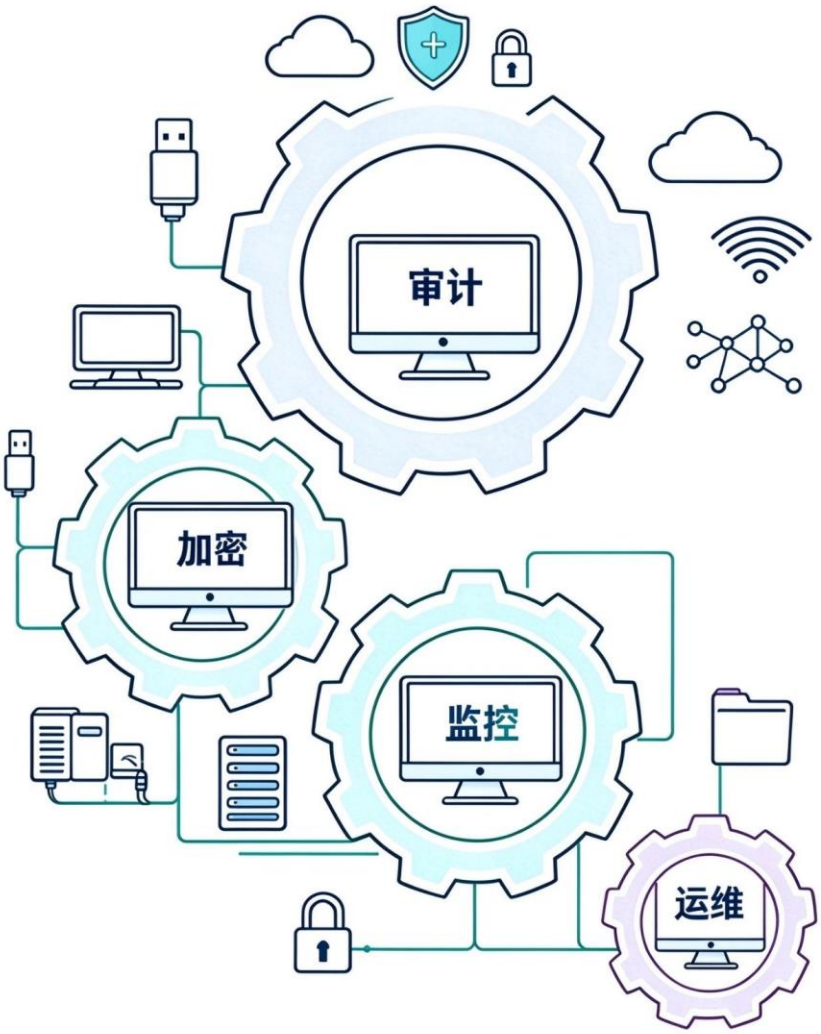
域智盾软件®

域智盾软件
数据安全解决方案白皮书

Technical White Paper on Data Security Solutions



河北中视新研软件开发有限公司

修订记录

本白皮书为技术文档，随产品版本迭代与行业实践更新而修订。修订记录如下。

版本	修订日期	修订内容	编制
V1.0	2026 年 11 月	首次发布，确立数据安全防护的场景化框架、功能分层、实施路径与实践观察	域智盾软件运营部

CONTENTS 目录

修订记录 2

序　言 5

一、行业现状 6

1.1 真实事件 6
1.2 数据安全趋势 7
1.2.1 从“保护系统”到“保护数据本体” 7
1.2.2 从“合规驱动”到“合规与业务并重” 7
1.2.3 从“边界防护”到“终端与身份并重” 8
1.2.4 从“单点工具”到“一体化平台” 8
1.2.5 从“事后追责”到“事中阻断与事前预警” 8
1.3 面临新挑战 8
1.3.1 数据分布失控 8
1.3.2 外发通道泛滥 8
1.3.3 内部人员风险上升 8
1.3.4 加密与效率的矛盾 9
1.4 数据安全新思路 9

二、方案介绍 10

2.1 版本 10
2.2 功能分层 10
2.3 系统架构 11
2.3.1 管理端界面 11
2.3.2 客户端界面 11
2.3.3 服务器端 12

三、方案概述 12

3.1 离职、转岗、外包 12
3.2 随手外发——微信、邮箱、U 盘、网盘 13
3.3 手机拍照泄密 14
3.4 误删、勒索与设备损坏 15
3.5 出差、居家与驻场 15
3.6 功能与场景对照 16

四、方案亮点与资质 16

4.1 方案亮点 16
4.1.1 资源占用可控 16
4.1.2 易用性强 17
4.1.3 完善的审批流程 17
4.1.4 完全本地私有化部署 17
4.1.5 专属工程师服务 17

4.2 资质与荣誉 *17*

五、常见顾虑与回应 **18**

六、实践案例 **19**

案例一：汽车零部件集团 19

案例二：金融科技公司 20

七、 未来展望 **21**

版权说明 **22**

免责声明 **22**

序　言

当前，数据资产的承载形态与流转边界，正在发生根本性变革。十余年间，企业数据不再局限于封闭机房内部，逐步扩散至员工笔记本、研发工作站、生产终端、移动设备、协同平台及各类云服务之中。同一份业务资料，可同时流转于邮件、即时通讯、共享存储、纸质打印载体，多副本分散流转已成常态，数据安全防护边界，从传统机房围墙下沉至每一台业务终端。

与此同时，国内数据安全法治体系持续完善：

- 2017 年 6 月 1 日《中华人民共和国网络安全法》开始施行，明确网络运营者安全保护主体责任；
- 2019 年 12 月 1 日《网络安全等级保护基本要求》（GB/T 22239）正式施行，将数据保密性、完整性、日志审计留存纳入测评指标；
- 2020 年 1 月 1 日《中华人民共和国密码法》正式施行，对商用密码应用实施规范化管理；
- 2021 年 6 月 10 日《数据安全法》通过，确立数据分类分级管理制度，对重要数据处理主体提出组织、人员管理要求；
- 2021 年 9 月 1 日《关键信息基础设施安全保护条例》正式施行，压实重点行业运营主体安全责任；
- 2021 年 11 月 1 日《中华人民共和国个人信息保护法》正式生效，规范个人信息全生命周期处理规则。

这些法规的共同指向，不是让企业多买一套产品，而是要求企业能够回答三个问题：

- 数据分了几级？
- 每一级由谁负责？
- 发生事件时依据什么判断？

这三个问题，靠一份制度文件回答不了，必须靠技术手段沉淀下来的记录回答。本白皮书初衷，是因为在实践中反复看到一种错位：不少企业在数据安全领域持续投入，但防护资源的投放位置与风险发生点位并不匹配。有鉴于此，本白皮书不做功能巡礼，从真实事件入手，介绍方案分层、界面结构、解决方案、相关资质、发展趋势。

一、行业现状

1.1 真实事件

数据安全的风险来源大致分两类：外部攻击者和内部人员。以下是两个公开报道过的事件，之所以被反复分析，不是因为损失金额大，而是因为攻击路径简单到几乎每家企业在自己的环境里都能复现。

案例一：全球教育平台 Canvas 遭黑客攻击

时间：2026 年

涉及机构：美国 Instructure 公司旗下的 Canvas 学习管理系统

泄密规模：黑客组织“闪亮猎人”声称获取了近 9000 所学校、超过 2.75 亿人的数据。

事件概况：2026 年 5 月，正值全球多所高校期末考试季，Canvas 平台遭遇网络攻击，服务一度中断。黑客声称窃取了用户名、电子邮箱、课程名称及选课信息等，并以此勒索。尽管核心教学数据（如作业提交记录）未受影响，但此次事件波及麻省理工学院、悉尼大学等全球众多知名学府，导致师生无法正常登录平台，引发了教育界对核心教学系统脆弱性的广泛关注。



4 新闻背景 环球时报 第6806用 2026年5月11日 星期一

近九千所学校受到影响 两亿多人数据或遭窃取

知名网络教育平台遭黑客攻击

本报驻澳大利亚特的记者 白 晓

知名网络教育平台Canvas近日遭学黑多攻市，服务一段中断，会球近9020年使用医学台的学校会到影响，目台Canvas已较受访问。

综合《据华报》，其取杜等美鞭设道，开发Canvas平台的美国Instructure公司在5月1日重贡“由倪哪将卖阳教网骆政市”。多为“闪亮猫人”的黑系组所声关对此次攻市事件金品。“勒索软卅亲网田陈平台”3日拉露的教未信显示，该国客银闪神已新浪在9000所学校细过205亿人的敢网，盟学组视师，全国学校未能在6日前安什裁会，教厕可综会关涸麻，随后，镇国以又蜡长了最沿斯舰，并猎示缪分学校已有共权敏，伏隋展开投间，Imkcuchnn公司首格执行宗委系。不能分子对不使用榄术进行了系统股校的时间。美国的的校网包够用户名，电子多何地址，重要名称，这书信电以及育仓内谙等，其心数学数据，这话理耙内等，作业来交记录以及账卒台能优已学受到影响，美国联剂语盖易（FNI）5月正主，读机中国了解设垦平台的服务中断济识，并蹋汉轰校睡生天持际交、学持本校发市的勿方徒引，1田猴碉，“网统计骗分子台合多大学教杆密已学院了被警校挺，以此从受莠者发生敞家钱财”。

美国首校电讽新闻网（CNN）称，Canvas已学同应建人名球众多斑校的日纳科学，生会学陈打均1000万名名胚用户，A Canvas上，美生可以没轩教宣会科，提步作业，在掏成抽以及参加参试，弃合员工学院学生文砖役·输交原，参校们天法使用Canvas公告动施后，正忙童麦投学生的电子特行地址。“这个同活县名网和学生在菲就之外联系的重要申间，直当构投们开泊平忙设计建设丧们的部瞬时，我才名识绕大学对它的校据已经忱么要了。”

参标社养，5月7日，本全珠阻用内。不少使用Canvas平台的大学都报告学生发生在问题，当天教间，Instructure公司称按员了大学分服务，但一些学校羌生尝安全风路仍部斐舰止学生和发师防问Canvas平台，一名美国等伦比亚大学学生展示，皮木手生中斯次生生，“据不会计资前酐照”，益多学生网认学的未的共板活动中推身，王要题人妥习的考试复习所行，施分学生的新卡复习舰习可能交异影响。

澳大利亚恩尼大学是使用Canvas平台的大学之一，《啊报报》箭的记荤了利到，该及学生直骑白使时何从日上等仍无法登录Canvas平台，这一机况一直教据到9日股受时代。服务中新如间，学生无生寇系校平台仔何内容，无注上作们龈或下饺馍杵。教据逃无法动问演平台，显尼大学10日发布通知作，游师设计利按国网网柱安会办公拿建义。相关平台已建受全面评例，当创从干安全状态。显尼大学教校长乔史妮·建筑在会学生的酬件中表示。目前设有行何证能裹明相生的脓癌被据妆生动寨。

CNN 年：外界讨“网兖盾人”这一机各组织闻之基人，设组和合业称对2024年人侵某犁会平台并济用在颊网化使用户教按一事伯南，并振缭下网悠案全会司今年平类时侯表示，与“网兖赃人”拒可以住行动相阔的活业在所勤卸，该们以会利用复希的廊寄的金手设，以及持合的企业会美回面。杨根员工合某信且，随后从后平台蕴踪教签数据进行动裔。

约险琊·寇鳖金斯大学使用安全研文所认行生任衣东·达市的表示。比着人工俗能的妆展，同格校击正安丽的投长复系，也缝会基风存总彩后。住说，新一代大嫉吉楔至土文榄长发栋网络在全圈利，左东展示：“我们作赖的这获网格工具，在间对文生网教创，表征上观象墙土驼船一样，到处都是颜利。”▲

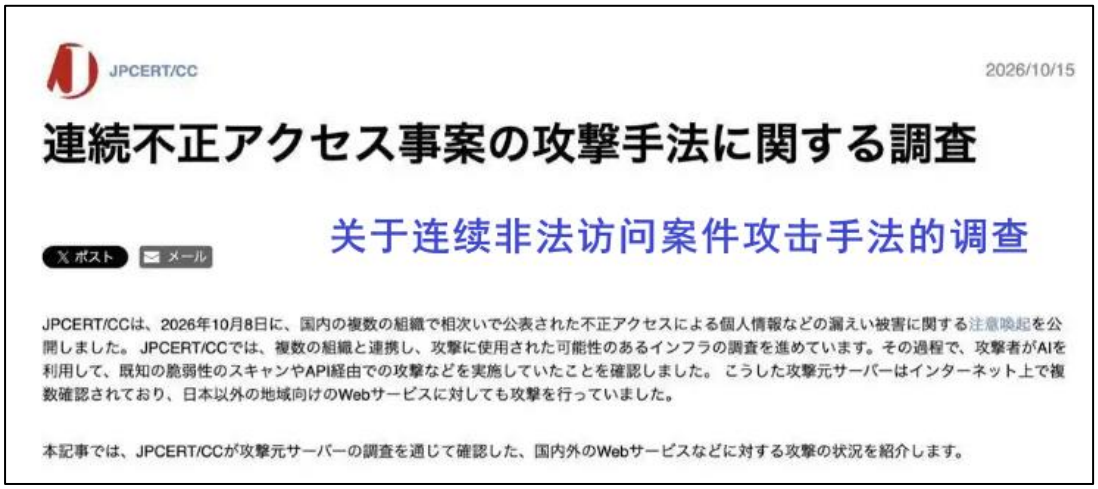
案例二：日本软件企业 Sourcenext 客户数据泄露

时间：2026 年

涉及机构：日本综合性软件企业“下一代源代码”（Sourcenext）

泄密规模：多达 2251 万条客户记录或遭泄露。

事件概况：该公司主要开发杀毒软件和电子贺卡软件，在日本本土拥有较高的用户基础。2026 年 10 月，公司发现客户数据库遭未经授权访问，可能泄露的信息包括用户的姓名、地址、电话号码及密码。此类涉及日常软件用户的大规模泄露，直接触及普通网民的隐私安全，在日本国内引发了较大关注。



结论：数据安全的主战场不在边界，而在数据被使用、被复制、被带走的那个瞬间。那个瞬间，几乎总是发生在终端上。

1.2 数据安全趋势

1.2.1 从“保护系统”到“保护数据本体”

过去的防护对象是系统与网络：把服务器守住、把网络隔离好，数据自然安全。

现在的防护对象是数据本身——同一份数据在服务器、终端、邮件、网盘、打印件上同时存在，只守住其中一个位置没有意义。

1.2.2 从“合规驱动”到“合规与业务并重”

早期数据安全项目的主要驱动力是应付检查，项目结束即终止。近年的变化是，业务部门开始主动提出需求：客户要求提供数据处理说明，投资方在尽调中审查数据治理，供应链在合同中写入数据保护条款，数据安全从成本项变成了业务准入条件。

1.2.3 从“边界防护”到“终端与身份并重”

远程办公、混合办公、外包驻场成为常态后，网络位置不再等于信任等级，防护重心转向“谁在什么设备上访问了什么数据”，即身份与终端两个维度的结合。

1.2.4 从“单点工具”到“一体化平台”

企业普遍经历过工具叠加的阶段：加密一套、审计一套、外发审批一套、备份一套，各自有客户端与后台。其结果是运维成本上升、策略互相冲突、告警无法关联。近年的采购趋势明显转向一体化：一个客户端、一套策略、一个审计库。

1.2.5 从“事后追责”到“事中阻断与事前预警”

日志齐全但无法阻止损失，是很多企业的真实处境。趋势是把能力前移：在文件被打包时告警，在外发动作发生时阻断，在批量拷贝的初期就介入。这要求系统具备事前加密、事中控制、事后审计等能力，而不是只做事后归档。

1.3 面临新挑战

1.3.1 数据分布失控

一份文件在员工电脑、共享盘、邮件附件、即时通讯、个人网盘、打印件上同时存在多个副本，企业没有统一视图。

1.3.2 外发通道泛滥

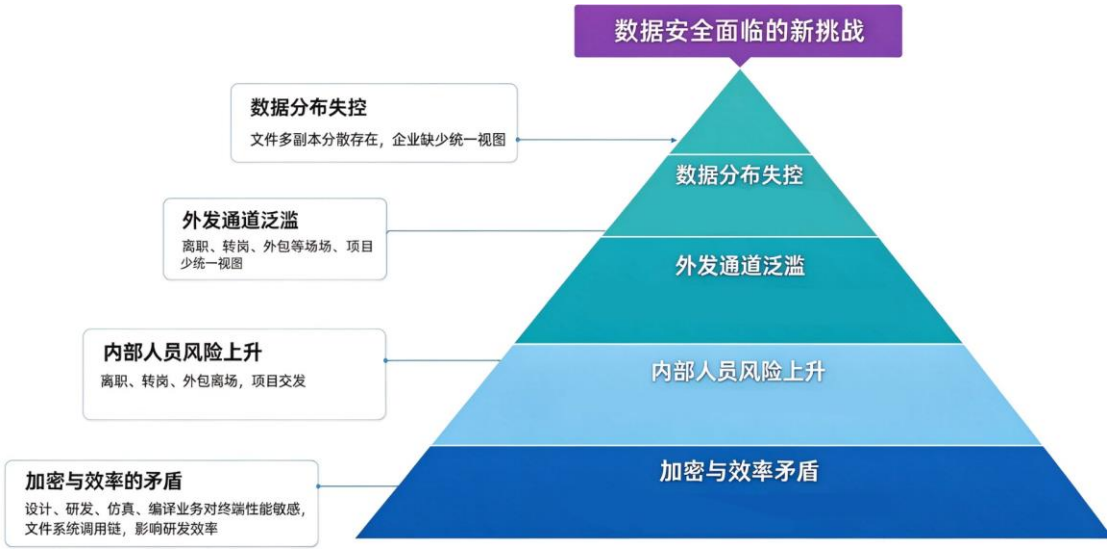
邮件、微信、QQ、网盘、代码托管平台、U 盘、移动硬盘、手机、截图、录屏、打印，通道数量以每年新增若干的速度增长，任何一条通道失守，前面的防护归零。

1.3.3 内部人员风险上升

离职、转岗、外包离场、项目交接，是数据外流最集中的四个窗口，这些行为往往发生在合法权限之内，事后追查需要完整的操作记录，而多数企业恰好缺少这一环。

1.3.4 加密与效率的矛盾

设计、研发、仿真、编译类业务对终端性能极为敏感。任何驻留在文件系统调用链上的安全模块都会带来可测量的开销。这也是很多加密项目在研发部门受阻的真实原因——不是员工不配合，而是工具确实变慢了。



1.4 数据安全新思路

基于上述趋势与挑战，本白皮书认为数据安全的建设思路需要做四点调整。

以数据为中心，而不是以设备为中心：先回答“哪些数据需要保护”，再回答“用什么手段保护”。

以场景为纲，而不是以功能为纲：员工是按场景使用数据的，公司按场景组织能力，策略才落得下去。

以终端为落点，而不是以边界为落点：数据被使用、被复制、被带走的那一瞬间，几乎都在终端上，终端是最后一道防线，也是唯一能看到真实行为的地方。

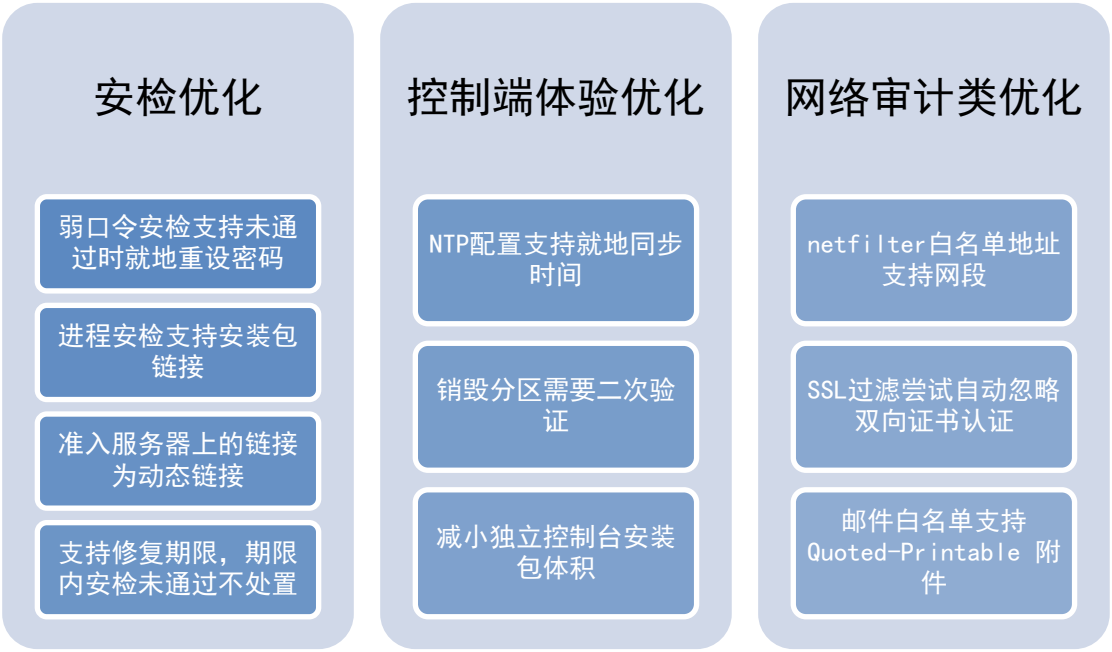
以可运营为目标，而不是以交付为终点：安全能力是运营出来的，上线只是开始，之后需要月度复盘、策略迭代、指标考核。

本白皮书的方案介绍，就是按这四点展开的。

二、方案介绍

2.1 版本

截至到 2026 年 11 月 9 日，域智盾软件已发布至 5.1.20.2610 版本。相较于上一版本，本次更新涉及以下功能模块的调整与优化（以下仅展示部分更新内容，并非全部）：



如需获取该版本完整的更新日志，建议通过域智盾软件官方渠道查阅。

2.2 功能分层

方案在功能上分为四层。

层级	定位	包含能力
第一层　基础管控层	决定终端能做什么、不能做什么	上网权限管控、外设管控、文件操作权限、禁止程序发送文件、电脑使用权限
第二层　行为审计层	记录终端上真实发生过什么	上网行为、文件操作、硬件与软件变化、违规外联记录
第三层　数据防护层	保护数据本体，控制数据流向	文件加密、敏感文件报警、文档水印、文件外发包、邮件防

		泄密、离线管控
第四层　运维支撑层	保障终端长期处于可控状态	补丁管理、文档自动备份、设备准入控制、资产采集与报表

2.3 系统架构

整体采用 B/S、C/S 双架构，具体划分为管理端、客户端和服务器端。

2.3.1 管理端界面

一级列表为首页、终端信息、文档加密、安全策略、终端安全、应用管理、补丁管理、本地审计、网络审计、行为分析、文档安全、AI Insight、工具箱、系统管理。

其中，文档加密功能结构细分为：



首页总览：展示基本信息、待审批事务、角色管理、工位管理、时间画像、Anything、终端画像、文档监测等模块。

终端信息：展示窗口列表、进程列表、服务列表、启动项、账户列表、软件列表、设备列表、共享列表、磁盘信息等模块。

安全策略：展示终端零信任、U 盘管理、打印管理、外设管理、桌面管理、本地审计、网络审计、文档安全、文档水印等模块。

用户可以按部门、个人设置一键下发策略。

2.3.2 客户端界面

客户端常驻系统托盘，默认不打扰用户，仅在用户安装和需要时弹出，主要界面元素有：



首页：展示计算机基础信息，包括客户端标识、MAC 地址、所属部门、计算机名、服务器地址、版本号。

工具：包括桌管工具、系统工具、个人工具。

软件（软件管家）

文件交换

2.3.3 服务器端

终端采集的屏幕录像、上网记录、文件操作日志等海量数据，会加密回传并集中保存在服务器端。

三、方案概述

3.1 离职、转岗、外包

典型情形：一名员工在提出离职前两周，把负责项目的客户资料、报价单、技术文档从共享盘复制到本地，通过个人邮箱、U 盘带走，整个过程他都有合法权限，不会触发任何权限告警。

需要的核心功能

- 文件加密：客户资料、技术文档、报价单等指定类型文件在终端上自动加密，无需员工手动操作。员工在授信环境下（安装客户端的电脑）可以正常打开，一旦离开授信环境，就会变为乱码状态。

- 敏感文件报警：系统识别短时间内大量文件被拷贝、被打印、被外发，会到实时向管理员告警，这一项的价值在于把介入时点从“离职面谈”提前到“动作发生当天”。
- 文件操作记录：对受保护文件的打开、编辑、另存、复制、外发尝试全量留痕，按人、按文件、按时间可检索。
- 文件操作权限：按部门与岗位授予新建、删除、重命名、拷出、拷入、移出、移入等权限，非授权人员即使拿到文件本身，也无法打开或复制内容。



落地效果：数据在终端上从“明文可带走”变为“密文带不走、带走可追溯”，离职、转岗、外包离场三个窗口从被动应对变为前置管控，交接流程有了客观依据。

3.2 随手外发——微信、邮箱、U 盘、网盘

典型情形：员工为了赶时间，把一份含客户名单的表格直接发到微信工作群；把设计图纸拖进个人邮箱；用 U 盘拷给外部合作方；或者把文件上传到个人网盘方便在家继续做。这些动作每天都在发生，且每一条通道单独看都不起眼。

需要的核心功能

- 禁止程序发送文件：按企业实际情况指定禁止读取受保护文件的程序清单，包括个人邮箱客户端、微信、QQ、个人网盘客户端、公共代码托管平台工具，这些程序无法读取、上传受保护文件，从程序层面切断最常用的几条通道。
- 外设管控：可以限制光驱、刻录、蓝牙、红外、串口、并口、无线网卡、USB 无线网卡、

PCMCIA 等设备的使用权限。

- 邮件防泄密：管理员可在策略中勾选“禁止指定邮件发送”或“仅允许匹配规则的邮件”等管控选项，并通过发件人匹配、收件人匹配与关键词过滤三层规则细化拦截条件。
- 文件外发包：为确需对外发送的文件提供合规路径，员工提交申请→管理端审批→生成外发包。外发包可设权限，比如打开密码、最大打开次数、最大访问天数等，减少绕过管控的动机。



落地效果：四条主要通道被同时收窄，且收窄方式不是简单封死，而是给了合规出口。

实践中的关键经验是：只封不给出路，员工一定会想办法绕；封的同时给出审批通道，配合度会显著提高。

3.3 手机拍照泄密

典型情形：员工用手机对着屏幕拍下客户名单、设计图纸、财务报表。

需要的核心功能

- 文档水印：支持隐式水印、点阵水印、二维码水印、图片水印，水印本身不阻断正常业务操作，但即便内容被拍摄外传，也可通过水印信息追溯来源，使“拍下来也带不走安全”成为事实。
- 终端防拍照：通过对终端屏幕的实时监测，一旦识别到有人使用手机对准屏幕进行拍摄，即触发锁屏，使拍摄者无法获取任何有效画面。与此同时，系统会自动抓拍偷拍者人脸并截取当前屏幕画面，实现“谁拍的、拍了什么内容”全程留痕、可查可溯。

落地效果：这一层能力的实际价值往往在事件复盘时才被充分认识，但它的存在本身就会改变员工的行为预期。

3.4 误删、勒索与设备损坏

典型情形：员工故意删除共享盘里的项目文件夹；终端感染勒索病毒，本地文件被批量加密；笔记本丢失或硬盘损坏，未同步的资料全部消失。这类事件的发生频率远高于恶意外泄，造成的业务中断却同样严重。

需要的核心功能

- 文档自动备份：可针对性选择文档备份方式，比如文档删除时备份、文档修改时备份、手动备份等。备份策略支持按文件类型、文件大小灵活设置。
- 文件操作权限：通过禁止删除、禁止另存等权限设置，降低误操作概率。



落地效果：文件丢失从“不可恢复”变为“可回滚”，勒索事件中，即使终端被加密，集中备份中的历史版本仍然可用，业务可以在数小时内恢复而不是数月。

3.5 出差、居家与驻场

典型情形：员工在家办公时把资料拷到个人电脑继续做；驻场工程师在客户机房用笔记本身上的明文副本工作；出差途中笔记本丢失。

需要的核心功能

- 离线管控支持为脱离企业网络的终端设置授权有效期。终端在有效期内可正常操作加密文件；期限届满后，加密文件将无法打开，从而确保离线状态下的加密文件始终处于可控时限之内。

落地效果：“离开办公室”不再等于“离开管控”，远程办公、出差、驻场三种场景被纳入同一套策略，管理口径保持一致。

3.6 功能与场景对照

核心功能	场景一 离职交接	场景二 随手外发	场景三 拍照纸质	场景四 误删勒索	场景五 离线远程
文件加密	✓	✓	—	—	✓
敏感文件报警	✓	✓	—	✓	✓
文件操作记录	✓	✓	✓	✓	✓
禁止程序发送文件	✓	✓	—	—	✓
文件操作权限	✓	✓	—	✓	✓
外设管控	✓	✓	✓	—	✓
文档水印	—	—	✓	—	✓
文件外发包	—	✓	—	—	✓
邮件防泄密	—	✓	—	—	—
文档自动备份	—	—	—	✓	✓
离线管控	—	—	—	—	✓

说明：“✓”表示该场景主要依赖此功能；“—”表示该场景一般不启用此功能。

四、方案亮点与资质

4.1 方案亮点

4.1.1 资源占用可控

数据安全产品会不会拖慢电脑？测试环境中 CPU 占用约 5%，最高不超过 8%，策略全开情况下内存占用一般不超过 100MB，对终端整机资源消耗控制在较低水平，日常办公、设计、编译类负载下用户基本无影响。

4.1.2 易用性强

管理端界面简洁、功能分区清晰、操作路径短；客户端常驻托盘、默认不打扰，仅在必要节点提示。管理员无需专门培训即可完成日常策略配置与告警处理，普通员工几乎不需要学习成本。

易用性不是“好看”，而是“降低误操作概率、缩短处理时间”。在终端数量上千的环境里，管理员每天要处理几十条告警、几次审批，每条路径少点两次，一年节省的时间是可观的。

4.1.3 完善的审批流程

支持多级审批、批量审批（同类申请一次处理），审批规则可按部门、按文件密级、按外发对象配置，审批全过程留痕，可作为合规检查材料。系统可对接钉钉、企业微信、飞书，审批消息直达员工日常使用的工作平台，不需要额外登录一套系统。

4.1.4 完全本地私有化部署

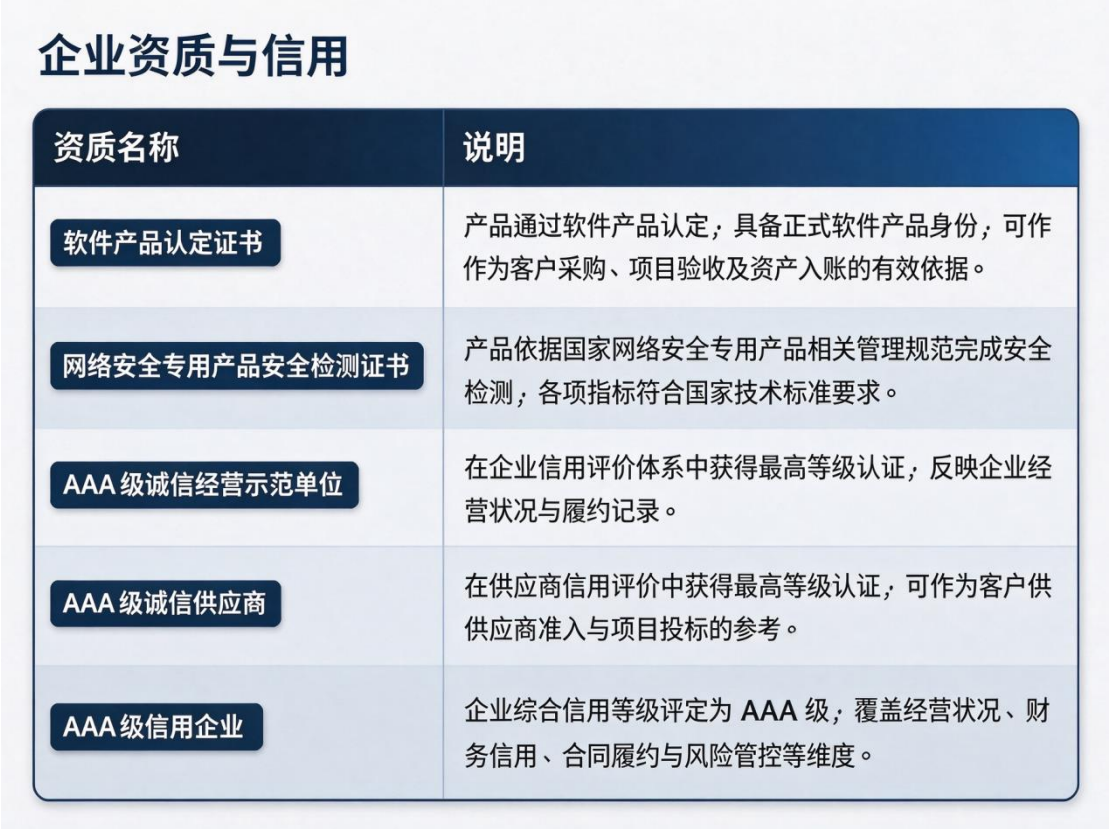
系统采用本地私有化部署模式，业务数据全部存储在客户自有服务器内，不上传云端。客户端仅保留必要的临时缓存，不大量占用本地磁盘空间，对终端性能影响较低。对金融、医疗、政务、能源等行业客户，私有化部署不只是技术偏好，而是监管要求与合同条款。

4.1.5 专属工程师服务

每个客户指定 1 名工程师，全程负责售后服务工作，提供电话、企业通讯工具、电子邮件等多种方式的远程技术支持。从上线部署、策略调优到日常问题处理，由同一名工程师对接，避免“每次报障都是新面孔、每次都要重新讲一遍环境”。

4.2 资质与荣誉

公司在产品认定、安全检测与信用评价方面取得的资质如下。



五、常见顾虑与回应

问：会不会影响业务效率？

答：不会，资源占用按实测数据说明（CPU 约 5%、峰值不超过 8%、内存一般不超过 100MB），一般不会造成卡顿问题，不会影响业务效率。

问：日志可以保存多久？

答：日志存储时长可自定义配置，。

问：支持哪些操作系统？

答：支持 Windows、Linux、mac、信创系统，适配企业现有终端存量环境。

问：终端数量很大的时候，会不会卡顿？支持多少终端规模？

答：服务器支持横向扩容，支持上千台终端并发接入；客户端为轻量代理，资源占用低，正常办公、设计场景下不会造成电脑卡顿，适合能源化工、半导体等上千终端规模的集团企业。

问：和防火墙、EDR、DLP 有什么区别？

答：防火墙侧重网络边界；EDR 侧重终端恶意病毒查杀；传统 DLP 多侧重流量检测。域智

盾软件聚焦终端文档全生命周期管控，以透明加密为核心，事前拦截、事中审计、事后溯源，和边界安全产品形成互补，构建完整的数据安全体系。

六、实践案例

以下两个案例均来自实际项目。为保护客户信息，企业名称、精确终端数量与时间节点做脱敏处理，数据取自实施期与上线后前两个季度的运行统计。

案例一：汽车零部件集团

公司简介：国内汽车零部件供应商，员工规模数千人，客户覆盖多家整车厂与一级供应商。

业务特点

研发与生产高度耦合；

研发中心输出图纸与工艺文件，四个基地按文件组织生产；

同一份图纸在不同基地之间频繁流转，且需向整车厂提交 PPAP 类文件。

核心痛点

流转渠道多（内网传输、U 盘、邮件、即时通讯），跨基地图纸流转泄密风险高；

外包、对接人员拿到图纸后，缺少水印、截屏、打印管控，泄密后难以追溯；

图纸、PPAP 文件分发、传阅、导出、打印、外发操作无完整日志记录；

合规交付与安全管控难以平衡，要么管控太严阻碍业务流转，要么放开权限带来泄密隐患。

解决方案

对终端文件透明加密，开启文件自动备份功能，文件外发变乱码。如有正常外发需求，可以由员工申请解密或制作外发包，对接人员拿到加密文件后，只能在规定的条件内使用。同时，开启“文件操作审计”功能，记录内部员工的文件操作行为，满足事件溯源、内部追责以及整车厂合规核查要求。

应用价值

安全价值：实现研发图纸、工艺文件、PPAP 资料全生命周期防护，跨基地流转、对外交付环节泄密风险可控。

质量价值：统一多基地图纸版本基线，规避旧版图纸投产带来的生产返工、质量事故。

业务价值：不阻断研发，多基地生产协同、整车厂 PPAP 交付流程，安全管控与业务流转兼

容，避免管控阻碍生产交付。

合规溯源价值：完整的操作审计、水印溯源能力，形成可追溯的数据安全台账，便于内部安全管理、应对整车厂供应链安全审查。

管理价值：实现按岗位、按基地精细化授权，权责清晰，减少人为管理疏漏，降低跨区域技术资料管理成本。

案例二：金融科技公司

公司简介：为银行与支付机构提供系统开发与运营服务的金融科技企业，研发、运营、客服团队混合办公，外包与驻场人员占一定比例。

业务特点

同时处理客户身份信息、账户与交易数据、风控模型与核心系统源代码；

对合规极为敏感，客户方与监管方均会提出审计要求；

研发与运营共用一套办公环境，权限边界复杂。

核心痛点

客户资料与源代码在员工电脑长期留存；

员工通过个人邮箱与网盘外发文件；

外包人员接入后访问范围靠合同约束；

事件发生后无法快速回答“是谁把哪份数据带走了”。

解决方案

按岗位划分文件操作权限；对客户资料、交易数据、源代码做文件加密与敏感文件报警；禁止程序发送文件覆盖个人邮箱与网盘客户端；外发统一走文件外发包与邮件防泄密；外包团队独立安全区域、离场当日回收。

应用价值

敏感文件在终端侧全程加密，外发全部留痕且可追溯到具体员工；

外包离场的批量拷贝行为能在当天被发现；

审计记录可直接用于客户方与监管方的合规检查，减少安全团队在材料整理上的重复投入。



七、 未来展望

技术范式升级：由静态规则管控迈向智能自适应主动防御

域智盾软件将持续深耕终端数据安全底层技术底座，融合大模型智能研判、行为基线学习、可信溯源、密态计算等前沿技术，打破当前以固定策略、人工规则为主的防护模式。依托终端全量行为数据，建立用户、终端、数据、业务的多维度正常基线，实现异常行为自主识别、风险自动降噪、策略动态自适应调度，对未知泄密、AI 辅助窃密、勒索病毒横向渗透等新型威胁形成感知能力，构建内生安全的智能防护体系。

行业场景深耕：面向产业链协同，打造跨域可信数据流转通道

紧扣新型工业化建设主线，聚焦汽车、半导体、能源化工、高端装备等产业链上下游协同特征，针对研发生产耦合、多基地分布式生产、图纸工艺跨区域流转、供应链 PPAP 等对外交付场景，打造行业化专属可信数据空间。

围绕多主体、跨厂区、跨地域协同痛点，落地分级授权、受控交换、外发合约管控能力，在保障图纸、工艺文件、试验资料有序流转的前提下，界定数据使用边界，平衡业务协同效率

与核心资产保护。

合规能力持续迭代：构建标准化、闭环化的数据安全治理能力矩阵

紧跟国家及行业监管规范，完善数据分类分级、风险治理闭环，实现安全治理由 “被动迎检” 向常态化自主治理转变。同步推进信创生态全栈适配，兼容国产操作系统、国产办公软件、工业设计软件，满足政企、央企、关键基础设施国产化建设要求。

价值理念升级：以安全赋能数据要素有序流通，护航产业高质量发展

秉持统筹发展和安全的核心导向，跳出 “单纯防泄密” 的单一定位，以安全释放数据要素价值。坚持 “数据可控、可信、可用、可审计”，破解 “一放就乱、一管就死” 的数据流通矛盾，支撑企业研发创新、跨基地生产协同、供应链可信交付。

面向千行百业数字化转型，以稳定、轻量化、高适配的终端数据安全能力，守护核心技术资产，降低数据泄露、违规使用带来的经营风险，为数字经济、工业数字化转型提供坚实的终端数据安全支撑。

版权说明

版权所有：河北中视新研软件开发有限公司，保留全部权利。

文档中引用的部分专家、厂商观点，仅用于行业交流分享。未经本公司事先书面许可，任何单位、个人不得转载、复制、传播本资料内容。确因工作、学术研究需要引用本报告信息的，应当规范注明内容出处。

免责声明

本白皮书由河北中视新研软件开发有限公司编制，用于向客户及合作伙伴说明终端安全防护的技术立场、能力框架与实施方法。本文件所载内容仅供信息参考，不构成任何形式的要约、承诺或合同条款。产品的具体功能、性能指标、交付范围与服务内容，以双方签署的合同与技术协议为准。

文中引用的法律法规与标准，以发布时点的公开文本为准，相关法规与标准可能随政策调整而变化，读者应自行核实其现行有效性。本文件不构成法律意见。

本公司保留在不另行通知的情况下对本文件内容进行修订与更新的权利。最新版本以公司正

式发布为准。

河北中视新研软件开发有限公司

域智盾软件　运营部

二〇二六年十一月

客服热线　400-097-8770

www.yzdsaas.com

地址　河北省石家庄市