总体要求：

1、采用C/S与B/S相结合方式。

2、支持Vmware、Citrix 、KVM以及国产任意虚拟化厂商。

3、支持本地和虚拟化环境下对数据防泄密以及桌面安全管理，并支持虚拟环境下的OA、ERP、PLM、PDM、数据库、邮件、教务、FTP等业务系统的业务数据在线编辑及下载/导出加密保护。

4、服务端操作系统支持微软32或64位的windows2012/windows2008/windows2003操作系统。

5、用户端操作系统支持微软32或64位的windows10/windows8/windows7/windowsXP，linux系统。

6、支持多服务器集群，支持多数据库集群；

7、双机热备：系统要求支持双机热备份，能够在服务器故障时，实现自动切换。

数据管理要求：

1、支持当终端用户从业务系统上获取商密信息时，获取到本地的商密信息将自动加密，加密过程在后台自动完成，对用户透明；解密控制：当终端用户将本地商密信息提交到业务系统(如OA、教务系统、FTP等、存储系统)上时，如果商密信息是加密的，解密过程在后台自动完成，对用户透明；终端用户在访问受保护的业务系统时，以标签和红框的方式提醒用户进入受保护状态；终端用户访问业务系统或者从后端业务系统（如教务系统、FTP、存储系统等）调用数据时，记录详细的操作日志并上传到本系统的服务器上，以备数据的追踪审计；终端用户在从业务系统上取文档到本地，或者在线阅读文档时，记录用户操作文档详细的行为，并将日志上传到本系统的服务器上，以备数据的追踪审计；存储控制：支持控制终端用户访问商密数据，包括如下三种方式：限制其只能在线访问数据；禁止将数据存储到本地；限制其只能将数据保存到安全存储箱；屏幕水印控制：终端用户在访问业务系统商密数据的过程中，可显示屏幕水印。屏幕水印的内容、字体、颜色可由企业配置，支持用户、时间、IP地址、MAC地址、计算机名的显示。当用户通过拍照等恶意行为窃取数据时，屏幕水印也会同时被摄取；终端用户在访问商密数据时，禁止通过块拷贝、拖拽等方式将商密数据转存到非商密文档中；截录屏控制：终端用户在访问商密数据时，禁止通过截屏键、截屏软件、录屏软件以及带有截录屏功能的软件，将商密数据转存到非商密文档中；安全存储箱：终端用户可以将商密数据存储到安全存储箱中，存储到安全存储箱的文档与外部环境完全分离，只有授权进程才能访问，且安全存储箱中的文档被移动到外部环境中时，将强制加密；通用设置：当文件落到本地成为加密文件时，相关功能及策略配置应完全覆盖安全文档管理所有项。

2、支持驱动层透明加解密，可通过应用层进程区分应用程序，确保不影响用户使用习惯；支持大型应用软件父子进程自动识别，在添加进程时仅需要添加一个主进程，子进程自动应用主进程加密策略，防止由于进程添加不全导致应用软件无法使用，甚至破换文件的可能，支持对某些非可编辑类的文件（如音频、视频、PDF等）打开即加密；支持对加密文件本身可赋予打印权限，打印权限分为真实打印、虚拟打印；支持进程指纹签名，防止进程伪冒，确保合法进程才能打开加密文件；加密驱动在微软Kernel级，采用双缓存机制，加密文件过加密驱动文件，非加密文件过微软文件缓存；加密技术与文件类型与应用程序种类无关。

3、支持客户端离线（虚拟环境除外）后在指定周期内（固定时间：4月5号之内；动态时间：每天的几点到几点）可以正常使用加密文件，但对操作文件权限有限制（支持可复选，包括完全不能用；只读，不能修改，禁止另存；禁止打印、禁止自解密加密文件），支持离线策略延时启用，延时时间设置后，客户端离线在指定的时间内继续使用离线策略，客户端超时后离线策略自动生效，无论此时是否插网线，支持离线策略漫游修改，当用户需要延长加密文件使用时间，通过验证码或者授权文件修改离线时长及策略。

4、支持根据统一策略，使用户端生成的文件自动带密级，不同密级的用户操作同一个文件的权限不一样；支持加密和非加密模式的转换，非加密模式不能打开密文文件，加密模式下打开非加密模式下产生的明文文件后加密；对文件打开周期、打开范围、是否有修改权限、是否能打印、打印水印、拷贝拖拽、截屏控制、等方面进行控制。

5、支持对文件外发给第三方后的打开口令、打开范围、打开次数、操作时长、修改权限、打印权限、水印等权限做控制；支持Web平台审批，流程可自定义，支持多级流程；支持对用户管理、使用系统的活动，如用户、角色的添加、删除，外发文件的申请、审批、制作，系统均记录日志。以便于以后审计与追踪；文件打开支持多因子认证，如密码、动态口令、绑定key等；支持对一个或多个目录进行授权。

6、支持内部已加密文件可带回家办公，即可以将加密文件放在授权U盘里，该授权U盘可带回家并插入到无客户端的电脑上并在授权U盘里打开加密文件，并对此文件具有权限控制，包含文档类型、使用时间、打印控制、打印水印、以及口令保护等。

桌面安全管理要求：

1、支持对http网站访问进行黑白名单控制，例如只允许访问百度，而不允许访问谷歌，并支持添加时间策略、同步客户端离线策略； 支持对webmail的黑白名单控制，支持对SMTP邮件，如foxmail、outlook等的控制，控制策略可选项有自由和禁止发送，支持过滤邮件关键字，并记录邮件内容，支持添加邮件收发时间策略、同步客户端离线策略；支持对FTP的应用控制，支持自由与禁止两种策略选择，并对FTP地址进行黑白名单控制，支持记录FTP文件内容、添加时间策略、同步客户端离线策略；支持对如QQ、MSN等及时通讯工具控制，如禁止发送文件、过滤聊天关键字等，并支持添加时间策略、同步客户端离线策略；支持对网络进程进行控制，如禁止P2P类（迅雷、BT下载软件）的使用；支持监控网络流量（实时\总体下载流量、实时总体上传流量），对下载\上传流量达到多少KB时，进行报警或者自动断网，支持同步客户端离线策略；支持对TCP\UDP 0—65535端口的黑白名单控制，ICMP协议控制，并支持添加时间策略、同步客户端离线策略。

2、支持对全网使用的移动存储介质做统一管理，禁止未经过注册的移动存储设备在内网中使用，实现移动介质的接入；对移动存储设备进行安全级别划分，级别不同或者级别较低，不能正常的访问移动存储设备；支持对移动存储数据的使用次数和使用时间进行控制，超过使用次数后，或者超过使用期限，可以限制移动设备的读写以及是否允许使用；可对用户使用授权的移动存储介质进行审计，对该移动存储介质从购买到销毁整个生命周期进行追踪。

3、支持对可移动介质进行：自由使用、禁止使用、只读使用、拷入明文文件直接加密的权限控制(提供截图)；支持对拷入内容进行文件名称审计和文件实际内容审计（提供截图）。

4、可对本地打印机、虚拟打印机、共享打印机及网络打印机进行管理，打印管理策略支持禁止使用、允许使用并记录打印日志。打印日志至少包括打印用户、打印文件名称、打印文件内容、打印文件页数、打印机信息等；在用户违规打印机时，系统可记录违规打印操作日志；可指定用户使用指定的网络打印机进行打印，并支持水印打印输出；可区分实体打印机和虚拟打印机进行控制，可以指定只有某进程可以打印。

5、支持对当前主流防病毒软件（至少20种）进行监控，监视防病毒软件的安装情况、运行状态和病毒库版本；对不符合安全策略的状态进行报警；支持防病毒软件监测特征的自定义及统一的数据报表功能。

6、支持Windows系统补丁和应用程序补丁，能够进行索引文件更新；支持补丁自动分发安装，在指定时间、指定网络范围内分发补丁，或者根据脚本策略统一控制客户端下载补丁；支持补丁测试功能，对新下载的补丁进行真实环境的测试，测试完成后确认补丁安全再在指定时间后大面积下发补丁；服务器的补丁程序获取支持至少以下方式，一是连接到Internet上从微软官方网站的提供的站点自动下载补丁程序；二是从厂家提供的光盘建立本地升级站点，给补丁服务器提供本地（不需上Internet网）获取方式；可对计算机终端进行补丁安装状况查询，获知所查询的补丁的安装情况并生成报表。

7、支持软件下载优先级设置；提供软件分发完成情况的统计报告。

8、支持对终端计算机的非法外联行为进行控制，实时检测内网用户通过调制解调器、ADSL、无线网卡、红外、蓝牙、多网卡等设备进行非法外联，当有非法外联行为后，系统自动报警并进行阻断；支持对非法外联行为进行详细记录，包括非法外联的计算机的名称、 单位、上网方式,并进行实时报警。

9、支持主机密级、移动存储密级控制：密级至少应分为四级：高级、中级、一般、普通（提供截图）；能对终端计算机进行密级绑定；可对移动存储介质进行密级绑定管理（提供截图）。根据移动存储介质的密级程度及其被允许的使用范围判断主机或用户是否可以读取密级文件。

产品资质及授权要求：

提供原厂商针对本项目的授权书原件，一年质保及免费售后服务承诺函原件；提供产品计算机软件著作权登记证书、商用密码产品生产定点单位证书、商用密码产品销售许可证、CMMI5证书、质量体系管理证书ISO9001、信息安全管理系统证书ISO27001。

备注：含1个服务端、120个授权用户端