**武义县人民检察院机房改造二期（等级保护）项目**

**一、采购设备（服务）清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **品牌型号** | **技术描述** | **单位** | **数量** |
| 1 | 等保一体机 | 深信服 SDSec-1000-A600主机 | 硬件平台：配置E5-2620 V4\*2，96G内存，128G\*1 SSD系统盘，240G\*1 SSD缓存盘，4T\*2数据盘，6个千兆电口。底层平台架构采用超融合虚拟化技术，支持安全组件按需扩展、故障自动迁移以及多副本机制保障数据安全性和设备稳定性。  **详见技术规格要求。** | 台 | 1 |
| 2 | 深信服SD-AF-200虚拟化下一代防火墙 | 虚拟化下一代防火墙：包含NAT地址转换、ACL、漏洞防护、web网站防护、网页防篡改、IPS防护、APT攻击防护等，提供三年软硬件质保和特征库升级。本次提供应用层200M吞吐量授权。  **详见技术规格要求。** | 套 | 1 |
| 3 | 深信服LAS-1000-V20虚拟化日志审计系统 | 虚拟化日志审计系统：含20个接入设备许可；10G/天日志处理能力；0.8T数据存储空间；包含日志分析系统全功能模块（日志的采集、过滤、归并、关联分析、展现、告警监控、实施事件监控、报表等）。  **详见技术规格要求。** | 套 | 1 |
| 4 | 防毒墙 | 瑞星RSW1300 | 网络接口：10/100/1000BASE-T接口：6个（支持2对Bypass接口）；吞吐量≥3Gbps；并发连接数≥650000；新增连接数≥16000个/秒；HTTP杀毒吞吐≥250Mbps；FTP杀毒吞吐 ≥100Mbps；SMTP杀毒吞吐≥100Mbps；POP3杀毒吞吐≥100Mbps；支持用户数≥100；  **详见技术规格要求。** | 台 | 1 |
| 5 | 上网行为管理 | 深信服AC-1000-C400 | 标准1U设备，支持带宽管理100M，支持用户数600人，支持上网行为管理、流量控制、用户认证、上网审计等功能，提供3年URL/应用规则库升级和软硬件质保。  **详见技术规格要求。** | 台 | 1 |
| 6 | 天擎数据管理 | 360安全U盘 | 能够通过本单位已在使用的天擎安全管理平台统一管理。  在天擎管理范围内，控制终端对安全U盘的读写权限。在管理范围外，控制外部终端对安全U盘的读写权限。并且记录和上报U盘使用过程中的读写行为至天擎服务器端。  **详见技术规格要求。** | 套 | 1 |
| 7 | 网站源码检测及加固 | 婺安网站源码检测及加固 | **缺陷检测：**  支持C、C++、C#、Java、PHP、JSP、Python等主流编程语言开发的软件源代码的检测。  支持缓冲区溢出、代码注入、跨站脚本、输入验证、API误用、密码管理、配置错误、危险函数等13个大类，600多个小类的缺陷检测。  兼容CWE、OWASP Top 10、CWE/SANS TOP25等国际主流缺陷和漏洞列表的检测。  **合规检测：**  支持CERT C/C++/Java安全编码标准、MISRA C/C++、ISO/IEC TR 24772等国际标准和规范的源代码合规检测。  提供方便的可扩展接口，针对组织和行业特有的代码规范，定制开发自动化检测规则，满足个性化需求。  **溯源检测：**  检测软件中是否引用了开源代码模块。  引用的开源代码模块存在哪些安全漏洞。 | 项 | 1 |
| 8 | 等保测评 |  | 办公网网站及OA两个系统二级等保评测 | 项 | 2 |
| **合计** |  |  | **总预算41万元** |  |  |
| **★商务要求** | **1、特别说明：为保证及时售后，仅限金华地区供应商报价，并只接受用户指定的品牌型号及参数，本项目提供的设备必须是原包装未拆封的全新设备。**  **2、设备技术规格要求中需提供的质保函、资质证书、功能截图等，必须于中标后签订合同前提供相关原厂盖章资料，不提供或者提供的资料不符合要求，作废标处理。**  **3、因为业务需要，报价结束后3日内必须签订合同，签订合同后5日内供货并完成安装调试（本项目所需的一切辅材配件费用包含在总价中，不作追加和另外支付）。** | | | | |

**二、具体技术规格要求**

**1、等保一体机**

|  |  |
| --- | --- |
| **项目** | **技术规格要求** |
| 硬件指标 | 6个千兆电口，CPU E5-2620 V4\*2，内存96G，硬盘128G SSD系统盘、240G SSD缓存盘、2\*4T SATA数据盘 |
| 产品形态 | 支持部署于通用X86服务器平台，无需绑定底层操作系统即可搭建  平台支持旁路引流及网关模式部署 |
| 基本要求 | 平台可扩展下一代防火墙、SSL VPN、上网行为管理、数据库审计、运维审计、日志审计、主机杀毒等安全功能组件。 |
| ★平台支持用户进行安全拓扑的编排，可根据实际业务环境定义业务安全区域，简化运维管理；（提供界面截图证明） |
| ★平台具备业务风险可视化界面，包括业务风险状况、风险事件状态及整体安全态势等，针对单独业务系统可提供业务风险提供业务状态及业务风险分析评估（提供界面截图证明） |
| 平台支持关键安全组件双机功能，保障安全组件高可用； |
| 下一代防火墙功能要求 | 对虚拟防火墙分布式策略管控，策略内容可以针对IP、MAC地址或通讯端口，可防护所有基于IP五元组（TCP、 UDP、 ICMP 等）； |
| 支持静态路由，ECMP等价路由，支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议，支持多播路由协议，支持路由异常告警功能； |
| 提供基本的安全防御，包括但不限于4-7层访问控制、入侵防御、病毒过滤、网页防篡改等安全功能； |
| 对所有应用系统进行漏洞的攻击防护，包括防跨站、防SQL注入、防篡改、防木马、防黑客攻击等。 |
| 支持根据国家/地区来进行地域访问控制； |
| 支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞；（提供界面截图证明） |
| 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；（提供界面截图证明） |
| 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；（提供界面截图证明） |
| 日志审计 | 内置20个主机审计许可证书 |
| 支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、Glftpd、Serv-u]； |
| 支持SNMP日志采集，支持日志类型：网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神] |
| 支持Opsec Lea日志采集；（提供产品页面截图证明） |
| 支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览、论坛微博]、入侵检测、业务检测、流量监控 |
| 支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储；（提供产品页面截图证明） |
| 支持文本型日志原始文件管理，可将系统作为日志服务器使用；（提供产品页面截图证明） |
| 支持按日志属性、日志类型、时间范围进行数据备份；（提供产品页面截图证明）  支持WEB界面备份及日志恢复导入工作；支持自动与手动两种备份归档方式；  系统支持以FTP上传方式将归档文件存储到第三方存储系统中；（提供产品页面截图证明） |
| 支持自定义配置实时监控的日志类型； |
| 支持自定义审计报告； |
| 支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索；（提供产品页面截图证明） |
| 审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明；（提供产品页面截图证明）  支持日志类型、IP地址权限设置；支持页面功能模块权限设置； |
| 系统内置多种类报表模板； |
| 系统内置安全防火墙；支持控制访问审计主机范围； |
| 支持内置归并策略，对HTTP数据进行自动归并处理；（提供产品页面截图证明） |
| 资质要求 | 提供《计算机信息系统安全专用产品销售许可证》，提供复印件并加盖厂商公章； |
| ★所投厂商为国家信息安全漏洞共享平台CNVD用户组成员，提供CNVD官网截图证明并加盖厂商公章； |
| ★所投厂商具备云安全成熟度成熟度模型CSA-CMMI 5认证，提供证书复印件并加盖厂商公章； |

**2、防毒墙**

|  |  |
| --- | --- |
| **项目** | **技术规格要求** |
| 硬件参数 | 产品类型:硬件, 产品必须为国有品牌，必须专业反病毒厂商产品，拥有自主知识产权；  产品构架:X86平台，具有多重病毒过滤技术、虚拟化病毒分析技术等应用基础；  多出口:要求支持多路链路出口；  接口参数:可以灵活定义接口属性，是WAN、LAN或DMZ；  硬件平台：要求双路多核专业网安硬件平台，保障设备处理性能  网络接口：10/100/1000BASE-T接口：6个（支持2对Bypass接口）；  平均无故障间隔时间≥50000小时。 |
| 性能参数 | 吞吐量≥3Gbps；  并发连接数≥650000；  新增连接数≥16000个/秒；  HTTP杀毒吞吐≥250Mbps；  FTP杀毒吞吐 ≥100Mbps；  SMTP杀毒吞吐≥100Mbps；  POP3杀毒吞吐≥100Mbps；  支持用户数≥100； |
| ★统一管理 | 多级部署：要求具备多级中心管理系统，可对网络中所有的防毒墙设备统一管理（提供功能截图）。 |
| 系统功能 | 产品成熟度：要求产品采用国内领先的检测过滤技术，并具有专门的安全操作系统；  部署模式：要求支持透明模式、路由模式、混合模式；透明模式支持多路透明网桥；接口要求支持PPPoE拨号模式、DHCP模式等接入方式；  管理方式：要求支持HTTPS、SSH、console方式；  帐户管理：要求支持指定管理员管理设备（绑定IP）；支持管理员账户超时、锁定等安全保护；  备份与恢复：要求对系统配置进行备份，恢复备份配置、恢复系统默认值。 |
| 病毒过滤技术 | 病毒监测能力：要求具有针对国内及全球病毒监测网络，具备新病毒及时发现、处置能力及专业技术资源，保障对新病毒的有效拦截及具备先进的病毒分析技术实力；  杀毒引擎：要求具有国内独立自主产权杀毒引擎，专业的网关病毒过滤引擎，保障防毒墙在网关过滤病毒的效率及性能；  数据并行处理技术：要求具有并行数据处理分析技术，可以完成多链路、高流量环境的病毒过滤；  病毒库特征码：要求具有针对国内用户的病毒库，病毒库特征码≥200万；  ★支持协议及多端口过滤技术：要求支持SMTP、POP3、FTP、HTTP和IMAP协议的病毒过滤，且可对SMTP、POP3、FTP、HTTP、IMAP协议通过不同端口传输的数据同时具有病毒过滤功能(提供功能截图)；  ★区域双向病毒过滤及病毒处理策略(提供功能截图并加盖原厂公章)：要求支持不同区域间双向查毒；例：WAN-LAN及LAN-WAN双向查毒，且要求可灵活定义病毒处理策略，例：查毒或杀毒阻断；  ★扩展病毒分析过滤技术：要求支持对恶意脚本、DOS可执行文件、恶意网页分析、图片格式病毒查杀;要求必须支持虚拟化病毒分析等脱壳技术，对加壳病毒具备识别及阻断能力、要求拥有对未知病毒识别及阻断能力(提供功能截图)；  ★病毒过滤策略（提供功能截图）：要求支持多层压缩文件中的病毒过滤，可定制压缩层数；要求可定制禁止文件传输类型；要求支持对病毒文件进行隔离。  病毒过滤白名单：要求支持定义HTTP协议网址白名单，对访问网址不进行病毒过滤；要求支持定义邮件地址或邮件域白名单，对特定邮件地址或域不进行病毒过滤。  恶意网站拦截：要求恶意网站URL数量≥1800万  恶意网站采集系统：具备恶意网站自动采集、分析、跟踪系统，具有云安全技术，维护恶意网站采集系统的有效性；要求拥有针对国内用户的恶意网站收集体系，国内云体系用户≥7800万。  ★安全联动：要求支持与企业版杀毒软件联动，检测终端是否安装杀毒软件、开启监控、病毒库升级到最新版本、是否存在高危系统漏洞等安全风险，可对存在安全风险终端采取阻断访问的措施，并可以发送告警给管理员（提供功能截图）；  病毒库升级：要求支持在线自动、手动方式升级，局域网升级；要求在国内有自主的分布式病毒库升级服务器，保障防毒墙设备病毒库升级的可持续性。  ★Web过滤技术（提供功能截图）：要求可定制禁用下级HTTP代理；要求可定制禁止运行Java、Java Applet、Active控件；要求可定制启用内部SQL注入防护。  ★URL攻击防御： 要求支持URL攻击防御，可定义阻断时间及攻击标准（提供功能截图）；  入侵防御：支持WEB\FTP\MAIL\数据库入侵防御，对利用重大漏洞入侵的行为可以阻断；支持Windows等重要漏洞的入侵防御。  自定义入侵防御特征：支持自定义防御特征码，对指定入侵行为实施防御。 |
| 防火墙功能 | 访问控制：要求支持基于对象组、服务组、时间组的访问控制策略，灵活控制访问；  地址转换：要求支持基于接口的NAT、SNAT、DNAT；  URL过滤：要求支持对URL过滤；用户可自行定义过滤URL、域名或文件类型；  流量控制：支持流量控制和带宽管理。 |
| 日志管理 | 日志管理：要求提供系统日志、病毒日志、隔离日志、管理日志、网络日志等；  日志报表：要求对详细病毒日志查询及日志统计，并支持日、周、月日志志报表功能，可发送日志信息给管理员；  远程日志：要求支持SYSLOG、MYSQL远程日志服务。 |
| 资质 | 产品资质：具有公安部安全产品销售许可证书；具有计算机软件著作权登记证书。  厂商资质：具有软件企业认定证书；  ★具有与信息安全领域反病毒、安全防范软件设计开发和技术支持服务相关对信息安全管理活动的信息安全管理体系认证证书（加盖原厂公章）；  ★具有信息安全领域杀毒、安全防范等软件系统的设计开发和服务的质量管理体系认证证书（加盖原厂公章）。  ★保修：三年原厂保修与服务，合同签订时提供原厂商针对本项目的三年保修服务承诺函原件（加盖原厂公章） |

**3、上网行为管理**

|  |  |
| --- | --- |
| **项目** | **技术规格要求** |
| 吞吐量 | ≥200Mbps |
| 用户规模 | ≥600人 |
| 设备接口 | 4个千兆电口 |
| 硬盘 | ≥128G SSD |
| 尺寸要求 | 标准1U架构 |
| BYPASS | 支持 |
| 设备架构 | 设备必须为多核X86架构，以保证软件库的灵活更新与升级。 |
| 部署方式 | 要求设备支持网关模式，支持NAT、路由转发、DHCP、GRE、OSPF等功能；支持网桥模式，以透明方式串接在网络中；支持两台及两台以上设备同时做主机的部署模式，支持基于虚拟化平台的软件版本，支持的虚拟平台包括：VMware、深信服虚拟化等。 |
| IPv6支持 | 支持部署在IPv6环境中，其所有功能（认证、应用控制、内容审计、报表等）都支持IPv6（提供产品界面截图） |
| IPSEC VPN功能 | 要求设备支持IPSEC VPN远程安全接入维护，能提供IPsec VPN客户端授权远程接入访问； |
| 链路负载 | 为了提高出口多链路利用率，要求支持支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载。支持使用VPN做专线备份，支持链路故障检测；（提供产品配置界面截图） |
| 业务需要 | 为减少短信费用投入，要求设备支持微信身份验证，用户可以通过微信“扫一扫”、关注公众号等操作获取上网权限，后台能够记录下用户微信的ID，支持与第三方微信平台对接，无需修改第三方平台代码 |
| 为满足访客PC的简易接入授权，访客终端接入无线网络后，终端自动弹出二维码页面，审核人通过手机扫描访客终端二维码，添加备注信息，访客即可完成上网，同时设备记录访客备注信息、接入终端MAC以及审核人帐号。（提供产品配置界面截图） |
| 支持认证页面分权分域管理。启用后，普通管理员只能看到自己有权限的页面，其他管理员页面不可见。 系统管理员可以将某个页面授权给指定的普通管理员管理。 |
| 为加强对我单位员工私接无线上网的行为管理，要求设备能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，匹配管理员配置的热点信任列表，对信任列表外非法接入的热点和终端能够进行阻止上网，支持冻结用户IP，并通过邮件形式告警通知管理员，支持显示以IP或用户名的维度统计一段时间内的趋势图。（提供产品配置界面截图） |
| 为确保我单位不会通过SSL加密内容发生通过互联网出口泄密事件，要求设备必须能够识别并过滤SSL加密的钓鱼网站、金融购物网站；识别和审计加密的邮箱（如GMAIL）等（必须具备自主知识产权证明）； |
| ★针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向web访问质量检测（提供产品配置界面截图） |
| 应用识别规则库 | 目前互联网应用种类较多，为了降低管理员配置应用管理策略的难度，要求设备能够按照管控需求对应用进行标签化管理，应用标签至少默认包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类，此外可根据我单位需求自定义标签，根据标签做应用控制。（提供产品配置界面截图） |
| 应用控制 | 1. 设备内置应用识别规则库，支持超过4700条应用规则数，支持超过2100种以上的应用，660种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率； 2. 支持根据应用的特征智能识别新更新的应用； 3. 支持根据IP、端口、协议等自定义应用规则；   支持根据不同的应用类型或具体的某种应用设置允许或拒绝； |
| 移动应用的细分控制 | 支持对移动应用的细分权限控制，微信：微信网页版、微信传文件、微信朋友圈、微信游戏。移动QQ：QQ传文件、QQ视频语音等。 |
| URL访问及关键字控制 | 要求设备内置海量的URL地址库，可根据访问URL的网页关键字进行过滤控制，特别对于SSL加密的网页、论坛、BBS上的发帖行为也需要支持关键字过滤控制 |
| 流控黑名单 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（提供产品配置界面截图）。 |
| 上网流速提醒 | 用户指定应用上网流速超过预设阈值后，网关自动提醒该用户； |
| 动态流控 | 要求设备可以针对整体线路或者某流量通道内流量情况进行实时监控，根据设定的流量空闲值自动的调整流控控制策略，提升我单位带宽使用率（提供产品配置界面证明） |
| P2P智能流控 | 要求设备有效抑制如迅雷、ppstream等P2P应用带宽，通过抑制可看到出口上下行带宽的明显改善。 |
| 多维度权限控制 | 要求设备可以根据员工的所在位置以及所使用终端配置不同的上网策略和流控策略，做到更精细化权限管理。 |
| 移动APP审计 | 支持常见论坛（天涯社区、猫扑社区、百度贴吧、新浪论坛、搜狐社区等  ）、微博（新浪）、新闻评论类（腾讯新闻、网易新闻、搜狐新闻、新浪新闻）的移动APP内容审计 |
| IM审计 | 支持对QQ（客户端版本）、阿里旺旺、万德（Wind）、路透等应用的聊天，群聊天等内容的审计。 |
| 邮件审计 | 支持对加密HTTPS、SMTP-SSL、SMTP-TLS、SMTP、Gmail、闪电邮客户端的邮件进行关键字过滤 |
| ★加密证书自动分发 | 审计SSL网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台PC单独安装证书的问题（要求提供产品界面截图） |
| 关键字订阅 | 支持预置几组关键字，当审计日志中出现这些关键字时，将定期以邮件的方式发送报告给指定邮箱（提供产品界面截图） |
| 网络整体状况报表 | 从带宽健康分析、工作效率分析、离职风险分析、合规性分析四个大块对网络整体状况进行说明 |
| 下钻查询 | 在流量时长分析、用户行为分析、终端接入分析等纬度相关页面支持对统计结果的向下钻取查询 |
| 病毒查杀 | 设备必须内置业界知名杀毒引擎（提供界面证明）；  必须能查杀网页、Email、FTP等流量中的病毒；  支持能查杀RAR，Gzip等压缩包中的病毒； |
| 特权用户 | 支持针对特权用户配置免认证key、免控制key |
| 数据中心 | 要求设备必须支持将审计数据备份到外置数据中心，实现海量存储；必须支持通过USBKEY方式对数据中心管理员进行身份验证，确保我单位核心数据不会外泄 |
| ★数据中心行为感知扩展 | 支持外置数据中心扩展行为感知系统，包含全网上网态势感知、办公上网态势感知、沉迷网络态势感知、敏感事件感知等（提供产品界面截图证明） |
| 投标产品资质要求 | 公安部公共信息网络安全监察局《计算机信息系统安全专用产品销售许可证》 |
| ★中国信息安全认证中心ISCCC《IT产品信息安全产品认证证书》 |
| 具有工信部颁发的《电信设备进网许可证》 |
| IPv6 Ready Phase-2认证 |
| 公司研发体系通过国际认证CMMI5 |

**4、天擎数据管理**

|  |  |  |
| --- | --- | --- |
| **项目** | | **技术规格要求** |
| 环境要求 | 控制中心安装环境要求 | 操作系统：Windows Server 2008 R2 64位 |
| CPU：Intel i3处理器以上 |
| 内存：不低于4GB |
| 硬盘：不低于100GB，建议200G以上（需要下载补丁文件存放） |
| 支持在虚拟机上安装控制中心 |
| Windows客户端安装环境要求 | 操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10 |
| 系统管理 | ★集中管理 | 能够通过本单位已在使用的天擎安全管理平台统一管理，对存储介质进行注册、注销、挂失、权限控制、日志审计 |
| 分组管理 | 在内网中，支持控制不同分组U盘在不同分组终端的读写权限；在外网中，支持控制不同分组U盘在外网的读写权限 |
| 移动存储管理功能 | 设备注册 | 支持根据介质的使用对象进行设定编号、名称及责任人等条件按不同使用要求进行注册，如选择设备类型、是否允许外出使用等，支持对已注册的移动介质进行管理，包括授权、启用、停用、删除、取消注册和筛选、导出设备清单等 |
| 支持对已注册的移动介质进行密码重置操作 |
| 可建立设备分组来对注册的移动介质进行统一的管理 |
| 支持同ID下的移动存储介质相互通用，不同ID下的则禁止使用 |
| 对已注册并丢失的移动介质进行管理，支持禁用丢失的移动存储介质继续在内网使用；当移动存储介质找回时，可在相应模块设置，即可重新恢复使用 |
| 支持按照设备的使用责任人及设备类型等信息，设定外出的责任人、使用原因、权限及有效期等策略 |
| 查看终端发起的使用申请和密码重置申请，并对所申请的内容进行审批 |
| 设备授权 | 产品接入系统，在身份认证之前，用户数据区属于禁止访问状态，受安全芯片全面保护 |
| 产品接入系统，在身份认证之后，对产品用户数据区的访问，需要通过调用安全芯片接口 |
| 支持“组授权”以及“计算机例外授权”，且支持只读、读写、禁用的分级授权，可查看指定组或计算机的可用设备数量，便于进行日常的统计与维护工作 |
| 支持对于未授权设备的使用权限管理，且支持只读、读写、禁用的分级授权 |
| 支持设备插入提示的设置，可根据不同授权的设备进行不同的提示设置 |
| 客户端管理 | 支持客户端安全U盘登录，设置密码，修改密码，拷入烤出文件，日志查看等操作. |
| 安全U盘 | 防止未授权访问与篡改 | 产品的启动区属于只读状态，可防止攻击者进行篡改；在身份认证之前不能访问数据区密文；在身份认证过程中，存在口令尝试次数限制，可有效防止暴力破解。口令认证过程受安全芯片保护 |
| 防止第三方访问与篡改 | 在身份认证之后，对360安全U盘用户数据区的访问，需要通过调用安全芯片接口。接口会对访问的进程进行合法性校验，第三方进程无法成功通过校验，从而阻止第三方的访问与篡改。 |
| 数据秘钥安全 | 在身份认证之前无法访问数据区密文，无法获取数据明文密文的配对；加密方法无法被第三方程序调试，密钥的生成和维护机制受安全芯片保护 |
| 文件系统安全 | 安全U盘自身产品采用私有的文件系统，需要通过私有文件系统接口，对文件进行读、写、访问。防止病毒木马主动传播。 |
| 固件指令加密 | 安全U盘底层通讯指令经过加密处理，防止通过USB总线嗅探工具获取关键指令，防止“指令重放攻击”。 |
| 高强度日志记录 | 日志记录不受网络限制，脱离内网仍可进行操作审计。 |
| 高强度读写权限控制 | 读写权限通过安全芯片统一管理。内、外往读写权限内置在U盘中，安全U盘可以区分内、外网环境控制读写权限，可以通过天擎配置内、外网读写权限。 |
| 商密安全资质 | 公司有“商用密码产品定点生产单位”资质。 |
| 日志报表 | U盘使用日志 | 记录安全U盘的文件操作时间，登录账号，操作记录，使用U盘的计算机名，源文件路径，目标文件等信息 |
| 日志抓取不受内外网限制，会如实抓取用户的操作行为 |
| 日志存储受安全芯片保护，防止篡改 |

**备注：★为必须满足项，不满足做废标处理。**