南通市第三人民医院网络安全改造项目

技术了解需求

## 一、建设目标与主要建设内容

本项目的建设目标是保护医院终端准入的可控性、终端防病毒的安全性和保证核心数据库的快速接管和业务连续性。遵循国家等级保护政策法规和医院行业相关安全建设标准，建立一整套合适的信息系统安全保障体系，并使得该管理体系能够切实可行地贯彻在南通市第三人民医院信息化相关工作的各个环节，成为信息安全建设的战略目标。

主要建设内容有以下三个方面：

1. **准入控制及桌面管理系统**

通过策略路由将内网的入网流量引流到准入设备，对入网设备进行检查，包括认证和客户端准入两个功能。只有获得授权的用户才能接入内网，不管是通过有线还是无线接入，或者通过插拔自助机的网线非法接入的都能识别并告警。对于合法接入的终端安装桌面管理系统软件，可以远程协助这些机器，检查机器的合规性，必须安装指定的软件或补丁才能入网，也可以防止非法外联。可以推送一些安装包满足客户端管理的需要。

1. **终端防病毒系统**

在虚拟化平台部署终端检测与响应平台（EDR）的服务器端，提供600点的客户端安装授权。EDR杀毒软件除了具有杀毒功能以外，还具有微隔离和补丁功能，可以阻止问题机器发包和封锁端口，修复补丁等功能。另外还可以和态势感知平台联动，对有问题机器进行远程杀毒和隔离。可以对安装了EDR的客户端做联动策略，一旦态势感知发现问题机器，就会推送全盘查杀指令。如果客户端主动对外发送攻击包，达到阈值就会触发阻断策略，封堵该客户端联网一段时间。从而从根本上解决客户端的病毒问题。

1. **数据库高性能复制平台**

当前医院核心HIS系统，Oracle RAC做到了数据库的备份和恢复，一旦发生业务宕机，无法快速恢复业务，不能满足互联互通中4.1.2.3的要求；无法满足电子病历五级的业务连续性的要求。

容灾数据库在数据复制过程中也始终处于打开状态，保证数据复制在逻辑上的完整性，保证灾难切换的时效性和可靠性，为生产中心系统提供了永远可用的后备数据库系统。所以，在源系统出现故障时，双活灾备方案灾备切换时间非常短，能在分钟级接管业务。

**二、需求清单及预算**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **项目** | **配置参数** | **数量** | **单位** |
| **1** | 准入控制及桌面管理 | 准入控制系统系统具备终端入网合规检测、旁路准入、干路准入等功能，准入授权1000点。桌面管理系统具备远程协助、日志审计、移动存储管理、外设管理、补丁管理、运维管理、水印管理、网络准入、安全检测等功能。（支持Windows系统和安卓系统），含1000点授权。原厂上门安装实施服务，5\*12小时电话、远程、邮件支持服务，紧急状况应急相应服务，数据迁移服务  | 1 | 套 |
| **2** | 终端防病毒 | PC高级版包括 周密预防：系统漏洞扫描，补丁修复管理、终端基线检查，资产盘点，资产主动发现，微隔离，轻补丁漏洞免疫； 全面防护：文件实时监控，勒索诱饵防护，勒索病毒立体防护，勒索攻击对抗，无文件攻击防护，停更系统智御； 灵敏检测：恶意文件检测，僵尸网络检测，暴力破解检测，网端联动杀毒； 快速响应：文件急速隔离，终端一键隔离，感染文件修复，病毒处置响应，网端深度联动（XDR），全网威胁定位； 简便运维：外设管控，违规外联检测，远程桌面，广告弹窗拦截；含3年升级维护费用。 | 600 | 套 |
| **3** | 数据库高性能复制平台 | 将生产系统中的数据实时同步复制到目标数据库，使目标库成为①灾备数据库/用于业务接管，②查询/报表数据库，降低生产系统的压力，③实现数据交互/共享平台，④数据抽取/合并/分发⑤数据库迁移/升级应用等。含：2个源端数据库复制模块授权，提供原厂安装调试、认证培训，一年原厂季度巡检、7×24响应、重大数据故障现场技术支持、计划性灾备切换演练、软件补丁和版本升级服务。 | 1 | 套 |

项目预算：48万元