**二、具体要求**

1. 采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **单位** | **预算** |
| 机房环境安全 | | | | 129万 |
| 1 | 蓄电池 | 448 | 节 |
| 2 | 电池监测模块 | 448 | 个 |
| 3 | 数据转换传输模块 | 14 | 个 |
| 4 | 电解气体探测器 | 3 | 套 |
| 5 | 电池监控软件集成 | 1 | 项 |
| 6 | 电解气体软件集成 | 1 | 项 |
| 7 | 综合监控管理软件升级 | 1 | 项 |
| 数据备份安全 | | | |
| 8 | 备份服务器 | 2 | 台 |
| 9 | 备份软件 | 1 | 套 |
| 10 | 备份集成服务 | 1 | 项 |
| 安全态势感知 | | | |
| 11 | 潜伏威胁探针系统 | 1 | 台 |
| 12 | 安全感知平台 | 1 | 台 |

1. 具体要求

|  |  |  |
| --- | --- | --- |
| **序号** | **设备名称** | **技术要求** |
| 1 | 蓄电池 | 12V,100AH；阀控密闭式铅酸胶体电池；电池要求为原厂生产电池，拒绝OEM产品，蓄电池生产厂家需符合国家工业和信息部铅酸电池行业规范条件（2015年本）企业准入资格, 保证蓄电池产品质量安全可靠。投标时提供原厂盖章的相关证书予以证明。原有旧电池需由中标单位委托符合环保要求（投标时提供相应证书复印件）的第三方单位进行清理回收，费用在蓄电池报价中综合考虑。  中标方供货时甲方将对电池质量包括重量、规格等进行核查，若发现有质量问题的将提交第三方检测，其费用均由中标方承担。 |
| 2 | 电池监测模块 | ▲监测每节电池的内阻、电压、电流及表面温度等参数；输出接口模式：支持单模光纤接口；电池电压：精度优于0.2%；总电压：精度优于0.5%；模拟量：精度优于1%；  年漂移量：< 0.1%；电池内阻测量精度：0.1%。投标时提供彩页并原厂盖章。 |
| 3 | 数据转换传输模块 | 规格：支持透明传输，支持MODBUS RTU转MODBUS TCP网关协议；供电：12V DC；串口：DB9；功能：自动侦测10M/100m以太网，支持ETHERNET、ARP、IP、UDP、TCP、ICMP协议；可选工作模式：TCP Server、TCP Client、UDP Server、UDP Client,MODBUS TCP,MODBUS-RTU,等多种模式，支持跨网关，跨路由通信，TCP SERVER模式支持4个TCP链接。  投标时提供原厂盖章的产品彩页以及与原有监控管理平台数据传输对接的技术实现方式的详细说明。 |
| 4 | 电解气体探测器 | ▲采样方式：扩散或管道；传感形式：电化学；测量范围：0-100%；  分辨率：±0.5%；负载电阻：500欧姆；防爆级别：Ex d IIC T6；  外壳保护：IP65；输出接口： RS485。  投标时需提供产品彩页并原厂盖章。 |
| 5 | 电池监控软件集成 | ▲通过软件二次开发读取每一节电池的电压、电流、内阻以及表面温度等数据，数据与原有机房综合监控管理软件无缝对接。投标时需提供原厂盖章的无缝集成的证明文件详细阐述无缝集成的具体实现方式的技术说明及相关的软件界面截图。 |
| 6 | 电解气体软件集成 | ▲通过软件二次开发UPS设备间各个区域的电解气体浓度数据，监控数据要求与原有机房综合监控管理软件无缝对接。时需提供原厂盖章的无缝集成的证明文件详细阐述无缝集成的具体实现方式的技术说明及相关的软件界面截图。 |
| 7 | 综合监控管理软件升级 | ▲增加原有综合监控管理平台的数据接入量，不少于50个license接入点(提供原厂盖章的证明文件)。项目所有的监测数据与原有管理平台无缝对接，实现统一管理。所有告警量数据短信告警与甲方原有监控平台无缝对接（提供无缝对接的证明文件）。投标时提供国家版权局颁发的有效的软件著作权证书。 |
| 8 | 备份服务器 | |  |  | | --- | --- | | **指标项** | **技术要求** | | 高度 | ≤2U机架式 | | 外观 | 配置滑动导轨 | | 配置带有安全锁前置机箱面板 | | 处理器 | 配置≥两颗Intel® Xeon® 铜牌3204可扩展处理器 | | 内存 | 配置≥64GB RDIMM，2666MT/s； | | 持久内存 | 最多支持12条NVDIMM；多达192G； | | 快擦硬盘/SSD | 服务器生命周期结束或者挪作它用时一键删除硬盘/SSD所有信息 | | 硬盘 | 配置≥2块600G 10K SAS 2.5英寸硬盘，10\*4T 7200RPM SATA硬盘； | | RAID卡 | 配置≥2GB高速缓存，支持RAID 0、1、5、6、10、50、60 | | RAID卡 缓存 | 最大支持8GB； | | M.2 SSD | 支持硬件Raid1，可用于部署虚拟化 | | PCI-E插槽 | 支持≥8个PCIe 3.0插槽； | | 网卡 | 配置≥4个1GE+2个10GE SFP+（含原装万兆光模块） ；支持25Gb网卡 | | DVD | 配置DVD光驱 | | 电源 | 配置2\*750W 冗余电源（1+1） | | VMware支持 | 提供VMware vCenter集成插件支持， | | Microsoft支持 | 提供Microsoft System Center集成插件支持， | | Oracle支持 | 提供Oracle Enterprise Manager集成插件支持 | | WIFI和蓝牙 | 支持本地WIFI和蓝牙方式管理技术，支持手持移动端管理； | | 易用性 | 服务器主板集成部署管理工具,能够免光盘安装服务器，安装管理服务器更加简单。 | | 管理 | ▲配置独立远程管理卡，支持远程监控图形界面，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开关机、重启、更新Firmware、虚拟KVM、虚拟软驱、虚拟光驱等操作 | | 功耗管理 | 虚拟机功耗映射，可以根据功耗对于虚拟机进行负载平衡以及按虚拟机报告功能 | | 安全 | ▲系统锁定特性，防止对BIOS，firmware，管理控制台 的非法访问和修改。 | | 性能分析软件 | ▲提供原厂性能分析软件，支持无代理远程运行，支持分析CPU、内存、IOPS、带宽等性能指标，提供原厂性能分析报告模板； | | 服务 | ▲原厂商5年硬件免费保修，原厂工程师7 x 24 x 4小时免费上门服务，配置3年服务器硬盘故障免回收。 | |
| 9 | 备份软件 | |  | | --- | | **1）、数据管理平台要求** | | ▲国际知名品牌，非OEM，要求投标产品为VMware全球合作伙伴联盟成员，投标时提供本次配置品牌对应的VMware官网截图 | | ▲投标产品须在VMware服务器虚拟化产品的兼容性列表中，以VMware官方网站截图为准 | | 支持 VMware vSAN深度集成，且获得VMware ready官方认证 | | 单一产品同时支持备份、还原、复制和容灾解决方案 | | 全面支持VMware vSphere、Microsoft Hyper-V和Nutanix AHV平台 | | **2）、数据备份特性** | | 无须在每一台虚拟机上安装代理程序 | | ▲无代理方式备份、复制和还原关键应用（Oracle, SQL, Exchange, SharePoint, AD以及其它应用系统） | | 支持应用程序一致性的映像级虚拟机备份和复制 | | 能够通过vCenter或者单个ESX /ESXi主机, 充分利用VSphere API进行数据保护 | | 支持VMware vSphere的块改变跟踪（CBT）技术, 或Microsoft Hyper-V虚拟机的 弹性变化跟踪（RCT）技术进行备份 | | 能够在备份作业运行期间动态的增加新虚拟机 | | 支持依据实际环境选择LAN、LAN-free或者Server-free备份，并能够自动选择最佳备份方式 | | 支持NFS直接访问，可通过基于文件的 (NFS) 主存储中直接备份，能够更快地执行 VSphere 备份、复制和还原，并降低对虚拟化环境的影响 | | 支持Windows/Linux Guest OS VIX接口, 在无法建立与VM的直接网络连接情况下，通过VIX接口，依然支持文件系统索引，应用感知处理，及文件级还原等操作 | | 支持从vSAN智能读取数据，选择最佳备份路径；并支持VMware SPBM策略的自动备份和还原 | | 支持thin模式和thick模式磁盘分配的虚拟机 | | 在设定的时间段内，过期的虚拟机备份镜像文件可以自动删除以节省存储空间 | | 支持对备份I/O进行设置，以确保备份和复制活动不会影响用于满足生产负荷的存储可用性 | | 支持正向增量/反转增量/合成全备份等备份方法 | | 能够从备份作业中排除虚拟机特殊类型的虚拟磁盘、单个文件或者文件夹，支持排除临时文件块以及交换空间、被删除文件块等无效数据块 | | 加密、重复数据删除和压缩功能已内嵌在软件中无须额外购买 | | 支持重复数据删除,可根据不同的网络环境来自定义数据去重的块大小 | | 可以并行和顺序处理备份作业 | | 支持备份到磁盘设备（包括DAS、SAN、NAS存储等）、LTO规格的磁带（备份和归档文件到磁带,归档备份文件到磁带）、以及具有去重功能的专业备份设备（例如：Dell EMC Data Domain Boost、HPE StoreOnce Catalyst 和 ExaGrid Accelerated Data Mover） | | 支持备份到对象存储，通过与内部、AWS、Microsoft Azure、IBM Cloud 及多种兼容 S3 的存储产品的原生对象存储集成。可同时提供复制和迁移功能，以支持在对象存储上进行长期保留。同时支持使用 S3 对象锁来锁定对象存储库并实现不可变性，进而防范勒索软件 | | 支持横向扩展式备份存储库，通过由软件定义的单一备份存储库来管理多个异构存储设备，可提升备份性能，降低存储硬件开支，降低维护风险。用户可利用密封模式来密封保护和安全范围，或者按计划逐步淘汰存储设备 | | 支持通过利用存储快照技术（Dell EMC、NetApp、HPE、Nimble、IBM、Lenovo、Cisco HyperFlex、 DataCore、富士通、华为、INFINIDAT、Pure Storage、等）来备份和复制虚拟机，减低物理服务器负载，实现更快速的虚拟机和应用程序保护 | | 支持广域网加速器，提升广域网虚拟机或备份数据容灾的性能，减小网络带宽占用 | | 可以对 Oracle RAC、物理 ASM 和 Oracle 容器数据库使用 RMAN 备份传输至备份存储库，支持 Oracle 数据库企业版的指向多个备份目标的同步备份副本，有可视化恢复工具对Oracle进行本机恢复及异机恢复 | | 可充分利用原生 SAP HANA 数据库方法简化备份与恢复；将 SAP HANA 备份传输至备份存储库；将增强的功能和用例用于现有脚本和调度方法 | | NAS备份支持NDMP备份到Tape设备。  支持SMB(CIFS) 版本1，2，3文件共享和NFS 版本3，4文件共享的备份。  支持Windows和Linux文件服务器的备份。  支持只备份指定的共享目录，而无需备份整个卷，从而减少备份的数据量，节省备份存储空间和缩短备份时间窗口。 | | NAS备份支持全备+永久增量的备份方式。  通过创新的文件变化跟踪（CFT）功能，加快NAS的增量备份，为PB级非结构化文件数据提供可扩展架构保护。  通过VSS快照备份方式和存储快照备份方式，支持对打开文件或锁定文件的备份，同时提高NAS备份性能和速度。 | | NAS备份数据支持短期保留和长期保留功能，将非结构化 NAS 备份数据灵活存储在成本更低的存储上。  支持备份数据第二副本的创建，可以基于不同的保留周期和不同的备份存储池。  NAS备份存储支持磁盘存储、内部和云对象存储、和专业去重设备等。 | | 支持仅基于存储快照的VMware vSphere虚拟机备份任务，用于大压力虚拟机备份 | | **3）、数据复制特性** | | ▲提供接近CDP级别的复制容灾功能，内置在产品中无须额外购买，提供原厂技术说明 | | ▲能够从生产中心和容灾中心的备份文件快速启动虚拟机接替生产，而无需将备份文件先恢复到生产存储,提供原厂技术说明 | | 提供一键故障切换机制，通过流程式的故障切换机制减低故障切换风险 | | 能进行应用一致性复制（包括Oracle, SQL, Exchange, SharePoint, AD以及其它应用系统） | | 虚拟机复制具备IP地址变更功能，方便容灾切换时虚拟机快速启动并接管业务 | | 虚拟机容灾具备从备份数据中抽取有效数据，用于加速建立初始容灾虚拟机功能 | | 虚拟机容灾具备可在第一次容灾复制时，对比生产虚拟机和容灾虚拟机的差异，只传输差异数据，用于加速建立初始容灾虚拟机功能 | | **4）、数据恢复特性** | | 能够支持整个虚拟机恢复、虚拟机文件、虚拟磁盘恢复，支持直接从备份文件中启动虚拟机和业务系统，同时支持将备份虚拟机直接恢复到公有云中（AWS、Microsoft Azure 和 Microsoft Azure Stack） | | 支持将任何本品牌的备份即时恢复至VMware vSphere，包括物理服务器或工作站，虚拟机或云实例等恢复为VMware vSphere VM。 | | 即时恢复引擎使用可识别工作负载的缓存，实现更好的的恢复性能。 | | 支持批量VM即时恢复，一次启动多个VM的还原，可将多个虚拟机应用快速恢复在线，轻松执行大规模即时还原，减少了与恢复和迁移操作相关的停机时间。 | | 支持即时还原单个磁盘，仅还原所需的磁盘，以减少即时还原的空间，即时将磁盘从备份装载到选定的VM。 | | 能够提供Guest OS层面的文件级即时恢复 | | 能够从EMC、HPE、NetApp、Nimble、IBM、Lenovo等企业存储级快照中恢复单个虚拟机、客户机操作系统文件或应用程序及程序中的子项目，还包括快照任务中的事务日志处理 — 以支持 Oracle 和 SQL 通过快照进行时间点恢复。 | | 能够备份并恢复虚拟机的配置文件，比如vSphere虚拟机的vmx文件 | | 能够支持无代理应用-条目级恢复（用于MS SQL 、Exchange、AD 、SharePoint、Oracle以及其它应用） | | 能够搜索和还原所有AD对象类型，包括用户、组、计算机账号、联系人以及计算机密码的恢复，多选还原、容器恢复、组策略对象还原等 | | 能够实现对单个Exchange项目（电子邮件、备份、联系人）、硬删除项目的项目恢复，支持还原回原始邮箱 | | 还原单个 SQL 数据库，支持本地时间点导出 SQL 数据库文件，无代理事务日志备份和重播，支持将数据库和 SQL 对象（表、存储的程序、视图等）事务级还原至原始或新 SQL 服务器的功能 | | 支持 SharePoint 细粒度还原并可对还原的项目执行保存、发送和导出操作.还支持还原至原始位置的功能 | | 还原单个 Oracle 数据库，包括无代理事务日志备份、存档日志管理以及将数据库事务级还原至原始或新Oracle 服务器的功能，并支持快速发布和导出Oracle数据库的功能 | | 可通过 Web 用户界面进行一键式的自助式恢复，包括文件、应用程序和虚拟机等 | | 通过Web访问的方式，可将恢复任务委派给特定用户或用户组，从而能够实现所有 Web UI 自助恢复功能 | | 提供NAS备份数据的多种恢复选项 —完整共享恢复、基于时间点共享恢复及文件级恢复（带支持日常运营恢复的全局搜索功能）。 | | **5）、数据利用特性** | | 自动验证备份映像和复制副本以确保虚拟机和应用程序可正常恢复,无需人工干预.自动检查相应虚拟机，操作系统和应用程序来确保可恢复性.验证报告邮件可配置为自动向管理员发送 | | 可实现安全的恢复验证，能够通过可选的实时杀毒扫描，扫描和验证备份，以提高安全性和减少病毒引起的中断事件；恢复至安全、未受感染的恢复点；为 Windows Defender、ESET 和 Symantec Protection Engine，及扩展至其他第三方杀毒工具提供独立支持。 | | 支持在隔离环境内直接从备份或者复制副本运行一个或多个虚拟机，能够在不影响业务运营的情况下进行故障排除、测试 | | 具备数据实验室功能，可以借助自定义脚本和自动化简化敏感数据的删除流程，如 GDPR（被遗忘权）；为确保安全、快速地恢复至生产阶段，先在隔离的生产环境中测试数据 | | 支持使用存储快照创建完全隔离的生产环境副本，以便快速轻松地进行测试和故障排除 | | **6）、管理特性** | | 提供基于独立控制台和Web两种管理方式。 | | 提供基于web方式的集中管理控制台，可同时管理多台备份服务器、集中报告和整合警报，支持启动和停止作业，以及执行还原的功能。 | | 可集中部署云端、虚拟和物理平台的管理工具，提供查看所有备份和恢复的单一平台。 | | 支持设置不同的用户权限，设置特定的用户只能查看备份状态或者进行恢复操作 | | 具备基于角色的访问控制 (RBAC)管理功能，可向用户授予创建、恢复和监控备份的角色和特权；将第三方授权系统中实施的权限与 VMware vSphere 权限同步；利用单个账户或安全组控制备份存储位置和配额。 | | 任务自动化支持RESTful API 和 PowerShell命令 | | **7）、配置要求** | | 包含3年原厂服务，包括：版本升级、补丁更新、原厂电话支持，Web门户支持、原厂知识库等等。  配置6CPU备份授权 | |
| 10 | 备份集成服务 | 1、完成学校虚拟化平台的备份，原虚拟化平台为VMWARE平台，平台运行学校关键数据库平台，需要具备专业技能的人员进行项目实施，要求实施团队具备备份软件认证工程师、vmware虚拟化工程师，Oracle认证工程师共同参与。  2、在服务期内，对本次所供设备提供每周7\*24小时、全年365天的技术服务支持，包含版本升级、补丁更新、原厂电话、Web门户支持、原厂知识库等等，提供电话支持和现场服务支持，并在规定的时间内完成。  3、在服务期内，每半年需要提供一次容灾演练，确保数据的可用性。事先安排好应急演练措施及流程，并和用户确认后方可进行，记录在《关键设备维护审批表》中。  4、在服务期内，对所供设备进行每季度一次例行巡检保养，并出具书面巡检报告及时发现并排除设备故障，确保设备及系统的正常运行。  5、定期组织技术交流及工作汇报会，向校方提供技术资料共享服务 |
| 11 | 潜伏威胁探针系统 | |  |  | | --- | --- | | **指标项** | **技术要求** | | 品牌要求 | 与安全感知平台为同一品牌 | | 性能指标： | 性能：4.5Gbps，硬件参数：2U，SATA 1T，标配6个千兆电口+4个千兆光口+2个万兆光口 | | 部署模式 | 旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响 | | 监测识别规则库 | 能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在4000条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号 | | 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（需提供截图证明） | | 支持DNS审计日志，主要用于平台dns flow分析引擎进行安全分析；HTTP审计日志，主要用于平台http flow分析引擎进行安全分析；SMB审计日志，主要用于平台SMB flow分析引擎进行安全分析；同步SMTP、POP3、IMAP审计日志，主要用于平台Mail flow分析引擎进行安全分析，同步AD域协议审计日志，主要用于平台AD域分析引擎进行安全分析（需提供截图证明） | | Web应用安全检测能力 | 支持针对B/S架构应用抵御SQL注入、XSS、系统命令等注入型攻击；支持跨站请求伪造CSRF攻击检测；支持对ASP,PHP,JSP等主流脚本语言编写的webshell后门脚本上传的检测；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等的检测；（要求对以上列出的攻击类型进行逐条响应并提供相应的功能界面截图）  支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤；（需提供截图证明） | | 僵尸网络检测 | 支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；（需提供截图证明） | | 违规访问检测 | 能够针对IP，IP组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式（需提供截图证明） | | 沙盒对接 | 支持将流量还原的文件发送至沙盒进行静态检测和动态模拟执行，可支持第三方沙盒对接（需提供截图证明）。 | | 抓包分析 | 支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式（需提供截图证明） | | 集中管控 | 支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级；（需提供截图证明） | | 防火墙设备联动 | 支持与我校现有防火墙进行联动响应，支持平台自动下发安全策略到防火墙上，阻断攻击流量。（需提供截图证明） | | SSL VPN设备联动 | 支持与我校现有SSL VPN设备同步用户用户信息，包括用户登录、登出、分配IP、访问资源记录的日志数据，实现远程接入用户与安全事件关联分析，分析出异常用户，以VPN用户为可视化视角，呈现风险问题、风险程度、内网资源访问情况等。支持同步管理员操作日志，满足审计要求（需提供截图证明）。 | | 产品资质 | 要求具备公安颁发的网络入侵检测系统销售许可证 | | 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，提供相关证明材料  厂商为国家信息安全漏洞共享平台CNVD用户组成员，提供CNVD官网截图证明； | |
| 12 | 安全感知平台 | |  |  | | --- | --- | | **指标项** | **技术要求** | | 性能指标 | 硬件指标：2U，96G内存，SSD 128G系统盘、SATA 32T存储、双电源，RAID50、标配4个千兆电口； | | 综合安全态势大屏 | 支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势，支持页面跳转到对应态势大屏；（需提供截图证明并加盖原厂商公章） | | 访问关系梳理大屏 | 支持大屏展示正常横向访问和正常外连监控，正常横向访问监控包括被访问最多的业务TOP5、最活跃终端TOP5、应用TOP5、实时访问监控等，正常外连监控包括外连最多的业务TOP5、外连最多终端TOP5、外连态势、外连国家TOP5,并支持国际、国内地图切换（需提供截图证明）。 | | 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（需提供截图证明）。 | | 业务风险外连态势 | 支持大屏展示业务外连态势，包括外连风险总览、外连威胁TOP10、外连态势、外连地区TOP5、实时威胁监控；支持国际、国内地图自主切换（需提供截图证明并加盖原厂商公章）。 | | 访问关系梳理大屏 | 支持大屏展示正常横向访问和正常外连监控，正常横向访问监控包括被访问最多的业务TOP5、最活跃终端TOP5、应用TOP5、实时访问监控等，正常外连监控包括外连最多的业务TOP5、外连最多终端TOP5、外连态势、外连国家TOP5,并支持国际、国内地图切换（需提供截图证明）。 | | 多视角大屏展示 | 支持综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势、正常横向访问监控、正常外连监控、设备运行态势11个独立的大屏展示功能，并支持大屏轮播，可自定义大屏轮播顺序（需提供截图证明） | | 与现有设备对接 | 为了方便设备的统一管理和运维，要求安全感知平台能与我中心现有的上网行为管理和SSL vpn设备实现联动对接，（提供设备对接截图证明）。 | | 弱密码 | 支持检测15类以上常见协议的弱密码,包括HTTP、FTP、LDAP、VMWARE、ORACLE、VNC等类型协议，检测列表包含账号、密码、服务器、所属分支和业务、最近登录源IP、类型、最近发现时间等信息，密码星号显示需超级管理员才可查看，并支持储存数据包；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（需提供截图证明）。 | | 配置不当 | 支持基于流量检测业务服务器的配置不当情况，检测列表包含服务器、所属业务、所属分支、配置不当类型、风险等级、发现时间等，支持配置不当类型下钻，展示配置不当详情，提供解决方案和数据包举证，并支持导出配置不当报告（需提供截图证明）。 | | 漏洞报告 | 支持基于流量实时漏洞功能，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、目录遍历漏洞、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。（需提供截图证明）。 | | 威胁分析 | 横向威胁感知展示包含横向威胁总览、横向攻击、违规访问、可疑行为、风险；其中横向风险总览包含发起与遭受横向威胁主机TOP5，发起视角包含发起者IP、发起者类型、所属分析、所属业务/终端组、横向威胁类型、遭受者数、遭受者类型、日志数（需提供截图证明） | | 外部智能分析 | 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，支持攻击事件列表详情里面还包括遭受攻击主机、攻击者来源区域、攻击手段、攻击次数、持续时间等（提供产品功能截图） | | 挖矿专项检测 | 具备挖矿专项检测，可实时查看挖矿各个攻击阶段，包括感染挖矿病毒、与控制端建立通信、获取挖矿任务、尝试挖矿、挖矿成功等；并支持挖矿币种分布、挖矿风险态势、受影响主机等维度分析统计（提供产品功能截图） | | UEBA异常行为分析 | 支持不同场景下数据库异常模型的算法编辑，可选择稀有值检测算法、ZScore异常检测算法、箱线图异常检测算法；可将不同类型的算法应用到不同的资产（需提供截图证明） | | 外网暴露面梳理 | 支持内网对外服务器外网暴露面分析，包括内网IP、资产名称、所属资产组、域名/URL、外网IP、策略已开放、实际被使用、关联防火墙、关联应用策略、存在风险、处置状态等，并支持导入与导出（需提供截图证明） | | 核心服务器梳理 | 支持核心服务器暴露面分析，包括内网IP、资产名称、所属资产组、策略允许访问、策略已开放、实际访问、实际被使用、关联应用控制策略、存在风险、处置状态等，并支持导入与导出（需提供截图证明） | | 等级保护管理服务 | 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（提供证明文件） | | SSL VPN设备联动 | 支持与我校现有SSL VPN设备同步用户用户信息，包括用户登录、登出、分配IP、访问资源记录的日志数据，实现远程接入用户与安全事件关联分析，分析出异常用户，以VPN用户为可视化视角，呈现风险问题、风险程度、内网资源访问情况等。支持同步管理员操作日志，满足审计要求（需提供截图证明）。 | | 上网行为设备联动 | 支持与我校现有上网行为管理设备进行联动响应，同步上网行为管理设备认证用户，实现与安全事件关联；支持通过浏览器推送用户提醒或冻结用户上网；（需提供截图证明，中标后进行演示）。 | | EDR组件联动 | 支持与我校终端EDR组件联动，支持平台自动下发策略禁止攻击流量出入站、一键病毒查杀、进程取证；支持反馈查杀的病毒信息和恶意域名通信的进程信息（需提供截图证明，中标后进行演示）。 | | 防火墙设备联动 | 支持与我校现有防火墙进行联动响应，支持平台自动下发安全策略到防火墙上，阻断攻击流量。（需提供截图证明，中标后进行演示） | | 深度检测引擎升级 | 具备安全日志分析引擎、DnsFlow行为分析引擎、HttpFLow分析引擎、NetFLow分析引擎、MailFLow分析引擎、SmbFLow分析引擎、威胁情报分析关联引擎、第三方安全检测引擎、文件威胁检测引擎等，支持定期自动升级或离线手动升级（需提供截图证明）。 | | 暴力破解检测 | 支持开启暴力破解实时检测，自动封堵攻击源的IP地址，封停时间支持配置；（提供界面截图证明） | | 支持展示终端检测到的暴力破解事件及事件详情，包括：攻击源、攻击类型、检测引擎、最后攻击时间、攻击方法、攻击内容、攻击历史；（提供界面截图证明） | | 基线合规检查 | 针对Linux系统提供如下安全基线合规检查：身份鉴别、访问控制、安全审计、 SSH策略检测、入侵防范、恶意代码防范；（提供界面截图证明） | | WebShell检测 | 支持配置WebShell实时扫描，一旦发现WebShell文件，自动隔离或仅上报不隔离。（提供界面截图证明） | | 支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，事件等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间，检测依据；（提供界面截图证明） | | 厂商资质 | 厂商需是中国反网络病毒联盟ANVA成员单位；  厂商是微软安全响应中心的MAPP计划成员  厂商为国家信息安全漏洞共享平台CNVD用户组成员，提供CNVD官网截图证明并加盖厂商公章 | |

## 三、商务要求

★**(一)交货期及交货地点**

交货时间：合同签订后30天内交货并安装完成；

地点：浙江中医药大学，甲方指定地点；

质保期：5年，验收合格第2个月起算。