**采购需求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 功能参数 | 数量 | 单位 |
| 1 | 堡垒机 | 1. 默认包含运维授权数≥50，最大可扩展资产数≥150，图形运维最大并发数≥100，字符运维最大并发数≥200。 标准1U设备，内存大小≥8G，硬盘容量≥2T SATA，单电源，接口≥6千兆电口。 2.支持根据不同应用匹配对应应用登录方式配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入。 3.为防止单一登录认证密码较弱容易被破解的问题，用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式；并支持各种认证方式和静态口令组合认证以提升认证强度同时降低被破解盗用的风险。 4.为方便统一管理及分权运维，明确运维分工提升运维效率支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权。 5.★为实现多部门之间业务协同配合实现资源统一调度，支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问。 6.★为提升运维工作与其他业务部门配合满意度，产品支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作。   7.为提升密码复杂度，产品支持密码策略设置，可自定义密码复杂程度，可设置密码中包含数字、字母、符号及禁用关键字等内容。 8.★全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计。 | 1 | 台 |
| 2 | 入侵防御 | 1. 网络层吞吐量≥6Gbps，IPS吞吐量≥650Mbps，并发连接数≥1800000，新建连接数≥60000。 标准1U设备，内存大小≥4G，硬盘容量≥128GB minisata SSD，单电源，接口≥6千兆电口+4千兆光口SFP。 2.支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能； 3.访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式，支持长连接功能并可以配置连接时长； 4.支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、地域、认证用户、子接口和VLAN等因素实现对象的流量控制 5.★支持同访问控制规则进行联动，可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间；  6.★支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；  7.支持安全策略一体化配置，通过一条策略快速实现不同安全功能的配置，简化策略配置工作；   8.★为保证运维便捷提升安全防护效果所投产品需能与已采购的终端杀毒软件进行深度联动处置。 | 1 | 台 |
| 3 | 全网行为管理 | 1. 网络层吞吐量≥5.8Gb，应用层吞吐量≥750Mb，带宽性能≥500Mb，包转发率≥90Kpps，每秒新建连接数≥10000，最大并发连接数≥500000，标准1U设备，内存大小≥8G，硬盘容量≥128GB MSATA，单电源，接口：≥6千兆电口。 2.支持网关模式、路由模式、网桥模式、网桥模式（多路桥接模式）和旁路模式等多种模式的网络部署方式，支持电口bypass。 3.基于IP网段地址、Vlan划分、MAC地址、SSID标识等实现上网人员差异化自动分组、认证规则。 4.支持多种协议对接认证、微信认证、短信认证、账号密码认证等机制，支持短信认证方式，用户输入手机号作为用户名，设备通过短信网关为用户手机发送密码。 5.支持对终端上U盘和移动硬盘接入设置可读写、拒绝、可读、告警；支持允许特定的外设（包括U盘/存储设备）在终端上使用，并提供批量获取硬件ID的工具。 6.★设备内置海量预分类的URL地址库，能够针对各种URL类型做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制。  7.支持常见远程控制软件的审计,包括但不限于Teamviewer、向日葵、Anydesk、RDP的的外发文件审计。 8.支持全网终端资产测绘，提供大屏可视化，可根据IP地址段展示全网终端上线情况、IP地址、Mac地址以及活跃时间等等。 9.为满足等保分权管理要求，设备支持设置四类管理员，分别为系统管理员、安全管理员、审计管理员，以及多种权限的超级管理员；管理员支持分级，高级别管理员的策略配置优先生效，并可修改低级管理员的策略。   10.★为保证运维便捷提升安全防护效果所投产品需能与已采购的终端杀毒软件进行深度联动处置。 | 1 | 台 |
| 4 | 安全感知管理平台 | 1. 存储容量≥14.4T，在带宽性能1Gbps时存储时长≥900天/1Gbps。 标准1U设备，内存≥3\*32GB DDR4 3200，系统盘≥1\*240GB SATA SSD，数据盘≥4\*4TB，标配盘位数≥8，冗余电源，接口：≥4千兆电口+4万兆光口。 2.大屏展示可以从多个维度对内网安全态势进行展示，例如：安全事件、安全事件趋势、安全事件前5、威胁攻击事件前10、攻击事件类型前5等。 3.支持以不同的维度管理不同类型的资产，例如硬件资产、软件资产和部门资产等，支持资产导入/导出和更新，并支持记录资产变更记录。 4.产品可以对SIEM日志关联结果可视化展示，对安全事件的发展趋势、网络中设备的接入状况、数据分布等进行展示。 5.产品可以对镜像流量中是否存在截获的口令信息进行检测分析，通过对IP、业务、分支、域名等等进行检测通过数据包举证的形式，降低因为数据明文传输导致的数据泄密问题。 6.★弱密码检测过程中支持主动扫描，能够对加密协议的弱口令进行检测，协议包括SSH、SMB、MySQL等，同时支持各类数据库的检测包括MySQL、Oracle、MongoDB等。 7.支持暴力破解攻击分析，分析维度包括威胁源总量、影响资产数、威胁源TOP5、影响业务系统TOP5、破解趋势、威胁列表等。   8.★为保证运维便捷提升安全防护效果所投产品需能直接通过安全感知管理平台对已采购的终端杀毒软件进行操作处置和联动。  9.★为保证运维便捷提升安全防护效果所投产品需能与已采购的行为管理设备进行深度联动处置。 | 1 | 台 |
| 5 | 日志审计 | 1.默认包含主机审计许可证书数量≥50，最大可扩展审计主机许可数≥150，可用存储量≥2TB，平均每秒处理日志数（eps）最大性能≥2500，标准2U设备，内存大小≥16G，硬盘容量≥128G minisata+2T SATA\*2，单电源，接口：≥6千兆电口+2万兆光口SFP+。 2.支持对日志源的批量采集和日志源数据的批量转发。 3.支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。 4.★支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志。  5.支持以FTP方式将日志数据备份至外部存储空间，支持备份数据的恢复和查询。 6.支持日志检索数据的投屏；支持日志查询结果的统计与导出，支持历史备份文件导入查询。 7.★支持将检索查询的条件收藏为查询模版，支持查询模版创建、导入导出、删除功能，支持历史搜索记录功能。  8.★支持灵活的自定义报表，可以选择模板、数据类型等生成导出报表。 | 1 | 台 |
| 6 | 下一代防火墙 | 1. 网络层吞吐量≥4G，应用层吞吐量≥2G，防病毒吞吐量≥600M，IPS吞吐量≥600M，全威胁吞吐量≥450M，并发连接数≥200万，HTTP新建连接数≥6万，标准1U设备，内存大小≥4G，硬盘容量≥128G SSD，单电源，接口：≥8千兆电口+2千兆光口SFP。 2.产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式。 3.★支持独立的入侵防护规则特征库，规则库支持根据漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等进行分类，特征总数在10000条以上，能对常见漏洞进行安全防护。 4.支持独立的WAF防护模块，WAF防护特征总数在4500条以上，支持针对地址、应用设置WAF白名单，支持攻击规则搜索以及自定义。 5.支持服务器抗恶意扫描功能，产品针对扫描源IP进行日志记录，并对恶意源IP联动封锁。 6.支持基于信誉的僵尸网络防护能力，具备可以持续升级的信誉库，当前僵尸网络信誉库≥120万种。 7.支持多对一、一对多和一对一等多种地址转换方式。 8.★支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。   9.★为保证运维便捷提升安全防护效果所投产品需能与已采购的终端杀毒软件进行深度联动处置。 | 1 | 台 |
| 7 | 内网流量探针 | 1. 网络层吞吐量≥500Mbps，应用层吞吐量≥160Mbps，标准1U设备，内存大小≥4G，硬盘容量≥128G minisata SSD，单电源，接口：≥6千兆电口。 2.在产品的系统管理页面可以看到吞出量、接口状态、资源状态等，能够进行可视化展示。 3.产品可以通过IP、业务端口、通讯协议、数据包流向等以自定义的方式来进行应用的识别。 4.产品支持多种形式的攻击检测能力，包括：SQL注入、XSS检测、webshell、JAVA代码的检测、PHP的代码检测等，能够管理员可以自行配置启动检测，选择高效检出低误报模式。 5.★产品可以检测到网络中的网络设备和部署位置的情况，从而能够直观的看到内网的网络状况。  6.系统支持多协议关联分析，能够自动关联不同协议、不同会话的威胁日志，筛选出严重事件，节省事件处理的人力成本。 7.★产品支持对端口异常、上行和下行流量、DNS、ICMP、HTTP、HFS等协议和检测到登录异常的流量进行检测。   8.★需提供软件著作权证书。 | 1 | 台 |
| 8 | 数据库审计 | 1.最大硬件吞吐量≥2Gbps，最大纯数据库流量≥400Mb/s，数据库实例个数≥30个，SQL处理性能≥30000条SQL/s，日志检索性能≥500000条/秒，标准1U设备，内存大小≥8G，硬盘容量≥2T SATA，单电源，接口：≥6千兆电口+2万兆光口SFP+。 2.★支持包括Redis、MongoDB、Hive、HBaseJavaAPI、kafka、ElasticSearchHttp、ElasticSearchJavaAPI等非关系型数据库。 3.能对已添加的Agent的运行情况进行监控，包括：编号、名称、部署位置、监控的IP地址、操作系统的类型、占用CPU资源以及内存资源情况、运行状态。 4.为保护访问数据安全，支持对日志模糊化处理，防止数据的二次泄密。用户能自定义策略配置，支持风险监控、白名单、黑名单不同策略类型，监控级别能分为高、中、低风险。 5.支持通过首页对全部引擎的审计曲线进行查看，同时支持根据数据库引擎查看单个引擎的审计曲线。且审计曲线支持根据实时、小时、天、周、月的时间维度进行查看。 6.★首页能实时的监控审计设备接收和发送的网络流量，支持对审计设备各网口接收和发送的网络流量进行实时的监控。  7.为实现能够给审计设备存储扩容的目的，支持在页面直接配置挂载硬盘。 8.★产品具有国家认证认可部门、机构颁发的《中国国家信息安全产品认证证书》。 | 1 | 台 |
| 9 | 外网流量探针 | 1. 网络层吞吐量≥500Mbps，应用层吞吐量≥160Mbps，标准1U设备，内存大小≥4G，硬盘容量≥128G minisata SSD，单电源，接口：≥6千兆电口。 2.在产品的系统管理页面可以看到吞出量、接口状态、资源状态等，能够进行可视化展示。 3.产品可以通过IP、业务端口、通讯协议、数据包流向等以自定义的方式来进行应用的识别。 4.产品支持多种形式的攻击检测能力，包括：SQL注入、XSS检测、webshell、JAVA代码的检测、PHP的代码检测等，能够管理员可以自行配置启动检测，选择高效检出低误报模式。 5.★产品通过探测模式可以检测到网络中的网络设备和部署位置的情况，从而能够直观的看到内网的网络状况。  6.系统支持多协议关联分析，能够自动关联不同协议、不同会话的威胁日志，筛选出严重事件，节省事件处理的人力成本。 7.★产品支持对端口异常、上行和下行流量、DNS、ICMP、HTTP、HFS等协议和检测到登录异常的流量进行检测。   8.★需提供产品软件著作权证书。 | 1 | 台 |
| 10 | 漏洞扫描 | 1.系统漏扫授权IP数≥100，WEB漏扫授权URL数≥20；主机漏扫最大并发IP数≥150，WEB漏扫最大并发URL数≥5。 标准1U设备，内存大小≥8G，硬盘容量≥128GB SSD+ 2TB SATA，单电源，接口：≥6千兆电口+2千兆光口SFP。 2.支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。 3.支持从“严重”、“高危”、“中危”、“低危”四个安全级别展示资产的风险分布情况 4.★支持资产发现功能，可基于IP地址、IP网段、IP范围、URL等方式进行资产发现扫描，支持EXCEL格式批量导入。 5.资产发现支持任务立即执行、指定时间执行和周期执行三种执行方式，且指定时间可以精确到分钟，周期执行可精确到每日、每周、每月和自定义周期等。 6.★内置不同的系统漏洞模板，包括高可利用系统漏洞、原理检测系统漏洞、中间件漏洞、数据库漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览，支持报表形式展示漏洞模板详情，包括漏洞总数、漏洞名称、漏洞类型、风险等级等信息。  7.★提供三年产品质保和软件升级服务提供厂家售后服务承诺函。 | 1 | 台 |
| 11 | 分布式存储 | 1.授权存储容量≥50T，标准2U设备，内存≥2\*32GB DDR4 2933，系统盘≥1\*240GB SATA SSD，数据盘≥6\*480G+12\*4T，标配盘位数≥12，冗余电源，接口：≥2千兆电口+2万兆光口。 2.支持硬盘亚健康预、检测和故障自动处理，坏道定时扫描，静默错误检测，能够提前预判硬盘故障风险，做好硬件更换准备，并在界面上做出提示 3.支持对卡慢盘进行检测和隔离处理，避免磁盘卡慢影响集群整体性能，从而对业务体验造成影响 4.当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，快速恢复数据的冗余度，确保用户数据的可靠性和安全性，并能够在界面上显示数据重建进度。 5.★支持对硬件平台的CPU、内存、磁盘、网卡状态进行监控和页面展示，并模拟实物服务器，硬件的故障亮灯展示在监控界面上，比如硬盘故障亮灯.  6.存储内置DNS负载均衡功能，存储根据节点资源开销统计算法选择合适的节点来应答客户端DNS请求，从而实现客户端访问存储集群的负载均衡。 | 3 | 台 |
| 12 | 灾备产品 | 1.标准2U设备，内存≥2\*32GB DDR4 2933，系统盘≥2\*240GB SATA SSD，数据盘≥24T，标配盘位数≥12，冗余电源，接口：≥4千兆电口+4万兆光口。 2.支持对X86下的物理主机、虚拟化主机、超融合主机、云主机提供CDP持续数据保护，实时备份磁盘任意时刻的状态，备份时间粒度最小可达秒级实现RPO趋近于0； 3.支持针对集群业务系统类似于Oracle RAC等整机集群CDP持续数据保护，保障核心应用系统数据完整性。 4.支持任意的小时/天/月/年/仅备份一次等策略执行定时备份，操作简单，策略灵活； 5.支持完整备份和增量备份，第一次备份时使用完整备份保留整机应用的完整状态，后续采用增量备份，大幅减少备份的数据量。 6.★可将选定的备份点加载为CIFS文件共享和网络共享路径可直接在WEB浏览器中直接URL访问，管理员可快速确认需被验证的备份点文件是否是符合预期，备份点是否可用、可靠；  7.可同时启动多个虚拟机对集群业务系统、Oracle RAC等共享存储的集群数据库和应用提供快速整机虚拟化验证 | 1 | 台 |
| 13 | 安全托管服务 | 1. 提供1年7\*24小时运营服务核心资产数≥10。 2.服务方需结合安全工具发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理。 3.服务正式开始前，需对发现的问题进行处置，避免带病上线；包含内网脆弱性问题，病毒类事件，入侵行为，勒索、挖矿类事件等。 4.需提供不少于每月一次针对服务范围内的资产的系统脆弱性和Web漏洞进行全量扫描，并针对发现的脆弱性进行验证。针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案。 5.对发现的脆弱性建立状态总览机制，自动化持续跟踪脆弱性情况，清晰直观地展示脆弱性的修复情况，遗留情况以及脆弱性对比情况，使得招标方可做到脆弱性的可视、可管、可控。 6.策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新。 7.支持面向客户的安全态势展示，展示出当前招标方遭受的威胁事件信息以及脆弱性信息统计，并支持服务专家按照资产类别、威胁类型进行定制化筛选查看，能直观感受到客户当前的风险态势情况。   8.★为保证运维便捷提升安全防护效果所提供服务需能与已采购的终端杀毒软件进行深度联动处置。  9.★服务平台支持面向招标方的安全报告与交付物管理，可生成、导出、下载各类安全报告，包括但不限于《安全服务值守日报》、《特殊时期值守报告》、《安全运营周报》、《安全运营月报》。 | 1 | 套 |
| 14 | 等保测评服务 | 对医院的 HIS 系统进行三级等保测评服务。 | 1 | 次 |