广州医科大学附属市八医院
诚邀供应商参与信息安全建设项目市场调研的公告

一、项目基本情况

项目名称：**信息安全建设项目**
最高限价：331万

采购需求：

按照《GB／T22239-2019 信息安全技术网络安全等级保护基本要求》等信息化标准要求，开展医院信息安全体系建设，提升医院信息系统安全等级水平，贯彻落实《网络安全法》的要求。

健全信息系统安全管理制度，不断深化信息安全保障体系建设，推动信息安全工作的贯彻落实。

提升医院信息安全管理水平，强化信息安全防御能力，加强信息安全应急处置能力。

建设医院网络信息安全空间，主动应对各类信息威胁，减少信息安全事件的发生机率及影响程度，为医院业务不断发展保驾护航。

详见需求文件。

二、供应商的资格要求

1、符合《中华人民共和国政府采购法》第二十二条所规定的条件；
2、有项目相关成功案例；
3、本项目不接受联合体投标。

三、获取采购文件

获取方式：医院官网下载。

四、报名文件提交

时间：2021年07 月 23日至 2021年 07月29日。

地点：广州市白云区华英路 8 号广州医科大学附属市八医院教学楼 3 楼信息科。

报名文件提交：报名需提供投标联系人和电话,三证合一营业执照的电子文件,信用证明,资质文件,发送电子邮件到 19282644@qq.com。

五、采购谈判时间

时间：具体时间邮件通知。

地点：广州市白云区华英路 8 号广州医科大学附属市八医院教学楼（具体地点以邮件通知为准）。

六、公告期限

自本公告发布之日起5天。

七、其他补充事宜

报名联系方式：电子邮件
项目联系人：孟工

报名截止日期：2021年 07月 29 日 17:00

广州医科大学附属市八医院

2021年信息安全建设项目需求

项目名称：广州医科大学附属市八医院 2021 年信息安全建设采购项目

项目预算：331 万元

项目需求

1.1.项目概述

1.1.1.项目名称

项目名称：广州医科大学附属市八医院 2021 年信息安全建设采购项目

1.1.2.项目背景

2017 年 6 月 1 日《中华人民共和国网络安全法》正式实施，第三章明确了“关键信息基础设施的运行安全”要求，网络安全上升到国家安全战略重要位置。2003 年中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）明确指出，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。2011-2015 年卫生信息化发展规划当中，“加强安全体系建设”作为“十二五”期间卫生信息化建设总体架构中的重要任务，体现国家及监管部门对医疗信息安全体系建设的重视。

随着《GB／T22239-2019 信息安全技术网络安全等级保护基本要求》在 2019 年 5 月 10 日发布，等保进入 2.0 时代。“等保 2.0”将网络安全从单纯强调防护，转变到注重预警、检测、响应的格局，安全能力从“防范”为主转向“持续检测和快速响应”，实时防御将以威胁为中心，以数据为驱动解决安全问题。

国家卫生健康委办公厅于 2020 年 2 月 3 日发布的关于“国家卫生健康委办公厅关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知”中明确要求要加强基础和安全保障，其中重点做出以下两条指示：

1. 加快基础网络升级改造，保障医疗信息系统平稳运行，确保疫情防控指挥体系稳定畅通。

2. 加强网络信息安全工作，以防攻击、防病毒、防篡改、防瘫痪、防泄密为重点，畅通信息收集发布渠道，保障数据规范使用，切实保护个人隐私安全，防范网络安全突发事件，为疫情防控工作提供可靠支撑。

因此，广州医科大学附属市八医院需要贯彻国家及行业要求，不断完善医院信息安全保障体系，建设医院网络安全空间，降低信息系统所面临的风险，确保医院各大信息系统安全稳定的运行。

1.1.3.建设目标

按照《GB / T22239-2019 信息安全技术网络安全等级保护基本要求》等信息化标准要求，开展医院信息安全体系建设，提升医院信息系统安全等级水平，贯彻落实《网络安全法》的要求。

健全信息系统安全管理制度，不断深化信息安全保障体系建设，推动信息安全工作的贯彻落实。

提升医院信息安全管理水平，强化信息安全防御能力，加强信息安全应急处置能力。

建设医院网络信息安全空间，主动应对各类信息威胁，减少信息安全事件的发生机率及影响程度，为医院业务不断发展保驾护航。

1.2.项目建设内容

A. 边界防火墙功能需求

序号	功能项	功能需求
1.	硬件平台	▲产品采用多核并行处理架构，提供中国信息安全测评中心、公安部信息安全产品检测中心、中国软件评测中心、国家版权局之中任意一家机构出具的关于“多核并行安全操作系统”的证书或测试报告。
2.	硬件规格与性能要求	★网络层吞吐≧6Gbps，应用层吞吐量≧2Gbps，并发连结数≧180W，新建连接数（CPS）≧6W；硬件参数≧1U，内存≧4G， SSD≧64G，接口数量≧6个千兆电口+4个千兆光口。为保证威胁统一管理与运维便利性，要求和态势感知系统为同一品牌，能够接入本项目的态势感知平台，并能够对平台监测发现的威胁进行自动化联动封堵，实现动态防御。（需提供产品功能截图证明并加盖原厂公章）
3.	部署方式	支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。
4.	路由功能	具备静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议。
5.		支持基于IP地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。
6.	地域访问控制	支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。
7.	流量控制	▲具备基于国家/地区的流量管理功能，提供具备CNAS（中国合格评定

		国家认可委员会）资质的第三方权威机构关于“国家/地区的流量管理”产品功能检测报告。
8.	DDoS防御	支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。
9.	入侵防御	产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则。
10.		具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。
11.	蜜罐联动	▲产品支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危IP。需提供产品功能截图证明，并提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“云蜜罐”的证书或检测报告证明功能有效性。
12.	网端云联动	▲具备网端云协同联动功能，提供具备CNAS（中国合格评定国家认可委员会）资质的第三方权威机构关于“网端云协同联动”产品功能检测报告。
13.	策略生命周期管理	支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。
14.	产品资质	▲要求所投产品具备EAL3+证书，提供有效证书复印件。
15.		要求所投产品具备国家信息安全漏洞库兼容性资质证书，提供有效证书复印件。
16.	原厂支持	▲提供3年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。需要提供产品原厂商针对本项目的授权函及售后服务承诺函，并加盖原厂公章。

B. 区域流量汇聚设备功能需求

序号	功能项	详细描述
1.	配置要求	★标准19英寸1U机架式结构（必须提供截图或拍照证明）。支持4个SFP+的万兆接口(兼容千兆)和24个SFP 千兆接口（需提供产品功能截图证明并加盖原厂公章）。支持一个10/100/1000M自适应带外管理端口及一个串口CONSOLE管理接口。设备支持交流220V或直流-48V供电，配置双电源冗余供电。
2.	功能要求	接收交换机镜像端口或分光采集器的10GE/GE接口输出的克隆数据，对接收的数据进行复制、汇聚、过滤、处理并从万兆端口输出给后端分析设备。 设备的所有端口均可以灵活配置为输入输出，可以设置为1:N、M:N、N:1等模式。 可根据数据报文特征，对采集流量进行有效过滤，只将满足条件的流量分发给后端分析工具。 设备基本管理功能。支持本地管理功能；支持通过远程登录方式进行管理；必须支持HTTP WEB界面完成系统支持的所有功能配置，同时支持基于SSH或TELNET命令行方式的远程管理功能； 设备10GE端口线速流量不丢包（64字节到1518字节）。 设备应支持7*24小时的稳定运行，整机处理性能不低于64Gbps
3.		前面LED状态指示灯支持当前状态的显示，如system状态，Power状态，每个业务端口的连接状态等。 可通过WEB图形方式查询端口状态，并在端口上进行性能统计，支持对任一接口当前流量曲线图实时展现；接口性能统计至少包含当前发送报文数、当前接收报文数、当前发送字节数、当前接收字节数、接口当前发送/接收速率、接口峰值发送/接收速率等统计指标。 设备支持以面板图形式直观展现前面板所有接口的LinkUP/LinkDOWN状态、接口字符串描述、接口当前速率、SFP模块插入/拔出状态，接口当前发送/接收报文计数等信息。 设备集中管理平台功能。设备应支持统一集中管理平台进行集中管理，提供统一的采集拓扑视图展现，提供接口状态、流量速率的集中查看与实时监控，支持链路状态异常的声光告警。

		设备在配置任意输入输出策略及规则时均可达到64字节小包线速不丢包性能。 系统应支持基于WEB的配置文件的导入和导出功能。 系统应支持基于web方式的远程在线升级功能。 设备基本管理功能：系统应支持本地日志记录和syslog服务配置。系统应支持SNMP V1/V2/V3协议管理。
4.		支持单纤输入输出及复用功能。即光接口在仅插入接收方向单纤时能够成功Link并采集流量，在端口通过单纤输入采集流量时同时能够通过同一端口单纤输出流量； 端口健康检测功能：支持实时检测后端监控分析设备的服务进程健康状况，当服务进程出现故障时，自动移除故障设备，以保证多端口负载均衡时的可靠性。 数据类型。支持VLAN 封装及MPLS封装的数据转发。支持透明转发以太网控制帧及BPDU流量。 基本流量复制汇聚功能。可将采集的一路或多路网络流量进行复制并分发给不同的工具处理；可将通过不同网络端口采集的网络流量进行汇聚，并分发给单台工具处理；可将采集的多路网络流量进行汇聚之后同时复制成多份输出给不同的工具处理。 流量过滤输出。可根据数据报文特征，对采集流量进行有效过滤，只将满足条件的流量分发给后端分析工具，其过滤条件应支持以下维度： 支持基于报文采集来源端口、五元组标准协议域、源/目的MAC地址、IP碎片标记、传输层端口范围、以太网类型字段、VLANID、TCPFlag、数据包长度、固定偏移特征等对流量进行分类过滤转发。 过滤条件支持一个或多个条件灵活搭配组合的配置模式。 单台设备需支持不少于2000条过滤规则。 在配置基于规则的过滤采集输出时，规则条数不影响系统性能，均能达到64字节小包线速处理能力。 输出处理功能：支持对分类流量进行各种策略的负载均衡分发，需至少支持以下四种： 支持哈希分流负载均衡方式输出。 支持基于过滤规则的报文分类输出。

		支持输出报文打VLAN标签功能。 支持对输出报文替换源MAC、目的MAC之后输出。 IPV6规则支持。设备应支持IPV6地址、协议号、IPV6流标签等IPV6报文的规则进行分类过滤。 动态负载均衡在执行分流负载均衡输出时，在同一端口组内的任一端口失效（DOWN）后支持将流量自动分配至组内其它正常（UP）端口，不需要人工干预重配置。 Span镜像端口隔离功能。在端口被配置为镜像输入采集模式时，各镜像输入端口之间应互相隔离，避免产生环路。
5.	质保要求	需要提供产品原厂商针对本项目的授权函及售后服务承诺函，并加盖原厂公章。提供3年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。

C. 外网日志审计平台功能需求

序号	功能项	功能需求
1.	产品资质	1. 提供产品的《计算机软件著作权登记证书》 2. 国家公安部计算机信息系统安全专用产品销售许可证； 3. 通过国家保密局涉密信息系统产品认证； 4. 国家网络安全测评中心产品3C认证证书
2.	产品结构	无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁；
3.	产品架构	▲采用标准2U**机架式硬件**，深度定制化Linux内核+Busybox，系统独立运行在1024M的SD卡中，系统运行不依赖于硬盘（需提供产品功能截图证明并加盖原厂公章）
4.	管理方式	B/S方式，采用HTTPS方式远程安全管理，无需安装管理客户端；
5.	接口	标配4个千兆电口，一个扩展插槽，可升级扩展为万兆光口或千兆光口。
6.	设备部署	提供旁路接入模式，设备部署不影响原有网络结构；
7.	数据存储	1. 所供系统设备必须自带本地存储功能； 2. 提供基于海量日志专用存储的文件系统著作权证书，禁止采用通用关系型数据库来存储日志；（提供乾坤文件系统证明文件） 3. 物理磁盘空间：2*4TB；RAID架构以保证数据可靠性； 4. 日志存储数量压缩比后不低于40亿条
8.	处理性能	日志采集能力：10000条/秒以上 不限主机日志采集源数量许可限制（需提供产品功能截图证明并加盖原厂

		公章）
9.	日志数据采集类型	1. 支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神]、AS400日志、[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、Glftpd、Serv-u]；
10.		2. 支持SNMP日志采集，支持日志类型：网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、深信服、网神] 3. 支持Opsec Lea日志采集；（需提供产品功能截图证明并加盖原厂公章） 4. 支持文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览、论坛微博]、入侵检测、业务检测、流量监控； 5. 支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储； 6. 支持文本型日志原始文件管理，可将系统作为日志服务器使用； 7. 审计系统支持以syslog、snmp trap、opsec lea、WMI等标准协议接口采集各类日志数据； 8. 审计系统自动将采集的操作语句解析为查询、增改、删除、过程等类型呈现； 9. 审计记录包括行为发生时间、员工工号、操作终端主机名及IP地址、终端工具名称、服务器端主机名及IP地址、数据库名、表名、SQL语句、返回结果等关键信息。 10. 提供工号信息接口，将数据库操作语句与操作者工号建立关联关系，实现操作者实名认证；（需提供产品功能截图证明并加盖原厂公章） 11. 审计系统能够对未经许可的客户端工具直接访问数据库的行为实施阻断；（需提供产品功能截图证明并加盖原厂公章） 12. 支持配置操作行为解析模型（黑白名单），灵活区别正常操作和异常操作事件； 13. 支持依据语句解析模型，以操作频率为条件实施行为阻断； 14. 支持将可疑的数据库查询语句以在线的方式反显执行，并即时在线查看返回结果； 15. 支持将异常操作的完整会话信息进行前后操作语句关联查看分析；

		16. 支持分中心部署方式，能够配置分支数据集中上传至中心机；
11.	监控功能	1. 支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况； 2. 支持自定义配置实时监控的日志类型； 3. 支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警； 4. 支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况； 5. 支持实时监控系统当前运行状态，包括系统CPU、内存、硬盘状态及管理员操作；
12.	报表分析功能	1. 系统内置多种类报表模板； 2. 支持动态\静态（日报、周报、月报）两种系统生成方式； 3. 支持报告的邮件转发、生成提醒功能；支持多人邮件接收； 4. 支持自定义审计报告； 5. 支持导出html、Excel、PDF； 6. 支持管理员自定义审计报表模板；
13.	查询分析功能	1. 支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索； 2. 支持以日志类型、时间范围及条件字段快速检索过滤； 3. 支持高级检索以多条件组合查询方式，可以将每一个日志字段作为查询条件进行查询； 4. 支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件； 5. 支持查询模版创建、修改、删除功能； 6. 支持查询结果导出； 7. 支持海量日志数据高性能查询分析行为审计分析引擎，（提供相关国家级产品技术证明并加盖原厂公章）
14.	策略管理功能	1. 支持内置归并策略，对HTTP数据进行自动归并处理； 2. 支持内置关联分析策略，可设定用户在规定时间内连续多次输入错误口令产生告警或事件； 3. 支持数据策略，可设定采集多种WEB访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问； 4. 支持自定义创建实时审计规则：根据日志字段为条件预设置分析策略； 5. 规则条件设定支持逻辑运算符与支持正则表达式； 6. 支持自定义三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息；（需提供产品功能截图证明并加盖原厂公章）

		7. 支持以告警页面、短信、邮件、SYSLOG、SNMP等各种方式呈现告警信息；
15.	数据管理功能	1. 支持按日志属性、日志类型、时间范围等进行数据备份；（需提供产品功能截图证明并加盖原厂公章） 2. 支持WEB界面备份及日志恢复导入工作； 3. 支持自动与手动两种备份归档方式； 4. 系统支持以FTP上传方式将归档文件存储到第三方存储系统中；
16.	系统配置功能	1. 支持审计系统用户（组）管理（添加、修改、删除、停用、启用）； 2. 支持资产管理，即所有采集日志源管理维护； 3. 支持密码长度、复杂度，密码猜测自动锁定账号以及系统超时设置安全策略； 4. 支持证书页面生成下载； 5. 支持系统配置备份恢复； 6. 支持时间同步页面配置； 7. 支持页面方式系统升级以及设备关闭、重启； 8. 支持从WEB界面查看网卡IP设置，修改静态路由设置等内容； 9. 支持安全页面（SSL）证书下载；
17.	系统自身安全	1. 系统内置安全防火墙；支持控制访问审计主机范围； 2. 必需提供内部通讯检查机制，传输 128 加密； 3. 管理接口支持串口或电口的方式管理； 4. 管理界面与其他功能模块分离；
18.	日志数据安全	1. 审计日志文件方式存储； 2. 审计日志加密导出审计系统； 3. 支持对所有审计管理员操作审计系统的动作进行审计；
19.	日志权限	1. 审计员只限于操作权限设置范围内的日志数据 2. 支持日志类型、IP 地址权限设置； 3. 支持页面功能模块权限设置；
20.	系统许可方式	永久许可方式，再增加审计用户的情况下不用增加授权许可；
21.	售后服务	▲提供3年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。

D. 动态令牌功能需求

序号	功能项	功能需求

1.	授权要求	在医院现有的内外网堡垒机增加动态口令模块，用于现有的内外网堡垒机登录认证，满足双因素认证要求。

E. 态势感知平台功能需求

序号	功能项	功能需求
1.	性能指标	★采用x86架构，尺寸≧1U， 内存≧32G，系统盘≧SSD 128G、SATA存储 ≧16T，接口数量≧6个千兆电口；为保证态势感知平台功能的有效性，要求与态势感知平台与态势感知探针为同一品牌。
2.	全网安全态势大屏可视	▲支持不同视角展示全网安全威胁分析，包括综合安全威胁分析、分支安全威胁分析、安全事件威胁分析、网络攻击威胁分析、外连风险威胁分析、横向威分析、脆弱性威胁分析、资产威胁分析、正常横向访问监控威胁分析、正常外连监控威胁分析、设备运行威胁分析等15个以上独立的大屏展示功能；支持大屏轮播，可自定义播放顺序（需提供产品功能截图证明及第三方检测机构证明，并加盖厂商公章）。
3.	横向威胁态势	支持大屏展示横向威胁态势，包括业务与终端访问、发起威胁终端TOP5、遭受威胁业务TOP5、访问趋势图；支持不同颜色标注横向攻击、违规访问、可疑行为、风险访问等行为；
4.	脆弱性态势	▲支持大屏展示业务脆弱性态势，包括漏洞风险态势、漏洞类型TOP5、高危漏洞TOP5、业务总览、脆弱性业务TOP5、实时脆弱性监测；（需提供产品功能截图证明及第三方检测机构证明，并加盖厂商公章）
5.	分支权限管理	支持总部管理员查看全局的安全信息，支持页面跳转各个分支的独立管理页面。
6.		支持自定义分支管理权限，分支管理员具备独立的管理页面，只能管理和查看所属分支的业务和终端资产的安全信息且具备完整的功能展示。
7.	资产全生命周期管理	支持资产多级分支管理，最多可至15级分支，支持资产全生命周期自动管理，包括资产自动发现、多级资产、资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等.
8.	资产发现	支持通过主动发送微量包的扫描方式探测潜在的服务器（影子资产）以及学习服务器的基础信息，资产指纹信息包括资产类型、端口、操作系统、mac地址、主机名等。
9.		支持跨三层取mac地址，识别资产mac地址，并能够解决不同资产IP冲突

		问题，以及DHCP场景IP变更的问题。
10.	弱密码检测	支持检测15类以上常见协议的弱密码，包括FTP、LDAP、VMWARE、ORACLE、REDIS、Elasticsearch等协议，检测信息包含账号、密码、服务器、所属分支和业务、类型、最近发现时间等；支持筛选管理员账号与是否登录成功，并支持导出弱密码报告；（需提供产品功能截图证明及第三方检测机构证明，并加盖厂商公章）
11.	漏洞分析	支持流量实时识别漏洞分析，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP等操作系统、数据库、Web应用等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告。
12.	Webshell检测	具备基于AI的webshell通信流量检测，可检出加密（如冰蝎）的通信流量。，具备650+webshell规则检测，且覆盖webshell整个攻击阶段检测，包括webshell上传点探测、webshell上传下载、webshell通信。
13.	事后异常行为检测	具备元数据行为分析引擎：httpflow、dnsflow、adflow、icmpflow、maillflow等, 通过异常行为分析，结合各类机器学习算法完成未知威胁检测。包括：内网穿透、代理、远控、隧道、反弹shell等事后检测场景。
14.	挖矿专项检测	▲支持挖矿专项检测页面，具备挖矿攻击事前、事中和事后全链路的检测分析能力，综合运用威胁情报、IPS特征规则和行为关联分析技术，如检测发现文件传输（上传下载）阶段的异常，对挖矿早期的准备动作即告警。（需提供产品功能截图证明并加盖原厂公章）
15.	第三方日志关联分析可视	▲支持第三方安全日志关联分析结果的可视化展示。包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供每一台设备专项分析的页面。如防火墙外部攻击场景分析、VPN账号异常场景分析、Windows服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析。 （需提供产品功能截图证明并加盖原厂公章）
16.	日志检索	支持安全检测日志、审计日志、第三方日志存储；日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS攻击、邮件安全、文件安全、网络流量、DNS、HTTP、用户、数据库、文件审计、POP3、SMTP、IMAP、LDAP、FTP、Telnet等。（需提供产品功能截图证明并加盖原

		厂公章）
17.	主机行为EBA分析	▲支持利用EBA技术进行资产的行为分析，对这些对象进行持续的学习和行为画像构建，以基线画像的形式检测异于基线的异常行为作为入口点，结合以降维、聚类、决策树为主的计算处理模型发现异常用户/资产行为。共含有19种异常行为学习模型；并支持用户对EBA基线进行自定义调整，优化模型。（需提供产品功能截图证明并加盖原厂公章）
18.	告警消减	支持多维度模糊聚类算法将大量外部攻击日志聚合成少量攻击事件，聚合维度包括攻击IP、攻击地址、攻击目标和目标手法。
19.	实战攻防中心	具备实战化攻防中心，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面梳理暴。实战阶段的实时攻击分析，实时展受害者IP、攻击者IP、XFF、攻击结果、攻击次数、事件类型、威胁等级、联动响应、状态码、确定性等级等20个以上类型。实战阶段的全过程可视溯源分析、总结阶段的值守报告等全过程流程。（需提供产品功能截图证明并加盖原厂公章）
20.	威胁情报共享	▲支持云端与本地威胁情报共享，实时收集同步攻击者IP，并详细展示情报列表，包括IOC、区域、来源、更新时间、剩余封锁时间、状态、操作等，并可对本地威胁情报及云端威胁情报联动同品牌防火墙实现自动封锁。（需提供产品功能截图证明并加盖原厂公章）
21.	溯源中心	支持自动化溯源，可自动化复现受害者从最开始的遭受攻击到权限维持各个阶段的黑客行为，包括攻击入口溯源。支持基于可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，能够直观的看到失陷主机的威胁影响面，同时基于列表模式展示攻击、违规访问、风险访问、可疑行为、正常访问等详细信息。 支持攻击溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息。（需提供产品功能截图证明并加盖原厂公章）
22.	全网安全态势报告	可快速生成月度、季度、年度PPT报表，包括网络安全整体解读、网络安全风险详情、告警及时间响应盘点等，帮助用户高效汇报，体现安全工作价值。
23.	告警推送	告警方式支持邮件告警、短信、微信告警方式。（需提供产品功能截图证明并加盖原厂公章）
24.	合规自检工	支持同品牌防火墙、上网行为管理等设备的配置核查并上报结果，提供

	具	自动化监测和配置引导。 （需提供产品功能截图证明并加盖原厂公章）
25.		▲支持对等级保护建设整改过程中系统定级、差距评估、备案、整改、测评过程中产生的文档结论进行统计归档，并使用可视化的统一界面进行展现与管理，最大程度发挥安全措施的保护能力；（需提供产品功能截图证明及第三方检测机构证明，并加盖厂商公章）
26.		支持已合规基线管控业务安全，实时监测等保差距项和高风险项，避免策略变更导致不合规，有效应对网监不定期抽查和复测场景。
27.	设备管理 接入设备管理	支持流量探针统一升级管理，支持监控流量探针与安全组件的运行状态，包含日志传输模式、日志传输量、最近同步信息等。
28.	管理员角色	支持管理员账号的新增、删除、启用、禁用等，支持免登陆及单点登录设置，支持可信IP设置。支持角色的管理范围及页面权限的收敛设置。支持系统管理员、安全保密管理员和安全审计员三个管理员角色。
29.	漏洞管理	需提供客观的漏洞修复优先级指导，不能以漏洞危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度
30.	威胁管理	实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件
31.	事件管理	▲基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案（需提供产品功能截图证明并加盖原厂公章）
32.	产品资质	要求具备公安颁发的安全管理平台销售许可证
33.		要求具备ISCCC中国国家信息安全产品认证证书
34.	厂商资质	厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位；
35.		▲厂商需是中国反网络病毒联盟ANVA成员单位；
36.	售后服务	▲提供3年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。需要提供产品原厂商针对本项目的授权函及售后服务承诺函，并加盖原厂公章。

F. 态势感知探针功能需求

序号	功能项	功能需求
1.	性能指标	★采用x86架构，性能指标≧2Gbps，硬件指标≧2U，SATA ≧1T，接口数量≧6个千兆电口+2个万兆光口；为保证系统管理与运维便利性，要求态势感知探针与态势感知平台同一品牌，日志统一分析展示。
2.	基础检测功能	具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意UR监测模式，可完成模式匹配并生成事件，可提取URL记录和域名记录。
3.	网站攻击检测	支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞等网站攻击检测
4.	敏感信息检测	▲支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤（需提供产品功能截图证明并加盖原厂公章）。
5.	漏洞利用攻击检测	支持Database漏洞攻击、DNS漏洞攻击、FTP漏洞攻击、Mail漏洞攻击、Network Device、Scan漏洞攻击、System漏洞攻击、Telnet漏洞攻击、Tftp漏洞攻击、Web漏洞攻击等服务漏洞攻击检测
6.		支持Application漏洞攻击、File漏洞攻击、Scan漏洞攻击、Shellcode漏洞攻击、System漏洞利用攻击、Web Activex等客户端漏洞攻击检测
7.		支持FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、VNC等协议暴力破解检测
8.	异常流量检测	支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等
9.		支持ICMP、UDP、SYN、DNS等协议外发异常流量检测，支持自定义阀值。
10.	僵尸网络行为检测	支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测。
11.	高级检测	支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求

12.		支持传输协议审计日志，包括https协议日志、http协议审计日志、DNS协议审计日志、邮件协议审计日志、SMB协议审计日志、AD域协议审计日志、WEB登录审计日志、FTP协议审计日志、Telnet协议审计日志、ICMP协议审计日志、LLMNR协议审计日志
13.	违规访问检测	支持IP，IP组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式
14.	抓包分析	支持流量抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式
15.	售后服务	提供3年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。

G. WEB防篡改系统功能需求

序号	功能项	功能需求
1.	授权要求	★本次采购现有WEB应用防火墙中4个应用系统防篡改保护授权，支持Linux及Windows操作系统。
2.	适配操作系统	防篡改节点支持主流的Linux、Windows；
3.	适配Web服务器	兼容所有类型Web服务器，如IIS、Apache、IBM http server、WebSphere、WebLogic、Tomcat、Jboss、Resin等
4.	数据库	兼容所有数据库类型，如MSSQL，Oracle、Sybase、Informix、DB2、MySQL等
5.	虚拟化环境	支持主流的虚拟化平台Vmware、KVM、Openstack等虚拟化平台
6.	IPv6/IPv4双栈支持	管理端支持IPv6/IPv4配置和运行、通信；
7.		防护节点支持IPv6/IPv4配置、运行、通信；
8.		管理端与防护节点间的通信均支持IPv6/IPv4。
9.	防篡改能力	支持操作系统底层驱动方式（内核态）和增强型事件触发方式的双防篡改引擎
10.		支持针对目录、子目录、任意文件类型的篡改检测和阻断
11.		支持增、删、改、重命名、修改属性等篡改行为的检测和阻断

12.		支持断线下篡改检测和阻断
13.		支持大规模连续篡改攻击的防护
14.		支持非法上传的检测和阻断
15.		支持实时检测篡改和实时阻断篡改行为
16.	策略配置	支持以信任进程方式允许网站正常更新，并可自定义信任进程的生效时间。
17.		支持对多台服务器分组进行防篡改策略
18.		排除目录功能（管理平台服务器组内支持配置排除目录，只对linux内核态和windows节点生效，可实现对保护目录下的部分子目录不进行防护。）
19.		支持多台服务器防篡改策略的一键批量启用和一键批量停用
20.	备份恢复	支持全量备份和增量备份
21.		支持网站备份过程自动化，即跟随网站的正常更新而同步更新备份目录
22.		支持对备份目录自我保护功能。 （linux内核态和windows节点对配置的备份目录进行保护，不允许对备份目录进行任何篡改操作。）
23.		支持自动恢复
24.	兼容所有第三方发布系统	支持兼容各类第三方发布系统，而且不改变原有网络结构和发布逻辑；
25.		支持以信任进程和信任进程生效时间的方式允许网站更新；
26.		支持定义网站更新时间，支持周期时间方式和指定日期时间方式；
27.		支持多时间段设置网站更新时间；
28.		支持一键启停服务器组中所有节点的防护；
29.	服务器节点深度集中管理	支持多台服务器防护节点集中管理、配置
30.		支持多台服务器防护节点一键批量激活，集中取消激活
31.		支持多台服务器防护节点一键批量升级
32.		支持服务器组的灵活变更，实现服务器组间防护节点的一键转移和移出
33.		支持多服务器节点的多层级管理，支持多节点划分到防护群组、管理域等多业务层级进行管理
34.	服务器节点状态集中展示和	支持由管理平台统一展示所有防护服务器自身的状态信息，如IP、名称、操作系统、内存、CPU、磁盘使用情况等。

35.	查询	支持由管理平台统一展示所有防护节点状态信息，如版本、在线状态、所属组、策略状态等。
36.		支持对当前系统存在可升级的节点及其数量的展示
37.	告警日志	支持对篡改事件进行详细的告警，内容包括服务器IP、所属组、告警时间、状态、篡改进程、篡改操作类型等
38.	系统审计日志	支持详细的系统操作日志的记录，包括系统的登录、退出、升级、修改策略等所
39.		支持按照时间、登录IP、账户、时间、角色、结果等对操作审计日志进行查询。
40.		支持详细的状态审计日志的记录，包括系统或服务器节点所有的运行状态相关的事件记录
41.	邮件通知	支持篡改告警的邮件通知，支持发送邮件服务器自定义
42.		支持根据邮箱绑定的账户下所管理的服务器节点、服务器组、管理域来定义所发送的篡改告警日志范围
43.		支持根据指定时间间隔来定义发送频率，支持立即发送
44.		支持根据篡改告警事件状态来筛选发送的篡改告警
45.	syslog通知	支持syslog方式的告警通知和日志集中存储
46.	角色管理	支持管理角色的自定义，支持按照系统详细的操作权限，数据权限自定义任意角色；
47.		支持自定义角色中操作权限如策略配置、日志管理、节点管理、账户管理、邮件配置等的分配；
48.		支持数据权限按照管理域整体划分给某个角色；
49.	账户管理	支持系统管理员或管理员分配的有相应权限的角色来添加自定义账户
50.		支持管理员对或管理员分配的有相应权限的角色如管理域管理员对全局、本管理域下的账户进行角色的修改和批量修改、批量删除
51.	分权分域	允许不同配置的服务器组划分为管理域，管理域作为整体管理单元划分到各角色账户
52.		支管理域通过账户控制实现数据隔离
53.	安装	支持使用脚本批量安装多服务器节点
54.	卸载	支持在管理端自动卸载，可实现服务器节点的集中卸载
55.		支持在服务器端手工卸载，卸载时需要输入卸载密码

56.	服务器节点版本控制	支持在管理端下载节点安装包，支持往管理平台上上传节点升级包和安装包
57.		支持从管理平台上对多台服务器防护节点的一键批量升级、单独特定节点的升级
58.		当有可升级包时，支持从管理平台检测和展示可升级节点
59.	全局维度	支持全局管理维度的统计和展示
60.	服务器组维度	支持根据所选服务器组的管理维度的统计和展示
61.	服务器节点维度	支持根据所选服务器节点的管理维度的统计和展示
62.	防护弹性扩展	支持由管理端控制防护节点的总量，在不超过管理端授权总量的情况下可弹性调整防护节点的部署，不需要重新授权，节点释放后不占用原有授权数量。
63.	管理扩展	具备标准的RestfulAPI接口，可灵活接入各类采用标准RestfulAPI接口的统一管控和运营管理平台
64.	自身安全性	服务器节点软件安装后能对安装文件进行保护，防止被非法篡改；
65.		对服务器节点上运行的程序进行监控，当常驻进程异常退出时，可自动恢复。
66.	通信安全性	管理端与服务器节点之间通讯进行加密传输，对通信过程中的整个报文或会话过程进行加密；
67.		采用密码技术对通信过程中的数据进行校验，保证通信过程中的数据完整性、不被篡改。
68.	登录安全	对于认证成功用户具有超时管理功能，支持对远程管理的连接进行超时；
69.		具有管理员和用户身份鉴别尝试次数限制功能，超出尝试次数限制锁定账户一段时间
70.		账号登录失败允许次数、登录失败超时次数锁定时间可自定义
71.		支持登录IP控制访问列表设置，包括IP黑名单和白名单设置
72.		支持登录时防止身份鉴别信息被暴力猜解的机制，支持登录验证码
73.	密码安全设置	对密码设置具有长度和复杂度的检查功能，能够进行弱密码检测，禁止用户设置弱密码；
74.		支持密码有效时间、密码最小长度、最大密码长度、密码强度的设置；

75.		支持弱口令密码字典的设置；
76.	支持水印授权	支持水印授权方式，通过证书文件与水印文件激活系统保证系统所有功能可用。
77.	质保要求	▲三年软件升级维护服务，提供原厂针对本项目的售后服务承诺函。

H. 静态数据脱敏系统功能需求

序号	功能项	功能需求
1.	基本要求	脱敏系统界面友善，简单易用，完全基于BS架构设计，提供中文操作界面，无需安装任何客户端或者代理，系统升级、维护方便。支持Linux、Windows、UNIX等操作系统。
2.		脱敏系统平稳运行，满足高峰交易处理的需要，使用过程中不出现crash，进行脱敏操作的过程中不需要频繁重启后台服务，脱敏操作对数据库(源库和目标库)影响小。
3.	硬件要求	1U机架式设备，6个电口、1×扩展槽位、32G内存、128G SSD、4T存储空间,4个千兆光口，含光模块。
4.	性能要求	★峰值事务处理能力需不低于每秒30万个数据单元，脱敏速度不小于50G/小时。
5.	脱敏支持	系统支持丰富的数据源和目标，数据源、目标配置通过系统界面实现： 1、关系型数据库 支持Oracle、DB2(包含AS400/UDB)、Sql Server、Sybase、Mysql、PostgreSQL、MariaDB、informix等主流关系型数据库，国产数据库（人大金仓、达梦、南大通用（gbase8t/8s）等）、以及cache后关系型数据库脱敏。 2、数据仓库 支持Teradata、Greenplum、Sybase IQ 、Vertica、Gbase 8a、TiDB、GaussDB、Sap Hana等数据仓库脱敏。 3、大数据平台 支持hive、impala、Hbase、Maxcompute、MongoDB、巨衫等大数据平台脱敏。 4、消息队列 支持Kafka脱敏。

		5、内存数据库 支持Redis脱敏。 6、文件 （1）文本文件 支持直接读取txt、csv、excel、xml、json等文件脱敏。 （2）▲数据库文件 支持直接读取oracle dump（exp/expdp）、mysql dump（sql文件）、dbf文件脱敏；（需提供产品功能截图证明并加盖原厂公章） 7、远程文件脱敏 支撑通过ftp、sftp方式对自动获取远程文件进行不落地脱敏。
6.	功能要求	▲支持多种脱敏方式： 源库到目标库脱敏（包含支持同库脱敏） 数据库到文件脱敏 脱敏后文件自动压缩成zip文件，并在脱敏系统界面上下载。 文件到文件脱敏 需要脱敏的文件可以通过脱敏系统客户端、脱敏服务器本地上传以及利用ftp、sftp从源端获取数据进行脱敏，脱敏后自动压缩成zip文件并在脱敏系统界面上下载脱敏后的文件。文件到数据库脱敏（需提供产品功能截图证明并加盖原厂公章）
7.		▲根据不同的应用场景，支持主流关系型数据库之间（Oracle、DB2、SQL Server、Mysql）不落地异构脱敏（需提供产品功能截图证明并加盖原厂公章）
8.		支持灵活的敏感信息自动发现： 1、通过文件导入或在系统界面上选择（关键词或正则表达式搜索）敏感信息发现的数据范围（schema、table等）；2、自定义抽样比例和匹配率。
9.		支持敏感数据增量发现，即：多次运行同一脱敏作业，如果源数据库DDL发生变动，自动检测到变动后，可对增量部分进行敏感信息发现，避免由于数据源DDL变动所带来敏感信息泄露。
10.		支持敏感数据自动发现： 1、脱敏系统预置丰富敏感字段发现规则，预置敏感字段发现规则包括：

		中文姓名、英文姓名、姓名拼音、韩文姓名、电话号码、邮箱、邮编、金额、日期、企业营业执照、组织机构代码证、银行卡号、军官证、港澳通行证、往来台湾通行证、护照、税务登记证、身份证、组织机构名称、地址、IP地址、社会统一信用代码、开户许可证、医疗机构登记号、医师资格证书、医师职业证书、证券代码、证券名称、基金名称、基金代码、车牌号码、JSON等； 2、支持混合类型的敏感数据发现： （1）一个字段多种敏感类型； （2）一个数据单元内多种敏感类型； 3、支持自定义敏感发现规则，可针对字段名、数据特征、内容字典进行敏感发现规则的设置，自定义敏感类型需要支持分段、数据字典等手段。 4、敏感信息扫描后，将敏感发现结果界面展现，显示敏感表名称、敏感字段名称、匹配敏感数据类型、样本匹配度（示例）以及样本效验（抽样数据确认敏感结果）等可对敏感发现的结果进行人工审核。
11.		支持灵活的脱敏规则管理： 1、脱敏系统需内置丰富的脱敏规则； 2、脱敏规则在界面方便管理，根据不同应用场景，设置脱敏规则（包含遮盖、SHA1加密、MD5加密、AES加密、RSA加密等）。 3、自定义增加脱敏规则 （1）提供随机映射、固定映射、替换、替换、截断、截取，以及保留、取整、范围内浮动、比例内浮动等各种脱敏算法以满足不同需求； （2）分段配置不同的脱敏规则 4、支持依赖脱敏，即：可根据依赖字段的值对数据进行不同类型的脱敏处理。 5、计算脱敏，支持数据脱敏后，需要保持其原来的计算公式，如数据的分组求和、依赖计算等。 6、json脱敏，可对于一个json字符串针对其中包含的敏感节点进行脱敏，并支持敏感节点发现。 7、xml脱敏，可对于一个XML字符串针对其中包含的敏感节点进行脱敏，并支持敏感节点发现。

12.		自定义字典发现及脱敏，用户需要将字典类数据进行脱敏处理，提供用户数据字典管理功能，并按照字典进行发现及脱敏，增加了系统整体发现和脱敏的灵活性。
13.		支持黑名单过滤，对于非常核心敏感的数据通过黑名称过滤，不脱敏或不迁移到目标端，提供独立管理页面。
14.		支持白名单过滤，经过脱敏处理数据需要跟未脱敏数据或外部数据进行联调，提供白名单过滤功能，可根据不同的字段内容设置过滤条件，即跟未脱敏数据或外部数据进行联调的字段设置成白名单不脱敏，支持库到库以及同库脱敏方式白名单设置。
15.		系统支持脱敏前环境的检查，如网络、用户权限、空间大小等，避免环境问题导致脱敏失败。
16.		根据客户要求创建测试数 据子集，并且对包含敏感信息进行脱敏。能够在界面上创建子集抽取规则（如：百分比、记录数以及根据相关条件设置），这样在脱敏任务中，调用定义好的子集规则，进行子集脱敏、迁移，最后形成的子集是大小适合、符合业务逻辑的测试数据集合。
17.		脱敏系统根据开发、测试要求，为了提高脱敏效率，不需要每次都全量脱敏，可以实现增量数据脱敏。
18.		▲支持API脱敏接口调用： （1）第三方系统根据请求将数据封装成JSON、XML格式，之后调用API脱敏接口对JSON、XML格式中的敏感数据进行脱敏，经过脱敏处理后将数据按照原来格式返回（JSON、XML）。（需提供产品功能截图证明并加盖原厂公章） （2）支持作业调度API，可通过API对于作业进行启动、暂停、终止操作，可通过该API查看作业当前的运行状态、处理的数据量、同步对象数量、处理进度、处理耗时等。（需提供产品功能截图证明并加盖原厂公章）
19.		▲系统支持数据水印，将任意水印信息嵌入到脱敏后数据中，并且支持数据溯源，如有数据泄露即可追溯到数据泄露的源头。（需提供产品功能截图证明并加盖原厂公章）
20.		支持表(包含分区表、簇表、索引组织表、队列表、压缩表、嵌套表)、主键、外键、索引（包含分区索引、位图索引、函数索引、压缩索引）

		、约束、视图、同义词、序列、队列、dblink、自定义类型、存储过程、函数、触发器、包等数据库对象脱敏后在目标库中自动创建。
21.		非数据类错误等待和重试： 1、对于磁盘空间不足等非数据类进行自动重试； 2、重试依然遭遇相同错误，则作业进入暂停状态，等待人工处理； 3、人工修复空间不足等错误之后通过点击重试继续脱敏作业。
22.		支持脱敏服务器性能监控： 1、对于脱敏服务器的cpu、内存、磁盘进行监控； 2、特别需要对于网络带宽吞吐量进行监控。
23.		支持脱敏结果集合重用，无需再次脱敏。
24.		脱敏后系统提供丰富的脱敏报表，包括脱敏作业报告、敏感数据分布统计、脱敏作业分析、用户操作统计等统计报表，便于领导了解脱敏的整体情况。
25.		支持邮件告警功能，当作业运行结束、暂停、终止、异常停止、异常终止等作业状态发生变化的时候发送邮件。
26.	安全性要求	脱敏系统具有完善的访问控制管理机制： 1、具有完善的角色、权限管理体系，权限划分细粒度到每个功能点，实现三权分立（管理员、安全员、审计员）； 2、根据不同的用户对数据源进行权限管理。
27.		脱敏算法秘钥机制，即脱敏算法加秘钥生成新脱敏算法，并且秘钥每隔一段时间脱敏管理员可自定义手工修改，修改秘钥后脱敏后的数据和原脱敏算法脱敏后的数据不同，便于脱敏规则安全管理。
28.	产品资质要求	具备国家版权局颁发的《计算机软件著作权登记证书》
29.		产品获得国家级质量监督检验中心检测
30.		产品获得中国网络安全审查技术与认证中心颁发的《IT产品信息安全认证证书》
31.	质保要求	▲提供3年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。需要提供产品原厂商针对本项目的授权函及售后服务承诺函，并加盖原厂公章。

I. 备份系统服务扩容功能需求

序号	功能项	功能需求
1.	基本要求	企业级备份软件，全中文图形化界面，非OEM
2.		永久许可，最终用户名为“广州市第八人民医院”
3.	配置	1、★现有备份软件授权（物理机备份许可×9、虚拟机备份许可×50）续费1年原厂软件升级服务，并将现有备份软件版本升级至11.0 SP24（软件序列号：FDE45，现版本10.0 SP15），并开启防勒索病毒功能
4.		1、★扩容以下许可，扩容的备份软件与医院现有备份系统兼容，能够统一控制台管理，备份策略统一下发，备份结果统一生成报表： 物理机备份许可×20，含系统、文件、数据库备份功能，含文件归档功能； 虚拟机备份许可×30，含文件备份功能； 支持备份到物理磁带库；不限重删数据量。
5.	重复数据删除	内嵌源端重删和目标端重删功能，支持跨越虚拟环境和物理环境。支持广域网环境去重功能，支持对不同站点去重后的数据再进行比对后全局二次去重。
6.		支持数据复制功能，将已源端去重的数据远程复制到异地机房，实现数据级的容灾。
7.	Oracle备份	对Oracle数据库可以进行全备份、增量备份和日志备份，基于块级备份技术实现一次全备份、永久增量备份；
8.		在全中文图形化界面下，可将Oracle数据库恢复到指定的时间点，可实现单表恢复；
9.		全图形化界面下，不用写脚本或改模板，不用在服务器上设置Crontab计划，可用定时在异机的不同路径进行恢复；
10.		在备份软件界面，可以同时查看RMAN日志和备份任务日志，查看两种日志时互不干扰；
11.		可以从图形化界面收集全部日志，日志收集完成后，支持发邮件、FTP、本地保存或共享路径保存；
12.		支持Oracle数据库断点续备；支持RAC恢复到单机；
13.		▲投标时提供Oracle断点续备功能截图证明并加盖原厂公章。
14.	SQL Serve备份	支持SQL Server 2005、2008、2008 R2、2012、2014、2016、2017、2019（Windows/Linux）；

15.		▲支持恢复时数据脱敏，可按用户制定的策略，对表中的字段进行脱敏处理，确保用户的信息安全（需提供产品功能截图证明并加盖原厂公章）
16.		支持数据块级别备份（BLB），支持合成全备份，并能提供表级别恢复；可以直接挂载，用于数据验证、开发、测试、审计等多种场景
17.	MySQL备份	支持Community Server Edition/Enterprise, Standard/Classic Edition - 5.5.x, 5.6.x，5.7.x 8.0.x，MariaDB 5.5.x, 10.0.x, 10.1.x, 10.2.x and 10.3.x等
18.		支持数据块级别备份（BLB），支持合成全备份，并提供表级别恢复；可以直接挂载，用于数据验证、开发、测试、审计等多种场景
19.		支持dump逻辑备份以及企业级MEB/SBT备份
20.	自动日志备份	对关键应用数据库的Log进行单独备份。定时对Log进行备份，在不影响生产的前提下提高关键数据库系统的保护频次，结合Log进行数据库恢复，提高RPO指标减少数据丢失；并对Log空间进行自动监控，可设置自动策略在Log空间占用达到设置值的情况下自动发起Log备份，防范Log空间不足引起的数据库停机。
21.		投标时提供软件厂商盖章的Oracle数据库日志自动备份功能截图证明并加盖原厂公章。
22.	PACS归档	内嵌PACS归档功能，能直接将文件系统上的3个月以上未访问的文件归档到物理带库中，归档后的文件在原址保留存根，用户可以通过存根直接发起对归档文件的回调和访问。无需管理员配合进行恢复，可自助回调。
23.		支持对归档之后的文件实现内容索引和搜索功能，通过文件的关键字或其他属性可以实现对备份或归档文件的快速搜索。
24.		▲投标时提供文件归档功能截图证明并加盖原厂公章。
25.	虚拟机备份	官方支持VMware、Hyper-V、XenServer、FusionCompute、AHV、OpenStack等多种虚拟机的无代理备份，支持单机和集群部署环境。虚拟化应用均支持以虚拟机、资源池和整个集群为单位进行备份保护保护，无需在虚拟机内部安装任何代理软件；
26.		支持颗粒度恢复，可针对虚拟机内的数据库实现一致性备份及颗粒度恢复，可在全图形化界面下恢复Oracle/MSSQL到任意时间点；

27.		内嵌VMware虚拟机即时挂载、即时恢复功能；
28.	虚拟机归档	按定义的策略对不经常使用的OpenStack、VMware虚拟机自动关机，对一段时间不开机的虚拟机自动归档到二级存储，需要访问时可恢复归档虚拟机，以降低主存储成本及释放虚拟服务器资源。
29.	防勒索病毒攻击	内嵌一键防勒索病毒功能，通过蜜罐文件自动检测客户端是否被勒索病毒攻击，当发现蜜罐文件被篡改，立刻发出攻击警告。
30.		防止任何非备份软件进程修改备份磁盘上的数据。
31.	网络隔离	内嵌网络隔离技术，安全站点可以禁止所有外部连接请求，需要时再主动连接，确保灾备数据不会被篡改。（需提供产品功能截图证明并加盖原厂公章）
32.	数据加密功能	备份数据以封闭格式存储，非tar、cpio等标准通用格式。支持对备份数据的加密功能，支持包括AES、3-DES在内至少三种加密算法。
33.	售后服务	▲1年5×8原厂远程技术支持服务，包含产品系统升级授权、产品保修服务、远程支持服务。需要提供产品原厂商针对本项目的授权函及售后服务承诺函，并加盖原厂公章。

J. 过期设备授权续期、安全证书续期等需求

序号	设备名称	需求	数量
1.	网御SSL VPN证书	包含1年的现有的SSL VPN证书授权。	1台
2.	安恒漏扫	DAS-RAS-H1000，包含1年的现有的漏洞扫描授权升级、硬件维保。	1台
3.	伟思网闸（2台）	设备型号：ViGapV6.5-400HJ-LL1200 序号号：110105682Y0046、110105682Y0048） 包含1年的现有的软件更新升级服务、硬件设备产品保修服务、故障远程支持服务，返厂检测备机服务。	2台
4.	SSL，https证书	包含1年的现有的SSL 、https证书授权。	1台
5.	WEB应用防护系统	设备型号:WAFNX3-P300序列号:14-32-L-0099：包含1年软件更新升级服务、硬件设备产品保修服务、故障远程支持服务，返厂检测备机服务；网站攻击特征库升级服务，防篡改模块特征库升级服务。	1台
6.	外网堡垒机	设备型号:SASNX3-H200C序列号:14-52-L-0502；包含1年	1台

		的现有的软件更新升级服务、硬件设备产品保修服务、故障远程支持服务，返厂检测备机服务。	
7.	内网堡垒机	设备型号:OSMSNX3-200C序列号:18-26-L-0539；包含1年的现有的软件更新升级服务、硬件设备产品保修服务、故障远程支持服务，返厂检测备机服务。	1台
8.	绿盟入侵检测系统	设备型号:NIDSNX3-N2000A序列号:16-38-P-0418；包含1年的现有的软件更新升级服务、硬件设备产品保修服务、故障远程支持服务，返厂检测备机服务。	1台
9.	数据库审计系统	设备型号:DASNX5-6000C序列号:16-52-J-0352；包含1年的现有的软件更新升级服务、硬件设备产品保修服务、故障远程支持服务，返厂检测备机服务。	1台
10.	企业安全中心系统	设备型号:ESPC-V7序列号:16-38-0419；包含1年的现有的软件更新升级服务、硬件设备产品保修服务、故障远程支持服务，返厂检测备机服务。	1台
11.	外网主出口防火墙	设备型号:NFNX3-G4000L序列号:15-45-J-0167；包含1年的现有的软件更新升级服务、硬件设备产品保修服务、故障远程支持服务，返厂检测备机服务、病毒特征库升级服务，入侵防御特征库升级服务。	1台
12.	外网备出口防火墙	设备型号:NFNX3-G4000L序列号:15-45-J0383；包含1年的现有的软件更新升级服务、硬件设备产品保修服务、故障远程支持服务，返厂检测备机服务、病毒特征库升级服务，入侵防御特征库升级服务。	1台

K. 服务区防火墙功能需求

序号	功能项	功能需求
1.	性能要求	★硬件平台采用先进的多核网络专用架构。硬件平台采用多核处理器，使用64位MIPS多核处理器，多核核数≥10个，吞吐量≥20Gbps，最大并发会话数≥900万，每秒新建会话数≥27万，IPSEC VPN隧道数最大可支持20000条，SSL VPN用户数标配100个并发用户数，最大可扩展至10000个并发用户（要求提供能证明多核CPU并行处理的截图）

2.	硬件接口数量	配备业务接口至少4个千兆电口，4个千兆光口，4个万兆接口（所有业务接口均可自定义使用）；标配1个Console口，1个USB2.0 口，1个HA口，1个MGT口和1个AUX 口；标配支持热拔插双冗余电源，标准机架设备。
3.	模块需求	每台设备配4个万兆光模块
4.	工作模式	支持透明、路由、混合、旁路4种工作模式
5.	NAT（网络地址转换）	支持源NAT和目的NAT,且支持NAT扩展技术，使单个公网IP支持的NAT转换端口突破65535限制（需提供产品功能截图证明并加盖原厂公章）；
6.		▲支持源目NAT命中分析，源目NAT状态、命中数统计、首次命中时间、最近一次命中时间、最近未命中天数、源目NAT创建时间分析显示。（需提供产品功能截图证明并加盖原厂公章）
7.	动态路由	支持OSPF、BGP、RIPv1/v2、IS-IS（动态路由协议非透传）路由
8.	BFD协议	支持BFD for Static/OSPF/BGP
9.	HA高可用性	支持A-P模式，A-A模式，解决非对称路由场景的对等模式
10.		▲支持与医院现有的服务器区防火墙组成双机热备，单台防火墙设备发生故障时自动切换，消除单点故障风险。
11.		▲支持基于接口、HTTP、PING、ARP、DNS、TCP等监测对象实现HA切换（需提供产品功能截图证明并加盖原厂公章）
12.	应用识别	具备对应用程序的识别和控制能力。应用程序特征库不少于4500种，并支持在线/手动更新
13.	抗DDOS攻击	抗DDOS攻击：支持抵御下所列所有攻击类型，包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、WinNuke
14.	网页访问控制	基于角色、时间、优先级、网页类别等条件的Web网页访问控制
15.		支持自定义URL类别
16.		支持千万级URL特征库，URL库支持网络实时更新
17.	访问控制	支持按照应用、时间、用户、IP地址、服务端口、协议等方式对数据进行访问控制
18.	策略管理	▲支持策略助手能够提取命中指定策略ID的流量作为流量数据分析源，并根据用户设置的聚合规则聚合流量数据列表，最后自动生成符合用户期望的安全策略规则。可基于源目IP及服务生存精细化安全策略

		，及基于源目IP聚合精细化策略。（需提供产品功能截图证明并加盖原厂公章）
19.		支持策略状态、命中数统计、首次命中时间、最近一次命中时间、最近未命中天数、策略创建时间分析显示。（需提供产品功能截图证明并加盖原厂公章）
20.		安全策略支持复制粘贴、导入导出、安全策略冗余检测、基于时间安全策略时间有效性检测、安全策略聚合（需提供产品功能截图证明并加盖原厂公章）
21.	链路负载均衡	支持基于接口实时查看接进链路的延迟、丢包率和抖动情况曲线图。
22.		支持基于带宽利用率，链路延时、抖动、丢包情况进行自动智能调节选路。（需提供产品功能截图证明并加盖原厂公章）
23.	智能流量管理	支持两层八级管道嵌套，能够同时做到两个维度的流量控制
24.		支持对多层级管道进行最大带宽限制、最小带宽保证、每IP或每用户的最大带宽限制和最小带宽保证
25.	特征库	具备8200种以上攻击特征库规则列表，至少支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征ID等方式的查询。
26.	HTTP类攻击防护	具备4000种以上HTTP特征库规则列表
27.		支持SQL注入、XSS防护，支持HTTP头域中的URL、Cookie、Referer、POST检查点配置防护策略
28.		▲支持外链检查防护，支持自定义外链特性，类型支持HTTP、HTTPS、FTP（需提供产品功能截图证明并加盖原厂公章）
29.		支持CC攻击检测，支持访问限速、代理限速、自定义请求阈值、爬虫友好等方法，检测到CC攻击时支持JS Cookie、重定向、访问确认、验证码四种认证方法
30.	病毒库	具备350万种以上病毒特征库规则列表。
31.	扫描文件类型	支持对HTTP、FTP、SMTP、POP3、IMAP协议的应用进行病毒扫描和过滤
32.	压缩文件扫描	支持对压缩文件类型的病毒检测，支持RAR、ZIP、GZIP、BZIP2、TAR等压缩文件类型；支持对多重压缩文件的病毒检测，且不小于5层压缩，支持对超出行为自定义处理方式
33.	系统回滚	支持2个系统软件并存，并支持系统软件回滚，防止配置不当或系统故障造成的网络中断，充分保证了系统的稳定性。

34.	配置文件保存	支持10个配置文件并存，并支持配置回滚
35.	流量包统计	支持按64字节、128字节、256字节、512字节等数据包流量统计
36.	页面抓包	支持源目IP、用户、应用、协议、源目端口7元组在线抓包，支持自定义抓包时长。
37.	多维度监控统计集	支持将统计数据类型（流量、会话、新建会话、AD攻击次数、URL访问次数、关键字阻断次数、应用阻断次数）与数据组织方式（安全域、接口、IP、用户、应用、VSYS）自由组合灵活统计集
38.	安全运维APP	▲提供SaaS模式的安全运维APP：通过手机可以第一时间获知设备的实时CPU、内存、流量趋势，以及应用、用户排名、威胁信息等安全状态、 帮助快速定位问题、安全可视化实时呈现。提供App下载URL。该APP不能是VPN 客户端软件。该APP不限制使用用户数。（需提供产品功能截图证明并加盖原厂公章）
39.	公安部销售许可证	投标产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》，（万兆增强级-高性能），提供证书文件并加盖原厂公章
40.	IT产品信息安全认证证书	具备中国网络安全审查技术与认证中心颁发的< IT产品信息安全认证证书>万兆EAL4增强级要求，提供证明文件并加盖原厂公章
41.	信息技术产品安全分级评估证书	具备国家网络与信息系统安全产品质量监督检验中心颁发的<信息技术产品安全分级评估证书>万兆评估保障级4增强级要求提供证明文件
42.	Gartner魔力象限	▲投标产品连续获得七年进入Gartner防火墙魔力象限，要求提供证书文件并加盖原厂公章
43.	客户选择	▲具备入选Gartner发布的Peer Insights 2020年网络防火墙客户选择榜单排名前五.提供证明材料，要求提供证书文件并加盖原厂公章
44.	原厂支持	▲提供3年原厂服务，包含产品系统升级授权、产品保修服务、远程支持服务。需要提供产品原厂商针对本项目的授权函及售后服务承诺函，并加盖原厂公章。

L. 汇聚交换机功能需求

序号	功能项	功能需求
1.	性能要求	支持6个总槽位（4个业务槽位，2个主控槽位）；2个电源槽位，标配不

		含电源；默认含满配1个风扇盘）。 1、交换容量≥25Tbps/86.4Tbps、包转发率≥3000Mpps/21200Mpps； 2、支持横向N:1虚拟化（N≥2）； 3、支持ISSU业务不中断系统升级、静态路由、RIP v1/v2、OSPF、BGP、策略路由 4、支持IPv6静态路由、RIPng、OSPFv3、BGP4+ 5、支持EAPS环网保护技术、VRRP冗余技术；6、主控板2块，交流电源模块*2块，具备千兆光口≥24个，千兆电口≥48个，万兆光口≥4个，复用千兆电口≥4个，千兆单模光模块≥6个，万兆光模块≥4个。
2.	原厂支持	提供三年软硬件售后服务；

M. 安全加固服务需求

对于8个系统（HIS、LIS、EMR、PACS、OA、集成平台、互联网医院以及官网系统）等保测评发现的各类安全不合规项、系统漏洞（来源为第三方漏洞扫描、渗透测试、最新严重漏洞）、基线安全配置等问题，进行修复风险评估、制定安全加固方案、回滚措施、协助对漏洞和不安全项进行整改加固，确保漏洞修复安全可控，满足等级保护验收要求，主要包含不限于以下内容：

（1）服务器安全加固服务

服务器的安全加固，将重点针对IIS、apache、mysql、MS SQL server、oracle等服务器及系统服务进行安全加固。

加固主要内容包括：

一、 服务器操作系统的身份鉴别安全加固，配置登陆失败、操作超时、限制非法登录以及自动退出等；

二、 配置服务器账号登录密码强度策略；

三、 严格控制服务器操作系统的远程管理，限制远程管理终端，配置使用加密远程管理方式等；

四、 对服务器操作系统账号的权限进行紧缩，遵循“最小权限”原则，防止对系统的越权访问；

五、 清理不再使用、旧的系统账号；

六、 禁用系统多余的、系统缺省打开却不必要服务系统服务，删除不再使用的共享；

七、 开启系统日志审计功能，对系统事件的日期、时间、类型、主体标识、客体标识等进行记录，并定期分析；

八、 配置服务器操作系统的防病毒及防恶意代码功能，安装防病毒软件，定期

进行病毒查杀；

九、 检查分析现有系统的安全漏洞和黑客后门等，更新服务器系统安全补丁；

十、 对服务器操作系统的运行状态、系统服务等进行监控；

十一、 配置应用平台（IIS、apache 等）的安全参数，加强应用安全。

（2）关键网络设备加固

十二、 根据相关策略对设备进行检查与设置，并进行优化调整；

十三、 对其配置进行检查，根据对实际应用情况的分析，删除冗余的配置，启用路由器中的 ACL 配置，提高接入的安全性等措施优化配置，实现设备加固。

（3）安全设备加固

十四、 根据相关策略对设备进行检查与设置，并进行优化调整。

十五、 对其配置进行检查，根据对实际应用情况的分析，删除冗余的配置，提高接入的安全性等措施优化配置，实现设备加固。

（4）管理制度梳理

十六、 进行基本管理制度修编。