**采购需求**

详细技术参数及产品资料、配品配件等：

1、支持物理工作站与服务器操作系统总数不少于1000个点位的3年安全防护授权（验收合格之日起开始计算）。工作站系统平台：Windows XP /Windows 7/Windows 8/Windows 10/ Windows 11（32位与64位）、MAC服务器系统平台:Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2008 R2/Windows Server 2012/Windows Server 2016/Windows Server 2019（64位）；必须支持Linux系统实时防病毒而非通过扫描的方式查杀病毒，即有恶意代码传入Linux系统立即查杀，提供支持Linux系统实时防病毒功能技术截图证明。

2、（1）能够实时监控和清除来自各种途径的病毒、木马、广告软件、勒索病毒、恶意插件、挖矿木马、黑客工具以及风险程序等。

（2）产品自带远程部署工具，便于管理员统一远程部署产品,支持网络自动分发，客户端在线自动升级。

（3）具备丰富的报表功能，展示全网终端健康状态、报警信息；展示全网终端病毒库日期比例，可方便的查看全网终端病毒库的情况能够按照中毒最多终端排名，网内感染新病毒告警定位等。

3、（1）防火墙支持基于应用程序与网络数据流两个级别的防护，能监控应用程序所使用端口，能对进出流量进行端口访问控制设置，可统一进行设置。

（2）具有漏洞利用防御功能，能对操作系统、Office、Oracle、Apache、SQL等常用未及时更新补丁的程序具有防护功能。

（3）主机入侵防御功能，能对类似永恒之蓝、暴力破解、端口扫描等网络攻击流量具有防护功能，防止在院内进行横向传播。

（4）针对共享目录提供专门的保护，防止在本地无病毒的情况，通过客户端对共享文件读写权限加密共享文件。

（5）关键业务服务器可以实现应用程序控制功能，允许启动的程序可以正常启动使用，未经允许的没有启动权限。可设置程序的读写权限，或者对某些关键存储位置只允许某些应用进行读写权限。

（6）产品具有云查杀功能，本地可疑文件可与云端进行查杀比对，提高查杀能力。

4、（1）为减少虚拟化资源的浪费，虚拟化防病毒安装需采用针对虚拟化系统专有安装程序，产品需要支持有代理和无代理两种模式，供用户选择或同时共存。

（2）有代理与无代理更新扫描通过部署在宿主机上的扫描与更新虚拟机进行，避免防病毒风暴、减少虚拟机性能影响。两种模式均支持压缩文件扫描，包含多级嵌套压缩文件，能够做到压缩包清毒。

（3）有代理提供主动防御技术，安全防护能力高于无代理模式，产品具备系统监控主动防御技术，当恶意行为对系统关键区域比如注册表进破坏或修改后，可回滚恶意软件在操作系统上执行的操作，如通过系统监控主动防御技术发现未知勒索病毒进行拦截的同时能够回滚还原被勒索病毒加密破坏的文件。

（4）有代理模式具备反网络攻击虚拟补丁功能，检测和抵御危险的网络活动和网络攻击，支持漏洞入侵防护技术，即系统未修补补丁程序可实现补丁自动热修复无需再安装补丁，并自动将攻击源加入攻击列表；例如在未安装补丁情况下对永恒之蓝攻击进行防御。

（5）有代理模式需要具备防火墙、防病毒、漏洞防护、入侵防御等物理客户端常见功能。

（6）支持与VMware vSphere或NSX集成，提供实时的无代理反恶意程序保护，无需在虚拟机上安装任何安全代理客户端软件，通过专属安全虚拟应用SVA与VMware接口集成进行无代理的安全防护模式，和传统防病毒客户端模式相比，专属安全虚拟应用SVA的无代理防护模式能减少对整个虚拟化资源池硬件资源的消耗。

（7）系统支持对受控主机的操作系统、软件和共享等目录中的文件的保护功能，设定访问、删除、修改权限；系统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。支持自动录屏、截屏等审计功能。

5、（1）要求管理控制中心能够统计网络中被管理客户端的操作系统及所安装软件的漏洞信息，并支持客户端漏洞补丁的下载和安装。

（2）具有病毒日志查询与统计功能，可以随时对网络中病毒发生的情况进行查询统计，能按时间（日、周或任意时间段）、按IP地址、机器名、按病毒名称、病毒类型进行统计查询，能将查询统计结果打印或导出，导出支持XLS、PDF等格式。支持多种事件导出方式联动SOC或SIEM等大数据分析系统平台，支持RFC5424、Splunk（CEF格式）、Arcsight（CEF格式）及QRadar（LEEF格式）。

（3）要求实现统一平台、统一管理和统一流程，管控中心可对传统终端计算机、物理服务器和虚拟化安全产品集中管控，并集中定制物理和虚拟化平台策略配置和报告输出。

6、★为保证兼容性需与院内现有杀毒软件统一管理，配置可以利旧，不用单独再次部署额外控制端，分配额外管理员进行日常维护管理，只需要简单继续安装扩容的授权即可

7、产品具有公安部计算机信息系统安全专用产品的销售许可证；

8、提供≥3年原厂质保。质保期内，提供原厂7\*24小时免费售后服务，免费无限次派工及工时，服务内容包括包退、包换、包修、技术支持、巡检维护、系统优化、软件升级等所有维保相关服务，所有费用包含在合同价款内，除合同价款外，质保期内不再产生其他任何费用；在标的物出现质量问题或甲方要求支持的情况下，供应商及原厂须在1小时内远程响应，4小时内上门服务，12小时内解决问题。提供原厂针对本项目的授权函及售后服务的承诺函。

9、提供本项目所需的软件安装、调试、调优等集成服务。

（五）售后服务条件及交货日期（或工期）：

* + - 1. 质保期内，如标的物经乙方 2 次维修仍不能达到合同约定的质量标准，或标的物经甲方送交具有法定资格条件的质量技术监督机构检测后，如检测结果认定标的物质量不符合合同约定标准的，则视作乙方不能交付标的物而违约，甲方有权退货并追究乙方的违约责任。
			2. 免费售后服务期内，因标的物质量问题导致甲方业务中断超过 2 个小时的，乙方应按合同总价的百分之 一 的款额向甲方支付违约金；超过 8 小时的，乙方应按合同总价的百分之 三 的款额向甲方支付违约金；超过 12 小时的，乙方应按合同总价的百分之 五 的款额向甲方支付违约金。
			3. 免费售后服务期内，乙方未按合同约定履行维保义务的情况发生1次的，乙方应按合同总价的百分之 三 的款额向甲方支付违约金；发生2次的，乙方应按合同总价的百分之 五 的款额向甲方支付违约金；发生3次的，乙方应按合同总价的百分之 十 的款额向甲方支付违约金；乙方偿付的违约金由甲方从质保金中扣除，不足的款额由乙方另向甲方支付。

4.交货期为合同签署后30日内。