吉利百矿集团数据防泄密系统
（DLP）技术要求

注：“基本要求”和带“*”符号的为必须满足的指标

指标	指标项	详细要求
基本要求	交付及部署	系统为软件交付，部署在百矿集团提供的服务器。系统必须为国产软件。含 3 年使用许可和售后服务；
	服务端安全性	用户未经授权不能对客户端进行卸载、关闭等操作。不能通过任务管理器关闭客户端程序；支持远程对客户端卸载操作。
	客户端数量	系统包含 400 个终端授权点，含 3 年使用许可和售后服务；
	客户端资源占用	客户端资源占用，客户端安装程序不超过 120M，在使用的过程中系统资源占用小，使员工不会觉得慢，不影响工作。DLP 监控工作状态 cpu≤10%。DLP 文件扫描状态支持自适应 cpu 调节能力，在用户操作时自动暂停或以极低的 cpu 占用率工作。
	系统配置要求	系统安装所需的操作系统和数据库软件无需额外购买，无版权问题。
	兼容性	服务器系统支持 Ubuntu、CentOS；客户端兼容 WindowsXP、Windows2003、Windows2008、Windows7、Winindows8、Windows10
功能要求	内容识别	1）某一范围内相邻关键字组合
		2）支持至少主流文件类型真实格式与内容的识别，识别文档的原有格式，不受后缀名称的影响；支持够对多层文档嵌套的泄露行为进行检查（不低于 15 层），发现任何一层文档中含有的敏感信息
		3）系统支持文档内容指纹方式精确识别敏感内容。即通过对待保护文档内容生成指纹后，与外发文档的指纹匹配相似度，如果相似度超过一定阈值则可判断外发敏感文档内容。
		4）系统支持文档内容块指纹方式精确识别敏感内容。即通过对待保护文档内容生成指纹后，与外发文档块的指纹匹配，如果指纹重合度超过一定阈值则判断外发敏感文档内容。
		5）系统支持图片 OCR 方式识别图片文字。
		6）系统支持识别简体中文、繁体中文、英文、日等多种语言。
	文件识别	1）支持常见的文件类型、文件内容格式、加密文件格式、压缩格式、图片格式的识别
		2）系统支持识别 Linux，Unix 等非 Windows 的文件类型

		3）系统支持关键字方式识别敏感内容；支持*通配符、忽略大小写、中、英文、多模关键字、某一范围内相邻关键字组合的匹配方式
		4）系统支持 PCRE 语法的正则表达式方式识别敏感内容
		5）系统支持数据标识符方式识别敏感内容，如：身份证、中国人名等；
		6）系统支持识别 GB2312、GBK、GB18030、UTF8、Unicode 等多种字符集
		7）系统支持文件属性检测，包括文件大小、文件名、文件类型检测。
		8）系统支持自定义文件类型检测
		9）支持未知文件检测功能
		10）支持“源代码”文件类型的识别，防止源代码文件的泄露（PHP、C#、VB、Html 等 13 种源代码）
		11）支持匹配文档的页数、字数、行数、以及图片数量等，也就是按照信息量的大小去界定是否敏感，在相关的外发通道时可以引用这些规则进行敏感检查，审计信息可以看到命中文档的页数、行数、字数、以及图片数量等，并且可以根据这些信息进行查询；
	异常行为识别	1）系统支持识别文档多层嵌套方式逃避检测行为；
		2）系统支持识别文件多层压缩方式逃避检测行为；
		3）系统支持识别文件加密方式逃避检测行为；
		4）系统支持识别邮件密送行为；
		5）系统支持识别文档的页眉页脚隐藏敏感信息的行为；
		6）系统支持识别敏感信息标识为隐藏段落方式的泄露行为；
		7）系统支持识别修改文件扩展名方式逃避检测的行为；
		8）系统支持识别图片格式嵌入敏感文档方式；
		9）支持识别截屏、拍照成图片的方式泄漏敏感信息行为
		10）支持识别拷贝文档部分内容方式泄漏敏感信息行为
	终端监控	1）支持对光盘刻录的检测；
		2）支持对拷贝到移动存储中的检测，包括另存为，拖拽等动作；
		3）支持 U 盘只读；
		4）支持对打印的的检测；
		5）支持对剪切板的检测；
		6）支持禁止截屏行为，包括 windows 自带，微信，QQ 的截屏等；

		7）支持蓝牙状态的检测
		8）*支持邮件、网页、网盘传输的检测；
		9）*支持主流 IM 即时通讯工具外发的检测，如 QQ、微信、飞秋等外发的消息、附件等；
		10）*支持网络共享传输的检测；
		11）支持对应用程序访问的检测；
		12）支持基于设备 GUID、设备实例路径、显示名称、设备服务名等进行某一类设备进行管控。
		13）支持根据通讯时间、通讯工具、设备名称、用户名称、通讯帐号、通讯昵称、通讯群号、设备 MAC、设备 IP、聊天对象等进行聊天内容查询以及文件记录查询，能够根据组合条件进行查询；支持聊天窗口模式展示与列表信息展示两种模式；支持外发文件敏感检查；
		14）*支持 QQ、企业 QQ、客户端版/web 版微信、企业微信、钉钉、企业微信等主流聊天工具聊天内容控制并审计，支持文字、图片、文件独立监控；支持外发文件敏感检查；支持即时通讯关键字告警；通过邮件进行告知管理员；
	数据追踪溯源及管理	1）支持文档标签追踪管控，对 office、wps、pdf 文档进行标签化处理，可根据文档 ID 定位定位到设备 ID、用户名称、ip 地址、MAC 地址；可根据文档流转 ID 查询文档的流转过程
		2）支持屏幕截图控制、附加盲水印（QQ、微信、企业微信、TIM、企业 QQ、钉钉、键盘按键截屏），可将截图上传至【水印溯源】进行隐水印码解析，实现信息泄露追溯
		3）支持将用户、设备信息以点阵矢量图形方式或者字符附圆点的方式，打印在文档上；支持设置点阵数量、圆点直径大小；
		4）支持对 Outlook、Foxmail 等邮件客户端审计和控制支对 QQ 邮箱、163 邮箱、Yeah.Net 邮箱、126 邮箱、QQ 企业邮箱、新浪邮箱等 WEB 邮箱做审计和控制
	终端保护	1）支持终端阻断响应动作；
		2）支持终端弹出告警提示；
		3）支持用户自行选择动作；
		4）支持对违规文件进行隔离；
		5）支持对违规事件进行邮件通知告警，告警邮件里能够提供违规文件名，违反的策略名称等信息；
		6）支持对违规事件进行 syslog 通知告警；
		7）支持对发送文件的数据进行分类分级处理。
	终端扫描	1）支持对终端存在的含敏感信息的文件进行扫描发现，可指定包含或排除特定的文件名进行扫描，支持通配符；可指定包含或排除特定的路径进行扫描，支持通配符；可限定扫描过程中对终端的最大 CPU 占用率

		2）可指定包含或排除特定的路径进行扫描，支持通配符
		3）可指定特定大小范围的文件进行扫描
		4）可指定文件的创建时间、修改时间、范围进行扫描
		5）可限定扫描过程中对终端的最大 CPU 占用率
		6）支持当终端键盘或鼠标无操作时进行闲时扫描，可设置 CPU、内存阀值，超过阀值停止扫描，
	文档操作管理	*通过移动存储介质（U 盘、SD 卡等存储类设备）拷贝文件出去的时候，客户端弹出告警框，支持审批流程
	策略管理	1）满足实际工作所需要的复杂策略，单条策略可以包含多个规则，内部规则之间可以通过“AND/OR”，“条件”以及“排除”的逻辑组合在一起。
		2）不仅能够基于内容来制定策略，还能结合发送者/接收者，文件特征，通讯协议等来制定策略。
		3）支持针对特定数据内容，如：关键字、文件类型、文件大小、协议等条件进行例外处理。
		4）支持规则的重用，方便策略的配置。
		5）提供大量的预定义策略模板，可以在模板策略的基础上，派生自定义策略。
		6）可以对单条策略进行导入/导出，也可批量导入/导出策略，方便运维管理。
		7）支持指定设备、设备组、用户、用户组、部门、IP、MAC、操作系统下发策略，
		8）断网状态下策略仍然生效，并可在用户离开当前网络时做到策略随行;支持例外策略下发管理
	报表审计	1）系统提供丰富的报表功能.包括最近 7 天、30 天、所有终端事件；按策略汇总、策略趋势；按月和状态汇总；按策略和状态汇总；按周和策略汇总；用户汇总-移动存储；用户汇总-磁盘事件；终端用户汇总；按事件状态汇总；按协议类型汇总；按终端位置汇总；
		2）系统记录事件信息足够详细，如阻断状态、协议或端口、终端用户、应用、文件、事件状态、匹配次数、发送者（邮箱，IP，用户名）、接收者（邮箱，IP，用户名）、发生时间、主题、严重性、违规策略等信息。
		3）系统具备事件快照功能，即可查看此事件的详细描述信息，包括：发送者，接收者，数据所有者，检测日期，事件注释，事件属性，违规策略,规则,条件，邮件违规信息，文件列表。可以下载文件。
		4）事件报表可通过灵活定义汇总统计项、排序项、过滤条件，创建自定义报表。

		5）事件报表支持以 PDF、CSV、XLS 格式导出。
		6）系统支持定时自动发送报表功能。可以周期时间将事件报告以邮件方式发给特定审计人员；
		7）系统支持事件归档功能
		8）系统提供用户认证、用户权限配置、策略管理、事件审计等操作日志，可对管理员操作进行审计。
		9）系统支持批量审计功能
	管理功能	1）*支持从 AD 域服务器、LDAP 服务器导入终端用户；
		2）支持终端用户权限进行管理，不同权限的用户允许发送不同的文件；
		3）支持终端用户登录状态查询，查询条件不限于用户名，mac 地址等；
		4）*支持终端客户端自动升级。
		5）支持网络资源访问控制，提供自定义协议与服务端口，支持 TCP、UDP、RDP、HTTP、FTP、共享；支持源或目的的双向控制，支持入站和出站的双向控制，支持对 DNS 的黑白名单控制；
		6）*支持远程对客户端进行进入特权、退出特权、卸载、重启操作；
		7）支持远程获取诊断信息和日志；
		8）支持带宽自动优化功能；支持远程传送文件功能、支持远程即时通讯；
		9）支持将组织架构中任意成员指定为系统管理员；支持设置不同权限管理员；可对不同的管理员配置不同的权限；
	其他功能	1）终端文件拷贝外发，支持发起审批流程，审批通过后可以外发文件；
		2）支持打印水印和屏幕水印，水印信息包括自定义信息（水印属性、水印进程）和操作者信息（计算机名称、MAC 地址、IP 地址等）；
		3）支持访问指定业务系统、指定进程、访问指定应用才会触发屏幕水印，且支持将两种及以上水印方案任意组合；支持屏幕水印仅显示在应用窗口，且能够跟随应用程序移动缩放而自适应移动缩放；
		4）支持软硬件资产信息采集，能显示完整的终端信息，包含但不限于：计算机名、用户名、操作系统版本及主机进程信息、主机端口信息、主机服务信息。
		5）*支持将文件审计信息存储位置进行分布式部署，针对不同分支、区域独立部署审计服务器存储路径，避免全公司上传总部造成拥塞。支持上传限速； 审计信息设计的文档进行加密存储，防止二次泄密
	集成联动	1）*系统提供 syslog 接口，供第三方事件管理系统集成。

		2) 系统支持以 LDAP 接口集成第三方目录服务的功能。通过 LDAP 集成扩展事件关联属性，如发送者工号、姓名、部门等等。通过 LDAP 集成可以实现分级用户权限管理。
		3) *系统提供开放的开发接口，供第三方系统读取数据、开发及整合。
		4）支持与企业微信、钉钉同步组织架构；
		5）支持将文件审计信息存储位置进行分离部署，针对不同分支、区域独立部署审计服务器存储路径，避免全公司上传总部造成拥塞。支持上传限速； 审计信息设计的文档进行加密存储，防止二次泄密。
资质要求	产品资质	1)* 产品具有计算机信息系统安全专用产品销售许可证（数据泄露防护产品）
		2) 产品具有计算机软件著作权登记证书
		3） 产品生产厂家具备 ISO9001 质量管理体系认证证书