

**杭州市富阳中医骨伤医院**

**信息安全加固一期**

**采购需求**

**2019年11月**

**目录**

1 项目概要 3

1.1 项目名称 3

2 建设背景 3

3 需求参数 3

4 建设周期、付款、保修要求 20

# 项目概要

## 项目名称

杭州市富阳中医骨伤医院信息安全加固一期

# 建设背景

根据国家公安部、保密局、国家密码管理局、国务院信息化领导小组办公室于联合颁布了861号文件《关于开展全国重要信息系统安全等级保护定级工作的通知》和《信息安全等级保护管理办法》要求通过本项目的采购达到“基础支撑系统”等保三级、“面向患者服务系统”等保三级要求。

# 需求参数

**3.1信息安全设备采购清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品类别** | **类型** | **数量** |
| 1 | 终端杀毒软件 | 终端安全管理系统 | 200 |
| 2 | 云终端EDR | 端点安全软件 | 400 |
| 端点安全软件（Windows Server） | 60 |
| 端点安全软件（Linux Server） | 30 |
| 3 | 备份一体机 | 容灾一体机 | 1 |
| 4 | 下一代防火墙 | IPS防火墙 | 1 |
| 5 | 准入控制 | 内网准入设备 | 2 |

**3.2信息安全设备需求**

**3.2.1 终端杀毒软件**

|  |  |
| --- | --- |
| **指标项** | **主要技术参数** |
| 授权点数 | 本次配置200个点WIndows终端防护 |
| 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； |
| 资产管理 | 按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控CPU温度、硬盘温度和主板温度 |
| 支持自动发现设备的IP-MAC地址的绑定 |
| 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 |
| 支持正版软件的正版序列号的读取功能，确保软件正版化。 |
| 病毒、恶意代码、木马防护 | 支持文件、引导区、内存、注册表、服务、进程、进出文件、目录、压缩文件、网页等恶意代码、恶意样本查杀; 支持内存实时监控查毒; 拦截下载器自动下载木马程序、恶意推广程序、盗号木马； |
| 要求能够支持XP系统的漏洞利用防御，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； |
| ★对敲诈者病毒提供防护机制，同时可提供相关解密工具，解密工具为自主研发 |
| 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（提供至少2个厂商认证证书） |
| 补丁分发与漏洞修复 | 要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型； |
| ★产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能 |
| 产品具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端P2P补丁分发加速，有效节省外网带宽资源 |
| 运维管控 | 支持远程协助终端（不依赖Windows远程桌面协议）、远程关机、重启终端； |
| 支持终端进程红名单、黑名单、白名单功能，可设置核心进程必须运行，也可保护核心进程不被结束。 |
| 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 |
| 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 |
| 支持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、杀毒软件检查 |
| 产品资质 | ★提供公安部颁发的《计算机信息系统安全专用产品销售许可证》内网主机监测（一级）资质证书。 |
| 具备该软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书。 |
| 原厂质保 | ★提供三年质保及病毒库升级 |

**3.2.2云终端EDR采购参数**

|  |  |
| --- | --- |
| **指标项** | **主要技术参数** |
| 授权点数 | 本次配置400个点Windows终端防护，60个Windows Server客户端许可，30个Linux SERVER客户端授权 |
| 产品组成 | 产品是软件形态，包含管理平台和终端Agent软件；单一管理控制中心可统一管理分别部署在Windows PC，Win服务器以及Linux服务器的客户端软件Agent软件支持32位和64位的Windows系统和64位的Linux系统。产品和国内主流云平台实现解耦和，适用于Vmware、华为云、华三云、阿里云、腾讯云等国内主流云平台的主机； |
| ★管理平台采用软件包方式提供安装，安装后其中必须具备终端管理、终端病毒查杀、文件实时监控防护、东西向访问微隔离、暴力破解检测响应、WebShell检测响应、设备联动响应等功能组件，保障平台的扩展性和兼容性。 |
| 联动要求 | 为方便我单位的安全管理智能化，要求可以和本次采购的防火墙设备、上网行为管理设备等同时联动，综合响应杀毒 |
| 上网行为管理联动：支持管理员在上网行为管理平台通过EDR管理平台对其下属终端下发快速查杀任务，并查看其下发的查杀任务中各个终端的查杀状态、查杀结果以及查杀任务中查杀出来的病毒进行处置 |
| 防火墙联动：支持防火墙通过配置终端检测响应管理平台IP地址实现与EDR平台的联动，实现端网安全联动；支持在防火墙上对下发的查杀任务中查杀出来的病毒进行处置； |
| 支持将终端安全软件客户端检测出来的恶意文件事件、暴力破解事件、微隔离事件的日志上报到同厂商安全态势感知平台，安全态势感知平台进行分析和展示； |
| 管理平台要求 | 支持终端资产盘点管理，支持自动收集终端资产状况，包括：主机名、在线/离线状态、IPv4地址、MAC地址、操作系统、终端Agent版本、病毒库版本、最近登录时间、最近登录的用户名； |
| 支持控制台显示当前平台终端总数、在线/离线数量、服务器终端/PC终端数量；支持Vmware、Ctrix、Hyper-V、华为云、华三云、阿里云、腾讯云等国内主流云平台的虚拟机防护，并可在同一个管理平台进行统一管理。 |
| 支持病毒查杀、Webshell、暴力破解等威胁事件的事件趋势和TOP5事件展示。支持控制台动态显示当前未处理的勒索病毒数量、暴力破解数量、WebShell后门数量及其各自影响的终端数量，支持点击对应的威胁类别，下钻到响应中心对应的威胁事件列表；支持热点安全事件动态更新和展示及全网终端已发生的热点安全事件及其数量；  |
| ★支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、WebShell检测的检测和威胁处置方式、暴力破解的威胁处置方式和Windows系统下信任区文件目录配置； |
| 支持根据统计周期、终端名称、IP地址、脚本命令名称和执行结果查询全网终端脚本执行日志，内容包括：任务名称、任务执行脚本名称、执行类型、执行时间、执行状态和脚本执行日志的导出； |
| 支持设备联动日志按策略来源、设备IP、终端名称、操作类型 (新增、编辑、删除)、封堵方向、封堵IP 、 封堵端口、封堵时长的设备联动日志查询和展示； |
| 支持图形化显示病毒、WebShell事件爆发top5终端，并会显示出该终端未处理的威胁事件数；支持图形化显示暴力破解入侵中最活跃的攻击发起者top10、被攻击最多的主机top10；支持在报表中给用户提供安全规划建设建议。 |
| ★支持本地安装包部署、网页推广部署、上网行为管理系统联动部署、虚拟机模板部署，终端安装部署可根据客户环境选择最优部署方式。 |
| 支持管理平台更新检测、自动下载升级和离线导入升级包升级；支持agent根据升级域的配置自动升级到最新版本； |
| 支持病毒库和引擎组件的更新检测、自动下载升级和离线导入升级包升级；支持全网终端统一病毒库和引擎组件升级。 |
|  威胁检测与响应能力 | ★具备基于多维度轻量级的无特征检测技术，多引擎协同工作，包括：基于AI技术的自研引擎、基于家族基因分析的特征检测引擎、基于虚拟执行和操作系统环境仿真技术的行为引擎、基于大数据分析平台的云查引擎。 |
| 终端Agent软件要求 | 支持极速、均衡、低耗三种扫描模式，以控制扫描时对业务系统CPU资源的占用；终端侧使用全盘文件缓存，加速本地二次扫描速度，减少对本地虚拟化环境的资源消耗；管理平台侧使用全网文件缓存，加速云查杀速度，减少通过互联网进行云查杀的带宽消耗。 |
| 支持通过管理平台下发立即扫描杀毒的任务，可针对某一台终端，也可针对某一组终端进行扫描杀毒；支持错峰扫描，可以设置定时扫描任务，实现终端分批错峰扫描、非业务时段扫描；支持配置跳过一定大小的文件，大小范围支持1M~100M；  |
| 支持展示勒索病毒事件、木马病毒事件、蠕虫病毒事件和其他病毒文件事件及其详情，包括：病毒文件名称，事件等级，受感染的文件，发现时间，检测引擎，文件Hash值，文件大小，文件创建时间。 |
| 支持对zip， rar， jar， cab， 7z等常见压缩文件的查杀，支持压缩文件查杀层级进行策略配置，最大可配置检查10层压缩文件；支持配置跳过一定大小的文件，大小范围支持1M~100M； |
| 支持威胁文件同步处置病毒时，选择是否在其它终端上同步处置。 |
| 支持基于Agent的RDP和SSH登录日志检测的暴力破解入侵检测，支持开启暴力破解实时检测，自动封堵攻击源的IP地址，封停时间支持配置； |
| 支持对暴力破解事件攻击源IP加入黑名单，已加入黑名单的IP无法访问网内所有终端； |
| 支持对指定终端/终端组进行终端基线合规性检查，对不合规的检查项提供设置建议；合规项包括不限于：身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范；支持windows系统永恒之蓝漏洞（MS17-010）的检测；  |
| 具备系统漏洞检测与修复功能，能够帮助管理员进行统一漏洞扫描和补丁分发，识别终端系统漏洞并进行风险修复，加强系统安全性。 |
| 支持配置WebShell定时扫描任务，配置参数包括：扫描周期（每日、每周、每月）、扫描时间精确到分、发现威胁处置方式（自动隔离、仅上报不隔离）；支持配置WebShell实时扫描，一旦发现WebShell文件，自动隔离或仅上报不隔离。 |
| 支持展示终端检测到的WebShell事件及事件详情，支持对WebShell事件的文件进行批量勾选一键隔离、信任和忽略操作； |
| 支持对流量进行过滤，包括未放通流量、已放通流量、业务之间流量、业务内部流量、业务流量、运维流量和其他流量； |
| 支持微隔离功能主界面图形化显示业务系统、服务器及流量详情；流量线详情支持展示该流量线对应的微隔离策略；支持图形化显示服务器间流量关系，包括访问详情、流量趋势等； |
| 支持对业务系统配置微隔离策略规则；支持选择微隔离安全级别，支持高低两种级别；高级别：所有业务都被保护，默认拒绝所有出入站策略；低级别：默认放通策略，所有业务都允许访问，用户可根据实际配置拒绝的访问策略；  |
| 云端联 动 | ★支持基于威胁情报的病毒md5值的全网终端定位搜索，适用于对变种流行病毒的快速响应，快速确认全网终端是否感染； |
| 原厂质保 | ★提供三年质保及病毒库升级 |

**3.2.3应急接管系统**

|  |  |
| --- | --- |
| **指标项** | **主要技术参数** |
| ★总体要求 | 国内知名品牌，拥有自主知识产权，提供计算机软件著作权登记证书，本地设有常驻机构保障后续服务能力。 |
| 管理平台基于WEB GUI全中文管理模式，禁止借用第三方软件整合且非汉化产品。 |
| 产品部署过程不对业务系统产生影响，旁路接入生产网络环境。 |
| 本次建设配置30个容灾授权。 |
| 采用无中心服务器部署，支持节点设备热插拔，全Scale-out架构，无缝横向扩展，可依据性能与容量的需求按需配置、无缝动态节点扩展，满足业务发展弹性需求。 |
| ★硬件要求 | 配置不低于2颗XEON E5-2620处理器。  |
| 2U机架式（12个硬盘槽位），本次配置7块3.5寸6TB 7200RPM/NL-SAS硬盘，1G阵列卡+超级电容；配置384GB用于安装系统及缓存；支持在线扩容，可通过后期在线添加磁盘和扩展磁盘柜的方式，进行备份介质容量的增加。 |
| 内存：配置384GB RAM，最大可扩容1024GB； |
| 配置少于2个千兆网络端口（电口），网络端口都可用且可分配不同的备份任务，提供不少于4个PCI-E扩容槽；冗余电源。 |
| 主动容灾平台要求 |
| 基本要求 | 提供全业务环境容灾功能，包括操作系统状态、应用程序和数据的一体化容灾保护，不接受分别对操作系统、应用、数据进行容灾备份方式。 |
| 针对生产系统逻辑故障，支持同时接管到任意时间点的生产系统快照，并可同时启动多个接管系统用于选择最佳的接管时间点。 |
| 生产系统数据变化实时同步至主动容灾平台，并且主动容灾平台必须实时保存每一次数据变化，预防发生逻辑故障后可将业务系统的整个工作负载恢复到任意时间点。 |
| 保护功能 | 可对业务系统的操作系统、应用、数据进行一体化的CDP保护，对磁盘的读写I/O级操作进行持续记录；当业务系统发生故障或数据丢失后，能够通过持续数据保护功能将业务和数据恢复到故障前的状态。 |
| 传输过程中具备断点续传能力，当传输链路中断或目标端故障时，故障修复完成后，两端可以迅速的完成增量数据的同步。 |
| 平台自身安全性 | 支持统一Web界面同时管理多个容灾节点，保护时可将设备分配到其它容灾节点进行保护，接管时可将故障系统接管到其它容灾接管。 |
| 接管和演练 | 支持跨网段、多网段业务接管 |
| ★主动容灾平台需支持同时保护物理服务器业务、虚拟化平台业务、云平台业务的能力；主动容灾平台同时可支持100个以上生产系统一体化(OS+APP+Data)的容灾保护，无需预先安装操作系统和应用软件。当被保护的多个生产系统故障时，主动容灾平台需支持3-5分钟快速故障系统的接管；针对生产系统的逻辑故障，支持同时接管到任意时间点的生产系统状态，并可在主动容灾平台上同时启动多个接管系统用于选择最佳的接管时间点；支持在主动容灾平台上直接修改接管系统IP地址和MAC地址，无需进入接管系统进行修改； |
| ★支持在完全不影响生产业务和灾备任务的前提下，随时随地进行容灾演练测试；容灾演练测试须操作简单，一键完成所有系统配置部分（系统配置、IP地址、机器名、服务启动状态等）自动化完成，且可同时一键生成和启动多个时间点容灾演练系统；容灾演练系统需与生产系统除硬件外完全一致。 |
| 扩展性 | ★考虑到后续业务架构调整需支持异构迁移功能扩展，扩展简单方便无需重新安装，扩展后需在同一Web界面进行迁移管理和容灾管理；支持将旧服务器或虚拟化平台上整个系统、应用程序和数据一体机化直接迁移至新的服务器或异构虚拟化平台，不需要安装系统、安装配置应用程序和拷贝数据，支持裸机迁移；迁移过程无须旧的生产系统停机，迁移过程变化的生产数据可增量同步到新服务器或异构虚拟化平台，保证数据的一致性。管理界面可查看迁移任务进度以及迁移速度，千兆带宽下迁移速度不低于70MB/s。 |
| 考虑到后续容灾备份体系的完善，需支持对Oracle、MySQL、Ms SQLServer的日志文件连续日志备份扩展，持续监控日志文件的变化情况，即时把新增日志的数据块进行备份，实现对数据库变化数据达到秒级以内的备份保护；需支持固定块、变长块的数据重删技术，在创建重删存储空间时，需要提供变长和固定数据的数据块大小选择； |
| 考虑到后期国产化的需求，主动容灾平台需支持龙芯、飞腾架构下的中标麒麟、银河麒麟等自主可控操作系统。 |
| 管理功能要求 | 支持主动容灾平台自身CPU、内存、硬盘、网络等资源的监控管理；主动容灾平台自带防火墙、安全策略、权限控制、访问控制等安全运维功能；支持三权分立功能；支持在5分钟内未操作自动锁屏功能；  |
| 兼容性 | 支持Windows、Linux、Mac OS、AS400、中标麒麟、银河麒麟等多种操作系统；支持Oracle、SQLserver、Sybase、MySQL、PostgreSQL 、Exchange、Lotus、DB2、MaxDB、SAP、BMDomino、达梦、人大金仓、神通等各类数据库，提供不少于三种数据库互认证书复印件，并加盖原厂公章；支持IIS、Tomcat、Jetty、Apache、JBOSS、WebLogic、WebSphere等各类中间件；支持多种主流虚拟化平台，包括不限于VMware、MS Hyper-V、citri、华为、华三、浪潮、曙光、中兴等虚拟化平台的保护;  |
| 备份策略 | 支持灵活备份策略的定制，包括：全备份、增量备份、合并快照等多种方式，并针对不同的业务系统提供不同的备份策略，要求以上备份策略包含在主动容灾模块中，无需单独购买许可。 |
| 可用性和可靠性 | 支持断点续传、流量控制等有效的广域网数据备份技术，减少网络通信流量，提高数据传输的稳定性和高效性。 |
| ★支持对备份的工作负载(OS+APP+DATA)进行一体化的异机恢复，支持恢复到不同平台（物理环境、虚拟环境或云环境等），恢复过程需通过Web进行管控 |
| ★千兆带宽下备份速度可达60MB/s以上，数据复制最小间隔为秒级，支持秒级、分钟级、小时级同步策略； |
| 服务能力 | ★原厂商必须具有获得工信部容灾备份管理师证书的工程师；提供管理师证书的扫描件或复印件，以保证项目的顺利实施以及后续服务保障。 |
| 产品资质证书 | 原厂商提供投标产品需具有由公安部颁发的《安全产品销售许可证》。 |
| 原厂商提供投标产品需具有中国信息安全认证中心颁发的《中国国家信息安全产品认证证书》。 |
| 原厂商需提供《质量管理体系认证证书》。 |
| 原厂商需提供《环境管理体系认证证书》。 |
| 厂商提供投标产品需具有国家版权局颁发的软件著作权证书。 |
| 原厂商需提供国家密码局颁发的《商用密码产品生产定点单位证书》 |
| 原厂质保 | ★提供三年质保 |

**3.2.4下一代防火墙**

|  |  |
| --- | --- |
| **指标项** | **主要技术参数** |
| 性能配置 | 产品为标准1U机架式设备，需满足多核X86架构。≥4G内存，≥128G SSD硬盘，标配≥8个千兆电口，≥2个千兆光口，并含≥2个高速USB2.0接口，≥1个RJ45串口，性能配置需满足：三层吞吐量≥8G；应用层吞吐量≥1.5G；并发连接数≥2000000；每秒新建连接数≥80000；支持BYPASS |
| 部署及网络特性 | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式，支持链路聚合功能，支持端口联动 |
| 基础功能 | 能够识别应用类型超过1200种，应用识别规则总数超过3000条； |
| 支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能； |
| 支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制； |
| 访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；  |
| 支持配置向导功能，并提供攻击源IP的攻击地图展示；攻击地图需包括攻击时间，攻击源归属地和IP，被攻击者IP，攻击类型和危害等级及当日安全事件统计 |
| DoS攻击防护 | 支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护、支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测； |
| 支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为； |
| 内容安全 | 内置病毒样本数量超过200万；支持应用协议命令级控制，如FTP可细化到rmdir、get、put等命令级控制； 支持压缩文件查杀 |
| ★支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤； |
| 支持采用无特征AI检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于AI技术的病毒检测报告； |
| 入侵防护 | 为了保证入侵防御系统识别的专业性，要求入侵防护漏洞规则特征库数量在7400条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号，参考信息和建议的解决方案； |
| 为了帮助管理员更好的应对一些突发的热点安全事件，要求设备可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； |
| Web应用安全防护 | 具备独立的Web应用防护规则库，Web应用防护规则总数在3500条以上； |
| 支持对web页面黑链进行检测； |
| ★支持对网站的恶意扫描防护和恶意爬虫攻击防护；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等； |
| 支持针对网站的漏洞扫描进行深度防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测，支持基于目录访问频率和敏感文件扫描等恶意扫描行为进行防护； |
| 支持对已经植入webshell后门的服务器持续检测，对后续非法的通信动作进行识别和阻断； |
| 设备需要具备web业务自学习能力，可自行判断与标记业务特征，确认业务模型学习趋势； |
| 僵尸主机检测 | 设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等，特征总数在60万条以上； |
| ★支持蜜罐功能，定位内网感染僵尸网络病毒的真实主机IP地址； |
| 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； |
| 支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址； |
| 安全可视化 | 支持业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别； |
| 支持对检测到的攻击行为按照IP地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息； |
| ★支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险； |
| 支持自动生成综合安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的统计，具备有效攻击行为次数统计和攻击举证； |
| 安全管理中心 | 为了更好的管理多台设备，要求支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能； |
| 支持安全策略一体化配置，通过一条策略既可实现不同安全功能的配置； |
| 支持SD-WAN智能选路功能； |
| 支持高级威胁事件分析，并展示热点事件详情，如全网威胁情报、高级黑客、持续性攻击、网站存在后门（webshell）、黑链、感染流行僵尸网络、大面积病毒感染、外发攻击等，并将高危事件推送到运维管理员手机微信端进行预警； |
| 原厂质保 | ★提供三年包含IPS，僵尸网络，核心软件升级及硬件质保服务 |

**3.2.5 准入控制**

|  |  |
| --- | --- |
| **指标** | **具体功能要求** |
| 部署方式 | 旁路模式 | 支持旁挂方式，部署不影响原有的网络结构 |
| 串接模式 | 支持串接模式，对业务进行强管控 |
| 高可用 | 支持主主模式和主备模式 |
| 网关管理 | 管理界面 | 支持SSL加密WEB方式、SSH命令行方式管理设备； |
| 告警设置 | 系统异常信息，支持邮件、syslog、snmp trap等告警方式通知管理员 |
| 配置备份与恢复 | 1. 支持自动备份配置
2. 支持手动备份和恢复配置
 |
| 实时监控 | 首页可视分析 | 支持首页分析显示接入用户人数、终端类型、行为日志等 |
| 在线用户管理 | 1. 实时显示在线用户数、在线的用户名称等信息
2. 可以对在线用户执行注销、冻结等操作
 |
| 网络行为监控 | 1. 可实时显示用户访问业务等行为
2. 可指定的组、IP、动作等方式进行过滤查
 |
| 终端安全检查 | 终端合规性检查 | 支持 补丁检查、杀毒软件安装检查、操作系统检查、启用文件要求检查、启用注册表项检查、启用软件配置检查、启用软件组配置检查，可设定检查不通过的终端不能接入网络，并给提醒终端客户 |
| 自定义任务计划 | 可以根据需求编写脚本，通过控制台下发执行，扩展实现各种个性化需求 |
| 终端绑定 | 1. 支持用户绑定IP或用户绑定MAC地址
2. 支持IP地址和MAC地址绑定
 |
| 多终端自绑定 | 同一个账号，支持与指定数量的多个终端进行自动绑定； |
| 有端无端可选 | 终端插件是可选组建，如果不做终端安全检查，仅做认证，可以选择不需要安装终端插件 |
| 接入认证 | 二层接入认证 | 1. 支持802.1x认证
2. 支持MAB认证
 |
| 三层接入认证 | 多种认证方式，支持触发式WEB认证，支持用户名密码认证、短信认证、微信认证、二维码认证、单点登录认证、USB-KEY认证等多种认证方式； |
| 本地密码认证 | 支持触发式WEB认证，静态用户名密码认证等； |
| 第三方认证 | 支持LDAP、Radius、POP3、Proxy等第三方认证； 支持ISA\lotus ldap\novel ldap\oracle、sql server、db2、mysql等数据库等第三方认证； |
| IP、MAC认证 | 支持绑定IP认证、绑定MAC认证，及IP/MAC绑定认证等；支持通过SNMP服务器跨三层获取MAC地址；支持绑定IP/MAC后，实现免认证 |
| 短信认证 | 支持短信认证方式，用户输入手机号作为用户名，通过短信猫或短信平台发送验证码；短信认证能够根据不同用户推送不同认证页面，该认证页面可自定义，编辑内容包括文字、颜色风格、图片，且图片支持轮询播放 |
| 微信认证 | 1. 支持与微信结合的认证方式，用户关注微信公众号后即通过身份认证，后台记录用户ID. |
| 二维码认证 | 支持二维码认证，管理员扫描访客的二维码后对其网络访问授权 |
| 新用户认证 | 1、支持认证黑白名单功能，黑名单是名单中用户不能认证，白名单是只有名单中用户才能认证；2、限制某个新用户只能在某个IP段、MAC段范围内登录； |
| 哑终端认证 | 支持哑终端通过MAC认证的方式接入网络 |
| 单点登录认证 | 支持radius、PPPOE、AD、POP3、Proxy、web等认证单点登录，简化用户操作； |
| 用户管理 | 账户有效期 | 指定账户支持有效期限制，并支持自动过期；支持自动删除长期不登录账号信息；  |
| ★用户属性 | 1、用户可以添加自定义属性，可以基于属性配置控制策略和审计策略 |
| 用户密码强度 | 可设置密码必须包括数字或字母或特殊字符；  |
| ★可做为统一认证中心，对外开放接口 | 1. 可对接多种系统，如HR、AD域等同步用户源；
2. 提供API接口将用户信息对接给第三方设备；
3. 提供LADP接口将用户信息对接给第三方设备；
 |
| 特权DKey | 支持针对特权用户配置免认证key、免审计key、免控制key |
| 跨三层取mac | 1. 支持通过SNMP跨三层取MAC地址

支持通过镜像数据包的方式跨三层取MAC地址 |
| web访问审计 | 必须能审计URL信息；必须支持只记录含有指定关键字的网页正文内容 |
| 邮件审计 | 1. 支持审计用户Email邮件的正文及附件
 |
| 终端访问审计 | web访问日志 | 支持查询和导出web访问的行为日志 |
| 日志中心 | 设备必须支持内置数据中心和独立数据中心 |
| 日志审查Key | 必须支持以USB-Key方式验证接入数据中心的管理员身份； |
| 日志中心 | 终端接入日志 | 支持查询和导出终端安全日志、登录注销日志等行为日志 |
| 用户行为分析 | 支持多维度统计分析用户访问业务行为，并支持下钻查询 |
| 终端接入分析 | 用户活跃天数排行、接入用户数趋势分析 |
| 非法外联管控 | 防非法外联 | 提供IP白名单和黑名单配置，终端只能访问与白名单的资源，严格禁止非法外联。 |
| 支持WIFI、4G无线上网卡外联管控：配置策略后，通过wifi、4G无线上网卡，只能访问指定的网段通信，禁止访问互联网； |
| 支持定时检测非法外联行为，可进行更多处置选择，如重启、关机、断网、隔离等控制操作，违规断网后，重启PC可恢复网络连接； |
| 外联检查外联控制 | 支持终端安全-检查规则，新增外联检查规则及控制规则； |
| 支持拨号行为、双网卡行为、有4G网卡、有无线网卡行为、连接非法wifi行为、使用非法网关行为、连接外网行为、自定义外联行为，8种外联方式的检查；  |
| 检查到非法外联行为后，支持发送告警邮件、断网的违规处理配置；  |
| 支持”只能访问以下地址”和“不能访问以下地址”的配置；  |
| 告警事件 | 告警事件中增加违规外联告警选项，用于对违规外联行为使用进行预警 |
| 外设管控 | 1、支持阻断终端用户使用外设，防止终端用户从内网拷贝信息；2、支持控制用户通过USB接口产生外联行为，便于在内网进行强管控，减少上报外联行为几率3、支持允许用户使用某种符合规定的外设；4、支持填写硬件ID白名单，并提供方法告诉管理员如何获取外设的ID; 5、支持外设类型：存储设备、网络设备、蓝牙设备、摄像头、打印机 |
| U盘或移动硬盘管控/审计 | 支持U盘管控功能：U盘可配置告警/可读/可读写/拒绝 4种管控类型；支持拷贝/修改/移动的文件内容以及插入和拔出行为的审计 |
| 日志中心多产品联动 | 支持与防火墙联动 | 能够与同品牌下一代防火墙系统实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录； |
| 支持与同品牌端点安全检测产品联动 | 能够与同品牌EDR产品实现联动，当检测到终端未安装EDR产品时，禁止上网并提示需要安装EDR终端软件；当发现终端威胁时，联动EDR进行查杀和隔离 |
| Ip管理 | IP管理 | 支持IP管理功能，管理员可以查看每个IP的详细使用情况，支持查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量； |
| 资产管理 | 自动发现和识别 | 1、自动发现网络里面的终端，如IP、Mac、厂商、操作系统、开放服务、开放端口等信息 |
| 资产管理展示 | 1、对网络接入的终端进行可视化和管理，展示终端详细信息、异常状态等；2、支持查看终端类型、类型分布以及终端详细信息（厂商，系统，端口等）； |
| 原厂质保 | ★提供三年软件升级及硬件质保服务 |

# 建设周期、付款、保修要求

要求合同签订收到首款后即马上施工，要求在3个月内完工。

要求整个系统保修三年及以上。

付款方式为分期付款，合同签订后付合同价格的30%，验收合格后付合同价格的65%，保修期结束后付合同价格的5%。