**堡垒机（运维审计系统） 技术要求：**

1. 标准2U机架式，≥6个千兆电口,支持≥2个接口扩展槽位，内置≥4TB硬盘，冗余电源，支持液晶屏，最大支持≥300路图形会话或≥800路字符会话并发。（说明：默认资源数≥100）含三年标准售后服务。
2. 支持物理旁路，逻辑串联模式，不影响正常业务流量，HA双机热备。
3. 支持基于水平可扩展的集群化架构设计与部署，支持跨地域、跨数据中心，多层次部署。
4. 支持NAT地址映射部署，通过映射后的IP地址访问堡垒机。
5. 支持SSH、RDP、TELNET、VNC、FTP、SFTP协议主机，支持发布MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client类型的应用。
6. 支持资源按标签管理，每个用户可以给每个资源打多个标签。
7. 支持导入阿里云、华为云、腾讯云和Ucloud等平台云主机。
8. 支持TELNET、SSH协议资源使用普通账户自动切换到root（或enable）账户。
9. 必须支持无需安装任何客户端，便可windows、linux、MAC OS等类操作系统登录堡垒机，并访问管理资源；支持IE、Edge、Chrome、FireFox、Safari等主流浏览器；提供截图证明，并加盖厂商公章。
10. 支持访问控制策略基于用户、用户组、资源账户、账户组、有效期、文件管理控制、文件传输控制（上传、下载）、RDP剪切板控制、时间限制、IP限制进行设置。
11. 支持访问控制策略支持配置双人授权候选人，针对核心设备，需要管理员现场审批才能操作。
12. 支持支持查看改密日志，了解改密账户总数、改密成功数量、改密失败数量和未修改数量；改密日志支持下载，查看改密前后密码变化。
13. 支持批量登录：支持SSH、RDP、TELNET、VNC协议资源的批量登录功能；支持SSH客户端、FTP客户端、SFTP客户端访问目标资源。
14. 支持通过堡垒机同时对多台网络设备执行相同命令；提供截图证明，并加盖厂商公章。
15. 提供类似云盘形式的文件存储，支持RDP、SSH、VNC协议类型主机的文件上传和下载，并进行审计。
16. 必须支持会话协同：运维过程中支持会话协同，可邀请其他用户参与、协助操作。会话协同过程中，支持参与者控制会话，同时支持创建者强制获取控制权。支持多个参与者使用相同的会话邀请链接进入会话，提供截图证明，并加盖厂商公章。
17. 预置命令：支持字符协议预置命令功能，可添加多个经常使用的命令在系统当中。
18. 系统内置多种系统报表和运维报表模板，支持按日、周、月为周期，自动生成报表。
19. 对剪切板拷贝文件行为和文本信息内容的记录，并支持通过搜索文本内容关键字定位审计回放。

**防病毒软件（终端安全管理软件） 技术要求：**

1. 产品分为服务器端和客户端两个部分，控制中心采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、网络流量管理、硬件资产管理以及各种报表和查询等功能。
2. 具备至少400个PC客户端授权，客户端具备防病毒功能、补丁静默升级。控制非法流量探测，外联等功能。含三年升级服务流量管理功能，可无缝兼容Windows XP、windows 7、windows 8、windows 10等操作系统，至少具备三年升级服务。
3. 投标产品具备至少20个服务器授权，针对Windwos Server操作系统进行病毒查杀能力，补丁管理功能，支持对全网终端系统漏洞发现、补丁智能修复、强制修复等、蓝屏修复、补丁分发流量控制、客户端P2P补丁分发加速等功能，系统默认支持windows server 2003、windows server 2008、windows server 2012操作系统，含三年病毒库升级服务。
4. 要求产品具备公有云检测能力，并且有公有云特征储备。
5. 支持私有云查杀，终端威胁统一到控制中心查询黑白并进行查杀。（提供证明，并加盖公司公章）。
6. 产品支持在断网状态下具备不依赖病毒库特征的情况下对未知病毒查杀的能力。
7. 产品支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件。
8. 支持文件审计，对全网终端的所有文件保持完整的审计，方便鉴定恶意软件从何而来并立即阻止恶意软件继续运行。
9. 支持正版软件的正版序列号的读取功能，确保软件正版化，支持软件变更，展示终端软件变动记录，可确认变更或删除记录。
10. 支持手动配置服务器、扫描参数、进行周期性扫描，可手动配置发现的终端类型，支持自动发现设备的IP-MAC地址的绑定。
11. 产品具备软件管理功能，支持软件监控，按软件显示展示全网安装的软件和涉及的终端；按终端显示展示全网每个终端安装的软件。
12. 支持通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件。
13. 支持冗余有线网卡、无线网卡、3G网卡、MODEM、ADSL、ISDN等设备的外联控制；违规外联发生时可针对内外网连接状态分别设置违规处理措施。
14. 产品支持外设管理，对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）等设置使用权限。
15. 产品支持漏洞利用防御，尤其对通过文件漏洞（尤其是0day漏洞）的攻击行为进行有效检测与防御。（提供功能截图，并加盖公司公章）
16. 对敲诈者病毒提供防护机制，同时提供解密工具。产品支持桌面安全加固，对终端桌面系统的账号密码、本地安全策略、控制面板、屏保与壁纸、浏览器安全、杀毒软件等检查。
17. 具备防止误配置或策略漏洞，有效避免设备带漏洞入网和运营。
18. 产品支持脆弱性评估，评定终端配置的脆弱程度。
19. 产品支持与防火墙联动，达到从终端防护到网关边界联动防御效果。