域智盾软件®

域智盾软件
终端安全防护技术白皮书

Endpoint Security Protection Technology White Paper



河北中视新研软件开发有限公司

CONTENTS 目录

序 言 4
一、行业现状 4
1.1 案例回望：“Sorry”勒索病毒 4
1.2 当前挑战 6
1.3 现有方案短板 6
二、技术介绍 7
2.1 方案概述 7
2.2 功能构成 8
2.2.1 上网行为审计 8
2.2.2 上网权限管控 8
2.2.3 数据防泄密 9
2.2.4 外设管控 9
2.2.5 违规外联报警 10
2.2.6 硬件和软件变化报警 11
2.2.7 电脑使用权限 11
2.2.8 补丁管理 11
2.2.9 设备准入控制 12
2.3 协同关系 12
三、方案创新与价值 13
3.1 结构性创新 13
3.1.1 从“多套系统”到“一套事实” 13
3.1.2 从“功能开关”到“组织授权” 13
3.1.3 从“事后取证”到“事前预警” 14
3.2 工程性创新 14
3.2.1 低干扰的终端体验 14
3.2.2 离线可用 14
3.3 运营性价值 14
四、落地方法论 15
4.1 阶段划分 15
阶段一：立项与基线调研 15
阶段二：试点 15
阶段三：策略调优与固化 16
阶段四：分批推广 16
阶段五：常态化运营 16
4.2 常见顾虑与回应 17
五、实践案例 17
5.1 汽车零部件集团：三千台终端的统一管控 17
5.2 三甲医院：临床终端与患者数据 18
六、计算机软件著作权登记证书 19
6.1 登记情况 19
6.2 对客户的实际意义 19

七、未来展望.....20
7.1 终端安全正在与零信任合流.....20
7.2 覆盖范围从“办公终端”扩展到“全场景终端”.....20
7.3 从“工具”走向“可运营的能力”.....20
7.4 我们的判断.....20
版权说明.....21
免责声明.....21

序 言

最近几年，勒索事件、数据外泄事件，绝大多数不是通过突破边界设备完成的，而是通过一个弱口令、一次远程桌面登录、一台长期未打补丁的终端、一个被员工随手安装的远程控制工具完成的。攻击者拿到的是一个合法账号，走的是一条合法路径，边界设备在这个过程中几乎没有可判断的异常。

目前，我国相关法律法规已逐步完善，《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》相继实施，《网络安全等级保护基本要求》（GB/T 22239）将终端管控、审计留存、外发控制列为基本要求，《关键信息基础设施安全保护条例》进一步明确了重点行业运营者的保护责任。合规不再是“做一份材料”，而是要拿出可核验的策略、日志与处置记录。

这份白皮书列出以下七大章节，研判终端数据安全技术演进方向与行业防护趋势。

- ✓ 第一章分析行业现状与现有方案的短板。
- ✓ 第二章说明域智盾软件在终端安全上的技术构成。
- ✓ 第三章讨论方案在工程上究竟解决了什么。
- ✓ 第四章给出一条可以照着走的上线路径。
- ✓ 第五章给出实践观察。
- ✓ 第六章说明产品的资质与产品登记情况。
- ✓ 第七章是对未来的判断。

一、行业现状

1.1 案例回望：“Sorry”勒索病毒

在讨论技术方案之前，有必要回顾一个足够典型、也被足够多人经历过的事件。以“Sorry”为勒索提示的勒索病毒家族，是近年国内企业受害面最广的勒索事件之一。它的攻击链条并不复杂，几乎每一个环节都对应着终端治理上的一个缺口。



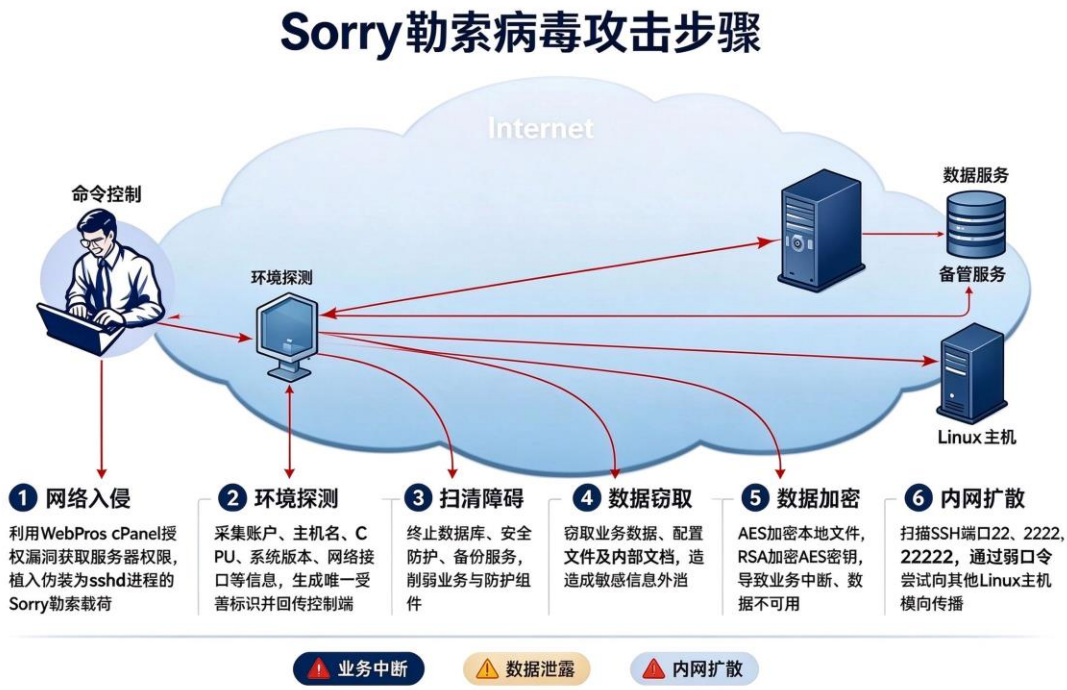
其关键特征为：

攻击对象：面向 IDC 服务器、企业 Linux 业务服务器、研发工作站（IC 设计、化工、能源等行业 Linux 环境）；

危害:同时造成业务中断 + 敏感数据外泄双重风险,区别于仅加密不窃取的传统勒索病毒；

传播特点：依托 SSH 弱口令横向扩散，在内网无隔离的服务器集群中极易批量中招。

攻击步骤：入侵投毒→信息探测→破坏防护→数据窃取→数据加密→内网扩散。



1.2 当前挑战

六大挑战：

终端形态高度异构。一个中型企业里同时存在 Windows、macOS、Linux、工控机、虚拟机、移动设备，操作系统版本跨越多个大版本，补丁状态参差不齐。

攻击手法持续演进。无文件攻击把载荷写在内存与注册表里，不落盘；DDL 白利用把恶意行为挂在合法的签名程序上；加密流量占比已超过九成，流量侧的检测手段被大幅削弱。

终端性能与业务连续性之间存在真实冲突。设计、仿真、渲染、编译类业务对 CPU、内存、磁盘 IO 极为敏感，任何驻留在文件系统调用链上的安全模块，都会带来可测量的性能损耗。

横向移动难以阻断。一旦某台终端失陷，攻击者会利用共享目录、域信任、运维工具向内扩散。

制度无法落地为策略。多数企业有《信息安全管理规定》《数据分级管理办法》，但文件里的“重要数据不得外发”在终端上没有对应的技术动作，制度只能靠自觉执行。

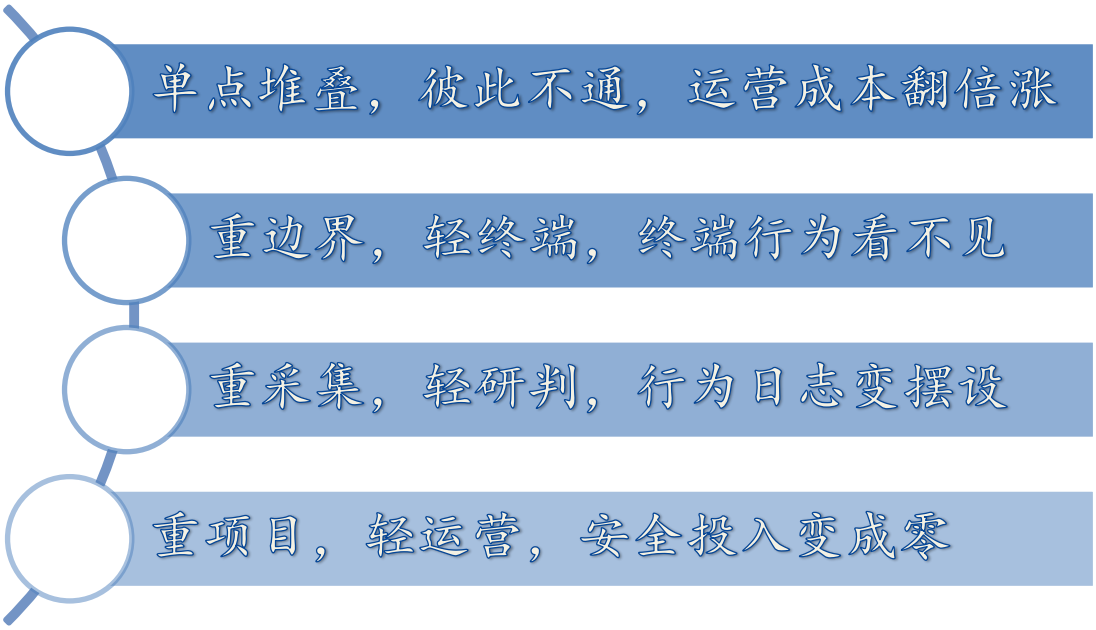
取证困难。事件进入调查阶段后，缺少终端侧的操作记录，无法形成有效证据。

1.3 现有方案短板

必须承认，多数企业并非没有做安全建设，而是建设方式存在问题。以下四个短板在实践中

反复出现。

- 单点堆叠，彼此不通：杀毒、桌管、DLP、准入、补丁各自成体系，各自有客户端、各自有后台、各自有告警。一个终端上装四五个代理，性能损耗叠加，策略互相冲突，运维成本翻倍增长。
- 重边界，轻终端：预算大头投向边界设备，而边界设备看得见流量，看不见终端上谁在拷贝文件、谁在插 U 盘、谁在装远程控制软件。
- 重采集，轻研判：日志采得很全，但没有关联分析，没有告警分级，没有处置流程。安全团队每天面对上万条记录，最终只能选择不看。
- 重项目，轻运营：上线验收即项目结束，没有月度复盘、没有策略迭代、没有责任到人。



这四个短板的共同点，是把安全当作“采购问题”而不是“治理问题”，而终端安全的本质，恰恰是一项需要长期运营的治理工作。

二、技术介绍

2.1 方案概述

域智盾软件支持 B/S、C/S 双重架构，整体划分为服务器端、客户端、管理端三层组件，部署方式为本地私有化部署。

各组件职责独立、协同联动，策略统一下发、数据集中归集，兼顾底层管控能力与 Web 运维便捷性，适配多分支机构、多部门、大规模终端的统一安全管控场景，核心数据留存于企业自有内网环境，保障数据主权与安全可控。

2.2 功能构成

2.2.1 上网行为审计

解决什么问题：企业需要知道网络带宽被谁占用、员工在上班时间访问了什么、是否存在访问恶意站点或数据外传的行为。

功能价值：记录每一次网站访问、网络搜索，展示终端用户访问的网页地址、网页标题、搜索关键词、搜索引擎、审计时间。审计数据支持按人、按部门、按应用、按时间段多维检索，并可导出为报表。

2.2.2 上网权限管控



解决什么问题：审计是事后，管控是事中，企业需要按岗位限制可访问的网站类别与可运行的程序，而不是对全员一刀切。

功能价值：按部门、岗位下发差异化策略，比如研发部门允许访问技术社区与文档站点，拦截娱乐、购物、下载站；财务部门拦截高风险站点；生产终端仅放行白名单内的业务系统地址。

企业得到什么：网络资源向业务倾斜，终端上运行的软件范围收敛到已知集合。同时，降低

“员工私自安装远程控制工具”“浏览器插件偷传数据”等风险。

2.2.3 数据防泄密

这是系统的核心能力，也是工程复杂度最高的一部分。它由四个相互配合的子能力组成。



（1）文件透明加密

对指定类型的文件自动加密，员工的操作方式、保存路径、快捷键全部不改变。一旦文件被违规外传到外部，对方得到的是乱码。

（2）敏感文件识别

不依赖人工标注。系统通过关键字类型、字符串值、正则表达式、分值多重维度识别敏感文件。

（3）外发通道管控

对邮件、即时通讯、浏览器上传、网盘客户端、打印等通道统一管控，受保护文件外发时按策略执行阻断或转人工审批。

（4）文件外发包

为确需对外发送的文件提供一条合规路径。发送人提交申请，注明接收方、用途、有效期；审批通过后系统对文件重新加密并附加接收方授权，接收方只能在指定时间内、指定设备上打开，到期自动失效，打开过程留痕。

2.2.4 外设管控

解决什么问题：U 盘与移动硬盘是最古老、也最有效的数据带出方式，至今仍是数据外泄案

件中出现频率最高的介质。

功能价值：

- 设置 U 盘使用权限：可选禁止使用、仅读取、仅写入、允许使用。
- 设置 U 盘白名单：将公司授权 U 盘添加至白名单，仅允许名单内的 U 盘使用，其他设备无法使用。
- 记录 U 盘使用行为：包括客户端、用户、所属部门、挂载点、卷标、容量、标识、序列号等信息。
- 管控其他外接设备：可以限制刻录、蓝牙、红外、串口、并口、无线网卡、USB 无线网卡、PCMCIA、1394 设备、便捷式设备等，防护更全面。

企业得到什么：外设从“默认可用”变为“按需授权”。研发、财务、设计等敏感岗位默认关闭，确需使用的走审批并绑定设备，介质外泄路径被显著收窄。

2.2.5 违规外联报警

解决什么问题：内网终端私自连接互联网、私接路由器、开热点共享、双网卡同时连接内外网，是绕过所有网络侧管控的经典手法。一台既能上内网又能上外网的电脑，等于把内网的数据直接接到了互联网。

功能价值：终端侧持续检测网络环境变化，判断是否出现新的网络接口、是否连接了未登记的热点、是否同时存在内外网连接，命中规则时立即上报并可按策略阻断该网络连接，同时向管理员告警，记录包含终端、用户、时间、接入方式、目标网络标识。

2.2.6 硬件和软件变化报警



解决什么问题：终端被拆走硬盘、被加装无线网卡、被安装远程控制软件、安全客户端被卸载。

功能价值：终端侧持续比对硬件清单（CPU、内存、硬盘、网卡、外设）、软件清单（已安装程序、服务、驱动）与关键变更（修改 IP 地址、计算机名），发生变更时上报差异。

2.2.7 电脑使用权限

解决什么问题：普通员工拥有本地管理员权限、可以改 IP、改计算机名、进注册表、开控制面板、装驱动、改网络配置。

功能价值：

按部门与岗位锁定关键配置项：

禁止修改 IP 地址与计算机名、禁止使用注册表编辑器、禁止访问控制面板指定项、禁止修改网络连接与防火墙设置、禁止安装未签名驱动、禁止修改系统时间、禁止使用任务管理器结束安全进程。

2.2.8 补丁管理

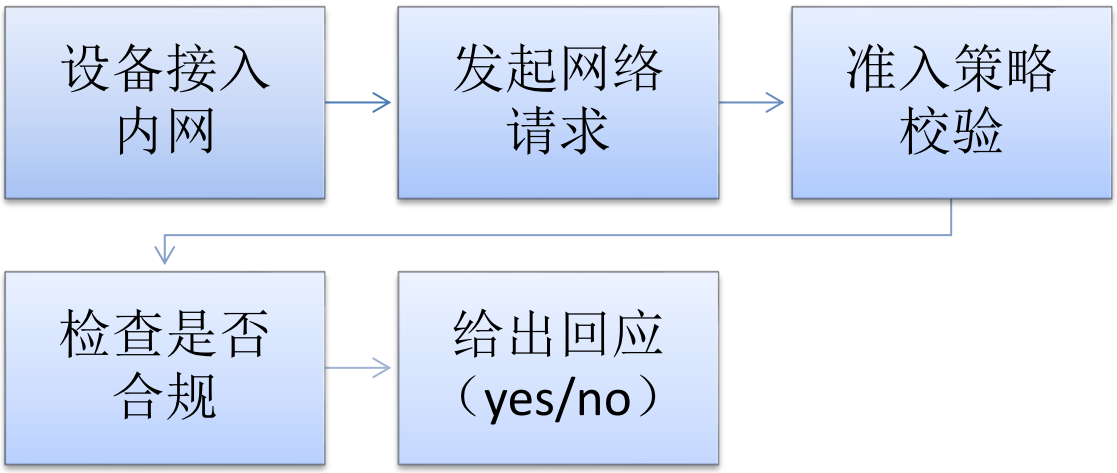
解决什么问题：勒索病毒与横向移动工具的入口，绝大多数是已知漏洞，企业仅仅依靠逐台手动安装，永远打不完。

功能价值：支持统一分发补丁，补丁安装状态、失败原因、剩余缺口在控制台集中可见。

2.2.9 设备准入控制

解决什么问题：外包笔记本、访客电脑、临时接入的调试设备、被卸载了代理的终端，违规接入内部网络。

功能价值：所有接入内网的设备在获得网络访问权限前必须通过准入校验，是否安装代理、补丁是否达标、杀毒是否开启、是否存在违规软件、是否为登记设备。不满足条件的设备被引导至隔离修复区，达标后方可接入内网。



2.3 协同关系

九项能力不是并列的功能清单，而是有明确分工的三层结构。

第一层：准入控制，决定谁能进入网络。

第二层：数据防泄密与外设管控，决定进入网络之后，数据能去哪里。

第三层：行为审计、权限管控、变更报警、补丁管理，决定终端长期处于什么状态。

三、方案创新与价值



3.1 结构性创新

3.1.1 从“多套系统”到“一套事实”

多数企业的安全建设是加法：缺审计加审计，缺加密加加密，缺准入加准入。加法的问题不在于成本，而在于每加一套系统，就多出一份互相不一致的事实，资产库有三份，日志时间不同步，告警无法关联，最终没有人相信任何一份数据。

本白皮书的做法是把资产、策略、日志收敛到同一套底座，同一台终端在资产视图、策略视图、审计视图、告警视图中是同一个对象，字段一致、时间一致、归属一致。这不只是技术上的简化，它改变了安全团队的工作方式：从“在四套系统之间对齐事实”变成“在一套事实上做判断”。

3.1.2 从“功能开关”到“组织授权”

策略的载体不是“全公司”，而是部门、岗位、项目组。安全团队配置的不是“是否允许外发”，而是“研发部不允许、市场部审批后允许、财务部仅允许发往指定域”。这种以组织为索引的策略模型，使安全策略能够与企业真实的管理结构对齐，也让策略调整成为一次组织调整的副产品，而不是一次技术攻坚。

3.1.3 从“事后取证”到“事前预警”

系统的审计能力不止用于事后。批量拷贝、非工作时段的海量文件读取、连续多次的外发尝试，这些组合行为本身构成风险信号。系统对这类行为做实时告警，把介入时点从“事件发生后”前移到“动作发生中”。在离职、外包离场、项目交接这些高风险窗口，这一点尤为关键。

3.2 工程性创新

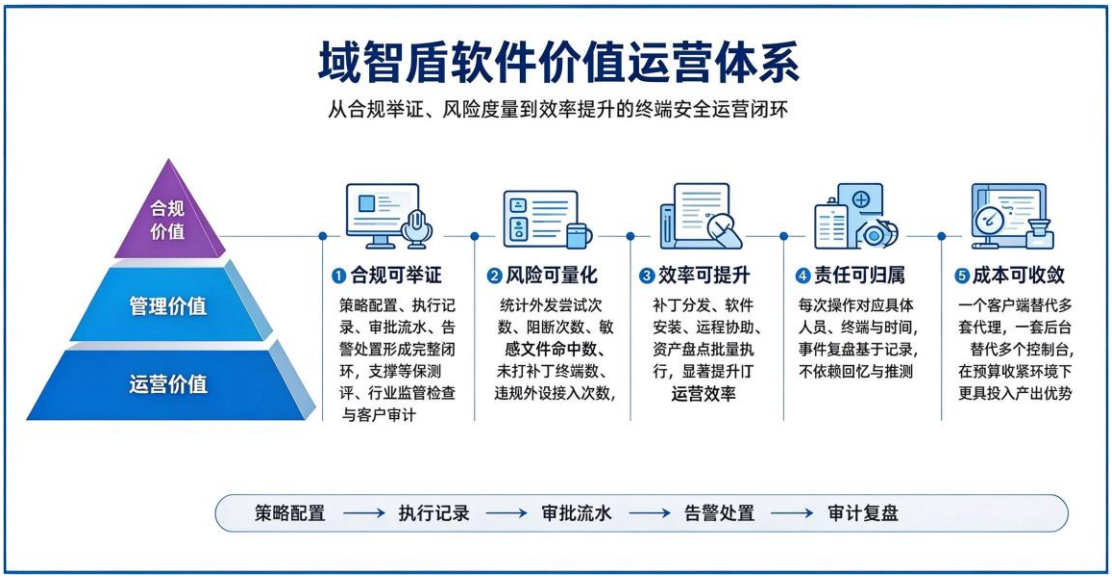
3.2.1 低干扰的终端体验

驻留在文件系统调用链上的安全模块，必然带来性能开销。系统的工程目标是把这个开销压到用户不可感知的量级：采用透明加密技术，文件在保存时自动加密，无需员工手动操作，CPU 占用约 5%，最高不超过 8%，是同类产品中占比最小的。

3.2.2 离线可用

终端脱离企业网络时，行为记录在本地缓存，恢复连接后自动回传，这一点对远程办公、出差、驻场场景是必需的，否则“离开办公室”就等于“离开管控”。

3.3 运营性价值



- 合规可举证：策略配置、执行记录、审批流水、告警处置形成完整闭环，可以直接支撑等保测评、行业监管检查与客户方审计。
- 风险可量化：外发尝试次数、阻断次数、敏感文件命中数、未打补丁终端数、违规外设接入次数，安全工作的价值第一次可以被度量。
- 效率可提升：补丁分发、软件安装、远程协助、资产盘点从逐台处理变为批量执行，IT 人均可维护终端数量显著提升。
- 责任可归属：每一次操作都对应到具体的人、具体的终端、具体的时间。跨部门的事件复盘不再依赖回忆与推测。
- 成本可收敛：一个客户端替代多套代理，一套后台替代多个控制台，在预算收紧的环境下，这往往比新增能力更有说服力。

四、落地方法论

以下路径来自多个行业的实施经验，目标是把“上线”这件事拆成可以逐步验证的动作，降低企业的落地顾虑。

4.1 阶段划分

阶段一：立项与基线调研

这一阶段不做部署，只做事实收集。需要完成四件事：

梳理终端总量与分布（部门、楼宇、操作系统、特殊设备）；

识别核心数据对象（哪些文件类型、哪些目录、哪些业务系统）；

确认组织架构与岗位职责（谁是部门管理员、谁是审批人）；

明确合规约束（等保级别、行业监管要求、客户审计要求）。

阶段二：试点

选择一个部门做试点，选择标准是：业务有代表性、有敏感数据、部门负责人愿意配合、终端数量在 50 至 200 台之间。整个过程保持每天一次的沟通会，收集业务反馈，处理兼容性问题，以及如何解决。

阶段三：策略调优与固化

核心原则是：

能不阻断就不阻断，先审计后管控；

高风险岗位从严，一般岗位从宽；

所有阻断类策略必须配置申请通道，避免员工因无路可走而想办法绕过。

阶段四：分批推广

推广不建议全网一次性铺开。按楼宇、按部门、按终端类型分批推进，每批完成后做一次小范围复盘。推广顺序上，先办公部门后研发设计部门，先普通岗位后关键岗位，先新采购终端后老旧终端。

阶段五：常态化运营

上线不是终点。建议建立三项固定动作：

月度策略复盘（查看告警分布、误报率、业务投诉，调整策略）；

季度合规输出（导出审计报表、审批流水、处置记录，供内审与外部检查）；

半年一次攻防视角自检（假设一名内部人员要带走一份核心文件，走一遍流程，看会在哪一步被拦住）。



4.2 常见顾虑与回应

- 会不会影响业务效率：不会，策略自动化执行，无需员工手动操作，实测不影响员工正常办公。
- 员工会不会抵触：抵触的来源通常不是管控本身，而是“被突然阻断且没有解释”。因此所有阻断类策略都配置申请通道，上线前做一次面向全员的说明，明确管什么、不管什么、怎么申请例外。
- 外包与驻场人员怎么管：为外包团队建立独立的安全区域与独立账号，权限最小化，项目结束当日自动回收。
- 老旧终端与特殊设备怎么办：不具备安装条件的设备（工控机、医疗设备、专用终端）通过准入控制做网络层限制，不强行安装客户端。

五、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、具体终端数量与时间节点做脱敏处理，数据取自项目实施期与上线后前两个季度的运行统计。

5.1 汽车零部件集团：三千台终端的统一管控

背景：该集团在国内拥有四个生产基地与一个研发中心，终端总量约三千台，覆盖办公、研发、车间与检测实验室。集团此前已部署边界防火墙与网络版杀毒，但各基地管理方式不一，总部无法掌握全网终端状态。

问题：

研发中心的图纸与工艺文件通过 U 盘与邮件在基地之间流转，无审批、无留痕；

车间终端长期不打补丁，曾因一次勒索事件导致两条产线停摆两天；

IT 部门维护的资产表与实际设备偏差超过一成。

方案：

先在生产基地做试点，上线资产采集、外设管控与补丁管理；

研发中心单独开启文件加密、文件权限、文件外发包、U 盘管控、邮件管控策略。

设置审批流程，文件解密、文件外发需由项目负责人与部门主管审批，两人审批通过方可进行下一步操作。

效果：

- 上线两个季度后，资产台账与现场设备一致；
- 未打补丁终端占比从推广前的多数收敛到少数，且新增缺口在两周内闭合；
- 图纸外发全部走审批通道，平均审批时长由原来的两三天缩短到半天以内；
- U 盘带出类事件归零。

5.2 三甲医院：临床终端与患者数据

背景：该院门诊、住院、医技、行政四类终端合计约两千台，业务系统包含 HIS、电子病历、PACS、LIS，信息科人手有限，日常以救火为主。

问题：

医生工作站本地留存大量病历与影像副本；

护士站共用电脑，操作无法对应到具体人员；

第三方运维与进修医生接入后权限范围不清；

终端补丁长期滞后。

方案：

以“不影响诊疗”为第一约束，加密只作用于病历、影像、报告类文件，业务系统进程全部加入白名单；

外设管控按科室分级，临床科室保留必要的读卡器与打印机；

开启“用户模式”，给同一台电脑的不同用户设置不同策略，使用不用规则，互不干扰；

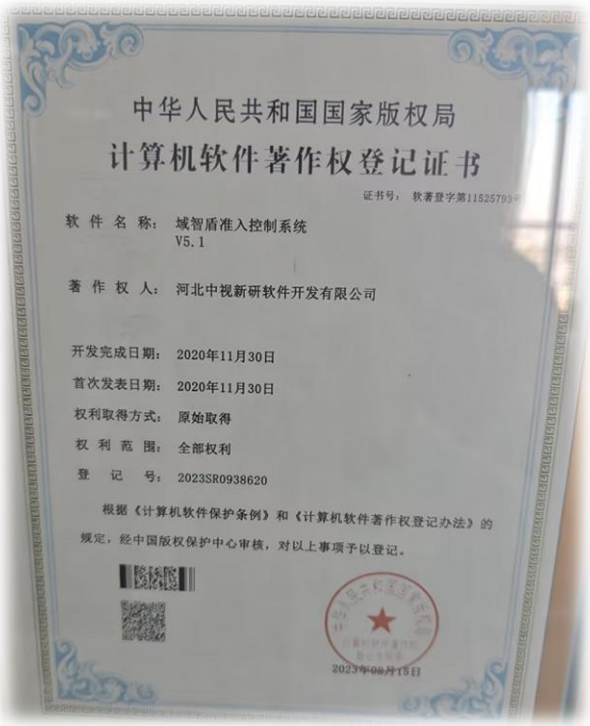
准入控制对接入内网的终端做基线校验，不达标引导至修复区。

效果：

- 病历与影像副本在终端上以密文形式存在，跨科室拷贝受到限制；
- 运维与进修人员接入全部走申请与审批，离场自动收回；
- 信息科通过控制台完成补丁分发，不再逐层跑科室。

六、计算机软件著作权登记证书

产品的技术自主性是终端安全类项目选型中的关键判断项。



根据《计算机软件保护条例》第五条：“中国公民、法人或者其他组织对其所开发的软件，不论是否发表，依照本条例享有著作权。”这意味着，软件著作权自软件开发完成之日起即自动产生，无需登记即可获得法律保护。

登记号：2023SR0938620

6.1 登记情况

公司已就域智盾软件系列产品的核心模块完成计算机软件著作权登记，登记证书由中华人民共和国国家版权局核发。

登记范围覆盖终端行为审计、文件透明加密、外设管控、设备准入控制、补丁分发、终端资产采集等主要功能模块，形成了对产品核心技术构成的完整覆盖。

软件著作权登记的意义不在于一张证书本身，而在于它对应着一套可被审查的源代码与文档。对客户而言，这意味着产品的核心能力是自研的，不依赖第三方组件的授权状态，也不会因为上游厂商的策略调整而中断服务。

6.2 对客户的实际意义

技术可控：加密驱动、敏感识别引擎、策略引擎、审计存储均为自有代码，可根据客户行业特点做定制适配，不因上游变更而受限。

合规可查：在等保测评、行业监管检查、客户方供应商审计中，软件著作权登记证书是证明自主研发能力的常规材料。

持续演进：自有代码意味着版本迭代节奏可控，客户提出的功能诉求可以进入产品规划，而不是只能等待第三方版本更新。

七、未来展望

7.1 终端安全正在与零信任合流

零信任的核心主张是“永不信任、持续验证”，而验证的落点最终在终端。设备是否合规、身份是否可信、行为是否异常，这三个判断都依赖终端侧的数据。可以预见，终端安全管理平台将逐步成为零信任架构中的策略执行点（PEP）与决策数据源（PDP）之一，而不是一个独立的安全孤岛。

7.2 覆盖范围从“办公终端”扩展到“全场景终端”

工控机、医疗设备、自助终端、车载与边缘设备正在成为新的接入点。这些设备往往不能安装常规客户端，未来的方案需要通过轻量化代理、网络侧识别与旁路准入的组合方式覆盖，而不是简单要求“装不了就不管”。

7.3 从“工具”走向“可运营的能力”

企业真正需要的不是更多功能，而是更少的管理成本。未来的产品竞争点将集中在三处：策略能否自动适配组织变化、告警能否自动分级并给出处置建议、效果能否自动量化为管理者可读的指标。安全能力的价值，最终要用可度量的方式呈现给管理层。

7.4 我们的判断

终端安全的下一阶段，不是把更多功能塞进客户端，而是把客户端产生的数据变成企业可以持续使用的治理资产。域智盾将继续沿着这条路径推进：保持一个客户端、一套策略、一个审计库的结构不变，在检测能力、跨平台覆盖与运营效率三个方向上持续投入。

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