# 办公网杀毒软件版本与特征库升级服务参数

1. 商务要求
2. ▲提供终端杀毒软件500授权点位和3年软件版本及特征库免费升级服务。
3. 要求兼容现有安全管理中心，要求新增授权统一归安全管理中心管理。

3.要求具备《国家计算机病毒应急处理中心检测报告》

4.要求具备《计算机软件著作权登记证书》

5.要求具备《计算机信息系统安全专用产品销售许可证》

1. 技术参数

1.▲需具备终端发现可以通过扫描发现需要安装但没有安装终端的计算机功能，以免出现漏管漏控的情况。

2.要求中心具备容灾备份功能，当主中心计算机遭受如宕机、断电、硬件/软件故障等意外情况或人为操作错误导致主中心计算机无法正常使用时，备用中心将顶替宕机的主中心且同步数据。

3.需提供备用中心查看和审批，支持通过本地安装的配置工具申请成为主中心的备用中心，主中心审批通过后，显示备用中心的相关信息。

4.要求支持邮件预警功能，当全网发现病毒事件、网络攻击事件、超过一周未更新时发送邮件通知。

5.要求支持备份终端信息,分组及规则,防护策略,事件日志,管理员信息,系统设置；支持自动备份，按照月/周/时间设置自动备份。

6.需具备按全网终端迁移或部分终端迁移功能，当网络环境发生变化或物理设备出现故障时可转移终端。

7.需具备可对终端添加多个中心地址功能,当终端接入网络环境时,中心可对终端实施管控。

8.需提供第三方软件调用API接口，包括调用漏洞修复信息查看、下发查杀任务、查看、创建、修改和删除分组信息、查询终端详情、终端资产信息、调用接口修改终端名称等。

9.要求中心可统计全网操作系统版本信息、安装时间、激活状态且具有操作系统占比可视化数据图；可统计全网终端硬件信息包括CPU、内存、硬盘、硬盘序列号、硬盘ID、网卡、显卡、主板、主机序列号、显示器且支持硬件清单导出、支持全网终端硬件、软件变更历史记录包括变更时间等其他信息。

10.须具备热补丁机制，利用产品自身防御功能，防护其他软件以及系统出现的漏洞，阻止对计算机造成损害与入侵.

11.▲要求具备反病毒底层技术，反病毒引擎为本地反病毒引擎，不依赖云（联网时的病毒查杀能力与断网时的病毒查杀能力一致）具有轻量级的病毒库，却有较强的病毒查杀能力；要求支持勒索病毒诱捕，可在根目录生成txt、pem、sql、xlsx、mdb、jpg、rtf、xls、doc、docx等格式的诱捕文件，当出现勒索行为，对其进行捕获并进行隔离。

12.要求具备恶意行为监控功能，通过监控程序运行过程中是否存在恶意操作来判断程序是否安全，从而可以作为传统特征查杀的补充，极大提升电脑反病毒能力。

13.要求具备暴破攻击防护能力，阻止黑客通过SMBv1、SMBv2、 RPC、SQLServer、PDP协议进行暴力破解攻击

14.▲要求具备横向渗透防护功能，防护内网中已中毒机器感染其他主机，阻止横向传播、病毒以及木马的扩散防护项包括默认共享访问、远程服务创建、远程计划任务创建、远程注册表篡改、远程MMC调用、远程DCOM调用、远程WMI调用有效阻止病毒横向渗透；支持系统加固，针对病毒会利用或修改的系统脆弱点，设置相应的防护规则，有效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，针对病毒特殊行为进行免疫等。

15.要求具备应用加固功能，通过对容易被恶意代码攻击的软件进行行为限制，防止这些软件被恶意代码利用

16.要求具备外设申请功能，管理员可审批终端用户的外设使用申请，支持设备截止时间设置，并支持信任设备列表和审批记录筛选搜索；

17.要求支持软件禁用功能，可以设置使用违规软件的处理方式，包括记录、提示卸载以及隔离，可添加软件黑白名单，设置软件是否可用；

18.▲要求具备违规外联设置探测功能，探测终端用户是否有违规连接外部网络的行为；要求具有终端动态口令验证功能，当终端用户登录计算机时都将弹出动态口令安全认证窗口，若用户设置了计算机密码，该弹窗将在用户输入正确的账户密码后弹出用户需再次输入正确的动态口令才可登入计算机且可设置应用范围：远程登录时启用或本地登录时启用。

19.终端应具有弹窗拦截工具，具备自动拦截方式，手动截图拦截方式，可拦截流氓、广告、以及恶意弹窗等

20.应具有导出安全分析报告功能，对当前中心进行安全状况分析并生成分析报告，可按照最近7天、最近30天、最近一年等时间范围生成报告，也可自定义时间范围生成报告；安全报告支持邮件订阅功能，可给管理员配置订阅功能。

1. 其他要求

1.项目验收

（1）实施完毕后，由信息网络中心组织验收。

（2）验收时服务商单位必须派代表在场，验收合格后，由服务商单位签署检验合格证书。

2.售后服务要求

软件运行期间，应提供电话、电子邮件等多种方式的技术咨询服务。公司应提供 7\*24 小时全天候服务技术服务支持，节假日有备班人员随时响应。包含远程技术支持和现场技术支持两种方式。

3.培训要求

服务商要求根据医院实际需要提供多种培训方式，对各类人员提供适当的培训内容。要求达到用户能够独立操作使用本该杀毒软件。

4.服务期内配合甲方定期开展网络安全自查，自查内容至少包括系统日常运行情况、系统漏洞等；配合甲方定期进行安全审计，审计内容至少包括系统账号、权限、操作行为和安全技术措施有效性等，及时发现和处理信息系统运行过程中的安全隐患，减少或避免网络安全事件的发生。