**数据安全管理平台及系统高可用加固项目**

**用户需求书**

## 项目背景

在医疗业务的微服务化、数据服务化趋势下，API承载了医院医疗应用各组件间高密度高价值数据流动，成为数据交互最重要的传输方式之一，但由于发展过快，业务优先，导致无法对API进行安全的开发和有效治理管理。医院对于API资产的可见性，以及威胁发现能力，漏洞、脆弱性难以看清；对于活动的医疗敏感数据也缺乏管控。国家卫健委相继出台的数据安全相关指南和管理办法中，明确提出了对API资产监测的要求。

随着医院业务的迅速发展以及所承载业务的多样化，为了解决单台服务器的处理性能瓶颈及单点故障问题，通过部署负载均衡设备，针对不同的业务类型，采用不同的调度算法，使流量处理逻辑更加贴合业务需求，防止服务器资源严重消耗并提高业务系统的高可用性。

医院的业务系统集中部署在超融合平台上，一旦发生意外事故导致数据丢失，则有可能直接导致医院遭受难以逆转的损害。对指定虚拟机开启实时CDP保护，通过IO镜像方式跟踪记录虚拟机IO变更情况，当虚拟机数据丢失或故障时，可使用备份的任意历史时间点进行恢复（RPO≈0，RTO<5min），从而大大降低风险。

## 项目建设清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品** | **详细技术要求** | **数量** | **单位** |
| 1 | 数据安全管理平台 | **1、数据安全管理系统** | 1 | 套 |
| （1）首页支持数据库资产和应用API资产的总览，能够掌握当前数据库、数据表、字段数量以及应用、API、涉敏应用和API的数量；针对数据库的资产管理，能够统计数据分类分级以及打标情况，针对应用/API的资产管理，能够掌握API数据接口脆弱性和访问风险的分布情况；（2）设备对接管理：支持统一管理接入的设备，能够新增、删除或编辑已接入的设备，通过设备管理列表能够查看设备名称、设备类型、运行状态、认证token、设备状态和最近同步的时间；平台支持一次性对接多种设备类型，包括数据库审计、数据安全大脑探针等，进行统一的日志上报和流转分析；支持通过设备详情查看对接的IP、端口、CPU和内存占用情况、流速、设备状态和最近同步时间，并支持编辑下发对接配置信息，满足日常运维需求。（3）探针管理：支持使用探针的方式采集流量到平台上，探针支持CentOS、Redhat6.5以上等操作系统，在平台上可直观看到已接入探针的整体运行情况，包括IP地址、资源占用、流速、监听端口、设备状态等，以便于进行探针的接入管理；支持在agent上指定网口、端口回传流量，避免影响数据库业务。（4）管理员账号管理：支持三权分立，提供系统管理员、安全管理员、审计员三个角色账户；支持设置管理员账号允许登录的IP范围，支持设置管理员账号登录允许尝试次数可配和长时间未操作自动退出，并支持管理员用户设置密码使用天数限制，超过指定天数进行强制修改密码，提升系统登录的安全性。 |
| **2、API风险监测预警模块** |
| （1）系统以数据为中心，着眼API接口，对敏感数据进行多重防护，有效应对数据泄露、黑客入侵、接口滥用等风险。包含：用户管理、防护管理、水印管理、访问控制等功能；（2）支持流量解析方式来发现应用是否涉敏，实现应用、接口、敏感数据关联关系的自动梳理，统计应用的域名、地址、关联的API、敏感数据类型等，并通过标识应用等级来区分需要重点关注的应用资产列表。（3）支持安全事件，基于基础风险告警进行关联聚合，结合常见的API数据泄漏事件场景，对api、风险主体、脆弱性等维度的关联，构建API攻击行为画像，形成场景化的安全事件，包括：参数遍历获取大量敏感数据、异常时间段频繁访问获取大量敏感数据、发生探测攻击并通过频繁访问获取敏感数据等，降低风险告警分析成本。（4）产品能够识别主流的接口脆弱性风险，支持OWASP TOP10风险识别，内置脆弱性规则条数不少于70种，包括失效的对象级授权、失效的用户身份认证、过度数据暴露、缺少资源/速率限制、失效的功能级授权、批量分配、安全配置错误、注入、资产管理不当等脆弱性规则；授权管理员可选择配置脆弱性等级和应用范围，设置排除API的白名单，限制检测范围。（5）能够基于UEBA行为识别技术，识别接口异常行为风险，内置数十种API异常行为风险检测模型，包括：账号多地多IP访问、境内外访问、敏感数据异常暴露、参数名缺失、高频访问API、参数值异常、参数值遍历、请求方法异常、访问码异常等风险规则，构建接口访问行为基线。（6）支持自定义风险规则，能够基于风险等级、风险主体、访问API、检测周期、返回数据类型、请求方法等进行条件组合，生成新的安全基线，并支持基于基础风险组合生成高级风险，满足不同场景下的风险检测要求。（7）支持编辑风险策略，选择指定风险等级，设置风险过滤条件，包括：基于应用、API分组设置访问API、IP属性（境内IP、境外IP）、检测周期、告警条件、排除账号的设置，以便于进行风险策略调优，优化风险模型。（8）支持场景化的安全事件规则，基于实战攻防经验进行风险告警关联聚合，来提升告警检出的精准率；授权管理员可自定义安全事件等级，安全事件策略模型包括：频繁访问获取大量敏感数据、异常时间段频繁访问获取大量敏感数据、发生探测攻击并通过频繁访问获取过量敏感数据、API接口遭遇渗透攻击等。（9）支持针对风险策略独立配置风险白名单，可选择指定的加白对象、风险名称、加白API、加白时长，进行检出范围的风险排除。（10）支持脆弱性告警，包括脆弱性等级占比的统计、脆弱性事件top10、脆弱性应用top5的展示，脆弱性告警列表可展示脆弱性名称、等级、关联的脆弱性API、所属应用、脆弱性类型、发生时间以及处理状态等，可下钻查看详细的脆弱性描述以及相关处置建议，进行脆弱性风险分析；可选择性筛选脆弱性告警列表中指定的应用、API分组、主体类型、风险等级、风险名称、处理状态等，快速定位告警事件。 |
| **3、数据安全采集探针** |
| 1. 支持实时获取Agent引流流量，根据配置信息进行数据预处理。

2、采用入库即时加载的处理机制，将处理完成的数据入库保存，来保障检测结果展示的实时性。3、支持使用agent的方式采集流量到探针上，agent支持CentOS、Redhat6.5以上等操作系统，在平台上可直观看到agent的整体运行情况。4、在宿主机上的CPU占用不超过5%，内存不超过5%，支持当运行主机CPU超过80%以后，agent做静默处理，避免影响业务。5、支持在agent上指定网口、端口回传流量，避免影响数据库业务。6、Agent采集的流量需要通过加密通路发送给数据探针，确保传输数据安全。 |
| 2 | 服务器负载均衡 | （1）2U标准机架式，内存大小≥8G，电源：冗余电源，接口≥6个千兆电口+2个万兆光口；四层吞吐量≥20G，四层并发连接数≥800万，四层新建连接数 CPS≥21万，7层新建请求数 RPS≥35万。（2）支持针对多条出口线路的链路负载均衡功能，实现inbound和outbound流量的均衡调度，以及链路之间的冗余互备。且单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权。(3)开通HTTP压缩、HTTP缓存、TCP连接复用、SSL卸载等功能，无需额外购买相应授权。（4）支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应、加权最小流量、按主机加权最小流量、加权源IP哈希、带宽比例、哈希、首个可用、优先级等算法。（5）支持源IP、Cookie（插入/被动/改写）、HTTP-Passive、SSL Session ID等多种会话保持机制，支持跨虚拟服务的会话保持。（6）支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的WebP或JPEG格式，优化加速效果。（7）支持显示设备的电源状态、风扇转速、磁盘温度、CPU温度、CPU和内存占用率、新建连接数、并发连接数、吞吐情况、SSL新建和SSL吞吐数据、压缩优化和缓存优化数据；业务的健康状态、新建连接数、并发连接数、上下行流量、每秒请求数；节点池的调度算法、健康状态、新建连接数、并发连接数、上下行流量；（8）支持串接部署方式和旁路部署方式，支持三角传输模式；支持双机热备部署方式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换；（9）支持高可用集群N+M部署方式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换.（10）为了保障产品的性能、功能，达到需求效果，采购人保留测试权利；（11）提供3年硬件质保、3年软件升级。 | 2 | 台 |
| 3 | 持续数据保护软件 | (1)支持无代理CDP技术，不需要在虚拟机内部安装任何代理软件，即可对虚拟机进行持续数据保护，CDP不影响保护虚拟机的性能； (2)最小提供RPO为秒级的数据保护； (3)支持业务虚拟机的快速恢复，可以指定策略覆盖原有虚拟机或者创建新虚拟机； (4)支持CDP备份任意时间点的数据克隆，通过克隆数据恢复虚拟机进行测试与验证； (5)支持通过CDP备份数据找回文件； (6)支持CDP功能升级扩展为异地CDP容灾能力； (7)支持提供CDP备份时间点图形化显示，并显示CDP时间点IO日志保存速率； 支持CDP日志丢失后的备份恢复容错能力；(8)提供一个超融合集群的CDP模块及50个虚拟机授权，三年软件升级服务。 | 1 | 项 |