四个信息化软件维保升级项目
技术标准和服务要求

一、防病毒软件维保升级项目技术标准和服务要求

1500 台设备 3 年版，要求详见下文

1. 终端支持 Windows 系列操作系统（包含 Windows XP/2003/ 7/8/10 等常见的操作系统平台，以及 Windows XP-64，Windows Server 2003-64/windows 2008/windows2012/Windows2016 等 64 位操作系统专业版和服务器版）；客户端安装完成后，无需重新启动计算机即可开启防护功能；优先支持 Linux、AIX、Free BSD、Solaris、CentOS 等操作系统，并且支持 MAC OS X 系列操作系统及安卓系统等；
2. 服务端和控制中心既可部署在 windows 服务器操作系统上，也能部署在 linux 服务器操作系。**投标文件中必须提供相关证明材料，包含但不限于官网链接或截图等材料**
3. 使用增强的 HTTP 协议(https)来访问 WEB 远程管理界面,使管理员在全网任何地方均可通过 web 浏览方式,监控和管理全网信息安全;
4. 管理员可直接通过远程管理控制台，配置、修改全网不同分组计算机的安全策略，修改策略后，网内各计算机自动实现策略变更，无需再次通过下发策略实现；策略可支持向下同步、合并；支持用户导入、导出和编辑 XML 格式的策略。通过一次性设定配置信息并导出设定档，集中应用于终端设备和用户组的方式，有效节

约管理人员工作时间，避免忙中出错。

5. 管理控制台需要有通知管理器功能，管理员可以新建或者根据默认的通知规则进行选择，方便管理员随时了解全网安全状况；单个管理控制台能够同时管理客户端的数量与硬件无关；根据许可证的数量，管理客户端；（无限制）；
6. 支持管理员分组、分级管理，支持客户端的分组功能，分组可支持与 windows 域的 AD 分组进行同步；支持不同组或客户端采用不同的病毒防护策略；支持远程/移动式管理，远程查杀策略设置，设定客户端定时查杀病毒；在控制台能实时显示客户端的状态、信息；
7. 为防止客户端未开机，而进行全网查杀或设置，在客户端下次启动时提供补做功能；
8. 支持远程控制客户端进行文件扫描、远程开启/关闭实时监控，远程控制客户端升级病毒库；
9. 支持远程安装、卸载客户端防病毒软件；实时监控客户端防病毒状况；并自动生成饼状、柱状图以及其它格式的报告；
10. 可以统计全局发现病毒的报告；可以统计指定对象、在指定的时间内发现病毒的报告；可以统计全局感染病毒最严重的计算机的报告；可以统计全局使用程序版本的报告；可以统计全局反病毒数据库更新的报告；可以统计全局计算机的程序错误报告；
11. 全网统一自动升级，不需要人为干涉；默认为每隔 1 小时进行病毒库和程序组件更新检测，确保快速有效的对网络内计算机进行安全

防护；当病毒库达到一定大小时，询问是否更新；病毒库增量升级，减少对网络资源的占用；

12.支持离线病毒库包，考虑到资源占用，升级的便捷，离线病毒库包不大于210M。支持直接或通过代理服务器从互联网升级病毒库；支持从自己局域网内架设的HTTP、本地文件夹等方式升级病毒库；病毒库升级方式提供三种模式供选择：定期更新、预发布更新、延迟的更新；病毒库更新支持快照功能，当更新出现异常，可回滚到正常状态以保证系统稳定；

13.可检测并清除隐藏于电子邮件、公共文件夹及数据库中的计算机病毒、恶性程序、垃圾邮件；

14.支持多种加壳文件的病毒查杀、打包文件查杀（不限层数）、内存查杀、文件复制和运行时查杀；压缩文件查毒、清毒（不限层数），支持的压缩格式不少于15种；能够有效查杀各类Office文档中的宏病毒；

15.防病毒软件能够自动隔离感染而暂时无法修复的文件，并在用户许可的情况下传送至生产商；

16.至少同时支持Foxmail、Outlook、Outlook Express、Notes、Mozilla Thunderbird和Netscape等客户端邮件系统的防（杀）病毒；邮件发送、接收时检测；邮件文件静态检测以及清除；邮箱静态检测、清毒；支持跨平台的Notes群件系统防（杀）病毒产品或解决方案,并且能够支持到Domino R6版本以上；

17.★采用启发式扫描和虚拟机技术相结合，即使在病毒库未能正常

升级情况下，也能高效侦测出已知的和未知的病毒威胁,并支持族群式变种病毒的查杀；

18.防病毒产品必须拥有强大的前摄性侦测功能，是一款可以查杀病毒 DNA 的智能软件；防病毒产品在进行文件扫描时，占用资源小，针对操作系统和处理器特殊优化,扫描和杀毒速度快,不影响正常办公；

19.★防病毒产品可对操作系统的安全性进行 1-9 级的风险检测，以便用户及时掌握系统的安全风险状况，做出管控决策。投标时需要提供安全性等级风险功能的截图证明；

20.★具有可配置规则的 HIPS 功能，如具备高级内存扫描、漏洞利用阻止功能，过滤模式具备自动模式、智能模式、交互模式、基于策略模式、学习模式等五种模式可选，可授予应用程序对哪些文件、注册表部分或其它应用程序的访问权限。

21.独立的 IDS 网络防御功能,分析网络通信的内容并防止网络攻击，阻止任何视为有害的通信。

22.具有系统漏洞防护（Exploit Blocker）功能，防止因为操作系统补丁停止更新后，被恶意程序入侵。具备漏洞阻止功能，强化应用程序的安全性，例如网页浏览器、PDF 阅读器等。

23.可设置演示模式，当用户在全屏幕使用应用程序、游戏或演示时，防病毒软件的提示信息、计划任务暂停，以保证用户的演示过程不被打扰；Office/IE、邮件系统嵌入杀毒，可疑文件上报，具有垃圾邮件过滤功能；

24.支持加密的 HTTPs、IMAPS、POP3s 协议扫描；增强的 U 盘病毒查

杀能力，必要时可以阻止U盘的访问；也可以针对不同用户组，设定相应的USB使用权限；

25.具备系统救援功能，允许用户创建自启动操作系统镜像，内含防毒软件程式，能够清除隐藏很深的系统病毒。在其他方式都不能奏效时，可以通过系统救援光盘或USB盘启动终端计算机进行病毒查杀，帮助恢复系统数据。

26.产品为国际知名品牌，支持0day漏洞保护，具有自主研发的启发式扫描病毒引擎，防病毒产品必须通过VB 100测试；须提供VB100官网截图证明。

27.★获得VMwareReady认证，表明此款安全产品完全兼容VMware虚拟作业环境;获得CitrixReady认证，表明此款安全产品完全兼容Citrix 虚拟作业环境。**投标文件中必须提供相关证明材料，包含但不限于官网链接或截图等材料**

二、防统方系统维保升级项目技术标准和服务要求

版本要求 V6.10 以上，5 年免费维保，要求详见下文

性能要求：

1.吞吐量 20Gbps

2.SQL 事务数/秒 200,000

3.接口　10/100/1000M 自适应电口 *6

光纤监听接口：SPF 多模光纤，最多扩展至 4 个

4.内存　64G

5.处理器 Intel Xeon E5-2620 v4*2 双处理器

6.存储容量　标配 8*2TB 企业级 HDD （含 64M 缓存），存储周期不少于 360 天

7.性能说明满足医院五年内的防统方使用需求，不会出现性能瓶颈。

功能设计要求

1.▲管理、审计用户权限分开，相应权限的用户只能查看、管理相应的系统功能，责任明确。

2.系统内置防统方知识库,且具有独立自主统方学习功能,并取得《实用新型专利证书》。

3.支持分布式部署集中式管理。

4.应用 AI 人工智能进行分析，并生成报告和相关建议规则反馈给用户。

5.多种部署方式（串接/并接）下都可以阻断客户端进行疑似的统方行为。

6.系统支持采用旁路部署方式，不需要更改现有网络结构、服务器相关配置，系统运行不得影响现有网络和业务的正常运行。系统应能独立完成审计数据采集，不依赖于数据库自身审计日志系统，不得在现

有服务器上安装可能带来风险的程序。

7.主动/被动方式监控关键服务器的开放端口，提供扫描现有应用系统的漏洞。

8.根据客户端应用程序名单，实时阻断非法客户端程序或伪装正常客户端程序对关键服务器的访问。

9.可疑对象定位功能，可以精确定位可疑对象的物理位置。

10.分析可疑对象的信息，包括 IP、端口、MAC、主机名、程序信息、数据库连接信息。

11.系统可以监控、记录并且还原客户端连接到服务器的 TELNET/FTP 等远程登录操作信息，记录内容包括客户端 IP 地址，客户端 MAC 地址，服务器地址以及产生记录的时间，并提供多种查询，支持多种文件格式导出。

12.可根据用户自定义规则实时发出手机短信通知和邮件提醒等多种方式的告警信息，并支持配备相应的告警信息发送设备。

13.支持医院各生产系统中财务数据、病人资料、药品信息、医院资产等核心数据的审计监控。

14.系统支持双密码用户，安全性更高。

15.所有系统数据都支持加密传输，防止信息外泄。

16.系统确保最小报警监控时间间隔为 5 秒，保证统方事件的及时告警。

17.系统的时间可以和关键服务器中的数据库的时间进行同步，确保记录时间的一致性。

18.支持加密方式的数据库连接信息分析，提供产品截图。

19.支持对 Oracle、MS-SQL 、DB2、MYSQL、CACHE DB、POSTGRESQL

和 Sybase 等数据库提供自动化评估、审计和保护功能,可审计的数据库或集群数量不少于 6 个，并且可以是一个 oracle 库而另外一个是其它服务器上的 SQL 数据库。

20.支持手机 APP 告警，提供产品截图。

21.阻断可疑会话功能，甄别数据访问，阻止非正常数据会话。能根据预定规则阻断 SQL 语句的“数据库墙”功能，如根据系统设置的客户端 IP/MAC 黑名单，以及数据内容中的敏感信息，实时阻断黑名单中的客户端对关键服务器的访问

22.系统从业务流程角度入手，结合核心数据特征，提供了高度集成的“事前+事中+事后”数据防护手段，获得《信息化创新医疗服务模式》认证。

23.用户可以根据需要自定义规则，并能根据设定的条件产生审计报告。能对审计结果进行多条件组合查询，比如按下列条件查询：IP 地址、MAC 地址、表名、操作方式、计算机名、数据库名、程序名等。并就能支持按关键词进行模糊查询。查询结果应支持多种格式(excel、pdf、txt 等)导出。

24.▲支持对指定时间内全院抗菌药物品种、剂型、规格、使用量、使用金额,使用量和使用金额分别排名前 N 位的抗菌药物品种进行分析，自动生成报表，提供产品截图厂家盖章，并可现场演示及测试，保证结果满足,否则视为强行应标,做投标无效处理,并加入黑名单。

25.产品从审计主体、审计客体、日志格式、规则分析能力、报表、告警、存储等模块完全按照等级保护基本要求和测评要求设计研制，该“防统方”系统产品取得《数据库安全审计检验报告》。

26.支持指定非关注策略，系统将非关注的内容进行过滤，不进行记

录，降低了存储空间和无用信息的堆砌。策略因子包括：数据库操作来源 IP 地址、数据库登录用户名称、数据库操作源程序名称、数据库操作源终端名称、数据库操作源终端用户名称、SQL 操作语句(DDL、DML、DCL)、数据库表组（表、列）等。

27.统方白名单权限的设置，可对授权统方行为的操作人员工号、操作类型、IP 地址、客户端工具、操作系统用户名、主机名、MAC 地址、SQL 语句和操作的时间范围等条件进行设置，只有通过了授权和验证才可以获得统方权限。

28.系统配置文件支持导入、导出。

29.支持集群,系统支持冗余备份。

30.系统将预留一定的接口以作维护，二次开发之用。

31.系统内置故障排错系统，判断故障所在，帮助管理人员快速排查问题。

32.支持医院信息管理系统多层结构，提供全方位的三层（应用层、中间层、数据库层）的访问审计，三层关联必需支持自动关联，以提升关联准确度和审计人员追踪索源难度，同时需要支持手动关联，可以直接追踪到前端业务的操作人员 IP 地址、MAC 地址和用户。

33.能够检测网络拷贝等操作,能够检测通过网络 KVM 发出的指令。

34.系统应为软硬一体机，支持千兆以上网络环境及大概至少 500 个客户端同时并发的监控,应达到每秒 100000 个以上的事务处理能力。

35.采用 B/S 架构，提供中文 WEB 管理界面以便于管理。并应可以根据不同的安全级别采用不同的实时告警响应方式，包括记录、消息、鸣音、邮件等，并能支持短信平台。

36.提供数据库登录用户名称异常探测、数据库操作源终端异常探测、

数据库操作源程序名称异常探测、数据库操作源终端用户名称异常探测，可设定异常黑白名单，对客户端地址、客户端程序、数据库账号、客户端用户名以及执行结果等异常的行为进行异常告警，支持自主学习能力。

37.系统应能支持多个网段客户端对数据库操作行为的会话审计，能够对各种访问数据的途径（如客户端软件、PL/SQL、SQL*Plus、PB、Toad 等各种 SQL 操作工具）进行监控和设计，可以跟踪审计某某时间、某某 IP、某某计算机名、某某用户对数据库服务器进行了该类操作，具有可疑对象定位功能，可以精确定位可疑对象的物理位置。

38.系统应能支持对数据库 SQL 操作语句的详细审计，可以分析出每条语句的操作方式、表名、存储过程名、详细操作内容，执行时长、操作成功/失败，受影响行数，关联表与关联表数等字段信息，可审计并还原 SQL 操作语句。

39.可根据 SQL 执行的时间长短设定规则，如命令执行时长超过 30 秒进行告警；可根据返回记录数多少设定规则，如 SQL 操作返回的记录数或受影响的行数大于等于 10000 行时进行告警。

40.支持对双向数据包的解析、识别及还原，不仅对数据库操作请求进行实时监控，而且还可对数据库系统返回结果进行完整的还原，根据统方行为的特征实时告警，提供产品截图。

41.可以对某统方行为的所有操作以及操作结果关联起来，以报表的形式呈现给使用部门，便于使用部门分析和追溯统方事件。

42.▲能够出具针对纪委、监察室相关人员使用的防统方审计报告（支持每天或多天生成统方审计报告，报告需简单明了，且具有主动将所有的计算机语言翻译成通俗易懂的自然语言的系统机制，支持将整条

SQL 语句翻译成中文，帮助医院建立基于内部网络的党风廉政、廉洁警示、院内敏感职权使用的防控专网，支持对接廉政风险防控系统，具有廉政风险防控系统的《软件著作权登记证书》，提供产品截图厂家盖章，并可现场演示及测试，保证结果满足，否则视为强行应标，做投标无效处理，并加入黑名单)。

43.支持包括 ASCII、Unicode、UTF-8、UTF-16、GB2312、EBCDIC 等编码格式，避免因编码格式不同而导致审计报表出现乱码的情况，保证了审计报表的可读性。

44.系统应能对自身的事件（包括登录、系统参数修改、系统异常等）进行审计，可以监控和审计用户对数据库中的数据库表 、视图、序列、包、存储过程、函数、库、索引、同义词、快照、触发器等的创建、修改和删除等，分析的内容可以精确到 SQL 操作语句一级。

45.▲医德医风功能：提供对接医德医风系统，具有医德医风系统的《软件著作权登记证书》，提供产品截图厂家盖章，并可现场演示及测试，保证结果满足，否则视为强行应标，做投标无效处理，并加入黑名单。

46.审计数据应能永久保存，并支持外接存储设备进行备份。数据应进行加密保管，只能通过专门工具进行恢复和查询浏览。

47.为了增加产品的登录认证安全性，必须具备双因素登录认证的功能，必须支持 USBKey 登录方式。

48.支持以下配置：

48.1 吞吐量：12Gbps。

48.2SQL 事务数/秒：120,000。

48.3 接口：10/100/1000M 自适应电口*6；支持光纤监听接口：SPF

多模光纤,可扩展。

48.4 存储容量：设备数据存储周期需满足《中华人民共和国网络安全法》和《信息安全等级保护管理办法》180 天的要求。

48.5 性能说明：需满足医院五年内的防统方使用需求，不会出现性能瓶颈。

其他

1、 系统免费升级与维护期为伍年(一次性招标五年吗)；

三、医保系统维保升级项目技术标准和服务要求

1.系统总体要求

为完成人社部门要求的医保系统接口改造和日常维护，完善现有住院收费系统，拟实施住院收费管理系统和医保系统接口改造以满足医院医保系统与HIS系统无缝链接，实时报销，简化报销流程等优化，提高结算工作效率，减轻收费室和医保科工作量。要求实现医院现有HIS系统与医保系统无缝连接，日常维护和升级改造过程中必须确保现有系统数据准确一致，账目清晰。

2.关键功能要求

功能模块	功能	描述
门诊收费	卡识别	★1）卡和身份识别管理，密码修改，支持读卡和身份证模式
	参保待遇查询	1） 参保个人待遇查询。 2） **门诊慢性病待遇资格信息查询**
	门诊收费	★1）支持门诊普通、慢病等病人医保实时结算。
	门诊退费	★1）支持门诊普通、慢病等病人医保实时退费结算。
住院结算系统	住院结算	1）住院结算系统升级和上线期间，确保现有系统平稳运行。
		3）支持病人费用查询多种方式统计。
		4）支持结算数据多种方式统计。
	医保补登记管理	★1）实现现有医保补办、取消医保登记。
		★2）实现现有医保费用上传，取消费用上传、审核、结算功能。
		3）结算单补打印功能。
医保接口系统	医保接口管理	★1）满足医保规范要求，进行基础数据的下载和匹配管理，对账要求。

	系统	★2）满足医保银海接口规范，进行基础数据的下载和三大目录导出功能，科室、医生信息上传管理。
		3）根据人社要求进行对账管理。
其他	日常维护	1）维护医院医保系统正常稳定运行。 2）根据医保政策变化，对相关程序功能进行维护。 3）根据工作需要调整报表。

四、HIS 系统 ORACLE 数据库维保升级项目技术标准和服务要求

1. 技术服务的目标：保障招标方 HIS 系统 ORACLE 数据库的正常安全运行

2. 技术服务的内容：

a) 技术维护服务

b) 数据库性能优化服务

c) 现场巡检（每年四次）

关键技术指标：

指标项	**指标要求**
维保数据库	HIS 系统 Oracle 数据库技术服务及 TRUST DBRA 容灾系统维护
7×24 小时远程支持服务	对数据库系统故障或与数据库系统相关联的系统故障，投标方提供 7*24 小时不间断非现场(包括：400 电话、e-mail、VPN、QQ 等多形式)支持服务，通过以上方式直接联络服务商的技术工程师，寻求问题的解决方案、技术文档以及技术指导，提供故障处理方案。远程支持响应时间：15 分钟。
7×24 小时现场应急响应支持服务	在整个服务期内，用户数据库发生对业务产生重大影响的数据库层面问题，需调派工程师，第一时间赶往客户现场，确保客户的系统尽快恢复，对于紧急响应的服务次数和服务时间不作限制。 如果确定问题是在数据库层面上，技术人员需要跟进到问题解决为止，对于非数据库系统造成的问题或问题目前缺少有效的解决方法（指数据库软件本身的 BUG 或内核级故障），技术人员需要确定问题的原因，

	评估改进的风险和代价，并提供完整的解决建议方案。 现场支持时间：3 小时以内到达现场支持。
▲数据库巡检服务	定期执行一次全面的现场数据库巡检服务：主要包含错误日志管理，性能管理，空间管理，对象管理，安全管理，备份管理等方面内容。数据库巡检工作由现场检查和系统数据分析构成，最终提供一份内容详尽的数据库巡检报告。数据库检查的内容至少包括以下部分： 1.检查相关软硬件、数据库配置和 SGA、PGA 的配置情况 2.检查数据库、备份结果集、各表空间的变化情况等，并对数据变化情况作评估 3.统计当前表空间、文件系统和数据文件的使用情况 4.检查数据库 alert.log 日志文件和相关 trace 文件 5.检查操作系统用户、数据库用户、系统本身的安全性 6.收集数据库运行期间的负载情况和 Instance 各性能指标 7.检查数据库备份是否正常 8.操作系统错误告警 9.操作系统实时性能监控 数据库巡检服务周期：3 个月 1 次，1 年共 4 次
▲数据库性能优化服务	性能优化以业务程序的响应时间为主要指标；若当前业务压力不大的前提下，需要进行性能优化，也可以定义 OS 开销指标，ORACLE 命中率指标，AWR 报告数据来实施。性能调优服务需要从以下几方面出发进行性能诊断和调整： 1.内存资源冲突

	2.IO 资源冲突 3.CPU 开销资源冲突 4.回滚段资源冲突 5.临时段资源冲突 6.数据“热”块资源冲突 7.索引效率低下 8.SQL 语句调整 9.可能影响数据库性能的其它方面。
★数据库容灾服务	1.实现所有数据库内的数据操作的复制，包括 INSERT\UPDATE\DELETE、DDL 操作、Create table..as 语句，ROWID 相关语句等。 2.实现所有数据库内的所有对象复制，包括普通表格、压缩表格、临时表格、垃圾箱内的闪回表格等。 3.要求两个库之间的所有对象完全相同，包括 ROWID，基表，视图，同义词，自定义 TYPE，IOT 表格，SYS 用户内的所有对象等。 4.要求支持误操作闪回服务，支持使灾难备份回到过去的某一时刻点，实现误操作等逻辑错误的灾难恢复。 5.要求采用物理同步方式，无需考虑复杂的内部数据关系，支持数据库中所有对象的同步，支持所有 DDL、DML 等语句的复制。 6.实现短时间内（比如 30 分钟的硬件升级）的计划性维护切换以支持日常运行涉及时间比较长的运行维护操作，实现从生产系统切换至容灾系统，从容灾系统切换回生产系统系统。支持一键式切换管理。 7.要求提供容灾系统桌面演练服务，能够在“沙盘”环境中模拟整个容灾切换过程，桌面演练可以在生产系统业务高峰期间进行，不增加生产系统额外资源开销（包括 CPU\内存\IO），不影响业务的继续运行。

	8.提供可视化、直观化、前台界面可操作的WEB管理过程，支持一键切换（一键启动、一键关闭），不需要复杂的流程即可完成容灾切换。 **注：以上要求需提供相关证明材料并盖章。**
服务人员要求	1.配备一名技术总监。负责项目服务中重大故障或疑难杂症等问题的协助处理，提供优质的二线支持服务。 2.至少安排两位专职责任OCM数据库工程师,采用A/B岗方式，提供固定服务响应支持。 以上服务人员需提供资质证明文件并盖章。