**分项报价表**

项目编号：ZFCG-G2018155号

项目名称：视频网安全管控、公安网IP扩容A包

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名 称** | **规格型号** | **技术****参数** | **单 位** | **数 量** | **单价** | **总价** | **产地及****厂家** |
| 1 | 视频安全集中管控平台 | 启明星辰泰合信息安全运营中心系统/v3.0-TSOC-USM-SW | 1、通用指标：所投产品支持B/S架构，采用浏览器登陆系统，支持SSL加密模式访问安全管理平台。支持多级、单级、分部署等部署方式。2、资产管理所投产品支持平台整合全网设备资产，支持设备细分为：摄像头、计算机、网络设备、其他设备。支持对资产数据进行基于区域，单位，类型等属性进行统计分析。所投产品提供软硬件资产录入，支持资产可用性、完整性、保密性管理，支持基于域的资产管理；根据资产价值、资产弱点和受威胁程度，支持计算资产安全等级和业务单元（域）安全风险、威胁等级。3、用户管理：所投产品支持用户按角色管理。支持用户和角色的权限管理。支持控制每个角色显示不同的功能菜单。4、事件管理：所投产品支持按预定义的字段显示事件。支持安全事件的响应预警方式包括：命令行，发送电子邮件，声音，短消息，工单处理等。支持根据以下条件选择查看事件：时间，事件名，时间类型，目的地址，源地址，资产号，优先级等。5、脆弱性管理：所投产品支持导入第三方漏洞扫描报告，支持：绿盟极光扫描报告、榕基扫描报告。支持将漏洞扫描报告和资产关联。支持资产弱点生命周期管理：新发现、确认、已消除、已防护。支持图形化方式表现资产脆弱性统计报表。6、实时监控：所投产品支持对视频网内网安全管理系统进行运维监控管理，支持监控内网安全管理系统使用状态是否正常，监控运行指标：CPU使用率、硬盘使用率、内存使用率等。所投产品支持对视频网网络接入控制网关进行运维监控管理，支持监控网关使用状态是否正常，监控运行指标：CPU使用率、硬盘使用率、内存使用率等。所投产品支持对视频网防病毒系统进行运维监控管理，监控视频网防病毒系统使用状态是否正常，支持监控运行指标：CPU使用率、硬盘使用率、内存使用率等。7、预警："所投产品支持支持全局预警，防范事件于未然。支持能够查看各辖区的各项违规预警统计信息、违规列表详细信息、审计信息、其他相关日志报表信息。"所投产品支持与视频网网络接入控制网关联动，支持通过平台直接网内设备进行白名单添加、设置阻断。支持接收所有网关的预警信息，被阻断设备信息等。8、终端管理：所投产品支持与视频网内网安全管理系统联动，支持平台直接通过视频网内网安全管理系统对注册终端进行实时点对点监控，支持监控内容包括：CPU、硬盘、内存、使用进程、使用端口、使用软件、计算机日志、安全策略、注册信息、计算机使用用户等。所投产品支持与视频网网络接入控制网关联动，可通过平台直接网内设备进行白名单添加、设置阻断。支持接收所有网关的预警信息，被阻断设备信息等。所投产品支持建立纵向的终端管理记录，辅助用户宏观掌握各级终端情况。所投产品支持终端报警实时展现和应急响应；支持迅速追踪到终端状况，定位问题终端，帮助用户管理控制终端风险。所投产品支持精准的终端信息查询,迅速了解终端最近的使用情况；支持事件快速定位到相关责任人,方便管理。9、级联管理：所投产品支持通过级联实现多级审计与预警管理。支持以级联方式对事件与终端进行远程管理。10、知识库管理：所投产品支持知识库分组包括：攻击库，漏洞库，补丁库，病毒库等。支持对知识库的管理，包括：增加，删除，查询，移动，导入，导出等操作。知识库存储数据支持12000000（条） | 套 | 1 | 190000 | 190000 | 北京北京启明星辰信息安全技术有限公司 |
| 2 | 视频网联网设备管理系统（准入管理） | 启明星辰天清视频安全防护系统V6.0-NGIPS5000-M1-VSG | 1、性能及部署要求:★所投产品支持硬件准入控制设备，具有4个1000BASE-T电口，4个1000BASE-T管理口，支持独立扩展槽位，支持4个1000BASE-T扩展口，支持扩展BYPASS电口，支持扩展BYPASS光口，4个USB接口，4个RS232串口（RJ-45），支持温度0℃～80℃(工作) -40℃～70℃(存储)；支持湿度5～95%RH不凝结。★所投产品支持流量吞吐量10Gbps,380万并发连接数，支持新建连接数69000个/S。支持单台10路业务控制。★所投产品支持硬件采用2U机架结构，提供I7处理器，最大主频3.5GHz，提供32G DDR3内存，提供1TB存储硬盘，配置6个千兆电口，电口默认支持路硬件BYPASS，4SFP接口BYPASS,2SFP+接口BYPASS，支持扩展4个端口千兆光纤扩展卡；支持扩展4个端口千兆光纤扩展卡；支持扩展2个端口万兆光钎扩展卡。所投产品支持双机热备功能，当主设备出现问题时，支持自动切换至备份设备。所投产品支持策略路由、旁路干扰、透明串接、虚拟网关等多种准入控制模式。所投产品支持集群式部署，支持通过管理平台统一管理多台准入网关，对其统一下发策略、统一信息收集。2、身份认证：所投产品支持未认证通过用户入网时进行阻断，能够提供Web重定向提醒，并说明入网阻断原因。支持能够在重定向页面上实现终端认证、身份认证、安全检查、访客入网等功能。所投产品支持注册审核管理功能，入网终端必须通过手动、自动审核通过之后才可以接入网络，支持实名审核功能，根据导入实名信息达到自动验证的目的，并支持自定义审核字段，实现匹配审核。所投产品支持认证方式支持本地认证、Radius认证、AD域同步认证、CA认证、PKI认证等。所投产品支持用户只有经过认证并且终端安全状态达标才允许接入网络。所投产品支持安全域控制功能，可依角色属性定制不同安全域。3、资产管理：所投产品支持自动发现和识别所有联网设备，类型要求包括计算机终端、哑终端、服务器终端、网络设备终端、专用设备终端等，并且能够自动识别联网设备的MAC地址、IP地址、主机名、厂商、品牌型号、终端类型、操作系统、网络指纹等。所投产品支持对已注册的视频图像监控设备被非法替换后，支持立即进行告警。支持对终端计算机软件的安装、变更数据，终端硬件的信息以及硬件变更信息及时记录并上报服务器。支持终端软硬件资产变动告警。4、准入控制：所投产品支持基于终端心跳和终端水印认证双重流量分析，判断入网终端访问合规性。所投产品支持支持计算机设备接入视频网时，支持自动判断计算机是否符合入网要求，符合入网要求则允许通过认证，不符合要求的直接通过阻断及跳转方式进行阻断其接入网络，支持禁止其访问内部资源。所投产品支持对接入视频网的终端计算机、服务器进行入网安全体检，达到入网要求才允许入网。所投产品支持准入策略制定功能,可根据访问IP源、目的域以及准入流程进行策略制定，目的域需是IP、端口以及目录的组合，可根据部门设置，支持贴标签等灵活的动态分组设置策略，支持根据终端类型设置策略，支持根据操作系统设置策略。所投产品支持准入流程差异化控制，支持根据准入策略控制终端仅注册、仅认证、注册及认证、注册认证并安检等差异化准入。所投产品支持对Windows桌面操作系统和非Windows桌面系统类型的识别并实施不同准入控制策略。所投产品支持Linux以及国产操作系统，有独立的客户端，支持对终端进行安全管控。所投产品支持不可网管交换机/HUB设备下多终端的接入控制，同一个不可网管交换机/HUB下合法终端可以访问视频网资源，非法终端不能访问。所投产品支持基于数据链路层安全域控制，同一vlan下，未授权终端无法访问注册授权终端，实现接入层准入管理。所投产品支持对交换机进行管理，可对交换机类型、地址、状态、802.1X状态进行监控，支持界面展示各交换机端口状态。5、安全检查：所投产品支持对入网终端进行安全检查，并对安检进度提供进度条提示，未通过安检的终端给出未通过项提示并阻断入网，支持用户在管理界面编辑安检结果显示内容。支持安检未通过终端一键修复功能。所投产品支持安检规范定义配置功能，支持根据用户属性定制不同的安检规范，安检规范应至少包含域登录检查、杀毒软件安装情况检查、补丁漏洞检查、系统共享资源检查、IE主页修改项检查、guest来宾帐户启用情况检查、远程桌面启用情况检查、系统启动项检查、系统进程检查、软件安装等。6、系统监控：所投产品支持对系统本身业务接口的连接状态以及接口速率进行监控，支持对系统本身的CPU以及内存使用率提供仪表盘式图形化实时监控数据，支持数据自动刷新。所投产品支持对在线终端状态提供图形化实时分析报表，分析内容至少包含接入设备、待审核设备、注册设备、认证设备、访客设备、入网设备、白名单设备、隔离设备、离线设备等不少于9种状态。 | 套 | 1 | 160000 | 160000 | 北京北京启明星辰信息安全技术有限公司 |
| 3 | 视频应用审计系统 | 启明星辰天玥网络安全审计系统V6.0-BA1500ER | ★1、性能指标：所投标产品支持带宽10G。存储时间36个月。自带2T硬盘存储空间。支持硬件叠加扩容的能力。2、功能指标：所投标产品支持设备旁路部署，通过交换机镜像口获取数据，不影响原有业务系统。所投标产品支持GB/T 28181协议、标准SIP协议操作信令还原、记录,支持H3C、博康、博路、海康、大华、烽火等主流的视频服务厂商协议。所投标产品支持能够发现并识别视频设备（摄像头、摄像头控制器）、控制中心、流媒体服务器、客户端代理。所投标产品支持根据设备类型、设备信息、源地址、目的地址、时间、操作类型、用户、协议内容检索审计记录。所投标产品支持审计数据自动分类，根据GB/T 28181协议对视频网访问行为进行自动识别，并分类展示和统计，支持识别的行为包括但不限于：认证行为、视频播放行为、视频设备访问行为等。所投标产品支持大屏投影展示，支持展示内容包括但不限于各个节点的事件状态分布，异常告警，重点指标趋势等。所投标产品支持根据设备类型、设备信息、源地址、目的地址、时间、操作类型、用户、协议内容、访问时长、访问次数自定义报警策略。所投标产品支持内置策略，支持未知设备发现，累计访问次数预警。所投标产品支持内置策略支持对异常访问行为自动分析和预警，详细分析判断参数可调。所投标产品支持通过策略配置，支持自动发现异常（违规）访问行为，并产生报警。所投标产品支持审计规则配置，支持通过IP、GB/T 28181协议内容等条件，调整事件级别，确定是否产生报警。所投标产品支持对同一用户、同一设备、同一IP基于访问次数、访问时长累计统计和排序。所投标产品支持通过excel导入设备信息库，支持定制从第三方网络准入系统获取设备信息库。所投标产品支持组织机构代码库导入。所投标产品支持根据区县、警种进行访问率、访问时长、设备故障率进行统计、排名。所投标产品支持向第三方平台报送审计数据。所投标产品支持多探针分布式部署模式。所投标产品支持远程SSH/telnet和本地串口两种管理模式。所投标产品支持三权分立模式，系统IP访问限定模式，支持多级管理员模式。 | 套 | 1 | 100000 | 100000 | 北京北京启明星辰信息安全技术有限公司 |
| 4 | 终端安全管理 | 启明星辰天珣内网安全风险管理与审计系统V6.0 | 1、通用要求：投标产品支持多级级联部署架构，支持三级及以上级联。上级平台可掌握所有下级平台的运行状态和报警信息，能够统计全网终端信息并生成图表，能够为下级平台下发强制级联策略、分发补丁等，亦可通过平台私有安全通道免密登录下级管理平台查看。投标产品支持双机热备，双机数据实时同步，支持主机发生故障时备机自动更改相应配置替换主机。投标产品支持安防和公安行业的数据格式标准和数据共享要求，支持数据格式与公安网“一机两用”系统数据格式标准一致。2、客户端要求：投标产品支持客户端在线、离线安装，支持防卸载、关闭及恶意破坏，支持有效的文件、服务及进程保护机制。支持管理员授权的在线、离线卸载，卸载时可通过查看卸载码卸载。投标产品支持客户端功能要求在操作系统安全模式下生效。投标产品支持客户端文件及本地审计内容要求加密存储，防止信息泄露。3、终端安全管理模块：投标产品支持系统要求支持管理网络终端软硬件资产，支持硬件设备信息、位置信息（设备名称、使用人、联系电话、所属部门等）、网络信息（MAC地址、IP地址等）、软件安装信息（操作系统、应用软件）等，支持手动修改和添加硬件信息。投标产品支持黑名单及白名单与准入控制系统联动，支持安全策略共同实现对黑白名单的同步管理与策略分配。投标产品支持对视频网终端计算机（服务器）上的无线网卡、光驱、红外、蓝牙、串并接口、USB等外设接口进行管控，防止视频网信息泄漏与病毒木马传播。投标产品支持控制硬件外设的使用，支持通过驱动层禁用，可禁用终端计算机的3G网卡、光驱、USB存储接口、USB非存储接口、 串行口、并行口、1394控制器、无线网卡及自定义设备。投标产品支持对软件安装进行黑白名单控制，即根据策略设定禁止安装的软件和可以安装的软件。违规软件禁止安装功能，禁止在注册表Run项里添加自启动项，禁止在注册表Services项里添加自启动项，禁止在程序启动项中添加项，禁止在程序项中添加快捷方式限制违规软件的安装，所有安装软件应能进行审计。投标产品支持进程管理功能：支持对（包括软件厂商名、源文件产品名、源文件名、进程名等）的进程进行黑白名单的控制，黑名单内进程自动被禁止，白名单内进程自动启动。投标产品支持进程保护功能，能够保护重要应用的进程不被篡改或结束。投标产品支持全网统一防火墙功能，能够设置终端可使用或访问的协议、IP、端口，支持设置被访问权限和访问权限，从而网络内建立虚拟的终端隔离区，防止用户越权访问。投标产品支持对终端计算机与服务器的账户安全策略配置进行检查，支持对账户弱口令、无效账户、过期账户、来宾用户等安全风险自动检测与报警。支持对全网终端的系统密码进行检测及管理，检测终端弱口令，支持员工设置的密码符合管理员设定的复杂度，如：大小写、中英文、数字等。投标产品支持系统提供注册表检查功能，对于病毒行为修改的注册表，可以通过强制注册表策略对其进行操作，可以自动创建、删除、修改相应的注册表键值，实现注册表安全管理。投标产品支持检测终端杀毒安装及运行情况，兼容市面所有杀毒软件。支持检测杀毒软件是否及时更新。投标产品支持IP与MAC绑定，禁止终端用户修改IP地址、网关等参数，并自动恢复、断网和提示等处理。支持设置可修改的IP范围，支持服务器同步绑定IP/MAC，防止终端重做系统后修改IP。投标产品支持对计算机终端的CPU、内存、硬盘的资源占用率和剩余空间进行监控，设定危险等级报警阀门，报警信息可在管理平台统一查看。投标产品支持对终端的流量进行监控，支持用户自主设定采样阈值，当流量（含出、入或总流量）超过一定限度并持续一定时间后，将信息上报至服务器。支持对日、周、月的流量使用进行自动排序。投标产品支持设定网络客户端流量上限阈值，对超过的进行报警上报、自动阻断、客户端提示等管理。投标产品支持在Web控制台对计算机终端的网络流入、流出和总流量进行监控和管理。并能够对产生总流量过大、分时段瞬时流量过大的终端进行统计。★投标产品支持对全网终端安全配置的核查，检查必须包括网络配置安全、系统用户安全、对象访问权限、系统权限分配、程序安全性核查、密码审核安全、系统环境检查、系统漏洞、杀毒软件检测等，超过37条检查项。投标产品支持注册表检查，通过对注册表的修复来达到禁用某些服务的功能。投标产品支持文件及软件推送分发安装，支持后台批量静默推送安装软件，具备消息推送功能，能够为指定范围内的终端推送通知消息，支持定时推送。4、终端数据安全监控和审计模块：投标产品支持对设定目录文件的操作审计，包括文件创建、打印、读写、复制、改名、删除、移动等的记录，同时将信息上报管理信息库供查询；具备对终端的系统、软件和共享等目录中的文件具有保护功能，设定访问、删除、修改权限；支持全盘文件禁止删除，审计自定义文件扩展名。投标产品支持对终端计算机进行打印、介质拷贝、网络文件拷贝等文件输出行为审计功能。各种审计信息包括时间、使用人、文件名等。投标产品支持对通过USB设备进行的文件拷入、拷出的行为进行审计，记录文件名称和操作时间。支持禁用usb数据对拷线。投标产品支持对终端通过网络共享拷贝的文件审计，支持对拷至网络盘的文件内容检查，包含敏感字的文件禁止考出。投标产品支持对终端的邮件发送行为进行审计；支持审计终端用户的上网行为，网址要求审计到每个子网站。投标产品支持审计终端系统账户的权限变更行为，支持批量修改用户账户的权限。投标产品支持对终端建立的wifi热点（笔记本自建wifi及随身wifi）进行管理，用户可以根据应用场景和终端用户权限的不同，允许或者禁止终端用户使用随时WIFI设备，同时还可以根据特殊情况，设定白名单或者黑名单，以便适应更复杂的使用环境，同时可以审计附近的WIFI热点和接入随身WIFI设备的终端。投标产品支持对通过内部终端创建的wifi热点接入的设备进行管理和审计，具体包括以下功能：禁止使用随身WIFI设备；允许使用随身WIFI设备；审计接入允许使用随身WIFI设备的终端信息；审计附近的WIFI热点信息；自定义不同的网络安全域执行不同的管控策略；自定义办公网和非办公网执行不同的管控策略； 投标产品支持能够自动识别任意移动存储介质的接入，可以通过策略分配在驱动级对移动存储设备的使用进行控制。在允许使用的情况下，进行更细致的移动存储设备管理；能够实现禁止用户使用移动存储设备，不影响非存储类设备的正常使用。投标产品支持对在内网使用的移动存储介质进行注册登记与加密处理。登记信息包括：使用人、使用部门、联系电话等等。投标产品支持对不同部门下发不同标签的功能，从而实现移动存储设备在部门/单位之间相互隔离，保障核心终端的数据安全。投标产品支持系统能够根据用户需要和用户使用情况将一块移动存储介质进行分区管理，至少能分交换区和保密区，系统能够自由分配交换区及保密区的大小。投标产品支持移动存储介质划分加密区后，只有在分配到该移动存储介质对应的标签认证策略的计算机终端上，并且通过正确的密码验证才可访问加密区的内容。投标产品支持系统能够详细的记录移动存储设备的插拔、标签分配情况、移动存储设备中数据的创建目录、创建文件、修改、复制、剪切、粘贴、重命名、删除等行为，支持离线审计，上线后提交。能够详细记录计算机终端用户插拔移动存储设备的具体时间、盘符、插拔状态等信息，记录包括文件名、审计描述、时间、用户名、部门、计算机终端IP地址、MAC地址等，支持对指定格式的文件审计过滤。★投标产品支持为保障数据安全，需提供16G公安安全U盘11个，该安全U盘应具备审计、防泄密、防病毒等功能，并且能够在本平台内实现。彻底杜绝通过移动存储设备的数据非法外泄。★投标产品支持为保障服务器安全，提供终端单点登录12个，并且能够在本平台内实现。投标产品支持计算机进行桌面点阵水印设置，点阵水印智能计算所在计算机的数据信息。可通过专用还原工具，对桌面水印图像进行还原，还原信息包括该图像所在计算机唯一特征，图像拍摄时间等息。投标产品支持摆渡机支持与杀毒软件联动，自动查杀接入摆渡机的普通移动存储设备和内部注册移动存储设备，防止病毒传播。5、补丁自动分发和管理模块：投标产品支持系统能够自动检测全网终端漏洞，在管理平台生成全网漏洞图表。★投标产品支持支持建立私有补丁库，具备补丁自动分发机制，能够根据终端操作系统类型及漏洞推送安装所需补丁，支持无需人工干预补丁库补丁数量超过20000。并支持私有补丁库和厂商补丁库进行联动。投标产品支持能够自动统计补丁自动分发的结果，可统计补丁下载成功/失败，安装成功失败的信息，供管理员查看。投标产品支持服务器支持补丁下载速度设定，支持补丁代理转发功能，同网段已下载补丁的终端可自动作为代理给未下载补丁的终端推送补丁，从而减轻服务器压力，提高补丁安装效率。投标产品支持补丁自动测试功能，即用户可自主选定内网部分设备为补丁安装测试设备，系统将新获得的补丁自动发送给这些设备，在测试设备安装指定时间间隔后再自动分发给其他设备。从而规避问题补丁，防止大量终端蓝屏现象。6、网络边界管理模块：投标产品支持互联网连通性检查，一旦发现与互联网连接，可立刻进行报警并阻断连接；要求同时监测视频网计算机联网状态，计算机一旦脱离视频网，则禁止其网卡所有网络数据通信，使视频网计算机形成离网单机，阻断连接任何视频网以外的网络。支持非法网关监测，检测其是否存在连接互联网的通道。投标产品支持网络线路串线检查并报警。支持双网卡状态检查并报警。投标产品支持视频网DHCP服务器检查并报警。7、接口联动：投标产品支持与视频网安全集中管控平台的联动，提供联动接口文件。 | 点 | 300 | 310 | 93000 | 北京北京启明星辰信息安全技术有限公司 |
| 5 | 防病毒系统 | 启明星辰景云网络防病毒系统1.0 | 1、操作平台：所投产品客户端支持常见的32位和64位操作系统：Windows XP Professional SP3、Windows Vista SP2、Windows 7 Professional、Windows 8 Professional、Windows Server 2003、Windows Server 2008、Windows Server 2012。2、数据库：所投产品服务端安装包提供内置数据库支持，不需要额外安装诸如SQL Server、MSDE、MySql、ACCESS等数据库软件。3、基础管理能力：所投产品支持良好的可扩展性和易用性，支持大型网络跨地域、跨网段的部署和管理，支持无限层网络架构，支持C/S及B/S两种模式对客户端进行管理。4、私有云：所投产品支持杀毒软件服务端具备企业内部云建设能力，可搭建私有云查杀平台，摒弃公有云，防止数据外泄，减少网络负载。5、通信安全：所投产品支持杀毒软件服务端能对所有客户端进行集中管控，通过控制台直接给客户端发送命令，指令采用国际标准的SSL方式加密。6、统一管理所投产品支持杀毒软件服务端能够实时监控客户端病毒查杀信息，并具备病毒日志查询与统计功能，可对网络中病毒动态进行查询统计，能按时间、按IP地址、机器名、按病毒名称、病毒类型进行统计查询，能将查询结果打印或导出。7、策略定制：所投产品支持订制化安全策略能力，可根据企业用户环境，可自由定制个性化的终端安全防护策略，为企业打造私有云安全模型以提高计算机安全等级。8、策略配置及强制机制：所投产品支持使终端强制执行中控所下发策略的能力。杀毒软件服务端可以对所提供的不同系统平台以及应用系统下的防护终端进行策略配置，在配置成功后，管理员可自定义锁定客户端策略及权限，强制终端用户执行策略。9、威胁管理：所投产品支持提供多维度，多粒度的病毒情报展示能力，可按边界类型、病毒类型、时间范围、终端组织结构等等参数对病毒情报进行详细筛选，能对选定项进行清除或者加白，能导出报表。10、审计日志：所投产品支持提供多维度，多粒度的日志汇总报表与分析报表的能力。并提供两种展示方式，图形报表和详细日志。所投产品支持图形报表：可折线图，饼状图等图表导出终端部署情况，日活统计，病毒库版本统计，病毒排名，感染情况统计等数据。所投产品支持详细日志：可展示所有终端的操作日志，通过触发原因，操作类型，操作状态，时间戳，操作员账户，终端名等搜索条件来筛选用户需要的信息，筛选完成后，可导出报表。11、智能追溯：所投产品支持病毒文件审计追踪能力，可智能快速定位病毒，及早处理感染源，减少病毒爆发造成的损失。12、自动升级：所投产品支持自定义病毒/软件版本升级时间能力，并且升级过程已进行智能负载均衡处理，避免占用过多内网带宽资源。13、定时扫描：所投产品支持自定义全网病毒查杀参数的能力。在指定的时间自动下发查杀指令至指定的终端进行病毒扫描可配置扫描时间，扫描类型等。14、发现病毒的处理方式：所投产品支持自定义病毒处理方式的能力，如通过下发查杀指令或定时扫描等方式发现了病毒，可设置是否直接自动清除。15、终端密码保护：所投产品支持保护终端不被非法退出或卸载的能力。用户在终端执行退出或卸载软件时，需要通过密码验证。16、安全报警：所投产品支持将风险警报或者系统日志发送给管理员的能力。可在内网威胁程度满足触发条件时发送邮件告警或系统日志至指定收件人，使管理员能快速响应并处理计算机病毒。17、查杀能力所投产品支持杀毒软件须具备机器学习能力，通过CNN深度学习算法以及大数据分析技术，来实现人工智能引擎，可有效应对未知病毒，在获得较高的检出率的同时能够有效地降低误报率，误报率低于万分之二。所投产品支持私有云查杀引擎须具备特征查杀能力。特征云查杀引擎：通过对样本特征关联性分析，具备识别未知病毒能力。所投产品支持杀毒软件须具备基于多步行为判断的主动防御技术，根据样本一系列的行为特征来进行综合的风险判定，其监控和判断能力由后台的大数据训练集群支持。所投产品支持杀毒软件须提供宏病毒专杀引擎，可以解析office所有常用版本的文档，处理被感染的文档，将恶意代码清除而保留正常文档。清除操作的粒度可以到清除excel公式、宏脚本中某个函数等。所投产品支持对未安装的已知补丁进行防护，还支持通过系统内核加固、应用加固等手段对0day漏洞或未知漏洞进行防护。所投产品支持压缩包查杀功能，支持35种解压缩格式，涵盖压缩包、安装包、文档格式解析能力。支持安装脚本级查杀，拦截流氓软件捆绑。所投产品支持主动防御模块，能够监控和清除来自各种途径的病毒、木马、广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等。.所投产品支持边界防护，对网页访问、程序下载、文件拷贝等敏感系统边界入口的实时监控，拦截危险文件的落地。所投产品支持与内网安全管理系统的移动存储摆渡机联动，能够自动查杀内网专用标签U盘内的病毒，避免病毒传入内部网络。18、★产品更新：所投产品支持拥有多个主干道服务器，保证企业中控平台自动选择最快的更新服务器，使用最快的速度获取最新的反病毒数据库，病毒库样本超过4,715万。所投产品支持反病毒软件在更新过程中遇不可抗力等意外情况下中断，在下次重新运行更新时，可使用增量更新技术，在中断之前更新的基础上继续更新，提高更新效率，节约网络流量。所投产品支持快速的反应能力，病毒库要求常规情况下，平均每周更新一次，反病毒更新模块允许从 Internet 或当地的服务器下载最新的反病毒数据库和组件。支持服务端更新后，能够自动迅速完成全网杀毒客户端的更新。所投产品支持对反病毒数据库更新源进行定制（互联网更新服务器、本地文件夹、网络共享文件夹、内部更新站点、U盘光盘等移动存储介质）。19、接口联动：所投产品支持与视频网安全集中管控平台的联动。 | 点 | 300 | 210 | 63000 | 北京北京启明星辰信息安全技术有限公司 |
| 6 | 存储介质信息消除系统 | 技佳存储介质信息消除系统 v6.0 | 1、可以对整个磁盘进行整体擦除2、对硬盘的擦除速度不能低于3GB/分钟3、支持00擦除、FF擦除、00擦除+FF擦除、BMB21-2007标准, 数据擦除不可恢复。4、 采用专用硬件载体 ,操作方便、支持触摸屏方式的操作5、★ 要求支持USB、IDE以及SATA接口，支持10个USB口，支持2个IDE口，支持4个SATA口。 | 套 | 1 | 105000 | 105000 | 北京北京技佳数据恢复公司 |
| 7 | 企业级应用服务器 | 联想ThinkSystem SR590 | 2颗Intel Xeon Silver 4112 2.4GHz处理器12MB L3 缓存；64GB ECC DDR3 1333 MHz内存；6\*300GB 3.5in SL HS 15K 6Gbps SAS HDD可热插拔硬盘；配置256MB高速缓存SAS RAID卡，配置电池保护，支持RAID0/1/1E/5/6/10/50/60；2块1000M高性能以太网卡；冗余服务器电源和风扇；DVD-RW | 台 | 3 | 37000 | 111000 | 北京联想（北京）信息技术有限公司 |
| 合 计 | 大写：捌拾贰万贰仟圆整 小写： 822000元 |