**内外网桌面安全管理系统需求**

|  |
| --- |
| 1. **性能要求**

1、控制中心采用B/S,客户端采用C/S部署方式，必须拥有自主知识产权的产品；2、支持全院内网6000个终端、外网3000个终端的桌面安全管理（内外网分开）；3、每个平台至少可管理300个Vlan；4、用户组和角色数要求大于1000个；5、客户端安装包轻量化，运行时少占内存、CPU资源； |
| 1. **功能要求**
 |
| 1、终端管理 | 1、全院内、外网终端分开隔离部署，各自独立统一管理；2、支持按VLAN，策略，区域、类型灵活分组，支持新终端自动发现，支持智能分类、分组；3、能采集终端的硬件、操作系统、安装应用程序、注册表、网络配置、系统日志、进程与服务等详细信息；4、可视化显示终端列表信息，支持多种条件模糊搜索；5、终端能兼容Windows XP、7、8、10、11，winServer 2003-2022，Linux，IOS，Android及国内主流国产机等版本的操作系统； |
| 2、用户管理 | 1、平台支持三权管理，且登录认证及密码管理需满足等保三级要求；2、权限细颗粒化管理、可根据不同用户（组）、角色分配不同的管理权限；3、支持双因子认证功能，除用户名密码认证外，其他认证不限于短信验证码、微信（限外网）、Ukey等技术； |
| 3、策略管理 | 1、安全策略应包含但不限于：双网卡（多网卡）、违规外联、外设管理、杀毒软件检测、补丁管理、文件监控、IP/MAC地址绑定、防火墙管理、密码强度管理等；2、行为策略应包含但不限于：触发特定条件录屏、定时截屏、网站访问管理、软件安装卸载监控（黑白名单）、打印刻录监控、访问范围管理、开关机监控，网络配置监控、流量监控等；3、支持专机策略，针对自助机、连接检查检验仪器的特殊终端能单独管理；4、时间段设置，对特定终端能设置限时段访问资源； |
| 4、运维管理 | 1、支持一键全网（或者自定义范围）立即（或者自定义时段）下发消息；2、支持一键全网（或者自定义范围）立即（或者自定义时段）下发文件或者静默安装软件、补丁；3、支持快速对终端高分辨率的远程监视/远程操作，远程时可自控开启/关闭共享粘贴板内容；4、支持对客户端一键远程开机、关机、重启、注销；5、支持批量远程修改客户端的计算机名、网络配置、主题、屏保、系统时间、默认浏览器、电源管理等配置信息；6、支持查看系统资源、磁盘使用状态、端口状态、运行服务、网络共享、打印任务等信息；7、支持对终端远程文件管理，后台无感传输文件；8、针对严重违规或者威胁终端可支持一键锁住（隔离）终端、使之断网并无法操作终端；9、支持在终端或者平台上一键关停（退出）桌管的管控；10、支持平台上一键卸载客户端； |
| 5、合规与补丁管理 | 1、支持基线核查功能，能对内外网、不同类型终端设置相应的合规基线；2、对不符合基线的终端能提供修复路径或者指引提示；3、支持实时监测终端状态（故障），根据终端类型，分配故障自动或半自动修复策略，实现终端故障自愈；4、支持补丁统一管理功能（平台内嵌或使用第三方补丁平台），能及时更新、同步最新微软、Linux、主流国产机的补丁库；5、平台上可自定义不同时段、周期、范围、操作系统类型、终端状态等条件下发补丁升级任务；并不能影响终端使用，升级完补丁不能强制重启；6、终端插件支持自动发现新补丁、自动修复的功能； |
| 6、日志分析与审计 | 1、支持查看管理员（操作员）对终端操作记录；2、支持可视化显示终端的资产信息、故障情况、安全违规等情况；3、支持查看、导出终端资产，违规，合规，故障等各种报表；4、支持查看终端的系统日志、安全日志和应用程序日志；5、支持对终端的打印刻录审计、软件安装卸载审计、网站访问审计、文件审计、流量审计、注册表审计、系统日志审计、外设使用审计、网络共享等审计。 |
| 7、软件管家 | 1、支持内嵌或外增的软件管家功能，能对终端软件的下载、安装、授权、版本控制、卸载、使用统计进行统一管理；2、对安装软件来源统一管理，确保软件正版合规，避免未知源带来的软件安全隐患。 |
| 1. **部署和管理**

1、部署时不改变当前全院网络结构，不断网，不影响用户当前的使用；2、能通过医院现有准入、旧桌管系统批量下发客户端，并静默无感安装部署；3、平台要求灵活部署，不限于独立部署、负载均衡部署、集群部署、云化等部署方式；4、客户端后台透明运行，可设置不显示图标，不弹窗，只在运维时可按特地组合键调出客户端管理界面；5、平台支持WEB中文管理界面（HTTP/HTTPS），界面友好、操作简易；6、支持手动和自动备份系统配置，可支持FTP和TFTP自动备份；7、支持客户端断网、离线后桌管的管理策略依旧生效；8、能监测系统平台自身运行状态，遇到网络故障、平台故障不影响客户端的运行使用；9、平台能联动医院现有时钟同步服务器，使平台及管控的终端按一定频率同步时间。10、平台自身需满足等保三级相关要求，比如日志能保存180天等； |
| 1. **资质及服务**

1. 提供开发接口与其他产品相结合联动，并配合院方作相应定制开发，例如与数据库审计、防火墙的策略下发、人事系统账号统一管理接口、应用系统单点登录、国密改造、态势感知系统相联动等等。2. 提供三年原厂保修及相关技术服务。3. 提供原厂桌面管理系系统的部署安装调试以及对本院管理人员、使用人员的使用培训。4. 必须具有所投产品的原厂商针对本项目的授权函原件和公司的售后服务承诺函原件。5. ISO9001质量管理体系证书。6. 产品必须有公安部颁发的《计算机信息系统安全专用产品销售许可证》。7. 产品厂家必须具备该产品的《计算机软件著作权登记证书》。8. 中国国家信息安全产品认证证书。 |