**南方医科大学第三附属医院**

**虚拟化平台防毒软件用户需求**

# 项目目标和范围

本次虚拟化安全防病毒软件建设主要针对南方医科大学第三附属医院新虚拟化系统所承载的服务器在虚拟化环境中面临的安全问题风险，依据服务器安全相关标准及行业最佳实践，为主机安全提供安全解决方案，提升整体虚拟化环境的安全防护能力。主要包括防病毒木马防治、恶意文件防护、爆发型威胁主动防御，进一步保障医院业务系统在虚拟化环境的安全性，整体监控虚拟化环境的文件安全态势，管理和维护虚拟化环境的主机系统安全。

# 项目概况及需求清单

1. 项目名称：虚拟化平台防毒软件
2. 交货地点：南方医科大学第三附属医院信息科或采购人指定地点

3.**报价人资格条件**

1. 必须是在中华人民共和国境内注册的具有独立承担民事责任能力的法人或其它组织。
2. 具有本项目相关的其他资质。
3. 所报价产品质量符合国家相关要求。
4. 报价人提供在近三年内商业活动中无违法、违规、违纪、违约行为的书面声明。
5. 本项目不接受联合体报名。
6. 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一项目报价, 一经发现按废标处理并标记为不诚信供应商。

4.服务期限：

本合同自双方签章之日起一年（服务满意可顺延一年，顺延不超过2次）

5.清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **商品名称** | **单位** | **数量** | **参考单价（元）** | **合计（元）** |
| 1 | 虚拟化防毒软件 | 套 | 1 |  |  |

# 技术要求

| **序号** | **参数类型** | **参数要求** |
| --- | --- | --- |
|  | **授权数量** | 提供10颗CPU授权或者70台服务器授权（不限制windows server和linux系统） |
|  | **架构及部署要求** | 控制中心需要支持B/S架构，管理员可只通过浏览器登录控制中心，即可对系统进行管理；终端采取轻代理部署模式。 |
|  | ★**操作系统兼容性** | 支持windows/linux主流操作系统，包括但不限于以下的操作系统：Windows Server 2003 SP2（x86/x64）、Windows Server 2008（x86/x64）、Windows Server 2012、Windows Server 2016、Windows Server 2019；  RedHat 4.3~RedHat 5.11（x86/x64）、RedHat 6.0~RedHat 6.7（x86/x64）、RedHat 7.0~RedHat 7.2 RedHat8.0 ；  CentOS 4.3~CentOS 5.11（x86/x64）、CentOS 6.0~CentOS 6.10（x86/x64）、CentOS 7.0~CentOS 7.6、Centos8.0；  Ubuntu10.0以上；  Suse 10~Suse 10 sp3、Suse 11~Suse 11 sp3、Suse12；中标麒麟、红旗Redflag3~4； |
|  | **产品安全机制** | 客户端具有反逆向、反调试功能、自保护功能，客户端和管理中心通信采用安全的加密机制 |
|  | ★支持自我防护技术，即使客户端被意外关闭，防护依然有效 |
|  | ★**病毒防护** | 支持采用主动的方式进行自动化病毒查杀，可支持Bitdefender、ClamAV、Qowl等多引擎技术识别并查杀最新病毒。 |
|  | 采用管理中心统一查杀模式，对服务器性能几乎无影响。避免本地扫描可能发生的性能风暴问题 |
|  | 查杀引擎对全网服务器进行实时检测，支持勒索，蠕虫，挖矿，木马，后门，黑客工具，僵尸程序等多种类型的病毒检测。 |
|  | 支持提供查看病毒文件静态信息，动态信息查看。 |
|  | 支持病毒文件自动隔离、自动删除、下载、不处理等多种处理方式。支持对特定服务器进行自定义扫描，并可将病毒查杀的结果到处报告 |
|  | **威胁总览** | 支持统计并展示服务器的可疑威胁及告警信息，包括：可疑威胁事件统计、可疑威胁分布、可疑问些趋势，以及具体的威胁事件列表，并可对威胁事件进行研判，还可将威胁事件导出为EXCEL格式的报告 |
|  | **防恶意扫描** | 以攻击者视角、受害者视角展示恶意扫描的事件，包括：服务器名称、负责人、所属部门、操作地址、最近发生时间、受害IP、攻击IP等信息，并可将事件加入黑名单或白名单，还可对受害的IP进行防端口扫描、屏蔽扫描器等设置**（提供产品截图证明并加盖厂商公章）** |
|  | **暴力破解检测** | 对暴力登录系统的账号和IP进行自动发现并上报暴力破解入侵事件，支持对RDP、SSH、FTP等服务的暴力破解行为进行检测拦截，支持设定暴力破解行为的请求范围、失败次数，针对暴力破解的IP支持设定锁定时长。 |
|  | **异常登陆监测** | 以违规登录、可疑登录的视角，对异常登录行为进行监控及告警，包括：登录账号、来源IP、登录区域、服务器IP、操作系统等，并可进行登陆规则的设置，以及告警设置**（提供产品截图证明并加盖厂商公章）** |
|  | **后门检测** | 支持对操作系统、文件、软件中存在的后门进行检测，包括：发现时间、后门名称、后门类型、风险等级、服务器名称、服务器IP、操作系统等，并可进行隔离、删除、加白、下载等操作，并提供后门的详情信息**（提供产品截图证明并加盖厂商公章）** |
|  | **Webshell检测** | 自动识别web服务目录，并实时进行webshell后门的扫描，包括：危险级别、文件路径、文件代销、文件MD5、文件修改时间、webshell发现时间、感染服务器等信息。 |
|  | **反弹shell检测** | 可实时发现反弹shell等危险的反链操作风险，包括：发起连接主机、服务器名称、服务器别名、AgentID、服务器IP、操作系统等信息，并支持事件的上报和阻断。 |
|  | **本地提权监测** | 基于进程运行态权限属性，判断进程是否有提权行为，并对提权行为进行上报。**（提供产品截图证明并加盖厂商公章）** |
|  | **无文件攻击监测** | 可通过无文件攻击检测引擎，对多种系统高危应用进行实时监控，实时监控服务器上发生的无文件攻击事件。及时告警，以便用户快速处置。**（提供产品截图证明并加盖厂商公章）** |
|  | **RCE利用行为分析** | 可基于行为分析，检测对外服务的远程命令执行漏洞利用行为，实现实时告警和追溯。**（提供产品截图证明并加盖厂商公章）** |
|  | **攻击溯源分析** | ▲支持记录当前所有服务器产生的事件日志，并提供筛选的功能和自定义时间段筛选查询，用户可通过安全日志快速锁定问题服务器，并进行相应处理。同时支持对安全事件进行溯源分析，对安全事件的等级、攻击类型、ATT&CK ID、ATT攻击阶段进行匹配。**（提供产品截图证明并加盖厂商公章）** |
|  | **应用防护** | ▲支持应用高级防护的设置，可有效拦截未知WebShell,及时发现网站程序中存在的漏洞并支持Java类Web的防护。包括：未知WebShell实时防护、未知SQL注入漏洞防护、未知上传漏洞防护、Struts2漏洞防护、反序列化漏洞防护、任意文件读取漏洞防护、命令执行漏洞防护等设置**（提供产品截图证明并加盖厂商公章）** |
|  | ▲支持RASP（Runtime Application Self Protection）运行时应用自我保护技术，可对ASP、.Net、PHP、Java四种语言进行RASP防护，通过对应用系统流量、上下文、行为进行持续监控，有效抵御一句话木马、变形/未活动/加密Webshell、SQL注入、命令执行、文件上传、任意文件读写、反序列化、Struts2漏洞等高级Web应用攻击**（提供产品截图证明并加盖厂商公章）** |
|  | ▲支持对应用漏洞防护的设置，可有效拦截各类WEB入侵，包括：SQL注入类、XSS防护、Web服务器溢出攻击防护、文件名解析漏洞防护、禁止浏览畸形文件、自动屏蔽扫描器、X-Forwarded-For防护、请求类型控制、禁止下载特定类型文件、网站浏览实时防护、HTTP请求头防护等。同时可对一句话木马利用工具进行防护，包括：ASP、PHP、ASPX等语言，并可禁止使用PHP://inpu、禁止使用PHP://fillter，以及SVN信息保护设置**（提供产品截图证明并加盖厂商公章）** |
|  | **系统防护加固** | 支持系统内核加固技术，对非法创建文件、非法更改系统设置、非法创建可执行文件、非法提权等恶意行为进行监控和防护。**（提供产品截图证明并加盖厂商公章）** |
|  | ★**文件防篡改** | 支持驱动级防篡改，可以保护整个目录、网页或文件不被恶意修改或者变更，支持监控和控制文件读取、写入、删除、链接、创建、执行、重命名等操作，支持对目录、进程进行例外设置。**（提供产品截图证明并加盖厂商公章）** |
|  | **防端口扫描** | ▲支持检测和防止恶意的端口扫描，并屏蔽扫描器恶意扫描**（提供产品截图证明并加盖厂商公章）** |
|  | **行为管理** | 支持自动学习服务器的网络外连行为、命令执行行为、文件创建行为，并自动进行时序、归化处理**（提供产品截图证明并加盖厂商公章）** |
|  | 支持对服务行为进行状态学习，可添加命令执行、文件创建、网络连接三种服务行为例外的白名单，针对学习行为之外的行为进行告警，支持对行为进行信任、例外操作**（提供产品截图证明并加盖厂商公章）** |
|  | 支持梳理学习主机上的应用运行情况，并进行白名单管理，针对白名单外的应用告警**（提供产品截图证明并加盖厂商公章）** |
|  | **微隔离** | 支持自动学习并梳理出对互联网暴露的服务器端口信息，并提供端口处置**（提供产品截图证明并加盖厂商公章）** |
|  | 支持自动学习并梳理出内网端口访问情况，并提供端口处置**（提供产品截图证明并加盖厂商公章）** |
|  | 支持对端口访问IP地址、IP端、主机进行例外设置**（提供产品截图证明并加盖厂商公章）** |
|  | **外连白名单** | 支持从服务器、进程维度监控分析进程外连情况，外连IP地址及域名，并提供告警**（提供产品截图证明并加盖厂商公章）** |
|  | **风险发现** | 支持服务器系统级、数据库、中间件、应用级的弱口令、口令复用扫描，并可对扫描的结果进行修复验证，还可对口令风险的扫描任务进行设置，包括任务名称、目标服务器、扫描类型、扫描所用字典、执行周期等方式。 |
|  | **软件漏洞检测** | 可对服务器的软件漏洞进行综合扫描，并可对扫描方式、扫描周期进行设置，并以报告的形式展示软件漏洞扫描结果，包括：问题机器TOP5、影响最多漏洞TOP5、漏洞发现趋势等 |
|  | **基线检查** | 可支持等级保护2.0的二级、三级检查、测评、整改的业务检查，系统内置官方等保2.0的二级、三级基线模板，满足等保二级及等保三级要求，同时支持用户自定义基线检查任务。并支持基线检查结果的图形化统计，包括：合规率、问题项TOP5、风险服务器TOP5等维度的统计，并可导出基线检查报告。 |
|  | **防护加固策略模板管理** | 支持对各类加固防护策略存为模板，并进行加固防护策略下发、导入导出等操作。包括：应用的高级防护、应用漏洞防护、应用暴力破解防护、系统文件监控与防护、操作系统加固防护、网络IP黑白名单防护、网络防端口扫描等防护策略。**（提供产品截图证明并加盖厂商公章）** |
|  | 支持批量对客户端的Web应用防护、系统加固、文件防护、网络防护等功能进行启停，支持通过模板的方式快速进行管理和配置下发**（提供产品截图证明并加盖厂商公章）** |
|  | **性能监控** | 支持对服务器主机的CPU利用率、内存使用率、磁盘使用率进行监控，支持展示近1小时、近半天、近1天、近7天、近1个月、近1年的监控数据 |
|  | 支持对自身Agent的CPU利用率、内存使用率进行监控，支持展示近1小时、近半天、近1天、近7天、近1个月、近1年的监控数据 |
|  | **报表生成下载** | 支持各类日志、安全报表、资产报表、事件报表、功能状态报表的综合下载导出，并可根据实际情况对报表内容进行自定义导出 |
|  | **产品后台管理** | 支持展示客户端的安装时间、当前客户端版本、最新客户端版本、启动时间、结束时间、更新状态进行展示 |
|  | 支持批量对客户端的版本进行更新 |
|  | 支持离线安装、命令安装客户端，采用命令安装时支持设置代理地址、默认端口、安装路径、磁盘检测、是否允许覆盖安装等参数 |
|  | **账号管理** | 支持创建子账号，创建账号时支持配置其角色、上级账户、绑定服务器，支持添加归属人、手机号、邮箱、备注等附属信息 |
|  | **主机资产清点** | 支持展示当前服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产数量统计，可对分类资产全局进行快速搜索，保留历史搜索记录并保存搜索条件以进行快捷搜索，同时提供服务器名、IP地址、操作系统、资产类型的筛选搜索；针对搜索结果，支持按资产类型导出 |
|  | 支持展示服务器名称、状态、操作系统、IP地址等基本服务器资产信息，CPU、内存、磁盘、分区等硬件配置信息，负责人、资产级别、联系电话、邮件等运维信息，并提供搜索及导出功能 |
|  | 可从进程和服务器两个维度展示进程的进程名、进程路径、启动用户、启动时间等进程信息，并提供搜索及导出功能 |
|  | 支持从账户和服务器两个维度展示账户的账户名、状态、目录、用户ID、登录时间等账户信息，并提供搜索及导出功能 |
|  | 支持从软件和服务器两个维度展示软件的名称、版本、安装文件路径、配置文件路径等软件应用信息，并提供搜索及导出功能 |
|  | 支持从数据库和服务器两个维度展示数据库的类型、路径、对应端口等数据信息，并提供搜索及导出功能 |
|  | 支持从端口和服务器两个维度展示端口的端口号、绑定ip、端口状态、进程路径等端口信息，并提供搜索及导出功能 |
|  | 支持展示服务器当前的网络连接情况，包括源目的端口、进程、协议等网络连接信息，并提供搜索及导出功能 |
|  | 支持从资产模式和服务器两个维度，展示启动的服务名、启动状态、服务描述、脚本路径、启动类型、文件公司名、文件MD5等信息，并提供搜索及导出功能 |
|  | 支持从安装包和服务器两个维度展示安装包的版本号、安装路径、程序大小、安装时间等安装包信息，并提供搜索及导出功能 |
|  | **主机资产发现** | 支持对局域网内服务器的服务器进行扫描，并自动获取服务器相关信息，包括服务器名、在线状态、别名、主机IP、AgentID、分组标签、操作系统、IPv4、IPv6、负责人、所属部门等信息，可通过自动、手动的进行资产发现的任务设置。 |
|  | **资质要求** | 产品拥有自主知识产权，非OEM、代理销售产品，具有国家版权局颁发的“计算机软件著作权登记证书” |
|  | 产品拥有公安部颁发的“主机文件监测（基本级）”安全专用销售许可证 |

# 四、服务要求

**1.实施服务要求**

供应商须保证所提供的产品包括相关附件为相应厂家原装正品，软件产品为相关厂家正版软件，符合国家有关规定。供应商须保证所提供产品具有合法的版权或使用权，本项目采购的产品，如在本项目范围内使用过程中出现版权或使用权纠纷，应由供应商负责。

**2.售后服务要求**

（1）软件免费保修期不少于1年。软件系统在免费保修期内，原有软件模块功能均享受免费升级服务。

（2）软件出现故障影响使用时，应1小时以内电话响应并远程处理，24小时以内到现场处理。

**3.培训要求**

（1）供应商应提供包括本项目顺利实施的所有培训服务，保证医院人员的使用与日常维护工作。所有的培训费用应计入本次服务总价。

（2）培训内容与课程要求：

提供信息管理系统操作、使用和维护培训；