附件

终端安全及防病毒服务采购项目

技术、服务、商务要求

一、技术/服务要求

（一）技术要求

1.网络版主机安全管理系统，配置管理中心≥1套，实现对终端的统一管理和策略下发，服务器终端操作系统授权10个，PC终端操作系统授权200个，提供3年病毒库、规则库和特征库升级服务；

2.具备系统漏洞扫描、补丁修复管理、广告弹窗拦截、主动防御、安全策略管理等安全管理功能；（提供功能截图证明材料并加盖供应商鲜章）

3.支持反病毒底层技术，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）。支持对资产进行快速扫描、全盘扫描、自定义扫描，具备病毒查杀、自定义病毒处理方式、感染文件修复等安全管理功能。（提供功能截图证明材料并加盖供应商鲜章）

4.支持Windows server 2003、Windows server 2008、Windows server 2012、Windows server 2016、Windows server 2022、Win 7、Win 8、Win 10、Win 11、Centos 5.0 +、Redhat5.0 +、Suse11 +、Ubuntu 14 +等操作系统；

5.支持监控系统CPU使用率、内存占用率、磁盘读写以及上下行流量，对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警；（提供功能截图证明材料并加盖供应商鲜章）

6.支持病毒库、Windows补丁库的离线升级及在线升级；支持管理平台、终端软件安装包、终端软件更新包、系统漏洞库的离线升级。可自定义客户端升级时间与升级速度，并支持错峰升级。

7.支持黑、白名单双模式，白名单模式可配置是否允许访问特定的网站和地址；黑名单模式可自定义恶意IP，支持黑名单告警和阻断；（提供功能截图证明材料并加盖供应商鲜章）

8.针对未知勒索病毒的诱饵防护引擎，诱捕未知勒索病毒的攻击，并进行实时阻断。支持在不依赖文件扫描的情况下，支持对主流的勒索家族病毒进程进行感知和拦截。（提供功能截图证明材料并加盖供应商鲜章）

9.管理平台支持设置客户端卸载密码、卸载监控端、解除绑定、停止/启动防护、关闭/重启主机、重启客户端、迁移资产；（提供功能截图证明材料并加盖供应商鲜章）

10.支持违规外联检测，实时感知违规外联行为，针对违规外联行为支持多种处置方式，包括不做处理、弹窗提醒用户并关机、弹窗提醒用户并断网；（提供功能截图证明材料并加盖供应商鲜章）

11.支持展示当前待处理的高危风险信息包括弱口令、待处理病毒、待处理漏洞数据。支持控制台动态更新显示全网终端安全状态分布，包括：终端总数、在线终端数、防护中终端数、异常设备数。支持查看当前安全防护信息数据，包括勒索深度防护、病毒实时防护、系统登录防护、Web应用防护；（提供功能截图证明材料并加盖供应商鲜章）

12.支持资产信息登记，资产主动发现等功能，针对未完整登记信息的终端支持设置提醒；（提供功能截图证明材料并加盖供应商鲜章）

13.支持管理员远程控制终端，处理终端及系统使用问题，并支持设置自动应答与需要终端用户相应两种模式。（提供功能截图证明材料并加盖供应商鲜章）

14.支持对终端的USB接口、串口/并口等接口的控制。（提供功能截图证明材料并加盖供应商鲜章）

15.支持对无线网卡、光驱、打印机、摄像头、鼠标、键盘等的权限管理。（提供功能截图证明材料并加盖供应商鲜章）

（二）服务要求

1、对于新发现的病毒、零日漏洞，厂商能够于24小时内作出响应，及时通知采购人，并提供专门应急预案、处置工具或专杀工具。

2、支持7\*24小时威胁溯源服务。

3、提供7\*8小时产品售后服务。

（三）履约能力要求

1.投标供应商若为代理商，须提供产品制造厂商关于本项目的项目授权函、3年原厂售后服务承诺书。

2.供应商提供2020年以来实施的与本项目相同产品的至少2家三甲综合医院项目业绩证明。（医疗行业具有特殊性，医院信息系统、接口种类繁多，服务器操作系统也具有多样性，所以需要相关产品具有较好的兼容性，有较多医院的案例。）

二、商务要求

1.交货时间：2023年8月1日

2.交货地点：四川省第五人民医院

3.付款方式：项目合同完成签订且成交供应商提供正规有效发票后30日内，采购人支付合同总金额的40%；产品部署完成并经医院验收小组验收合格后，由成交供应商提供正规有效票后30日内，采购人支付项目总金额的60%。

4.验收标准：相关产品部署完成后，医院验收小组根据询价文件技术、服务和商务要求和供应商响应文件进行验收。

5.其他商务要求

5.1对采购人员进行免费操作培训。

5.2提供产品免费安装调试。