1. **采购清单及预算**

|  |  |  |  |
| --- | --- | --- | --- |
| 产品名称 | 主要参数 | 数量 | 规格要求 |
| 终端安全管理系统 | **★**终端安全管理系统维保，包含Windows PC功能授权（包含防病毒+补丁管理+主机防火墙+终端管控+移动存储+停服系统加固），提供一年软件升级和技术支持服务。 | 1010套 | 详见技术参数要求 |
| **★**终端安全管理系统维保，包含Windows server授权（防病毒+补丁管理），提供一年软件升级和技术支持服务。 | 15套 | 详见技术参数要求 |
|  | **★**终端安全管理系统维保，包含 Linux服务器授权（防病毒），提供一年软件升级和技术支持服务。 | 2套 | 详见技术参数要求 |
| 服务器安全管理系统 | **★**服务器安全管理系统维保，包含包括资产梳理、风险发现、病毒扫描、安全基线、入侵检测等功能，提供一套控制中心，提供一年软件升级和技术支持服务。 | 100套 | 详见技术参数要求 |
| 1、★中标后需提供原厂商针对本项目的一年质保服务承诺函。  2、文件中所有打★条款为必要条件，如出现负偏离作为无效报价处理。 | | | |

1. **技术参数要求**

2.1终端安全管理系统

|  |  |  |
| --- | --- | --- |
| 技术指标 | | 指标要求 |
| 平台环境要求 | 产品形态 | 软件形态，包含管理控制中心、客户端软件 |
| 控制中心要求 | 控制中心支持单机部署和集群部署两种方式，控制中心根据客户端点数的增加支持横向扩展； ★管理中心操作系统支持Windows Server 2012 R2/2016/2019/2022的64位版本（简体中文版）； 支持CentOS 7系统； |
| 控制中心支持安装在虚拟机上； |
| 控制中心支持级联管理，可支持5级级联部署，亦可单机和集群部署混合级联； |
| winpc客户端 | 操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10/windows 11 |
| winserver客户端 | 操作系统：Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019； |
| linux客户端/linux服务器 | 操作系统：CentOS 5~8/Red Hat Enterprise Linux 5~8/Ubuntu1610 |
| macos客户端 | 操作系统：macOS X 10.15、macOS 11.1、macOS 12.0.1、macOS 12.1 |
| 国产化客户端 | 中标麒麟、银河麒麟、麒麟V10、统信UOS v20 |
| 基础功能 | 终端许可管理 | 支持按照终端类型/分组统计及分配管理每个功能的终端授权使用数量。 |
| 语言要求 | 产品全功能支持简体中文/繁体中体/英语自由切换。 |
| 基础功能 | 支持根据分组、计算机名称、IP地址、MAC地址、通信IP地址、接入点、客户端类型、操作系统类型、操作系统版本等条件的组合筛选出符合条件的终端进行管理，自由对终端进行转移分组、删除终端、重启系统和终端跃迁。 |
| ★支持不同分组，客户端轻量化模式一键切换功能；【提供功能截图】 |
| 管理控制中心首页支持图形监测当前控制中心的CPU、内存、硬盘占用百分比。 |
| 支持自定义告警规则，例如系统一段时间内病毒和未知文件超过一定数量后会通过邮件发送给收件人查阅。支持邮件和阿里云平台的短信告警通知。 |
| 安全小助手 | 垃圾清理 | 支持手动扫描和清理软件安装残留文件以及系统历史记录文件。 |
| 启动项管理 | 支持检测系统启动项、服务项、计划任务，并支持启动项的优化。 |
| 防病毒防护 | 病毒防护概况 | 病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本 |
| 病毒查杀日志 | 病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间。 |
| 病毒防护报表 | 病毒报表支持病毒查杀趋势、扫描触发方式趋势、发现病毒趋势、终端感染趋势、病毒类型统计、病毒处理结果统计、病毒发现触、方式统计、趋势图表、按分组、按终端、按病毒名称。 |
| 黑白名单 | 支持手动导入、导出黑白名单，添加黑白名单。支持通过文件导入添加黑白名单。 |
| 支持通过文件数字签名添加黑白名单管理。【提供功能截图】 |
| 病毒扫描 | 支持信任区设置，病毒扫描或实时防护时不扫描目录或文件。 |
| 支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式。 |
| ★支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描。【提供功能截图】 |
| 主动防御 | 支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护。 |
| 勒索软件防护：支持勒索病毒免疫防护，同时支持诱饵文件防护、预防勒索病毒变种 |
| 网络防护 | 支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录。 |
| 支持ARP攻击防护根据策略检测和拦截局域网中的ARP欺骗攻击行为。 |
| 终端病毒处理弹窗 | 客户端弹窗支持免打扰模式和智能模式，使用免打扰模式可以对不能弹窗的终端设备中避免弹窗。使用智能模式是智能调整弹窗，对已知的病毒自动处理，对未知的病毒提示处理。【提供功能截图】 |
| 杀毒引擎 | ★支持不少于三个杀毒引擎混合使用，提高病毒检出率。【提供功能截图】 |
| 补丁管理 | 补丁类型 | 支持对Windows操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat和Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复。 |
| 支持按补丁类型和级别修复，补丁级别需包括：安全更新、重要补丁、功能补丁、可选补丁。支持仅安装指定补丁设置。 |
| 漏洞修复设置 | ★支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。【提供功能截图】 |
| 支持影响到编辑Office文档时提醒，可取消此次修复任务。 |
| 允许终端用户手动修复漏洞，如果发现“修复内容”中设置的需要修复的漏洞和功能缺陷没有修复成功则提醒终端用户修复。 |
| 漏洞挖掘 | ★为了体现产品原厂商在漏洞挖掘方面的实力，提供原厂商2023年向CNVD国家信息安全漏洞共享平台贡献漏洞不少于5万条。 |
| 补丁日志 | 支持展示终端信息、补丁号、补丁级别、补丁类型、安装日期、事件上报时间、事件类型、详细描述。 |
| 支持按终端统计补丁安装和生效情况，支持按照终端维度统计，统计每台终端的各个级别的补丁未安装数量，以及已安装、已安装未生效、已排除的总数量，并支持导出统计报表。 |
| 支持对停服系统补丁管理，支持统计即将停服的操作系统，显示操作系统、版本类型、系统位数、停服日期、终端数和升级建议，可直接下发策略进行升级。 |
| 支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、漏洞CVE编号、漏洞CNNVD编号、未安装、已安装、已安装未生效、已排除、未更新补丁库。并支持导出统计报表。 |
| 主机防火墙 | | 支持主机防火墙功能，通过添加IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标IP，支持输入IP范围。 |
| 为了避免规则过大，导致日志上报造成网络堵塞或撑满服务器，支持设置日志上报频率。 |
| 终端管控 | 外设管理 | 支持对终端各种外设（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）设置使用权限，并支持生效时间设置。 |
| 支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID和设备来源。 |
| 可禁止使用大容量USB存储设备（大容量设备自持自定义大小阈值） |
| ★支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。【提供功能截图】 |
| 外发管控 | 可对通过蓝牙、网页的外发文件进行管控，不断开网络和蓝牙本身的连接 |
| 网络防护 | 支持对网卡进行防护，支持阻止终端修改IP地址、使用动态IP地址、热点创建和IPV6地址使用等，可自定义提示内容和生效时间。 |
| 准入控制 | | ★须与内网现有准入控制系统进行兼容，实现同一客户端，无须安装其他客户端。【提供功能截图】 |
| 移动存储管理 | | 支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、取消注册、导出注册列表等 |
| 支持移动存储介质外出管理，并可以设置外出使用权限与有效时间； |
| 支持移动存储介质权限设为普通设备与加密设备，可设置是否允许网外使用 |
| 统计移动存储设备的注册信息生成报表，包括U盘插拔日志、管理员注册日志和安全U盘日志 |
| ★资质要求（提供相关复印件） | | 原厂商具备CCRC信息安全服务资质（信息系统安全运维一级）认证 |
| 原厂商要具备网络安全服务能力评定证书（网络安全应急响应服务二级） |
| 原厂商要求为“信息安全等级保护关键技术国家工程实验室”参建单位之一 |

2.2服务器安全管理系统

| 技术指标 | 指标要求 |
| --- | --- |
| 操作系统兼容性客户端 | Windows Server 2003 sp2/R2 x86/x64  Windows Server 2008 sp1及以上/R2 x86/x64  Windows Server 2012~2019 sp1及以上/R2 x86/x64  CentOs 5.0及以上 x86/x64  RHEL 5.5及以上 x86/x64  Ubuntu 14.04及以上 x86/x64  SUSE 11及以上版本 x86/x64 |
| Kylin Linux 4.18.0-147  Deepin-4.19.0-arm64-server\_1707/1813 |
| 资产管理 | 支持全量资产的关键字及语法搜索，支持检索的语法包括但不限于：服务器资产类、进程资产类、账号资产类、软件应用类、web资产类、web服务类、web框架、数据库类、端口资产类、网络连接类、启动服务类、安装包类、计划任务类、环境变量类、内核类、类库资产类、注册表类、证书资产类进行检索； |
| 支持以列表的形式，统一列出Windows/Linux服务器Web服务资产，并可查看Web服务名称、版本号、服务类型、监听端口、安装路径等信息。 |
| 支持以列表的形式，统一列出Windows/Linux服务器的计划任务，并可查看计划任务的名称、任务描述、定时启动时间、执行用户等信息。 |
| 支持以列表的形式，统一列出Windows/Linux的资产变更信息，对账号、端口、计划任务的变更进行监控，并显示变更的类型及变更内容。 |
| 可通过自动、手动的任务设置，对局域网内服务器的服务器进行扫描（支持ARP、Ping、Nmap扫描方式，并支持离线分析），并自动获取服务器相关信息，包括MAC地址、设备类型、未知主机IP、操作系统、发现方式、首次发现时间等信息。 |
| 风险发现 | 1、支持对服务器中的风险账户进行检测，发现可能存在的风险账号，并可对风险账号进行标记修复、加白等操作；  2、对服务器进行弱口令扫描，提供系统级、数据库、中间件等应用  3、支持域控弱口令扫描检测； |
| 内置等保二级、三级、CIS、系统服务核查、账户安全核查、系统配置安全检查、应用配置安全检项，并以图表的形式展示检查项的合规率、TOP5、风险服务器TOP5，并对检查出的问题给出修改意见。 |
| 可对服务器杀毒引擎进行综合的设置，支持本地查杀、控制中心查杀的设置与切换，并可对某台服务器的查杀规则进行详细设置。 |
| 1、可对服务器的软件漏洞进行综合扫描，并可对扫描方式、扫描周期进行设置，并以报告的形式展示软件漏洞扫描结果，包括：问题机器TOP5、影响最多漏洞TOP5、漏洞发现趋势等；  2、可对扫描出的软件漏洞进行标记修复、加白等操作，并支持漏洞复扫。 |
| 威胁监测 | 1、支持以图形化的形式统计展示服务器受到的告警信息/可疑威胁、拦截事件，包括：可疑威胁事件统计、可疑威胁分布、可疑威胁趋势以及具体的威胁事件列表；  2、支持在事件列表的详情中，查看事件的基础信息、检测说明、动态攻击路径信息、资产等信息，并可在详情中以前后翻页的形式连续查看事件； |
| 对暴力登录系统的账号和IP进行自动发现并上报暴力破解入侵事件，并可对攻击的IP进行封停、解封、加白等操作。 |
| 基于行为分析，检测对外服务的远程命令执行漏洞利用行为，实现实时告警和追溯。 |
| 分析中心 | 1、记录当前所有服务器产生的事件日志，并支持全量日志的关键字及语法搜索，支持检索的语法包括但不限于：服务器相关参数、访问主体相关参数、网络相关参数、操作相关参数、客体相关参数、登陆日志相关参数等进行检索，并支持返回上次筛选的关键词（至少可返回不少于5个）；  2、支持以柱状图的形式展示某段时间内的日志数量，并在柱状图下方展示具体的日志事件，并在日志上方以标签形式展示服务器名称、IP地址、日志类型、日志等级、拦截状态等信息；  3、可查看某条日志的具体攻击全路径。 |
| 安全运维 | 显示当前所有服务器的环境现状，包括内存使用率、硬盘空间、操作系统、agent利用率等等信息，并提供报警和导出功能。 |
| 下载中心 | 支持各类日志、安全报表、资产报表、事件报表、功能状态报表的综合下载导出，并可根据实际情况对报表内容进行自定义导出。 |
| 提供Linux客户端、Windows客户端、Arm客户端的下载与安装，并支持以安装包形式和生成安装命令形式进行安装。 |
| 子账户管理 | 提供子账号的管理，支持账号名称、账号角色、上级账户关联、归属人、手机号、邮箱、备注设置，并支持服务器的绑定； |
| ★资质 | 原厂商具备国测信息安全服务资质-云计算安全类 |