**一、项目名称**

2024年度服务器、移动端和工作站防病毒安全运维项目

**二、项目参数:**

**（一）项目内容及要求**

**一、项目背景**

为切实落实工作计划中提到的上述工作要求，结合新华医院信息中心日常工作中面临的终端设备、服务器及移动查房设备“数量大、范围广、管控细、人手少”的现实问题。本次采购考虑在采购服务器及终端杀毒的同时，并配备“杀毒+终端安全统一管理”结合的推行方式。

项目建设目标：本次运维主要包括服务器端防病毒系统、移动终端设备防病毒系统、终端防病毒系统、终端安全管理系统和TDA威胁发现系统五个部分。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 内容 | 运维许可数量 | 服务和授权  许可时间 |
| 1 | 服务器端防病毒系统运维 | 1000个 | 2024年7月1日-2025年6月30日 |
| 2 | 移动终端设备防病毒系统运维 | 1000个 |
| 3 | 终端防病毒系统运维 | 3800个 |
| 4 | 终端安全管理系统运维 | 3800个 |
| 5 | TDA威胁发现系统运维 | 1套 |
| 6 | 常规运维原厂授权  认证工程师服务 | / |
| 7 | 应急响应原厂  资深认证工程师服务 | / |
| 8 | 厂家售后服务电话支持服务 | / |
| 9 | 远程服务支持 | / |

**二、服务器防病毒运维需求**

授权数：服务器端防病毒系统，1000点

部署位置：用户服务器端

授权许可时间：一年软件授权许可（2024年7月1日-2025年6月30日）

质保时间：一年软件升级及服务（2024年7月1日-2025年6月30日）

病毒防护分为三个方面：扫描，实时防护，主动防御。

扫描：通过用户端程序进行文件扫描，根据用户环境使用公有云引擎、私有云或鉴定中心，进行威胁文件的识别。在扫描过程中除了上述云引擎，同时启用云查引擎、启发引擎、脚本引擎、AI引擎、主防引擎(本地库)五大引擎，全方位扫描文件，不放过一个死角。

实时防护：在文件被访问时对文件进行扫描，及时拦截活动的病毒，对病毒进行免疫，防止系统敏感区域被病毒利用。在发现病毒时能及时通过提示窗口警告用户，迅速处理。

主动防御：全方位立体化阻止病毒、木马和可疑程序入侵。跟踪分析病毒入侵系统的链路，锁定病毒最常利用的目录、文件、注册表位置，阻止病毒利用，免疫流行病毒。实现对动态链接库劫持的免疫，以及对流行木马的免疫，免疫点应根据流行病毒的发展变化而及时增加。

1. 应用管理
2. 应用程序管理

（1）进程库：进程在终端运行后会自动上报至服务器，形成进程库，支持进程分组管理。

（2）黑名单：禁止允许的程序（系统进程默认例外）

（3）白名单：只允许运行白名单中的程序（系统进程默认例外）

（4）红名单：必须运行的程序（需要指定进程启动路径），红名单启动失败会产生告警日志。

（5）支持在线、离线策略。

1. 网络防护

（1）黑名单：禁止终端访问黑名单中的地址/端口，终端尝试访问黑名单中的进程会被阻止，同时产生告警信息。

（2）白名单：只允许访问黑名单中的地址/端口，终端尝试访问白名单以外的地址会被阻止，同时产生告警信息。

（3）持在线、离线策略。

1. 主要性能指标

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 服务器用户端安装环境要求 | 操作系统:Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012/ Windows Server 2016/Deepin/SUSE Linux/Red Hat Linux等 |
| 系统管理 | 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、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能。 |
| 产品支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行。 |
| 支持网页访问部署、离线安装包部署、域推送等部署方式，可自定义部署通知邮件及部署通知公告 |
| 病毒查杀 | 要求产品具备本地多引擎查杀能力，且引擎可配置。 |
| 支持linux、国产操作系统杀毒、云桌面产品 |
| 要求产品具备应用级沙箱技术。 |
| 要求支持以自定义黑白名单的方式来管理全网终端的文件。管理员可以将文件加入白名单或者黑名单。如果文件被加入白名单，用户端就不会再查杀此文件，加入黑名单，用户端就不可以执行此文件。 |
| 要求支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力。 |
| 对敲诈者病毒提供防护机制，同时提供解密工具，解密工具应为自主研发。 |
| 病毒库升级管理 | 要求支持服务器端病毒库的定时更新和手动更新两种升级模式。 |
| 要求支持用户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽。 |
| 日志报表 | 展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表； |
| 展示全网终端木马库日期比例，可方便的查看全网终端木马库的情况； |
| 展示全网终端病毒库日期比例，可方便的查看全网终端病毒库的情况 |
| 支持大数据引擎系统，可将全网终端日常运维数据汇聚存储分析，并根据客户运维管理所需的要求定制报表 |
| 要求支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件到相关人。邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等 |

**三、移动终端设备防病毒系统运维需求**

授权数：移动终端设备防病毒系统，1000点

部署位置：移动端设备，如护士移动PDA、移动查房车等设备

授权许可时间：一年软件授权许可（2024年7月1日-2025年6月30日）

质保时间：一年软件升级及服务（2024年7月1日-2025年6月30日）

1.移动端防病毒

* + 1. 应用安全检测

包含风险应用检测、木马应用检测、广告应用检测；移动端病毒查杀；

* + 1. 网络安全检测

包含网络状态检测、DNS劫持风险检测、ARP攻击检测、加密异常检测、钓鱼或伪装WiFi检测；

* + 1. 系统安全检测

包含设备Root/越狱状态检测、USB调试模式开启检测、锁屏密码是否开启检测 、设备管理器激活检测；

* + 1. 系统漏洞检测

移动终端设备系统漏洞检测、引用漏洞检测；

* + 1. 安全分析

通过对用户端上报的应用风险、网络风险、系统风险、配置风险各项威胁数据，形成数据图表，对移动终端数据直观了解，包含：风险应用统计、不安全终端数、终端风险事件等；

* + 1. 运营分析

控制台对移动终端的使用数据进行收集，并对其进行相应展示，使系统管理人员可直观的对移动终端的状态进行分析，包含：终端设备详情、终端活跃度、离线设备状态、终端应用详情、业务应用使用情况等；

2.主要性能指标

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 1. 授权数 | 1000个 |
| 1. 性能要求 | 支持最大终端授权数实配不低于4000 |
| 1. 安全要求 | 杀毒引擎支持病毒库更新 |
| 1. 用户端 | 支持APP或SDK方式 |
| 1. 服务端 | 支持MySQL数据库 |
| 1. 终端统计 | 支持统计不同平台终端数、活跃终端数、终端风险累计扫描次数、累计扫描终端、发现风险、处理风险、遗留风险数的统计 |
| 1. 终端安全统计 | 支持对有风险终端和无风险终端数统计 |
| 1. 安全状态统计 | 支持对应用风险、网络风险、系统风险的终端安全状态数量统计 |
| 1. 活跃统计 | 支持统计近一段时间终端活跃统计 |
| 1. 风险排行 | 支持对不同风险终端数进行排行 |
| 1. 离线统计 | 支持对离线终端的时长统计 |
| 1. 风险遗留统计 | 支持对未处理风险的终端进行统计 |
| 1. 应用风险检测 | 支持对移动终端木马应用、广告应用、风险应用进行检测 |
| 1. 云查杀 | 支持本地查杀和云查杀能力，云查杀可使用云端恶意样本库； |
| 1. 应用动态监控 | 支持实时动态感知，安装新应用自动进行风险检测 |
| 1. 网络风险检测 | 支持对网络风险状态检测、DNS劫持风险、ARP攻击检测、加密异常检测、钓鱼、伪装WiFi检测 |
| 1. 网络动态监控 | 支持网络动态感知，可根据网络切换、网络开启进行动态检测更新 |
| 1. 系统风险检测 | 支持对系统的ROOT状态、USB调试模式开启、锁屏密码是否开启、设备管理器激活等风险项进行检测 |
| 1. 系统漏洞检测 | 支持对Android系统漏洞的检测 |
| 1. 风险评级 | 支持对终端环境安全的评级，通过终端上报各项风险系数，对终端安全状态有安全、潜在风险、一般风险、严重风险不同评级; |
| 1. 评级自定义 | 支持用户自定义每个风险项安全等级，安全分数，实现对每个终端的安全评级； |
| 1. 检测记录 | 支持对每个终端安全检测记录跟踪，对每个终端的绑定账号、终端型号、IMEI号、具体风险、检测记录进行详细跟踪； |
| 1. 风险详情 | 支持对每个终端应用风险详情展示：应用包名、病毒文件路径、病毒风险详情等 |
| 1. 威胁数据 | 支持对应用风险、网络风险、系统风险的终端、风险最早发现时间、风险类型、感染终端、具体哪些终端感染进行数据统计和展示。 |
| 1. 服务端集成服务 | 通过对移动终端的环境、系统运行状态及安全事件的可预知风险持续监控，并且对每个终端进行安全评级，提供第三方可查询终端安全评级的标准接口 |
| 1. 用户端集成服务 | 提供第三方应用可集成的标准SDK和对接文档、demo应用，让第三方应用具备风险感知能力 |
| 1. 提供接口 | 提供应用风险、网络风险检测、系统风险检测接口，提供对制定路径的文件扫描接口 |

**四、终端防病毒系统运维需求**

授权数：终端防病毒系统，3800点

部署位置：医院PC终端

授权许可时间：一年软件授权许可（2024年7月1日-2025年6月30日）

质保时间：一年软件升级及服务（2024年7月1日-2025年6月30日）

|  |  |  |
| --- | --- | --- |
| **技术指标** | | **指标要求** |
| 多语言 | | 全功能支持简体中文、繁体中文、英文。 |
| 终端运维 | 终端概览 | 查看终端的整体的安全状态和关键安全信息。支持自定义列和导出。 查看终端的硬件信息，包括电脑品牌、设备出厂日期、硬盘文档、硬盘序列号、以及终端硬件（硬盘、内存）变化信息等。 支持收集终端IP地址和NAT转换IP地址(客户端到服务器如果有地址转换，地址转换后的地址)。 |
| 客户端密码保护 | 通过验证动态验证码或者固定密码防止终端被卸载、退出，当终端用户卸载或者退出客户端时需要输入正确的验证码或者密码才可以卸载、退出。 |
| 客户端防安装 | 防安装密码为了限制外来终端安装后占用企业授权数量问题，企业内部人员通过安装密码才可以安装成功。 |
| 时间同步 | 支持通过NTP时间服务器同步时间，让终端时间保持与时间服务器相同。 |
| 资产登记 | 对资产信息（如资产分类、资产用途等）进行登记。 将资产责任人与资产进行绑定，确认资产的责任关系。同时支持根据资产责任人自动划分终端分组。 Windows PC/Server支持自动绑定域账户为资产责任人、首次绑定修改密码。 国产通用终端/服务器支持首次绑定资产责任人修改密码。 |
| 收集排障日志 | 主动收集客户端运行时产生的日志以及终端当前的网络等相关信息。用于反馈问题时提供服务人员排障。 |
| 系统崩溃日志收集 | 在终端出现系统卡顿时通过按键可触发系统蓝屏以记录系统卡顿日志。反馈服务人员分析卡顿原因并解决。 |
| 客户端定制 | 可自定义定制终端标题、皮肤、语言、产品LOGO、企业LOGO。 支持关闭在客户端显示策略、任务列表、已安装模块。 支持模块化安装功能模块。 |
| 定时公告 | 支持配置一次性、开机时展示、周期公告。 |
| 单点维护 | 终端视角查看终端信息、策略、进程信息、网络配置等信息。 |
| 级联部署搜索终端 | 支持在管理系统级联部署下快速定位查找下级的终端。 |
| 全面支持基于用户的终端安全管理 | 用户登录 | 通过用户登录功能确定终端的使用人，以实现按照使用人管理。 支持强制登录、域环境自动登录，以及逃生通道。 支持本地账户、第三方认证源认证。 支持用户退出，退出后使用人与终端解除关系。 |
| 用户策略 | 用户策略是实现基于管理重要手段，策略跟人走，登录时使用用户策略，退出时使用终端策略。避免终端临时更换其他人使用，不能正确审计使用人。 |
| 用户报表 | 支持按照使用人信息管理终端，实现基于人的终端安全管理闭环。 |
| 终端分组 | 多维度的分组 | 支持同时按照多种维度划分终端分组（自定义组），比如主要按照组织架构分组，同时管理例外终端，不影响组织架构分组。 支持资产责任人的组织架构、IP地址、内存容量、CPU数量、操作系统版本、接入点、安装包名称划分分组。 |
| 自动分组 | 通过给分组设置规则，当终端的属性满足分组规则则被自动进入到对应的分组中。同时支持一次性划分分组，也支持动态根据终端属性变化自动重新划分分组。 |
| 手动分组 | 支持管理员手动划分终端分组。 |
| 调整分组顺序 | 通过手动调整分组的排列顺序可以对分组树进行自定义排序。 |
| 用户分组 | 多维度的分组 | 支持同时按照多种维度划分用户分组，比如主要按照组织架构分组，同时可以自建用户分组，不影响组织架构分组。 支持用户名、岗位等用户属性划分分组。 |
| 自动分组 | 通过给分组设置规则，当用户首次连接到系统后，会自动进入到符合规则的分组中。 |
| 手动分组 | 支持管理员手动划分终端分组。 |
| 调整分组顺序 | 通过手动调整分组的排列顺序可以对分组树进行自定义排序。 |
| 策略管理 | 终端策略 | 终端策略即策略针对固定终端进行生效，而不针对用户变化而改变。 支持精细的策略项配置，每一项策略配置项均支持关闭、是否强制执行（强制下级组的终端执行）、是否允许终端修改。 |
| 用户策略 | 用户策略即策略针对用户生效，用户登录的终端优先执行用户策略，用户策略优先级高于终端策略。用户退出后，停止执行用户策略。 |
| 策略生效条件 | 定义策略生效的时间规则、场景条件，用于管控策略。 |
| 策略抵达 | 支持统计每条策略抵达终端的情况。 |
| 级联策略 | 1. 级联策略支持分发终端策略和用户策略。 2. 级联策略支持停止/开启。 3. 级联策略仅作用于下级系统，不影响本级的终端/用户。当级联关系解除后，下级系统接收到的级联策略自动失效，并且自动删除策略。 4. 级联策略支持强制策略和普通策略。 i. 级联强制策略的优先级高于下级系统的所有策略。 ii. 级联普通策略的优先级低于下级系统的所有策略。 5. 级联策略支持分发给指定的下级系统并且包含子孙系统、指定的下级系统但不包含子孙系统。 6. 级联策略支持分发给下级系统的部分终端/用户，可通过“表达式”或者分组描述部分终端/用户。 7. 级联策略支持按照“安全业务类型、客户端类型”颗粒度分发和管理权限。 |
| 策略锁定 | 支持灵活锁定策略配置项，某项策略被管理员锁定，终端用户则不能再修改。同时支持允许终端用户自定义策略设置。 |
| 策略合并 | 支持策略合并，智能合并来此多处的策略，方便管理员管理。 |
| 任务管理 | 任务下发 | 可针对单终端，分组，自定义数量终端下发任务，如全盘查杀病毒，扫描漏洞，安装软件等。 |
| 再次执行 | 支持对执行失败的终端再次执行。 |
| 查看任务进度 | 可以查看每个任务的下发执行进度，支持“未接收、已接收待执行、执行中、管理员取消、用户取消、执行成功、执行失败、终端不支持、已过期”9种执行状态，以及查看执行失败的原因。 支持通过执行状态、失败原因、IP地址等条件进行筛选。 |
| 查看历史任务 | 可以查看历史上发布的任务详情，并支持通过执行状态、失败原因、IP地址等条件进行筛选。 |
| 删除历史任务 | 可以手动删除历史上已结束的任务。 |
| 终端部署 | 在线部署 | 设置客户端部署URL，安装时策略，管理员可以复制该链接通过公司的邮件、OA等通讯方式通知给终端用户，完成部署，部署通知通过富文本的方式通知公司员工部署客户端。 |
| 一体化安装包 | 可以配置接入点、客户端类型、策略、安装模块、安装保护等提供灵活的离线安装包。 |
| 更新包 | 通过更新包可以对无法连接管理中心的终端进行终端程序文件以及库文件的更新。选择最新版本，则将管理中心上程序以及库的最新版本数据制作到离线更新包中，选择全网可更新版本，则将管理中心上全网计算机均可升级的程序以及库文件数据制作到离线更新包中。 |
| 域推送包 | 在有AD域的场景下，可以利用域推送的方式快速的进行安装推广。 |
| 安装界面定制 | 为部署和安装包制作提供安装界面定制，通过上传自有的图片来定制终端安装的界面。 |
| 自动切换接入点 | 客户端根据终端网络情况自动切换连接合适的接入点，用于用户出差、接入点灾备等场景。支持按照优先级顺序切换和随机切换。 |
| 自动切换服务器 | 终端在多套管理系统之间自动迁移的功能。用于按照安全域管理的场景，终端根据接入的安全域自动切换到对应的管理系统中。 |
| 文件分发 | 文件分发 | 支持分发文档、可执行文件、脚本，辅助管理员做终端运维。 |
| 支持在有已有重名文件时重命名新分发文件，避免覆盖已有文件。 |
| 支持指定分发时机：操作系统账号是否登录，终端CPU使用率。 |
| 支持强制指定分发的文件在终端上的保存路径。 |
| 支持自动清理客户端上已分发的文件功能，清理超出保存时间的文件，释放终端磁盘空间。 |
| 支持限制分发的文件类型。 |
| 支持分发500MB的文件，并且可自定义限制分发的文件大小。 |
| 知识库 | 进程知识库 | 汇总展示内网终端上报的进程信息，支持设置进程匹配规则，其他业务可直接调用创建好的进程规则或者进程分组 |
| 外设库 | 统计终端外接的各种设备-（厂商、设备型号识别） |
| 出口白名单 | 统计终端的出口地址 |
| WIFI库 | 搜集终端连接的无线信号信息统一展示，标识出ssid可连通互联网，可连通服务器的情况 |
| 终端日志 | 终端更新日志 | 记录终端客户端更新的日志包括，更新时间，计算机名，终端分组，IP地址，MAC地址，操作系统版本等。 |
| 自我保护日志 | 记录终端客户端更新的日志包括，更新时间，计算机名，终端分组，IP地址，MAC地址，操作系统版本等。 |
| 终端跃迁日志 | 记录终端客户端自我保护的日志包括，触发时间，事件，行为动作等。 |
| 终端排障日志 | 记录终端客户端运行时的相关日志包括，安装/更新/运行/网络环境等信息用于远程排障。 |
| 终端硬件变化日志 | 记录终端的硬盘、内存发生变化时的相关日志，包括终端详情、硬件名称等。 |
| 系统设置 | 系统设置 | 设置服务器联网状态及终端部署页面配置，下载页面支持HTTPS和HTTP两种方式，在通知外发服务中可对接的SMTP服务器和短信网关服务器及syslog服务器方便及时收到告警信息。 |
| 安全设置 | 设置系统加密算法，加密算法支持国密和哈希两种。 |
| 数据外发 | 开启syslog数据外发配置需要发送的内容。 |
| 业务设置 | 对文件分发，补丁管理，数据防泄漏，基线核查，移动存储，病毒防护的业务配置，包含对报表和日志进行设置，配置高发内容规则，等级包括高命中和极高命中。风险终端定义包括，低危，中危，高危等。 |
| 更新管理 | 在线更新 | 服务器在互联网环境下，支持在线更新病毒库、补丁库、威胁情报等数据，并且支持“按月、按周、按天、按小时”灵活设置更新时间。 客户端支持在离线情况下从互联网检查更新病毒库，并支持设置下载源。 支持指定客户端的更新时间。 |
| 离线更新 | 提供离线更新工具，支持在隔离网环境下更新服务器的病毒库、补丁库等数据，支持命令行后台静默运行。 |
| 灰度更新 | 终端更新主程序、病毒库、补丁库等支持灰度多批次的灰度更新，保持在低风险中完成终端数据更新。 支持按照终端类型设置灰度批次。 支持仅允许灰度范围内的终端更新数据。 支持在灰度期更新新数据后，自动重头开始进行灰度，也支持进行中的灰度完成后，开展新的灰度测试。 支持通过分发更新任务触发客户端立即更新，用于灰度前期主动触发客户端更新以观察更新效果。 支持管理系统级联部署下的更新管理，支持全网所有管理系统统一灰度更新，也支持下级管理系统各自从互联网更新。 |
| 系统日志 | 管理员操作日志 | 审计管理员的所有管理操作行为，用于时候审计和追踪溯源。 |
| 服务器运行日志 | 记录服务端后台重要任务的执行结果 |
| 账号管理 | 组织架构 | 支持本地新建，也可以支持从第三方同步组织架构 |
| 本地帐号 | 本地账号用于在没有身份认证系统情况下自建账号管理体系。能够添加、删除、重置账号、停用账号。 |
| 通用账号 | 终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心。 |
| 权限 | 通过角色，能够对有相同权限需求的用户进行授权，达到复用的能力；而对于没有复用的权限，可通过基于规则方式进行授权，简化管理员对角色的管理成本，提高效率。 |
| 账号密码有效期 | 设置账号密码有效期，超过有效期后账号不能登录，管理员重置有效期后，可再次正常使用。 |
| 账号密码策略 | 设置密码强度，配置组合数量及长度。密码组合和长度不符合时无法成功创建账号或修改密码。 |
| 账户锁定策略 | 当账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。 |
| 安全认证 | 登录支持单因子登录，也支持双因子，在密码认证的基础上可以再加上动态口令等其它认证，提高安全性。 |
| 个人中心 | 个人基础信息和安全相关项，如修改密码，重置动态口令等。 |
| 许可证管理 | 许可证概况 | 展示企业整体授权状态，各平台总数量及已使用数量。可以更新授权，自行更换授权Logo。 |
| 许可证使用情况 | 支持按照终端类型/分组统计及管理每个模块的终端授权使用数量。 |
| 在线激活 | 在服务器联网模式下，支持通过许可证ID在线绑定激活。 |
| 审批工作流 | 多节点审批 | 支持自定义多个串行和平行审批节点，平行节点可设置部分通过即整个节点审批通过 |
| 控制台审批+终端审批 | 支持登录控制台进行审批操作，也支持通过终端网络端口在客户端页面进行审批 |
| 自动审批 | 用户可设置系统托管进行自动通过或自动拒绝审批 |
| 告警中心 | 告警处置规则 | 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。 |
| 告警方式 | 支持邮件、阿里云平台的短信告警。 |
| 服务器运维 | 日志清理 | 按天数配置自动清理数据库的数据。 |
| 网络限速 | 网络限速 | 1.支持对终端下载文件和上传文件限速。 2.支持按照时间段限速下载和上传文件。 3.支持按照终端的IP地址段限速下载和上传文件。 4.支持对终端上传日志限速。 |
| 服务器部署 | Windows单服务器部署 | 适用于中小客户群体。 支持IPv6（双栈）。 管理系统支持达梦数据库DM8版本（仅用于管理系统Linux单机部署）。 支持部署X86和ARM处理的服务器。 |
| 集群部署 | 适用于大中型客户群体。 |
| 级联部署 | 适用于拥有需要独立安全运营的分支机构的政企单位。级联部署即将多个独立的终端安全管理系统按照上下级关系连接起来，以实现独立运维和统一安全管理。 支持 5 级级联部署，亦可单机和集群部署混合级联。 支持免密登录下级管理中心管理终端、策略、任务等操作，但不支持查询下级系统的日志。 |
| 网络代理 | 支持通过网络代理更新主程序、下载病毒库等互联网资源。 |
| 多个管理终端的通信地址 | 管理中心支持配置多个终端通信地址，适用于服务器双网卡、同时管理内外网终端等场景。 |
| 接入点 | 配置管理 | 配套管理中心提高带宽利用率。管理系统集群部署和单机部署都可以。 |
| 下载文件缓存 | 支持文件下载分级缓存，降低带宽使用。 |
| 预缓存文件 | 支持闲时预缓存软件安装包文件，提高闲时带宽利用率。 |
| 下载文件限速 | 1.支持本接入点到上级下载文件的限速。 2.支持闲时预缓存软件安装包文件。 3.支持按照终端的IP地址段限速。 |
| 日志上传限速 | 支持终端上传文件限速和接入点（分支机构）到总部的上传日志限速。 |
| 就近到互联网下载文件 | 支持从接入点到互联网下载主程序、下载病毒库等互联网资源。 |
| 多级接入点 | 支持最多部署5级接入点，用于大型政企单位。 |
| 数据联动 | 数据查询 | 通过webservice服务为第三方系统提供数据获取能力（ODP）。 |
| 数据外发 | 通过SYSLOG协议终端发送的安全日志数据到第三方系统。 |
| 数据外发 | 支持通过SYSLOG协议发送终端概况信息、系统日志到第三方系统。 |
| 数据外发 | 支持通过Kafka协议发送将终端行为数据（EDR）给第三方系统。 |
| 数据推送 | 通过工具将当前系统部分数据发送到防火墙服务器（依赖基线核查许可）。 |
| 联动响应 | 联动处置 | 通过OpenC2协议与第三方系统联动。可实现从第三方分析平台对天擎终端下发病毒扫描（依赖防病毒、威胁处置许可）；进程文件终止\隔离（依赖威胁处置许可），以及对终端下发终端网络隔离（威胁处置许可）的操作任务；支持由第三方系统修改终端的分组。 |
| 策略分发联动 | 客户端接收和执行第三方系统分发的策略。当前支持病毒防护、终端管控、移动存储、主机防火墙策略。 |
| 切换客户端连接的接入点 | 支持由第三方系统指定和切换客户端连接的接入点。 |
| 报表中心 | 视图 | 通过业务数据集自定义图表进行数据统计。终端概况、终端软件概况、终端硬件资产的业务数据自定义图表类型进行统计。 |
| 仪表板 | 在仪表板添加多个标签，在标签页下添加多个视图，自定义视图大小、位置，仪表板支持导出。 |
| 周期报告 | 基于仪表板创建周期报告，可定时生成报告，支持发送邮件。 |
| 病毒概况 | 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。 |
| 病毒日志 | 病毒防护日志 | 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、网页安全防护日志。支持按分组、按终端、按时间查询 |
| 病毒报表 | 病毒防护报表 | 病毒防护报表有：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。按分组、按终端、按病毒名称统计。 |
| 扫描分析 | 扫描分析 | 对用户、管理员任务、管理员策略触发的扫描结果进行综合分析 |
| 主防分析 | 实时防护分析 | 实时防护是病毒防护的第一道防线。分析报表包含13项内容：实时防护概况、实时防护趋势、处理结果分布、处理结果趋势、检出引擎分布、病毒类型TOP10、检出终端TOP10、 病毒名称TOP10、 病毒文件TOP10 、 病毒路径TOP10、勒索程序TOP10、 挖矿木马TOP10 、WebShell木马TOP10 |
| 主动防御分析 | 主动防御是病毒防护的第二道防线。分析报表提供了18项防护的拦截趋势。其中，对于进程防护、驱动防护、勒索软件防护、网络入侵防护、僵尸网络攻击防护等五项防护提供了详细分析 |
| 黑白名单 | 支持手动导入，文本 | 支持手动导入、导出黑白名单，添加黑白名单。 |
| 支持文件导入 | 支持通过文件导入增加黑白名单。 |
| 支持一键鉴定 | 对于已加入的数据进行核对，供管理员参考，防止误入白和误拉黑 |
| 病毒防护任务 | 病毒扫描 | 病毒防护任务支持：全盘扫描、快速扫描、强力查杀、文件专杀、隔离区恢复、查杀未处理、断点续扫、支持自定义扫描策略 |
| 策略-通用设置 | 检测偏好 | 跟进内网环境选择检测偏好类型：高检出、低误报、均衡型。 |
| 开启关闭引擎 | 通过开关开开启关闭引擎的使用 |
| 云查杀模式 | 选择云查模式优先级，通过服务器代理云查、直连公有云、直连私有云、隔离网不云查。 |
| 引擎使用范围 | 选择引擎用于扫描、实时防护和主防 |
| 未知文件鉴定 | 样本鉴定开关，决定是否上报未知PE样本到相应的鉴定服务器 |
| 鉴定文件的大小设置 | 设置上传样本的最大大小。不鉴定超出范围的文件。 |
| 文件/路径信任设置 | 信任文件或者路径的设置，添加后病毒扫描将不扫描添加项。 |
| 扩展名信任设置 | 设置受信任的扩展名，检测病毒时会忽略该扩展名的文件。 |
| 禁止/允许终端用户修改路径文件白名单 | ▲是否允许用户添加黑白名单的设置，提供软件功能截图。 |
| 禁止/允许终端用户修改扩展名白名单 | 是否允许用户添加黑白后缀的设置。 |
| 文件黑白签名设置 | 添加设置信任或拦截的文件数字签名。 |
| 隔离区强安全管控 | 禁止从隔离区恢复数据 |
| 策略-病毒扫描 | 隔离区空间大小 | 设置隔离区大小，解决因隔离区占用过大，导致磁盘撑爆的问题；设置隔离区数据保留期限； |
| 病毒库更新提醒 | 设置在系统中进行病毒库过期提醒。 |
| 扫描文件类型 | ▲设置扫描文件的类型，提供软件功能截图。 |
| 发现病毒的处理方式 | 发现病毒的处理方式，自动处理、用户处理、仅上报不处理。 |
| 是否扫描网络路径 | 网络路径是否扫描的设置，解决可能因为扫描网络路径导致系统卡慢的问题。 |
| 全盘扫描是否扫描网络映射驱动器 | 网络路径是否扫描的设置，解决可能因为扫描网络路径导致系统卡慢的问题。 |
| 受限账号是否扫描网络映射驱动器 | 网络路径是否扫描的设置，解决可能因为扫描网络路径导致系统卡慢的问题。 |
| 扫描结果个性化展示 | 将扫描的结果完整展示，以解决非文件路径扫描处理不能被展示的问题。。 |
| 是否扫描压缩包 | 扫描过程中是否扫描压缩包的设置，设置为不扫描压缩包可以增加扫描的速度。 |
| 扫压缩包层数 | 压缩包层数设置，层数的多少影响扫描的速度。 |
| 扫描压缩包大小 | 扫描压缩包大小的设置，扫描压缩包大小决定了压缩包的扫描时间。 |
| 压缩包扫描检出的方式 | 可检出压缩包中全部病毒，但会增加扫描时间。 |
| 深度查杀模式进入方式 | 发现感染文件是否进入深度查杀模式的设置。 |
| 扫描任务是否允许终端用户暂停或停止 | 是否允许用户暂停停止扫描的设置。 |
| 扫描资源占用配置 | 扫描时候资源占用的配置，根据系统的整体配置来适当调整。 |
| 策略-实时防护 | 开启关闭实时防护 | 实时防护的开启功能选项。 |
| 发现病毒的处理方式 | 发现病毒的处理方式，自动处理、用户处理、仅上报不处理。 |
| 监控文件类型配置 | 配置实时防护的扫描文件类型所有文件/程序或文档。 |
| 是否监控压缩包 | 实时防护是否检测压缩包的设置。 |
| 监控压缩包的层数 | 实时防护检测压缩包的层数设置。 |
| 监控压缩包的大小限制 | 实时防护检测压缩包的大小限制。 |
| 监控文件的操作类型 | 实时防护监控文件的行为设置创建/修改，只读。 |
| 策略-主动防御 | 发现病毒的处理方式 | 发现病毒的处理方式，自动处理、用户处理、仅上报不处理。 |
| 进程防护 | 实时监测活跃进程的各种系统行为，发现风险自动进行提示和拦截。 |
| 注册表防护 | 实时监测系统关键注册表的创建、修改和删除行为，发现风险自动进行提示和拦截。 |
| 键盘记录防护 | 实时监测系统的键盘记录行为，当判定为恶意行为时根据策略进行提示和拦截。 |
| 系统账户防护 | 实时检测和拦截恶意程序创建、修改系统账户的行为，发现恶意行为时进行提示和拦截 。 |
| 驱动防护 | 实时监测系统的驱动安装、加载、卸载等行为，发现风险行为时进行提示和拦截。 |
| U盘防护 | 实时检测到系统接入可移动存储设备的行为，并对设备中关键位置的文件进行安全扫描，发现风险文件进行提示和清理。支持将U盘病毒文件隔离在系统盘中。 |
| 邮件防护 | 实时检测邮件客户端接收文件的安全性，对发现的风险进行提示和清理。 |
| 下载防护 | 对下载软件、浏览器下载的文件进行安全检测，发现风险文件的风险进行提示和清理。 |
| IM防护 | 对通讯工具(IM)下载的文件进行安全检测，发现风险进行提示和清理。 |
| 局域网文件防护 | 实时检测局域网网络共享文件的拷入、执行行为，当检测文件不安全时进行提示和拦截。 |
| 网页安全防护 | 对浏览器中访问的URL和网页内容进行安全扫描，发现的风险进行提示和拦截。 |
| 勒索软件防护 | 实时监测未知风险程序的篡改文件和勒索病毒相关特征行为，拦截和阻止勒索病毒入侵。 |
| win7加固 | 解决Win7系统停服后的漏洞利用问题，为系统RCE，浏览器、Office应用等进行漏洞利用防护 |
| XP加固 | 解决WinXP系统停服后的漏洞利用问题，为系统RCE，浏览器、Office应用等进行漏洞利用防护。 |
| 网络入侵防护 | 对流入本机的网络包数据和行为进行检测，在网络层拦截漏洞攻击、黑客入侵等威胁。 |
| 僵尸网络防护 | 防护对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2连接等威胁。。 |
| 网络攻击防护 | 防护对流出本机的网络包数据和行为进行检测，在网络层拦截本机风险程序对外的漏洞攻击行为。 |
| DNS防护 | 检测和保护本机DNS的安全性，防止终端DNS和HOSTS被恶意篡改 |
| ARP攻击防护 | 检测和拦截局域网中的ARP欺骗攻击行为。 |
| 远程登录防护 | 对黑客常用的远程登录密码爆破行为进行检测，拦截恶意远程登录的行为；支持设置终端白名单。 |
| 策略-高级威胁防御 | 无文件攻击防护 | 针对Powershell、VBS、JS等脚本化攻击场景，对WMI在内存执行行为进行监控，能有效发现无文件攻击行为，并能对其攻击进行防护阻断。 |
| 文档攻击防护 | 针对Office执行VBA宏代码、远程模版执行、DDE、内嵌对象执行、Excel 4.0宏等攻击行为的监测，并能对其攻击进行防护阻断。 |
| 横移渗透攻击防护 | 针对内网横向移动渗透攻击进行防护，可以有效的防护阻断高危蠕虫病毒传播扩散以及减少勒索、挖矿等风险的发生。 |
| 内存攻击防护 | 针对可疑程序启动内存威胁攻击行为检测，高级威胁攻击、攻防演练场景和日益复杂、更具攻击性的未知威胁的防御，阻截传统防病毒方案难以防护的安全威胁。 |
| 策略-定时查杀 | 配置定时查杀计划 | ▲添加定时查杀计划，提供软件功能截图。 |
| 支持开机查杀计划 | 添加在开机的时候进行查杀的计划。 |
| 支持执行错过的查杀计划 | 在扫描任务启动时间错过后，在指定的时间内继续执行该任务计划。 |
| 策略-弹窗设置 | 查杀任务可配置自定义策略扫描 | 可以根据不同的查杀任务配置不同的查杀策略。 |
| 免打扰模式 | 病毒检出和处置都不弹框；应用于不能弹窗的终端。 |
| 智能模式 | 对已知的病毒自动处理，对未知的病毒提示处理。 |
| 告警中心 | 自定义模式 | 自定义弹窗模式，可以根据需要选择需要模块弹窗的提示。 |
| 开放平台（syslog） | 支持病毒防护接入告警中心 | 通过监控业务软件目录、文件的方式对终端误报进行告警；支持配置告警规则。 |
| 其他 | 病毒查杀日志 | syslog支持输出：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、网页安全防护日志。 |
| 未登录扫描 | 对不经常登录设备，保障在未登录的情况下，能够执行管理员分发的扫描任务。。 |
| 支持注册Windows安全中心 | 加入微软MVI(Microsoft Virus Initiative)，支持接管Windows安全中心。 |
| 支持Windows PC | 支持Windows PC版本功能。 |
| 支持Windows Server | 支持Windows Server版本功能。 |
| 支持命令行扫描 | 支持命令行方式对指定文件、路径进行扫描。 |
| 支持拖拽扫描 | 扫描将文件直接拖拽到天擎界面，直接发起扫描。 |
| 病毒类型 | 木马、病毒、蠕虫、漏洞攻击类、危险程序、勒索程序、挖矿木马、广告程序、恶作剧类程序、后门程序、病毒生成器、木马释放器、黑客程序、可疑加壳的程序、内核类恶意驱动、修改启动分区的程序、下载者、间谍程序、拒绝服务类程序、泛洪攻击类程序、网银木马、外挂类程序、病毒源、流量劫持类程序、代理型木马、拨号型木马、键盘记录器、分布式拒绝服务类程序、虚假告警类程序、被滥用的程序、BAT脚本恶意文件、网页恶意文件（含webshell）、JS脚本恶意文件、VBX脚本恶意文件、POWERSHELL脚本恶意文件、BASH脚本恶意文件、宏病毒、危险的快捷方式命令行、信息窃取应用、恶意扣费应用、风险应用、禁止访问的程序、具有潜在风险的程序。 |
| 引擎支持 | 扫描范围 | 病毒扫描支持扫描：启动项、系统服务、系统驱动、任务计划、浏览器插件、内存进程 |
| 自研引擎 | QCE-云查杀引擎、QRE-云规则引擎、OWL-启发式特征检测引擎、QDE-人工智能检测引擎、TDE-威胁情报检测引擎（云引擎中） |
| BD-知名国际品牌杀毒引擎 | 覆盖国外威胁样本 |
| 精细化运维 | 自动修复 | 自动选取合适时间修复漏洞。 |
| 按时间段修复 | 支持自定义设置多个修复时间段，一周七天可设置多个不同的时间段。 |
| 支持按照产品类型修复漏洞 | 支持按照产品类型精确修复漏洞，比如操作系统、IE、Office。 |
| 按操作系统版本修复漏洞 | 支持精细配置按照操作系统版本修复漏洞 |
| 按Office版本修复漏洞 | 支持精细配置按照Office版本修复漏洞 |
| 按漏洞级别修复 | 支持按照漏洞级别（安全更新、重要补丁、功能补丁、功能补丁）修复漏洞 |
| 有未修复漏洞或者功能缺陷时提醒终端用户修复 | 支持不强制修复漏洞，仅提醒，终端用户可自主修复漏洞，给企业管理更多的灵活选择。 |
| 支持禁止终端忽略漏洞补丁 | 防止终端用户违规忽略漏洞，遗留安全隐患。也允许终端用户忽略补丁。 |
| 支持禁止终端用户修复，制定统一的补丁安装策略。 | 防止用户自助进行补丁修复，企业统一设置补丁策略。 |
| 支持按时间段禁止终端用户修复，防止终端用户自己在办公时间安装补丁影响办公 | 防止在办公时间修复补丁，占用公司网络带宽同时影响用户办公 |
| 可设置补丁下载、安装顺序 | 逐个下载和安装（有效节省漏洞修复时间）或全部下载完之后再安装（可大幅减少下载时的CPU 占用） |
| 支持关闭Windows update | 支持关闭Windows7及以下版本的Windows update，避免终端安装了有问题的补丁，影响办公。 |
| 打补丁影响到编辑Office文档时提醒 | 打补丁影响到编辑Office文档时提醒终端用户，避免丢失在编辑的文档。 |
| 支持设置终端保存补丁文件时间 | 支持自定义终端补丁文件保留时间，节省终端磁盘空间。 |
| 支持自定义终端保存补丁文件目录 | 支持自定义终端保存补丁文件目录，用于在系统盘空间不充足的情况下，将补丁文件保存在其他分区，提高补丁安装成功率。 |
| 补丁生效设置 | 支持仅提醒一次，减少对终端用户的打扰。 |
|  |
| 支持间隔提醒，用于催促终端用户重启。 |  |
| 在补丁安装完成后根据策略自动重启系统，适用于无人值守、共用终端。 |  |
| 在补丁安装完成后根据策略自动重启系统，适用于无人值守、共用终端、服务器，重启时间可控，更为稳妥。 |  |
| 智能忽略 | 智能分析补丁安装失败。成功的补丁。 |  |
| 支持区分补丁安装者 | 支持区分补丁安装者，自动安装、终端用户手动安装还是其他程序。 |  |
| 支持禁止用户卸载补丁 | 支持终端用户自行卸载补丁面临风险。 |  |
| 强制取消安装补丁 | 用于紧急情况，当发现补丁有严重问题，需要立即停止所有的安装。 |  |
| 支持终端用户手动修复 | 终端可视化界面，支持终端用户主动修复漏洞。 |  |
| 补丁任务 | 补丁安装 | 支持主动扫描终端的扫描的补丁安装情况。 |  |
| 支持主动修复终端发现的补丁。 |  |
| 支持管理员统一强制卸载/提醒后卸载一台终端的多个补丁。 |  |
| 补丁文件管理 | 为终端提供下载补丁文件的服务 | 为终端提供下载补丁文件的服务。 |  |
| 补丁文件可视管理功能 | ▲查看、管理服务器补丁下载情况补丁功能，提供软件功能截图 |  |
| 隔离网的下补丁更新 | 支持隔离网离线更新补丁库、补丁文件、系统升级包等补丁管理业务需要的数据。 |  |
| 离线更新工具支持按照补丁号搜索下载。 |  |
| 自动清理过期补丁文件 | 自动清理过期补丁文件。 |  |
| 补丁日志 | 记录安装、卸载补丁的事件日志 | 终端信息、补丁号、补丁级别、补丁类型、事件类型、结果、详细描述、发生时间。 |  |
| 补丁统计 | 按终端维度统计补丁安装情况 | 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。 |  |
| 支持查看终端的补丁库版本、最近扫描时间。 |  |
| 支持查看分析未安装补丁的原因，以帮助运维管理员提高补丁安装率。 |  |
| 支持查看终端补丁已安装、未安装的详细列表。 |  |
| 按补丁维度统计补丁安装情况 | 支持按照补丁（漏洞）的维度统计漏洞修复情况，包括补丁号、CVE号、安全公告、补丁名称、补丁描述、漏洞级别、发布日期、未安装终端数、已安装终端数、已安装未生效终端、已忽略终端数、已排除终端数，并支持统计数据导出。 |  |
| 补丁统计报表 | 统计一段时间内新发现补丁、安装补丁的趋势。 |  |
| 统计一段时间内补丁未安装的原因分类。 |  |
| 统计一段时间内补丁安装失败的原因分类。 |  |
| 统计一段时间内已安装的级别分类。 |  |
| 统计一段时间内终端、分组、补丁安装次数的TOP10。 |  |
| 按照分组维度统计补丁安装次数。 |  |
| 按照终端维度统计补丁安装次数。 |  |
| 按照补丁维度统计补丁安装次数。 |  |
| 系统升级 | 管理员通过下发任务升级已经或者即将停服的系统。 |  |
| 终端用户主动升级操作系统。但是升级的版本受管理员控制，以免随便升级出现软件兼容等问题影响工作。 |  |

**五、终端安全管理系统运维需求**

授权数：终端安全管理系统，3800点

部署位置：医院PC终端

授权许可时间：一年软件授权许可（2024年7月1日-2025年6月30日）

质保时间：一年软件升级及服务（2024年7月1日-2025年6月30日）

|  |  |  |  |
| --- | --- | --- | --- |
| 技术指标 | | | 指标要求 |
| 资产管理 | 单点维护 | 单点-进程查看 | 远程查看终端实时运行的进程，需要包含进程名称，进程用户、命令行（执行路径+执行参数）、内存占用、签名、产品名称、公司名称，支持远程停止进程 |
| 单点-网络信息 | 远程查看计算机各个网卡配置信息、流量以及网络连接详情 |
| 终端管控 | 远程协助 | ▲远程协助 | 支持管理员对在线终端进行远程协助，提供软件功能截图。 |
| 锁屏时远程 | 支持被控端锁屏时建立远程连接 |
| 无客户端远程 | 支持主控端无天擎客户端时建立远程连接 |
| 中继器指定 | 支持配置客户端指向的远程中继器地址 |
| 远程协助-文件传输 | 管理员对在线终端进行远程时，支持在被控端和主控端直接进行文件传输 |
| 外设管理 | 外设控制 | 禁用usb口、串口、并口、1394、PCMCIA |
| 支持光驱的读盘、刻盘权限控制 |
| 支持对USB存储设备、存储卡、冗余硬盘、软驱、打印机、扫描仪、键盘、鼠标、红外、蓝牙、摄像头、手机/平板进行设备控制 |
| 支持对磁带机、移动数据网卡、MODEM设备、ISDN设备、ADSL设备进行控制 |
| 支持对U盘设备、闪存设备、移动硬盘进行只读和写入权限的划分 |
| 可禁止连接所有蓝牙设备或只禁止连接手机、电脑类型的蓝牙设备 |
| 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） |
| 单独设备控制 | 支持自定义根据PID,VID/设备实例路径/设备名称进行设备管控 |
| 禁用提示 | 自定义提示消息，当终端违规使用外设时助手会产生消息提示 |
| ▲违规日志 | 记录终端用户违规使用外设行为，提供软件功能截图。 |
| 进程管理 | 管控模式 | 部署模式：只告警，不拦截违规进程；防护模式：拦截违规进程，同时上报告警日志 |
| 应用进程 | 第三方进程采用白名单模式或黑名单模式管控 |
| 进程白名单 | 根据进程的名称，MD5值，签名等属性允许名单中的进程运行，运行名单外的进程时，弹框告警，同时上报告警日志（系统和天擎进程默认放行） |
| 进程黑名单 | 根据进程的名称，MD5值，签名等属性禁止名单中的进程运行，同时上报告警日志（系统和天擎进程默认放行） |
| 进程红名单 | 对指定的进程进行运行保护 |
| 检测到进程未运行时主动拉起运行 |
| 进程流量监控 | 设置某进程的流量阈值，超过阈值可断网 |
| 进程性能监控 | 可设置在一定时间长度内，内存或CPU持续占用超过一定百分比时进行监控 |
| 日志上报 | 根据进程管控规则设置日志是否进行上报 |
| 违规外联 | 自定义地址探测 | 支持普通地址、外联响应中心地址、探测中心三种探测目标 |
| Tracert路径探测 | 可记录tracert探测路径作为探测依据 |
| 特殊字符校验 | 普通地址探测时，收到的返回报文中特殊字符校验 |
| 外联响应中心 | 天擎提供的外联探测校验程序，由客户放置在公网环境，作为内网终端外联探测的目标地址 |
| 出口探测 | 支持对终端访问互联网的出口进行探测，对使用不合规出口的终端进行网络隔离 违规外联告警、告警时长统计、出口统计及互联网出口使用情况 |
| 能耗管理 | 节能管理 | 设置终端工作时间，对在工作时间外开机的终端进行处置措施，并产生告警日志 |
| ▲设置终端每天定时关机，提供软件功能截图 |
| 设置终端指定运行时长后，对终端进行处置措施，并产生告警日志 |
| 设置终端空闲（无键鼠操作）指定时长后，对终端进行处置措施，并产生告警日志 |
| 支持关机，重启，注销，锁定，休眠，睡眠等处置措施 |
| 设置终端关机前倒计时提醒时间 |
| 设置终端关机前提示文字 |
| 终端弹出关机提示后，终端可主动取消定时关机，同时上报告警日志 |
| 终端性能监控 | CPU、内存、磁盘使用监控和告警 |
| 网络管控 |  | 可禁用启用本机创建热点 |
| 可禁止IPV6地址的使用 |
| 禁止修改IP地址 |
| 禁止修改MAC地址 |
| 禁止使用无线网卡 |
| 禁止使用USB网卡 |
| 可禁用启用无线网卡的使用 |
| 动态获取或统一给终端设置DNS地址，支持IPV4/IPV6两种协议 |
| WiFi管理 | 可限制SSID连接和多SSID同时使用。支持设置wifi白名单、支持验证无线ap的mac地址是否合法，匹配成功才允许连接指定的ssid信号。 |
| 隐藏被禁止连接的无线网络 |
| 可限制无线有线网卡同时使用 |
| 网络流量监控 | 监控单位时间内的网络流量，超过阈值可断网 |
| 终端网络流量 | 查看终端流量使用汇总情况 |
| 终端网络连接 | 查看进程网络连接的详情 |
| 违规日志 | 对终端违规使用网络行为进行告警 |
| 服务管控 | 服务 | ▲支持对指定名称的服务禁止运行，提供软件功能截图 |
| 支持对指定名称的服务设置自动运行 |
| 支持对指定名称的服务设置禁止启动、开机自启动、启动、停止、开机不启动 |
| 外发管控 | 文件外发管控 | 禁止通过蓝牙进行文件外发，不影响蓝牙耳机、键盘、鼠标等设备使用 |
| 网页上传管控 | 可对网页文件上传行为进行阻断，支持通过URL、文件类型进行放行；支持对大文件上传行为进行放行；支持对数据防泄密中申请加白的文件进行放行 |
| 桌面加固 | 自定义桌面壁纸 | 可自定义上传图片并进行桌面壁纸的替换 |
| 自定义屏保 | 可定义系统进入屏保的最长等待时间，并支持将自定义屏保文件上传且生效 |
| 本地安全策略 | 权限禁用：修改计算机名、开启文件共享、注册表编辑器 |
| Internet-信任站点 | 支持对浏览器的信任站点进行配置添加管理 |
| Internet-代理服务器 | 支持对浏览器的代理进行禁止代理或代理配置管控 |
| 安全模式管理 | 支持对终端的安全模式进行管控，支持设置安全模式登录密码或禁用系统安全模式 |
| 配置检测周期 | 对桌面加固的配置检测自定义检测周期 |
| 自定义桌面壁纸 | 可自定义上传图片并进行桌面壁纸的替换 |
| 屏幕保护 | 可定义系统进入屏保的最长等待时间 |
| 账户安全策略 | 可自定义账户无效登录次数，并支持禁止提升账户权限、紧张增加/删除账户 |
| 共享安全策略 | 支持共享管控 |
| 外设管理日志 |  | 记录终端的外设，进程，违规外联，能耗，远程协助，网络，服务使用情况，包括发生时间，计算名，终端分组，IP-MAC地址，操作系统等同时可按照时间和分组对日志进行查询 |
| 进程管理日志 |
| 违规外联日志 |
| 能耗管理日志 |
| 远程协助日志 |
| 远程文件传输日志 |
| 网络管控日志 |
| 网页上传管控日志 |
| 服务管理日志 |
| 外设管理 |  | 对终端的外设，进程，违规外联，能耗，网络使用情况进行统计，可按照时间和分组进行统计 |
| 进程管理 |
| 违规外联 |
| 能耗管理 |
| 网络管控 |

**六、TDA 威胁发现系统运维需求**

授权数：TDA威胁发现系统1套

部署位置：医院内网旁路

授权许可时间：一年软件授权许可（2024年7月1日-2025年6月30日）

质保时间：一年软件升级及服务（2024年7月1日-2025年6月30日）

|  |  |  |
| --- | --- | --- |
| **软件性能参数** | | |
| 项目 | 参数 | 内容说明 |
| 侦测分析能力 | 扫描对象 | 1. 可扫描网络第2层至第7层数据流量 |
| 2. 可选择特定协议或IP地址自定义检测 |
| 3. 支持自定义IP地址、URL、域名与文件的访问监控 |
| 支持协议 | 支持超过 100 种以上的网络协议支持，如 HTTP, FTP, TFTP, SMTP, POP3, IMAP, SNMP, IRC, DNS, DHCP, P2P, SMB, RDP, VNC, TELNET, TCP, UDP和数据库协议（MSSQL, MySQL, Oracle）等。 |
| 恶意文件侦测 | 能够侦测各种文件型病毒，如木马、僵尸、后门等 |
| 移动设备恶意程序侦测 | 1. 可侦测识别iOS、赛班、安卓、微软等移动设备 |
| 2. 可与移动应用信誉系统（MRS）联动，侦测安卓系统的恶意应用App |
| 恶意行为分析侦测 | 威胁流量与协议异常检测 ，如零日攻击、网络蠕虫、木马、后门、僵尸、间谍软件、网络漏洞、网页威胁（网页漏洞、跨网站攻击）、钓鱼邮件、暴力攻击、数据库注入攻击等 |
| 未知威胁侦测（含沙盒分析） | 1. 具有虚拟化沙盒系统 |
| 2. 能够对样本进行过滤去重减少分析数量 |
| 3. 具有安全风险评估技术分析：包含针对注册表、内存、程序、网络活动、文件系统等操作系统环境的变化进行记录与分析 |
| 4. 具有高度定制化，可以支持使用用户环境特性的Windows操作系统平台与应用 |
| 服务器级：Windows 2003/2008/2012 |
| 用户端级：Windows XP/7/8/10 |
| 5. 支持未知威胁事件证据留存 |
| 6. 文档分析支持：Acrobat Reader 7, 8, 9, X, 微软Office常用版本（Word, Excel, Powerpoint）、Flash常用版本、LNK、执行文件，微软 HTML Application（HTA）, JS, JSE, VBS, VBE, Java, Java Applet，PowerShell Script 等。 |
| 7. 提供分析结果的自动入库：侦测设备自我学习功能 |
| 8. 报表事件 |
| 应用程序侦测 | 1. P2P流量：Ares、Bittorent、Blubster、eDonkey、Kazaa、Gnutella、Winny、Foxy |
| 2. 实时通讯软件：AIM、Goggle Talk、MSN、Skype、Yahoo Messenger |
| 3. 流媒体：RTMP、RTSP、SHOUTCast、WMSP |
| 信誉分析 | 1. 中国区域恶意网页评估系统 |
| 2. 恶意网站与域名分析 |
| 3. 僵尸网站与控制服务器分析 |
| 4. 移动应用分析 |
| 多协议关联分析 | 能够自动关联不同协议、不同会话的威胁日志，筛选出严重事件 |
| 终端识别 | 1. 支持在动态IP环境辨认真实终端MAC地址 |
| 2. 支持XFF，在web代理环境中辨认真实终端 |
| 3. 识别终端操作系统，包含Windows、iOS、安卓等。 |
| 定制化黑白名单 | 可将用户长期累积的黑白名单（如IP/URL/Domain/File SHA1） 汇入TDA实行侦测或是排除。 |
| 常见漏洞检测 | Tomcat写文件漏洞，ImageMagick命令执行漏洞，ElasticSearch 命令执行漏洞，Samba 远程命令执行漏洞, ThinkPHP Builder.php SQL injection, Adobe ColdFusion 文件上传导致任意代码执行漏洞, GhostScript 沙箱绕过漏洞, Spring Data REST PATCH请求代码执行漏洞, Weblogic wls9\_async\_response 反序列化远程命令执行漏洞, Jenkins RCE, Spring Data Commons组件远程代码执行漏洞,spring-messaging Remote Code Execution, Fastjson反序列化漏洞等 |
| WebShell检测 | 支持如下Webshell检测：ghost webshell，PHP webshell2，ASP webshell1，PHP webshell3，PHP Webshell4，ASP webshell\_2 |
| 黑客工具检测 | 支持如下黑客工具攻击检测：Cknife，SQLmap，havij，awvs，Nmap，pangolin，EarthWorm，sql综合利用工具，dirbuster，w3af，OWASP ZAP 2.6.0，Bbscan，OpenVAS，Golismero security scanner, IIS\_shortname\_Scanner, HeartbleedScanner, Heartbleed-msf |
| 病毒爆发遏制服务 | 高危病毒侦测 | 支持多种高危病毒的侦测: WORM\_DOWNAD.E/ WORM\_RONTKBR/ WORM\_SILLYIM/ WORM\_WALEDAC/ TROJ\_ILOMO/ TROJ\_FAKEAV/ PE\_VIRUX |
| 高危病毒侦测实时通知 | 实时邮件通知，同时内容包含攻击源与感染源等讯息 |
| 高危病毒流量阻断 | 实时阻断高危病毒流量 |
| 高危病毒列表更新 | 自动更新高危病毒列表 |
| 威胁流量存储能力 | 威胁流量存储 | 支持基于IP地址段、检测规则条件的威胁流量存储设置 |
| 威胁流量数据下载 | 支持威胁流量的自动存储，及威胁流量PCAP文件格式下载 |
| 威胁验伤能力 | 网络流量威胁验伤 | 支持对网络Http攻击流量的应答码及攻击状态展示 |
| 主机威胁联动验伤 | 1. 支持与主机威胁回溯调查的自动验伤功能，支持威胁类型包括如下： |
| -勒索病毒(Ransomwares) |
| -木马病毒(Trojan) |
| -恶意代码(Malware) |
| -僵尸网络(Botnet) |
| -钓鱼网站(Phishing) |
| -渗透工具 |
| -挖矿网址 |
| -挖矿病毒 |
| -带毒邮件攻击(Mail attack) |
| 2. 支持主机威胁联动验伤报告的自动生成 |
| 3. 主机威胁联动验伤报告支持客户自定义徽标功能 |
| 4. 主机威胁联动验伤报告支持客户自定义水印功能 |
| 日志、报表、事件管理 | 日志管理 | 1. 可显示受感染主机的APT攻击阶段，帮助管理者制定响应策略 |
| 2. 提供智能日志搜寻以及可定制化过滤条件，定制化过滤条件并可支持存储以及汇出汇入 |
| 3. 内建常用过滤条件，可快速过滤出常见攻击类别(如勒索软件，横向扩散攻击等) |
| 4. 支持Syslog协议，可以实时传输日志到syslog服务器，选择传输的内容类型 |
| 5. 自动检查日志数据库健康与修复数据库 |
| 6. 可以依据时间,协议,威胁类型,IP网段,监控群组等查询条件查询日志 |
| 报表系统 | 1. 自动提供经过分析后的图形化日/周/月报表 |
| 2. 自动寄送报表与处理建议功能 |
| 3. 提供多协议关连分析引擎，自动分析日志，降低人为分析成本 |
| 4. 集成用户统一威胁预警地图显示，结合地理位置直观标示威胁位置，在地图中实时风险事件定位与威胁流量监控，同时可以区域与威胁事件关连，结合威胁仪表板，深入了解区域威胁情况 |
| 5. 具有用户威胁仪表板接口，提供用户整体安全等级，同时以威胁/群组/用户端三个面向设定查询时间进行数据分析 |
| 6. 支持多种报表模板 |
| 工具 | 可提供快速响应与专杀工具 |
| 监控仪表板 | 1. 模块化插件设计：可以客制弹性配置监控仪表板 |
| 2. 仪表板地图式展示：展示攻击来自哪些区域,用户计算机连接到哪些区域 |
| 3. 监视列表：可将重要资产如服务器或是终端用户等加入仪表板中的监视列表中随时查看 |
| 4. 提供可选排名5/10/20事件以表格,饼图,柱状图展示 |
| 5. 沙盒分析状态：分析统计信息，排名靠前的主机，排名靠前的可疑文档等 |
| 6. 威胁流量的比例分布 |
| 7. 硬件系统使用状态（CPU，内存，硬盘） |
| 8. 实时性 |
| 安全精密联动 | 网络、终端、服务器的全面联动分析及响应 | 支持沙箱分析产品DDAN、终端安全OSCE、网关安全DeepEdge, 邮件沙箱DDEI,  云主机安全Deep Security等 |
| 日志统一分析 | 多设备日志统一呈现 | 1.支持多台TDA设备的告警日志的统一收集和存储 |
| 2.多设备日志的统一分析及图形化展示，包括柱状图、饼图、列表等，且支持数据的实时更新 |
| 日志告警 | 支持基于特定条件的告警设置，如敏感字段、告警数量值等，支持基于告警内容的邮件提醒功能 |
| 权限管理功能 | 1.支持基于数据流的分权管理 |
| 2.支持产品日志的分级查询，不同权限管理者拥有不同的日志查看级别 |
| 报表功能 | 支持TDA报表功能，包括日报、周报、月报以及按需设定等多种周期报表 |
| 关联分析功能 | 1.支持多台TDA的威胁数据处理，自动生成基于主机的网络攻击脉络图 |
| 2.支持精密联动日志关联分析报告 |
| 通知 | 检测潜在安全风险通知 | 自动寄送报表与处理建议功能 |
| 提供多协议关连分析引擎,自动分析日志降低人为分析成本 |
| 具备有报表系统, |
| 可以依据1)进出流量方向 2)时间段 3)数量 4)潜在威胁类型进行设定通知 |
| 检测到已知安全风险时进行通知,可以依据1)进出流量方向 2)时间段 3)数量 4)潜在威胁类型进行设定通知 |
| 检测已知安全风险通知 | 检测到已知安全风险时进行通知,可以依据1)进出流量方向 2)时间段 3)数量 4)潜在威胁类型进行设定通知 |
| 检测高风险用户端通知 | 各个IP地址的检测数在设定时间段达到阈值时进行通知 |
| 高网络通信量通知 | 可以自动侦测一天24小时内每个时段的流量或管理设定网络通信流量时，当超过阀值设定通知 |
| 文件分析状态通知 | 可通知管理员无法分析的文件 |
| 部署与管理 | 部署 | 1. 支持旁路安装模式 |
| 2. 支持TAP分流安装模式 |
| 3. 支持非对称路由 |
| 4. 支持思科与华为的远程端口镜像协议 |
| 设备管理 | 1. 基于B/S的管理架构，Web界面支持 MS IE、Netscape、Firefox、Opera、Chrome 五大浏览器 |
| 2. 提供命令列（CLI）配置模式 |
| 3. 提供SSH远程调试模式 |
| 4. 支持SNMP |
| 5. 可利用中央管理系统对多台设备统一进行管理 |
| 升级 | 升级方式 | 1. 支持实时在线升级、自动在线升级、手工升级多种升级方式 |
| 2. 每周两次升级频率以上 |
| 侦测设备自我学习升级 | 沙盒系统分析结果自动回馈到云端大数据平台，可以下发到更多的侦测设备 |
| 更新源 | 全球升级架构以及本地升级源的设计降低升级带宽使用 |
| 设备安全 | 安全性 | 1. 设备失效侦测 |
| 2. 通过强加密的SSL安全通道进行通讯 |
| 3. 数据库自动修复功能 |
| 联动性 | 联动性 | 1. 能够与威胁阻断系统联动，根据监控结果自动阻止不安全计算机的网络通讯，或是阻断恶意通讯连接 |
| 2. 支持中央管理系统，多台设备可统一管理 |
| 3. 支持中央报表生成系统，多台设备可集中生成报表 |
| 4. 能够集成外接沙盒分析系统，提高未知威胁分析处理能力 |
| 5. Syslog日志为CEF或LEEF格式，可集成第三方SIEM/SOC系统 |
| 6. 提供 Web API 以利第三方集成使用本地威胁情报 |
| 7. 支持态势感知平台 |
| 8. 支持调查取证平台 |

**七、服务和支持要求**

1、运维响应时间

每月一次例行检查，检查完成后，投标人提交检查报告。5\*8\*NBD标准维护服务响应，一周五天，每天8小时工作时间，承诺当日响应服务；

2、应急响应时间

7\*24\*2应急现场服务响应，一周7天，每天24小时内，2小时现场响应，当系统出现严重故障影响招标人工作正常开展, 投标人按7\*24\*2小时响应服务，按招标人要求派工程师现场响应服务。

3、售后服务说明

1. ★提供原厂售后服务承诺函
2. 常规运维原厂授权认证工程师服务
3. 应急响应原厂资深认证工程师服务
4. 厂家售后服务电话支持服务
5. 远程服务支持

4、部署要求

1）时间：2024-6-30,24:00前完成

2）人员：由中标人提供不少于2名本公司专业工程师现场专职服务，需要提供最近六个月内社保证明。

3）▲中标人在部署前需完成原设备上防病毒软件卸载或版本升级，投标文件中提供承诺函。

5、培训要求

为招标方提供完整的培训服务，确保招标方正确了解项目全况，在投标文件中提供具体方案。

6、系统测试条款

▲中标后3日内提供相关产品软件进行功能测试，功能测试结果需完全满足招标文件的要求。投标文件中提供承诺函。

7、数据保密要求

满足等保三级2.0要求。

**（二）预算金额**

人民币110.00万元

**（三）资格条件**

1）在中华人民共和国境内注册，具有独立承担民事责任的能力。

2）本项目不接受联合体投标；

3）本项目不接受分包、转包；

4）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

5）近三年未被列入信用中国网站(https://www.creditchina.gov.cn)失信被执行人、异常经营名录、税收违法黑名单、政府采购严重违法失信行为记录名单；中国政府采购网(www.ccgp.gov.cn)严重违法失信行为记录名单；“国家企业信用信息公示系统”（http://gsxt.saic.gov.cn/） “行政处罚信息（较大数额罚款）”、“列入经营异常名录信息”、“列入严重违法失信企业名单（黑名单）信息”。