招标项目技术、服务、政府采购合同内容条款及其他商务要求

前提：本章中标注“*”的条款为本项目的实质性条款，投标人不满足的，将按照无效投标处理。

（一）. 项目概述

1.项目概况：本项目共1个包，采购成都市公共卫生临床医疗中心新老院区网络改造（内外网安全隔离）

2. 本招标文件中“制造厂家”,“制造商”,“生产厂商”指代的均为同一对象。

3.标的名称及所属行业：

包号：01	品目号	标的名称	所属行业
	1-1	核心交换机	工业
	1-2	汇聚交换机-1	
	1-3	汇聚交换机-2	
	1-4	接入交换机-1	
	1-5	接入交换机-2	
	1-6	硬件支撑平台	
	1-7	终端安全管理系统	软件和信息技术服务业
	1-8	防火墙	工业
	1-9	APT高级威胁检测平台	软件和信息技术服务业
	1-10	文件威胁鉴定系统	

	1-11	数据库审计系统	

＊（二）. 商务要求

1. 交货期及地点

1.1 交货期：合同签订后3个月内完成实施、培训。

1.2 交货地点：成都市公共卫生临床医疗中心。

2. 付款方法和条件

合同签订后7日内预付合同总金额的30%，货物安装、调试验收合格后30日内支付合同总金额的65%，余下5%合同款待验收合格一年期满后7日内无息支付。

3.质保期

3.1质保期:（硬件）原厂质保三年;（软件）原厂三年协议特征库升级更新服务。

3.2质保期内卖方应负责设备维修及抢修。

4.安装调试及验收

4.1卖方负责全院（含静居寺院区、航天院区）所有外网信息点位的综合布线系统工程（包含综合布线材料、工程施工、调测、各类辅助材料、配件及技术支持等各项工程实施服务)。

4.2卖方负责设备安装、调试。

4.3 货物到达生产现场后，卖方接到买方通知后7日内到达现场组织安装、调试,达到正常运行要求,保证买方正常使用。所需的费用包括在投标总价格中。

4.4卖方应就设备的安装、调试、操作、维修、保养等对买方维修技术人员进行培训。设备安装调试完毕后，卖方应对买方操作人员进行现场培训，直至买方的技术人员能独立操作，同时能完成一般常见故障的维修工作。

4.5根据《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号），相关国家行业规范及招标文件要求为验收依据进行验收。双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由采购人在招标文件与投标文件中按质量要求和技术指标比较优胜的原则确定该项的

约定标准进行验收。如产品验收不能满足招标文件要求，或者投标人虚假响应招标文件要求导致产品不能达到招标文件要求的，合同设备经中标供应商 1 次优化、维修或设备上线后 5 个工作日内仍不能达到上述质量及验收标准的，采购人有权退货，并视作成交人不能交付货物而须支付违约赔偿金给采购人，采购人还可依法追究成交人的违约责任。

5.售后服务

5.1 备件送达期限：在设备的使用寿命期内，卖方应保证国内不超过 7 天。

5.2 终身零配件供应：投标人应保证设备停产后的备件供应保证 10 年，并以优惠的价格提供该设备所需的维修零配件。

5.3 质保期后，卖方应向用户提供及时的、优质的、价格优惠的技术服务和备品备件供应。

（三）.技术、服务要求

序号	名称	技术指标	数量	单位	备注
	核心交换机	▲1、整机槽位数量≥5 个，配置冗余引擎后，整机业务槽位数量≥3 个；整机交换容量≥19Tbps，包转发率≥2800Mpps，以官网公布最小值为准（提供官网截图证明材料复印件）； ▲2、配置要求：配置双主控引擎，电源数量≥2 个，千兆电端口数量≥24 个，万兆 SFP+光端口数量≥24 个；万兆单模光模块≥20 个；万兆多模光模块≥240 个； 3、支持 N：1 虚拟化功能（N≥4），将多台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合；	2	套	

		4、支持 1：N 虚拟化功能，将一台物理交换机虚拟化成 N 台逻辑交换机，交换机间硬件独立且相互隔离，并且支持虚拟化融合功能在 N:1 虚拟化系统实现 1：N 虚拟化功能（提供国家认可的检测机构出具的检测（或测试）报告复印件，报告封面应有 CMA 或 CAL 或 CNAS 标志）； 5、支持将核心/汇聚和接入设备通过纵向虚拟化技术形成一台纵向逻辑虚拟设备； 6、支持 FCOE、TRILL、EVB、OpenFlow 等功能。 7、支持 VxLAN 二层、三网关能力； 8、支持 CPU 防护攻击能力，保障 CPU 工作安全（提供国家认可的检测机构出具的检测（或测试）报告复印件，报告封面应有 CMA 或 CAL 或 CNAS 标志）； 9、支持环网协议，支持 RRPP、ERPS 和 RPR 等环网技术，并且平均收敛时间≤50ms； 10、支持配置 EPON 接口模块，作为 OLT 设备使用，支持 10G EPON 功能，支持 10G 对称和非对称 ONU； 11、支持 40G 和 100G 扩展，单槽位支持 40G 业务单板端口密度≥24 个,100G 业务单板端口密度≥4 个； 12、支持多速率业务接口板卡，支持 10G/5G/2.5G/1G 自适应电端口数量≥24 个； 13、支持多业务扩展安全扩展模块，至少可以提供防火墙、入侵防御、应用控制、负载均衡等安全插卡（提供官网截图证明材料复印件）； 14、支持交换机融合无线控制器功能，无需独立的 AC 板卡或带 AC 功能的接口板，即支持无线 AP 管理功能，实现有线无线网络一体化建设；			

		15、支持内置智能图形化管理功能，能够实现通过图形化界面设备配置及命令一键下发和版本智能升级功能（提供国家认可的检测机构出具的检测（或测试）报告复印件，报告封面应有 CMA 或 CAL 或 CNAS 标志）； 16、支持流量可视化管理，Telemetry 流量可视化功能。 17、支持 MACSec（IEEE 802.1ae）介质访问控制安全技术（提供国家认可的检测机构出具的检测（或测试）报告复印件，报告封面应有 CMA 或 CAL 或 CNAS 标志）； ▲18、支持多业务融合板卡，能够与设备紧耦合无需外部连线，支持内连端口备份提升可靠性；支持部署 Windows Server 及相关配套应用，实现解决方案一体化部署（提供国家认可的检测机构出具的检测（或测试）报告复印件，报告封面应有 CMA 或 CAL 或 CNAS 标志）。 *19、提供所投产品由中华人民共和国工业和信息化部颁发的电信设备进网许可证（提供证书复印件）。			
	汇聚交换机-1	▲1、设备尺寸不高于 1U，交换容量≥750Gbps，包转发率≥330Mpps（提供官网截图证明材料复印件）； 2、主机固化≥24 个 GE 端口，≥4 个万兆 SFP+口，支持个 2 个业务板卡扩展插槽；支持双电源，模块化双风扇，前/后通风，风道可调； 3、MAC 地址表≥96K，路由表容量≥48K，缓存≥5M；	2	套	

		▲4、支持实现 ERPS 功能，能够快速阻断环路，链路收敛时间≤50ms（提供国家认可的检测机构出具的检测（或测试）报告，报告封面应有 CMA 或 CAL 或 CNAS 标志）； ▲5、支持实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作（提供国家认可的检测机构出具的检测（或测试）报告，报告封面应有 CMA 或 CAL 或 CNAS 标志）； ▲6、支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms（提供国家认可的检测机构出具的检测（或测试）报告，报告封面应有 CMA 或 CAL 或 CNAS 标志）； 7、支持基于第二层、第三层和第四层的 ACL；整机提供 ACl 条目数≥8K 条； 8、支持出方向 ACL，以便于灵活实现数据包过滤；支持 802.1x 认证，支持集中式 MAC 地址认证； 9、支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换。 *10、提供所投产品由中华人民共和国工业和信息化部颁发的电信设备进网许可证（提供证书复印件）。			
	汇聚交换机-2	1、支持模块化风扇，独立的风扇插槽数量≥2 个，并支持灵活的选择风扇的出风方向； ▲2、采用紧凑型机框设计，提高机房空间利用率，设备高度≤1U，设备整机交换容量≥2.5Tbps，整机包转发率≥700Mpps（提供官网截图证明材料复印件）；	1	套	

		▲3、主机默认自带配置 10G/1G BASE-X SFP+端口数量≥24 个，40G QSFP+端口数量≥2 个；除去主机自带端口，额外支持扩展槽位数量≥2 个； 4、支持不同速率的端口灵活扩展，支持 1G、2.5G、5G、10G、25G、40G 端口扩展； 5、支持扩展防火墙安全插槽功能； 6、支持将多台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合； 7、支持 RIP、OSPF、BGP、ISIS 等三层动态路由协议； 8、主机集成无线控制器功能，无需配置 AC 插卡即可以实现对 AP 的管理，实现有线网络和无线网络一体化（提供官网截图证明材料复印件）； 9、支持并实配 VxLAN 功能，支持 VxLAN 二层、三层互通功能，支持 EVPN 功能（提供国家认可的检测机构出具的检测（或测试）报告，报告封面应有 CMA 或 CAL 或 CNAS 标志）； 10、支持适配 SDN 组网，支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换； ▲11、支持内置智能图形化管理功能，支持作为管理设备对其他成员设备管理；支持网络拓扑管理、设备列表管理等，支持对成员设备下发配置、版本升级、备份等功能； 12、配置独立的风扇模块数量≥2 个，模块化可热插拔电源数量≥2 个。 *13、提供所投产品由中华人民共和国工业和信息化部颁发的电信设备进网许可证（提供证书复印件）。			

	接入交换机-1	▲1、交换容量≥500Gbps（若官网有 X/Y 值、以 X 为准），包转发率≥170Mpps（若官网有 X/Y 值、以 X 为准）（提供官网截图证明材料复印件）； ▲2、配置≥48 个 1000M BASE-T 以太网电口，≥6 个 10G SFP+端口（提供官网截图证明材料复印件）； 3、支持 MAC 地址学习功能，整机 MAC 地址表容量≥32K； 4、支持 VLAN 中继功能，支持将本地 VLAN 配置向其他设备发送，同时还能够接收来自其他设备的 VLAN 配置，并动态更新本地 VLAN 配置，从而使所有设备的 VLAN 信息一致； 5、支持虚拟化堆叠，支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预，最大堆叠台数≥9 台； 6、支持 IPv4/IPv6 双栈，支持静态路由、RIP、OSPF 等路由协议； ▲7、设备内置图形化操作的方式，支持组网拓扑可视及管理（提供证明材料复印件）； 8、支持通过标准以太网电口进行堆叠（万兆或千兆均支持）； 9、支持 802.1X，集中式 MAC 地址认证，端口安全，端口隔离； ▲10、符合 IEEE 802.3az（EEE）节能标准，整机满负荷最大功耗≤54W（提供证明材料复印件）； 11、支持 STP/RSTP/MSTP 协议,支持 G.8032 以太网环保护协议 ERPS，切换时间≤50ms； 12、支持 OPENFLOW 1.3 标准，支持普通模式和 Openflow 模式切换；	61	套	

		13、支持 SNMP、Telemetry 协议。 *14、提供所投产品由中华人民共和国工业和信息化部颁发的电信设备进网许可证（提供证书复印件）。			
	接入交换机-2	▲1、交换容量≥500Gbps（若官网有 X/Y 值、以 X 为准），包转发率≥100Mpps（若官网有 X/Y 值、以 X 为准）（提供官网截图证明材料复印件）； 2、配置≥24 个 1000M BASE-T 以太网电口，≥4 个 10G SFP+端口； 3、支持 MAC 地址学习功能，整机 MAC 地址表容量≥32K； 4、支持 VLAN 中继功能，支持将本地 VLAN 配置向其他设备发送，同时还能够接收来自其他设备的 VLAN 配置，并动态更新本地 VLAN 配置，从而使所有设备的 VLAN 信息一致； 5、支持虚拟化堆叠，支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预，最大堆叠台数≥9 台； 6、支持 IPv4/IPv6 双栈，支持静态路由、RIP、OSPF 等路由协议； ▲7、设备内置图形化操作的方式，支持组网拓扑可视及管理（提供证明材料复印件）； 8、支持通过标准以太网电口进行堆叠（万兆或千兆均支持）； 9、支持 802.1X，集中式 MAC 地址认证，端口安全，端口隔离； ▲10、符合 IEEE 802.3az（EEE）节能标准，整机满负荷最大功耗≤54W（提供证明材料复印件）；	56	套	

		11、支持 STP/RSTP/MSTP 协议,支持 G.8032 以太网环保护协议 ERPS，切换时间≤50ms； 12、支持 OPENFLOW 1.3 标准，支持普通模式和 Openflow 模式切换； 13、支持 SNMP、Telemetry 协议。 *14、提供所投产品由中华人民共和国工业和信息化部颁发的电信设备进网许可证（提供证书复印件）。			
	硬件支撑平台	1、2U 机架式，标配导轨； 2、配置≥2 颗 Intel® Xeon® 可扩展处理器，核心数量≥10 核、主频≥2.4GHz； 3、配置≥32GB DDR4 2933MHz 内存，≥24 个内存槽位，支持 Advanced ECC 先进内存保护技术及联机备用模式，可配置 LRDIMM 和 RDIMM 内存； 4、配置≥2 块 2.4TB 12G SAS 10K 硬盘；最大可扩展至≥40 块 SAS/SATA/SSD 硬盘，支持≥30 个 NVMe； 5、支持≥10 个 PCIe3.0 插槽，≥3 块双宽或 8 块单宽 GPU 卡； 6、配置≥4 个 1Gb 以太网电接口，≥2 个 10Gb 以太网光接口（满配光模块）,支持扩展 1Gb/10Gb/25Gb 以太网卡、8/16/32Gb FC HBA 以及 100Gb IB HCA； 7、配置冗余风扇、1+1 冗余热插拔电源，功率≥550W。	1	套	
	终端安全管理系统	▲1、配置≥700 点 PC 终端防病毒功能；≥700 点 PC 终端 Windows 系统补丁更新功能；≥ 700 点 PC 终端运维管控功能。 2、控制中心：采用 B/S 架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀	1	套	

		毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能。 3、支持控制中心防暴力破解功能，采用手机APP动态令牌方式进行二次认证，针对控制中心高危操作支持动态口令验证。 4、支持中标麒麟/银河麒麟/普华/深度/红旗桌面操作系统。 5、对敲诈者病毒提供防护机制，同时提供解密工具。 6、终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁。 ▲7、防病毒的病毒查杀引擎包括云查杀引擎、AVE、QEX、QVM等引擎，支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS病毒等进行查杀，提供主动防御系统防护等功能（提供功能截图证明材料复印件）。 8、产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能（提供功能截图证明材料复印件）。 9、运维管控功能支持对终端上传下载速度与流量进行管控；支持对各种外接设备进行外联控制，并根据违规外联发生时内外网连接状态分别设置违规处理措施。 10、后续支持在同一终端管理系统客户端上平滑扩展：终端准入、移动存储介质管理、文件加解密功能模块。 11、为阻止入侵者关闭或者破坏客户端防护、以及放行勒索病毒，将阻止服务器客户端退出和卸载，终端			

		无法添加信任和开发者信任，客户端无法关闭自我保护，禁止应用程序加载驱动。 12、针对服务器系统，支持开启远程登录保护功能，加强对黑客远程弱口令扫描防护。 13、支持温度检测以折线图形式实时展示 CPU、主板、显卡、硬盘的温度变化。 14、支持终端进程的黑白红名单设置；支持网址黑白名单策略；支持对终端各种外设、接口设置使用权限；支持对终端桌面系统的账号密码、本地安全策略、控制面板、屏保与壁纸、浏览器安全、杀毒软件检查进行管控策略配置。 *15、提供所投产品由国家公安部颁发的计算机信息系统安全专用产品销售许可证（提供证书复印件）。			
	防火墙	▲1、多核架构，标准 2U 机架式设备，冗余电源，配置≥6 个 10/100/1000M 自适应电口，≥4 个千兆 SFP 光接口，支持预留≥2 个扩展槽（支持扩展≥8 个万兆光口）；网络处理能力≥14G，并发连接≥300 万，每秒新建连接≥22 万/秒；配置防火墙安全防护全功能模块，包括：应用特征库/URL 网址过滤/AV 防病毒/IPS 入侵防御/威胁情报。 2、支持 VTEP（VxLan Tunnel EndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI（VXLAN Network Identifier）、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定。 ▲3、支持配置基于 IPv6 地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL 过滤、应	1	套	

		用识别、反间谍软件等安全功能；支持针对 IPv6 流量通过 HTTP、HTTPS 实现 Web 认证，用户身份信息可存储在本地或 Active Directory\Radius\TACACS+\POP3 等第三方服务器；通过 HTTPS 实现 Web 认证必须支持使用本地 CA 颁发的证书同时使用证书验证客户端身份（提供功能截图证明材料复印件）。 4、支持虚拟防火墙功能，在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计。 5、支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类;支持在防火墙间谍软件签名库直接查阅攻击的名称、严重性、描述等信息。 ▲6、产品的漏洞防护特征库支持包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息（提供功能截图证明材料复印件）。 7、支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断。 ▲8、产品须支持与现网部署的终端安全管理系统联动，实现基于终端健康状态的访问控制，支持阻断			

		“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址（提供功能截图证明材料复印件）。 9、支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括 Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常、IP 分片等；并可在设备页面显示每种攻击类型的丢包统计结果。 10、支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的防护。 *11、提供所投产品由国家公安部颁发的计算机信息系统安全专用产品销售许可证（提供证书复印件）。 *12.提供所投产品由中国信息安全认证中心或中国网络安全审查技术与认证中心按国家标准认证颁发的有效认证证书（提供认证证书复印件）。			
	APT 高级威胁检测平台	1、系统采用大数据核心分析平台及流量采集探针架构，均为独立硬件。 ▲2、核心分析平台：2U 标准机架式设备，冗余电源，配置≥4 个千兆电口，≥3 个 USB3.0 接口，内存≥128G；≥960G SSD 存储硬盘及≥32TB SATA 存储硬盘。 ▲3、流量采集探针：2U 标准机架式设备，配置≥6 个千兆电口，≥1TB SATA 存储硬盘，吞吐≥1.5Gbps，配置入侵检测、网站漏洞利用、webshell 上传和威胁情报功能模块。	1	套	

		4、支持以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产。 5、支持以受害资产维度进行分析，分析内容包括失陷状态、受到的攻击类型、威胁级别、处于的攻击阶段、所属的资产分组。 6、支持基于威胁情报的威胁检测，检测类型包含APT 事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报。 7、应用安全的细分维度包括：WEB 安全、数据库安全、邮件安全、中间件安全；系统安全的细分维度包括：主机爆破、弱口令、未授权行为、挖矿行为。 8、支持对告警进行加白，加白参数包括受害 IP、攻击 IP、威胁情报、规则、XFF、URL、威胁名称。 9、支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等。 10、支持对业务资产主动外连行为检测，包含：外连 IP、外连 IP 归属、服务商、外连流量大小。 11、支持检索异常报文、域名解析、文件传输、FTP 控制通道、LDAP 行为、登录动作、邮件行为、MQ 流量、网络阻断、数据库操作、SSL 加密协商、TCP 流量、Telnet 行为、UDP 流量、WEB 访问等网络流量日志，并可基于时间、IP、端口、协议、上下行负载等多重字段组合进行日志检索。			

		12、支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力。 13、支持大屏展示网络攻击态势，包括整体网络风险指数、告警总数、攻击次数、攻击 IP 数、攻击源国家/地区 TOP5、攻击态势，并支持自动翻转的攻击全景地图展示。 14、支持基于 IP 地址的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断。 ▲15、产品支持与现网部署的终端安全管理系统进行联动，发现威胁事件后支持在终端上进行追踪溯源发现相应的恶意进程并对其进行查杀（提供功能截图证明材料复印件）。 ▲16、产品支持与现网部署的防火墙进行联动，发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断，将策略下发给防火墙，由防火墙执行阻断（提供功能截图证明材料复印件）。 *17、提供所投产品由国家公安部颁发的计算机信息系统安全专用产品销售许可证（提供证书复印件）。			
	文件威胁鉴定系统	▲1、2U 标准机架市设备，冗余电源；配置≥4 个 10/100/1000 自适应电口；≥4 个 USB 接口；配置≥960G SSD 存储硬盘及≥4TB SATA 存储硬盘。 2、支持 windows XP、windows 7、windows 10、Windows Server2003/2008/2012、Linux（含 CentOS7 32/64bit、Debian）、Android4.1 等操作系统和软件部署环境。 3、支持对移动应用文件 apk、压缩文件（zip、rar、7z、gz、ace、arj、z、bz、tar、tgz、cab、lzh、iso、rpm、deb 等）、linux 文件（shell、elf、perl）等进行检测分析。	1	套	

		4、支持 office 内嵌的宏、OLE 对象，PDF 内嵌的 JavaScript、附件，JPG 等图片内嵌的 PE 对象提取。 5、支持对文档类文件(doc、xls、ppt、pdf、docx、xlsx、pptx、rtf、wps 等)进行检测分析。 6、支持多种静态属性分析功能，包括提取文件图标、检测样本是否内嵌 PE 文件、是否包含宏代码、是否含有 shellcode、是否有密码保护、是否有 URL 链接等。 ▲7、支持灵活设置动态检测策略，包含全过动态、全不过动态和基于策略选择、基于选定文档类型、静态风险系数等策略配置（提供功能截图证明材料复印件）。 ▲8、支持动态行为监控功能可监控文件、进程、网络、注册表等操作相关的系统和内核调用接口（提供功能截图证明材料复印件）。 9、支持按一定时间间隔和分析事件对样本在虚拟机系统内的分析过程截图；并可智能化对动态分析过程截图去重。 10、支持提取利用漏洞攻击行为中的攻击代码，实现未知漏洞攻击检测。 *11、提供所投产品由国家公安部颁发的计算机信息系统安全专用产品销售许可证（提供证书复印件）。			
	数据库审计系统	1、标准 1U 机箱，专用硬件平台和安全操作系统，内置硬盘容量≥1T，主机配置≥6 个千兆自适应电口（包含 2 组 bypass），1 个 Console 口，事件处理能力≥10000 条/秒。 2、能支持：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用 Gbase、神舟、REDIS 等数据库的审计。 3、全面支持后关系型数据库 Cache 的审计，包括 terminal、portal、studio、Sqlmanager、MedTrak 等工具访问的审计，Portal 可审计 Sql 语句、查询	1	套	

		Global 变量以及二者的返回内容，Terminal 可审计M 语句及返回内容，MedTrak 可审计工号、操作报表以及二者的返回内容，studio 可审计到编译、代码更改等操作，Sqlmanager 可审计数据库账号和操作的 sql 语句。 4、在无需重启被审计数据库的情况下，支持对 MS SQLSserver 加密协议的审计，可正常审计到数据库账号、操作系统用户名、操作系统主机名等身份信息。 5、支持 B/S 架构 Http 应用三层审计，可提取包括应用系统的人员工号（账号）的身份信息，精确定位到人，并可获取 XML 返回结果。支持 C/S 架构 COM、COM+、DCOM 组件的三层审计，可提取应用层工号（账号）的身份信息，精确定位到人；支持框架：tomcat、apache、weblogic、jboss。 6、审计策略支持 18 种以上分项响应条件，可支持数据库操作命令（包括 select、create 等 14 个命令）、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端 MAC、客户端 IP、客户端端口、进程名、会话 ID、关键字、时间（含开始结束日期）等。 7、支持对 SQL 注入、跨站脚本攻击等 web 攻击的识别与告警。 *8、提供所投产品由国家公安部颁发的计算机信息系统安全专用产品销售许可证（提供证书复印件）。 *9.提供所投产品由中国信息安全认证中心或中国网络安全审查技术与认证中心按国家标准认证颁发的有效认证证书（提供认证证书复印件）。			