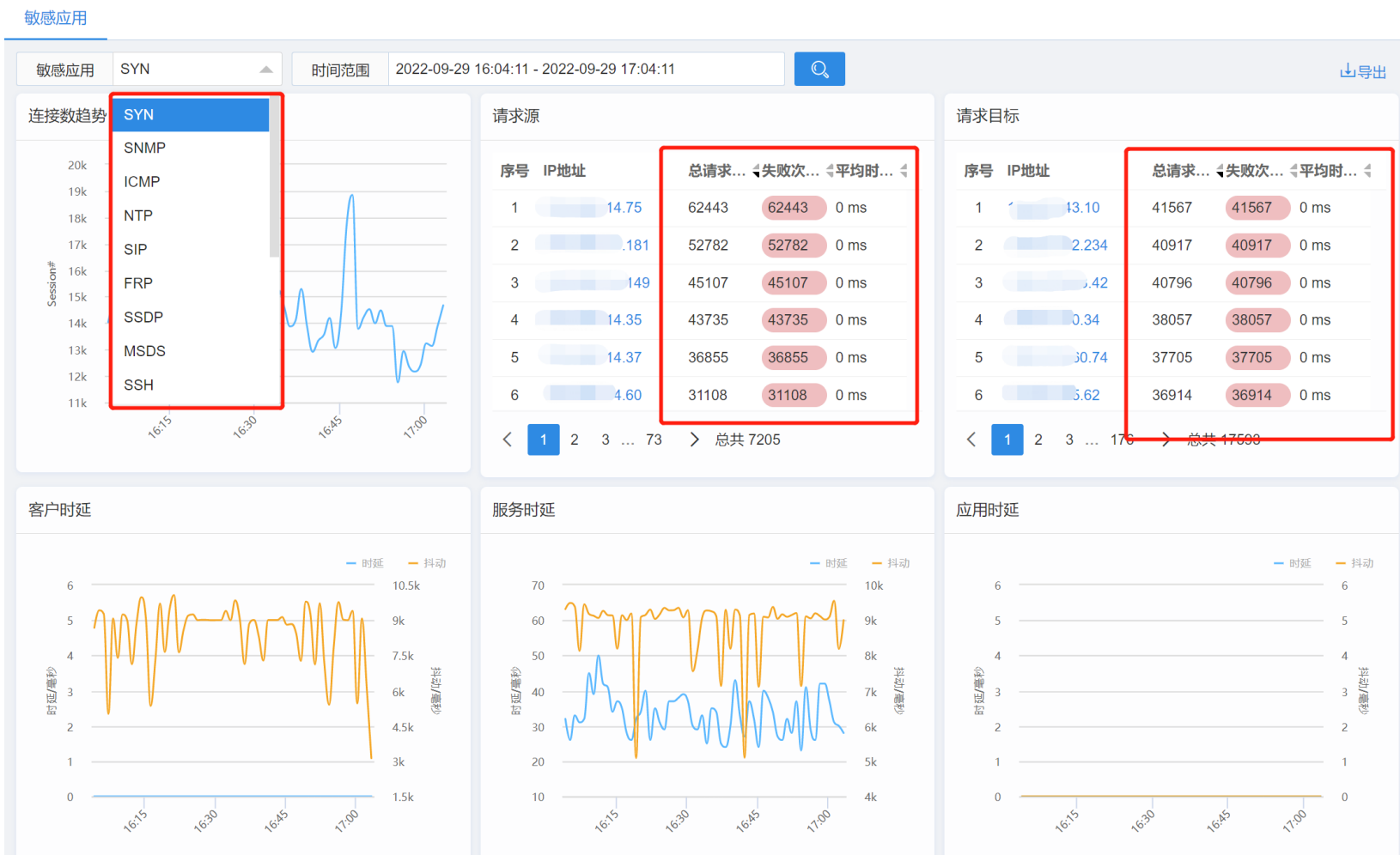
序号	目标IP	命中次数	情报类型
10	2.17	262	数字货币
11	109	209	数字货币
12	136	203	数字货币
13	53	200	C2节点
14	4.71	199	数字货币
15	114.40	198	数字货币
16	14.215	198	数字货币
17	114.192	197	数字货币

< 1 2 3 4 > 总共 389

序号	访问域名	命中次数	情报类型
1	1.65	125	可疑行为
2	search.namequery...	110	可疑行为
3	js.tv.itc.cn	33	恶意软件
4	apl.echoit1.com	22	僵尸网络
5	1.1	21	可疑行为
6	material.mediv.com	20	恶意软件
7	pro.csocools.com	20	恶意软件
8	neirong.funshion.com	19	恶意软件

< 1 > 总共 11

敏感应用&异常行为发现告警

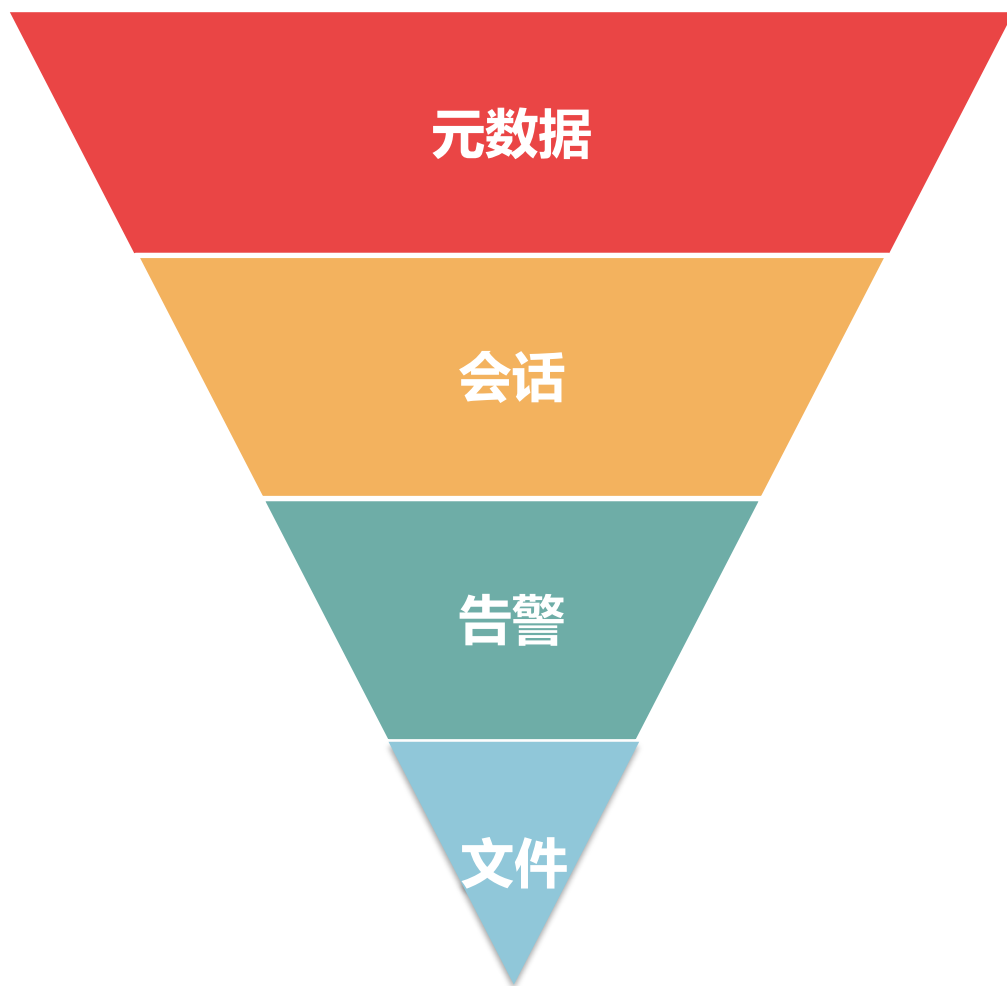


常见安全协议重点展示

未知威胁安全隐患定位

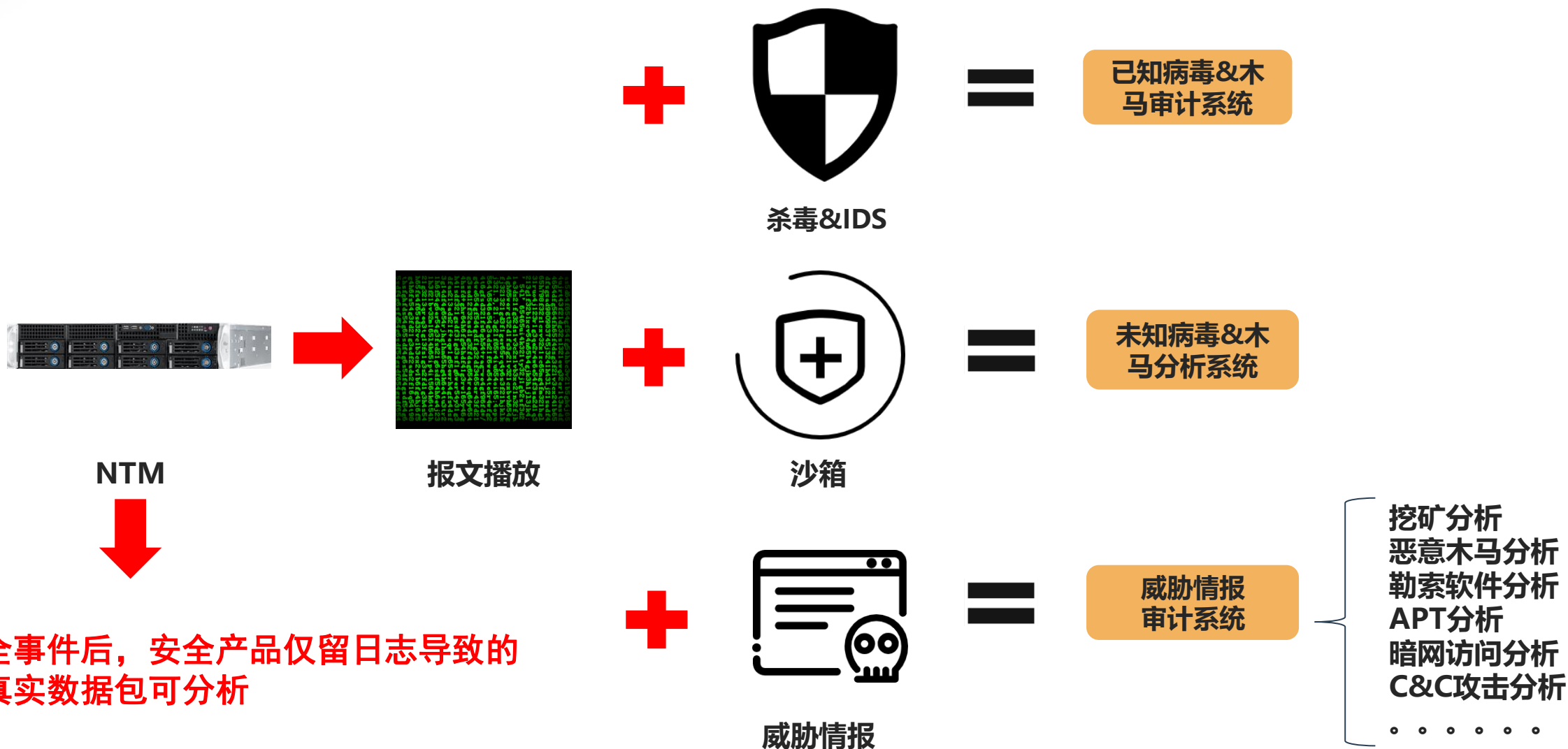
深度下钻挖掘中毒主机

主动告警联动网关防控

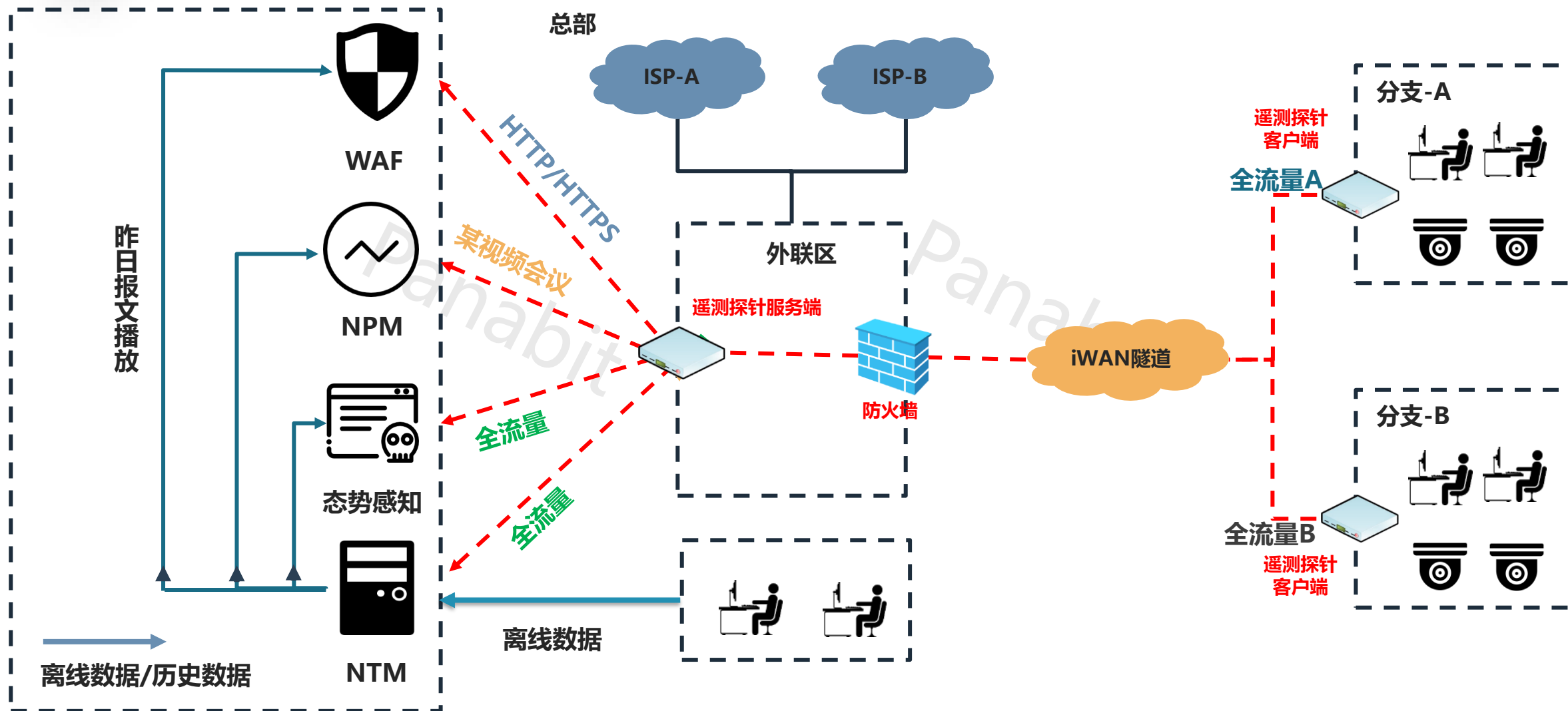


- 元数据、会话、威胁情报，加速数据分析定位
- 离线元数据和文件还原辅助分析
- 质量+情报+行为，监测锁定网络&安全问题
- 一镜到底，提供从会话至原始数据的锁定

NTM提高了安全溯源分析的时间范围



遥测加NTM组网



遥测天生具备**原生分布式组网**及数据采集回传的能力

全流量数据包留存，实现真正免责



- 完整保存历史流量数据
- 事件责任划分有据可依
- 满足相关部门法规要求

记录每条会话的所有数据包

报文分析 -> OpenVPN - 个人 - Microsoft Edge

应用协议: OpenVPN 报文下载

序号	时间	源地址	目标地址	网络协议	长度	详情
1	0.000000	11...9	11...189	TCP	70	53234 -> 443 [SYN] Seq=0 Win=14600 Len=0
2	0.002831	11...4.189	11...9	TCP	66	443 -> 53234 [SYN, ACK] Seq=0 Ack=1 Win=28
3	0.006782	11...9	11...189	TCP	64	53234 -> 443 [ACK] Seq=1 Ack=1 Win=14848
4	0.007323	11...9	11...189	TLSv1	301	Client Hello
5	0.009913	11...4.189	11...9	TCP	60	443 -> 53234 [ACK] Seq=1 Ack=244 Win=30336
6	0.010957	11...4.189	11...9	TLSv1.2	1510	Server Hello
7	0.010958	11...4.189	11...9	TCP	1510	443 -> 53234 [ACK] Seq=1457 Ack=244 Win=30
8	0.010959	11...4.189	11...9	TLSv1.2	501	Certificate, Server Key Exchange, Server Hello
9	0.014890	11...9	11...4.189	TCP	64	53234 -> 443 [ACK] Seq=244 Ack=1457 Win=1

Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

Ethernet II, Src: 58:6a:b1:e0:81:f3 (58:6a:b1:e0:81:f3), Dst: b0:b5:78:58:01:20 (b0:b5:78:58:01:20)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3102

Internet Protocol Version 4, Src: 11..., Dst: 11...9

Transmission Control Protocol, Src Port: 53234, Dst Port: 443, Seq: 0, Len: 0

数据包

安全做到事前防御、事中分析、事后溯源

事前

- 威胁情报库主动防御
- 异常流量&行为告警

事中

- 新病毒、0day、APT攻击分析发现
- 联动网关设备快速阻断

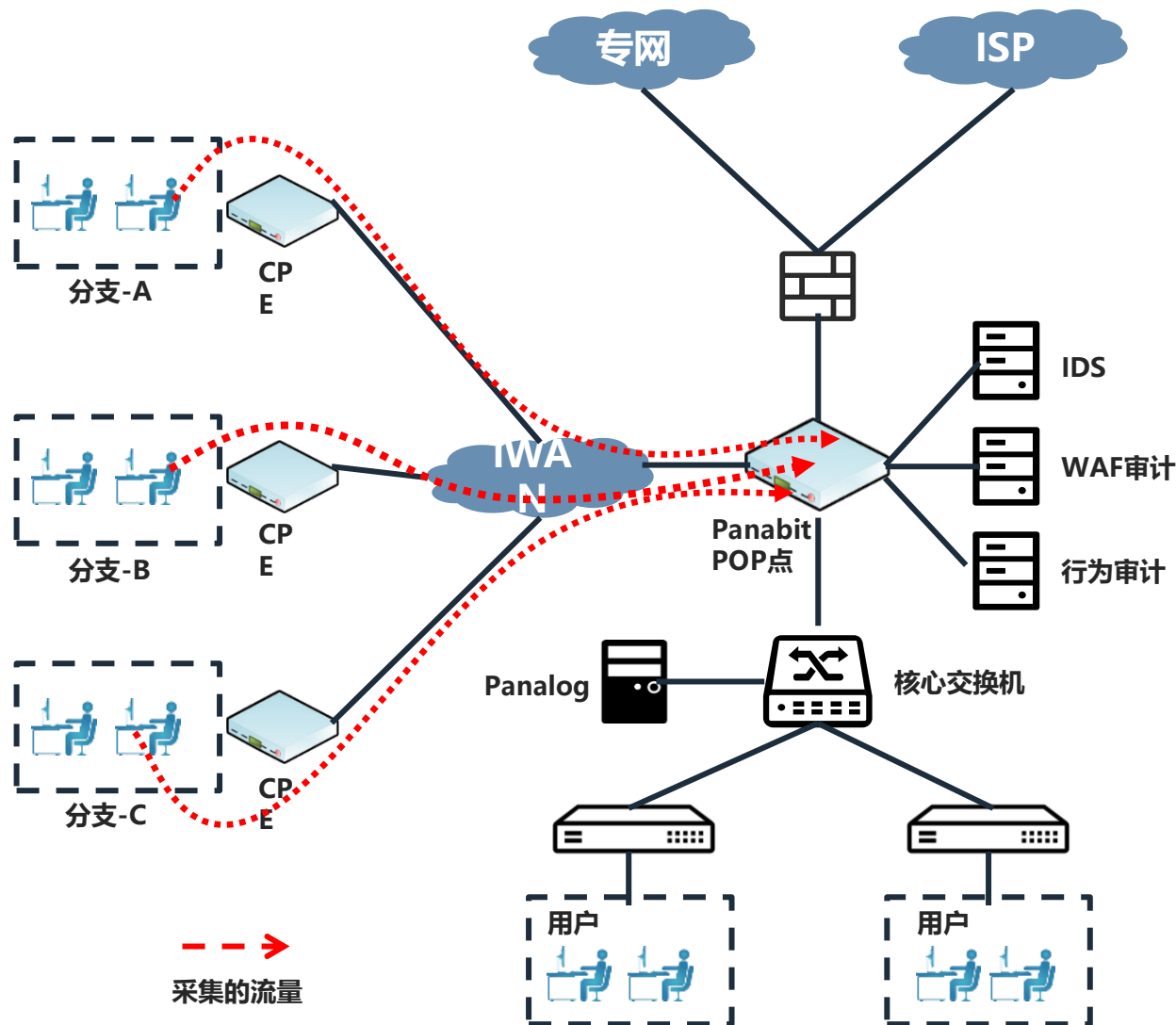
事后

- 原始数据包共享，三方安全联动溯源分析
- 原始数据包留存，满足相关部门溯源要求

03

典型案例

XXX分布式全量回溯能力平台建设项目



需求背景

XXXX信息科技有限公司是国内唯一专业从事国资国企网络信息安全科技的国家队

1. 根据国资委要求，进行网络整改
2. 用户投诉业务卡顿（视频会议、学习强国、邮箱等应用），影响用户上网体验
3. 各分支的流量需要汇聚到总部进行统一分析

解决方案

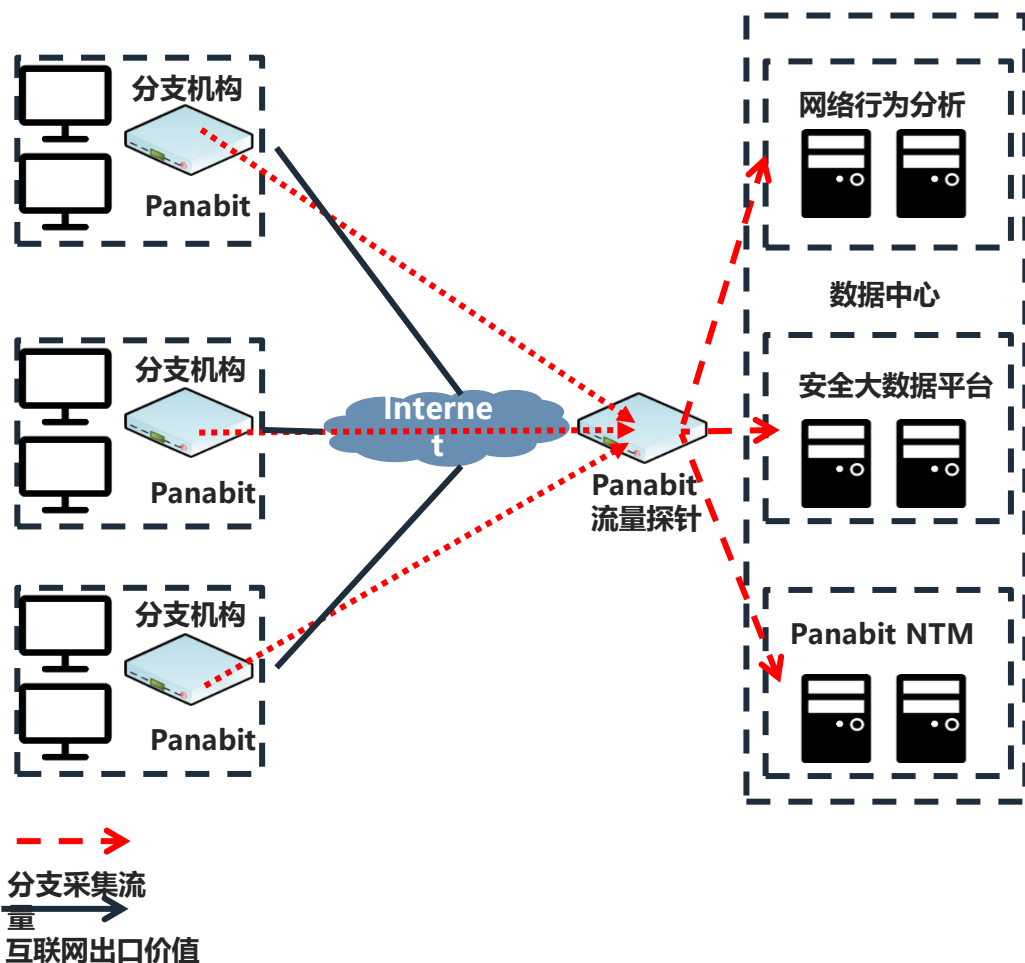
1. 在每个节点部署Panabit，实现对数据的统一监控、分析、溯源等需求
2. 核心部署Panabit对流量进行筛选，去掉如P2P、音视频等低价值流量，或者可以根据需求，保留关键业务
3. 核心交换机旁路部署Panalog，做数据留存、审计

应用价值

1. 异常流量分析，网络流量控制
2. 流量可视化，NPM协助精确故障定位
3. 自研iWAN隧道组网，快速稳定



中国XX集团网络及业务态势感知优化方案



需求背景

中国XX集团有限公司，属与XXX国有资产监督管理委员会管理的中央企业

1. 需要对分支机构的流量进行安全分析，质量监测
2. 根据新推出的《网络安全法》，需要对敏感数据进行数据留存
3. 网络设备种类繁多，发生网络故障，无法快速定位故障范围，运维压力大

解决方案

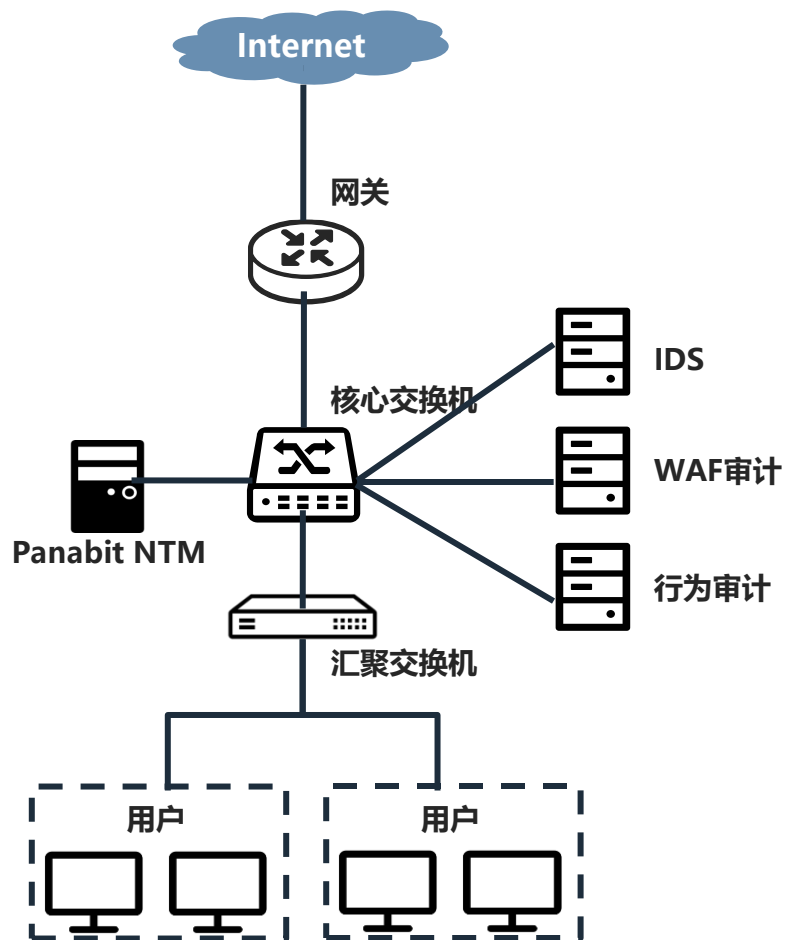
1. 分支机构部署Panabit，各个分支机构将流量镜像给Panabit流量探针，进行实时的网络服务质量监测、安全分析
2. 数据中心部署Panabit NTM可以按照应用、五元组等策略进行原始数据包的抓取和回溯分析，并生成超级摘要，快速定位问题

应用价值

1. 流量可视化，NPM协助精确故障定位
2. 全网1:1流量、会话日志留存
3. 按需采集，按需回传，打造轻量级可视网络
4. 异常流量随时发现，及时管控，排除网络安全隐患



中国XX商用网络优化项目



需求背景

中国XX商用集团是中央直接管理的国有特大型企业

1. 根据《网络安全法》需要对数据留存180天
2. 无法对接第三方安全分析平台设备
3. 异常流量无法监测，网络体验差，经常遭到用户投诉

解决方案

1. 在总部旁路部署一台Panabit NTM,进行实时的网络服务质量监测,以及重要数据的留存和溯源分析
2. NTM通过对收到的数据进行深度分析,针对业务质量、常见攻击、异常流量等内容进行分析展示,提高网络质量
3. NTM对原始数据进行深度加工,产生超级摘要,对接第三方分析平台,大大提高数据分析师的工作效率,

应用价值

1. 全流量数据留存
2. 故障回溯及定位
3. 全网流量可视化



2022

畅享连世界

THANK YOU