|  |  |  |
| --- | --- | --- |
| **名称** | **产品说明** | **数量** |
| 日志审计 | 1.规格：2U，内存大小≥16G，硬盘容量≥128G SSD+4T SATA，接口≥6千兆电口+2万兆光口。要求提供产品必须支持国产化芯片和国产化操作系统  2.包含主机审计许可证书数量≥100，可扩展审计主机许可数≥500，可用存储量≥4TB（RAID0 模式），平均每秒处理日志数（eps）性能≥2500。  3.可自定义设置日志存储天数，容量告警提示等；满足存储超过6个月以上的合规要求  4.基于logstash的接入架构，可供多台设备同时接入同步数据，并实时分析展示  5.支持600种以上的第三方日志采集器（需提供截图证明）  6.要求具备公安颁发的日志分析（一级）安全专用产品销售许可证  7.要求具备国家版权局颁发的软件著作权登记证书  8.要求提供三年软件升级和产品质保服务 | 1 |
| 数据库审计 | 1.提供30个数据库实例；SQL处理性能≥3万条SQL/s，日志检索性能≥40万条/秒。  2.吞吐量≥2Gbps，最大数据库纯SQL流量≥400Mb/s，要求为国产化产品，支持国产操作系统  3.硬盘容量≥128G SSD+4T SATA，接口≥6千兆电口。电源：单电源。  4.支持主流数据库和国产数据库  5.可以通过自定义交互分析设置正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统、风险总次数这几个维度实时监控内网数据威胁态势并且提供交互式分析视图帮助快速溯源。（提供界面截图证明）  6.要求具备公安颁发的安全管理平台销售许可证  7.要求具备中国国家信息安全产品认证证书  8.中国信息安全认证中心《中国国家信息安全产品认证证书》  9.要求提供三年软件升级和产品质保服务产品质保（标准版）(\*3年); | 1 |
| 堡垒机 | 1.硬盘容量≥64GB SSD+1TB SATA，接口≥6千兆电口，≥4千兆光口SFP。包含运维授权数不少于300个，图形运维最大并发数不低于50个。字符运维最大并发数不低于100.要求所投产品必须支持国产化芯片和国产化操作系统  2.字符协议：SSHv1、SSHv2、TELNET；文件传输协议：FTP、SFTP、RDP磁盘映射、RDP剪切板；图形协议：RDP、VNC；支持通过协议前置机进行协议扩展，至少支持扩展KVM、Vmware、数据库、http/https、CS应用等  3.支持通过动作流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（提供截图）  4.支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期  5.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（提供截图）  6.支持Windows AD域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号（提供截图）  7.内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴（提供截图）  8.支持unix资源、windows资源、网络设备资源、数据库资源、C/S资源、B/S资源  9.支持批量导入、导出资源信息；支持手动添加、删除、编辑、查询资源，支持变更默认运维端口  10.支持RDP安全模式（RDP、NLA、TLS、ANY）设置，以适应RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合FIPS标准等加密级别（提供截图）  11.支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开  12.支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯  13.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  14.要求具备公安颁发的安全管理平台销售许可证  15.要求具备中国国家信息安全产品认证证书  16.要求提供三年软件升级和产品质保服务 | 1 |