杀毒软件三年维保项目需求

杀毒软件三年维保项目——以增强医院安全防护为核心的杀毒软件系统，拟于2025年4月启动招标采购，预算金额53万元。

为制定更加全面、科学、满足医院实际需要的采购需求，并做好招标控制价的核定，现面向社会开展市场调研工作。

本项目需满足的基本需求包括：

一、数据中心服务器深度防护系统扩容升级

（一）统一防护服务平台升级扩容内容：

1.平台内置云主机安全、终端安全等应用中心，支持单独查看每个接入系统的威胁情况；

2.提供在一个页面上从威胁的生命周期（至少包含侦测、分析、响应）角度进行监控；

3.能展示全网已发现威胁、已拦截威胁、潜在威胁、热门威胁的统计数据；

4.提供终端安全事件分析。能对终端安全事件进行聚合，事件记录最少包含事件名称、风险级别、威胁类型、处置动作、告警次数、影响主机数、首次发现时间、最近发现时间、事件来源、事件状态等。能通过文件SHA1、IP地址、域名、URL等维度对终端安全事件进行白名单设置。

5.能结合专门的主机分析产品，从主机、范围两个维度进行溯源分析,并提供溯源分析报告。

6.提供单条或批量手动添加威胁情报，威胁情报维度包括文件SH1、IP地址、域名、URL。

7.能对威胁情报的处置动作进行全局配置，配置的动作包括记录、阻断、隔离.

8.提供从威胁治理生命周期角度提供报表，报告要体现威胁的提交、分析、确认、响应等4个维度。

9.提供对云主机防护系统、终端防护系统等接入系统进行策略统一下发能力，并且能看到策略下发的状态。

10.提供对所管理产品进行状态监控，监控的维度包括CPU使用率、内存使用率、硬盘使用率、在线状态、设备名称、IP地址等。

11.支持邮件告警,提供告警功能，包括字段内容告警、字段聚合告警、消息数量告警和搜索条件数量告警。

（二）数据中心服务器深度防护系统升级扩容内容

1.对现有VMware虚拟环境和传统物理环境的所有服务器提供安全防护服务，满足医院数据中心扩展需求，实现医院数据中心的统一安全管理。

2.具备防恶意程序（AV），支持Web信誉，可以阻止用户访问恶意Web站点。支持完整性监控，实时检测并报告对文件和系统注册表的恶意及意外更改。支持防火墙，减少物理和虚拟服务器的攻击面。具备入侵防御（DPI），在已知漏洞修复之前，屏蔽漏洞以免遭受无限制的入侵。支持日志审查，捕获和分析系统日志，为组织提供审计证据，可以将日志审计配置为将可疑事件转发到安全信息和事件管理系统（SIEM）；

3.提供两种安装部署模式，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，两种模式可以结合使用；无代理部署支持宿主机及虚拟机的防护。

4.提供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SQL Server， Oracle，Postgresql等；

5.提供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；

6.支持对外部沙箱实现集成，同步沙箱的检测结果，检测未知威胁并处理；

7.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；

8.提供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虚拟机，NSX安全标记可与NSX Service Composer一起使用，以自动执行某些任务，例如隔离受感染的VM虚拟机；

9.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；

10.提供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；

11.提供对主机的日志审计，包括收集操作系统、数据库、中间件、Web应用、和应用程序日志，提供日志解码器将各种类型日志进行范式化，支持将事件转至控制平台，做关联性分析、报告和归档，遵循PCI-DSS 10.6规范；

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.提供进行等保三级基线核查，自动识别Windows系统、Linux系统对应核查项；

14.安全服务扫描出的漏洞可以与虚拟补丁进行关联，对于无法打实体补丁的业务主机，可以一键启用对应的虚拟补丁；

二、终端安全防护系统扩容升级

1.对医院内外网PC电脑提供终端安全防护服务，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、更新和部署等服务，并提供主机防火墙、爆发阻止、Web站点信誉服务、预测机器学习、行为监控、勒索病毒防护等服务。

2.提供基于程序行为评估其可信度，并阻止未授权更改；

3.提供多种（不少于五种）扫描引擎，所有防毒引擎必须为自主知识产品非OEM产品；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（锁定）、监控、更名等措施，以保证对于文件多种处理的可选择性；

6.提供多种客户端安装方式,包括但不限与：打包安装、MSI安装、浏览器安装、远程安装、登录脚本安装、UNC安装；

7.提供病毒爆发防御功能。当最新病毒爆发时,可在病毒代码未完成之前自动对企业网络中的病毒传播端口、共享等进行关闭,切断病毒传播途径,预防最新病毒的攻击；

8.提供防勒索软件防护功能，可配置在检测到勒索行为前备份文档；

9.提供根据CVE编号实现虚拟补丁配置功能，支持对Office、Adobe、FTP等应用漏洞进行安全防护；

10.客户端选择云安全扫描和传统病毒码扫描两种运行方式；

11.对插入移动设备内的所有文件进行安全检测；

12.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.组件更新还原功能，支持扫描引擎和病毒码回滚机制；

14.具备将可疑文件提交沙盒设备的联动能力，可自动提交可疑恶意文件，并可接收；

三、提供软件维保3年服务。