### **杀毒软件技术参数要求**：

|  |  |  |
| --- | --- | --- |
| 序号 | 指标 | 参数 |
| 1 | 产品资质 | 软件著作权，必须具有中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》； |
| 2 | 安装环境要求 | 工作站系统平台：Windows XP/Windows Vista/Windows 7/Windows 8/Windows 10（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 Server2019（32位与64位）  Linux系统平台：SUSE Linux/Red Hat Linux/CentOS/Ubuntu/中标麒麟Linux等  移动设备：Android、IOS |
| 3 | 产品功能 | （1）杀毒市场知名品牌，三年版本、病毒库和版本免费升级。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、隐蔽软件、黑客工具以及风险程序等。  （2）本次要求配置支持200个工作站、服务器用户授权。  （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 |
| 4 | 管理中心功能 | （1）c/s架构和B/S架构集于一体，支持多级管理控制中心（系统中心），对多级管理控制中心能统一集中管理，至少支持5级以上管理。能够统一升级，统一管理。管理端应支持对虚拟化客户端与实体机客户端的统一管理，管理中心可对客户端进行远程操作，集中定制管理策略和报告输出。  （2）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。  （3）实现统一平台、统一管理和统一流程，考虑到未来云计算平台的搭建和应用，原厂商须具备虚拟化安全的解决方案，且管控中心能够管理包括物理（Windows、Linux、Mac OS等操作系统）、移动（Android、IOS等操作系统）和虚拟化（VMware、Citrix、Hyper-V、KVM）在内的所有安全产品，并集中定制物理、移动和虚拟化的策略配置和报告输出。 |
| 5 | 反病毒数据库更新能力 | （1）本地反病毒数据库条数达到1000万条以上。  （2）要求有快速的反应能力，反病毒数据库应至少每天进行一次有效升级。  （3）具备机器学习技术，实现处理更多未知复杂恶意程序和拦截未知的针对性攻击行为并确保最低的误报率，机器学习模型提供了基于决策组合的恶意实体的预执行检测，从观察、启发分析到精确定位，提供深层次安全防护策略  （4）杀毒软件须拥有回滚数据库功能。在遇到不可抗力等意外情况下，病毒数据库损坏时，可以成功恢复上一次完成更新时的状态，保证反病毒软件正常运作。 |
| 6 | 客户端功能模块 | （1）文件反病毒－具有增量扫描技术，优化扫描速度；  （2）云安全－产品具备云技术，并能够在相应的界面看到相关的数据信息。  （3）邮件反病毒－扫描 POP3，IMAP，MAPI ，POP3和 NNTP 等协议流量；包含附件过滤功能；  （4）网页反病毒－实时扫描 HTTP 协议流量，防御有害脚本和程序；对浏览中遇到的URL地址进行反钓鱼网站检测和可疑链接检测，可自定义添加信任URL。  （5）系统监控－具备本地主动防御技术，当恶意行为对系统文件、注册表等破坏或修改后，可回滚病毒在操作系统上执行的恶意操作，通过主动防御技术发现未知勒索病毒进行即刻拦截，同时能够立即还原被勒索病毒加密的文件。  （6）防火墙－支持网络数据包规则的防火墙功能，通过建立防火墙策略规则对特定端口选定数据协议发送和接收网络流量，支持根据应用程序建立网络访问规则，对特定应用程序的网络活动评估和限制，阻止不合法的应用程序网络连接。  （7）反网络攻击-具备主机IPS功能，检测和抵御危险的网络活动和网络攻击，并自动将攻击源加入攻击列表，针对永恒之蓝等网络攻击型病毒，可查看和定位攻击源，便于管理员快速定位及时处理，提供产品功能截图；  （8）应用程序控制- 根据终端应用程序的启动和使用权限进行细致的控制。通过不同组和组策略的制定，确保灵活和有保证的安全设置  （9）网页控制－可以对网内用户访问网站进行有效控制，可以根据访问网页内容（视频，音频，图片等）、访问网页类型（网上购物、社交网站、在线邮箱等）、访问网页时间以及访问网址进行详细的定义，并且可以对不同的计算机账户进行权限的设置。  （10）对威胁的发展进行审查和分析，并向安全员或管理员提供有关潜在攻击的信息，以便及时响应威胁。通过记录终端与网络事件（大量端点级系统的行为与相关事件，譬如用户、文件、进程、注册表、内存和网络事件），结合已知的入侵指标 (Indicators of Compromise，IOC)、行为分析和机器学习技术来监测任何可能的安全问题，识别信息泄露（包括内部威胁）的风险，并对这些安全威胁做出快速响应。 |
| 7 | 技术支持 | 生产厂商提供24小时×365天的技术支持，具备400技术支持电话。生产厂商应具有在河南本地的服务中心，在国内具备病毒处理中心，能够根据中国地区的新病毒以及全球性病毒，并基于云查杀在最短15分钟内做出响应，并更新反病毒数据库。 |
| 8 | 维保服务 | 提供叁年软件版本及特征库免费升级服务。 |