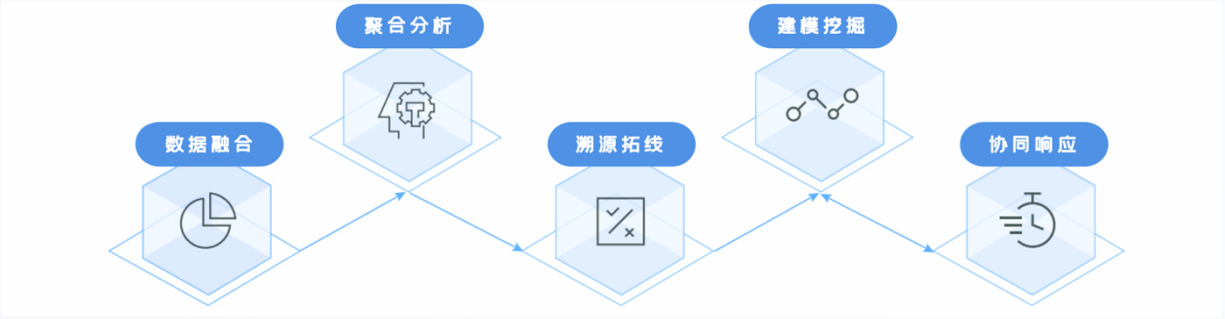
全流量融合分析平台

一、需求分析

随着企业数字化转型和网络架构的日益复杂，网络流量数据呈现海量化、异构化、分散化的特点。传统基于单一数据源或独立分析工具的分析模式，已难以满足对网络性能全局洞察、安全威胁精准溯源和业务体验保障的综合性需求。构建一个统一的全流量融合分析平台，旨在打通不同来源、不同格式的网络数据孤岛，通过关联分析与深度挖掘，实现从网络基础设施到上层应用业务的全景可视、融合分析与协同处置，提升网络运维效率、安全防御水平和业务支撑能力。

二、产品简介

全流量融合分析平台是启明星辰自主研发的，集成并处理来自各类监测探针的数据，通过深度挖掘与综合分析，动态优化监测策略与检测规则，从而形成集数据汇聚、深度解析、综合判定与策略下发于一体的闭环管控能力。



平台旨在实现对安全威胁告警的高效研判与处置。一方面，针对已知威胁，平台能够对多源、海量的告警信息进行实时整合与关联分析，有效提炼关键事件，大幅降低干扰信息。另一方面，通过对网络通信会话与行为线索进行融合解析、异常识别及应用梳理，平台具备发现潜在风险与未知威胁的能力。最终，平台通过整合系统能力、协调各

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

类资源，实现跨网络的一体化联动与智能化响应。

（产品技术白皮书请通过客服获取）

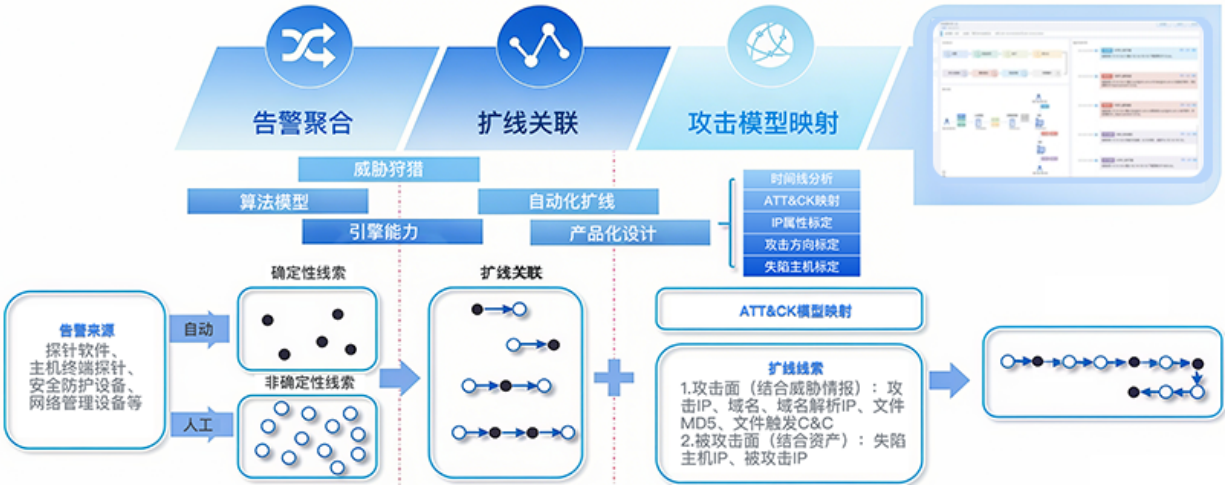
三、产品特点

告警聚合降噪

在实际应用中，由于网络环境的复杂性和异构性，不同探针产生的告警信息格式和内容往往存在差异。平台首先对异构探针告警进行统一格式转换和标准化处理。通过过滤无效日志、归并不同探针的同类告警等步骤，实现告警信息的聚合降噪。从海量告警中筛选出需要快速处置进行防御能力提升的薄弱点，并以较强的可解释性、明确的漏洞说明、处置建议辅助一线用户快速进行威胁排查和事件处置。

攻击过程还原

引入攻击链模型和 ATT&CK 模型分析从侦查、渗透、攻陷、控制、破坏一整套攻击流程进行事中监测，威胁定位；利用流量日志融合，提供更多攻击上下文信息，在调查和攻击溯源方面进行事后取证，案例总结。



同时可依托系统内置的关联模型，自动关联与事件相关的强、弱线索，结合人工上传研判信息，实现对事件的综合拓线分析。提供攻击分析池进行数据输入定制还原和自

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

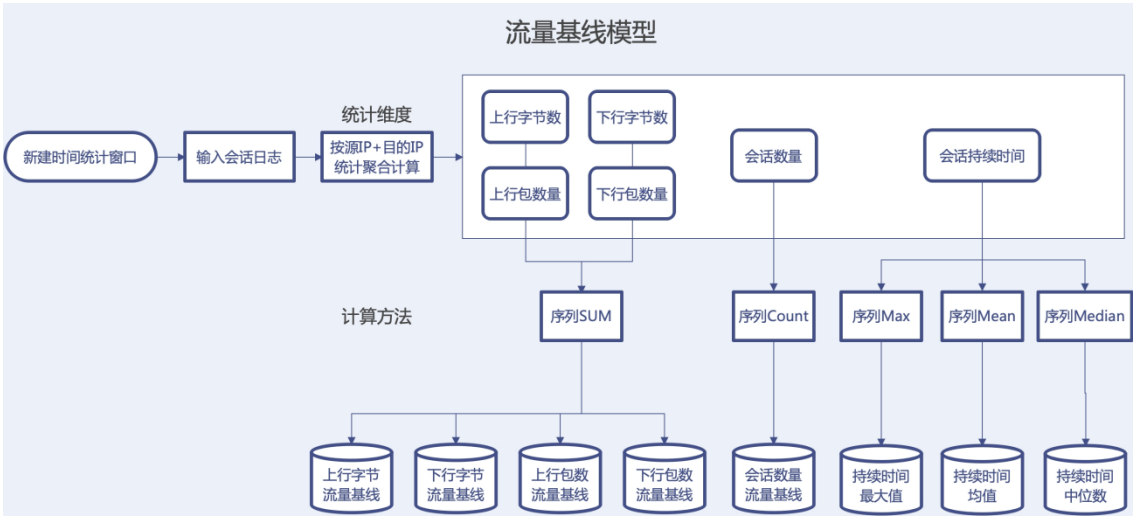
动还原攻击链功能，攻击分析池中的数据可按照攻击时序进行自动还原也可自定义攻击链还原模板进行攻击链还原。

告警协同处置

提供自动化任务分配功能，以目标为导向，将日常具体的各项工作内容固化为工作流上的一个节点，通过有序的排列组合，编排为某一重复工作的一个工作流程。通过统一下发任务的方式，对任务活动进行灵活编排，按需把任务分发给不同逻辑位置上的角色，支持进行任务拆解和共同处置。提供数据源、数据动作、联动响应的配置；可针对系统采集的告警进行原始流量分析、样本提取、关联分析、攻击链还原、告警加白、告警降级和综合研判进行分析任务分配，最终对各模块结果进行聚合复用和综合研判。

通信会话建模分析

通信会话建模分析在会话角度，建立基于资产的稳定访问关系，并结合专家经验进行网络资产梳理。



目标画像模型基于网络设备资产数据和网络通信行为数据构建而成，以资产数据的 IP 为关联条件对会话日志的源、目的 IP 添加资产属性标记，包括资产的名称、设备类型、地理位置、开放的端口以及每个端口所对应的服务，针对标记资产信息后的会话日志分

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

析其业务服务身份。上图是一个流量基线模型建立的过程示意图，利用该模型可统计网络会话日志并生成流量基线。在网络安全领域，流量基线模型是一种重要的工具，它通过对网络会话日志的统计分析，生成一个表示正常网络活动的参考标准。当实际流量与这个基线出现较大偏差时，系统可以及时发现异常情况，从而采取相应的措施。

未知威胁挖掘

针对未知网络攻击，利用基于会话日志数据流的未知攻击线索发现建模方法，基于资产的稳定访问关系进行异常线索发现。未知攻击线索发现方法包括新增异常检测、流量异常检测和行为异常检测。

新增异常检测基于主机 IP 的稳态端口集合发现新增异常端口；基于主机 IP 之间的稳定访问方式，包括协议和端口，发现新增异常访问方式；基于主机 IP 之间的稳定访问关系，发现异常新增访问关系。

流量异常检测利用会话流量特征信息，包括上下行字节数、上下行包数量、会话持续时间和会话数量，建议主机 IP 之间的会话流量基线。基于历史会话流量基线，预测下一时刻的正常流量指标范围，如果出现偏离正常范围较远则认为出现了异常。

行为异常检测则主要是针对攻击活动前期的扫描探测行为进行监视，包括端口扫描、地址扫描和病毒传播，也会对攻击活动后期的 DDoS 行为进行监视。

专题监测分析

可将重要时间段内的重要目标设定为专题，进行专项监测和分析。可总览监测目标的互联拓扑，进行互联目标核验标注。专题管理提供系统层面的全局数据重构及展示内容配置，提供所有数据源字段的组合筛选以及多维数据和资产属性的逻辑关联组合展示。可以图表方式展示筛选后的数据，用户选择进入某专题后所有的数据目标即为该专题选

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

定的数据，不再展示其他无关数据，该专题下的分析处置内容也会以专题中选定的数据为主。可辅助用户将重要资源专注于需要重点关注的专题中。

设备综合管理

支持设备综合管理，可管理现网多厂家、多类型设备，实现设备状态、资源监测，及多类数据采集，并可在平台自由抽取。系统可实现与下设设备的策略配置、下发等一键配置功能。

在功能表现上探针管理具有新增、修改、删除、连接、断开探针的能力，可在需要的时候对探针进行上下线处理。实时监测并展示探针的在线状态、CPU 使用率、内存使用率等信息。具备规则管理功能，对威胁检测规则、数据采集规则的统一管理，支持对内置规则的升级，支持创建自定义规则并发探针，平台可按需自由抽取下设各类探针的原始流量。

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、产品规格

产品名称	全流量融合分析平台
产品用途	全流量融合分析平台是网络安全运营的智能分析决策中心。它通过深度关联多源数据，实现对已知威胁的精准告警研判与未知风险的主动挖掘，同时支撑网络与业务性能的快速故障定界，全面提升组织的主动防御能力和运维效率。
产品性能	具备分布式架构，支持对日均 TB 级原始流量的实时摄入、解析与存储，数据处理延迟不高于 1 分钟。
产品功能	支持标准化接口，可接入并解析至少包括元数据、威胁告警、原始流量在内的多类型数据源。
	全流量存储与回溯，支持原始流量数据与元数据的长期存储，关键数据可回溯查询时长不低于 30 天。
	关键业务流性能监控基线，能够针对指定的关键业务自动学习其正常情况下的流量平均值、流量峰值、流量最小值等基线，并对偏离基线情况进行告警。
	异常行为建模与检测，提供基于机器学习的无监督异常检测能力，可对网络通信、用户行为进行基线建模，并自动发现偏离基线的可疑活动。
	攻击链可视化与调查，具备交互式调查界面，可对安全事件进行攻击链全景展示，支持从告警钻取至原始流量会话记录。
	全网资产自动发现与画像，能够自动识别并梳理网络中的活跃 IP、应用与业务群落，持续更新资产画像及访问关系图谱。
	多人协同研判工作台，支持安全事件或线索的在线分派、协同标注，所有调查过程与结论可关联记录，形成完整的研判案例。

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

	标准化协议输出，平台具备将内部标准化后的数据，以标准协议（如Syslog、Kafka）向外输出能力，供第三方系统消费。
产品扩展性	具备数据外发接口，支持将系统业务告警数据、日志数据、运行数据等关键数据上报至安全大数据平台，实现安全数据集中存储，支撑安全数据汇聚分析。
	预留策略上报、策略接收接口,支持安全策略集中管控系统对安全策略的统一管理。
	软件运行稳定性方面，应严格执行软件工程化要求，并采取避错设计、查错设计、容错设计等措施，产品连续工作 7X24 小时无故障,应尽量采用成熟技术及简化、冗余备份、模块化设计。
	系统可维护性方面，错误信息提示应明确有效，便于故障分析与排除，记录系统运行日志、异常日志及故障信息。
	具备容错能力,在非硬件故障或非通讯故障时，算法能够保证正常运行，并有足够的提示信息帮助用户有效正确地完成任务。
	适配主流国产自主可控软硬件平台；
	支撑开展必要的系统集成工作与定制开发工作。
产品可靠性	平均故障恢复时间≤30 分钟

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