南阳市公安局内网安全加固和外联防范项目
政府采购合同

甲方（采购人）：南阳市公安局

乙方（供应商）：河南数字磐牛科技有限公司

签订时间：　2024年12月30日

南阳市公安局通过公开招标的方式对南阳市公安局内网安全加固和外联防范项目（项目编号：南阳政采公开-2024-92）进行了政府采购。按照评标委员会评审推荐，甲方确定乙方为中标单位。现甲乙双方协商同意签订本合同。

第一条：合同文件

下列与本次采购活动有关的文件及附件是本合同不可分割的组成部分，与本合同具有同等法律效力，这些文件包括但不限于：

1、招标采购文件

2、投标文件

3、乙方在投标时的书面承诺

4、中标通知书

5、合同补充条款或说明

第二条：合同标的

乙方根据甲方需求提供下列货物，货物名称、规格及数量等（详见《供货一览表》）。

第三条：合同总金额

大写：壹佰肆拾捌万圆整。

本合同项下货物总金额：￥1480000.00元。

分项价款在《供货一览表》中有明确规定。

本合同总价款包括货物、软件、标准附件、备品备件、专用工具、图纸资料、技术服务，包装、运输、装卸、保险、税金，货到就位以及安装、调试、培训、保修等验收合格之前和质保期内的售后服务等一切税金和费用。

本合同执行期间合同总价款不变。

第四条：权利和质量保证

1、乙方应保证甲方在使用该货物或其任何一部分时不受第三方提出侵犯其专利权、版权、商标权或其他权利的起诉。一旦出现侵权，索赔或诉讼，乙方应承担全部责任。

2、乙方保证货物是全新的、未使用过的，完全符合国家规范及甲乙双方确认的投标文件、本合同关于货物数量、质量的要求。货物符合实行国家“三包”规定的，应执行“三包”规定。

3、本项目免费质保期为自验收合格之日起3年（防病毒软件为2年）。质保到期后软件可以继续使用，但不提供免费升级服务。

4、乙方提交的货物应符合投标文件中所记载的详细配置、技术参数、参数及性能，并应附有此类货物完整、详细的技术资料和说明文件。

5、乙方提交的货物必须按照招标采购文件的要求和中标人投标文件的承诺，以约定标准进行制造、安装；经政府采购管理部门批准采购的进口产品应执行原产地国家有关部门最新颁布的相应正式标准并提供国家商检、海关报关等手续。

6、乙方应保证将货物按照国家或专业标准包装、确保货物安全无损运抵合同规定的交货地点，并进行安装、试运行。

7、乙方保证货物不存在危及人身及财产安全的产品缺陷，否则应承担全部法律责任。

第五条：付款方式

1、本合同项下所有款项均以人民币支付。

2、乙方向甲方提交下列文件材料，经甲方审核无误后支付采购资金：

(1) 经甲方确认的发票；

(2) 经甲乙双方确认签署的《验收报告》；

(3) 其他材料。

3、款项的支付进度：项目完工经采购人组织验收合格，并报审计部门审核后，15个工作日内支付全部货款。

第六条：交货与验收

1、交货时间：自签订合同之日起30日历天内供货完毕。

交货地点：南阳市公安局。

安装调试时间：自签订合同之日起30日历天内安装调试完毕。

2、乙方应对提供的货物作出全面自查和整理，并列出清单，作为甲方验收和使用的技术条件依据，清单应随提供的验收资料交给甲方。

3、乙方提供的货物应包括本合同“第二条合同标的”规定的全部货物及其附（辅）件、资料。

4、甲方应当在到货后的10个工作日内对货物进行验收。货物验收时，甲乙双方必须同时在场，双方共同确认货物与本合同规定的生产厂家产地、品牌、规格型号、数量、质量、技术参数和性能等是否一致。乙方所交付的货物不符合合同规定的，甲方有权拒收。乙方应及时按本合同规定和甲方要求免费对拒收货物采取更换或其他必要的补救措施，直至验收合格，方视为乙方按本合同规定完成交货。

5、需要乙方对货物（包括软件）或系统进行安装调试的，甲乙双方应在货物安装调试完毕后的10个工作日内进行运行效果验收。在验收之前，乙方需提前提交相应的调试计划(包括调试程序、环境、内容和检验标准、调试时间安排等）供甲方确认，乙方还应对所有检验验收调试的结果、步骤、原始数据等作妥善记录。如甲方要求，乙方应将记录提供给甲方。调试检验出现全部或部分未达到本合同所约定的技术指标，甲方有权选择下列任一处理方式：

（1）重新调试直至合格为止；

（2）要求乙方对货物进行免费更换，然后重新调试直至合格为止。甲方因乙方原因所产生的所有费用均由乙方负担。

6、验收合格的，由双方共同签署《验收报告》。

7、甲方可以视项目规模或复杂情况聘请专业人员参与验收，大型或复杂项目，以及特种货物应当邀请的第三方质量检测机构及专家参与验收。

8、货物验收包括：货物包装是否完好，产地生产厂家名称、品牌、型号、规格、数量、外观质量、配置、内在质量，以及调试运行是否达到“第一条合同文件”规定的效果。乙方应将所提供货物的装箱清单、产品合格证、甲方手册、原厂保修卡、随机资料及备品备件、易损件、专用工具等交付给甲方；乙方不能完整交付货物、附（辅）件和资料的，视为未按合同约定交货，乙方负责补齐，因此导致逾期交付的，由乙方承担相关的违约责任。

9、货物达不到本合同“第二条合同标的”规定的数量、质量要求和运行效果，甲方有权拒收，并可以解除合同；由此引起甲方损失及赔偿责任由乙方承担。

10、如果合同双方对《验收报告》有分歧，双方须于出现分歧后10天内给对方书面声明，以陈述己方的理由及要求，并附有关证据。分歧应通过协商解决。

第七条：项目管理服务

乙方应指定不少于一人全权全程负责本项目的商务服务，以及货物安装、调试、咨询、培训和售后等技术服务工作。

项目负责人姓名：王跃；联系电话：18737706800。

第八条：售后服务

1、质量保证期为自货物通过最终验收之日起36个月（防病毒软件为24个月）。若国家有明确规定的质量保证期高于此质量保证期的，执行国家规定。

2、在货物质保期内，乙方应对由于设计、工艺、质量（含环保节能要求）、材料和的缺陷而发生的任何不足或故障负责，并解决存在的问题。

3、对不符合本合同第四条规定要求的货物应立即进行调换，调换本身并不影响甲方就其损失向乙方索赔的权利。

4、货物安装调试完成后，乙方应继续向甲方提供良好的技术支持。应当由专门队伍从事此项工作，并提供全天候的热线技术支持服务，应当对甲方所反映的任何问题在2小时之内做出及时响应，在24时之内赶到现场实地解决问题。若问题、故障在检修1个工作日后仍无法解决，乙方应在5个工作日内免费提供不低于故障货物规格型号档次的备用货物供甲方使用，直至故障货物修复。

5、乙方应当建立健全售后服务体系，确保货物正常运行。乙方应当遵守甲方的有关管理制度、操作规程。对于乙方违规操作造成甲方损失的，由乙方按照本合同第十二条的约定承担赔偿责任。

6、乙方应负责货物及主要部件、配件维修更换。质保期内，乙方对货物（人为故意损坏除外）提供全免费保修或免费更换；质保期后，收取维修成本费（备品备件乙方应以投标文件承诺的优惠价格提供)。

第九条：合同的生效

1、本合同经甲乙双方法定代表人/负责人或授权代表签订并加盖公章或合同专用章后生效。授权代表签订的需提供加盖公章的授权委托书及被授权人身份证明。

2、生效后，除《政府采购法》第49条、第50条第二款规定的情形外，甲乙双方不得擅自变更、中止或终止合同。

第十条：违约责任

1、乙方所交付的货物不符合本合同规定的，甲方有权拒收，乙方在得到甲方通知之日起5个工作日内采取补救措施，逾期仍未采取有效措施的，乙方应向甲方支付合同总价0.1%的违约金。

2、甲方无正当理由拒收货物的，甲方应向乙方偿付拒付货款0.1%的违约金。

3、乙方无正当理由逾期交付货物的，每逾期1天，乙方向甲方偿付逾期交货部分货款总额的1‰的违约金，但累计违约金总额不超过欠款总额的20%。如乙方逾期交货达10天，甲方有权解除合同，甲方解除合同的通知自到达乙方时生效。在此情况下,乙方给甲方造成的实际损失高于违约金的，对高出违约金的部分乙方应予以赔偿。

4、乙方不按照售后服务约定履行的，应向甲方支付合同总金额0.1%的违约金。在乙方承诺的或国家规定的质量保证期内(取两者中最长的期限),如经乙方两次维修，货物仍不能达到合同约定的质量标准、运行效果的甲方有权要求乙方更换为全新合格货物并按本条第1款处理,同时乙方还须赔偿甲方因此遭受的损失。

5、其它未尽事宜，以《民法典》和《政府采购法》等有关法律法规规定为准，无相关规定的，双方协商解决。

第十一条：不可抗力

甲、乙方中任何一方，因不可抗力不能按时或完全履行合同的，应及时通知对方，并在10个工作日内提供相应证明。未履行完合同部分是否继续履行、如何履行等问题，可由双方初步协商，并向主管部门和政府采购管理部门报告。确定为不可抗力原因造成的损失，免予承担责任。

第十二条：争议解决方式

1、因货物的质量问题发生争议的，应当邀请国家认可的质量检测机构对货物质量进行鉴定。货物符合标准的，鉴定费由甲方承担；货物不符合质量标准的，鉴定费由乙方承担。

2、在解释或者执行本合同的过程中发生争议时，双方应通过协商方式解决。

3、经协商不能解决的争议，双方可选择以下第①种方式解决：

①向有管辖权的法院提起诉讼；

②向仲裁委员会提出仲裁。

4、在法院审理和仲裁期间，除有争议部分外，本合同其他部分可以履行的

仍应按合同条款继续履行。

第十三条：送达

1、各方确认，为更好地履行本合同，本合同所提供的地址等信息作为本合同项下各方沟通、送达各类通知、函件等文件的有效送达地址。

2、通过快递等方式送达时，对方签收之日视为有效送达；对方拒收或退回的，视为签收。

3、本合同各方提供的联系方式同时作为有效司法送达地址。

4、一方变更联系方式，应以书面形式通知对方；否则，原联系方式仍视为有效，由未通知方承担由此而引起的相关责任。

5、本联系方式条款为独立条款，不受合同整体或其他条款的效力影响，始终有效。

第十四条：保密义务

甲、乙双方对采购和合同履行过程中所获悉的国家秘密、工作秘密、商业秘密或者其他应当保密的信息，均有保密义务且不受合同有效期所限，直至该信息成为公开信息。泄露、不正当地使用国家秘密、工作秘密、商业秘密或者其他应当保密的信息，应当承担相应责任。

第十五条：其他

1、符合《政府采购法》第49条规定的，经双方协商，办理政府采购手续后，可签订补充合同，所签订的补充合同与本合同具有同等法律效力。

2、本合同附件是合同的组成部分，与本合同具有同等法律效力。

3、本合同一式陆份，甲、乙双方各执叁份。

附件：供货一览表

（本页无正文，为签署页）

甲方： 名称：南阳市公安局（盖章） 负责人/授权代表：（签字） 2024年12月30日 统一社会信用代码：11411300006001258C 开户银行： 银行账号： 联系人：魏铮 联系方式：18639826150 联系地址：河南省南阳市张衡路1号	**乙方：** 名称：河南数字磐牛科技有限公司（盖章） 法定代表人/授权代表：（签字） 2024年12月30日 统一社会信用代码：91411300MADL8ATJ02 开户银行：中国工商银行股份有限公司南阳行政支行 银行账号：1714020509100202551 联系人：王跃 联系方式：18737706800 联系地址：河南省南阳市城乡一体化示范区长江路与机场南二路交叉口蓝天集团大楼401室

附件：

供货一览表

序号	设备名称	品牌型号	规格、技术指标	生产厂家	单位	数量	单价（元）	总价（元）
1	内网安全监管系统升级加固	远望、V4.0	对原有的内网安全监管系统进行升级，在原有的通过在计算上安装客户端软件的方式，对普通“违规外联”进行防范的基础上，新增对IPV6违规外联、线路外联的防范，并新增禁止修改IP地址、禁用DHCP、禁用无线网卡、限制访问范围、离开公安网禁用网络连接等功能。 当计算机发生IPV6等违规外联时，系统可通过客户端软件对计算机进行断网关机处理，防止事态扩大造成恶劣影响。 构建计算机IP控制白名单，只允许计算机与白名单库公安信息网IP地址范围通信，所有超出该白名单地址范围的通信都会被阻止，限制终端主机可用的网络范围。 应能够通过客户端软件禁用计算机的无线网卡设备。 应能够通过客户端软件禁止计算机私自修改IP地址。 应能够通过客户端软件禁用计算机的DHCP服务，防止通过DHCP服务自动获取IP地址。 应能够监测公安信息网计算机联网状态，公安网计算机一旦脱离公安网，则禁止其网卡所有网络数据通信，使公安网计算机形成离网单机，阻断连接任何公安网以外的网络，避免发生违规外联。 应能够探测发现我市公安信息网内的所有线路外联行为，并将线路外联点进行上报。 为不重复建设以及利旧原则，新建系统能与原有的内网安全监管系统无缝对接，并能有效防范公安网一机两用行为。	浙江远望信息股份有限公司	套	1	100000	100000
2	网络资产与边界感知系统	远望、ABPS1700-2H2X-2U	处理器：2颗*4核；内存：16GB；硬盘：128GB硬盘；网络接口：6个千兆电口，2个万兆光口，2个USB接口 最大镜像流量：20Gbps 最大扫描速率：50Mb/s 支持不安装客户端的情况下，通过镜像流量分析和主动扫描，自动发现管理域内同时连接内网和其他网络（如：互联网）的设备。 支持监测发现基于IPv6地址的外联行为。 支持在外联服务器上取证，取证信息包含：外联设备内网IP、外联出口IP、发现次数、	浙江远望信息股份有限公司	台	1	240000	240000

			首次发现时间和最后更新时间等信息。 支持数据在外联告警系统与内网管理系统间的导出和导入。 支持不安装客户端的情况下，自动发现管理域内曾经脱离内网并且连接过互联网等其他网络的设备。 支持在外联服务器上取证，取证信息包含：外联设备内网IP、外联出口IP、发现次数、首次发现时间和最后更新时间等信息。 支持数据在外联告警系统与内网管理系统间的导出和导入。 支持依赖客户端或不依赖客户端两种模式，自动发现管理域内内网网络设备（如：交换机、路由器等）与其他网络（如：互联网）相连，造成大量内网设备潜在外联的重大隐患。 支持在外联服务器上取证，取证信息包含：外联设备管理口IP、外联设备MAC、外联出口IP、发现次数、首次发现时间和最后更新时间等信息。 支持识别外联设备的厂商信息，辅助对外联设备进行定位和取证。 支持数据在外联告警系统与内网管理系统间的导出和导入。 支持自动发现网络管理域内将内网应用系统或网站页面保存后，拷贝至其他网络（如：互联网）计算机打开的疑似信息外泄行为。 支持在外联服务器上取证，取证信息包含：设备内网IP、外泄时外网IP、首次发现时间、最后更新时间和外泄网址等信息。 支持数据在外联告警系统与内网管理系统间的导出和导入。 支持不依赖客户端，对违规外联的设备实现定点阻断。同时，对于违规行为，支持通过网页访问跳转警示。 支持自动发现网络管理域内的NAT设备和通过该设备私自搭建的局域网，同时上报其边界点设备IP地址、运行状态、首次发现时间、最后更新时间等信息，并能发现NAT子网中设备的IP地址等信息。 在支持不依赖于客户端技术的情况下，支持自动发现管理域内的移动设备接入行为，上报设备的IP、操作系统、厂商类型等信息。 支持发现网络管理域内同时使用多张网卡的设备，获取每个网卡的IP、MAC信息； 支持采集展现其他网卡所在网络区域（子网）内可通信设备的IP、MAC等信息； 支持识别设备的多网卡间是否开启共享，以发现该潜在的网络边界扩展安全隐患。 支持对该设备进行终端提醒、断网、关机等管控操作。					

			支持监测发现网络管理域内注册设备上配置的代理服务器，获取代理服务器IP、运行状态、首次发现时间、最后更新时间等信息，并能对配置该代理服务器的设备进行终端提醒、断网、关机等操作。 支持监测发现网络管理域内的无线AP设备，可获取该无线AP设备IP、生产厂商等信息，支持识别主流无线AP厂商类型。 支持对上报的边界点进行人工备案管理，包括完善其边界基础信息，明确其责任人、责任部门、联系电话、用途等信息，通过人工报备方式对已知边界进行人工备案管理。 支持审计记录网络边界和违规行为的网络流量，统计范围包括：NAT边界、内外网互联、非授权外联、移动设备接入和网页外泄。审计信息包括：协议类型、源地址、目标地址、目标端口、上行流量、下行流量、总流量等。 支持外联事件的核查取证，提供交换机ARP缓存表和PORT-MAC表的历史记录以供查询定位设备所在物理位置。 支持以主动扫描和交换机信息采集等技术手段发现网络内部的存活资产。 支持网络资产类型识别，包括：计算机设备、安全设备、安防设备、办公设备、专用设备等。 支持检测发现主流安防厂商的网络摄像头等安防设备存在的弱口令情况。 支持从C类段的维度查看管控范围内IP使用情况，当前未存在设备的C类段不做展示； 支持从组织结构的维度查看某个部门IP范围内IP使用情况，并以C类段分段展示。可选择的C类段包含当前未存在设备的C类段，但不包含已分配给下级部门的C类段。					
3	违规外联监测服务软件	远望、V2.0	客户端可感知应用层的请求-应答回路（公安信息网与互联网），从而发现“内外网互联”通道，客户端一旦感知到互联通信链路（包括IPV4和IPV6），会向此链路发送验证数据包，数据包能到达外网监测服务器，即表明互联违规行为的存在。 客户端向浏览器以静默的方式推送和运行插件，用户使用浏览器时触发插件检查网络环境，并将取到的信息缓存在本地，具备条件时向外网服务器发送或再次回到内网时向内网服务器发送。 客户端通过收集内网所有的非公安网地址，发现后向外网监测服务器发送探测包，如果探测包可以和外网监测服务器通信，则表明公安网内存在线路外联情况。 支持在外联告警系统对最新发生的外联事件进行查处后，可人工确认和标记。 系统可对告警发生的具体时间、告警的IP地址、MAC地址、部门、联系电话、互联网出口地址、互联网出口端口号、互联网IP归属地进行详细的记录和留存，方便事后的原因	浙江远望信息股份有限公司	套	1	100000	100000

			分析和回溯。 支持通过短信或邮件的方式向指定用户发送告警信息； 支持配置每日发送短信上限。 支持对外联告警数据按时间、用户归属、IP归属等维度进行统计分析。 支持通过开启短信认证模式，实现系统登录时双因子认证。					
4	终端防病毒软件	辰信景云终端安全管理系统7.0	1、管理中心可安装在windowsserver、linux等主流服务器系统，客户端支持windows、linux等操作系统；实配windows客户端授权15000点、linux客户端和其他客户端授权3000点。 2、有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，支持多级级联架构，支持C/S及B/S两种模式对客户端进行管理。 3、杀毒软件管理端须具备集中管理全网各类型终端能力，终端类型包括各版本的windows，linux以及其他操作系统等。 4、展示服务器性能数据，并支持自动刷新，包括：CPU,内存，储存空间占用、疑似威胁磁盘占用率。 5、展示全网终端杀毒相关的状态信息，包括扫描进度、终端名、使用人、IP地址、MAC地址、操作系统、威胁数量、病毒库版本、软件版本、上次扫描时间、更多详情。并支持对展示字段进行选择展示。 6、支持IP自动分组，设置IP自动分组规则后，IP段内的未分组终端将自动分组。 7、具备病毒文件审计追踪能力，可智能定位病毒，及早处理感染源，减少病毒爆发造成的损失。 8、具备基于多步行为判断的主动防御技术，能够根据样本一系列的行为特征来进行综合的风险判定。 9、能够监控和清除病毒、木马、恶意程序、广告/捆绑、防护系统关键点、注册表改写、驱动加载、进程注入等。 10、杀毒软件具备机器学习能力，要求在断网状态下具备不依赖病毒库特征，而采用人工智能识别方式对未知病毒进行查杀。	北京辰信领创信息技术有限公司	年	2	200000	400000

5	脆弱性扫描与管理系统	天镜脆弱性扫描与管理系统V6.0 TJCS-UVS1200	1、标准1U设备，配置6个千兆电口、4个千兆SFP接口，1个RJ45Console口，2个USB接口，单电源；内存：8G；内置存储：128SSD+1TSSD。 2、可扫描IP地址总数无限制。 3、支持对主流操作系统的识别与扫描，包括：Windows、Redhat、Ubuntu、Debian、深度、红旗、麒麟、新支点等。 4、支持扫描容器镜像存在的漏洞，支持扫描互联网上公开仓库中的镜像以及私有仓库中的镜像。 5、支持对主流数据库的识别与扫描，包括：Oracle、Sybase、GBASE、GaussDB、神通、达梦、人大金仓、优炫等。 6、支持对主流大数据组件的识别与扫描，包括：Ambari、Cassandra、Elasticsearch、Flume、Hadoop、Hbase、Hive、Impala、Kafka、Mongodb、Oozie、Redis、Spark、Storm、Splunk、Yarn、Zookeeper，能够扫描的大数据组件漏洞扫描方法不小于300种。 7、支持多种协议口令猜测，包括SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM、REDIS、SMTP等，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。 8、支持扫描任务完成后自动生成指定格式和内容的报表,格式包含html、pdf、word、excel、wps、xml等，内容包含封面摘要、章节目录、任务信息、统计信息、参考信息等。 9、支持端口扫描策略设置，包含标准、常用、快速、全端口、自定义等多种策略。	北京启明星辰信息安全技术有限公司	台	1	120000	120000
6	主机监控与审计系统	远望、V4.0	系统采用B/S架构，管理员只需浏览器即可连接到系统进行各种操作。 管理控制服务端支持运行在国产CPU、操作系统。 终端代理程序支持运行在国产CPU、操作系统。 支持同时管控windows终端、linux和其他终端。 本次实配windows客户端授权15000点、linux客户端和其他客户端授权3000点 支持按设备类型、按区域/部门等条件对管辖区域内设备信息进行查询，设备信息包括基础信息（如：IP地址、MAC地址、使用人、责任人、联系电话、所属部门、设备类型、注册状态、在线状态、保护状态、阻断状态、注册信息锁定状态）、开放端口情况、在线/离线审计； 支持设备操作：保护/取消保护、阻断/取消阻断、编辑、删除、导出、设备部门重置、指定天数的未上线设备删除；	浙江远望信息股份有限公司	套	1	520000	520000

			对已注册且在线设备支持实时点对点控制，包含：在线临时解绑、编辑IP、消息推送、屏幕控制、卸载终端、查看软件、查看硬件、查看服务、查看端口、查看进程、查看策略、查看计算机账户、查看服务端防护日志。 支持从C类段的维度查看管控范围内IP使用情况，当前未存在设备的C类段不做展示； 支持从组织结构的维度查看某个部门IP范围内IP使用情况，并以C类段分段展示。可选择的C类段包含当前未存在设备的C类段，但不包含已分配给下级部门的C类段。 支持IP申请及审核，对管控范围内的IP资源进行合理分配； 支持对IP未申请但已被发现以及IP已分配未使用的IP地址进行告警； 支持对IP在台账中的部门与部门配置的IP范围不一致的情况进行IP资源使用异常告警。 支持注册IP审核,需展示信息包含：IP地址、MAC地址、责任人、联系电话、所属部门、设备所在地、审核状态、申请时间，其中待审核数据支持操作审核通过、审核不通过。 支持注册审核开关配置，开启注册审核后，新安装终端代理程序的设备需管理员审核通过后允许入网。 支持注册密码启用/禁用状态切换，启用后支持设置生效方式（永久生效、生效天数、生效次数）、禁止注册时间段。 对未注册设备提供ARP阻断功能，支持生效范围及例外设备的配置；可查看阻断日志，内容包含IP地址、MAC地址、最后一次阻断时间。 支持每日统计设备注册状态，并支持按区域、按部门进行统计查询，包含：IP设备总数、应注册数、已注册数、保护数、非应注册数、应注册未注册数、应注册未注册已保护数、注册率； 支持定时对设备类型进行统计，并支持按区域、按部门进行统计查询； 支持设备操作系统统计，支持按区域、按部门进行统计查询。 支持发现HTTP和HTTPS两种协议的网站，支持根据IP范围区分管控范围内的网站和管控范围外的网站； 支持根据区域/部门，按注册状态统计范围内网站总数； 实现管理端批量向注册终端设备推送消息，消息以窗口形式提醒终端用户； 消息推送以任务为载体，终端支持多任务同时进行： 支持按所有设备、IP范围、设备自定义组和级联分配任务； 支持任务的启停控制、添加、删除和修改任务； 支持指定推送周期、推送时间，其中周期包含：一次性/每天/每周/每月；					

			支持指定消息级别，包含：普通/重要/紧急/危急； 文件管理：支持文件上传、删除，通过选择文件作为待分发文件； 文件分发任务：支持分发普通文件、屏保文件、桌面壁纸，分发类型支持FTP和HTTP，支持下发文件路径自定义，分发完成后支持静默执行和执行前提示，支持管理员身份运行，为加快分发速度支持共享模式分发； 当已安装终端代理程序的设备出现IP重复时，客户端发出消息提醒，消息提醒样式分为普通、重要、紧急、危急，提醒内容自定义。 支持IP/MAC绑定、DNS绑定。其中IP/MAC绑定分为与当前IP绑定、绑定到指定IP范围，DNS绑定可指定绑定IP范围。 实现终端设备使用的IP与网卡MAC地址的绑定，禁止用户随意修改IP。 通过设置鼠标键盘未操作时间来定义空闲，支持设置关机倒计时时间、策略执行时间、有效时间。 提供对指定范围内的设备上的硬件配置信息变化情况记入审计日志，并支持检索查询。可按照所属部门、IP地址、上报时间、变更动作、变更内容查看审计日志，展示内容包含：设备基本属性信息、硬件ID、变更动作、变更内容、审计时间、上报时间。 提供对指定范围内的设备上的软件配置信息变化情况记入审计日志，并支持检索查询。可按照所属部门、IP地址、上报时间、变更动作、变更内容查看审计日志，展示内容包含：设备基本属性信息、变更动作、变更内容、审计时间、上报时间。 为终端代理的默认检查功能，无需策略驱动； 杀毒软件检查前对终端进行提醒，提醒内容及提醒方式可配； 检查完成记录未安装杀毒软件及未运行杀毒软件检查的设备； 支持按照IP地址、责任人、上报时间三个条件查询未安装杀毒软件的设备，展示内容包含：设备基本属性信息、检查时间、上报时间，支持点对点终端提醒； 支持对指定范围内的设备进行软件安装情况检查，支持禁止安装软件列表和必须安装软件列表配置； 支持按照IP地址、责任人、检查类型、上报时间、软件名称五个条件查询客户端必须安装的软件和违规安装的软件的安装情况，展示内容包含：设备基本属性信息、软件名称、检查类型、上报时间，支持点对点终端提醒。 支持按照所属区域、所属部门、IP地址、责任人查询使用无线网卡的设备，点击无线网卡数展示具体的无线网卡信息包括无线网卡名称等，支持点对点终端提醒。					

			对指定范围的设备硬盘上的文件名称进行检索； 支持按照IP地址、所属部门、文件名称、上报时间查询。 对指定范围的设备进行系统账户弱口令检查，支持多个弱口令列表指定； 展示内容包含：设备基本属性信息、账户名称、检查时间、上报时间。 对指定范围的设备进行系统账户空口令检查；展示内容包含：设备基本属性信息、账户名称、检查时间、上报时间。 对指定范围的设备进行过期系统账户检查；展示内容包含：设备基本属性信息、账户名称、检查时间、上报时间。 无用账户即指定时间内未使用的账户，时间可配； 支持对指定范围的设备进行无用账户检查； 展示内容包含：设备基本属性信息、账户名称、检查时间、上报时间。 对指定范围的设备的进程运行情况进行检查； 支持禁止运行进程列表和必须运行的进程列表配置； 展示内容包含：设备基本属性信息、进程名称、检查类型、上报时间。 提供对指定进程的禁用功能； 提供定期对指定进程的CPU占用和内存占用进行监测，监测间隔时间支持配置。 提供对指定服务的禁用功能。 按照配置的规则对数据访问进行控制。 按照配置的隔离规则来对数据访问进行控制；隔离对象支持按IP范围隔离、按组隔离； 隔离规则支持指定的允许访问对象、访问协议以及指定的允许来访对象、访问协议。 提供对指定范围内设备的流量使用异常监测功能；支持按照所属部门、IP地址、责任人、上报时间查看异常日志；展示内容包含：设备基本属性信息、异常描述、发现时间、上报时间。 提供对指定范围内设备的应用点击异常监测功能；支持按照所属部门、IP地址、责任人、上报时间查看异常日志；展示内容包含：设备基本属性信息、异常描述、发现时间、上报时间。 提供对指定范围内设备的瞬间连接异常监测功能；支持按照所属部门、IP地址、责任人、上报时间查看异常日志；展示内容包含：设备基本属性信息、异常描述、发现时间、上报时间。 对打印输出的行为和结果进行监控与审计；支持所属部门、IP地址、文件标题、打印时					

			间查看审计日志；展示内容包含：设备基本属性信息、文件标题、打印时间、打印机名称、打印页数、打印份数、计算机账户、打印状态。 对光盘刻录的行为和结果进行监控与审计，包括但不限于内置光驱、外置光驱等途径的刻录行为；审计内容包含：设备基本属性信息、任务名称、文件数量、刻录机型号、光盘属性、计算机账户、刻录状态。 支持对主机插入数字证书的审计，审计内容包括：姓名、证书号、访问系统名称、访问时间，并可以通过时间范围、查询次数、组织架构进行检索。 对FTP访问的行为和结果进行监控与审计；审计内容包含：设备基本属性信息、FTP地址、动作类型等。 对TELNET访问的行为和结果进行监控与审计；审计内容包含：设备基本属性信息、TELNET客户端、TELNET服务端等。 对共享操作进行审计；支持共享名称、共享状态的查询；审计内容包含：设备基本属性信息、共享名称、共享路径、共享模式、共享状态等。 支持对设备的远程桌面共享、磁盘共享、打印机共享的禁用。 支持按照IP地址、责任人查询客户端USB使用痕迹情况，点击痕迹数具体展示U盘硬件ID、使用时间。 监测违规外联事件，控制外联持续发生，上报外联信息，支持外联事件包含：接入互联网（即外联后接回内网、同时连接内外网、仅连接外网）和接入私网。 支持外联探测地址的配置，包含外联服务器或外网域名； 支持外联目标信息的获取； 支持发生外联后采取终端提醒、断开网络、强制关机等防护动作，并可设置防护动作在重启计算机后是否持续有效，还可设置持续强制关机解锁密码； 支持外联时向外联服务器上传日志； 支持外联后回归至内网时向内网服务器上报日志。 提供对安全区域内设备非法连接互联网的监控；支持按照外联类型（外联后接回内网/同时连接内外网/仅连接外网）、IP地址、责任人查询；展示内容包含：设备基本属性信息、外联类型、外联IP、外联时间等。 提供安全区域内设备非法连接其他私有网络的监控；支持按照IP地址、责任人查询；展示内容包含：设备基本属性信息、脱网时间、归网时间等。 提供对指定范围的设备进行游戏娱乐、下载行为、聊天行为、炒股行为、视频应用、黑					

			客行为的监测；支持按照应用名称、事件状态查询客户端应用行为；展示内容包含：设备基本属性信息、应用名称、应用全路径、时间状态、发现时间、终止时间等。 用于查询和记录用户浏览器历史访问痕迹；支持按照IP地址、责任人查询客户端浏览器访问痕迹情况；展示内容包含：设备基本属性信息、痕迹数等；点击痕迹数具体展示访问地址、访问时间等详细信息。 提供对指定范围内的设备上的最近打开文档的痕迹检查功能；支持按照IP地址、责任人查询客户最近打开的文档痕迹检查情况；展示内容包含：设备基本属性信息、痕迹数等；点击痕迹数具体展示文档名称、路径等详细信息。 用于查询和记录用户通过浏览器对网络摄像机的登录、预览、下载、回放的动作审计；审计内容包含：设备基本属性信息、目标IP、设备名、厂商、操作类型、检查时间、审计时间等。 配置外设控制策略，提供对USB设备、网卡的控制功能，支持控制日志的展示和接入日志的展示。 支持交换机基础信息配置，包含：管理口IP、MAC地址、设备名称、设备别名、设备类型、厂商、所属部门、设备型号、负责人、所在位置； 支持SNMP采集配置，包括SNMP协议v2和v3版本的配置，其中v2版本需要配置SNMP只读团体名，v3版本需要配置USM用户名、认证算法、认证密码、隐私算法、隐私密码； 支持远程登录配置，配置信息包括：远程登录方式、登录端口、登录用户、登录密码。					
总计								1480000