招标编号：NTEYZBGG2018003

南通市第二人民医院

终端安全管理系统需求文件

1. 项目名称：终端安全管理系统
2. 项目预算：9万元
3. 付款方式：软件安装培训调试验收完毕，凭验收报告付款90%，余款一年内付清
4. 项目概况：含400个终端及控制中心所有功能一年的升级费用，提供技术支持。一年后的年升级费用将作为续签升级费用合同的价格依据。
5. 参数技术要求：

|  |  |  |
| --- | --- | --- |
| **指标项** | | **指标要求** |
| 系统管理 | | 控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能； |
| 客户端提供控制中心管理所需的相关数据信息，通讯可选择非明文方式； 客户端执行最终的木马病毒查杀、漏洞修复等安全操作； |
| 产品支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行； 要求客户端程序具备自保功能，避免被恶意篡改 |
| 支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告； |
| 支持自定义默认分组的终端默认功能模块,包括产品功能模块及实用工具等； |
| 支持加密的控制中心远程访问，支持管理账户并发、密码有效期、鉴别失败锁定等设置； |
| 支持设置日志上报的带宽限制； |
| 支持根据分组、计算机名称、IP地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理； |
| 支持控制中心迁移、数据备份、数据恢复； 支持多升级服务器； |
| 资产管理 | | 按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控CPU温度、硬盘温度和主板温度 |
| 支持终端软、硬件变更审计，资产清单报表； |
| 支持统计指定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率 |
| 支持自动发现设备的IP-MAC地址的绑定（提供产品界面截图） |
| 支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件（提供产品界面截图） |
| 支持正版软件的正版序列号的读取功能，确保软件正版化。（提供功能截图证明） |
| 日志报表 | | 展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表； 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 |
| 展示指定时间段内指定终端修复漏洞，病毒查杀，木马查杀的情况 |
| 要求支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人。邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等 |
| 提供系统升级、热备、管理员操作、管理员远程等系统日志； |
| 设备联动 | | 支持与旁路威胁检测系统设备、NGFW、上网行为管理、VPN产品联动，达到网关边界联动防御效果（提供产品界面截图） |
| 终端授权 | | 配置不少于400个点终端PC杀毒功能授权、补丁管理功能授权、运维管控功能授权 |
| 病毒、恶意代码、木马防护 | 内存防护 | 支持内存实时监控查毒，能够自动隔离感染而暂时无法修复的文件； |
| 启动防护 | 支持抢先加载防毒，在系统未加载前启动文件监控，通常情况下不必重启到安全模式也能清除病毒； |
| 注册表、引导区防护 | 支持文件、引导区、内存、注册表、服务、进程、进出文件、目录、压缩文件、网页等恶意代码、恶意样本查杀 |
| 电子邮件防护 | 支持电子邮件内文件检测，可清除隐藏于电子邮件计算机病毒和恶性程序； |
| 网页安全防护 | 能够对网页提供安全防护，发现网页中的危险行为实时阻断；能够对网页挂马进行拦截，能够自动拦截网页中的钓鱼、欺诈信息； |
| 网络安全防护 | 拦截下载器自动下载木马程序、恶意推广程序、盗号木马；  拦截黑客远程控制本机； |
| 嵌入式防御 | 支持用户添加嵌入杀毒的应用程序；支持FlashGet、NetAnts、WinZip、WellGet、WinRAR等工具的嵌入式杀毒功能； |
| 移动设备病毒防护 | 要求提供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； |
| 局域网共享查杀 | 能够对局域网共享文件传输进行检测和查杀； |
| 浏览器防护 | 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（提供功能截图证明） |
| 聊天安全防护 | 检测QQ、MSN、阿里旺旺等常用聊天软件传输文件的安全性，确保传输文件不中毒；  检测QQ、YY、飞信等聊天软件中对方发来网址的安全性  聊天软件传输某些文件会添加“.重命名”，如果文件安全，将自动去除“.重命名” |
| 输入法防护 | 要求可以拦截伪装成输入法程序的木马；  要求拦截利用输入法启动的木马程序 |
| 文件传输防护 | 支持U盘等移动磁盘设备和电脑硬盘间文件传输检测；  支持局域网共享文件传输检测； |
| 攻击防护 | 能够实时检测和拦截攻击行为，包括改写系统关键文件、修改注册表关键键值、感染移动存储介质、创建系统账号 |
| 云修复 | 支持扫描发现文件遭破坏或被感染时触发修复流程，修复通过公有云下载正常文件替换遭破坏的文件； |
| 定时查杀 | 要求能够自定义时间、自定义扫描频率，自定义扫描类型，对终端进行定时查毒，并且可以自定义查杀病毒后的处理方式自定义； |
| 黑白名单例外 | 支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件；  支持手工导入MD5+SHA1的黑白名单方式，支持txt批量导入方式；  文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件；（提供功能截图证明）  支持下发忽略白名单的病毒扫描；  支持对windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理; |
| 病毒查杀统计 | 要求支持通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件；（提供功能截图证明） |
| 支持按病毒、木马、终端等维度统计全网病毒感染状况； |
| 要求支持对网内未知文件云查询的控制，可以选择直接连接互联网云查询中心查询，也可以选择采用私有云查杀引擎完成未知文件查询； |
| 要求上报文件至少包括:文件名称、发现时间、鉴定结果、文件大小、数字签名和文件所属源计算机等信息 |
| 压缩包杀毒 | 要求支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力；  可对压缩包层级设置以节省终端计算资源； |
| 备份区隔离区管理 | 可对备份区、隔离区的文件进行有效管理。能够对单个、指定的文件和全部文件，进行文件的删除、恢复等多项管理措施。 |
| 敲诈者病毒防御 | 对敲诈者病毒提供防护机制，同时可提供相关解密工具，解密工具为自主研发；（提供功能截图证明） |
| 多杀毒引擎 | 要求产品具备本地多引擎查杀能力，且引擎可配置；（提供功能截图证明） |
| 病毒库升级管理 | 要求支持服务器端病毒库的定时更新和手动更新两种升级模式。 |
| 要求支持客户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽。（提供功能截图证明） |
| 补丁分发与漏洞修复 | | 要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型； |
| 支持漏洞修复影响文档编辑时提醒功能； |
| 支持补丁下载安装顺序设置，可以有效节省漏洞修复时间与减少CPU占用； |
| 支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃； |
| 终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁（要求提供截图）； |
| ★产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能（要求提供截图） |
| 产品具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端P2P补丁分发加速，有效节省外网带宽资源（要求提供截图） |
| 要求产品生产公司具备热补丁修复功能（至少需要8个以上为用户提供Windows漏洞修复的热补丁列表） |
| 运维管控 | | 可远程协助终端（不依赖Windows远程桌面协议）、远程关机、重启终端； 支持远程操作时锁定屏幕、截取屏幕，远程锁定屏幕后需要输入解锁密码才可再次使用； |
| 可监控指定终端网络、应用程序的上传，下载速度与流量； |
| ★支持冗余有线网卡、无线网卡、3G网卡、MODEM、ADSL、ISDN等设备的外联控制； 违规外联发生时可针对内外网连接状态分别设置违规处理措施 |
| 支持终端进程红名单、黑名单、白名单功能，可设置核心进程必须运行，也可保护核心进程不被结束。 |
| 支持网址白名单，通过信任网址白名单可以管理企业网络内信任的网址，加入信任后终端不再将此网址视为威胁 支持网址黑名单，可设置终端不能访问的网址URL，终端访问这些URL时会被拦截，并展示拦截记录 |
| ★支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限 |
| 支持对终端桌面系统的账号密码、本地安全策略、控制面板、屏保与壁纸、浏览器安全、杀毒软件检查，支持对终端消息发送 |
| 终端支持在线、离线策略，可同时使用在线或离线两种状态，保证终端安全运行；  支持按照域名、操作系统、WIFI SSID等条件匹配预先设定好的场景策略； 支持LDAP账号的终端用户策略模式； |
| 资质要求 | | 具备销售许可证  具备软件著作权  中国信息安全测评中心信息技术产品安全测评证书 EAL 2  以上证书要求提供相关证书或者证明复印件 |
| 其他要求 | | 提供原厂一年质保服务，提供原厂质保函；提供原厂针对该项目的授权书  中标人在中标后15个工作日内需提供测试，并进行所承诺的所有功能测试，提供测试报告，如经测试发现与标书要求或投标文件不一致或投标单位有意拖延测试，则视为欺诈行为，招标人将不授予合同，投标单位将承担一切后果与责任 |

**开标一览表**

投标公司全称（加盖公章）：

业务员： 联系电话：

|  |  |  |  |
| --- | --- | --- | --- |
| 招标编号 | | NTEYZBGG2018003 | |
| 项目名称 | | 主要服务内容 | |
| 终端安全管理系统 | | 含400个终端防护、管控及控制中心，一年的升级费用 | |
| 投标总价 | 大写： | | |
| 终端防护每年升级费用合计  （含病毒库更新、程序更新、漏洞修复等病毒、木马查杀所有功能） | | | 元/年 |
| 终端管控每年升级费用合计  （含所有终端管控的功能） | | | 元/年 |
| 其他优惠条件 |  | | |
| 备注 |  | | |

投标日期： 年 月 日