**需求**

2021年国家出台“数据安全法”，对敏感数据的保护上升到法律层面，由于我院特殊性涉及的医患、科研等数据更具敏感性，对数据的保护防泄漏，不被网络黑客出于政治或经济目的攻击，必须加强防范。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 产品 | 功能 | 数量 | 单位 |
| 数据安全综合治理平台 | 数据防泄露管理分析平台 | 数据防泄露管理分析平台：实现在线数据梳理及分类分级；集中下发数据分类识别规则、不同产品模块数据防泄漏策略；数据发现；集中进行敏感数据安全事件监控、处理、审计和统计分析；实现不同场景下的数据泄露防护功能。 | 1 | 套 |
| 网络数据防泄漏系统探针 | 部署在网络出口，发现并监控网络流量中的敏感数据传输，监控并控制HTTP、HTTPS、SMTP、POP3、FTP、SMB、IMAP等网络协议传输的敏感数据行为。支持网络带宽≥500M。 | 1 | 套 |
| 终端数据防泄漏系统探针 | 部署在院内敏感计算机终端，发现、识别、监控终端中的敏感数据，对医院数据资产分布、敏感数据的违规存储进行展现，同时对敏感数据的违规使用、扩散等敏感行为进行策略响应控制。 | 1 | 套 |
| 数据库脱敏系统 | 脱敏速度每小时≥100GB；配置≥2颗CPU20核；内置≥4TB磁盘存储空间；冗余电源；标配≥4个千兆自适应电口；≥2个万兆SFP接口插槽；≥4个千兆SFP接口插槽。 | 1 | 套 |
| 数据中心核心防火墙 | 网络处理能力≥120G，并发连接数标配≥1000万，每秒新建连接≥120万/秒，冗余电源； 标配主机带1个Console口 、1个HA接口，1个管理网口，支持液晶屏，支持≥8个扩展板卡插槽，支持≥12个40G QSFP接口，配置≥8个万兆光口；配置下一代防火墙全功能模块，包含：应用特征库/URL网址过滤/AV防病毒/IPS入侵防御/威胁情报。 | 2 | 套 |
| 安全接入网关 | 安全接入网关专用系统主机，≥6\*10/100/1000电口，≥2个SFP接口，≥1个扩展槽，≥1T硬盘，单台支持最大并发用户数≥800，配置≥200用户授权许可。 | 1 | 套 |
| 抗拒绝服务系统 | 流量清洗能力≥2Gbps，64字节小包处理能力≥280万,主机防护数量≥100万，新建连接数≥15万，并发连接数≥600万。设备支持≥2路防护清洗，标准配置≥4个10/100/1000M自适应电口，≥4个SFP插槽，1个独立HA口，1个独立MGT管理口，≥2个扩展卡插槽。 | 1 | 套 |