五、开标一览表

采购单位：吉林省吉林中西医结合医院

标书编号：采购计划-[2023]-00070-J2023ZCY108

项目名称	投标报价 （单位：元）	投标保证金	供货期
吉林省吉林中西医结合医院购置网络版杀毒软件内外网服务器授权与防毒墙项目	987,745.00 元	有	合同签订后 7 日内

单位名称（盖章）： 吉林市网众惠诚科技有限公司

法定代表人（负责人）盖章：

日期： 2023 年 10 月 8 日

备注：

1、投标报价应包括材料款、货物款、附件款、安装调试费、运输费、税费、保险费、公证费及到达指定地点验收前的其他一切费用。

2、开标一览表中须填报所投报各包的投标报价的总价，无需填报每包中所涉及的具体单项价格。

3、开标一览表中投标总价须与投标文件中投标报价明细表的投标总价保持一致，如出现不同，以开标一览表中价格为准。

六、报价明细表

序号	货物名称	性能技术指标要求	单位	数量	投标品牌/型号	单价（元）	合计（元）	备注
1	安全云主机深度病毒防护系统	1.防病毒功能：病毒保护,Web 信誉度检测功能 2.系统支持两种安装部署模式,需要安装客户端的轻代理模式和无需安装客户端的无代理模式,两种模式可以混合使用。 3.轻代理模式客户端支持 Windows、RHEL、CentOS、OracleLinux、SUSE、Ubuntu、Debian 等操作系统。 4.系统提供Windows和Linux批量化安装部署脚本，主机分组、安全策略、更新源等脚本内容参数支持用户按需选择，并自动生成。 ★5.系统控制台支持横向扩容,支持多节点集群化部署，保证系统高可用性。控制台离线，客户端仍可进行安全防护。 ★6.支持接入外置企业级数据库,防止因数据库异常导致数据丢失,安全策略无法下发，包括且不限于 SQLServer，Oracle，Postgresql 等。 ★7.针对大规模部署场景下提供分布式更新方式，可以把任意客户端，设置为分布式的更新源,可指定任意客户端从此更新源进行更新。 8.支持通过网络掩码或 IP 范围查找未安装客户端的计算机，并且将发现的 IP 解析为主机名方便管理。 9.支持与 VMwarevCenter,新华三 CAS、华为 FusionCompute 等云平台对接,同步虚拟机相关信息。	套	40	亚信安全云主机深度安全防护系统应用软件 Deep Security V20.0 有代理防病毒模块	1,495.00	59,800.00	

		10.应提供自动分组功能，可配置分组策略，策略包括不限于主机名、操作系统、IP 地址、安全策略、物理机/虚拟机/Docker 主机分类等。 11.勒索病毒：支持通过行为监控的方式，如检测可疑活动和未经授权的更改，防止勒索软件感染，并提供针对勒索软件事件专有历史纪录和勒索软件统计的监控组件。 12.恶意站点拦截：具备 web 信誉库，通过 Web 信誉支持阻止主机访问恶意站点，支持恶意站点自定义。 13.包含 40 台虚拟机授权，一年软件升级服务。						
2	安全云主机深度补丁防护系统	1.入侵检测、虚拟补丁、防火墙功能。 2.网络访问控制：支持网络访问控制功能，自定义防火墙策略，支持 IP、MAC 地址、端口，支持协议：TCP、UDP、ICMP、ICMPv6、IGMP、IDP 等，支持 IPv4、IPv6、ARP、RARP 等。 ★3.安全标签：支持 NSX 安全标签，一旦检测到恶意威胁，可将 NSX 安全标记应用于受保护的 VM，NSX 安全标记可与 NSXServiceComposer 一起使用，以自动执行某些任务，例如隔离受感染的 VM。 4.入侵防御：支持网络入侵攻击的防护，包含支持防护 SQL 注入，Cookie 注入，命令注入，跨站脚本(XSS)，跨站请求伪造(CSRF)，WebShell 攻击防护等。 5.入侵防御：内置入侵防御的规则库，支持关联 ATT&CK 框架的技术 ID，便于了解网络入侵技战术点。 6.漏洞防护：通过流量检测技术，实现漏洞利用的攻击防护，支持操作系统、	套	40	亚信安全云主机深度安全防护系统应用软件 Deep Security V20.0-有代理深度包检测模块	2,470.00	98,800.00	核心产品

		数据库、邮件服务、办公软件、中间件、Web 应用、应用等类型的漏洞。 7.漏洞扫描：提供操作系统和应用漏洞扫描功能，根据扫描结果自动下发对应的防护规则。 8.定制规则：支持 0Day 漏洞暴露后，快速定制入侵防御规则，包括不限于签名、特征码、XML 等方式，进行 0day 的快速防护，同时可支持配置优先级、检测或阻止模式、严重性等。 ★9.SSL 流量支持：支持对 https 流量的识别，支持配置 SSL 证书及密码进行解密。 10.报文捕获：支持对恶意流量的报文进行捕获，将 HTTP 流量转化为事件日志，支持溯源及审查。 11.支持 SSH 弱口令扫描，支持端口、超时时间、重试次数配置，可配置密码字典和白名单。 12.针对隐藏在操作系统日志和应用程序日志中的重要事件，如暴力破解、日志非法清除、非法添加用户等高风险事件自动化实时告警。 13.包含 40 台虚拟机授权，一年软件升级服务。						
3	防病毒软件网络版	1.防病毒软件（客户机版）解决方案。抵御病毒、间谍软件、网络钓鱼和其它灰色软件的攻击。同时提供集中的管理、监控、更新和部署等功能，并具备主机防火墙、爆发阻止、Web 站点信誉服务、预测机器学习、行为监控、勒索病毒防护等能力。支持平台：WindowsXP/7/8/8.1/10/11。 2.产品管理端需要提供工具集，针对管理端、客户端提供用于自身配置的工具。同时 WEB 界面，需要提供有关如何	套	200	亚信安全防毒墙网络版软件 V16.0	198.00	39,600.00	

		使用工具的帮助信息； 3.产品需要支持根据 IP 地址（包含 IPv6）、操作系统、在线状态、处理器结构、病毒码版本、防火墙状态、爆发阻止状态等条件的组合搜索出符合条件的终端进行管理； 4.为适应配置低的终端需求，不影响生产办公，终端在进行手动以及预设扫描时必须可以设置扫描时 CPU 占用比例，分高、中、低三个级别。低占比下不得超过 CPU 使用率的 20%； ★5.支持基于程序行为评估其可信度，并阻止未授权更改； ★6.产品需提供多种扫描引擎不少于五种，针对于机器学习必须使用独立扫描引擎，同时所有防毒引擎必须为自主知识产品非 OEM 产品； 7.对于文件扫描方式至少支持三种以上，包括所有文件统一措施、推荐扫描措施、以及针对不同类型病毒/恶意软件提供不同扫描措施，同时不同病毒/恶意软件类型不少于 7 种分类。 8.★8.扫描策略必须包含清除、隔离、删除处理措施，同时还应具备对病毒/恶意软件的不予处理、拒绝访问、更名等措施，以保证对于文件处理的灵活性； 9.支持云安全扫描和传统病毒码扫描两种运行方式； 10.产品需要支持主机入侵检测系统； 11.可对插入移动存储引导区或者移动设备的所有文件进行扫描设置； ★12.具备 Web 信誉评估功能，包含 HTTPS 通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新。						

		13.包含 200 台终端授权，一年软件升级服务。						
4	安全云主机深度病毒防护系统	1.防病毒功能：病毒保护,Web 信誉度检测功能 2.系统支持两种安装部署模式,需要安装客户端的轻代理模式和无需安装客户端的无代理模式,两种模式可以混合使用。 3.轻代理模式客户端支持 Windows、RHEL、CentOS、OracleLinux、SUSE、Ubuntu、Debian 等操作系统。 4.系统提供Windows和Linux批量化安装部署脚本，主机分组、安全策略、更新源等脚本内容参数支持用户按需选择，并自动生成。 ★5.系统控制台支持横向扩容,支持多节点集群化部署，保证系统高可用性。控制台离线，客户端仍可进行安全防护。 ★6.支持接入外置企业级数据库,防止因数据库异常导致数据丢失,安全策略无法下发，包括且不限于 SQLServer，Oracle，Postgresql 等。 ★7.针对大规模部署场景下提供分布式更新方式，可以把任意客户端，设置为分布式的更新源,可指定任意客户端从此更新源进行更新。 8.支持通过网络掩码或 IP 范围查找未安装客户端的计算机，并且将发现的 IP 解析为主机名方便管理。 9.支持与 VMwarevCenter,新华三 CAS、华为 FusionCompute 等云平台对接,同步虚拟机相关信息。 10.应提供自动分组功能，可配置分组策略，策略包括不限于主机名、操作系统、IP 地址、安全策略、物理机/虚拟	套	53	亚信安全云主机深度安全防护系统应用软件 Deep Security V20.0-有代理防病毒模块	1,495.00	79,235.00	

		机/Docker 主机分类等。 11.勒索病毒：支持通过行为监控的方式，如检测可疑活动和未经授权的更改，防止勒索软件感染，并提供针对勒索软件事件专有历史纪录和勒索软件统计的监控组件. 12.恶意站点拦截：具备 web 信誉库，通过 Web 信誉支持阻止主机访问恶意站点，支持恶意站点自定义。 13.包含 53 台虚拟机授权，一年软件升级服务。						
5	安全云主机深度补丁防护系统	1.入侵检测、虚拟补丁、防火墙功能。 2.网络访问控制：支持网络访问控制功能，自定义防火墙策略，支持 IP、MAC 地址、端口，支持协议：TCP、UDP、ICMP、ICMPv6、IGMP、IDP 等，支持 IPv4、IPv6、ARP、RARP 等。 ★3.安全标签：支持 NSX 安全标签，一旦检测到恶意威胁，可将 NSX 安全标记应用于受保护的 VM，NSX 安全标记可与 NSXServiceComposer 一起使用，以自动执行某些任务，例如隔离受感染的 VM。 4.入侵防御：支持网络入侵攻击的防护，包含支持防护 SQL 注入，Cookie 注入，命令注入，跨站脚本(XSS)，跨站请求伪造(CSRF)，WebShell 攻击防护等。 5.入侵防御：内置入侵防御的规则库，支持关联 ATT&CK 框架的技术 ID，便于了解网络入侵技战术点。 6.漏洞防护：通过流量检测技术，实现漏洞利用的攻击防护，支持操作系统、数据库、邮件服务、办公软件、中间件、Web 应用、应用等类型的漏洞。 7.漏洞扫描：提供操作系统和应用漏洞	套	53	亚信安全云主机深度安全防护系统应用软件 Deep Security V20.0-有代理深度包检测模块	2,470.00	130,910.00	

		扫描功能，根据扫描结果自动下发对应的防护规则。 8.定制规则：支持 0Day 漏洞暴露后，快速定制入侵防御规则，包括不限于签名、特征码、XML 等方式，进行 0day 的快速防护，同时可支持配置优先级、检测或阻止模式、严重性等。 ★9.SSL 流量支持：支持对 https 流量的识别，支持配置 SSL 证书及密码进行解密。 10.报文捕获：支持对恶意流量的报文进行捕获，将 HTTP 流量转化为事件日志，支持溯源及审查。 11.支持 SSH 弱口令扫描，支持端口、超时时间、重试次数配置，可配置密码字典和白名单。 12.针对隐藏在操作系统日志和应用程序日志中的重要事件，如暴力破解、日志非法清除、非法添加用户等高风险事件自动化实时告警。 13.包含 53 台虚拟机授权，一年软件升级服务。						
6	安全云主机深度安全防护系统平	提供服务器、虚拟机、私有云、公有云的统一安全防护，实现集中的管理、监控、更新和部署等能力，集中管理客户端防病毒、入侵检测、虚拟补丁、防火墙、Web 信誉、资产管理、日志审计等功能，帮助实现企业混合云、跨云的安全管理；包含数据中心防护系统控制台 1 套，一年软件升级服务。	套	1	亚信安全云主机深度安全防护系统应用软件 Deep Security V20.	39,800.00	39,800.00	

	台管理端				0-安全防护系统管理平台			
7	防毒墙	1.硬件参数：板载自带接口：2GE+4GE；Bypass 网络层吞吐率：4Gbps；防病毒吞吐率：800Mbps；电源：300W*2；扩展插槽：*2；硬件外形：软硬一体化 1U 标准机架式设备；CPU：2 核*1；内存：32G；硬盘容量：1T；。 2.功能描述：防病毒功能用于检测并阻止恶意程序，如勒索软件、病毒、僵木蠕、间谍软件、网页木马。可拦截间谍软件的回拨企图，阻止间谍软件下载，阻止恶意程序通过即时通信程序进行扩散。 ★3.能够对威胁进行可视化展示，展示维度至少包括威胁类型统计（至少包含勒索、挖矿、病毒、APT、漏洞利用威胁事件）、近 30 天威胁事件趋势、攻击源 IPTOP5、受影响主机 TOP5、勒索&挖矿事件拦截统计、热门威胁事件 TOP5、自定义黑名单 TOP5 等。 4.能够支持超过 100 种协议的解析，包括但不限于 HTTP/SMTP/POP3/FTP/SMB/TFTP/TCP/UDP/NFS/SNMP/ICMP/RTMP/DNS/IRC 等。 5.能够支持 win7、win10 的 SMB 文件共享协议的病毒检测查杀。 6.能够支持两个的防病毒引擎同时工作，并能够按需开启。 7.能够允许定义被扫描文件的大小范围，最大不小于 2G。 ★8.供应商具备整体联动能力（整理联	台	2	亚信安全高 AIS Edge EE (EE) V7.0 E680 D 级威胁网络防护系统	269,800.00	539,600.00	

		动的组件包括：数据中心防护系统和终端防病毒软件），从终端到数据中心实现整个计算中心已知、未知威胁全方位发现、拦截的功能。 ★9.所投产品需部署方式灵活以适应客户丰富的应用场景，支持 ICAP 部署模式。 ★10.可对 CPU、内存阈值进行设置，当超过该阈值，防毒墙主进程自动清理且不中断业务。 ★11.产品必须具备防病毒网关类的销售许可证，非防火墙产品，并且在计算信息系统安全专用产销售许可服务平台上的防病毒类中的网关防病毒类别内可查询。（https://www.ispl.cn/ispl/jsp/common/ProductList_Public.jsp）和销售许可证复印件。 ★12.获得 IPv6ReadyLogo 认证证书。 13.包含 3 年软件升级及硬件维保服务。					
投标总价（大写）	玖拾捌万柒仟柒佰肆拾伍元整	小写		987,745.00 元	供货期（日历日）	合同签订后 7 日内		

备注：

1、投标报价应包括材料款、货物款、附件款、安装调试费、运输费、税费、保险费、公证费及到达指定地点验收前的其他一切费用。

2、开标一览表中须填报所投报各包的投标报价的总价，无需填报每包中所涉及的具体单项价格。

3、开标一览表中投标总价须与投标文件中投标报价明细表的投标总价保持一致，如出现不同，以开标一览表中价格为准。

报价单位（公章）：

法定代表人（名章）：