# 一、项目概述

随着医疗信息化的不断发展，医院内网存在各种各样的终端设备,如医生办公终端、医疗手持终端、医疗器械、IoT终端等。这些终端未经可信认证就能随意接入医院内网和无线网络，并且这些终端本身可能存在一定的安全隐患，给内网带来了巨大隐患。若任由不合规终端接入网络，将给内网带来严重威胁，例如导致病毒在内网疯狂传播。

当前四川省妇幼保健院已经构筑了基础网络安全防护能力，有效地支持了医院各项业务的有效开展，然而新型威胁不断涌现，网络安全工作面临前所未有的挑战，需要进一步加强现有安全设备相关防护能力。网络安全相关政策要求《网络安全等级保护制度》2.0版本、电子病历、互联互通、智慧化医院等行业政策要求下，对终端安全、安全接入等方面都提出了对应要求。

本次需要对医院内网终端进行安全防护部署杀毒软件、部署网络准入且要求检测终端杀毒软件，实现未安装杀毒软件禁止接入网络。通过部署上述系统，实现终端杀毒、网络准入、安全态势感知的三方协调响应机制，达到威胁发现到处置的闭环安全效果，从而提高医院整体的安全防护能力。

**二、功能要求**

|  |  |
| --- | --- |
| 描述 | 要求 |
| 网络准入扩容授权 | 1. 基于医院现有的网络行为管理设备上配置网络准入功能模块，提供1500个终端的准入授权。
2. 若无法满足上述要求，可提供单独网络准入设备实现终端准入功能。
 |
| 无感知平台软系统 | 1. 为简化终端管理，要求支持自动收集终端资产状况，本次需配置pc端≥800，服务器端≥200；并提供不少于三年的使用、升级与更新授权；
2. 支持展示终端资产状况，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端agent版本、病毒库版本、最近登录时间、最近登录的用户名；
3. 支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell后门数量、高危漏洞及其各自影响的终端数量；
4. 支持彻底清除当前流行的蠕虫\挖矿病毒：驱动人生病毒、DorkBot、Morto等；支持主流感染型病毒的清除，包括：Ramnit、Neshta、Parite、Virut、Jadtre、viking、Expiro；支持对宏病毒和感染型病毒的查杀和修复，覆盖office2003和office2007格式的文档和模板；
5. 支持跳转链接至云端安全威胁响应系统，针对已发生的病毒的基本信息，影响分析、威胁分析和处理建议；
6. 支持远程控制管控终端桌面的功能，便于管理员能够及时对存在故障的终端进行维护；
7. 提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数；
8. 支持对70+款软件进行广告弹窗拦截，让办公环境更纯净，支持在客户端查看拦截效果，包括拦截内容、拦截次数等；
9. 支持基于威胁情报的病毒文件哈希值和域名全网终端搜索，可定位出全网终端该病毒的感染情况；
10. 支持展示全球热点风险事件在网内终端的爆发情况，及时了解、处置网内终端的热点风险事件，并显示影响终端数量；
11. 支持导出针对全网终端的终端风险报告，从整体分析全网安全状况，快速了解业务和网络的安全风险，提供安全规划建设建议；
12. 支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间；可配置WebShell实时扫描，一旦发现WebShell文件，可自动隔离或仅上报不隔离；
13. 支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具；
14. 基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御；
15. 与医院现与网络准入控制系统联动，实现终端用户无感知认证功能。
16. 与医院现有网络安全态势感知系统联动，实现终端用户安全事件的联动处置。
17. 与医院现有服务器安全防护系统平台实现统一管理、运维、处置。
 |