询价文件编号：T-250036

京港地铁终端数据防泄漏系统（DLP）采购项目

更正公告

京港地铁终端数据防泄漏系统（DLP）采购项目招标公告变更如下：

增加了附件六：技术需求书

增加了附件七：POC 测试评审表

详情如下。

北京京港地铁有限公司

北京京港十六号线地铁有限公司

北京京港十七号线地铁有限公司

2025 年 4 月 8 日

附件六：技术需求书

引言

目的

建立一套数据泄漏防护统一管控平台和终端数据泄漏防护系统，通过监测终端“由内向外”数据存储、使用和传输的数据信息，形成终端数据泄漏防护策略基线。提供符合我司实际场景下针对数据违规、越权存储、使用及外发价值数据集敏感信息数据的保护能力。主要涵盖：结构化及非结构化数据的内容分析技术、机器学习技术、智能内容分析技术、图片内容识别技术、网络流量还原技术、URL 提取及安全分析技术、高级恶意威胁、用户行为分析等。安全覆盖范围包括京港地铁 OA 办公网终端。

建设目标主要针对京港地铁 OA 办公网办公终端敏感数据的生命周期中三种重要状态的保护。内容包括：

（1） 静态中的数据：包括扫描存储设备与其他数据存储区，以识别机密数据所存放的位置。例如：扫描应用开发部门的文件服务器，识别含有源代码等敏感数据的文件，如果指定服务器或者目录并未授权存放此类数据，可以将数据加密、删除、移动至其他目录等，并提示该文件的拥有者；

（2） 使用中的数据：通过终端代理实时监控终端用户对于敏感数据的操作行为，比如：移动介质，打印，光盘刻录等等；

（3） 终端数据防泄漏能力包括应用程序监控、IM 监控、网络协议监控、外设数据传输监控、水印显示、Web 访问干预等。

（4） 实现终端数据存储合规监控、数据使用安全监控以及“内-外”数据传输合规监控和数据泄漏监控、同时实现数据安全统一管理分析和可视化。

（5） 终端数据防泄漏能力及上网安全监控能力。

引用文档

序号	资料名称	文件编号	发表日期	出版单位
1	《中华人民共和国数据安全法》	中华人民共和国主席令第 84 号	2021-06 -10	全国人民代表大会常务委员会
2	《中华人民共和国个人信息保护法》	中华人民共和国主席令 第 91 号	2021-08-20	全国人民代表大会常务委员会
3	《中华人民共和国网络安全法》	中华人民共和国主席令第 53 号	2016-11-01	全国人民代表大会常务委员会
4	《关键信息基础设施安全保护条例》	中华人民共和国国务院令第 745 号	2021-07-30	全国人民代表大会常务委员会

定义

序号	术语或缩略语	说明性定义
1	DLP	数据泄密防护，数据泄密防护(DLP)是通过一定的技术手

		段，防止企业的指定数据或信息资产以违反安全策略规定的形式流出企业的一种策略。
2	OCR	optical character recognition，光学字符识别

系统概述

系统目标

基于京港地铁数据安全建设需求，计划采购一套数据泄漏防护统一管控平台和终端数据防泄漏系统，支持对各类数据泄漏防护系统和设备的统一管控、策略规划和下发，以及日志归集及分析。

采购系统基于企业级数据防泄漏技术，依从于国际标准的企业级数据防泄漏体系，数据泄漏防护统一管控平台除支持管控终端数据防泄漏系统外，还需具备管理网络数据防泄漏系统及邮件数据防泄漏系统的扩展能力，以便在京港地铁搭建一套高稳定性、可扩展、可持续迭代的数据防泄漏系统，以满足京港地铁数据建设安全方面的持续要求。

满足对京港地铁 OA 办公网终端的数据传输监控及数据泄漏防护，持续提升终端数据安全风险抵御能力，缩短各类数据安全事件处理响应和分析时间，有效保障内部网络安全及业务系统持续正常运行，并针对内部数据资产进行持续风险审计。

系统范围

业务范围

对京港地铁 OA 办公网终端进行数据泄漏防护、异常数据存储安全监控、数据使用安全监控和防护，并提供数据安全态势的可视化展示能力。

数据安全设备及安全工具（包括但不限于以下设备）：

序号	设备名称	数量	备注
1	数据防泄漏统一管控平台	1 套	
2	终端数据防泄漏软件	4100 点	

组织范围

本次计划采购终端数据防泄漏软件，其中包含一套数据防泄漏统一管控平台及终端数据泄漏防护系统，防止通过办公终端造成敏感数据外泄。

功能范围

终端数据防泄漏项目包括终端流量审计、数据的保护、策略统一管理以及具有事件报表输出展示功能。需求包含对数据发现、移动存储、应用程序、IM、外设设备的数据进行监控审计或阻断的能力。

具体需求

功能需求

所有功能必须经过现场实际验证，并提供双方一致认可的测试报告。具体需求内容如下：

终端数据防泄漏

终端数据发现

终端本地存储的数据合规性检查，避免违规数据存储、敏感数据超期存储。

终端邮件数据防泄漏

终端通过邮件客户端、网页邮件等场景进行内容监控，具备对用户邮件数据泄漏行为的内容识别和阻断的能力，记录安全事件。同时在终端上进行安全提示，告知用户此邮件被拦截的原因。

终端外设数据防泄漏

对终端在办公环境中使用 U 盘、移动硬盘、光盘、打印机等场景的数据泄露行为，具备记录当前用户行为并阻断的能力，可进行相关审计。

终端网络数据防泄漏

终端通过 HTTP、HTTPS、FTP、SMTP 等协议进行数据传输时，可进行实时内容分析，具备对数据泄漏行为进行阻断的能力，生成安全事件并实时取证。

终端应用程序数据防泄漏

对 QQ、微信、企业微信、钉钉 TIM、Skype for business 等即时通讯聊天应用进行实时内容分析，具备并对数据泄漏行为具备阻断的能力，可生成安全事件并对聊天窗口实时取证。

对网盘工具、云笔记工具等云数据同步应用的数据泄漏行为，可进行实时内容分析，并具备对数据泄漏行为进行阻断的能力，生成安全事件并实时取证。

终端水印防护

以水印方式对操作敏感数据场景进行安全警示，提供多种水印防护，并支持水印信息定制化。提供屏幕显示水印、敏感内容触发水印及基于应用程序的打印水印防护。

网络访问数据泄漏监测和防护

根据上网安全策略，对用户 web 访问动作进行安全判断和合规判断，具备阻断异常 web 访问动作的能力，避免发生数据泄漏事件。

数据防泄漏统一管控平台

统一管理

避免繁琐调试配置策略，数据防泄漏产品需要具备集中统一管理的能力，对相应的设备和产品进行管控和事件归集。同时，还要具备相应的报表输出（XLS\PDF）,具备相应的图表可视化显示，可适应大屏动态展示，便于信息安全管理人员，及时准确的发现数据泄密事件，并加以处理。

统一安全分析及可视化呈现

在事件功能方面，需具备详细的审计内容，比如针对违规事件的发送者、内容（证据）、接收者、命中策略项及原因、命中次数等具备详细的记录和展示，做到统一管控平台可以对违规事件一览可见。

统一数据发现

对文件服务器、数据库、网络、邮件服务器等存放大量数据的位置进行数据发现操作了解机密敏感信息的具体位置，以便对相应的数据进行分类分级保护，相应的 DLP 产品应具备较为成熟的预置模板和功能来进行分类分级辅助。

性能需求

数据安全统一管控系统各组件性能要求

管理平台		
硬件规格	规格	标准机架式设备
	CPU	至少两颗 Intel Xeon E5 系列 CPU，每颗 CPU≥16C 物理核心、32 线程，主频不低于 2.10GHz
	内存	内存≥128GB
	存储(数据盘)	≥600GB（RAID 1）(系统盘) ≥2000GB（RAID 1）（数据盘）
	网口	千兆电口≥4
	电源	双电源
	机架套件	1 * 上架导轨套件（含导轨）
性能规格	最大处理能力	≥10000 个设备（终端 Agent）

终端数据防泄漏软件

终端数据防泄漏软件		
适配能力	系统	支持 Windows，Mac 和国产化终端，各平台数据防泄漏保护能力需要保持一致，软件安装后，软件自身 Agent 闲时系统内存占用不超过 0.3GB，平均 CPU 占用不超过 50%

技术需求

“*”图标为必须满足项。不满足或部分满足都示为投标文件无效。

所有功能项必须在京港地铁现场进行 POC 测试，并出据双方都认可的测试报告。

统一管理分析平台功能技术要求

序号	测试功能	功能项	招标要求
1	管理能力	部署方式	*系统应支持集中管理，在同一管理平台上同时管理网络 DLP、邮件 DLP、终端 DLP、应用 DLP、发现 DLP、移动 DLP 等多个产品组合，并提供统一的策略管理、事件证据管理及相关策略组件管理功能，便于未来进行扩展。
2			*系统应支持管理控制台的分级管理架构，能够通过 IP 地址段、组织

			架构、管理设备等多层次架构，实现统一的事件管理、策略下发等功能和性能要求。系统需支持上级管理本级和下级的用户、日志、策略和设备。各分支机构管理员应能够根据分级架构分配权限，并支持策略优先级设置及策略继承。
3			系统应支持数据库和证据文件的本地化部署和外部部署两种方式。外部证据部署应提供加密或明文部署的选择，以满足不同安全要求。
4		API 对接	*系统应提供关键规则元素的 API 对接能力，允许外部系统进行策略、黑白名单的增删改等操作，确保灵活的集成与管理。
5	用户管理	监控用户信息集成	系统应支持定时或手动通过 Active Directory（AD）、LDAP、Domino、ADAM 进行用户信息的同步，并允许根据实际需求自动选择和修改同步方式。
6			系统应支持在界面上自定义输入组织架构信息，包括用户、用户主管、部门、部门主管及计算机组织结构信息。同时，系统还应支持通过 CSV 文件方式导入用户及组织架构数据。
7		管理用户配置	系统应支持详细的权限管理，允许管理员为每个角色定制权限，包括报告事件管理（如仅系统查阅、禁止下载、本地敏感数据脱敏等）、配置管理和系统管理的具体权限设置。
8			*系统应支持四权分立功能，支持配置独立的角色管理，包括系统管理员、事件管理员、审计管理员和安全管理员，各角色功能独立无交叉。系统管理员负责日常管理和角色、账号维护；事件管理员管理事件和报告；审计管理员查看和导出审计日志；安全管理员审批账号和策略变更。所有角色和账号的创建、修改均需安全管理员审批通过。
9	系统管理	备份与还原	系统应支持配置、事件、证据文件、邮件日志、邮件原文及网络主机信息的定期备份和恢复功能，备份方式应包括本地备份和远程备份，确保数据安全和系统可恢复性。
10		升级/补丁	系统应支持通过管理平台进行产品升级，提供在线下载升级和本地上传升级两种方式，确保系统灵活性和便捷性。
11		系统安全	管理控制台应具备系统强校验、失败锁定和登录 IP 限制等安全管控功能，并支持密码与登录验证码的组合验证，确保系统安全性。
12		语言支持	*系统应支持用户语言绑定功能，允许用户根据需求在中英文界面之间切换，提升用户体验。
13		系统监控	系统应支持实时监测并警示设备及相关模块的健康状态，包括 CPU、内存、网卡和设备授权等，及重要配置如邮件服务器和告警设置。系统告警应支持手动清除。
14	报告及事件管理	定制报告	系统应支持提供预置及定制的趋势分析报告，包括一周内的事件趋势图、安全等级事件趋势图、策略事件趋势图、来源事件 TOPN、目标事件 TOPN，以及来源总匹配 TOP20 等报告。系统应支持定制数据统计分析，能够以直观图表形式同时显示多个报告，并可展开额外的事件细节。系统还应支持根据需求定时将报告通过邮件发送给特定管理人员。
15		风险评估报告	*系统应支持以人为中心的报告生成，涵盖个人风险值、个人风险排名及个人事件数据统计等内容，提供全面的个体风险分析。
16		事件列表展示	系统应支持自定义筛选条件，包括部门、组织单元、组、文件名称、策略名称、详细信息等，并允许灵活调整和排序筛选条件，并将自定义筛选条件保存为事件的默认筛选规则。
17		事件详情展示	系统应支持证据记录及详情查看，事件日志中应详细记录事件类型、发生时间、上报时间、发送者、接收者、违反策略、告警级别等信息，并支持事件的脱敏展示功能。
18		大屏监控	系统应支持大屏监控展示定制，能够实时展现敏感数据或安全行为，提供直观的安全监控可视化效果。

19		第三方支持	系统应支持将违规事件日志或审计日志通过 SYSLOG/SIEM、Kafka 等方式上传至外部服务器，并允许定制传递的日志字段。
20		事件管理	*系统应支持完整的事件安全管理流程，包括备注和标签添加、安全级别和状态更新、邮件审核与释放、事件删除和忽略，以及事件状态显示顺序调整等功能。
21	策略管理	策略灵活性	系统应支持多个策略规则的任意条件组合（如与、或、必选项、M 选 N），并允许针对多个特定规则条件进行例外处理。同时，支持对来源/目标的精确匹配，根据策略设置不同动作，如放行、阻断、加密、隔离等。系统还应支持针对网络和终端通道的不同协议设置相应策略，如请求、响应、请求方法等，并支持多种检测类型。
22		策略黑白名单	系统应支持对发件人邮箱、来源 IP/IP 段、目标 IP/IP 段、目标域名、UNC 路径、应用程序路径及来源/目标组合等方式进行灵活的配置，实现对来源目标的黑白名单配置，以绕过 DLP 分析。
23	内容识别技术	分类	*系统应基于“数据分类”进行内容安全防护，支持引导用户对敏感数据进行分类，并根据分类结果制定 DLP 安全策略。系统应能够在事件和报告中展示数据分类分析结果，并通过数据分类呈现数据安全报告。
24		标签	*系统应支持标签作为策略检测规则和数据分类规则使用，并能根据应用程序触发不同敏感内容打不同标签。同时，管理控制台应能展示标签内容及其操作历史。
25		关键字	系统应支持关键字和关键字对的管理，并能够进行精确匹配和自动匹配简体/繁体中文。关键字规则中的“精确匹配”功能需支持区分大小写。
26		正则表达式	系统应支持正则表达式检测内容，并提供常见的正则表达式模板，如手机号码、固话号码、姓名、地址等。
27		脚本	系统应预置身份证、护照、信用卡等常用数据检测脚本，并支持对源代码（如 C、Java、Python 等）进行准确检测，确保快速识别和保护敏感信息和代码内容。
28		指纹	*系统应支持数据库和文档的敏感数据指纹学习，涵盖多种数据库类型和 ODBC 连接。支持本地文件和远程共享目录的指纹学习，提供 10%-90%相似度阈值调节的指纹相似度检测。支持增量和全量指纹学习、定时任务计划、反向指纹学习及离线指纹生成工具，确保数据泄漏防护和减少误报。
29		字典	系统应预置开箱即用的权重字典，能够识别常见敏感数据，包括国家领导人、政治言论、高管信息、法轮 X、技术方案、会议纪要、采购计划、网络安全、投资信息、简历等。系统还应支持自定义和导入字典，并提供字典搜索查询功能，方便用户在大量条目中快速定位和维护字典规则项。
30		智能学习	系统应支持对规范模板类文件的有效学习，防护业务敏感数据，确保类似文件内容自动识别，无需单独制定指纹策略。同时应支持正反向机器学习训练，提升识别能力，并智能检测潜在数据泄漏威胁。另外应该支持远程目录自动学习及结果导出，并配备数据聚类工具进行自动分级分类，优化 DLP 策略。
31		文件属性	系统应支持对文件名称进行检测匹配，并允许设置匹配阈值。系统内最少预置 800 种以上文件类型，并提供自定义文件类型创建功能。支持识别 WPS 加密“.dpt/.ppt”文件格式及 Hadoop ORC 文件格式，能够进行文件大小检测匹配，支持检测文件的所有者、修改日期、创建日期、访问日期等属性，以及主题、类别、标记、备注和最后一次保存者等信息。
32		数据聚类	*系统应支持通过机器学习技术，将用户提供的大量无序文件样本按内容自动聚类，实现文档分级分类。聚类后的文件应支持指纹生成和智

			能学习，辅助更有效地制定 DLP 策略。
33		复杂检查能力	系统应支持多语言内容检测，涵盖中文、英文、泰文、俄文等主要语言，并具备对邮件正文、附件、发件人、收件人及邮件头的匹配检测功能。可以支持文档位置匹配检测，精准识别和处理 Office 类型文件（如 Word、Excel、PPT）中的页眉、页脚、正文及嵌入内容。此外还应支持基于数据大小规则的 DLP 策略控制，对 Web POST 表单数据和 Email 原文进行管理和限制，并支持对邮件附件数量及所有属性（包括附件名称）的检查匹配。
34		文件真实格式识别技术	系统应支持主流 Office/PDF 加密格式、ZIP/7zip/RAR 压缩格式，且支持最新的 RAR5 和 7zip 的全部四种压缩格式。能够检测多层文档嵌套中的泄露行为，发现任何一层文档中的敏感信息，并支持对通过更改文件名、后缀、压缩包后缀、转换文件类型等规避手段处理过的文件内容进行检查。
35		图片内容识别 OCR 能力	系统应预置高性能高精度 OCR 图片内容识别引擎，支持简体中文、繁体中文和英文的高精度识别，无需独立部署或另购。可以支持对常见图片文件及嵌套在 Office 文档和压缩包中的图片内容进行检查，包括 JPEG、TIF、TIFF、BMP、PNG 等常见图片格式。并至少提供三种识别模式以适应实际的检测需求：高效精确度低、效率与精确度兼顾、高精确度但效率较低。
36		点滴式监测技术	*系统应支持在自定义时间范围内对累计达到告警阈值的检测技术进行监控，包括策略触发次数和违规内容触发次数。

终端数据防泄漏功能技术要求

序号	测试功能	功能项	招标要求
1	终端系统与管理	操作系统支持	*系统应支持在 32/64 位 Windows XP/7/8/10/11、Windows Server、macOS 10.9 及以上版本，麒麟 Linux（国产化平台龙芯+中标麒麟）、UOS、CentOS 等操作系统上进行终端 DLP 部署。对所有的操作系统均需要支持监控和阻断能力，相关能力在不同操作系统上应具备一致性。
2		运行支持	系统应支持简体中文、繁体中文和英文操作系统，具备显示运行和隐藏运行（用户无感知）模式，在隐性模式下可在进程列表中隐藏进程信息，确保用户无感。同时，系统应支持在 Windows 安全模式下运行，允许管理员自定义终端阻断页面的提示语言和配置模板，定制公司名称和提示内容等信息。
3		安装用户的绑定	*系统应支持读取登录 AD 用户的信息，也应支持读取企业内已部署的联软、360、H3C、iNode、天擎等终端软件的用户信息作为管控和策略控制的依据，同时应支持手工绑定用户账号并对接 AD 进行密码验证，并在必要时允许清除已绑定的账号进行重新绑定。
4		卸载	系统应支持对终端的强制卸载，并清除系统残余文件，同时提供卸载密码保护功能，要求密码校验正确（支持提供全局密码和临时密码）方可卸载。可以提供终端远程申请卸载和离线申请禁用功能，允许管理端进行远程在线卸载和禁用的操作。
5		终端资源控制与保护	系统应支持对终端 DLP 使用的 CPU 占用、带宽、日志存储大小进行控制，避免过度占用操作系统主机资源。允许通过终端配置设置资源消耗能力，以适应不同应用场景下的计算机资源要求。系统应具备终端进程保护功能，防止用户强行终止，并支持保护终端安装目录及重要文件，防止被删除，同时应执行运行在安全模式下保护能力依然生效。

6		终端信息	系统应记录所有注册终端的详细信息，包括主机名、登录名、IP、操作系统（OS）、同步状态、连接状态等，并支持展示终端的健康状态，记录终端的安装时间。系统还应允许管理员对离线终端或需要备注的终端进行手工备注，例如未加域的电脑。
7		终端位置判定	系统应支持通过服务器连通性、DNS 解析的域名地址、PING 连通性、IP 范围、DNS 地址等多种条件和逻辑组合判断终端所处位置，根据位置执行不同数据安全策略，并确保终端在离线状态下防护策略依然有效。
8	终端标签	终端文件标记	*系统应支持终端文件的标记能力，能够通过多种手段为终端上的具有 meta 属性的数据文件添加标记，包括但不限于：基于终端数据发现任务自动为敏感文件打上分类标签，手动右键对单个文件或批量文件进行打标，对常见的 Office 程序在文件保存时弹窗提示用户选择对应标签，以及自动为从指定 URL 或文件共享下载的文件进行标记。
9		标签溯源	*系统应支持在完成嵌入式标签操作后，当数据泄露事件发生时，登录管理控制台利用标签信息追踪。
10	数据传输内容审计	终端协议支持	系统应支持对通过 HTTP、HTTPS、SMB、SMTP、FTP、AirDrop 和 RDP 协议上传、下载的内容进行分析，并支持放行、阻断、确认动作，同时自适应 HTTP2 协议。
11		终端下载检测	*系统应支持对通过浏览器下载文件和从外部共享文件夹中拷贝文件的行为进行 DLP 内容分析和策略匹配，防止敏感数据被下载到用户计算机上。
12		终端邮件客户端检测	*系统应支持对使用 Foxmail、Outlook 等特定的邮件客户端发送的邮件进行内容检测，并支持放行、阻断、确认等操作。
13		终端 IM 检测	*系统应支持终端上的 QQ、企业 QQ、微信、企业微信、Skype、Skype for Business、钉钉、阿里旺旺、TIM、飞秋、飞书、CoCall 等即时通讯软件的聊天内容和传输文件进行检测，并支持放行、阻断、确认等操作。系统还应支持阻断 IM 图片发送、禁用转发功能，并能够记录聊天账号信息。对于触发策略的聊天内容，系统应能够截屏当前聊天窗口并上传作为证据。
14		终端打印检测	系统应支持对打印文件进行内容分析，预防敏感数据通过打印外泄，并支持放行、阻断、附加水印、确认等操作。水印应支持明文水印和暗水印。
15		终端应用传输控制	系统应支持对自定义应用程序的复制/剪切、粘贴、截屏、文件访问和水印内容进行分析，应用程序包括但不限于网盘、云笔记等具备外发能力的应用程序。在使用应用程序进行截屏时，系统应支持放行或直接阻断，并保存事件前后 N 张截屏作为证据。
16		外设数据传输检测	系统应支持对刻录至 CD/DVD 的文件、通过蓝牙传输的文件、拷贝至 USB 的文件进行内容分析，并支持放行、阻断、确认等操作。USB 拷贝允许对敏感文件采用个人密码加密操作，且支持记录并展示移动存储设备的实例 ID。
17		策略触发控制	*系统应支持对通过所有终端通道发送的数据包括经过 Microsoft RMS 加密的文件进行敏感内容监控，当触发策略可以进行自动截屏并存储为证据。同时还应支持对终端数据的审批动作，通过 API 对接企业的审批平台，当文件被阻断时触发审批窗口实现终端审批。
18		IPv6 检测支持	*系统应支持终端在策略和白名单中定义 IPv6 相关配置参数，适应 IPv6 环境下的流量检测需求。
19	数据发现	终端数据扫描发现	*系统应支持对指定计算机和指定磁盘路径进行实时或计划定期的深度发现扫描，包括增量和全量扫描。在发现敏感数据后，系统应能够执行保护、隔离、自动标签等动作，并可以使用自定义脚本进行额外

			的动作处理。
20			*系统支持通过终端监控实时控制发现任务的开始、停止和暂停操作。
21			*系统应支持通过终端数据发现任务，将敏感文件保存到保险箱服务器端。
22	终端水印	终端水印	系统应支持基于终端配置启用/禁用屏幕水印，并具备隐性水印能力。隐性水印信息在用户截屏后完全不可见，但管理员可以通过登录控制台进行隐性水印信息的还原。
23			*系统应支持应用水印，支持的应用包括 Office 系列、WPS 系列、MAC Keynote/Numbers/Pages、Notepad、Textedit、Preview、Adobe PDF、各类浏览器等，当且仅当文档应用包含敏感数据或者浏览器访问了指定网站，才显示水印内容。
24			系统应支持直接启用或对经过内容分析后针对敏感文档的打印水印，适用于常用的 Office、WPS、浏览器、图片、Notepad、Adobe PDF 等应用，既支持常见的明文水印、二维码水印，也可以在打印文件上以隐蔽方式随机分布水印信息，便于对员工打印的文件进行追溯。
25			水印类型应包括明文水印、二维码水印和点状水印，并提供详细的水印参数配置。其中，二维码水印应可通过微信、支付宝等应用扫描还原明文信息，点状水印可通过管理控制台进行反查。
26	其他控制检测能力	外设控制	系统应支持对多种外设的启用、禁用及只读控制，包括 USB 存储设备、MTP/PTP 手机、CD/DVD 驱动器,支持对 USB 蓝牙、USB WIFI、软驱、串口/并口、IEEE 1394 接口、PCMCIA 接口、截屏功能、红外功能、蓝牙以及 AirDrop（MAC）的启用和禁用控制。
27		Web URL 控制	*系统应支持根据客户端访问的外部 URL 分类、URL 风险级别和 URL 风险类别（包括挂马网站、非法网站、黑客指挥中心、黑客工具等），过滤用户的 Web 访问请求，在发现风险时进行告警或阻断风险的 Web 访问。 支持对访问网站进行时间段控制。
28		操作系统代理控制	*系统应支持对终端操作系统的浏览器进行代理设置锁定，同时支持指定 PAC 路径。
29		终端文件勒索检测	*系统应支持定义终端诱饵文件，并检测对这些诱饵文件的修改、删除操作，记录勒索事件。系统应与 ITM 勒索检测模型配合，检测和识别疑似勒索行为。
30		终端审批	*系统应支持终端敏感文件审批外发能力，可设定规定外发的时间和次数。

安全运维服务需求

基于数据防泄漏统一管控平台，完成日常安全运维服务要求，主要包括配置调试优化、事件管理、运维汇报管理等方面的内容。具体需求内容如下：

系统巡检服务

为保障平台系统正常运转，服务人员需要对系统 CPU、存储情况、系统时间、授权、功能模块等巡检，避免故障影响服务工具正常运行，巡检发现故障后，服务人员协调跟踪产品并对产品进行故障修复。

服务频率：每季度一次。

提交成果：《服务运维季报》（每季一次）。

培训服务及知识转移

为保证数据防泄漏系统上线后，方便内部人员管理及使用，需提供数据防泄漏系统管理员操作培训及数据防泄漏系统日常运维培训。

服务频率：2 次

培训时间：8 小时

提交成果：《培训记录》

策略优化调试

策略的制订以前期内部数据调研的数据梳理、分级分类项目的输出结果为基础，对关键数据，敏感信息，以及非法手段进行有效监控。初期将采用内置策略模板优先进行部署，并根据事件数量和触发频率，调整策略的阈值和逻辑关系。

配合数据安全治理工作

辅助和配合我司数据安全治理相关工作的执行落地。

安全事件响应

故障分类方式如下

一级故障（P1）：系统故障，或对最终用户的业务运作有重大影响。

二级故障（P2）：系统严重故障、部分重要服务不正常。

三级故障（P3）：系统个别服务不正常，但大部分业务运作仍可正常工作。

四级故障（P4）：在产品功能、安装或配置方面需要信息或支援。对自身的业务运作影响较小或无影响。

服务频率：7 天×24 小时×365 天。

交付成果清单

日常安全运维服务项目交付成果清单		
序号	服务内容	交付成果
1	内部 PC 环境摸排	《环境调查问卷表》
2	数据调研	《数据调研表》
3	事件管理	《服务运维季报》
4	安全策略优化建议	《安全优化建议》
5	数据防泄漏系统管理员操作培训	《培训记录》、《产品手册》
6	数据防泄漏系统日常运维培训	

服务要求

SLA 服务等级要求

故障类型	支持方式	响应要求	响应时间	缓解时间
P1	远程/现场支持	7×24	15 分钟	3 小时
P2	远程/现场支持	7×24	30 分钟	5 小时
P3	远程/电话支持	7×24	2 小时	7 小时
P4	邮件 / 电话支持	7×24	24 小时更新	72 小时更新

安全保密需求

严格遵守合同规定，执行国家《保密法》及有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，相关人员恪守职业道德，服从采购人的管理，严格遵守采购人的保密规定和工作制度，并承担相应的保密责任。

所有参与本项目的服务人员，都必须签订《保密承诺书》（模板见附件）。中标人负责对《保密承诺书》归档保管，接受采购人检查。中标人对承诺履行情况负有监督责任，一经发现违反承诺情况，要及时向采购人报告。

中标人自觉接受采购人的安全保密监督和管理，中标人如违反安全保密条款，采购人有权追究其责任，对重大的泄密事件将移交司法部门追究其法律责任；对中标人泄漏系统资料，造成伤害的，除依据有关规定追究有关责任人员法律责任外，还将依法承担相应的民事责任。

售后服务需求

项目服务保障周期

项目所投软件提供为期 5 年的软件维保服务，包括数据防泄漏统一管控平台、终端数据防泄漏产品，及授权终端点数 4100 点（目前我司办公终端数量）5 年授权，质保期内客户端更换操作系统（例如由 Windows 改为信创系统），在授权点数不变的情况下不产生其它额外费用；硬件需提供 5 年质保服务(由服务器原厂提供)，质保期内如果出现硬件损坏提供检测、维修、更换等服务。

售后服务

项目所投产品软件乙方需具备完善的应急相应处置手段，描述厂商关于售后服务的售后

服务组织、售后服务流程。

提供免费的电话技术支持服务，当出现安全事件或产品问题后，技术支持团队将提供第一时间的处理和响应。

升级服务

提供为期 5 年的产品升级服务，包括系统版本更新、产品 bug 修复、规则库更新、固件更新等。

日常咨询

提供日常售后服务支持方式，包含但不限于 E-mail、在线支持和电话支持等方式提供售后服务的日常咨询。

巡检服务

在质保期内为甲方免费提供每季度一次的巡检服务，并提供相关平台的巡检报告。

策略调优服务

在质保期内为甲方免费提供每季度一次的策略调优服务，对数据防泄漏策略的合理性进行评估和提供优化建议。

培训要求

至少提供 2 次(不少于 8 小时)产品使用安全培训服务，培训内容包含但不限于产品 的日常使用，产品常见问题处理等。

资质与服务保障要求

资质要求

- 投标人应具有信息安全管理体系证书（ISO27001）；
- 投标产品具备《中华人民共和国国家版权局计算机软件著作权登记证书》或专利证明文件；
- 投标人提供本次应答产品的相关信创资质。

服务保障要求

由于网络安全防护的专业性、复杂性和长期性，对安全服务保障技术支持团队要求如下：

（1）拥有一支稳定的服务保障队伍，并具有较强的技术保障实力。

（2）本项目配备项目经理 1 名，项目经理具备 PMP 相关资质或同类型资质证书；至少 1 名专职售后实施工程师服务于项目。在项目实施过程中如遇问题经双方协商可按照协商结果调整项目实施进度。

（3）提供项目实施的工作计划，工作内容以及服务进度安排。

（4）为本项目提供 1 名信息安全技术专家，遇到突发情况时能够及时解决问题。

（5）为本项目提供的专业安全团队至少包括 1 名安全技术人员、1 名方案分析和制作人员、1 名专业维护人员。

（6）团队有明确分工和侧重点，基本人员均掌握一般的安全服务方法并能解决普遍性安全问题。

（7）具备提供 7 天*24 小时安全运维服务能力。

（8）具有良好的职业道德，不损害用户利益。

安全要求

1) 供应商应确保所提供的以及后续开发涉及的软件及程序，均有正版授权或软件著作权，并提供正版授权书复印件，因版权产生的所有问题和损失，由供应商承担全部责任。
2) 供应商应确保其基础设施、运维地点、用户数据、用户个人信息均位于中国境内。
3) 供应商应承诺代码中无漏洞及后门程序，并且系统上线前须经过专门安全检测，提交第三方出具的安全检测报告。
4) 与供应商签署的服务协议中应规定供应商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等。
5) 应承诺不得将开发过程涉及的京港地铁相关数据泄露给第三方；如系统涉及收集公司敏感信息及个人信息，应采取技术措施确保公司敏感信息及个人信息保护符合《数据安全法》、《个人信息保护法》等法律及行政法规的规定，并防止未经授权的访问以及数据的泄露、篡改、丢失。如发生或者可能发生数据泄露、篡改、丢失的情况，应立即通知京港地铁相关人员，并及时采取补救措施。如因泄露产生纠纷，供应商需要承担相关法律责任。
6) 供应商所提供和使用的软件及程序在维保期内接受相关安全部门审查（如公安部或交通委等单位的安全检查或相关安全文件要求），如有不符合项，由供应商负责免费整改。
7) 如系统涉及处理公司敏感信息及个人信息，供应商应在系统立项初期配合京港地铁开展数据保护影响评估，确定数据收集范围、数据处理目的、数据保护方案，确保收集信息的相称性和最小化。
8) 供应商近三年无信息安全违规事件。
9) 系统实施要遵守京港地铁公司的《公司信息安全管理制度》。

附件：安全保密责任

为切实做好本次项目的保密工作，防止发生失泄密事件，根据《中华人民共和国保守国家秘密法》的相关要求，特签订本责任书，内容如下：

一、参加单位要经常组织人员学习《保密法》和有关保密工作的规定，严格遵守《保密法》，提高警惕，严防失泄密事件发生。自觉做到不该看的文件不看，不该说的不说。

二、参与项目的实施人员，面对甲方其他办公场所时，做到无关人员不得随意进入。对涉及项目保密的纸质文件的起草、制作、分发、传递、使用、复制、保存、销毁，要严格按照国家有关规定进行，坚决杜绝将涉密纸质文件随意丢放、携带出差、带回家中、擅自扩大阅知范围、向无关人员透露等现象。

三、对涉密计算机必须重点监管，严禁涉密电脑上互联网。处理涉密信息的计算机信息系统不得接入互联网，必须采取与互联网完全隔离的保密技术措施。

四、严禁擅自将移动硬盘、U 盘、光盘等磁介质随意插入涉密计算机、工作机，如确需拷贝资料，需经机主进行保密隔离处理之后方可。连接互联网的计算机不得通过 QQ、邮箱等方式传递公文内容特别是涉密信息。

附件七：POC（Proof of Concept）测试评审表

统一管理分析平台功能测试内容

序号	测试功能	功能项	统一管理分析平台功能测试内容
1	管理能力	部署方式	系统应支持集中管理，在同一管理平台上同时管理网络 DLP、邮件 DLP、终端 DLP、应用 DLP、发现 DLP、移动 DLP 等多个产品组合，并提供统一的策略管理、事件证据管理及相关策略组件管理功能，便于未来进行扩展。
2			系统应支持管理控制台的分级管理架构，能够通过 IP 地址段、组织架构、管理设备等多层次架构，实现统一的事件管理、策略下发等功能和性能要求。系统需支持上级管理本级和下级的用户、日志、策略和设备。各分支机构管理员应能够根据分级架构分配权限，并支持策略优先级设置及策略继承。
4		API 对接	系统应提供关键规则元素的 API 对接能力，允许外部系统进行策略、黑白名单的增删改等操作，确保灵活的集成与管理。
5	用户管理	监控用户信息集成	系统应支持定时或手动通过 Active Directory（AD）、LDAP、Domino、ADAM 进行用户信息的同步，并允许根据实际需求自动选择和修改同步方式。
6			系统应支持在界面上自定义输入组织架构信息，包括用户、用户主管、部门、部门主管及计算机组织结构信息。同时，系统还应支持通过 CSV 文件方式导入用户及组织架构数据。
7		管理用户配置	系统应支持详细的权限管理，允许管理员为每个角色定制权限，包括报告事件管理（如仅系统查阅、禁止下载、本地敏感数据脱敏等）、配置管理和系统管理的具体权限设置。
8			系统应支持四权分立功能，支持配置独立的角色管理，包括系统管理员、事件管理员、审计管理员和安全管理员，各角色功能独立无交叉。系统管理员负责日常管理和角色、账号维护；事件管理员管理事件和报告；审计管理员查看和导出审计日志；安全管理员审批账号和策略变更。所有角色和账号的创建、修改均需安全管理员审批通过。
9	系统管理	备份与还原	系统应支持配置、事件、证据文件、邮件日志、邮件原文及网络主机信息的定期备份和恢复功能，备份方式应包括本地备份和远程备份，确保数据安全和系统可恢复性。
10		升级/补丁	系统应支持通过管理平台进行产品升级，提供在线下载升级和本地上传升级两种方式，确保系统灵活性和便捷性。
11		系统安全	管理控制台应具备系统强校验、失败锁定和登录 IP 限制等安全管控功能，并支持密码与登录验证码的组合验证，确保系统安全性。
12		语言支持	系统应支持用户语言绑定功能，允许用户根据需求在中英文界面之间切换，提升用户体验。
13		系统监控	系统应支持实时监测并警示设备及相关模块的健康状态，包括 CPU、内存、网卡和设备授权等，及重要配置如邮件服务器和告警设置。系统告警应支持手动清除。
14	报告及事件管理	定制报告	系统应支持提供预置及定制的趋势分析报告，包括一周内的事件趋势图、安全等级事件趋势图、策略事件趋势图、来源事件 TOPN、目标事件 TOPN，以及来源总匹配 TOP20 等报告。系统应支持定制数据统计分析，能够以直观图表形式同时显示多个报告，并可展开额外的事件细节。系统还应支持根据需求定时将报告通过邮件发送给特定管理人员。
15		风险评估报告	系统应支持以人为中心的报告生成，涵盖个人风险值、个人风险排名及个人事件数据统计等内容，提供全面的个体风险分析。

16		事件列表展示	系统应支持自定义筛选条件，包括部门、组织单元、组、文件名称、策略名称、详细信息等，并允许灵活调整和排序筛选条件，并将自定义筛选条件保存为事件的默认筛选规则。
17		事件详情展示	系统应支持证据记录及详情查看，事件日志中应详细记录事件类型、发生时间、上报时间、发送者、接收者、违反策略、告警级别等信息，并支持事件的脱敏展示功能。
18		大屏监控	系统应支持大屏监控展示定制，能够实时展现敏感数据或安全行为，提供直观的安全监控可视化效果。
19		第三方支持	系统应支持将违规事件日志或审计日志通过 SYSLOG/SIEM、Kafka 等方式上传至外部服务器，并允许定制传递的日志字段。
20		事件管理	系统应支持完整的事件安全管理流程，包括备注和标签添加、安全级别和状态更新、邮件审核与释放、事件删除和忽略，以及事件状态显示顺序调整等功能。
21	策略管理	策略灵活性	系统应支持多个策略规则的任意条件组合（如与、或、必选项、M 选 N），并允许针对多个特定规则条件进行例外处理。同时，支持对来源/目标的精确匹配，根据策略设置不同动作，如放行、阻断、加密、隔离等。系统还应支持针对网络和终端通道的不同协议设置相应策略，如请求、响应、请求方法等，并支持多种检测类型。
22		策略黑白名单	系统应支持对发件人邮箱、来源 IP/IP 段、目标 IP/IP 段、目标域名、UNC 路径、应用程序路径及来源/目标组合等方式进行灵活的配置，实现对来源目标的黑白名单配置，以绕过 DLP 分析。
23	内容识别技术	分类	系统应基于“数据分类”进行内容安全防护，支持引导用户对敏感数据进行分类，并根据分类结果制定 DLP 安全策略。系统应能够在事件和报告中展示数据分类分析结果，并通过数据分类呈现数据安全报告。
24		标签	系统应支持标签作为策略检测规则和数据分类规则使用，并能根据应用程序触发不同敏感内容打不同标签。同时，管理控制台应能展示标签内容及其操作历史。
25		关键字	系统应支持关键字和关键字对的管理，并能够进行精确匹配和自动匹配简体/繁体中文。关键字规则中的“精确匹配”功能需支持区分大小写。
26		正则表达式	系统应支持正则表达式检测内容，并提供常见的正则表达式模板，如手机号码、固话号码、姓名、地址等。
27		脚本	系统应预置身份证、护照、信用卡等常用数据检测脚本，并支持对源代码（如 C、Java、Python 等）进行准确检测，确保快速识别和保护敏感信息和代码内容。
28		指纹	系统应支持数据库和文档的敏感数据指纹学习，涵盖多种数据库类型和 ODBC 连接。支持本地文件和远程共享目录的指纹学习，提供 10%-90%相似度阈值调节的指纹相似度检测。支持增量和全量指纹学习、定时任务计划、反向指纹学习及离线指纹生成工具，确保数据泄漏防护和减少误报。
29		字典	系统应预置开箱即用的权重字典，能够识别常见敏感数据，包括国家领导人、政治言论、高管信息、法轮 X、技术方案、会议纪要、采购计划、网络安全、投资信息、简历等。系统还应支持自定义和导入字典，并提供字典搜索查询功能，方便用户在大量条目中快速定位和维护字典规则项。
30		智能学习	系统应支持对规范模板类文件的有效学习，防护业务敏感数据，确保类似文件内容自动识别，无需单独制定指纹策略。同时应支持正反向机器学习训练，提升识别能力，并智能检测潜在数据泄漏威胁。另外应该支持远程目录自动学习及结果导出，并配备数据聚类工具进行自动分级分类，优化 DLP 策略。

31		文件属性	系统应支持对文件名称进行检测匹配，并允许设置匹配阈值。系统内最少预置 800 种以上文件类型，并提供自定义文件类型创建功能。支持识别 WPS 加密“.dpt/.ppt”文件格式及 Hadoop ORC 文件格式，能够进行文件大小检测匹配，支持检测文件的所有者、修改日期、创建日期、访问日期等属性，以及主题、类别、标记、备注和最后一次保存者等信息。
32		数据聚类	系统应支持通过机器学习技术，将用户提供的大量无序文件样本按内容自动聚类，实现文档分级分类。聚类后的文件应支持指纹生成和智能学习，辅助更有效地制定 DLP 策略。
33		复杂检查能力	系统应支持多语言内容检测，涵盖中文、英文、泰文、俄文等主要语言（至少满足中文、英文），并具备对邮件正文、附件、发件人、收件人及邮件头的匹配检测功能。可以支持文档位置匹配检测，精准识别和处理 Office 类型文件（如 Word、Excel、PPT）中的页眉、页脚、正文及嵌入内容。此外还应支持基于数据大小规则的 DLP 策略控制，对 Web POST 表单数据和 Email 原文进行管理和限制，并支持对邮件附件数量及所有属性（包括附件名称）的检查匹配。
34		文件真实格式识别技术	系统应支持主流 Office/PDF 加密格式、ZIP/7zip/RAR 压缩格式，且支持最新的 RAR5 和 7zip 的全部四种压缩格式。能够检测多层文档嵌套中的泄露行为，发现任何一层文档中的敏感信息，并支持对通过更改文件名、后缀、压缩包后缀、转换文件类型等规避手段处理过的文件内容进行检查。
35		图片内容识别 OCR 能力	系统应预置高性能高精度 OCR 图片内容识别引擎，支持简体中文、繁体中文和英文的高精度识别，无需独立部署或另购。可以支持对常见图片文件及嵌套在 Office 文档和压缩包中的图片内容进行检查，包括 JPEG、TIF、TIFF、BMP、PNG 等常见图片格式。并至少提供三种识别模式以适应实际的检测需求：高效精确度低、效率与精确度兼顾、高精确度但效率较低。
36		点滴式监测技术	系统应支持在自定义时间范围内对累计达到告警阈值的检测技术进行监控，包括策略触发次数和违规内容触发次数。

备注：以上测试项目有任一项不满足测试标准，则 POC 测试不通过。

终端数据防泄漏功能测试内容

序号	测试功能	功能项	终端数据防泄漏功能测试内容
1	终端系统与管理	操作系统支持	系统应支持在 32/64 位 Windows XP/7/8/10/11、Windows Server、macOS 10.9 及以上版本，麒麟 Linux（国产化平台龙芯+中标麒麟）、UOS、CentOS 等操作系统上进行终端 DLP 部署。对所有的操作系统均需要支持监控和阻断能力，相关能力在不同操作系统上应具备一致性。（提供产品适配列表，并可在产品界面中看到对应类别的配置界面）
2		运行支持	系统应支持简体中文、繁体中文和英文操作系统，具备显示运行和隐藏运行（用户无感知）模式，在隐性模式下可在进程列表中隐藏进程信息，确保用户无感。同时，系统应支持在 Windows 安全模式下运行，允许管理员自定义终端阻断页面的提示语言和配置模板，定制公司名称和提示内容等信息。
3		安装用户的绑定	系统应支持读取登录 AD 用户的信息，也应支持读取企业内已部署的联软、360、H3C、iNode、天擎等终端软件（至少需支持联软）的用户信息作为管控和策略控制的依据，同时应支持手工绑定用户账号并对接 AD 进行密码验证，并在必要时允许清除已绑定的账号进行重新绑定。
4		卸载	系统应支持对终端的强制卸载，并清除系统残余文件，同时提供卸载密码保护功能，要求密码校验正确（支持提供全局密码和临时密码）方可卸载。可以提供终端远程申请卸载和离线申请禁用功能，允许管理端进行远程在线卸载和禁用的操作。
5		终端资源控制与保护	系统应支持对终端 DLP 使用的 CPU 占用、带宽、日志存储大小进行控制，避免过度占用操作系统主机资源。允许通过终端配置设置资源消耗能力，以适应不同应用场景下的计算机资源要求。系统应具备终端进程保护功能，防止用户强行终止，并支持保护终端安装目录及重要文件，防止被删除，同时应执行运行在安全模式下保护能力依然生效。
6		性能	各平台数据防泄漏保护能力需要保持一致，软件安装后，软件自身 Agent 闲时系统内存占用不超过 0.3GB，平均 CPU 占用不超过 50%。
7		终端信息	系统应记录所有注册终端的详细信息，包括主机名、登录名、IP、操作系统（OS）、同步状态、连接状态等，并支持展示终端的健康状态，记录终端的安装时间。系统还应允许管理员对离线终端或需要备注的终端进行手工备注，例如未加域的电脑。
8		终端位置判定	系统应支持通过服务器连通性、DNS 解析的域名地址、PING 连通性、IP 范围、DNS 地址等多种条件和逻辑组合判断终端所处位置，根据位置执行不同数据安全策略，并确保终端在离线状态下防护策略依然有效。
9	终端标签	终端文件标记	系统应支持终端文件的标记能力，能够通过多种手段为终端上的具有 meta 属性的数据文件添加标记，包括但不限于：基于终端数据发现任务自动为敏感文件打上分类标签，手动右键对单个文件或批量文件进行打标，对常见的 Office 程序在文件保存时弹窗提示用户选择对应标签，以及自动为从指定 URL 或文件共享下载的文件进行标记。
10		标签溯源	系统应支持在完成嵌入式标签操作后，当数据泄露事件发生时，登录管理控制台利用标签信息追踪。
11	数据传输内容审计	终端协议支持	系统应支持对通过 HTTP、HTTPS、SMB、SMTP、FTP、AirDrop 和 RDP 协议上传、下载的内容进行分析，并支持放行、阻断、确认动作，同时自适应 HTTP2 协议。
12		终端下载检测	系统应支持对通过浏览器下载文件和从外部共享文件夹中拷贝文件的行为进行 DLP 内容分析和策略匹配，防止敏感数据被下载到用户计算

			机上。
13		终端邮件客户端检测	系统应支持对使用 Foxmail、Outlook 等特定的邮件客户端发送的邮件进行内容检测，并支持放行、阻断、确认等操作。
14		终端 IM 检测	系统应支持终端上的 QQ、企业 QQ、微信、企业微信、Skype、Skype for Business、钉钉、阿里旺旺、TIM、飞秋、飞书、CoCall 等即时通讯软件（至少需满足 QQ、微信、企业微信）的聊天内容和传输文件进行检测，并支持放行、阻断、确认等操作。系统还应支持阻断 IM 图片发送、禁用转发功能，并能够记录聊天账号信息。对于触发策略的聊天内容，系统应能够截屏当前聊天窗口并上传作为证据。
15		终端打印检测	系统应支持对打印文件进行内容分析，预防敏感数据通过打印外泄，并支持放行、阻断、附加水印、确认等操作。水印应支持明文水印和暗水印。
16		终端应用传输控制	系统应支持对自定义应用程序的复制/剪切、粘贴、截屏、文件访问和水印内容进行分析，应用程序包括但不限于网盘、云笔记等具备外发能力的应用程序。在使用应用程序进行截屏时，系统应支持放行或直接阻断，并保存事件前后 N 张截屏作为证据。
17		外设数据传输检测	系统应支持对刻录至 CD/DVD 的文件、通过蓝牙传输的文件、拷贝至 USB 的文件进行内容分析，并支持放行、阻断、确认等操作。USB 拷贝允许对敏感文件采用个人密码加密操作，且支持记录并展示移动存储设备的实例 ID。
18		策略触发控制	系统应支持对通过所有终端通道发送的数据包括经过 Microsoft RMS 加密的文件进行敏感内容监控，当触发策略可以进行自动截屏并存储为证据。同时还应支持对终端数据的审批动作，通过 API 对接企业的审批平台，当文件被阻断时触发审批窗口实现终端审批。
19		IPv6 检测支持	系统应支持终端在策略和白名单中定义 IPv6 相关配置参数，适应 IPv6 环境下的流量检测需求。
20	数据发现	终端数据扫描发现	系统应支持对指定计算机和指定磁盘路径进行实时或计划定期的深度发现扫描，包括增量和全量扫描。在发现敏感数据后，系统应能够执行保护、隔离、自动标签等动作，并可以使用自定义脚本进行额外的动作处理。
21			系统支持通过终端监控实时控制发现任务的开始、停止和暂停操作。
22			系统应支持通过终端数据发现任务，将敏感文件保存到保险箱服务器端。
23	终端水印	终端水印	系统应支持基于终端配置启用/禁用屏幕水印，并具备隐性水印能力。隐性水印信息在用户截屏后完全不可见，但管理员可以通过登录控制台进行隐性水印信息的还原。
24			系统应支持应用水印，支持的应用包括 Office 系列、WPS 系列、MAC Keynote/Numbers/Pages、Notepad、Textedit、Preview、Adobe PDF、各类浏览器等（至少满足 Office 系列、WPS 系列、notepad），当且仅当文档应用包含敏感数据或者浏览器访问了指定网站，才显示水印内容。
25			系统应支持直接启用或对经过内容分析后针对敏感文档的打印水印，适用于常用的 Office、WPS、浏览器、图片、Notepad、Adobe PDF 等应用，既支持常见的明文水印、二维码水印，也可以在打印文件上以隐蔽方式随机分布水印信息，便于对员工打印的文件进行追溯。
26			水印类型应包括明文水印、二维码水印和点状水印，并提供详细的水印参数配置。其中，二维码水印应可通过微信、支付宝等应用扫描还原明文信息，点状水印可通过管理控制台进行反查。
27	其他控制检测能力	外设控制	系统应支持对多种外设的启用、禁用及只读控制，包括 USB 存储设备、MTP/PTP 手机、CD/DVD 驱动器,支持对 USB 蓝牙、USB WIFI、

			软驱、串口/并口、IEEE 1394 接口、PCMCIA 接口、红外功能、蓝牙以及 AirDrop（MAC）的启用和禁用控制。
28		Web URL 控制	系统应支持根据客户端访问的外部 URL 分类、URL 风险级别和 URL 风险类别（包括挂马网站、非法网站、黑客指挥中心、黑客工具等），过滤用户的 Web 访问请求，在发现风险时进行告警或阻断风险的 Web 访问。 支持对访问网站进行时间段控制。
29		操作系统代理控制	系统应支持对终端操作系统的浏览器进行代理设置锁定，同时支持指定 PAC 路径。
30		终端文件勒索检测	系统应支持定义终端诱饵文件，并检测对这些诱饵文件的修改、删除操作，记录勒索事件，检测和识别疑似勒索行为。
31		终端审批	系统应支持终端敏感文件审批外发能力，可设定规定外发的时间和次数。

备注：以上测试项目有任一项不满足测试标准，则 POC 测试不通过。