上海市口腔医院2025年度网络安全加固项目

（网络安全）

需求文件

2025年3月

# 项目简介

上海市口腔医院始建于1946年，时名上海牙病中心防治所，是上海最早的公立口腔医疗机构。自上世纪50年代起，受上海市卫生健康委员会委托，指导全市口腔病防控工作，拥有全国最完整的口腔公共卫生三级防治网络，是本市口腔科普总召集人单位。医院设有北京东路院区、复兴中路院区、浦锦院区、永嘉路门诊部和天津路科研教学中心。年门急诊服务量70余万人次，是上海市口腔质量控制中心分中心，牵头上海市口腔病防治联合体及复旦大学口腔医疗联合体。

随着医院信息化、数字化的加速发展，为提升患者的就诊体验奠定了坚实基础，但是医疗信息的网络安全以及数据安全问题也伴随而来。在每年度上海市卫生健康行业网络安全管理绩效考核工作方案中明确提出，将网络安全管理工作纳入市管党政领导班于年度绩效考核内容。在此大背景下，结合各类法律法规指南，我院需要从信息安全保障体系建设的多个角度进行差距分析，并确定了本次项目需求。

## 项目目标

依据国家信息安全等级保护制度，遵循国家及上海市相关标准规范，明确信息安全保障重点，建立信息安全等级保护工作机制，切实提高中心信息安全防护能力、隐患发现能力、应急处置能力，有效满足系统的可靠性、安全性、稳定性和先进性要求，为中心信息化健康发展提供可靠保障，全面维护患者利益、公共利益和社会秩序。

## 项目依据

* 《信息安全技术关键信息基础设施安全检查评估指南》；
* 《信息安全技术关键信息基础设施安全保障评价指标体系》;
* 《关键信息基础设施安全保护条例》(国务院令第745号);
* 《计算机信息系统安全保护等级划分准则》（GB17859-1999）；
* 《信息安全等级保护定级指南》（GB/T22240-2020）；
* 《信息安全等级保护基本要求》（GB/T22239-2019）；
* 《信息系统通用安全技术要求》（GB/T20271-2006）；
* 《信息系统等级保护安全设计技术要求》（GB/T25070-2019）；

# 项目建设内容

## 项目清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品/服务名称 | 产品规格-描述内容 | 单位 | 数量 |
| 1 | 服务器虚拟补丁 | 服务器虚拟补丁200点，通过控制受影响的应用程序的输入或输出，来改变或消除漏洞，不需要重启或进行大范围应用系统的回归测试。3年软件升级及维保。 | 套 | 1 |
| 2 | 流量复制器 | 不少于24个万兆光口，不少于4个千兆电口。3年硬件维保、软件升级。 | 台 | 2 |
| 3 | WEB全栈加密安全防护订阅服务 | 服务形式的使用授权。 | 年 | 1 |
| 4 | IPV6防护订阅服务 | 服务形式的使用授权。 | 年 | 1 |
| 5 | 医疗文档云订阅服务 | 服务形式的使用授权。 | 年 | 1 |
| 6 | 安全服务 | 安全评估 | 套 | 1 |

## 技术参数

### 服务器虚拟补丁

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 系统 | ▲（提供承诺书并加盖公章）管理控制台与医院现有防病毒系统兼容 |
| 功能 | （提供系统截图证明并加盖公章）虚拟补丁支持Windows、信 创、Linux三类操作系统的虚拟补丁规则和漏洞攻击防护。 |
| 支持虚拟补丁规则库的周期性更新，同时支持规则库的还原 |
| 支持虚拟补丁规则的维护，包括：虚拟补丁的导入导出、删除、复制、应用、取消应用等 |
| 支持虚拟补丁规则应用给全部客户端，或按分组、指定客户端应用。 |
| （提供系统截图证明并加盖公章）支持以虚拟补丁维度查看每条虚拟补丁规则已应用的客户端范围，和推荐应用的客户端范围。支持以终端维度查看每台客户端已应用的虚拟补丁规则，和推荐应用的虚拟补丁规则。支持立即应用和取消应用。 |
| 入侵防御规则可以拦截试图利用该漏洞的流量。可识别正在访问网络的恶意软件，并增加了对正在访问网络的应用程序的可见性或控制。 |
| （提供系统截图证明并加盖公章）支持入侵防御规则8000条以上，支持应用程序类型400条以上， 可根据需求更改规则及应用类型的配置，且能自动更新及分配所需要的入侵防御规则。 |
| 支持对会话和应用层（如 DNS、HTTP、SSL 和 SMTP）以及根据这些更高层协议的这些数据包进行扫描 |
| 支持对文件共享和消息传递软件流量的检测 |
| 支持网络入侵攻击的防护，包含支持防护SQL注入,Cookie 注入，命令注入，跨站脚本(XSS)，跨站请求伪造(CSRF)，WebShell攻击防护等。 |
| 内置入侵防御的规则库，支持关联ATT&CK框架的技术ID，便于了解网络入侵技战术点。 |
| 通过流量检测技术，实现漏洞利用的攻击防护，支持操作系统、数据库、邮件服务、办公软件、中间件、Web应用、应用等类型的漏洞 |
| ▲（提供系统截图证明并加盖公章）支持0Day漏洞暴露后，快速定制入侵防御规则，包括不限于签名、特征码、XML等方式，进行0day的快速防护，同时可支持配置优先级、检测或阻止模式、严重性等。 |
| 支持3种方式自定义入侵检测规则：签名（匹配单个特征值）、开始/结束/特征码 （ 匹配多个特征值）、定制 (XML)。 |
| 支持设置至少5个规则优先级，当匹配多个规则时，先应用高优先级的规则，然后应用低优先级的规则。 |
| 实现对web程序发现，例如配置规则读取http 头获取nginx等信息，当规则匹配后，可以记录流量记录命中的前后流量信息。 |
| 具有独立的网络引擎处理所有规则，对所有的入侵防御规则开启“仅检测模式”或者“阻止模式”； |
| 支持设置入侵防御规则的生效时间段，例如每日一次、全天、周末等。 |
| 支持显示特定漏洞的相关信息。适用时，将显示通用安全漏洞评分系统(CVSS) |
| 支持将一个或多个入侵防御规则以 XML 或 CSV 文件类型进行导出，并且可以从 XML 文件导入规则 |
| 支持对攻击事件的日志记录，包含攻击来源、攻击时间及试图利用什么方式进行攻击等必要信息。 |
| 支持将多个虚拟补丁规则组合成一个集 合，根据不同的场景创建不同的规则集，可以更方便快捷地应用给客户端。 |
| 售后要求 | 提供三年原厂售后服务承诺函及原厂授权函 |

### 流量复制器

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 接口数量 | 不少于24个万兆光口，不少于4个千兆电口 |
| 工作模式 | 旁路模式 | 支持旁路监听分析模式 |
| 应用协议识别 | 识别数量 | 支持常用协议总量大于1200种1、支持对2～7层流量的识别能力，特别是针对第 7层的应用识别能力，能够识别主要应用协议，并逐级细分P2P下载、网络视频、网络电话、游戏、HTTP协议的子类别和具体客户端名称，比如HTP协议---Web视频---土豆、网络游戏---移动游戏等。2、支持国内各类常见协议>=1000种，其中大型游戏>=300种，移动APP应用>=30种（将持续新增至>=200种移动APP应用），现网协议识别率 >= 95%（提供系统截图证明并加盖公章） |
| 协议识别 | 支持DPI、DFI、节点跟踪、主动探测、加密分析等多种技术。1、对已经采用加密技术的P2P类应用比如BT、迅雷、Skype、eDonkey、Qvod、PPFilm、百度影音等精确识别。2、可以区分迅雷、网际快车等下载工具的HTTP下载和IE浏览器下载3、支持“迅雷增强识别”，大幅度改进对迅雷加密流量识别4、支持“P2P智能识别”，大幅度改进P2P加密协议识别5、协议精细分类且必须包含：移动浏览器（如iPhone手机上网）、应用商店（如安卓市场、手机报等）、云服务、网络支付（招商银行、兴业银行等）、移动游戏（手机游戏、iPad游戏） |
| 虚拟身份识别 | 支持虚拟身份的识别，如QQ号码、MSN帐号、POP3帐号、新浪微博、百度贴吧等 |
| 特征库更新 | 支持在线状态下的特征库的更新升级 |
| 识别准确率 | 现网识别准确率在95%以上 |
| 业务识别率 | 现网业务识别率在95%以上 |
| 自定义协议 | 支持自定义协议、自定义协议组 |
| 分流管理 | 流量复制转发 | 支持基于策略的流量复制转发，策略条目数不低于65535 |
| 支持基于端口输入\输出双向的流量复制 |
| 支持基于IP五元组、VLAN的流量复制 |
| 支持基于应用协议的流量复制（提供系统截图证明并加盖公章） |
| 支持基于协议群组的流量复制（提供系统截图证明并加盖公章） |
| 支持基于域名的流量复制（提供系统截图证明并加盖公章） |
| 支持基于时间的流量复制策略调度 |
| 支持基于指定输出接口转发 |
| 支持对多个策略组进行调度，多个策略组可以同时生效 |
| 支持两级策略匹配，先匹配策略组，后匹配策略，实现策略的高度灵活性、高效率，方便维护 |
| 支持多条策略的一键“启用”、“禁用”和“删除”功能 |
| 负载均衡 | 支持全局同源同宿负载均衡 |
| 支持端口健康状态监测，实时检测后端监控分析系统的健康状态，当设备宕机，立即停止数据转发，进行负载均衡组内的数据负载均衡转发 |
| 支持负载均衡输出到指定的单个或多个输出端口组，端口组支持输出流量权重配比 |
| 报文剥离 | 支持内/外层 VLAN、MPLS、GRE、VXLAN、PPPoE报文的识别和外层头部去封装 |
| 流量监控统计 | 实时流量分析 | 支持实时显示设备接入的流量信息（上行，下行，连接数） |
| 支持实时显示每个接口的流量信息（上行，下行，连接数） |
| 支持显示实时的在线IP用户数，以及近期（1周）的峰值信息 |
| 支持实时显示接入流量的应用协议流量占比 |
| 支持实时显示接入流量的应用协议连接数占比 |
| 支持对应于协议类型进行下转，显示指定协议的统计信息，包括流量趋势，流量大小，关联的IP用户等信息 |
| 支持实时显示某个应用下的Top用户 |
| 支持实时显示当前所有在线IP用户数 |
| 支持按组织架构方式展示IP用户信息 |
| 支持实时显示当前所有连接数信息 |
| 支持实时显示IP用户画像信息（按IP进行用户画像，关联MAC、移动终端、流量大小、连接数、应用协议、连接信息、对端服务信息、虚拟身份等信息进行关联） |
| 支持实时显示应用协议画像信息（按协议进行协议画像，关联协议访问的流量趋势，访问IP用户，连接排名，流量大小，连接数节点信息等进行关联分析和展示。） |
| 支持实时显示接入流量的TOP IP信息 |
| 支持实时显示接入流量的TOP应用协议信息 |
| 支持实时显示接入流量的TOP连接信息 |
| 支持实时显示每一个IP流量速率和当前各个应用的速率明细； |
| 流量统计分析 | 支持提供整个系统、各链路的流量和连接数统计图表 |
| 支持提供最近10分钟流量、累计流量、并发连接数统计图表 |
| 支持实时显示各协议组的当前速率、连接数等统计信息，自动刷新 |
| 支持显示最近一天、最近一周和最近一月的流量趋势图表 |
| 支持显示上行流量、下行流量、并发连接数的“三日对比”趋势图 |
| 支持TOP应用排序 |
| 支持TOP用户排序 |
| 支持实时显示每一个IP流量速率和当前各个应用的速率明细（如同时在线60万IP用户） |
| 支持实时显示某个IP的当前速率及连接明细，以便于异常流量诊断 |
| 支持对IP对应的身份信息，如QQ号码、MSN帐号、POP3帐号、微博帐号等 |
| 支持基于应用速率、流量和连接数等条件进行排序 |
| 可提供在线并发连接、连接新建和删除速率等数据的趋势图表 |
| 可提供在线IP数和共享用户趋势图表 |
| 可选择两个或多个应用协议进行趋势图分析对比 |
| 可提供“应用分流”前后的速率对比 |
| 支持“移动终端”信息统计，包含手机类型、访问IP和时间等 |
| 支持TOP连接排序，可以指定应用和IP条件进行IP（内网IP和外网IP均可）连接数排名统计，以快速定位攻击或被攻击IP |
| 支持通过趋势图方式显示网络数据包PPS（Packet Per Second）的趋势 |
| 支持通过趋势图方式显示TCP SYN数据包和SYN + ACK数据包的PPS（Packet Per Second）的趋势 |
| 增加显示流量所匹配具体的某条策略路由信息 |
| 增加连接信息中的TCP会话状态的显示功能 |
| 支持自动区分会话源目功能 |
| 业务级质量测量 | 业务质量测量（NPM） | 支持分析流量中每一条会话，进行基于应用级的质量测量。（提供系统截图证明并加盖公章） |
| 支持对每条会话监测客户时延，服务时延，应用时延的指标测量。（设备到客户端的网络时延），服务时延（设备到服务器的网络时延），应用时延（会话上下行首包时间差），最大包长（会话上下行最大包的长度）。 |
| 支持每IP用户的实时连接应用的质量监测 |
| 支持每IP用户对端服务应用的质量监测 |
| 支持基于五元组进行业务质量分析 |
| 支持基于应用进行业务质量分析 |
| 支持基于域名进行业务质量分析 |
| 支持会话级别的上下行流量查询 |
| 支持会话级别的丢包率和重传率查询 |
| 配置管理 | 在线更新 | 支持在线更新协议特征库 |
| 支持在线更新策略 |
| 支持在线更新对象库文件 |
| 配置管理 | ▲支持 CLI、SNMP、WEB 管理，配置界面具有友好性易用性，WEB 界面支持 HTTPS 且可完成所有配置管理；支持远程升级，系统配置不覆盖（提供系统截图证明并加盖公章） |
| 产品质保 | 提供3年软硬件服务及原厂保修及技术支持服务，提供原厂商出具的授权书 |

### WEB全栈加密安全防护订阅服务

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 授权 | 1年服务形式的使用授权：含10套系统域名License加密授权。与医院现有系统兼容~~，涉及授权断档时间需要补齐~~ |
| 系统能力 | 支持直通模式，流量经过系统，不做任何检测及拦截处理。【提供功能截图，并加盖公章】 |
| 支持中文域名的安全防护。 |
| 所投产品的防护配置和查询功能须支持IPv6。【针对防护配置、日志查询展示分别提供功能截图，并加盖公章】 |
| 平台具备HA部署能力。能够进行在线状态检测，并根据检测结果自动切换，并保持配置同步、session同步。 |
| 本项目中所投产品不应含有使用Flash技术用于访问重要策略控制的内容。 |
| 系统管理员具备账户管理功能，支持对口令复杂度和口令生存期的设置。 |
| 具备自检信息功能，可显示设备自身系统运行状态信息及异常告警。 |
| 报警功能支持界面及邮件报警。 |
| 支持反向代理部署模式，逻辑串联。支持IP地址收敛效果，支持互联网端对非标端口收敛效果。 |
| 安全防护 | 支持对源站非80/443端口但为HTTP协议的防护，支持对HTTP协议的异常元素、异常参数、非法编码和解码的灵活控制与处理。 |
| 支持域名或IP地址及多端口形式访问防护。 |
| 能基于多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT等。 |
| 支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等；插件应覆盖：dedecms、phpmuadmin、PHPWind、shopex、discuz、echsop、vbulletin、wordpress等。 |
| 支持SQL注入、XSS、SSI指令、Webshell防护，路径穿越及远程文件包含的攻击防护。支持使HTTP头域中的Cookie、Referer、User-Agent，Except字段过防护策略。 |
| 支持CSRF（跨站请求伪造）防护。 |
| 支持爬虫防护，实现对爬虫特征进行识别和阻断，防止页面因爬虫而引起信息泄露等问题。 |
| 支持工具类软件对站点高频扫描的防护，并提供应用层人机识别的拦截手段。【提供功能截图和人机识别效果截图，并加盖公章】 |
| 支持识别非法上传/下载行为，阻断敏感信息泄露、恶意代码攻击、错误配置攻击、隐藏字段攻击、会话劫持攻击、参数篡改攻击、弱口令攻击、Webshell行为拦截。 |
| 支持识别并阻断自动化攻击及第三方引擎的访问。 |
| 防应用层 HTTP DDoS（CC）攻击。 |
| 支持白名单功能，可添加单个或一个段落的地址开放于白名单内，不受策略限制。 |
| 支持攻击黑名单限制，可将识别到的黑IP加入黑名单内，并可设定黑名单时长，时间到后可自动解禁。 |
| 安全加固 | 支持Web站点隐藏和伪装的安全策略，包括操作系统类型、WEB服务器类型、HTTP响应报文头。 |
| 支持自定义错误页面的拦截，防止404、403、502等报错页面泄露敏感信息。 |
| 支持TLS加固策略，至少能够提供TLS1.2以上的安全加固措施。 |
| 支持HTTPS强制跳转。 |
| 支持站点锁定，可以将站点页面缓存到防护平台。 |
| 支持对响应（POST）数据和响应（GET）代码进行脱敏。 |
| web组件加密 | ▲支持Cookie内容加密。【提供功能截图和通过burpsuite工具抓包后依然加密的效果截图，并加盖公章】 |
| 支持针对WEB站点中的代码文件名称进行加密。【提供功能截图和通过burpsuite工具抓包后依然加密的效果截图，并加盖公章】 |
| 支持 HTML 内容整体动态加密，可防站点目录爬取、防爬虫解析等。通过浏览器查看网络传输到应用层的页面代码应为密文。【提供功能截图和通过burpsuite工具抓包后依然加密的效果截图，并加盖公章】 |
| ▲支持 JS 文件源码实时动态加密，可防关键代码分析调试、可防 JS 开源框架漏洞。支持反馈给浏览器的源代码加密，阻止源代码浏览器端的代码分析调试。【提供功能截图和通过burpsuite工具抓包后依然加密的效果截图，并加盖公章】 |
| 数据安全 | 支持WebAPI动态发现、监测、管理及加密等功能。【提供功能截图，并加盖公章】 |
| 支持针对请求数据进行安全检查，支持对SQL注入、XSS注入、CMD注入、自动化攻击、Webshell等场景进行安全防护。 |
| ▲支持对API接口名称进行动态加密，加密算法采用国密算法SM2/SM3/SM4标准。【提供功能截图和通过burpsuite工具抓包后依然加密的效果截图，并加盖公章】 |
| 支持对API上行（POST）数据进行动态加密，加密算法采用国密算法SM2/SM3/SM4标准。【提供功能截图和通过burpsuite工具抓包后依然加密的效果截图，并加盖公章】 |
| ▲支持对API下行数据进行动态加密，加密算法采用国密算法SM2/SM3/SM4标准。【提供功能截图和通过burpsuite工具抓包后依然加密的效果截图，并加盖公章】 |
| 支持针对浏览器端WebAPI加密环境安全检查，针对拟爬虫浏览器检查。【提供功能截图，并加盖公章】 |
| 重保模式 | 支持重点时期开启重保模式，业务系统对互联网显示重保模式页面。 |
| 重保模式页面支持对每个不同站点进行个性化自定义设置。【提供功能截图，并加盖公章】 |
| 重保模式的页面内容支持用户自定义，上传自定义内容后实时生效。 |
| 重保模式支持用户对日期范围、时间段范围进行自定义，自定义后实时生效，其中日期支持周一至周日的复合选择自定义。【提供功能截图，并加盖公章】 |
| 重保模式支持用户自定义IP白名单，如白名单内的IP不显示重保模式。 |
| 重保模式效果支持用户提前设置各种参数，时间到了后会自动生效。 |
| 支持提供站点和策略的多对多的绑定关系，单个站点可以绑定多个重保策略，单个策略可以匹配多个站点【提供功能截图，并加盖公章】 |
| 后台管理系统安全性 | 后台Web管理界面须为中文界面显示。 |
| 后台支持对保护的域名或IP资产进行管理及监测(包括状态及流量) 。 |
| 后台管理系统需要B/S架构，支持PC端机器访问时HTTPS双向身份认证，即只对安装了证书的系统才支持业务访问。 |
| 后台管理系统需要B/S架构，敏感数据或业务数据需要加密保护。 |
| 支持后台管理系统三权分立，包括系统管理员、策略管理员、审计管理员。 |
| 日志功能 | 支持基于时间、域名、动作、事件类型、URL、返回码等条件的日志查询。 |
| 支持在安全日志中带有客户端真实IP地址，便于IP溯源。 |
| 支持日志分时段导出、全部导出。 |
| 支持以Syslog格式向指定统一Syslog日志中心推送本地日志信息。 |
| 支持日志存放周期管理，须支持6个月及以上天数的存放，过期日志可配置自动清理。 |
| 兼容性 | 需完成在申威、龙芯、鲲鹏、飞腾、海光及兆芯平台的兼容性测试、功能性测试、性能测试、安全可靠性测试。 |
| 其他要求 | 提供一年软件升级服务及原厂保修及技术支持服务，提供原厂商出具的授权书 |

###  IPV6防护订阅服务

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 授权数量 | 1年服务形式的使用授权，与医院现有系统兼容。 |
| 集中管控 | 1.支持配置全局IP黑名单，所配置黑名单IP针对账号所有域名生效，从而实现在重保等特殊期间快速处置威胁IP； |
| 2.支持独立的黑白名单IP维护页面，可以被具体域名引用，从而实现快速访问控制处置； |
| 3.支持SSL证书集中管理； |
| 4.支持定制配置模板和通过指定域名生成模版服务，可提前配置好防御策略，一键应用到具体网站，提高配置效率； |
| 防篡改功能 | 1.具备网站页面备份能力，启用后可锁定网站内容，特殊时期保障网站永远在线，防止网页内容被篡改。支持主动方式生成备份内容，支持自定义抓取层级和页面数；支持多个备份副本，可按需使用，同一网站支持至少5个备份副本； |
| 2.具备敏感词过滤能力，平台提供默认词库，可根据需要自定义需要替换的敏感词，过滤模式支持默认、自定义和混合模式。支持忽略指定的敏感词； |
| 站点配置 | 1.具备文件上传大小自定义配置； |
| 2.支持WebSocket、SSE； |
| 3.支持回源负载均衡方式设置，负载均衡方式需要支持轮询和IP哈希； |
| 4.支持回源到IP或者域名； |
| 5.支持自定义回源SNI； |
| 6.   支持回源新建链接超时时间、读连接超时时间、写连接超时时间自定义；支持启用回源长连接、支持启用回源重试； |
| 加速配置 | 1.支持js、css和html页面压缩能力； |
| 2.支持自定义CDN缓存规则，需支持后缀名、路径和目录设置，缓存时间设置支持秒为单位；缓存规则支持忽略请求头中Cache-Control和pragma、支持缓存时忽略URL中参数； |
| 3.支持IPv6，以满足网站支持IPv4和IPv6双栈需求； |
| 4.支持HTTP、HTTPS、HTTP2.0、HSTS、HTTP强制跳转HTTPS； |
| 5.支持自定义500、502/504和404状态码错误页面； |
| 6.支持自定义HTTP响应头和HTTP请求头； |
| 日志报告 | 1.安全日志存储不低于6个月；支持在线日志查询，支持通过IP、区域、威胁等级、处置动作等进行日志筛选； |
| 2.具备安全服务报告功能，支持按计划生成，支持word和pdf格式； |

### 医疗文档云订阅服务

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 授权数量 | 1年服务形式的使用授权；本地一套（含500点用户），公有云一套（含200点用户）与医院现有系统兼容。提供长期培训服务，指导各科室新员工使用，有问题反馈及时处理，协助医院推行U盘禁用。 |
| 基本要求 | 投标产品应为国内主流品牌，非OEM产品。 |
| 部署服务 | 支持本地部署、云端部署、单独及混合分布式部署，每个站点可以支持集群，多个站点可以形成统一的大规模分布式集群部署架构。站点的数据本身保证高可用和安全性，全局重复数据删除。同时为了保证访问体验，支持方向代理加速，提升跨站点文档访问体验。 |
| 可满足分布式部署，每个站点的用户就近存储访问，跨站点统一共享，对于分院，在同一个项目文件夹中共享，统一视图。 |
| 分布式部署中，既可以支持多组织架构树，也可以统一组织架构树，支持多个单位统一身份认证或者灵活的不同单位不同认证体系； |
| 平台管理配置服务 | 系统管理可以通过登录Web，统一管理云共享服务（包括创建用户组织、自定义文档库、权限管理、访问控制、安全访问管理控制等、访问日志）。 |
| 系统管理员可以通过登陆Web了解包括在线人数监控、文件分类数量统计、文件操作变化统计，可以提供实时、每日、每月及年度的报表。 |
| 文档分类 | 支持个人文档库访问，以个人用户的用户名为文件库名称，为个人用户所有，属于个人私密性和专属性的文档库。支持开启或者关闭个人文档库。 |
| 支持群组文档库访问，用户可以基于群组文档库与组织内的人进行共享协作。 |
| 支持自定义文档库访问，由系统管理员创建或者普通管理员创建分类、创建文档库并指派所有者，文档库所有者可以为相应组织的成员配置访问权限，这样成员就可以看到相应的文档库资料。 |
| 支持共享文档，他人共享给我的文档，包括文件或者文件夹，共享的文件和文件夹都是带权限的，共享的文件可以被修改、编辑，而且会自动更新，不是简单的下载副本资料。 |
| 访问方式 | 支持PC客户端、移动客户端（Android、IOS）、Web、MAC OS访问。 |
| 支持与Microsoft Office和WPS Office办公软件无缝结合，支持通过插件实线OFFICE办公软件直接操作和保存云端文件，实现医院内部办公业务闭环。 |
| 文档管理 | 支持文件编目功能，管理员可设置不同的文件编目，满足不同类型的文件归类所需；普通用户可以根据编目策略选择文件的编目值，并且系统提供基于文件编目的全文检索服务。 |
| 支持基于云存储的全文检索，当用户想找某个文档资料，希望找到某个关键词相近的文档，输入关键词，获取全文检索的结果，支持文件类型、位置范围过滤，搜索结果支持时间排序。 |
| 支持同级审核、会签审核、逐级审核三种模式。普通用户针对文件或者目录发起流程审核，审核过程中，审核员收到相应的消息提醒，并且能够实时查看审核状态。 |
| 音视频文件无需下载即可通过浏览器和移动客户端在线播放。 |
| 支持把会议资料开启共享，提供二维码，与会者在微信上扫描二维码，可在线预览会议资料，形成无纸化会议。 |
| 文档删除后自动移动至回收站中存放，可还原文件，回收站按文档库分类呈现，且可以支持文件名、删除位置和删除者的搜索，以便更好的找回误删除文件。 |
| 支持对文件手工单个或批量设置标签，以及基于标签的全文检索。 |
| 非法内容管控 | 系统支持基于管理员自定义敏感词对上传的文件进行过滤，并自动隔离包含敏感词的文件，防止非法内容在企业中扩散造成不良影响。用户发现自己的文档被误隔离以后，可以在系统中针对文档发起申诉，经管理员审查同意后可以还原文档。 |
| 数据重删和秒传 | 支持文件重复数据删除技术，相同的文件只上传一次，对于重复上传者而言实现文件的秒传。 |
| 安全特性 | 支持文档预览水印，文件类型覆盖Office文件、PDF文件、图片等，包括自定义水印、时间及访问者信息水印（包含用户名和显示名），支持自定义水印版式、字号、颜色等。 |
| 支持视频预览水印，包括自定义水印、时间水印及访问者信息水印（包含用户名和显示名），支持自定义水印版式、字号、颜色等。 |
| 支持HTTP共享者在开启链接时设置预览/下载水印，其他用户访问该HTTPLink，预览/下载文件时，显示的是HTTP共享里设置的水印。 |
| 支持文件类型过滤，预置已知可疑文件、病毒文件类型，选择性禁止风险文件的上传，也可根据需要自行添加需要屏蔽的文件后缀名。 |
| 支持双因子认证登录方式，包括短信验证码认证、图形验证、动态密码验证三种方式，防止撞库攻击与密码暴力破解。 |
| 当有用户通过HTTPLink的方式将文件外发给外部人员时，支持对外文件内容进行留底，可对外部人员查看或下载的文件内容进行审查和取证。 |
| 支持基于日志的文件安全分析和行为分析，包括运维监控、敏感文件分析、热门用户/资源、文档点击率及访问人员、文档修订情况、敏感用户监控、警告操作审计、文件外发风险控制、文件历史时间轴等。 |
| 文档协作 | 支持常见office文档的多人同时Web在线编辑，支持编辑自动保存，同时能够实时刷新他人编辑的内容，且可以看到当前有哪些人正在对该文档进行编辑。 |
| 支持管理员设置文件评论策略。开启文件评论后普通用户可以针对文件进行评论，查看评论，回复他人评论以及删除自己发表的评论。支持针对文件进行评分； |
| 支持多终端消息通知（Windows、Web、移动端）和邮件提醒，当有文件共享、审核时，相关人员可以通过消息通知或邮件即时的看到共享信息或审核相关内容 |
| 内外网文档交换 | 支持普通用户将内网数据外发至外网，但是文件外发之前需要经过文档审核管理员进行审核；支持普通用户将外网转发至内网，文件转发至内网之前需要经过文档审核管理员进行审核； |
| 在开启跨网络数据交换的前提下，管理员可以在控制台启用文档库内外网同步，并且可以灵活配置同步范围，即选择部分文档库进行同步。 |
| 支持放入特定文件夹的文档自动触发内外网审核和交换流程。 |
| 支持文档交换前自动触发敏感内容检测，管理员可事先自定义敏感内容关键字，当检测到交换的文档包含定义的敏感信息，自动进入到审核员进行审核，审核不通过的文档自动隔离； |

### 安全服务

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **服务内容** | **单位** | **数量** |
| 1 | 攻防演练 | 以攻击者视角，组织安全专家作为红队（攻击队），针对客户单位的信息资产，不限攻击路径、不限攻击目标、不限攻击手段，展开贴近真实遭遇攻击场景，以验证系统整体安全防御水平。交付物：《攻防演练报告》 | 次 | 1 |
| 2 | 安全制度优化 | 针对**市网信办、市卫健委**的监管要求提供安全管理体系制度有针对性的咨询服务，并同步完成安全制度优化。对于一些不满足要求的监管要求，提出整改方案。对接上级部门的安全信息填报。交付物：《安全管理制度》、《整改方案》 | 套 | 1 |
| 3 | 安全漏洞评估 | 对系统中相关的网络设备、操作系统、数据库和应用服务中存在的安全漏洞进行检测。交付物：《漏洞扫描报告》 | 次 | 4 |
| 4 | 渗透测试 | 从攻击者的视角，模拟黑客所使用的攻击手段对目标系统进行模拟入侵，以充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁，包含复测，对修复的高危，进行人工验证。交付物：《渗透测试报告》 | 系统 | 12 |
| 5 | 三级等保咨询服务 | 针对信息系统等级保护的初测、整改、复测，直到医院获得测评证书，全程协助医院做好各项文书、技术工作，为医院提供安全技术支持、提供安全加固支持。交付物：《差距分析报告》 | 系统 | 5 |
| 6 | 漏洞管理服务 | 提供漏洞闭环管理服务，针对院内所有服务器操作系统漏洞提供解决方案，告知并跟踪修复进度，保证域控补丁服务器的正常使用。交付物：《漏洞修复进度表》 | 年 | 1 |
| 7 | 文档云配合落地服务 | 配合医院完成文档云平台的使用和落地工作，具体包含：文档云平台的日常运维，故障处理；平台账户维护；各个科室的使用培训；交付物：《培训记录》 | 年 | 1 |
| 8 | 新业务上线安全评估以及配合落地服务 | 针对医院不断上线的新业务需求，从安全的角度参与方案的评审工作，对系统部署位置、技术平台的选择、需要达到的安全要求等提出专业的意见供甲方参考。并在业务上线过程中提供相应的安全设置调整配合工作。交付物：《配置变更单》 | 年 | 1 |
| 9 | 安全产品测试服务 | 对于前沿的安全技术和优秀的解决方案或产品，医院需要引入进行测试和评估，乙方需要提供测试的配合工作，并参与产品的价值评估，提出专业的意见供甲方参考。交付物：《产品测试报告》 | 年 | 1 |
| 10 | 各类检查应对牵头服务 | 针对每年都会开展的卫健委要求的自查、飞行检查、医保检查等各类安全检查提供支持服务，应对各类检查文件或者现场检查。需要及时补足检查发现的安全问题。交付物：按照各检查要求交付 | 年 | 1 |
| 11 | 重保应急响应服务 | 针对每年发生的两会、进博会等关键时间节点，提供重保服务，加强对安全设备的监测，同时提供7\*24小时的应急响应服务。交付物：《应急响应报告》（按需） | 年 | 1 |
| 12 | 资产暴露面收敛服务 | 针对目前医院对外开放的IP、端口、域名信息进行完整的梳理，确认不需要开放的服务，有计划性的推动配置的缩减，减小不必要的资产暴露面。并及时跟进医院业务变化，快速跟进调整。确保对外暴露的资产始终保持最小。交付物：《出口防火墙NAT策略表》、《DNS解析记录表》 | 年 | 1 |
| 13 | 应急演练服务 | 牵头完成应急演练。包括：制定演练计划、记录演练过程、配合协调演练开展、输出应急演练报告。交付物：《应急演练方案》、《应急演练报告》 | 次 | 2 |
| 14 | 安全意识培训服务 | 为甲方提供安全意识培训。交付物：《培训PPT》、《培训记录》 | 次 | 2 |
| 15 | 老院区服务器迁移牵头 | 医院需要将老院区服务器迁移至新院区，乙方在这个过程中需要提供支持服务，配合对各安全设备策略进行变更调整。交付物：《配置变更单》 | 次 | 1 |
| 16 | 联软控制台合并牵头服务 | 医院目前新老院区合并，需要将多套联软设备的控制台合并成一个。乙方需要针对这个事项制定合理的实施方案。并协调厂商完成控制台合并工作。确保整个过程对医院业务影响最小化。交付物：《配置变更单》 | 次 | 1 |

#### 攻防演练

以攻击者视角，组织安全专家作为红队（攻击队），针对客户单位的信息资产，不限攻击路径、不限攻击目标、不限攻击手段，展开贴近真实遭遇攻击场景，以验证系统整体安全防御水平。

#### 安全制度优化

根据**市网信办、市卫健委**的监管要求，提供全套的制度整改服务，补充当前医院现有管理制度和相关表单。提出的信息安全保障体系设计规划需求，提供专业咨询服务，结合医院实际情况及当前的安全威胁，依据信息安全相关的国际/国内标准规范、协助企业建立信息安全保障的建设目标，选择和组合信息安全控制措施，完成信息安全保障体系架构设计，并合理规划信息安全保障体系的建设步骤和资源投入，最终达成有序提升信息安全风险管控能力，保障信息系统安全运营，完善医院安全保障体系的目标。

#### 安全漏洞评估

漏洞扫描：制定安全扫描计划，通过评估工具以本地扫描的方式对评估范围内的系统和网络进行安全扫描，从内网和外网两个角度来查找网络结构、网络设备、服务器主机、中间件、数据和用户账号/口令等安全对象目标存在的安全风险、漏洞和威胁。

* 测试方案：根据业务系统情况编制漏洞扫描方案及实施计划，其中方案需注明所使用的测试工具及特点。
* 信息收集：开启端口集 合、开启服务列表、同服务器其他网站列表收集。
* 漏洞发现:主机安全漏洞、中间件安全漏洞、数据库安全漏洞发现、弱口令等安全隐患问题。
* 报告编写:完成应用系统、主机操作系统、数据库系统的漏洞扫描工作，并针对扫描结果中的漏洞进行验证，给出扫描报告。
* 加固指导：根据检测结果对所有安全漏洞给予加固建议与指导。

#### 渗透测试

以模拟黑客的攻击方法，对信息系统进行非破坏性质的攻击测试，查找存在的漏洞并给出详细的修复建议。除使用公安部认定的产品和工具扫描外，更重要的需要进行人工渗透。渗透项目包括但不限于以下项，且需要对发现的漏洞进行验证和利用。

|  |  |  |
| --- | --- | --- |
| 渗透测试 | 测试方案 | 根据业务系统情况编制渗透测试方案及测试计划，其中测试方案需注明所使用的测试工具、测试方法以及测试项等信息。 |
| 信息收集 | 对业务系统进行信息收集、专业安全工具扫描收集漏洞相关信息。 |
| 漏洞挖掘 | 对业务系统进行重定向和转发、文件包含、跨站脚本攻击、未授权访问、越权访问、CSRF、中间件、安全配置错误、SQL注入、授权绕过漏洞、请求重放漏洞、欺骗密码找回漏洞、系统应用程序测试等渗透测试。 |
| 报告编写 | 针对整体渗透测试情况编写报告并进行相应的问题复查。 |

#### 三级等保咨询服务

从政策、制度、规范、流程等方面入手，依据等级保护相关要求，给予客户等级保护管理制度和技术方面的评估、分析、改进等。包含系统的定级备案、差距分析、安全整改、安全评估，管理制度的编制和梳理等相关内容，按照基本要求三级标准或行业标准对现有系统进行定级；通过配置核查、漏洞扫描等手段收集现状信息进行差距分析；结合差距分析结果给出整体整改方案；依据整改方案进行建设整改确保系统通过等保测评。交付物：《差距分析报告》

#### 漏洞管理服务

针对漏扫、渗透、监管各种检查出来的漏洞，提供闭环管理。合理安排漏洞修复进度，确定各种漏洞修复的负责人。完成修复的漏洞需要进行复测确认是否的确已经修复完成。

交付物：《漏洞修复进度表》

#### 文档云配合落地服务

配合医院完成文档云平台的使用和落地工作，具体包含：文档云平台的日常运维，故障处理；平台账户维护；各个科室的使用培训；交付物：《培训记录》

#### 新业务上线安全评估以及配合落地服务

针对医院不断上线的新业务需求，从安全的角度参与方案的评审工作，对系统部署位置、技术平台的选择、需要达到的安全要求等提出专业的意见供甲方参考。并在业务上线过程中提供相应的安全设置调整配合工作。交付物：《配置变更单》

#### 安全产品测试服务

对于前沿的安全技术和优秀的解决方案或产品，医院需要引入进行测试和评估，乙方需要提供测试的配合工作，并参与产品的价值评估，提出专业的意见供甲方参考。交付物：《产品测试报告》

#### 各类检查应对牵头服务

针对每年都会开展的卫健委要求的自查、飞行检查、医保检查等各类安全检查提供支持服务，应对各类检查文件或者现场检查。需要及时补足检查发现的安全问题。交付物：按照各检查要求交付

#### 重保应急响应服务

针对每年发生的两会、进博会等关键时间节点，提供重保服务，加强对安全设备的监测，同时提供7\*24小时的应急响应服务。交付物：《应急响应报告》（按需）

#### 资产暴露面收敛服务

针对目前医院对外开放的IP、端口、域名信息进行完整的梳理，确认不需要开放的服务，有计划性的推动配置的缩减，减小不必要的资产暴露面。并及时跟进医院业务变化，快速跟进调整。确保对外暴露的资产始终保持最小。交付物：《出口防火墙NAT策略表》、《DNS解析记录表》

#### 应急演练服务

配合完成应急演练。包括：制定演练计划、记录演练过程、配合协调演练开展、输出应急演练报告。交付物：《应急演练方案》、《应急演练报告》

#### 安全意识培训服务

为甲方提供安全意识培训。交付物：《培训PPT》、《培训记录》

#### 老院区服务器迁移牵头服务

医院需要将老院区服务器迁移至新院区，乙方在这个过程中需要提供支持服务，配合对各安全设备策略进行变更调整。交付物：《配置变更单》

#### 联软控制台合并牵头服务

医院目前新老院区合并，需要将多套联软设备的控制台合并成一个。乙方需要针对这个事项制定合理的实施方案。并协调厂商完成控制台合并工作。确保整个过程对医院业务影响最小化。交付物：《配置变更单》

## 付款方式说明

第一笔-预付款（50%）：合同签订且采购人收到履约保证金和与支付款项等额的发票后10个工作日内，支付第一笔合同款；第二笔-付款（20%）：产品、授权全部到货且采购人收到与支付款项等额的发票后10个工作日内，支付第二笔合同款；

第三笔-尾款（30%）：完成项目终验且验收合格，采购人收到与支付款项等额的发票后10个工作日内，支付尾款。

2.4 项目要求

## 1）实施要求

项目实施前须向采购人提交详细技术服务方案，方案应包含但不限于技术人员安排、使用工具和应急响应措施等内容，且方案应完善并符合采购人现场实际情况、针对性及操作性强，经采购人确认后方可实施。

## 2）项目组人员要求

投标人应充分理解本项目的技术及实施复杂度，组建技术服务团队，参与本项目的各类人员应具备相应的技术能力。在服务期内，投标人不得随意更换项目组技术人员，若因特殊情况需要更换服务人员时，需经采购人同意后，方可更换技术能力、资格条件相同或更高的技术人员。

项目经理具备三年以上信息类项目管理经验，具有注册信息安全工程师CISP证书、信息化类高级工程师职称证书、信息系统项目管理师证书的优先考虑；

提供不少于5人团队（不包含项目经理）且团队成员（不包含项目经理）具备注册信息安全专业人员CISP的优先考虑。

## 3）工期进度

自合同签订之日起1年。

## 4）售后服务要求

投标人应承担所供产品的安装、调试和配置工作，同时应提供完整的安装调试文档及系统配置文件。投标人应全力与用户及其他相关产品供应商配合，保证系统按时、正常地投入运行。投标人需保证项目实施的过程不能影响采购人各项业务的正常进行，对危险操作提出风险规避方案和相应的应急预案，并指明可能产生的后果，在征得采购人批准后方可实施。投标人需保证所配置的产品有合法的使用权。硬件及产品软件验收合格后三年（订阅及安全服务不涉及）

## 5）验收要求

根据采购人需求内容完成实施后，应及时进行根据合同的规定进行服务验收。投标人应当以书面形式向采购人递交验收通知书，采购人在收到验收通知书后的10个工作日内，确定具体日期，由双方按照本合同的规定完成服务验收。采购人有权委托第三方进行验收，对此投标人应当配合。

## 6）其他要求

1.投标人具有ISO27001 信息安全管理体系证书、中国网络安全审查技术与认证中心信息系统安全集成服务资质认证的优先考虑；

2.投标人具有自2022年1月1日以来承接的有效的类似项目业绩的优先考虑。