华为CIS网络安全智能系统

APT（Advanced Persistent Threat，高级持续性威胁）是黑客以窃取核心资料为目的，针对企业发动的网络攻击和侵袭行为。其目标是访问企业网络、获取数据，并长期地秘密监视目标计算机系统。近年来，APT攻击已经成为业界关注和讨论的热点。因其独特的攻击方式和手段，传统的安全防御工具无法有效防御。典型的APT攻击，包括多个攻击过程，如：资源侦查、外部渗透、命令与控制、内部扩散、数据外发等。一旦攻入企业内部，黑客能在企业内部持续横向渗透，收集敏感信息并回传，造成巨大的损失。

华为推出的CIS（Cybersecurity Intelligence System，网络安全智能系统），采用最新大数据分析和机器学习技术，可用于抵御APT攻击。它从海量数据中提取关键信息，通过多维度风险评估，采用大数据分析方法关联单点异常行为，从而还原出APT攻击链，准确识别和防御APT攻击，避免核心信息资产损失。

产品图

方案亮点

全面检测：基于APT攻击链，检测单点事件，关联组合威胁

全网协防：威胁联动安全设备、终端设备处置闭环、云端信誉共享

全网可视：安全态势实时感知，PB级数据秒级检索溯源

方案架构

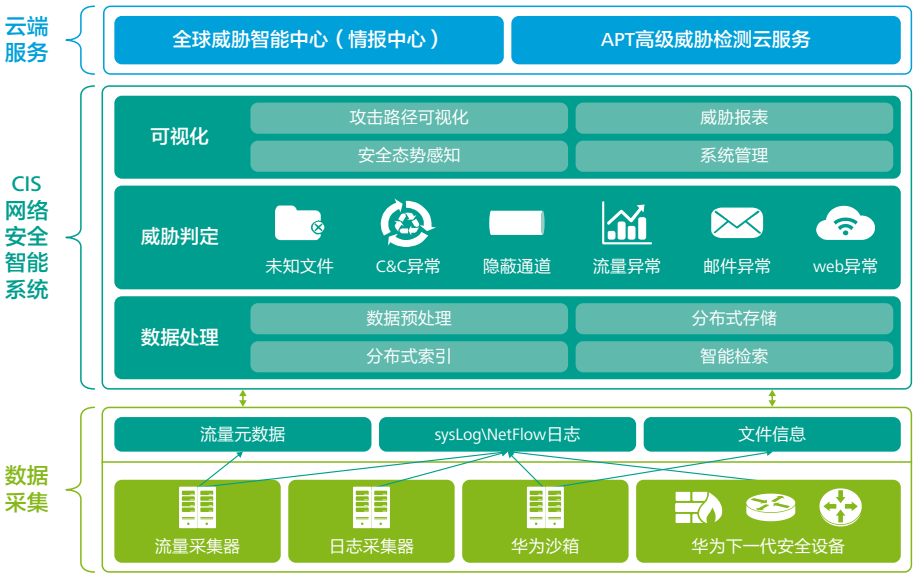


图1. 方案架构

数据采集：

通过流探针采集全网流量元数据、日志采集器采集网络安全设备的日志信息、华为沙箱上报文件信息等，CIS网络安全智能系统进行格式化预处理、针对不同类型的数据进行分布式存储、对关键的格式化数据建议索引，以提供快速检索、威胁检测、威胁可视化等服务。

CIS网络安全智能系统：

CIS系统基于多种数据源进行分析，流量元数据，用于C&C检测、隐蔽通道检测、Mail检测等；日志用于日志关联分析；netflow用于流量异常分析；在mail异常、隐蔽通道异常检测中，结合文件信息，帮助判断是否异常。以时间、空间、IP等信息为关联，CIS系统将单点异常事件进行关联并综合评估，得出攻击链，并进行高级威胁判定。

CIS系统可视化层，能够对攻击链进行可视化呈现、展示全网安全态势、提供威胁报表等，展示资源侦查、外部渗透、命令与控制、内部扩散、数据外发等APT攻击过程，感知全网威胁态势、攻击路径、高危资产等信息，帮助快速掌控全网威胁。

云端服务：

CIS系统检测出的高级威胁情报信息，还能上传到全球威胁智能中心，做到全网威胁实时、全面共享。华为APT高级检测云服务，对本地没有CIS系统的用户，提供上传未知文件到云端检测的服务。

另外，华为网络安全设备能够根据CIS系统检出的高级威胁情报信息，进行实时阻断。

关键组件

数据采集	流探针	通过镜像或者分光链路流量，提取流量的元数据，并上传元数据信息给CIS，其中文件还原后上传给沙箱检测；
	日志采集器	采集网络中关键设备、第三方SIEM系统的Syslog日志/Netflow数据进行采集和归一化处理。
	安全沙箱	通过还原交换机或者传统安全设备镜像的网络流量，在虚拟的环境内对网络中传输的文件进行检测，实现对未知恶意文件的检测。检测结果以日志形式，连同原始文件上传到CIS平台，提供APT攻击渗透阶段信息。
可视化	可视化节点	负责数据呈现，包括威胁态势呈现、攻击链路可视化、高级威胁报表、配置管理、智能检索等。
数据处理	集群控制节点	负责对检测存储节点和数据分发节点的集群状态进行统一管理和资源调度。
	数据分发节点	对流探针和采集器上报的数据进行预处理，并负责数据的转发。
	存储/检测节点	负责数据统一存储和分布式数据索引，另外还通过分布式数据处理和分析提供威胁检测功能。

关键特性

全面检测：基于APT攻击链，检测单点事件，关联组合威胁

CIS系统基于大数据平台，采用机器学习模式，针对APT全攻击链中的每个步骤，渗透、驻点、提权、侦查、外发等各个阶段进行检测，建立文件异常、mail 异常、C&C异常检测、流量异常、日志关联、web 异常检测、隐蔽通道等检测模型并关联检测出高级威胁：

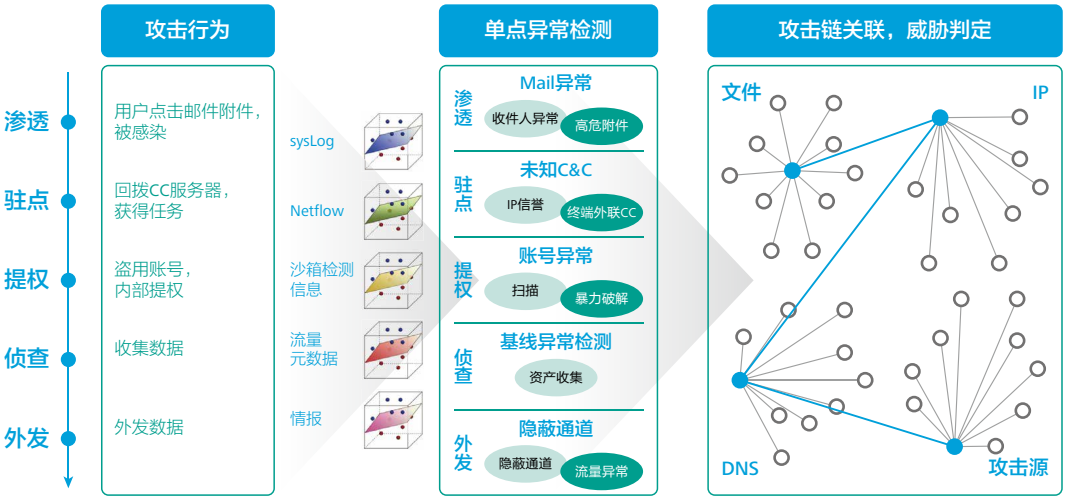
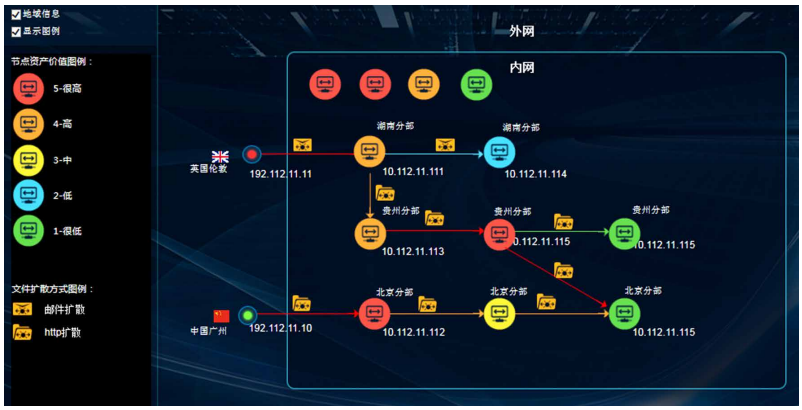
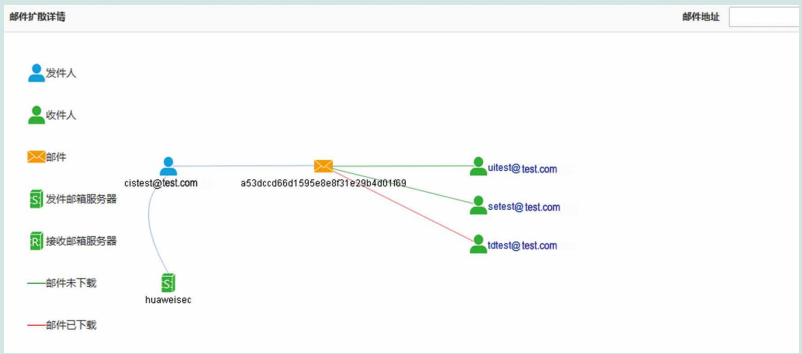


图2. 基于APT攻击链的检测

文件异常检测日志	对于http、smtp、pop3、imap、ftp协议的流量中还原出其中的未知文件，沙箱能够对其进行检测，判断威胁程度，并将检测结果以日志形式发给CIS，CIS的邮件异常检测、web异常检测可结合文件检测结果，进行关联分析。  图3. 文件渗透攻击链
Mail异常检测	邮件异常检测是通过对互联网出口SMTP/POP3/IMAP协议流量的分析，结合沙箱的文件检测结果，发现一些邮件所携带的附件为恶意或可疑文件，或者发现一些邮件所携带URL链接不安全，那么这些邮件被检测为是恶意/可疑邮件。  图4. 邮件异常检测
C&C检测	C&C检测：即命令与控制通道检测，发现内网感染主机与外部C&C主机通信。通过对互联网出口的DNS协议流量的分析，检测出内网到外网的异常连接。  图5. C&C异常检测

流量基线异常检测	发现内网与外网、内网之间互通的异常流量。通过上线学习的白名单或者用户自定义的流量异常策略检测网络访问访问行为，发现违规访问、访问频次和访问路径异常。
日志关联	提取日志数据的特征数据，构建统一格式的日志事件，根据预设的规则对事件进行交叉关联分析和事件流逻辑关联分析。
隐蔽通道检测	发现内部感染主机通过隐蔽通道外发数据。隐蔽通道异常检测主要用于发现被入侵主机通过正常的协议和通道传输非授权数据的异常，检测方法包括Ping Tunnel、DNS Tunnel和文件防躲避检测。
攻击链关联	以上检测结果，在CIS系统中分为高级威胁和普通威胁。高级威胁是指威胁跨越了多个攻击阶段的组合攻击，而普通威胁是基于单个攻击阶段的单点攻击。 支持从威胁、邮件和文件多个维度展示攻击扩散路径和影响范围。在威胁维度的攻击扩散展示维度，有效呈现高级威胁的多个攻击阶段，包括：外部渗透阶段、命令与控制阶段、内部扩散阶段、数据窃取阶，并直观清晰呈现来自不同地区的外部攻击源/命令控制服务器和企业内部受到危害和影响的主机，帮助客户有效洞察企业面临的威胁  图6. APT全攻击链关联

全网协防：威胁联动安全设备、终端设备处置闭环，云端信誉共享

安全设备联动	CIS系统检测出的威胁信息，能够在分钟内联动到华为NGFW设备，在网络侧进行阻断。
终端设备联动	CIS系统可将检测结果同步给第三方终端设备，在终端进行检测并清除威胁。
云端共享	CIS系统检测出的威胁情报信息，能够上传到全球威胁智能中心，智能中心对外提供信誉查询服务。同时，CIS系统还能够根据客户需求，自动或手动到云端信誉中心，查询IP信誉、Domain信誉、文件信誉等，结合信誉信息做高级分析；CIS系统还提供云端情报web查询界面，协助客户对检测出的威胁做进一步的调查分析。

全网可视：安全态势实时感知，PB级数据秒级检索溯源

1. 威胁地图呈现：通过威胁地图直观展示企业在全球范围内面的威胁和最近发现的威胁事件，方便安全运维分析人员能及时发现威胁、预判全网安全走势。
2. 舞台模式聚焦关注区域：CIS安全态势，提供舞台模式态势呈现，即根据客户关注的省、市、区县等，定制开发以该省、市、区县在舞台中心，世界各大洲分布在舞台四周，来展示世界各地针对舞台中心地区的攻击态势。

图7. 全球安全态势感知图

3. 支持通过关键字、条件表达式、时间范围对事件和流量元数据进行快速检索，快速定位到安全运维分析人员关注的威胁和上下文数据，并支持查看数量趋势统计和检索结果详细数据，10亿条记录查询5秒内返回结果。
4. 支持基于攻击链进行事件调查，通过不同的攻击阶段关联流量元数据，在流量元数据检索结果列表可以下载元数据相关的PCAP文件，在同一个界面方便安全运维分析人员进一步取证分析，调查效率高效快速。

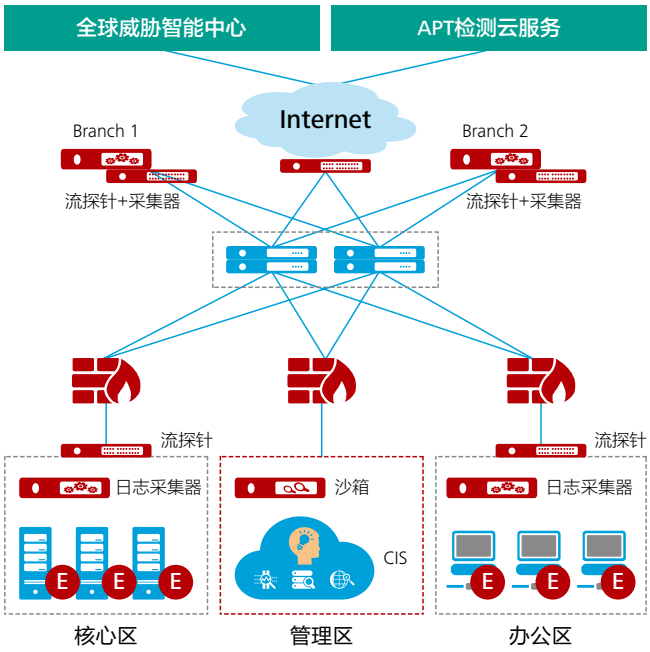
图8. 威胁时间列表

其他功能：

1. 大数据平台分层架构、模块化功能组合、开放接口，易于南向对接威胁日志，北向对接第三方综合安全管理系统

应用场景

1. 金融、大企业信息安全



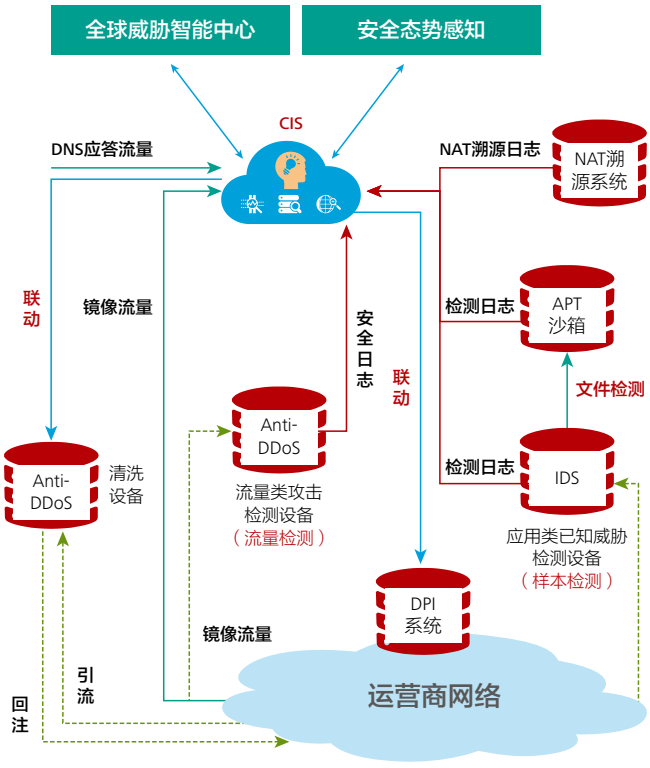
关键需求

1. 检测恶意威胁
2. 阻断APT攻击
3. 安全态势可视化

部署要点

1. 在Internet边界和分支边界部署流探针，针对具体情况配置相应的策略。内部边界可选择性部署
2. 在管理区部署沙箱和CIS系统
3. 在网络边界部署NGFW/NGIPS等安全设备
4. 在办公区和核心区分别部署终端和服务器探针
5. 通过防火墙等安全设备检测已知威胁；通过流探针、沙箱和CIS系统，检测未知威胁；CIS联动防火墙等执行组件阻断APT攻击；可视化呈现全网安全态势

2. 安全态势感知场景



方案价值

1. 已知威胁检测
   1）基于流量检测DDoS攻击，识别僵尸主
   2）基于流量检测应用层入侵，识别网络入侵攻击行为
   3）基于文件检测恶意软件，识别恶意文件传输
2. 未知、高级威胁检测
   1）基于流量检测未知攻击，识别未知感染主机、未知僵尸主机
   2）基于文件检测未知恶意文件，识别未知恶意文件传输
   3）基于文件和流量，检测APT渗透、隐蔽通道
3. 攻击溯源/调查取证
   1）大数据平台，存储协议元数据，辅助调查分析高级威胁
   2）可疑流量PCAP抓包，辅助事件确认调查分析
4. 全网安全态势感知
   全网感知僵木蠕、C&C、高级威胁攻击、内网感染主机

产品规格

型号	CIS		
功能特性			
流量采集	支持HTTP协议、邮件协议、DNS协议解析，能对HTTP文件、邮件附件还原，并按照抓包规则进行抓包		
日志采集	可采集ArcSight设备和FireHunter设备的sysLog日志，华为路由器、交换机的NetFlow日志，流探针的NetFlow日志		
C&C异常检测	DGA域名检测、Fast-Flux域名检测		
事件关联分析	对日志有预定义规则、并可自定义关联规则、子规则		
流量基线异常检测	可配置流量控制规则、支持垂直扫描和水平扫描		
流量异常检测	支持检测违规访问、流量超限、频次超限		
邮件异常检测	发件服务器分析、收发件人分析、用户自定义邮件黑白名单、邮件附件检测		
隐蔽通道检测	可检测Ping Tunnel、DNS Tunnel、文件方躲避检测		
信誉管理	支持本地IP信誉查询、DNS信誉生成、文件信誉查询		
攻击路径可视化	攻击扩散路径可视化，可查看外网到内网的攻击、内网内部的扩散、内网到外网的C&C连接		
全网威胁态势	威胁分析、恶意可疑邮件分析、恶意可疑文件分析、受威胁主机维度分析、恶意域名维度分析、关联事件显示、流量异常事件显示		
智能检索	数据检索、检索结果钻取		
黑白名单管理	邮件、URL、IP、域名黑白名单管理		
节点服务器规格			
节点名称	服务器类型	服务器配置	说明
流探针节点 (高端)	RH2288H V3	CPU：2*10核2.3G 内存：64G 系统盘：2*300G SAS (支持RAID1) 数据盘：6*2T SATA (支持RAID6)	采集全网流量，上报流量元数据、netflow给CIS系统，性能10Gbps
流探针节点 (低端)	RH1288H V3	CPU：1*10核2.3G 内存：32G 系统盘：2*300G SAS (支持RAID1) 数据盘：2*1T SATA	采集全网流量，上报流量元数据、netflow给CIS系统，性能0.5Gbps
采集器节点	RH2288H V3	CPU：2*10核2.3G 内存：64G 系统盘：2*300G SAS (支持RAID1) 数据盘：6*2T SATA (支持RAID6)	采集日志，并进行归一化处理。性能sysLog日志15000EPS，Netflow日志120000EPS
CIS系统大数据后台业务节点	RH2288H V3	CPU: 2*12核2.3G 内存：256G 系统盘：2*600G SAS (支持RAID1) 数据盘：23*1.2T SAS (支持RAID6)	数据预处理、分布式存储、分布式检索、威胁检测分析

可视化管理节点	RH2288H V3	CPU：2*10核2.3G 内存：64G 系统盘：2*300G SAS (支持RAID1) 数据盘：6*2T SATA (支持RAID6)	攻击链展示、报表生成、安全态势感知、系统管理

尺寸、电源、运行环境	
尺寸 (W * D * H)	探针服务器：436mm × 708mm × 43mm (1U) 后台业务服务器、可视化管理/探针服务器：447mm × 748mm × 86.1mm (2U)
重量	满配净重 探针服务器：20Kg 后台业务服务器、可视化管理/探针服务器：30Kg 包装材料重量：5Kg
电源AC	交流输入：100V AC～240V AC 兼容240V高压直流输入：192V DC～288V DC
电源DC	-36V～-75V，额定-48V
最大功耗	探针服务器：364W 后台业务服务器：638W 可视化管理/探针服务器：426W
工作环境温度	工作温度：5°C～45°C (41°F～113°F) 存储温度：-40°C～+65°C (-40°F～149°F) 温度变化每小时小于20°C (36°F) 长时间存放温度：21°C～27°C (69.8°F～80.6°F)
环境湿度	工作湿度：8% RH～90% RH非凝结 存储湿度：5% RH～95% RH非凝结 湿度变化每小时小于20% RH 长时间存放湿度：30% RH～69% RH非凝结

订购信息

对外型号	软件
CISSOFTWARE-CD	终端物理软件-CIS-CISSOFTWARE-CIS软件包-CD
CIS-PLATFORM	CIS大数据基础平台
CIS-FAD	流量异常检测
CIS-CA	关联分析
CIS-CCAD	C&C异常检测
CIS-HTD	隐蔽通道异常检测
CIS-MAD	邮件异常检测
CIS-ALV	攻击路径可视化

CISEXPLIC	性能扩容license	
	服务器	
SEC-SERVER-AC-03	安全产品服务器交流配置03（2*750W交流，滑轨）	CIS的业务节点服务器，包括集群控制节点、数据分发节点、检测与存储节点服务器
SEC-SERVER-AC-04	安全产品服务器交流配置04（2*750W交流，滑轨）	包括CIS的可视化节点、峰值15000EPS日志采集器或峰值120000FPS日志采集器或10Gbps混合流量探针服务器或1Gbps DNS流量探针
SEC-SERVER-AC-05	安全产品服务器交流配置05（2*460W交流，滑轨）	低端节点，此机型处理性能为0.5Gbps探针服务器或0.05Gbps DNS流探针。
	配套	
G0MYSQL04	系统软件-Light Application Data Management Software Package(5.6 E)，1年标准产品服务-Paper License	
CIS-LNX-CD	Linux预安装软件	
SC1GSUSE1101	Novell SuSE LINUX Enterprise Server 11，1年7*24服务	