**敏感数据管控平台采购项目招标公告**

根据嵊州农村商业银行股份有限公司（以下简称嵊州农商银行或本行）统一部署要求，在遵循“公开、公平、公正”竞争的原则下，本行决定以公开招标的方式，对敏感数据管控平台采购项目实施招投标，现将有关事项说明如下：

1. **投标简介**
2. 招标单位：嵊州农商银行
3. 招标项目：敏感数据管控平台采购项目
4. 投标截止时间：2024年11月25日17︰00时
5. 保证金截止日期：2024年11月25日14:00时
6. 开标地点：嵊州农商银行总行大楼
7. 投标费用：投标公司因参与本项目招投标活动，所产生的费用由投标公司自负。
8. 联系人：王凯权

联系电话：0575－83903665

地址：浙江省嵊州市官河路398号

**第二章 投标须知**

1. **投标单位资格及要求**

1.参与本项目投标的公司，必须在中华人民共和国境内注册，注册资本人民币200万元（含）以上，具有独立承担民事责任和履行合同能力，不允许以挂靠形式参与本项目投标，公司中标后不得以任何形式转包、分包给其它供货商。以上情况一经发现核实，本行有权单方面取消中标资格，并保留追究其法律责任的权利。

**2.所有参与投标的公司，不得有联合投标、串通投标或无故退出投标（未得到本项目招标小组同意）行为，中标前不得用本行名义在市场渠道商家处进行货物报备。一经发现投标公司存在上述行为，将永久取消该公司参与本行组织的招投标活动资格。若在事后发现中标公司存在上述行为，立即取消中标人资格，并追究相关公司的法律责任。**

3.投标公司必须遵守相关国家法律、行政法规，具有良好信誉和诚实的商业道德；在近三年内的经营活动中没有重大违规违法记录；**需提供近三个月内信用中国、中国政府采购网截图证明并加盖公章**。

4.参与投标的公司，须在**保证金截止日期前向本行缴纳投标保证金人民币贰仟元整（¥2000.00）**，缴纳的投标保证金在本项目定标前一律不予退还。开标后，中标单位投标保证金在合同正常签订后退还，其余投标公司在未违反本招标文件条款的基础上，本行将在15个工作日内退还投标保证金。投标保证金及合同保证金一律不计利息。保证金户名：浙江嵊州农村商业银行股份有限公司，保证金账号：89300001262199006208。

5.投标公司应具备较强的服务能力，拥有较强的专业技术队伍，确保现场服务及时响应，并按投标承诺书要求承诺。

6.投标公司应按本行要求对采购的产品（或服务）进行安装调试及免费培训，提供技术支持及详细的设备档案资料，并承担保密责任。

7.本项目标的物的保修及技术服务必须符合本行规定要求。

8.本项目标的物应具有升级功能，若国标、省行标准有所变动，中标单位应免费提供技术升级。

9.本项目款项一律采用转账方式结算。在完成项目合同签订、全部标的物到货并经验收合格后，本行在收到项目增值税专用发票后向中标公司支付合同总价的30%款项；完成安装、调试并经本行项目验收合格后，本行向中标公司支付合同总价的60%款项；验收后3个月内无软硬件问题，本行向中标公司支付合同总价的10%款项。

10.本项目中标的物的技术标准必须符合相关文件标准，有相关部门颁发的生产许可证等。若中标的产品无法通过标准验收，中标单位应无条件替换不低于该档次的设备，其造成的损失由中标单位承担，本行概不负责，且替代产品不重新报价。

11.投标企业在投标本项目时，对本项目标的物必须**提供原厂保修服务并承诺提供产品升级、维修服务**。

**12.在投标截止时间未收到投标公司投标资料，本行视为投标公司自动放弃投标权利，已交纳的投标保证金不予退还。**

**13.投标有效期为投标截止时间后60天。**

14.满足本招标文件规定的其它要求。

**二、交付要求**

1.本项目涉及的相关产品实施所需的辅材（如光纤线、网线、上架螺丝、扎带等）及工具（螺丝刀、剪刀、设备调试工具等）均由中标公司提供，如需现场或电话调研可与项目联系人对接。

2.所有产品相关配置、调试、培训工作由中标公司完成，本行科技人员负责配合工作。

3.所有与本次项目相关的光纤线、网线、电源线必须按照本行科技要求进行线路整理及标签制作工作。

4.实施完成后按本行科技部门要求提交包括但不限于实施方案、验收报告、验收单、竣工报告。

5.以上为项目交付验收要求，中标单位须严格按照上述要求进行项目实施。

**三、投标文件内容及要求**

（一）要求

 1.投标公司应仔细阅读招标文件的所有内容，按招标文件的要求提供投标资料，并保证所提供的全部资料真实有效。

 2.详细的投标报价清单，需严格按照本招标文件“附件”项目填写,不得更改格式。

**3.投标公司须提供本公司章程（投标截止时间前一个月内）、营业执照复印件（三证合一或五证合一）、法定代表人身份证复印件、法定代表人授权委托书、投标人身份证复印件、投标承诺书、项目案例、厂商对本项目出具的《项目授权函》；投标公司意向中标后，在项目验收前10个工作日内必须提供产品（或服务）厂商针对本项目出具的《产品质保函》，逾期不提供将按违约处理，本行有权进行追责。**

 **4.投标公司认真测算项目施工过程中所需的相关辅助材料和费用，并在投标报价时一并考虑，项目施工过程中不再单独结算运输、安装、调试、住宿、就餐等费用（设备安装包括设备参数配置、设备上软件系统安装调试、外接设备支持调试及现场服务等）。**

 **5.设备安装时间计划和周期须符合本行要求。**

6.所有提供的资料都采用标准A4纸质，每份材料都必须加盖企业公章，若某份材料有多张A4纸组成，需在每页标明页码，并一起加盖骑缝章。

 7.若缺少本招标文件要求资料，该投标资料将作废标处理。

（二）报价说明

1.除招标文件中另有规定外，计量单位为我国法定计量单位。

2.投标报价及货款一律使用人民币计算。

3.投标报价为含税(包括运输、安装、调试、住宿、就餐等一切其它费用)，是指标的物到达本行指定地点正常使用后的开票价格。

（三）投标文件递交

1.投标公司应将投标资料装订成册，装入统一监制的文件袋内，文件袋的接缝处用薄纸粘封，并在封条与文件袋的接缝处加盖法定代表人印章及法人企业公章。文件袋和投标封面应写明招标单位、项目名称、投标公司名称、地址、邮政编码、联系电话及联系人，并加盖法人企业公章及法定代表人印章。

**2.参与投标的公司需另行制作投标资料副本一份，副本投标材料需等同投标资料正本，一旦正本与副本有差异，以正本为准**。

3.投标人应在招标文件规定的截止日期前将密封合格的投标资料送至嵊州农商银行，同时提供保证金打款证明文件。标书的投递手续，如：电报、电话、传真概不受理。

（四）投标文件的修改和撤回

投标公司在规定时间递交投标文件后，在截止时间前征得本项目招标小组认可的情况下，可以书面形式提出补充、修改或撤回其投标资料，在投标截止时间后不得修改或撤回投标资料。

**三、开标、评标、定标办法**

（一）开标

1.招标单位将择日在嵊州农商银行总行举行开标；本次招标活动不邀请投标公司参与开标。

2.招标单位宣读招标小组成员名单，招标小组成员了解招标项目情况，讨论确定评标、定标原则和办法。

3.招标小组核查投标资料的密封状况，在确认无误后，按投标公司报送的投标资料先后的逆顺序进行拆封唱标。

（二）投标文件初审

1.对投标资料进行初审，内容以投标资料为准，主要检查投标资料是否符合招标文件的要求，内容是否完整，资料签署是否齐全。

2.投标公司的投标资料出现与本行招标文件要求不相符的内容，该投标资料将被作废。有下列情形之一的都按废标处理：

（1）投标资料缺少招标文件中规定必须提供的内容或要求。

（2）投标资料中附有本行不能接受的条件。

（3）投标资料中填写报价单等重要信息字迹模糊无法辨认的。

（4）投标资料中存在2份(含)以上同类报价单，或同一张报价中对相同标的物2次(含)以上报价，且未书面说明哪份有效。

（5）更改报价清单（附件内容）格式、内容。

（6）投标资料中有未加盖公章或法人代表或授权代理人(附授权书)印章的材料。

（三）评标、定标

1.评标依据

本项目评标以《敏感数据管控平台采购项目招标文件》作为评议的主要依据。

2.定标

本行招标小组将认真审阅、分析，各投标公司的有效投标资料，根据招标文件要求提出评标报告和中标候选人，评议结果上报总行，择优确定中标公司。

**第三章 合同签订与执行**

**一、合同签订**

本行将及时以书面形式通知根据招标文件核准的中标公司，中标公司在接到通知书后，应按中标通知书上规定日期和招标文件的条款与本行签订本项目采购合同。

 1.招标文件（含附件）、中标公司的投标资料均为签订采购合同的依据。

 2.本行在授予合同时有权对产品（或服务）的数量和服务予以适当的增加或减少。

 3.项目产品费用按货物实际到货并验收合格情况进行结算。

**二、合同执行**

 1.本行及中标公司双方严格按合同条款执行。

2.因特殊原因不能按时交货，中标公司应在合同规定的交货期限内提前与本行进行沟通，征得本行同意后可顺延。

3.如需变更合同标的物，中标单位须和本行设备采购领导小组办公室协商之后再定。

 4.无特殊原因中标公司拒不履行合同条款，本行可有权单方面取消本项目采购合同，并将采取法律手段追究中标公司的违约责任。

**注：1.投标公司在获得本文件后，请仔细阅读每一章节，有不清楚情况请及时联系本行联系人；2.本文件最终解释权归嵊州农商银行所有。**

附件：

1.敏感数据管控平台采购项目报价清单

1. 投标承诺书
2. 标书符合指引（放置于首页，如有目录，则在目录之后）
3. 投标单位法定代表人（负责人）授权书
4. 功能明细清单

嵊州农商银行

2024年11月1日

附件1：

**敏感数据管控平台采购项目报价清单**

投标公司名称（签章）

|  |
| --- |
| 敏感数据管控平台采购项目 |
| **序号** | **名称** | **产品型号** | **配 置 描 述** | **数量/套** | **单价（元）** | **合计（元）** |
| 1 | 敏感数据管控平台 | **UCSS-1100-VM** | **SecGator安全鳄系统UCSS-1100-VM**主要功能：敏感数据集中管理平台 ：敏感数据定义、数据资产盘点、统一策略分发、定期报表统计、敏感数据流转集中展现、网络敏感数据资产盘点、数据库合规扫描等能力；对存储文件共享SMB/NFS/FTP等服务器、Domino Lotus、Sharepoint、邮件Exchange、Office 365 Online、Outlook PST、阿里OS，S3等站点数据资产盘点，对常用关系型数据库，sql server, pgsql，DB2、MYSQL、oracle、MongoDB等表单合规扫描等能力；一年原厂商保修服务。 | 1 | .00 | .00 |
| 2 | 敏感数据管控端点 | **UCSC-WIN/MAC****/LNX--SW** | **SecGator安全鳄系统UCSC-WIN/MAC/LNX—SW****安装在windows/MAC/信创终端上**功能描述：PC端落盘数据资产盘点、数据合规扫描、个人隐私专项检查、外包人员敏感敏感管控、敏感数据外发管控等能力；一年原厂商保修服务。 | 300 | .00 | .00 |
| **投标总金额** | ***请在此处填写人民币大写投标总金额*** | **¥ .00** |

附件2：

**投标承诺书**

**投标单位服务承诺：**

**1.已仔细阅读本招标文件每一章节内容，知悉项目投标要求。**

**2.在标的物服务期内提供7\*24小时电话支持服务；现场技术服务（2小时内达到现场）；项目实施期限内出现产品故障，投标单位免费更换。**

**3.产品到货周期承诺。**

**4.产品质量保证承诺。**

**5.提供一年原厂维保升级服务。**

**注：**各投标公司在投标时，须特别关注标的物质量和保修、运维服务要求条款。若公司在中标本项目履行合同期间，发生下述不良行为，本行有权单方面终止合同执行，并有权依法追究相关损失。

1.中标公司在产品（或服务）供应期间以次充好（本行将对设备进行不定期抽样送检）；

2.在保修、安装、调试、培训、运维服务期间未能按本行要求提供服务或服务不良，经本行领导或职能部门与公司方主要负责人进行谈话协商，仍然无法达到服务要求。

3.服务期指合同签订日起至合同约定的维保或服务到期之间的时间。

法定代表人（签章）：

日期：年月日

附件3：

|  |
| --- |
| **标书符合指引** |
| 序号 | 投标要求 | 是否符合 | 标书页 |
| 1 | 注册资金不少于200万元 |  |  |
| 2 | 无近三年经营活动重大违规违法记录 |  |  |
| 3 | 公司章程（最新） |  |  |
| 4 | 营业执照复印件 |  |  |
| 5 | 法定代表人身份证复印件 |  |  |
| 6 | 投标单位法定代表人（负责人）授权书 |  |  |
| 7 | 投标人身份证复印件 |  |  |
| 8 | 投标承诺书 |  |  |
| 9 | 厂商项目授权函 |  |  |
| 10 | 敏感数据管控平台采购项目报价清单 |  |  |
| 11 | 项目案例 |  |  |

附件4：

投标单位法定代表人（负责人）授权书

致：浙江嵊州农村商业银行股份有限公司

（投标单位全称）法人代表授权（全权代表姓名）为全权代表，参加贵行组织的招标活动，全权处理招标活动中的一切事宜，我司对授权人的签名负全部责任。

本授权书有效期为　　天。

投标单位（公章）： 法人代表签字：

年月日

附件5：功能明细清单

|  |  |  |  |
| --- | --- | --- | --- |
| **功能名称** | **功能项** | **功能子项** | **功能说明** |
| **平台管理能力** | 管理平台 | 界面 | **\***支持信创环境部署及行内软件化部署，平台可对网络防泄漏设备、邮件网关设备、终端敏感数据扫描设备、应用数据防泄漏设备、API级别检测等策略管理与事件证据管理，为后期统一数据安全架可平滑扩容，平台支持不少于2000终端负载 |
| 语言支持 | 多语言界面 | 支持IPV4及IPV6环境部署，支持虚拟化部署，产品系统应支持中英文界面，根据登录用户的设置自动进行显示 |
| 权限分离 | 三权分立 | 产品应能通过管理平台后台配置启用三权分立，提供多权分立角色管理，各角色之间的功能没有交叉，每一种角色类型都有预置的管理员，包括系统管理员、事件管理员、审计管理员、安全管理员等，产品应支持基于实际需要的权限分配，结合用户分组和分级进行灵活定义 |
| 用户管理 | 用户目录集成 | 产品应支持集成的第三方系统：AD、Generic Ldap等，或者支持定期及手动方式从第三方同步用户信息 |
| 自定义组织架构 | 产品应支持自定义组织架构及导入导出功能，包括自定义用户、用户主管、部门、部门主管、计算机组织架构信息，产品应支持基于用户目录及自定义组织架构定义用户目录组，实现已有系统用户信息及自定义用户的重新分组，用于策略通知、事件审批及告警通知 |
| 敏感数据扫描 | 共享文件扫描 | 包含对SMB/NFS/FTP等远程文件服务器存储文件做扫描发现，并对相应扫描的敏感数据做审计、删除等动作 |
| 远程目录标签能力 | **\***远程目录SMB/NFS/FTP等远程文件服务器存储文件做扫描发现可根据文件内容打标签，例如三级文件打三级分类标签，可以根据标签级别做管控 |
| **\***远程目录SMB/NFS/FTP等远程文件服务器存储文件做扫描发现可根据文件内容删除标签，例如已经打三级标签，平台可进行定期扫描自动删除标签 |
| 云文件扫描 | \*支持远程文件阿里OS，S3文件类型扫描发现能力，并对相应扫描的敏感数据做审计等动作； |
| 远程站点扫描 | **\***支持远程站点 Salesforce、Domino Lotus、Sharepoint、OneDrive、Exchange、Online Office 365、Outlook PST并对相应扫描的敏感数据做审计及脚本动作 |
| 数据库扫描 | 管理平台具备对数据库扫描发现能力，包含对常用关系型数据，DB2、MYSQL、oracle、PostgreSQL、SQL server、sybase\_ase、teradata、informix等常见关系数据库中的敏感数据并记录分布 |
| 扫描设置 | 支持数据库扫描基础表、视图表 |
| 支持扫描进度呈现，数据库随机扫描2000行，或指定扫描 |
| 支持数据库发现任务定时执行，一次/每小时/天/周/月/持续性，以及支持暂停时段扫描 |
| 支持扫描进度展示 |
| 策略管理 | 策略规则灵活性 | 产品应支持多个策略规则的任意条件组合（与、或、必选项、M选N），及对来源/目标精确匹配，多个特定规则条件进行例外处理 |
| 产品应支持针对策略设置不同动作，如投递、阻断、弹窗确认、审计、审批等动作 |
| 策略导出/导入 | 产品应可以对策略进行模板模式的实时导出/导入，方便运维管理 |
| 策略模版策略模版 | 系统支持不少100条脚本策略，预置脚本策略须包含源代码、银行卡等检测脚本 |
| **\***策略模板平台预置不少于500条策略模板同时包含不少于15条GDPR法规数检测据模板、压缩文件层数、真实文件类型检测模板等 |
| **\***个人信息系统预置国内手机号欧洲国家保险号、英国银行帐号、俄罗斯个人养老帐号、港澳通行证、欧盟银行卡号等正则内容 |
| 事件管理 | 事件及日志 | 产品应支持自定义筛选条件(例如，部门，组织单元，组，文件名称，策略名称，详细信息等)，支持筛选条件的灵活调整，也可直接从目录服务中导入组、组织单元等筛选条件，支持用户自定义事件查询条件实现对事件的查询和报表统计 |
| **\***系统维护集中、简单，日志清晰.明确，其中证据预览功能仅显示命中详情上下文信息，不暴露全文，避免造成二次泄漏，在一个事件产生时，系统可以自动的发送邮件警告给用户、用户上级，管理员。邮件的主题，信体等内容均可以定制，支持通过API方式读取事件证据文件 |
|  |
| **\***支持命中敏感信息：身份证、手机号可脱敏感呈现在事件列表或指定报告中，避免二次泄漏 |
| 日志集成接口 | 支持将泄露事件、日志发送至其他日志或大数据平台，支持Syslog与SIEM(Splunk/ArcSight/Qradar/Nitro)，日志类型至少包括：泄露事件、审计日志、系统日志等 |
| **\***支持事件API，管理员可把此API集成到第三方平台（运维管理平台），可通过API方式调取天空卫士的终端事件，通过第三方平台进行多源、多维度的统计分析 |
| 以个人为中心的风险评估报告 | **\***可以针对个人风险值、个人风险排名、个人事件数据统计等生成以人为中心的报告 |
| 文件追溯 | **\***基于数据泄露事件中的标签文件唯一ID（例如标签）和文件MD5，对检索到的数据泄露事件进行文件的流转溯源展示，可展示该文件经过终端、网络、邮件等流转视图 |
| 完整的事件历史 | 产品支持在一个事件产生时，系统可以自动的发送邮件警告给用户、用户上级，数据泄露事件管理员，邮件的主题，信体等内容均可以定制，能查看完全的事件历史，包括备注，事件经过哪些处理，所有过程 |
| 事件安全管理流程 | 产品应支持为事件添加备注、添加标签、更改安全级别、删除事件和设置忽略状态 |
| 支持自动备份功能，支持定期备份，可备份至指定服务器 |
| 产品应支持事件状态（新/进行中/关闭/误报/提级）更新功能 |
| 总匹配统计 | 产品应支持违规内容总匹配次数展示，排名； |
| 自动邮件通知 | 产品应提供针对敏感事件发送邮件通知，如发送事件告警给用户、用户上级，数据泄露安全管理员。邮件的主题，信体等内容均可以定制 |
| 报表管理 | 定制报告 | 产品应提供预置及定制趋势分析的报告，包括：支持显示一周内的事件趋势图、支持显示安全等级事件趋势图、支持显示策略事件趋势图、来源事件TOPN、目标事件TOPN、来源总匹配TOP20，产品应提供设置定时事件报告发送给特定的管理人员 |
| 预置报告模板 | 系统预置长用周/日等统计报告 |
| **终端基本功能** | 终端系统与管理能力 | Window系统 | 支持Windows 7/8/10/11 32位及64系统，server2012/2016等系统 |
| 苹果系统 | **\***支持macOS 10.12~14终端环境部署; 支持Apple M1,M2芯片设备内容识别与阻断 |
| 信创系统 | **\***支持国产操作系统(麒麟OS \统信）终端部署，包括X86与ARM架构及指定版本ubuntu系统 |
| 推送及部署管理 | 支持通过SCCM/Landesk/JAMF/天擎等管理软件进行终端的推送 |
| 支持终端离线（如离开公司内网）时所有终端防护策略依然有效（离线可控） |
| 终端用户与自定义组织架构手动匹配绑定，绑定后终端用户有唯一标识，不会随着用户主机名变更导致日志无法定位 |
| 性能管理 | 支持终端CPU占用、带宽、日志存储大小控制 |
| 数据内容识别能力 | 分类 | 产品应支持基于“数据分类”的内容安全防护，此功能主要是引导用户先做敏感数据分类，然后再根据数据分类来做数据防泄露安全策略，同时将数据分类分析结果在事件、报告里呈现，并且以数据分类来呈现数据安全报告 |
| 关键字权重 | 制定关键字词组权重包含监控、银行、机密，信息每个计10分钟，银行计分5分，当文件内容内容含权重关健词达25，可根据权重信息管控 |
| 正则表达式 | 产品应支持正则表达式检测内容。要求应提供常见的正则表达式，如手机号码、固话号码、姓名、地址等 |
| 指纹 | 产品应支持对常用文件系统office/pdf类进行非结构化数据提取指纹，同时对代码类及数据库结构化及半结构化数据提取数据 |
| 字典库 | 产品应具备预置开箱即用的权重字典识别常见敏感数据。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、投资信息等、简历等，并支持自定义、导入 |
| 文件类型 | 产品应预置超过1000种文件类型支持，并支持通过文件类型工具进行自定义文件类型创建 |
| 文件大小 | 产品应支持对文件大小进行检测匹配 |
| 附件数量 | 产品应支持对邮件的附件数量进行检查匹配 |
| 智能学习 | 产品应能够有效学习一些有规范的模板类文件，有效防护此类业务敏感数据。学习以后类似的文件内容会被正确识别，不需要再单独做指文策略。支持正向、反向机器学习训练以提高识别能力 |
| 文件属性 | 产品应支持针对文件所有者、修改日期、创建日期、访问日期，文件名称等属性做识别 |
| 数据聚类 | 产品应支持通过机器学习等技术，将用户提供的大量无序文件样本按照文件内容自动进行聚类，帮助自动进行文档分级分类，聚类后文件可以进行指纹、智能学习等，辅助更有效的数据防泄露安全策略制定。 |
| 文档位置匹配 | 产品应支持文档匹配位置检测，针对包含页眉、页脚、正文的文件，如Word、Excel、PPT等Office类型文件 |
| 数据校验识别技术 | 产品应支持比正则表达式更精准的检查方式，支持对数据的有效性进行验证。如身份证号，中国银行卡号（包括信用卡号）进一步降低误报 |
| 指纹导入导出 | 产品应支持指纹导出和导入，并支持对已完成的指纹任务直接导出指纹库 |
| 点滴式流量检测 | 策略对应多条分类\对象\目标\动作、“点滴式”泄漏防护等手段、提供在一定时间内根据命中次数，不同做不同响应动作例如1小时命中5次审计，4小时命中10次邮件通知，24小时命中14次隔离阻断等动作； |
| 离线指纹工具 | **\***产品支持离线指纹生成工具，用户部门可以使用该工具对重要敏感数据进行离线指纹学习，管理员仅需将生成的指纹导入到系统中即可 |
| 修改后缀 | 产品应支持对更对改文件名、更改文件后缀、更改压缩包后缀、转换文件类型等常见规避手段处理过的文件内容进行检查 |
| 压缩层数检测 | **\***支持外发文件压缩包层数检测，例如大于5层无论是否含有敏感信息阻断 |
| 终端数据扫描 | 支持终端磁盘文件数据进行按安全策略进行深度发现扫描，发现存储在终端上的违规数据 |
| 支持对终端扫描任务实时控制（开始、暂停、停止） |
| 支持终端数据扫描计划任务定期扫描，支持增量与全量扫描 |
| **\***支持终端扫描敏感数据后进行保护、隔离、根据文件扫描内容打相应级别标签、第三方自定义脚本动作 |
| **\***支持终端扫描敏感隔离至文件保险箱，本地隔离后可根据需求还原被隔离的敏感文件 |
| 通道审计 | 支持终端HTTP/HTTPS/SMTP/FTP/SMB协议级(不限制浏览器或应用程序)共享传输的内容检测与拦截阻断 |
| 支持Foxmail、Outlook等邮件客户与Web客户端外发内容的检测与阻断 |
| **\***支持终端QQ、微信、钉钉、企业微信、飞书、飞秋,skype等即时通讯聊天发送消息文字需根据敏感内容审计、弹窗确认、阻断；支持获得接收和发送人员信息，支持自动截屏保留证据 |
| **\***支持终端QQ、微信、钉钉、企业微信、飞书、飞秋,skype等即时通讯发文件需根据敏感内容审计、弹窗确认、阻断、审批等动作；支持获得接收和发送人员信息，支持自动截屏保留证据 |
| 支持对USB文件传输敏感文件时确认、自主加密、删除动作 |
| 支持百度网盘，WPS，腾讯会议，向日葵等应用程序传输敏感文件时审计，阻断，弹窗确认等动作 |
| 支持对自定义应用程序的复制/粘贴、截屏、文件访问内容分析与阻断 |
| 终端水印技术 | 支持终端打开文件时依据内容审计结果动态在应用程序窗口内显示屏幕水印 |
| 水印技术 | 支持终端明文水印、二维码、矢量水印、暗水印（打印） |
| 支持屏幕隐性水印(暗水印)，在用户截屏前完全不可见水印信息，在截屏后通过预置工具还原 |
| 支持打印文件根据数据安全策略对敏感文件添加明文水印以及隐性水印，以追踪敏感文件打印 |
| 支持配置水印内容，包括主机名、IP/MAC地址、登陆账号、日期时间及自定义显示内容 |
| 标签技术 | 分类标签及指纹标签 | 支持用户端分级分类标签定义功能，支持终端用户手动方式右键属性标记分类标签，支持终端用户手动方式右键属性标记指纹标签 |
| **\***分类标签具有唯一性，打上标签的文件具有不可能修改能力同时对文件本身无影响 |
| **\***支持数据扫描发现对存量敏感文档根据数据内容策略进行自动批量设置分类标签以辅助数据安全治理与文件分类分级 |
| **\***支持应用程序自动打标签，如针对关键应用程序所产生的文件自动打上标签。 |
| **\***支持基于URL/UNC路径标签，如从业务系统URL或者关键共享存储UNC地址下载的文件自动打上标签。 |
| 支持标签显示在文档页眉/页脚，协助管理员进行文档标级，如（一级、二级、三级）、（绝密、机密、秘密、公开）； |
|  |  | 勒索攻击检测 | **\***终端文件防勒索用于控制用户或进程能否对指定的文件路径和文件进行读取、修改、删除等操作，防止非授信进程例如勒索软件、病毒、木马等对授信路径和文件的加密、篡改、删除等行为。 |
|  | 防勒索攻击 | 文件保险箱 | **\***终端发现扫描支持备份至文件保险箱，在遇到勒索攻击等灾难性数据丢失事件后，用户可以一键选择最近三个版本中的任何一个版本将数据恢复到本机。 |
|  |  | URL分类检测 | 支持控制web终端访问的web网站，根据post/put/get等http协议访问控制，同时员工访问URL情况根据分类进行统计 |
|  | URL分类检测 | URL安全检测 | **\***支持对终端web访问的URL安全性进行评估及控制 |