2025统一安全管理中心及杀毒软件需求

2025年7月

根据《基本医疗卫生与健康促进法》、《网络安全法》、《密码法》、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》、《网络安全审查办法》以及网络安全等级保护制度等有关法律法规要求，响应《医疗卫生机构网络安全管理办法》（以下简称“办法”）政策要求，督导青浦区属各医疗卫生单位落实《关于持续做好2025年本市卫生健康行业信息系统病毒防治工作的通知》（沪卫信息便函[2025]1号）要求的各项工作，压实网络安全主体责任，完善网络安全监督管理机制，加强关键信息基础设施安全保护，强化网络安全技术防护能力，提高网络安全态势感知、预警和协同能力，提升突发网络安全事件应急响应能力，同时加强财政资金使用效率，我区拟为12家社区卫生服务中心、朱家角人民医院和区级数据中心进行统一安全管理中心及杀毒软件系统建设。

**一、建设目标**

本次将在区一级建设统一安全管理中心，其中包括用于统一管理区卫健委信息中心、全区12个社区卫生服务中心及朱家角人民医院的杀毒软件系统和态势感知平台两部分，以便及时收集、汇总、分析各方网络安全信息，加强威胁情报工作，组织开展网络安全威胁分析和态势研判，及时通报预警和处置，防止网络被破坏、数据外泄等事件。

统一安全管理中心及杀毒软件项目总体目标为：实现区卫健委及所辖区域医疗卫生机构的病毒防护，并根据分组、分部门部署安全策略，管理中心为运维管理人员提供统一防病毒、统一补丁管理、终端安全策略管理、终端审计等多种管理功能，支持级联部署，并与区态势感知实现威胁情报联动联动，管理员可以通过控制台直接对网内所有终端进行统一管控。确保全网终端安全看得见、管得住。

杀毒软件终端可以收集终端上的各种安全状态信息，包括：漏洞修复情况、病毒木马情况、危险项情况、安全配置以及终端各种软硬件信息等。这些安全状态信息会汇集到区统一安全管理中心，使管理员全面了解网内所有终端的安全情况、硬件状态以及软件安装情况等。可以帮助管理员对全网安全态势掌握一目了然。

终端具有漏洞修复、系统加固、病毒查杀、勒索防护等多样化的防护手段，从网络管控、外设管控、终端用户行为控制等多个层次，为用户构建立体防护网，防篡改、防入侵、防窃密、防插播、防挂马、防病毒、防瘫痪，确保医卫终端安全。

为了提高医疗机构信息系统的安全性，确保患者数据和医院运营的安全，需要在所有相关机构中部署统一的安全管理中心和杀毒软件。本项目将为全区12家社区卫生服务中心、朱家角人民医院和区级数据中心的医疗终端和相应服务器等建设一个包含安全管理中心及提供终端杀毒软件服务和统一管理平台，配合各单位开展网络安全建设，全面落实网络安全保护措施。

1. 项目安全现状
   1. 区卫健委信息中心安全现状

区卫健委信息中心现有主要网络安全设备包括政务网出口防火墙、服务器区域核心防火墙，通过政务网与各社区卫生服务中心的政务网前置机进行数据交互。使用态势感知区级平台进行相关安全威胁发现与运营管理，态势感知品牌型号：华三NS-SecCenterCSAP主要功能：支持基于规则引擎对告警接收、过滤、压缩、归并、升级的事件处理流程，并具备基于 AI算法的动态阈值与故障根源定位能力;提供可视化运行态势感知;支持与流程、自动化联动，实现故障派发工单、故障自愈等联动处置能力，实现故障处理的标准化与规范化。

区卫健委信息中心安全运营体系建设以《信息安全技术网络安全等级保护基本要求》为指引，以《信息技术服务管理体系标准》为准则，以《数据安全法》为合规标尺，对青浦卫生健康行业相关的环境基础设施、计算机网络设备、服务器设备、应用系统软件和应用业务数据等进行安全服务设计。同时针对青浦区医疗付费“一件事”区级平台、青浦区区域卫生信息共享交换平台、青浦区区域影像中心、青浦区数字健康城区系统、青浦区便捷就医数字化转型系统等关键平台构建高效率、细粒度的实战化安全运营体系，打造威胁检测响应新范式，推动单位安全工作迈向“更高、更快、更强”新局面。

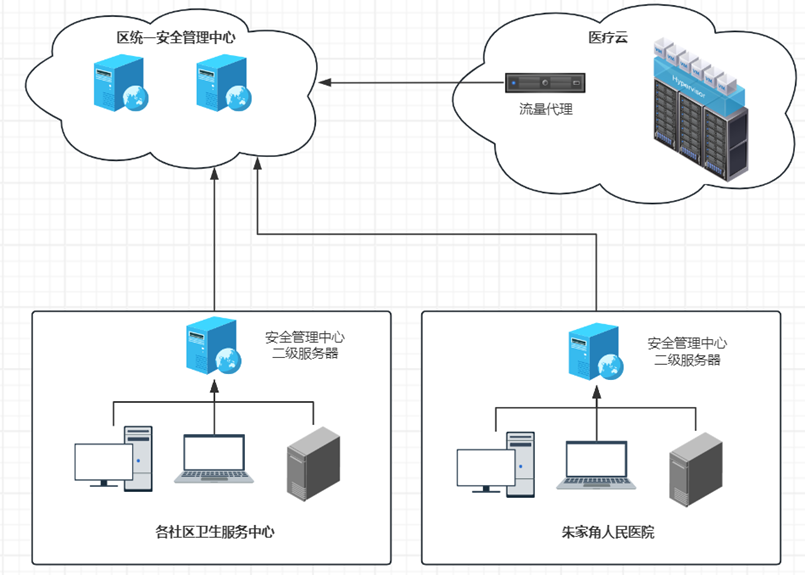
* 1. 各社区卫生服务中心安全现状

下属社区卫生服务中心现在主要网络安全设备包括内网核心交换机、政务网出口防火墙、服务器内网防火墙，态势感知探针。通过政务网平台前置机与区卫发中心一级安全管理中心进行数据交互。主要安全设备为等保一体机，品牌型号：华三NS-SecCenter X6020主要功能：日志审计模块，数据库审计模块，堡垒机模块，漏洞扫描模块。内网终端通过平台前置机访问社区核心业务系统：院内重要信息系统。

* 1. 朱家角人民医院安全现状

上海市青浦区朱家角人民医院作为上海市卫生健康行业的重要组成部分，随着信息技术的快速发展，医院的业务运行越来越依赖于IT基础设施。其中终端安全尤为重要，现有安全设备包括内网核心防火墙、政务网出口防火墙、互联网医院防火墙，医院通过政务网前置机与区平台一级中心进行数据交互。业务终端通过内网访问医院业务系统，核心业务系统包括HIS、LIS、PACS、长三角互联网医院系统。

1. 项目整体架构



针对我区医疗卫生单位规模、级别不一，位置分散的特点，平台应采用混合云架构，既支持为卫生行政管理单位、社区卫生服务中心等医疗终端提供基于公有云的杀毒软件服务，也支持大型二三级医院私有化部署二级安全中心并级联至区平台，平台管理采用B/S架构，支持通过WEB访问；终端管理采用C/S架构；支持一个中心统管全区范围内的客户端，降低管理运维复杂度，减小安全暴露面。

1. 运行性能需求

杀毒软件系统应支持在区内各类软硬件基础设施平台进行部署，其中系统中心和客户端均应支持在物理机、虚拟机上部署，应支持在兆芯、海光、飞腾、鲲鹏、龙芯等CPU平台部署，应支持在CentOS、华为Euler、龙蜥等主流Linux开源版及统信、中标麒麟、银河麒麟等商业版操作系统上部署。

杀毒软件运行过程中必须与现有系统完全兼容，不影响现有医疗服务流程。客户端应最小化对系统资源的占用。在确保安全防护能力的同时，对用户办公主机及生产服务器的CPU占用不得高于25%，内存占用不得超过500M。

杀毒软件系统需具备良好的兼容性和可用性，为现有医疗业务应用提供白名单放行功能，无论查杀还是防御均不可损耗业务系统的运行性能。

杀毒软件系统的杀毒引擎更新、病毒特征码、漏洞补丁下载等功能均应支持网络限速，防止业务时间段对医疗卫生机构网络资源造成较大消耗。

系统可靠性

杀毒软件系统管理平台应具备高可用设计，支持万点以上客户端同时接入管理；应支持设置定期数据备份策略。

系统可扩展性

杀毒软件系统应具备良好的可扩展性，包括平台规模的横向扩展及系统性能的纵向扩展。

系统安全保密性

杀毒软件系统应符合密码应用安全评测要求，对账号、口令、资产信息等用户数据进行加密传输及存储；系统支持强制高强度密码策略，强制定期修改密码；支持进行登录IP限制、登录失败锁定等安全限制；支持进行多因素身份鉴别。

1. 功能需求

为落实各项网络安全保护法规政策及《关于持续做好2024年本市卫生健康行业信息系统病毒防治工作的通知》的要求，杀毒软件系统应具备如下功能：

4.1管理能力

支持网页访问部署、离线安装包部署等部署方式。

支持对不活动终端设置过期时间，不活动终端超时后将自动从中心删除，腾退出授权点数。

支持常态化病毒特征库升级，支持管理员通过控制台手动下发和设置定时升级任务。

4.2病毒防护能力

支持对僵尸网络、木马、蠕虫等常见流行病毒的查杀防御。

支持对压缩包文件进行扫描。

支持对宏病毒进行查杀防御，具备文档保护和修复能力。

支持对感染型病毒查杀和修复，具有代码级修复能力。

支持U盘接入电脑时自动扫描。

支持对勒索病毒提供查杀防护，支持采用虚拟钓饵方式拦截勒索病毒。

支持对浏览器、局域网共享、即时通讯工具等传输的文件进行落地扫描。

支持客户端自保护，阻止非法退出和卸载杀毒软件。

支持自定义设置查杀和防御白名单。

支持管理员通过控制台手动下发查杀任务和设置定时查杀任务。

支持对新型未知病毒（挖矿、勒索）进行防护。

支持对勒索病毒传播进行专项监测。

4.3漏洞修复能力

支持定期展开漏洞监测，支持按照补丁维度与终端维度两种模式统计全网终端系统补丁安装情况。

支持管理员通过控制台统一手动下发和设置定时漏洞修复任务。

4.4运维管控能力

支持对终端进行账号口令合规检查，管理员可查看终端是否有弱口令、默认账号、超级账号、共享账号、无用账号等情况。

支持检查终端主机安全审计配置，包括审核登录事件、审核策略更改、审核帐户登录事件以及管理审核和安全日志等安全项。

支持检查终端主机入侵防范配置合规性，包括禁用共享、启用系统防火墙等安全项。

支持终端资产登记功能，将计算机IP、MAC与使用人进行关联。

支持集中统一管理终端软硬件资产。

支持对移动存储介质进行使用权限管控，包括可用及不可用管控，注册使用管控等。

支持对终端进行网络管控，支持设置网络访问黑白名单。

支持对终端进行违规外联监测。

4.5威胁检测与响应能力

为构建统一安全管理中心，最大化发挥区内各类网络安全设备功效，避免重复投入，本项目将采用支持异构多元安全态势感知的杀毒软件产品，支持接收其他品牌安全设备的威胁情报，整合区内已部署的现有各品牌安全设备情报能力，形成安全运营管理中台，实现“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”。

杀毒软件系统应支持汇总各类安全设备威胁事件情报的主要信息，并根据威胁类型进行分类，查看威胁事件详情。

杀毒软件系统应支持支持与网络安全设备和准入控制系统联动，管理员可手动下发联动操作指令，形成威胁事件处理闭环。

杀毒软件系统应支持进行威胁响应处置剧本（Playbook）编排，实现威胁事件的自动化闭环处理。

为保证项目建设的可持续性，投标方需获取厂商承诺，免费提供后续对我区威胁情报来源设备及联动处置设备的兼容适配工作。

4.6态势感知联动

为充分利用我区卫发中心现有态势感知系统能力，投标方应完成与区卫发中心现有态势感知系统H3C安全威胁发现与运营管理平台联动功能的适配，支持将自身数据作为威胁情报来源同步至态势感知系统，并支持将自身作为态势感知系统的威胁检测引擎的病毒特征库来源。

杀毒软件系统应支持与区内现有态势感知系统H3C安全威胁发现与运营管理平台联动，同步响应态势感知系统的剧本进行终端处置动作。

**二、项目清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 描述 | 单位 | 数量 |
| 统一安全管理中心 | 一年授权服务 | 套 | 1 |
| 客户端 | 一年授权 | 套 | 2464 |
| 服务器端（windows) | 一年授权 | 套 | 539 |
| 服务器端（linux) | 一年授权 | 套 | 100 |
| 系统中心 | 一年授权 | 套 | 14 |

终端及服务端杀毒软件明细如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **需求单位** | | **客户端（内网）** | **windows服务器端** | **linux服务器端** | **系统中心** |
| 1 | 区卫健委信息中心 | | 7 | 108 | 18 | 1 |
| 2 | 社区卫生服务中心（包含分中心） | 金泽镇社区卫生服务中心 | 236 | 35 | 5 | 1 |
| 3 | 练塘镇社区卫生服务中心 | 225 | 35 | 5 | 1 |
| 4 | 朱家角 | 150 | 15 | 5 | 1 |
| 5 | 夏阳街道社区卫生服务中心 | 230 | 30 | 8 | 1 |
| 6 | 白鹤镇社区卫生服务中心 | 180 | 30 | 5 | 1 |
| 7 | 重固镇社区卫生服务中心 | 118 | 30 | 5 | 1 |
| 8 | 赵巷镇社区卫生服务中心 | 118 | 30 | 5 | 1 |
| 9 | 华新镇社区卫生服务中心 | 128 | 26 | 4 | 1 |
| 10 | 盈浦街道社区卫生服务中心 | 336 | 30 | 5 | 1 |
| 11 | 香花桥街道社区卫生服务中心 | 220 | 30 | 5 | 1 |
| 12 | 徐泾镇社区卫生服务中心 | 156 | 30 | 5 | 1 |
| 13 | 徐泾北大居社区卫生服务中心 | 60 | 15 | 20 | 1 |
| 14 | 朱家角人民医院 | | 300 | 95 | 5 | 1 |
| **合计数量** | | | **2464** | **539** | **100** | **14** |

**三、技术要求**

**1、统一安全管理中心要求**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务要求 | | 服务内容 |
| 1 | 资产安全运营 | 资产发现 | 根据给定的IP、IP段或者端口主动进行资产探测，基于探测结果进行分析，准确研判出被探测目标的操作系统、开放端口、开放服务、MAC地址、资产名称。相关资产数据采用人工或自动化工具的方式传入资产数据库便于统一运营管理。 |
| 2 | 能够主动通过测绘形式发现资产，并使用自动化的方式传入资产数据库。（提供能力证明材料） |
| 3 | 能够通过分析网络流量，发现其中存在的资产信息，并使用自动化的方式传入资产数据库。 |
| 4 | 对资产端口进行有效管理，如对端口、端口组的创建、启用、禁用、删除，以及对端口信息的传入输出。 |
| 5 | 资产管理 | 从不同维度实现对资产的运营管理，如硬件、软件、部门等，能够对资产进行传入输出。 |
| 6 | 能够对资产的变更进行有效记录。（提供有效变更证明材料） |
| 7 | 漏洞安全运营 | 漏洞检测 | 能够通过流量分析检测出安全漏洞，漏洞检测能力不少于8000个，能够对近5年的热点漏洞进行检测，检测能力不少于2500个（提供漏洞检出数量能力证明）。能够分析研判检测出web攻击、恶意文件攻击、远程控制、web后门访问行为分析、smb远程溢出攻击、弱口令拒绝服务攻击、隧道通信、暴力破解、挖矿恶意工具、矿池外联、渗透扫描、漏洞利用、钓鱼邮件等。 |
| 8 | 使用引擎或沙箱工具，对现网传输进行有效分析，发现广告软件、APT工具、后门软件、挖矿软件、勒索病毒、破解工具、提权工具等非法文件，特别是黑客工具。 |
| 9 | 漏洞运营过程中，能够检测挖矿木马投递、横向移动行为，检测挖矿软件、矿池域名解析、矿池协议、虚拟币种等威胁行为。 |
| 10 | 漏洞情报 | 定期提供各类威胁情报的IOC，包括但不限于IP、域名、文件哈希、URL，覆盖僵尸网络、恶意站点、矿池域名、各类恶意软件等。 |
| 11 | 安全威胁运营 | 威胁狩猎 | 通过IP地址进行威胁狩猎工作，根据攻击者和受害者的风险要素进行逐层分析和逐级追踪，基于所掌握的IP进行综合分析，发现与该IP相关的设备告警信息和访问信息，并按照时间顺序还原相关资产遭受攻击的过程。（提供狩猎能力的证明材料） |
| 12 | 能够快速编制、修改、删除狩猎报告，将星空图和相关异常元素，快速编入威胁狩猎报告中。（提供威胁报告管理证明材料） |
| 13 | 能够基于可疑IP开展攻击溯源和威胁狩猎，并在星空图中描述待分析IP和可疑IP的关系。 |
| 14 | 当IP出现异常时，能够主动展示异常点，并从主机、网络设备、数据库、应用系统、中间件等维度查看异常信息，并关联到系统漏洞、弱口令、基线违规、访问流量等。 |
| 15 | 安全事件运营 | 事件发现 | 使用规则引擎和融合建模的方式，对原始日志或内部事件，进行关联、聚合分析构建安全事件；安全规则分析、融合关联分析引擎，对多源告警进行关联，并对告警进行聚合，告警中识别安全事件，杜绝告警风暴。 |
| 16 | 按照给定的事件类型、事件等级、处置状态、攻击阶段等信息，发现符合的安全事件。（提供安全事件发现能力证明材料） |
| 17 | 事件可视 | 将安全事件统计信息，包含事件类型、事件数量、等级、受攻击IP等内容以可视化方式进行展示。 |
| 18 | 提供安全事件的处置建议、统计报表和事件详情等信息。批量处置聚合形成的事件告警。提供安全事件概览，直观展现什么时间、什么资产发生哪些安全事件，相关元素可以拖拽分析查看。 |
| 19 | 设备运营 | 剧本编制 | 能够以剧本形式开展安全运营，提供防毒墙一键封堵、终端病毒一键查杀、Web病毒一键查杀、挖矿检测防护、主机异常监控、勒索漏洞防护、漏洞攻击防护、应用漏洞防护、资产勒索防护、域名勒索防护等至少10类剧本（提供剧本证明材料） |
| 20 | 自动化运营 | 提供安全剧本，或根据要求自定义剧本，包含自动处置、人工处置节点。 |
| 21 | 将防毒墙、云主机安全、终端安全管理等产品进行联动，实现防毒墙一键封堵、终端病毒一键查杀、Web病毒一键查杀、挖矿检测防护、主机异常监控、勒索漏洞防护、漏洞攻击防护、应用漏洞防护、资产勒索防护、域名勒索防护等。（提供相应能力证明材料） |
| 22 | 将剧本与安全告警结合，使安全告警激活剧本。 |
| 23 | 运营监测 | 告警管理 | 能够基于IP、端口、域名、URL等信息与本地威胁情报库的失陷库碰撞，命中威胁情报发出安全告警。（提供能力证明材料） |
| 24 | 对于网络流量类告警，能够查看原始网络流量数据，支持基于原始数据包序列，提供安全告警的上下文网络会话信息。 |
| 25 | 可视化运营 | 综合展示 | 从综合态势、安全告警、外部威胁、横向威胁、外连威胁、脆弱性威胁、恶意程序、资产态势、资产画像9种维度，进行安全运营展示，展示能以3D效果呈现。 |
| 26 | 展示内容可以进行轮播，指定展示维度和展示时间。可以批量或单独对展示维度进行参数设置包括否情报命中、安全域、组织机构等。（提供展示维度证明材料） |
| 27 | 能够从运维人员角度去展示运维拓扑，将各类资产及资产间的互访关联关系，以逻辑拓扑的方式进行展现，并在拓扑上展示攻击路径，使得用户直观掌握整个网络的拓扑结构和资产的安全状态。（提供相应能力证明材料） |
| 28 | 运营汇报 | 运营报告 | 提供运营报告模块，包括安全日报、安全周报、安全月报等，并可以快速生成报告 |
| 29 | 报告内容包括系统的资产信息、安全告警、监测结果、处置建议等信息 |
| 30 | 能够利用AI降噪引擎，利用自研机器学习模型结合人工实现人机互动，释放研判海量、重复的告警人力，提升告警精度，助力安全运营。（提供相应能力证明材料） |

**2、终端及服务器端（含系统中心）杀毒软件技术要求（核心设备）**

**2.1、系统中心安装部署要求**

★支持采用多级系统中心部署，支持在医疗卫生机构内本地部署下级系统中心服务器，从而实现性能和流量负载分担。区系统中心可实时监控下级系统中心的名称、在线状态、IP地址、客户端程序版本、客户端病毒库版本。（提供功能截图，加盖厂商公章）。

▲系统中心支持通过流量代理转发方式提供接入服务，提供接入点（AP）组件，用于部署在各医疗卫生机构或医疗业务专用网络内，支持虚拟主机在不配置网关参数的情况下将其杀毒软件客户端通讯流量转发至区系统中心，实现一个中心统管全区客户端；无需在每个专有网络下设管理服务器，节约资源利用，降低运维工作压力，同时区系统中心仅需对下属单位的特定接入点IP开放访问服务，降低资产暴露面；支持在系统中心控制台对接入点进行集中展示管理，显示包括AP的在线状态、IP地址、软件版本、通讯流量、最新通讯时间等信息（提供功能截图，加盖厂商公章）。

系统应提供多级多租户的管理特性；支持按照本单位的组织架构为每个分支部门创建独立的租户分级，支持为每个租户分配对应管理员账号，以便实现日常安全运维工作分担；支持租户隔离，租户管理员账号仅能管理当前租户所辖客户端；支持按照机构部门架构创建下级部门分组，支持至少5级分组；支持管理员自主创建下级管理员账号并指派分管的租户分级或分组；支持指派下级管理员账号同时管理多个租户分级或分组下的客户端（提供功能截图，加盖厂商公章）。

系统中心支持多种分组规则，如手动分组、IP分组等,支持按照指定IP段一键刷新客户端到对应分组；支持将用户AD域组织架构同步到系统中心，依照用户现有架构进行管理。支持生成分组安装包，安装后自动进入该分组；支持搜索分组安装包。

系统中心支持网页访问部署、离线安装包部署等部署方式，可自定义部署通知邮件及部署通知公告。

提供支持互联网访问的厂商官方下载网站，用于用户及时获得最新安装包、升级包、特征库升级，提供x86\_64、amd64、arm64、aarch64、mips64、loongarch64等主流技术路线的程序安装包、升级包。（提供功能截图或其他证明材料，加盖厂商公章）

为节省总体安全运营成本，系统中心应支持对不活动终端设置过期时间，不活动终端超时后将自动从中心删除，腾退出授权点数。

系统中心支持推送消息公告给终端，支持对全网和分组推送，并支持导出消息公告历史记录。

通用客户端兼容性：支持WindowsXP及以上版本桌面操作系统、WindowsServer2003及以上版本服务器操作系统，支持主流Linux发行版如RedHat、CentOS、Ubuntu等。

信创客户端兼容性：支持中标麒麟、银河麒麟、UOS操作系统；支持兆芯、海光、飞腾、鲲鹏、龙芯等CPU环境。

支持国产数据库，至少包括达梦、人大金仓、南大通用、瀚高。（提供功能截图或其他证明材料，加盖厂商公章）

2.2、病毒查杀与防护

客户端支持对压缩包格式的病毒文件进行查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力，支持1-32层压缩扫描，且用户可以自定义设置解压扫描层数。

客户端支持连接公有云、私有云进行病毒特征查询，支持与恶意代码检测设备联动对未知文件鉴定功能。

支持对宏病毒的查杀，可以对文档保护和修复。

支持对感染型病毒查杀和修复，具有代码级修复能力。

U盘接入电脑时自动扫描根目录下文件、自动扫描被病毒修改的项目，保护电脑不被感染。

支持远程控制爆破防护，阻止黑客通过SMBv1、SMBv2协议进行口令暴力破解攻击。

支持保护系统关键文件不被篡改、破坏或恶意创建；防止特定注册表项目不被恶意篡改；监控针对系统的敏感行为，拦截高风险动作；阻止特定命令行被恶意利用的行为；保护系统关键进程不被攻击利用。

支持对QQ、MSN、阿里旺旺等即时通讯软件下载的文件扫描，保证文件的安全性。

支持提供U盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马。

能够对局域网共享文件传输进行检测和查杀。

支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置。

对勒索者病毒提供防护机制，采用虚拟钓饵方式有效拦截勒索者病毒，当出现勒索行为，对其进行捕获并进行隔离。

支持对CobaltStrike、Sliver等工具的木马攻击进行防御，并提供专项报表统计（提供功能截图，加盖厂商公章）。

当文件被执行、生成、访问时，文件监控通过对相应文件进行扫描。用户可以根据自己需求配置不同的监控策略，包括扫描时机和反病毒引擎相关配置等，从而在不影响日常电脑使用的基础上，实时保护电脑不受病毒侵害。

支持客户端自保护，阻止非法软件结束客户端进程，支持设置客户端的退出、卸载、管理员密码。

支持分别设置查杀和防御白名单，支持按文件名、文件路径、文件后缀名予以放行，防止误杀或误拦截影响系统稳定运行。

支持系统平台自定义文件黑名单，提供文件上传加黑，文件MD5加黑等多种方式，以便快速进行新型病毒响应（提供功能截图，加盖厂商公章）。

支持多种查杀扫描模式，包括快速查杀、全盘查杀、指定路径查杀，支持控制台手动下发查杀指令或通过计划任务进行查杀，计划任务查杀支持按日、周、月指定时间段进行。

支持对终端防护策略进行细粒度配置：包括进程保护（进程启动、线程启动、进程打开、现程打开等）、注册表防御（注册表创建、修改、删除、关闭）、文件防御（关键目录文件创建、修改、删除、关闭等）、网络驱动，可根据不同终端需求定制不同的策略。

**2.3、补丁管理功能**

系统中心支持按照补丁维度与终端维度两种模式统计全网终端系统补丁安装情况，可对全网推送补丁安装且支持导出补丁清单。

补丁文件管理，缓存在系统中心本地的补丁，可进行下载。

补丁忽略：可以按照补丁进行忽略，忽略的补丁将不再修复，防止终端打补丁后造成系统或业务进程崩溃。

**2.4、终端运维管控功能**

系统中心支持按照软件维度与终端维度两种模式统计全网终端软件安装情况，可对全网推送软件卸载任务通知且支持导出软件清单。

系统中心支持按照设备维度与终端维度两种模式统计全网终端硬件信息包括CPU、内存、硬盘、显卡、显示器且支持硬件清单导出，构建资产清单报表。

系统中心支持硬件资产变更审计，包括CPU，内存，主板，硬盘，显卡、显示器等。

系统中心可对全网终端下发登记任务，需登记的信息可自定义内容且可开启终端安装时资产登记功能。

支持终端网络通讯端口过滤，可进行许可及不许可访问设置。支持网络访问IP黑白名单，设置为黑名单的IP不能访问,白名单可访问，支持双向访问控制。

支持自定义黑名单URL禁止访问，自定义白名单URL只许可访问，限制访问不受信任的网站。

支持按终端总流量限制设置，并且可以对终端分别进行上行及下行方向的流量限制设置和离线生效设置。

支持外设使用权限管控，包括对串口、并口、USB口、1394、PCMCIA等接口进行管控，支持可用及不可用管控。针对外设设备，除了支持按接口类型的管理，还支持具体设备类型管控，如U盘、打印机、蓝牙、扫描器、光盘等，同时支持可用及不可用管控。

支持U盘注册管控，U盘注册后才可在装有客户端的终端上使用，同时注册时对U盘进行备案记录，包括U盘信息、使用终端信息、相关责任人信息等。

支持对终端进行违规外联监测，管理员可自定义非法外联IP，便于发现安全隔离区域因各类原因出现的网络管控缺口（提供功能截图，加盖厂商公章）。

支持对终端的网络外联访问行为进行日志记录，便于对安全事件进行多渠道情报比对及威胁溯源。

**2.5、终端基线合规检查**

支持检查终端主机身份鉴别配置合规性，对包括密码复杂性、长度最小值、密码最短使用期限、密码最长使用期限、强制密码历史、账户锁定阈值、账户锁定时间等安全项进行检查。

支持检查终端主机访问控制配置合规性，包括Guest账户状态、admin账户是否重命名、开机自动登录、文件夹的共享权限禁止设置为Everyone组等安全项进行检查。

支持检查终端主机安全审计配置合规性，包括审核登录事件、审核策略更改、审核帐户登录事件以及管理审核和安全日志等安全项进行检查。

支持检查终端主机入侵防范配置合规性，包括禁用共享、启用系统防火墙等安全项进行检查（提供功能截图，加盖厂商公章）。

支持进行终端系统状态合规性检查，对包括高危补丁、高危端口、高危服务、弱口令等安全项进行检查（提供功能截图，加盖厂商公章）。

**2.6、威胁检测与响应**

▲系统中心应支持异构多源安全态势感知，可接收其他品牌安全设备的威胁情报，利于整合区内已部署的现有各品牌安全设备情报能力，形成安全运营管理中台（提供与三个已兼容其他品牌设备情报联动功能截图，加盖厂商公章）。

支持从威胁事件维度展示事件的主要信息，包括威胁级别、最近发现时间、威胁标签、影响主机、处理状态和操作等，并支持根据威胁类型进行分类，查看威胁事件详情。

支持从威胁终端维度展示终端的主要信息，包括威胁级别、最近发现威胁时间、威胁标签、影响主机IP、终端状态、处理状态和操作等，并支持根据严重级别进行分类，查看威胁终端详情。

提供威胁总览，包括剧本执行情况、威胁数量统计、威胁终端统计、响应动作关联剧本数量等展示维度，并支持按时间筛选。

▲支持与网络安全设备和准入控制系统联动，将异构设备的同类型安全能力整合利用。当平台监控发现威胁事件时，联动相应的设备自动或者管理员通过系统中心手动下发操作指令进行动作联动，形成威胁事件闭环处理（提供与其他品牌网络设备联动功能截图，加盖厂商公章）。

▲支持进行威胁响应处置剧本（Playbook）编排，管理员可自定义剧本信息：包含剧本的触发条件、响应动作配置、后置执行动作等，实现威胁事件的自动化闭环处理（提供功能截图，加盖厂商公章）。

支持威胁响应处置剧本执行历史记录，记录每个剧本在每台终端的详细执行状态。

支持记录联动设备的请求参数和请求结果日志。

▲支持设置威胁响应处置剧本白名单，加入白名单后，白名单终端不自动执行剧本（提供功能截图，加盖厂商公章）。

投标人需获取厂商承诺，免费提供后续对我区威胁情报来源设备及联动处置设备的兼容适配工作。（提供厂商兼容服务承诺函，加盖厂商公章）

2.6、与现有安全设备及态势感知联动

▲系统中心应支持与区内现有态势感知系统H3C安全威胁发现与运营管理平台联动，提供数据作为威胁情报来源，数据类型包括资产信息和病毒情报；资产信息数据内容包括计算机名、IP、MAC、所属组织、病毒库版本、上一次扫描时间等；病毒情报数据内容包括计算机名、IP、MAC、感染时间、病毒名、病毒类型、病毒文件类型、MD5、发现方式、处置方式、处置结果等（提供投标产品的威胁情报可在H3C态势感知设备上展示的页面截图，加盖投标厂商公章）。

▲系统中心应支持与区内现有态势感知系统H3C安全威胁发现与运营管理平台联动，提供亿级以上病毒特征库数量，作为态势感知系统的威胁检测引擎的云端查询来源（提供投标产品页面上云引擎特征数量的截图以及可以在用户H3C态势感知设备展示的截图，加盖投标产品厂商公章）

▲系统中心应支持与区内现有态势感知系统H3C安全威胁发现与运营管理平台联动，响应态势感知系统的剧本进行终端处置动作；支持同步态感系统的剧本到系统中心作为外部剧本来源，并进行管理及展示，包括剧本名称、类型、来源、执行方式、触发条件、响应动作等（提供投标产品的系统中心可以与用户现有H3C态势感知设备进行剧本同步的展示页面截图，加盖投标产品厂商公章）。

**2.7、报表管理功能**

支持展示系统中心授权信息、终端活跃概况、安装卸载概况、病毒概况、感染病毒TOP10、感染终端、病毒感染走势，并支持导出。

支持展示病毒态势报表，包括感染次数、感染终端、感染病毒种类的Top10排名、病毒感染区分类型统计，至少包括：木马病毒、蠕虫病毒、后门程序、黑客工具、文档病毒、感染型病毒、系统异常项等，并支持导出。

3.支持细粒度展示病毒日志，记录每台终端的病毒感染上报时间、病毒名称、病毒源、病毒MD5、病毒类型、病毒处理状态，并支持导出。

支持展示终端违规外联日志，包括终端名称、IP地址、MAC地址、外联IP、访问域名、外联进程、进程文件MD5等信息。

支持展示终端外联监测日志，包括终端名称、IP地址、MAC地址、外联IP、访问域名等信息。

★提供对“勒索病毒”等具有严重破坏能力的病毒进行专项防御统计，并对统计结果进行呈现的功能（提供功能截图，加盖厂商公章）。

**2.8、客户端工具**

提供对系统启动速度的优化功能，加速系统启动。

提供系统垃圾文件清理功能，提升磁盘空间容量。

提供对系统注册表清理功能，删除无用、冗余的注册表信息。

提供对各类上网、软件等的痕迹功能，保护个人隐私。

支持通过控制台发起对具有图形化界面的国产操作系统的远程桌面连接，至少支持麒麟、统信两种操作系统。（提供功能截图或其他证明材料，加盖厂商公章）

支持弹窗过滤功能，终端上报弹窗信息且管理员通过其信息或可自定义添加规则来过滤第三方恶意弹窗，确保不因流氓弹窗软件影响工作秩序。

▲支持客户端软件商店功能，支持管理员通过系统中心上传常用软件安装程序，构建内部软件库，用户可通过客户端软件商店下载安装，避免因安装不明来源的软件导致的系统故障（提供功能截图，加盖厂商公章）。

**2.9、杀毒软件资质要求**

提供《网络安全专用产品安全检测证书》或《销售许可证》

▲提供计算机病毒防治产品类增强级《网络安全专用产品安全检测报告》并提供国家版权局颁发的《计算机软件著作权登记证书》

**四、实施要求**

**1.安装调试范围：**

1.1、朱家角人民医院的所有内网服务器和医疗终端设备。

1.2、12家社区卫生服务中心（包含分中心）的所有服务器和医疗终端设备。

1.3、所有村卫生室（卫生站）的医疗终端设备。

1.4、卫健委信息中心的区级系统中心及所有服务器和内网终端设备。

1.5、统一安全管理中心的建设

**2.安装调试内容：**

2.1、区信息中心建立统一的安全管理中心及区级系统中心、并提供安全管理服务。

2.2、在上述安装范围内配置指定的杀毒软件。

**3.兼容性要求：**

3.1、提供的安全管理中心服务和杀毒软件必须与现有操作系统兼容。

3.2、现有操作系统包括：windows、统信、麒麟、中科方德。

**4.实施时间：**

4.1、投标人需在签订合同后10个工作日内完成所有的安装调试工作，逾期不能完成采购人有权中止合同。（提供承诺函）

**5.实施过程要求：**

5.1、实施过程中不得对服务器进行重新启动，确保业务连续性。

5.2、实施工作应在医疗机构的非高峰时段进行，以最小化对医生正常诊疗工作的影响。

5.3、实施团队应提前与各医疗机构协调，确定实施计划和时间表。

5.4、项目实施工程中投标人需确保医疗业务不中断，若因投标人项目实施过程中造成医疗业务中断，采购人有权追究投标人责任并终止合同。由此造成的所有损失由投标人承担（提供承诺函）。

**6.安全要求：**

6.1、实施过程中应确保所有敏感数据的安全，不得泄露患者信息。

**7.培训与服务支持：**

7.1、实施完成后，提供必要的培训给IT人员和医务人员，确保他们能够正确使用新的安全管理系统和软件。

7.3、提供一年内的技术支持和维护服务，每周进行一次现场病毒库及补丁升级，确保系统的稳定运行。

7.3、提供应急响应服务，出现问题，5分钟响应，15钟到达现场。

**五、人员要求**

为保证项目顺利实施，投标人在项目实施期间须提供现场不少于15人的项目实施团队，在投标书中提供书面名单，提供项目组成员姓名、其相关资质、在本项目中的职责及以前参与过的项目情况说明等。

由于本项目的服务覆盖青浦区12家社区卫生服中心（含分中心，村卫生室，卫生站点）、朱家角人民医院及区卫健委信息中心，服务范围覆盖整个青浦区行政范围，为满足应对日常网络病毒风险处置的能力，要求投标单位在青浦西片区安排两名，青浦城区、东片区、北片区各安排一名具有相关经验的驻场运维工程师，5名工程师工作时间为5\*8小时驻场，7\*24小时应急响应，为期一年，接受考勤，驻场时间从项目合同签订之日起，投标文件内需提供5位驻场运维工程师名单、身份证、联系方式、相关在职证明以及简要的运维服务经验。

投标人应提供项目经理个人简历和项目团队成员名单，且应提供本地化服务。项目团队成员应具有相应技能证书，项目团队需具有注册信息安全工程师（CISP）证书以及信息安全保障人员认证证书（CISAW）证书。

项目建设期间，项目团队成员应有固定场所，业主方有权要求全部或部分项目成员工作日常驻业主方现场开展工作。

**六、现有安全设备**

本项目现有主要安全设备有：

1. 态势感知区级平台，品牌型号：华三NS-SecCenterCSAP主要功能：支持基于规则引擎对告警接收、过滤、压缩、归并、升级的事件处理流程，并具备基于 AI算法的动态阈值与故障根源定位能力;提供可视化运行态势感知;支持与流程、自动化联动，实现故障派发工单、故障自愈等联动处置能力，实现故障处理的标准化与规范化。
2. 等保一体机，品牌型号：华三NS-SecCenter X6020主要功能：日志审计模块，数据库审计模块，堡垒机模块，漏洞扫描模块。

**七、验收要求**

1、中标方已提供了合同规定的全部货物、和资料。

2、所有点位部署完成且正常在线运行。

**八、其他要求**

1、提供杀毒软件厂商的原厂授权函和原厂服务承诺函

2、提供“5名工程师5\*8小时驻场，7\*24小时应急响应，为期一年，接受考勤”的承诺函

3、投标人在项目投标过程中提供的承诺函及技术参数响应若未能兑现，采购人有权中止合同，投标人需为此承担相应的法律后果

4、投标单位信息系统安全运维服务资质应符合CCRC三级服务资质要求（提供CCRC三级认证证书并加盖投标单位公章）

5、本项目的服务期限为：2025年9月16日至2026年9月15日

6、本项目所需杀毒软件授权数量因业务需求变化，需要增加授权数量在5%以内的由投标单位承担，采购人不再另行支付费用。