**1、硬件服务器安全加固系统**

| **参数类型** | **参数要求** |
| --- | --- |
| **操作系统兼容性** | 支持windows/linux主流操作系统，包括但不限于以下的操作系统：Windows Server 2003 SP2（x86/x64）、Windows Server 2008（x86/x64）、Windows Server 2012、Windows Server 2016、Windows Server 2019；RedHat 4.3~RedHat 5.11（x86/x64）、RedHat 6.0~RedHat 6.7（x86/x64）、RedHat 7.0~RedHat 7.2 RedHat8.0 ；CentOS 4.3~CentOS 5.11（x86/x64）、CentOS 6.0~CentOS 6.10（x86/x64）、CentOS 7.0~CentOS 7.6、Centos8.0；Ubuntu10.0以上；Suse 10~Suse 10 sp3、Suse 11~Suse 11 sp3、Suse12；中标麒麟、红旗Redflag3~4； |
| **产品安全机制** | 客户端具有反逆向、反调试功能、自保护功能，客户端和管理中心通信采用安全的加密机制 |
| 支持自我防护技术，即使客户端被意外关闭，防护依然有效 |
| **主机资产清点** | 支持展示当前服务器、进程、账户、软件应用、Web资产、Web服务、Web框架、数据库、端口、网络连接、启动服务、安装包、计划任务、环境变量、内核模块等分类资产数量统计，可对分类资产全局进行快速搜索，保留历史搜索记录并保存搜索条件以进行快捷搜索，同时提供服务器名、IP地址、操作系统、资产类型的筛选搜索；针对搜索结果，支持按资产类型导出 |
| 支持展示服务器名称、状态、操作系统、IP地址等基本服务器资产信息，CPU、内存、磁盘、分区等硬件配置信息，负责人、资产级别、联系电话、邮件等运维信息，并提供搜索及导出功能 |
| **主机资产发现** | 支持对局域网内服务器的服务器进行扫描，并自动获取服务器相关信息，包括服务器名、在线状态、别名、主机IP、AgentID、分组标签、操作系统、IPv4、IPv6、负责人、所属部门等信息，可通过自动、手动的进行资产发现的任务设置。 |
| **微隔离** | ★支持自动学习并梳理出对互联网暴露的服务器端口信息，并提供端口处置**（提供产品截图证明并加盖厂商公章）** |
| ★支持自动学习并梳理出内网端口访问情况，并提供端口处置**（提供产品截图证明并加盖厂商公章）** |
| **外连白名单** | ★支持从服务器、进程维度监控分析进程外连情况，外连IP地址及域名，并提供告警**（提供产品截图证明并加盖厂商公章）** |
| **风险发现** | 支持服务器系统级、数据库、中间件、应用级的弱口令、口令复用扫描，并可对扫描的结果进行修复验证，还可对口令风险的扫描任务进行设置，包括任务名称、目标服务器、扫描类型、扫描所用字典、执行周期等方式。 |
| **软件漏洞检测** | 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 |
| **基线检查** | 可支持等级保护2.0的二级、三级检查、测评、整改的业务检查，系统内置官方等保2.0的二级、三级基线模板，满足等保二级及等保三级要求，同时支持用户自定义基线检查任务。并支持基线检查结果的图形化统计，包括：合规率、问题项TOP5、风险服务器TOP5等维度的统计，并可导出基线检查报告。 |
| **病毒查杀** | 采用主动的方式进行自动化病毒查杀，可支持Bitdefender、ClamAV、Qowl等多引擎技术识别并查杀最新病毒；可支持病毒文件自动隔离、自动删除、不处理三种方式。并可将病毒查杀的结果导出报告 |
| **异常登陆监测** | 以违规登录、可疑登录的视角，对异常登录行为进行监控及告警，包括：登录账号、来源IP、登录区域、服务器IP、操作系统等，并可进行登陆规则的设置，以及告警设置 |
| **Webshell检测** | 自动识别web服务目录，并实时进行webshell后门的扫描，包括：危险级别、文件路径、文件代销、文件MD5、文件修改时间、webshell发现时间、感染服务器等信息。 |
| **攻击溯源分析** | ★支持记录当前所有服务器产生的事件日志，并提供筛选的功能和自定义时间段筛选查询，用户可通过安全日志快速锁定问题服务器，并进行相应处理。同时支持对安全事件进行溯源分析，对安全事件的等级、攻击类型、ATT&CK ID、ATT攻击阶段进行匹配。**（提供产品截图证明并加盖厂商公章）** |
| **应用防护** | ★支持RASP（Runtime Application Self Protection）运行时应用自我保护技术，可对ASP、.Net、PHP、Java四种语言进行RASP防护，通过对应用系统流量、上下文、行为进行持续监控，有效抵御一句话木马、变形/未活动/加密Webshell、SQL注入、命令执行、文件上传、任意文件读写、反序列化、Struts2漏洞等高级Web应用攻击**（提供产品截图证明并加盖厂商公章）** |
| **系统防护加固** | 支持系统内核加固技术，对非法创建文件、非法更改系统设置、非法创建可执行文件、非法提权等恶意行为进行监控和防护。 |
| **文件防篡改** | 支持驱动级防篡改，可以保护整个目录、网页或文件不被恶意修改或者变更，支持监控和控制文件读取、写入、删除、链接、创建、执行、重命名等操作，支持对目录、进程进行例外设置。 |
| **防端口扫描** | ★支持检测和防止恶意的端口扫描，并屏蔽扫描器恶意扫描**（提供产品截图证明并加盖厂商公章）** |
| **报表生成下载** | 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 |
| **账号管理** | 支持创建子账号，创建账号时支持配置其角色、上级账户、绑定服务器，支持添加归属人、手机号、邮箱、备注等附属信息 |
| **资质要求** | 产品拥有自主知识产权，非OEM、代理销售产品，具有国家版权局颁发的“计算机软件著作权登记证书” |
| 产品拥有公安部颁发的“主机文件监测（基本级）”安全专用销售许可证 |

**2、虚拟化服务器安全防护系统**

|  |  |  |
| --- | --- | --- |
| **指标项** | **指标子项** | **指标要求** |
| **系统**  **要求** | **架构要求** | 系统需要支持B/S架构，管理员可只通过浏览器登录控制中心，即可对系统进行管理。 |
| **部署要求** | ★系统需支持无代理部署模式及有代理部署模式，以便结合管理需求选择相应部署模式； |
| 需支持一套管控中心统一管理，包括有代理、无代理部署模式统一管理；物理服务器、虚拟服务器统一管理；Windows、Linux、信创操作系统统一管理；私有云、公有云、容器环境统一管理； |
| **数据库要求** | 系统需支持自带高性能数据库，不需要额外单独采购数据库。 |
| **操作系统**  **支持** | 支持windows/linux主流操作系统（不限于下）：  1、Windows Server 2003、2008、2012、2016、2019；  2、Windows 7、Windows 8、Windows 10、Windows Vista；  3、RedHat Enterprise Linux 6.0-7.7、CentOS6.0-8.4、Ubuntu 10.04-20.04、SUSE 11、12、15 、中兴新支点NewStart、BC-linux、Oracle Serve、Deepin、RE-DCOS、NeoKylin Linux等操作系统。 |
| **信创适配** | ★支持信创ARM平台的中标麒麟、银河麒麟、麒麟V10、统信UOS。**（投标文件需要提供能够体现上述证明文件加盖原厂公章。）** |
| **云平台适配** | VMware、Citrix XenServer、华为FusionSphere、华为FusionCompute (kvm)、H3C、OpenStack、CloudManager云管理平台、浪潮 InCloud Sphere、QingCloud青云、曙光云、斯坦德云、机敏云等云平台。 |
| **功能**  **要求** | **资产管理** | 提供主机管理及终端管理功能，包括支持对主流虚拟化平台导入功能，非虚拟化平台支持可支持单台计算机或网段IP导入。支持对终端提供分组管理、安全策略配置、安全功能防护、特征库更新、客户端程序更新等功能。 |
| ★提供十五类资产的清点能力，包括服务器资产、账号资产、端口资产、网络连接、进程资产、软件应用、web服务、web站点、数据库、Jar包、系统安装包、启动服务、计划任务、环境变量、内核模块。**（投标文件需要提供能够体现上述功能及配置选项的截图加盖原厂公章。）** |
| **病毒查杀** | 采用主动的方式进行自动化病毒查杀，支持多引擎联动防护Bitdefender、QOWL、云查杀、支持灵活开启或停用引擎；支持病毒文件自动隔离、自动删除、修复、监控多种处理方式。支持病毒查杀的结果生成报告。提供防护策略控制可避免启动风暴和查杀风暴。 |
| ★支持人工智能引擎**（投标文件需要提供能够体现上述功能及配置选项的截图加盖原厂公章。）** |
| 支持提供病毒防护等级设置、支持对操作系统资源占用进行配置； |
| ★提供基于“诱饵”行为监测的勒索病毒防御，Windows平台支持针对已知勒索病毒家族及其变种，通过内存抢占模式，实现该类病毒免疫，同时保护Windows系统还原点，禁止还原点被恶意删除，保障系统业务恢复。**（投标文件需要提供能够体现上述功能及配置选项的截图加盖原厂公章。）** |
| **风险发现** | 提供风险发现功能，通过风险扫描功能对服务器的弱口令风险、webshell、安全补丁、漏洞风险，系统配置风险进行检测，发现服务器上的风险异常。支持安全风险评级，可直观展现评级与分数，支持按风险等级、TOP5风险、易受攻击TPO5等维度提供可视化呈现。 |
| **系统加固** | 产品支持 SSH、RDP、telnet等服务的暴力破解检测，可对来自网络的暴力破解行为进行拦截，支持配置时间、破解次数、拦截时长，并提供暴力破解IP或IP段的黑白名单设置 |
| **微隔离** | 提供防火墙功能，支持虚拟机/终端系统的双向控制。可提供对威胁情报实时分析网络流量功能，检测出失陷主机并提供监控及阻止失陷主机与恶意域名的连接功能。系统需支持对DDoS等异常流量进行拦截和清洗能力。 |
| **入侵防御** | 系统应支持入侵防御功能，可针对出入虚拟机的流量进行检测识别，防御网络攻击及入侵行为，通过真实漏洞利用流量的特征来检测或阻止漏洞利用(虚拟补丁防护能力)  产品预置入侵防御规则应不少于8000条次（不包含自定义规则），需覆盖系统、数据库、应用漏洞、防勒索、防挖矿等多种类型防御规则，防御规则支持严格、高、中三种预定义级别，针入侵威胁，提供检测和阻止模式，可以自动捕获违反规则的网络包，供验证和分析使用。 |
| 支持为IPV6的主机提供入侵防御功能。 |
| **分析呈现** | 1、提供数据中心威胁态势感知，大屏动态展示安全运维状况，结合地理位置信息全面呈现威胁攻击详情；  2、支持按总流量（下图中显示为“流量统计”）、恶意流量、新建连接对流量进行统计和展示；  3、支持按照不同分组、虚拟机/终端、网络协议、网络协议组、国家/地区、城市，分不同威胁类别以柱状图、折线图（曲线图）、饼图、原始日志等形式进行展示，支持手动或者定时定期生成报表；  4、支持日志查询与操作员日志审计功能；  5、网络流量日志，支持端口识别与显示，支持关联进程 |
| **产品资质** | **产品资质** | ★所投产品提供公安部销售许可证 虚拟化安全防护产品(增强级) |