## 业务网杀毒软件版本与特征库升级服务参数

1. 商务要求

1.▲提供防病毒系统终端授权点位1800点和3年软件版本及特征库免费升级服务。

2.授权需兼容现有已部署终端杀毒软件及管理控制台。

3.需具有公安部计算机病毒防治产品检验中心检验报告。

4.需具有国家计算机病毒应急处理中心计算机病毒防治产品检验实验室颁发的《网络安全专用产品安全检测证书》。

1. 部署要求

1.产品授权应支持各类Windows 32/64位操作系统(Windows XP、Windows 7、Windows 8、Windows 10、Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016等）、Linux系统等。

2.需支持多种安装方式，至少包括下载安装、远程安装、共享安装、Web安装、脚本登录安装和域组策略安装，支持通过管理控制台方式进行远程安装，支持通过WEB方式进行远程安装。

3.▲在同一个控制台下面一个产品授权要求同时支持Windows、Linux、Mac、IOS、Android等操作系统。

4.需能够自动识别服务器或桌面系统，提供不同的防护功能。

5.必须具备从本地或管理端检测和卸载不兼容软件功能，以避免系统冲突。

1. 技术参数

1.具备实时监控病毒、木马、广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等功能。

2.要求具备文件、邮件、即时通讯和网页的反病毒功能模块，必须支持Linux系统实时防病毒功能，即有病毒传入系统立即拦截。

3.▲要求具备勒索病毒加密回滚还原功能。通过主动防御技术拦截未知威胁并且当前时间还原已被加密的文件。

4.▲要求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。

5.▲需具备漏洞曝露阻挡，自动漏洞利用防护功能。

6.▲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。

7.要求具备压缩文件扫描，包含多级嵌套压缩文件，需提供压缩包内清毒，加密压缩文件扫描功能。

8.▲产品必须具备iSwift或类似扫描技术，只扫描新建和被修改的文件，减少扫描时间和资源占用。

9.▲要求具备云安全网络技术，产品需提供云辅助技术用以提高对未知病毒的响应速度并减少误报，抵御零日漏洞攻击。

10.需具备主动防御技术，主动防御使用BSS行为流特征码，在检测到恶意软件活动时可选择操作。

11.需具备扫描内存和正在运行的文件功能，能够扫描和清除内存和文件中病毒和蠕虫。

12.应能够监控和阻止应用程序的异常行为。如Office应用程序的活动，windows management instrument的使用，脚本引擎和框架的活动等。

13.需具备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。

14.应能够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。

15.▲必须具备反网络攻击功能，检测到攻击时能够将攻击计算机加入到阻止计算机列表，可自定义阻止的时间。

16.▲必须具备反网络攻击功能，检测到攻击时能够将攻击计算机加入到阻止计算机列表，可自定义阻止的时间。

17.▲可以设置终端应用程序的黑、白名单（仅允许白名单中的程序运行）。黑、白名单控制是否可以基于文件指纹方式（HASH等）进行控制。

18.▲需具备移动存储介质控制功能，如控制U盘、移动硬盘、手机等设备接入终端，避免移动介质传播病毒的风险，需具备外接设备认证功能，即特定的U盘可以使用其他则不可以。

19.▲需具备根因分析：威胁传播图表可显示受影响或警报中涉及的关键过程、网络连接、动态链接库 (DLL) 和注册表配置单元。

20.▲所有检测都在图表上予以突出显示，从而为分析师提供事件的完整背景，并有助于揭示受影响的组件。

21.▲应具有发现和限制对云资源的不适当或未经授权的使用，以及浪费在社交网络和聊天工具上的时间。

22.▲被检测的每项云服务都有一个评分，指示使用该服务的风险等级。

23.▲应提供IOS和Android等移动设备安全防护功能，检测并清除移动设备上的威胁。 实时保护设备免受威胁、病毒和其他恶意应用程序的攻击。

24.▲应提供禁止在设备上使用摄像头、蓝牙和 Wi-Fi 模块功能，以最大限度地降低敏感数据泄露的风险，并能够在安卓设备上配置与企业 Wi-Fi 网络的自动连接。

25.▲需提供基于云和本地的两种管理控制台

26.▲本地控制台应具备集中管控中心功能，需支持统一平台、统一管理和统一流程，原厂商须具备虚拟化系统安全解决方案，且集中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、OpenStack）在内的所有终端防护产品，并集中定制物理、移动系统和虚拟化系统的策略配置和报告输出。

27.▲管理控制中心统一收集漏洞信息，须支持按漏洞优先级为全部或单个客户端进行修复。

28.漏洞评估：需提供安装在终端设备上的应用程序概述，以及将这些应用程序更新为最新版本的可用补丁列表。

29.▲应具有减少网络负载功能，管理控制中心可针对IP子网或者IP段进行数据传输速度的控制，通过建立相关配置规则，可对最大传输速率和时间等参数进行定义。

30.应具有相关报表功能，包括：保护状态、感染最严重的情况、客户端被网络攻击的情况、终端产品版本和病毒库版本等。

31.可以建立自动迁移规则，客户端根据条件自动分组，包括IP地址段，计算机名、操作系统类型、代理状态、虚拟机类型、已安装应用程序等。

1. 其他要求

1.项目管理

服务商需提供完善的项目管理方案，包含但不限于实施进度表、项目组织结构、项目质量控制等。

2.成员组成

（1）实施工程师：1人，要求具备同类项目管理工作经验，并报院方认可。

（2）项目开发人员：具备同类项目实施经验。

3.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。

4.售后服务要求

服务期间，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。

5.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系统的目标。

6.安全要求

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。