天阗入侵检测与管理系统 V7.0

天阗入侵检测与管理系统 V7.0，是业内第一款全流量存储的攻击取证溯源产品，产品通过精确存储网络中的全部流量数据，用于对攻击行为的取证（原始数据）、攻击链溯源、攻击证据在线分析、数据业务分析、数据传输时序分析、历史流量回溯分析等能力，可以提供全包的自动化攻击取证、任意时刻的威胁溯源分析、历史流量的回放重复检测等能力。

天阗入侵检测与管理系统 V7.0 具备完整攻击链的全过程信息存储和展示，实现完整的攻击过程在网络数据传输中的快照，根据自动查询规则或手工查询的方式，展示出整个攻击链的所有相关信息；此外，全流量分析取证系统可协助识别网络攻击的有效性，实现网络攻击超低误报，通过全流量分析取证设备上记录的完整攻击过程信息和客户端/服务器行为，能够帮助安全检测设备快速准确甄别误报信息；全流量分析取证系统还可以实现基于多种复杂流量组合的攻击过程分析；在 pcap 原始数据、协议元数据、流统计信息等全维度信息的基础上，实现在线/实时、离线/批量的安全模型分析。帮助企业从源头上解决企业网络中的安全问题，尽可能地减少安全威胁对企业带来的损失。

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

一、核心功能

数据包线速捕捉技术

天阗入侵检测与管理系统 V7.0 提供 100%精准、可靠的高性能数据包记录功能，为每个数据包提供纳秒级时间戳，支持以 NTP、PTP 方式获取时间，数据包级保序，确保高速网络场景下不丢包，数据采集采用最新的 Intel DPDK 技术，能够大幅提升数据包的采集性能，获得更好的成本和性能优势，针对海量数据的采集，采用数据聚合、数据落盘时写入大文件的方式进行数据存储，网络数据包缓存到指定阈值大小后一次性写入，可确保基于大块文件的顺序写 IO 操作，可以实现高效的数据顺序写操作，充分利用多磁盘并发的性能。

零碎片存储技术

针对数据的存储方法，直接决定数据的检索速度。天阗入侵检测与管理系统 V7.0 产品针对海量原始数据的存储，采用数据聚合、数据落盘时写入大文件的方式进行数据存储，实现高效的数据顺序写操作，网络数据包缓存到指定阈值大小后一次性写入，可确保基于大块文件的顺序写 IO 操作，充分利用多磁盘并发的性能。

高速检索技术

天阗入侵检测与管理系统 V7.0 产品能够从海量的历史数据快速中查询到攻击原始数据，这依赖于强大的灵活高效的检索技术支持。天阗入侵检测与管理系统 V7.0 以时间段+五元组信息+子网 ID 的组合作为最直观通用的检索方式。

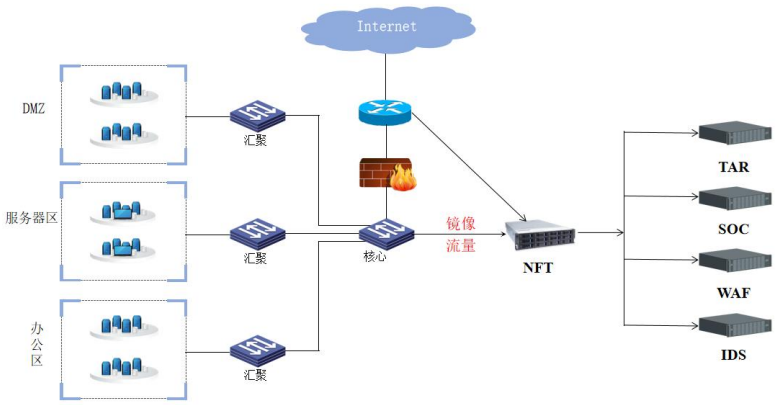
通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

二、产品部署

单节点部署方案

适用场景：流量较低、原始数据存储时间较短的场景。

部署方案：旁路部署在核心交换机处，通过镜像的方式，将流量镜像到天阗入侵检测与管理系统 V7.0 产品上采集分析。单机部署同样支持多个流量采集点，可直接将出口流量，核心流量同时接入天阗入侵检测与管理系统 V7.0 产品，实现东西向流量和南北向流量采集分析。

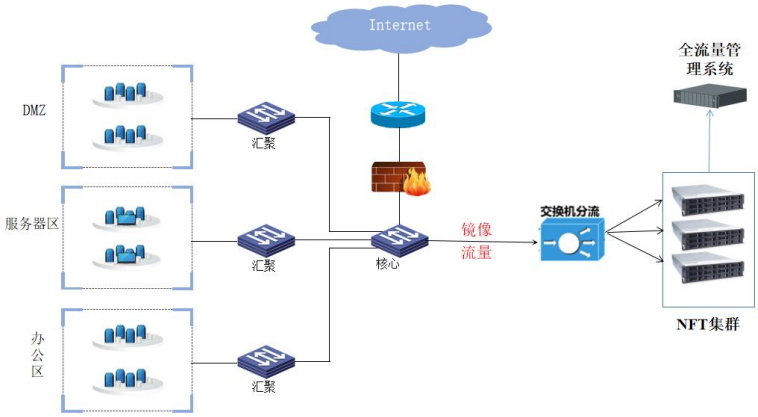


通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

集群部署方案

使用场景：流量较大、原始数据较长的场景

部署方案：通过镜像的方式，将核心流量镜像到交换机分流器上，通过分流将流量分担到不同的天阗入侵检测与管理系统 V7.0 产品上，最后通过全流量管理系统统一管理。



通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

三、产品规格

产品名称	**天阗入侵检测与管理系统 V7.0**
产品型号	**NT10000-NFT-FT-5000QA**
产品用途	主要用于基于网络全流量存储能力，实现对威胁的原始流量分析和任意时刻流量的调查取证，快速实现攻击行为的取证研判和攻击链溯源。
产品配置	国产化硬件设备，标准机架式设备，高度 2U，冗余电源，采用 FT-2000+/64 核处理器，银河麒麟 V10 操作系统；配置 256G 内存，96T+960GB*2 SSD 硬盘，配置 4 个千兆电口，4 个千兆光口，4 个万兆光口；
产品性能	实际网络环境处理能力（混合包、混合流）：5Gbps，
	数据检索速度：120TB/秒。
产品功能	1、支持旁路部署，支持采集镜像、分光、分流的原始流量数据包。
	2、具备全包采集能力，采用软件级汇聚分流，无需借助其他硬件，具有实时流量复制分发功能，可将接收的流量实时转发，流量复制接口支持 web 页面灵活设置，支持一进一出、一进多出、多进一出、多进多出的流量复制分发能力。
	3、具备捕获过滤功能，产品支持 BPF 语法过滤和流过滤条件过滤,过滤条件包括源 IP、源端口、目的 IP、目的端口、协议、VLANID 等，支持与、或、非的组合方式过滤流量。
	4、支持数据包 100%全包存储，无数据截断，无丢包。
	5、支持检索单个数据包落盘大于 8GB，可自定义设置最大落盘流量。
	6、支持存储过滤功能，支持配置报文只解析不存储策略规则，可查看到对应解析会话日志，无法下载对应报文。
	7、支持应用协议识别，包括 140 种应用子分类，49000 种应用协议。

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

	8、支持应用自定义，定义规则包括：IP、协议、端口、签名，签名类型包括十六进制和 ASCⅡ两种方式。
	9、支持协议自定义解析，能够完成私有协议解析工作。
	10、支持 HTTP、TELNET、FTP、POP3、SMTP、IMAP、DNS、RLOGIN、SSL、ICMP、SSH、TFTP、RDP、SMB、SNMP、NTP、MYSQL、NGAP、GTPU、PFCP、EGD、IEC104、OPCUA、CIP、BACNET、ENIP、S7COMM、MODBUS 等不少于 60 种协议元数据解析提取。
	11、支持 SSL 元数据解析，可支持提取服务器名称、客户端指纹、服务端指纹、SSL 版本、SSL 加密套件、证书发布者、证书使用者、证书有效期等元数据信息。
	12、支持资产关联分析，可对任意资产地址进行回溯关联，通过点状图可视化呈现资产连接情况，快速判断访问路径。
	13、支持流量统计分析，支持资产流量数据统计分析功能,可图形化展示对应资产流量信息,包括上行流量、下行流量、总流量、访问次数 TOP 访问主机、TOP 访问资产、TOP 访间应用等。
	14、支持离线数据包导入功能，支持本地数据包 WEB 页面直接上传、FTP 站点数据包导入分析等，能够支持离线数据包分析功能，支持离线数据包流量信息统计分析，包括:总流量大小、上行流量大小、下行流量大小、平均包长、会话数统计、数据包统计、协议占比、TOP 主机、TOP 目的端口等；
	15、支持协议元数据解析，可按照 url、referer、cookie、accept 等元数据字段信息进行模糊、精确检索；
	16、支持统计分析流量会话信息，包括会话五元组、开始结束时间、总字节数、总包数、应用协议、源目地理位置、持续时长等;；
	17、支持基于情报和特征信息的回溯分析，可快速发现离线数据包中

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博

	的攻击行为。
	18、支持实时统计检索 PCAP 文件的需检索容量、已检索数据容量，落盘 PCAP 文件的包数量、流数量、字节数以及数据落盘起始时间。
	19、支持 IP 通联关系分析,可对任意主机 IP/IP 对进行任意时间段内图形化展示主机IP通连关系,可区分展示目标IP访问/被访问星状关系图，星状图支持 5 层访问关系下钻分析，以此获取更为深层次的访问信息，支持图像化展示主机通联关系，支持统计分析访问 IP、访问域名、整体流量情况，支持自动关联威胁告警信息，支持一键下钻获取对应会话日志以及原始流量。
	20、支持隧道检测功能，支持 HTTP 隧道检测、HTTPS 隧道检测、DNS 隧道检测，可精准识别风险隧道通信情况，支持告警加白功能。
	21、支持通过对主机正常网络访问数据（如流量大小、访问频率、协议类型、连接对象等）进行统计分析形成的主机画像，可进行基于流量访问基线的狩猎，返回分析结果，可进行流量异常告警，支持异常行为建模功能，支持添加单向、双向检测模型，模型元素包括：地理位置信息、资产分组、IP 地址、端口信息、应用协议以及对应的协议元数据，包括 url、host-name、cookie、请求方法、响应码等。
	22、支持历史流量特征捞捕功能，有对应告警信息，支持自定义 0day/1day 漏洞攻击特征，可溯源历史网络流量中是否遭受过此项攻击，从而发现前期无法检测到的未知攻击行为并可进行 PCAP 在线分析确认以及 PCAP 下载取证。
配套资料、配件	提供完整的用户手册，含纸质版 1 套和光盘 1 张。
	配件含万兆光纤 2 根，普通直连网线 2，电源线两根

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin
官方微信　官方微博