域智盾软件®

域智盾统一端点安全管理系统产品白皮书

Unified Endpoint Security Management System Product White Paper



河北中视新研软件开发有限公司

CONTENTS 目录

修订记录 4

序　言 5

一、统一端点安全管理需求和挑战 5

1.1 需求分析 5

1.1.1 看得见的需求 5

1.1.2 管得住的需求 6

1.1.3 说得清的需求 6

1.1.4 省得下的需求 6

1.2 面临的挑战 7

1.3 如何应对挑战 7

二、产品介绍 8

2.1 方案概述 8

2.2 一体化管理 9

2.2.1 一个管理端，同时管控多个客户端 9

2.2.2 一体化的四层含义 9

2.2.3 一体化带来的直接收益 10

2.3 能力矩阵 10

2.4 方案内容 10

2.4.1 统一部署 10

2.4.2 统一资产 11

2.4.3 统一可视 12

2.4.4 统一审计 12

2.4.5 统一桌面 13

2.4.6 统一管控 14

2.4.7 统一运维 14

2.4.8 统一画像 15

2.4.9 统一分析 15

2.4.10 统一预警 16

2.4.11 统一加密 17

2.4.12 统一边界 17

三、产品部署 18

四、方案创新与价值 19

4.1 结构创新 19

4.2 工程创新 19

4.3 价值落点 20

五、　资质与荣誉 21

六、　落地方法 21

阶段一：明确对象 21
阶段二：启用模块 21
阶段三：小范围试用 22
阶段四：推广固化 22
七、实践案例 22
八、未来展望 23
版权说明 23
免责声明 24

修订记录

本白皮书随产品版本迭代与用户实践更新，修订情况记录如下。

版本	修订日期	修订内容	编制
V1.0	2026 年 11 月	首次发布。确立统一端点安全管理的需求框架、一体化架构、十二项统一能力与部署实施路径。	域智盾软件运营部

序　言

端点这个词，在安全行业里被用得越来越宽。过去它主要指员工的台式机；现在它包括笔记本、设计工作站、服务器、虚拟机、云桌面、移动终端，以及车间里那些常年不联网却必须接入一次的业务设备。

两种主要变换

- 数量上的变化

一家中型企业的端点数，从十年前的数百台增长到今天的数千台；一家集团型企业，端点数过万并不罕见。

- 管理上的变化

终端不再固定在工位上，员工带着设备进会议室、回家、出差、驻场；外包与协作方带着自己的设备进入企业网络；业务系统从本地机房迁到云端，访问路径从“进内网”变成“随时随地”。

端点数量与形态的变化，带来的是管理复杂度的指数级上升。一个常见的场景是：企业为上网行为买了一套系统，为数据防泄漏买了一套系统，为资产盘点又买了一套系统，每套系统都有自己的客户端、自己的后台、自己的账号体系。IT 部门每天要在三个控制台之间切换，看三份并不一致的资产清单，处理三套互不关联的告警。

本白皮书讨论的是“如何用一个平台搞定端点安全管理”，下面通过讨论核心需求、主要挑战、产品方案、部署方式、创新价值、落地路径和真实案例，完成这一重要课题。

一、统一端点安全管理需求和挑战

1.1 需求分析

端点安全的需求，来自四个不同方向的压力，最终都定位在同一批设备上。

1.1.1 看得见的需求

管理层与安全负责人首先要回答的，是“我们有多少台设备、装了什么、谁在用、状态如何”。这个看似基础的问题，在多数组织中回答得很不准确：资产台账滞后于现实、虚拟化与云桌

面不在台账内、外包与临时设备从未登记、报废设备仍挂在账上。资产不清晰，后续所有管理动作都建立在错误的前提上。

1.1.2 管得住的需求

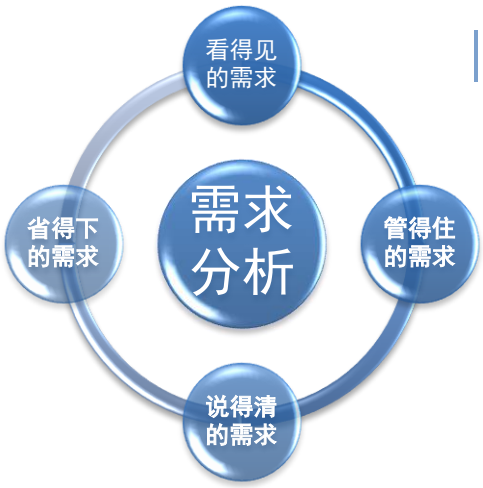
看得见之后是管得住。哪些程序允许运行、哪些网站允许访问、哪些外设允许接入、哪些文件允许外发，需要一个可以按岗位差异化配置、并且能够真正生效的执行层。制度写在纸上不会自动生效，必须落到终端上的具体动作。

1.1.3 说得清的需求

事件发生之后，需要说得清。谁在什么时间做了什么，依据什么判断，处置过程如何，都要有记录。等级保护测评、行业监管检查、客户方审计、内部追责，四项工作都要求同一份材料能够被反复引用，而不是每次重新整理。

1.1.4 省得下的需求

最后是省得下。IT 人力不会随端点数量同比增长，补丁分发、软件安装、故障排查、资产盘点如果继续依赖逐台处理，人力永远是瓶颈。端点数翻倍而人力不变，唯一的出路是批量化与自动化。



我们有多少台设备、装了什么、谁在用、状态如何

哪些程序允许运行、哪些网站允许访问、哪些外设允许接入、哪些文件允许外发

谁在什么时间做了什么，依据什么判断，处置过程如何，都要有记录

补丁分发、软件安装、故障排查、资产盘点实现批量化与自动化

图 1-1 统一端点安全管理需求分析

1.2 面临的挑战

- 端点形态高度异构：Windows、macOS、Linux、国产操作系统并存，物理机、虚拟机、云桌面、移动终端混杂，不同形态的可管控程度差异很大，统一策略在落地时经常被迫分成多套。
- 管理边界不断外移：远程办公与混合办公成为常态，终端可能在任何网络下工作，依赖“在内网才管控”的方案，在员工离开办公室的第一天就失效。
- 安全系统彼此割裂：上网行为、终端管控、数据防泄漏、资产管理由不同厂商提供，客户端叠加、策略冲突、日志口径不一，运维成本随系统数量线性上升。
- 告警量与处置力不匹配：多套系统每天产生数千条告警，安全团队按现有编制只能处理其中一小部分。
- 合规要求持续细化：等级保护、行业监管、数据安全专项检查的要求逐年在细化，材料准备从“有制度”转向“有记录、有处置、有闭环”，靠临时补材料已难以应对。

1.3 如何应对挑战

针对上述挑战，本产品采取的应对路径有五条。

✓ 在结构上做减法

不以“增加一套系统”的方式解决问题，而是把能力收拢到一个管理端、一套客户端、一份资产台账、一份审计库，系统数量减少，管理复杂度才会真正下降。

✓ 在能力上做加法

在统一的结构内扩展能力覆盖从资产到行为、从行为到数据、从数据到网络边界，形成一条完整的观察与干预链条。

✓ 在策略上做分层

策略按组织架构分层配置，界面简洁、功能清晰、操作简单、易用性强，节省用户学习成。

✓ 在数据上做同源

资产、行为、告警、审批共用同一套标识体系，一台设备在所有视图中是同一个对象，避免跨系统对齐。

✓ 在运营上做闭环

每一项能力都对应可输出的记录与可考核的指标，使安全工作从“做了”变成“可验证做成

了”。

二、产品介绍

2.1 方案概述

域智盾统一端点安全管理系统由终端客户端、管理服务端、管理控制台三部分构成。系统支持轻量化部署，依托客户端推送安装即可完成落地实施，部署全过程无需改造、调整现有网络拓扑，兼容用户原有网络架构，对业务链路无扰动，可快速融入现有信息化体系。

产品坚持一体化端点安全的核心设计理念，平台内部打通策略引擎、数据底座、事件联动能力，各类管控策略、日志数据、告警事件统一汇聚、统一调度、统一呈现，消除多套独立安全工具并存带来的策略冲突、数据孤岛、运维割裂等痛点。

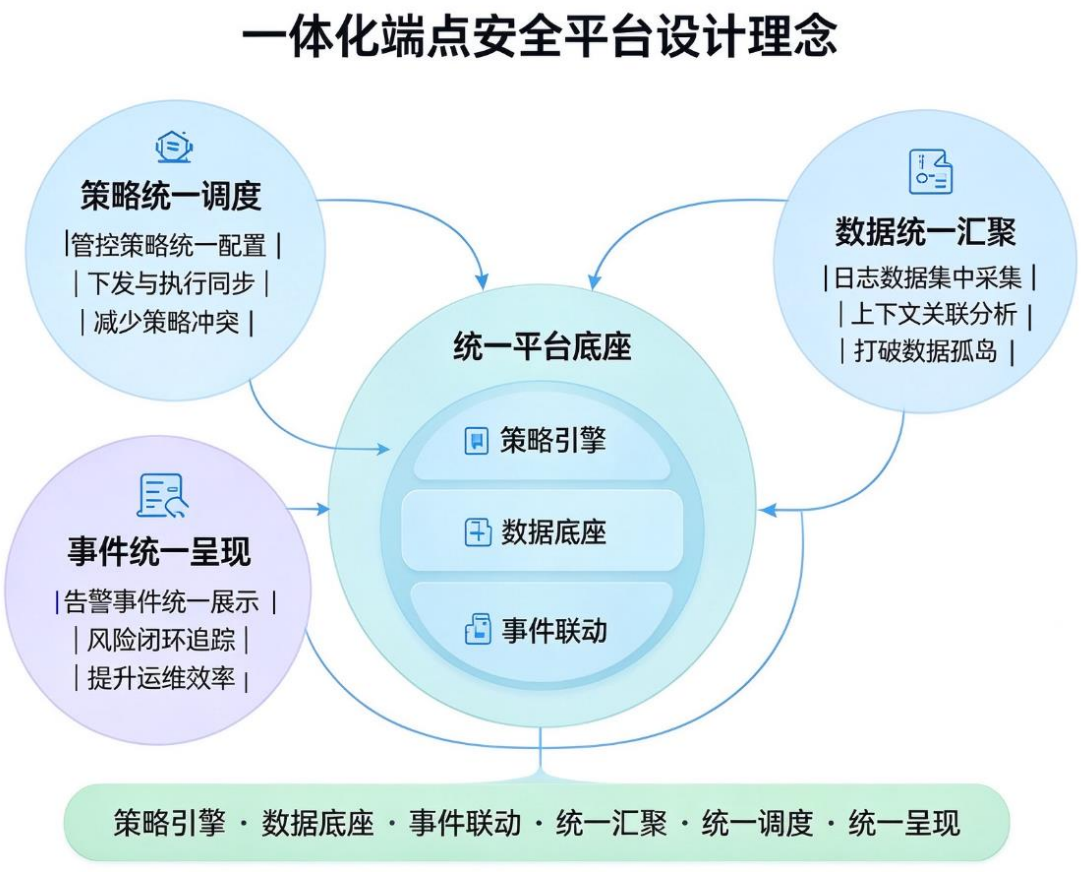


图 1-2 一体化端点安全平台设计理念

管理员依托统一管理控制台完成分权分域策略编排、任务下发、状态监测、审计追溯与闭环处置，可按照单位组织架构、岗位权责、业务场景差异化配置管控基线，兼顾安全合规要求

与办公业务效率，面向政府机关、科研院所、制造业、半导体研发等行业，构建事前预防、事中管控、事后追溯的端点纵深安全防护体系，支撑《中华人民共和国网络安全法》《中华人民共和国数据安全法》、等保 2.0 及保密管理相关规范落地。

2.2 一体化管理

这是本产品与多数同类方案最直观的差异，也是全部能力能够协同的前提，因此单独说明。

2.2.1 一个管理端，同时管控多个客户端

“多个客户端”指的不是多台设备，而是多种客户端形态。同一套管理端可以同时纳管以下几类终端：

办公与业务终端客户端，覆盖 Windows、macOS、Linux 及国产操作系统；

服务器与虚拟机客户端，用于承载服务器侧的文件保护与操作审计；

移动终端管理模块，用于平板与手持业务设备的应用与配置管理。

这些客户端在管理端中呈现为统一的资产条目，共用同一套组织架构、同一套账号体系、同一套策略语言、同一份审计库，管理员在一个界面完成配置，不需要为每种形态单独登录一套系统。

2.2.2 一体化的四层含义

- 统一账号：构建终端身份统一认证体系，打通人员、岗位、终端身份映射关系，保障身份可识别、权责可追溯。
- 统一策略：依托组织架构、岗位、终端维度统一制定安全管控基线，实现策略全生命周期闭环管理，规避多套安全产品策略冲突、执行不一致的问题。
- 统一资产：硬件基础信息、已安装软件清单、所属策略归属、终端行为日志、历史告警事件等全要素数据，资产档案一站式呈现，实现终端资产全景可视。
- 统一审计：支持按人员、终端、时间维度开展联合检索与关联分析，形成完整、可核验的安全审计证据链，满足等保、保密检查等合规审计要求。

2.2.3 一体化带来的直接收益

最直接的变化是运维界面从多个减为一个。对多数企业而言，这意味着少维护若干套账号、少维护若干份资产表、少处理若干套互不关联的告警。

系统数量减少带来的不只是成本下降，更是判断力的恢复——当所有事实集中在一处，安全团队才有可能做真正的分析，而不是在系统之间搬运数据。

2.3 能力矩阵

十二项统一能力按下表分布，覆盖资产、行为、管控、数据、边界五个方向。

方向	统一能力	解决的问题
资产	统一部署、统一资产	设备在哪、装了什么、谁在用
可视	统一可视、统一桌面	屏幕上发生了什么、桌面是否一致
审计	统一审计、统一画像、统一分析	行为是否合规、状态是否异常、效率是否合理
管控	统一管控、统一运维、统一预警	该禁的是否禁住、故障能否快速处理、风险能否提前发现
数据	统一加密	文件离开授权环境后是否仍受控
边界	统一边界	终端自身的网络出入口是否可控

图 1-3 产品能力矩阵

2.4 方案内容

2.4.1 统一部署

核心痛点：端点分散在总部、分支、车间、门店，逐台上门安装不现实，版本不一致可能导致同一策略在不同终端上表现不同。

功能详解：

支持集中下发安装包，客户端填写基本信息（包含客户端昵称、部门）后，自动接入管理端。接入后可以看到客户端基本信息，包括 IP 地址、所属部门、MAC 地址、操作系统、客户端版本、在线状态等。

功能价值：部署周期从“数周逐台”压缩到“数日批量”，且过程可见，IT 不必反复核对，

版本一致性得到保证。

2.4.2 统一资产

核心痛点：资产台账靠人工维护，与实际设备长期不符，硬件更换、软件私装、设备报废没有记录，盘点一次要停半天工，结果仍不可信。

功能详解：

终端自动上报硬件构成（CPU、内存、硬盘、网卡、显示器、外接设备）与软件清单（已装程序、版本、安装日期），形成实时资产台账；

硬件变更与软件安装卸载实时上报差异，记录变更前后信息，且支持导出资产报表与盘点清单。

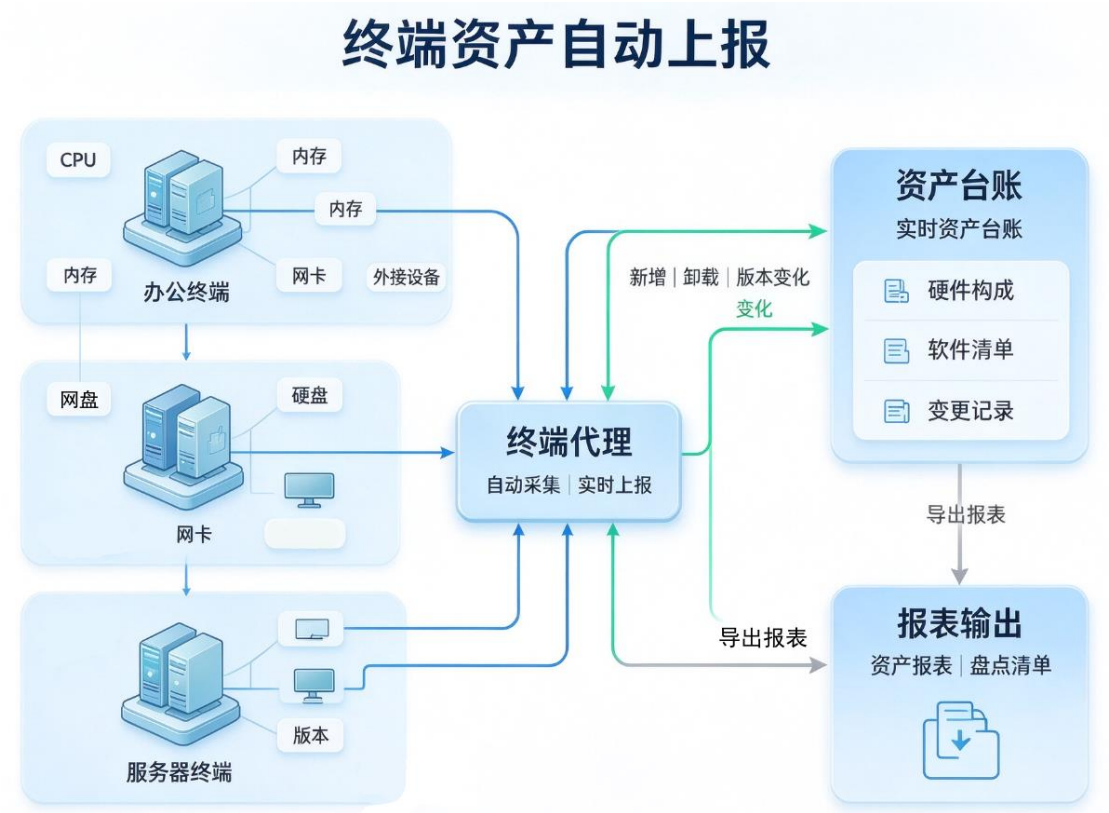


图 1-4 统一资产管理

功能价值：资产从“定期盘”变为“持续准”，盘点由现场清点转为系统导出，一次盘点的时间从数天缩短到数分钟，且结果可复核。

2.4.3 统一可视

核心痛点：终端上到底发生了什么，管理者只能靠汇报与抽查，涉及违规操作的争议，往往因为没有画面证据而无法认定。

功能详解：

平台提供实时屏幕、屏幕快照、屏幕录像三类可视化审计手段，构建终端操作行为可视化监管能力。

- 实时屏幕：支持多终端同屏查看，管理员可按需选择目标终端，同步监看终端实时操作画面，满足批量终端巡检、重点岗位实时监管需求。
- 屏幕快照：支持基于安全策略配置，实现定时自动抓取（2-60 秒自定义），按时间序列留存终端屏幕图像，完整记录关键节点操作画面，便于事后核查关键操作片段。
- 屏幕录像：在授权管控范围内，对终端操作全过程进行录制留存，支持按指定时间点定位回溯，完整还原终端操作场景，为安全事件溯源、违规行为认定提供直观依据。

功能价值：把“听说”变成“看见”，争议处置有画面依据，操作规范检查有客观材料，同时通过权限与留痕约束查看行为本身，避免监控能力被误用。

2.4.4 统一审计

核心痛点：行为记录散落在多套系统中，文档操作在一处、上网记录在另一处、邮件与移动介质各自独立，核查时需要在多个后台之间拼接，一份完整清单往往要花数天。

平台支持对七类终端关键操作行为实施统一采集、标准化归集留存，覆盖终端全场景操作轨迹。

- 文档操作：捕获文件新建、打开、修改、删除、重命名等操作事件；
- 进程列表：记录进程名、进程 id、用户名、CPU 占用率、内存占用等信息；
- 网站浏览：采集客户端、用户、所属部门、网页地址、网页标题、浏览器、审计时间等上网数据；
- 网络搜索：捕获搜索关键词、搜索引擎、搜索发生时间；
- 邮件收发：留存客户端、用户、部门、发件人、收件人、主题、附件数量、审计时间等邮件相关日志；
- U 盘使用日志：包括挂载点、卷标、容量、标识、序列号、USB 实例、磁盘驱动器实例、

昵称、描述、动作、审计时间等信息；

- 上传下载：记录文件名、文件大小、动作类型、途径、详情、附件、审计时间等信息。

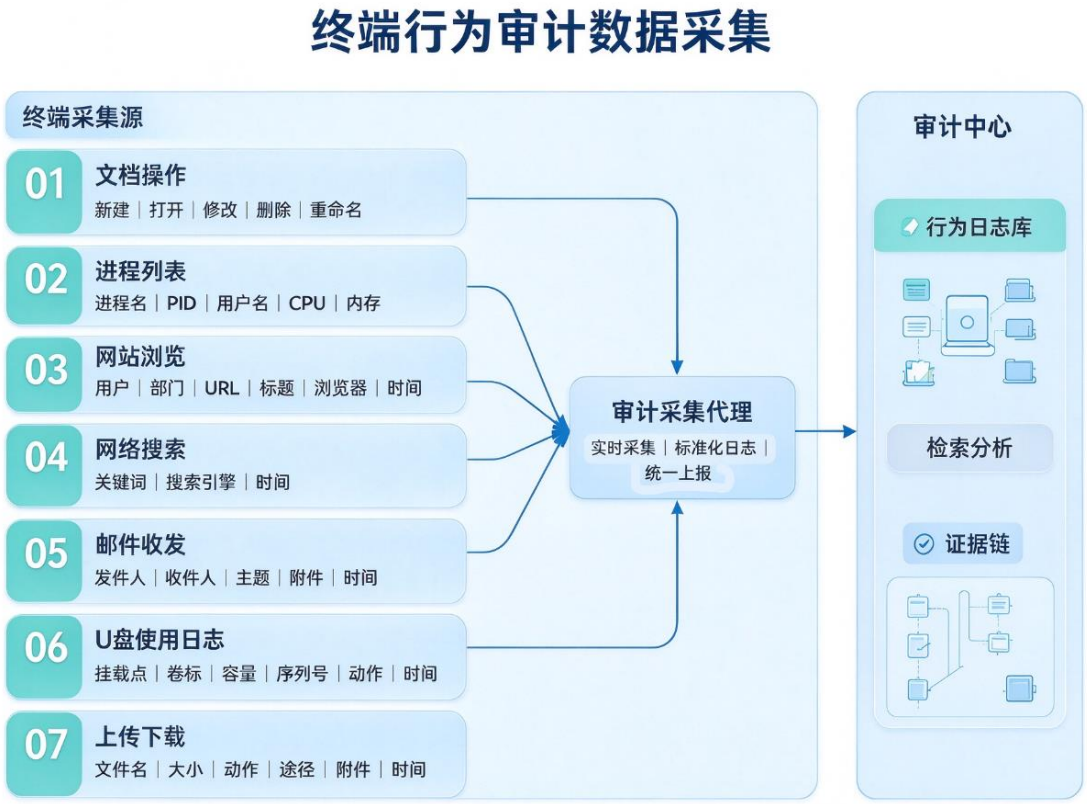


图 1-5 终端行为审计数据采集

功能价值：该能力推动终端审计模式由传统零散日志逐条翻阅，转向以人为中心、以设备为载体的一体化档案核查模式，大幅压缩安全事件溯源、合规核查的处置周期。

2.4.5 统一桌面

核心痛点：同一单位的终端桌面五花八门，壁纸、屏保各不相同，桌面文件随意堆放，交接时无从整理。

功能详解：

- 统一壁纸屏保联动

平台支持统一壁纸与屏保策略联动下发，管理员可在管理控制台集中编排配置，面向全单位终端批量推送预置企业标识 Logo、保密警示宣传内容的桌面壁纸及屏保方案。策略下发后终端自动完成同步生效，无需逐台人工配置。

- 客户端工具定制

平台支持管理员对终端客户端助手进行自定义配置，可按需将指定业务程序、业务网页添加

至客户端助手快捷入口。该快捷入口具备防篡改保护机制，终端本地用户无法自行删除、修改已配置的快捷项，保障业务访问入口稳定统一。

- 文档快搜

平台内置终端本地文档快速检索能力，员工可在终端本地启用文档快搜功能，通过输入文件关键词即可对本机文档进行检索定位，快速查找目标文件，优化本地文件查找效率，解决传统系统检索速度慢、检索能力有限的问题。

功能价值：该组配套运维与办公辅助功能，在不增加基层终端运维负担的前提下，实现安全宣贯标准化、业务入口固化管控与本地文档高效检索三者协同，实现安全管理与业务效率双向兼顾。

2.4.6 统一管控

核心痛点：员工在工作时间运行与工作无关的程序、访问与工作无关的网站、随意插入 U 盘与外设，管控一旦靠自觉，执行情况就无法掌握。

功能详解

- 程序黑白名单管控：白名单是指仅允许名单内的软件运行，其他软件无法打开；黑名单是指禁止名单内的软件运行，其他软件不做限制，可根据业务场景灵活切换管控模式。
- 网站黑白名单管控：与程序黑白名单管控原则类似，只不过它针对的网站，可以实现不同时段上网访问权限灵活调整，精准规范公务上网访问边界。
- U 盘管控：针对 U 盘等移动存储介质，可设置完全禁用、仅读取、仅写入、允许使用，实现移动存储介质全生命周期精细化管控，防范涉密与内部文件经由移动介质违规拷贝外泄。
- USB 端口管控：可分别针对 USB 存储设备、打印机、串口、并口、蓝牙、光驱、红外等外设进行启用或禁用策略配置，按业务需要开放必要外设，封堵非授权外设接入通道，实现 USB 接口分类型可控管理。

2.4.7 统一运维

核心痛点：员工报障后，IT 需要到工位现场处理，跨楼层、跨基地的工单响应周期长，远程工具本身缺少管控，存在被滥用为外泄通道的风险。

功能详解：

支持对授权终端发起远程控制，协助模式有交互模式、旁观模式、兼容模式、独占模式、无人值守。同时，支持远程桌面查看、远程文件传输、远程批量操作。

功能价值：故障平均处理时长下降，跨基地支持成本降低，同时杜绝了远程工具被当作外泄通道的隐患。

2.4.8 统一画像

核心痛点：管理者对一名员工的工作状态判断，主要依赖印象与汇报，加班、离岗、专注度、协作频次这些维度缺少客观依据。

功能详解：

平台面向管理人员提供员工终端操作时间画像能力，基于终端采集的操作行为数据，直观呈现员工每日上岗起始时间、中途休息时长、累计办公时长、网页访问时长、应用程序运行时长等维度信息，完整刻画员工终端操作时间分布特征，实现人员办公行为时序可视化。

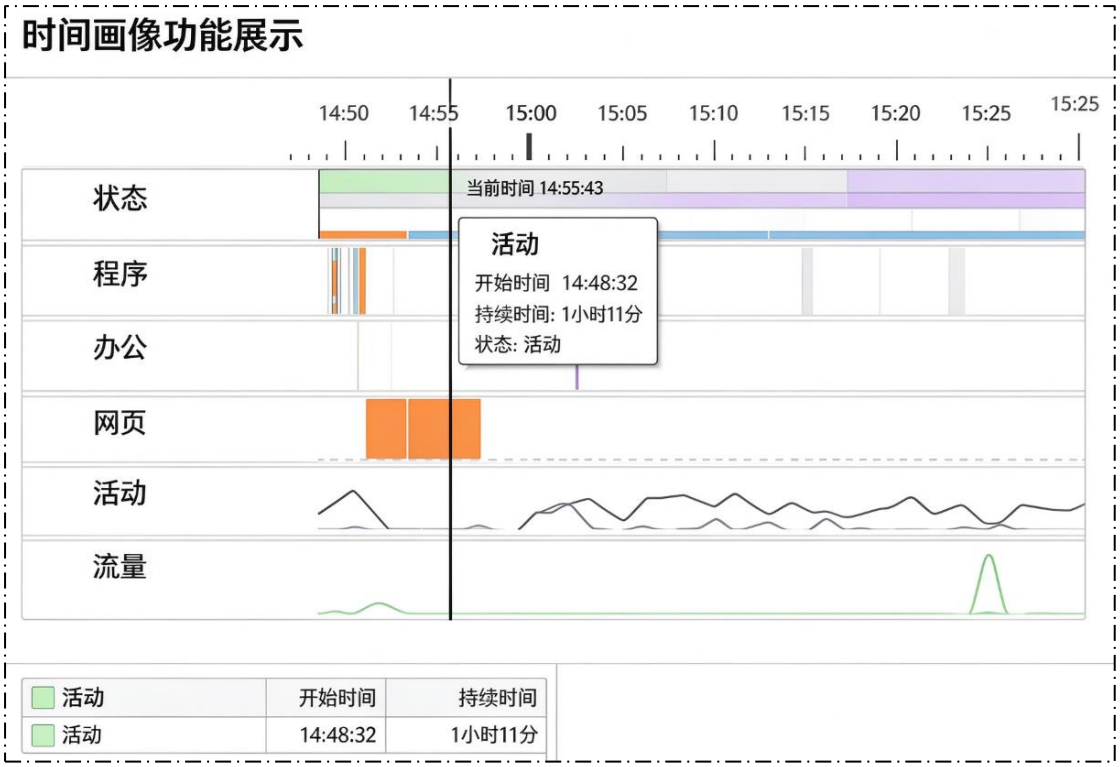


图 1-6 终端画像功能展示

2.4.9 统一分析

核心痛点：工作效率高低、人员是否有离职倾向，管理层只能凭感觉。

功能详解：

- 工作效率统计分析：平台内置工作效率统计模块，可对团队整体办公效能进行汇总分析，统计指标涵盖参与统计总人数、人均每日办公时长、日均活跃操作时长、怠工人员数量等，以量化数据呈现团队整体办公活跃状态，支撑管理人员掌握团队整体效能情况。
- 终端使用率分析：平台提供终端设备使用率多维统计报表，统计维度包含终端客户端、统计日期、设备开机总时长、有效活动时长、人员离开时长、待机时长、办公时长，全面反映单台终端设备的资源利用情况，实现终端资产使用情况量化监测。
- 离职风险分析：核心统计指标包含分析总人数、人员异动人数、高危风险人数，辅助管理人员直观识别人员异常行为信号，提前感知潜在人员异动风险。

功能价值：管理决策有了量化依据，可及时识别异常作息、终端长时间空闲等风险信号，实现风险早发现、早干预，辅助管理决策更加科学精准。

2.4.10 统一预警

核心痛点：敏感信息外流、违规外联、设备异常变更，往往在造成后果后才被发现；多套系统的告警各自弹出，真正重要的那条淹没在噪声里。

功能详解：

- 敏感词报警：按关键词、正则、文件指纹识别含敏感内容的文件，命中即告警并可阻断；
- 违规外联报警：检测私接热点、加装无线上网设备、内外网同时连接，实时上报并可阻断；
- 软硬件变化报警：硬件更换、软件安装、安全客户端被卸载等变更实时告警，关键变更可自动恢复。



图 1-7 统一预警能力

功能价值：发现时点从“事后”前移到“事中”。告警经过分级与合并后数量可控，团队能把精力放在真正需要处置的那部分。

2.4.11 统一加密

核心痛点：设计图纸、客户资料、财务报表、源代码在终端上以明文存在，一旦被拷贝、误发、随设备丢失，损失不可逆。

功能详解：对指定类型与目录的文件自动加密，脱离授权环境即为密文。如有正常外发需求，可以申请解密或制作成外发包，管理员审批通过后可正常外发。

功能价值：加密在系统层完成，业务程序无需改造，用户操作习惯不变。

2.4.12 统一边界

核心痛点：终端自身的网络出入口缺少控制，程序可随意连接外部地址，端口可随意开放，终端在被感染后成为向内网扩散的跳板。

功能详解：

- IP 端口防火墙管控

网站通常承载网页访问、文件上传、邮件收发等多类业务服务，不同业务服务依托独立端口

通信，管理员通过配置目标 IP 及对应端口，能够实现对该网站单项服务的精准限制，而非整站一刀切拦截。

- 指定程序端口访问管控

不同网络服务依托对应端口进行通信，例如 443 端口为 HTTPS 协议通信端口，对目标程序配置阻断 80、443 端口后，即可限制该程序访问 HTTPS 类网站，按应用独立管控网络通信通道，避免全局端口管控影响其他正常业务程序。

- 程序内网地址访问管控

支持配置策略，禁止指定程序访问、扫描内网设备地址，覆盖内网打印机、共享文件服务器、路由设备等内网资产，阻断程序对内网资产的探测扫描行为，防范病毒、恶意程序对内网设施发起探测与攻击，强化内网区域安全防护，保障内部网络基础设施稳定安全。

功能价值：即使终端已在内网，其对外连接仍受约束，横向移动与数据外传的通道被同时收窄。

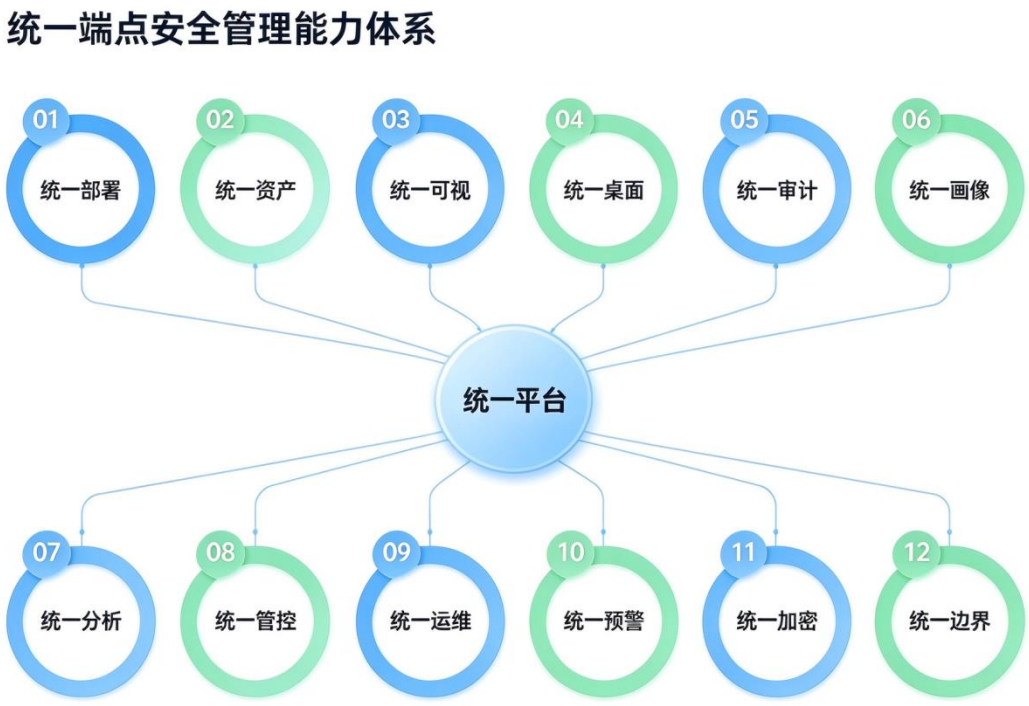


图 1-8 统一端点安全管理能力体系

三、产品部署

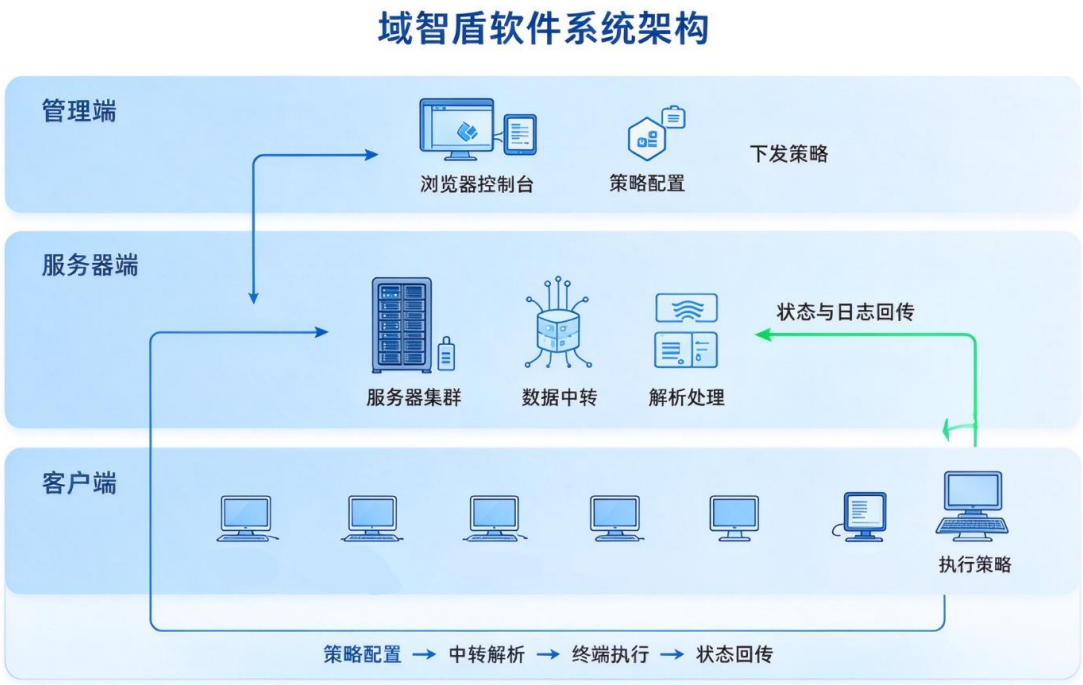


图 1-9 产品部署架构

四、方案创新与价值

4.1 结构创新

- 一管多端：把多种客户端形态收进同一个管理端，企业不再需要为“办公终端一套、服务器一套、云桌面一套”分别维护，管理口径从源头统一。
- 能力可编排：十二项能力不是并列的功能开关，而是可编排的组合，形成对某个具体风险场景的整体应对，而不是逐项打补丁。
- 同源数据：资产、行为、告警、审批共用同一套标识，不必在系统之间搬运与核对。

4.2 工程创新

- 低占用：客户端在测试环境中 CPU 占用约 5%，峰值不超过 8%；策略全开情况下内存占用一般不超过 100MB。

- 离线可用：终端脱离管理网络时，本地策略继续生效，行为记录在本地执行并缓存，恢复连接后自动回传。
- 私有化部署：全部业务数据存储在客户自有服务器，客户端仅保留必要临时缓存，不占用大量本地磁盘空间。
- 审批可外接：可免费对接钉钉、企业微信、飞书，审批消息直达员工日常工作平台。

4.3 价值落点

- 看得见：资产、行为、屏幕、告警集中呈现，管理判断建立在自己看到的事实上。
- 管得住：程序、网站、外设、文件、网络五个方向均有执行层，制度不再停留在文本。
- 说得清：记录同源、可联合检索，事件复盘与合规检查使用同一份材料。
- 省得下：部署、补丁、软件、盘点和故障处理批量化执行，人力瓶颈得到缓解。
- 可运营：每一项能力都有对应指标，安全工作可以被度量、被考核、被迭代。

五、 资质与荣誉



图 1-10 资质与荣誉

六、 落地方法

阶段一：明确对象

企业先行梳理终端资产底数，圈定纳入统一端点安全管理的终端范围、岗位角色与核心数据资产类型，优先覆盖研发、工艺、财务、人事、涉密办公等高价值终端，完成终端分组、部门归属、角色权限基线确认。

阶段二：启用模块

优先上线基础端点管控能力，部署服务端与客户端代理，启用终端资产采集、外设管控、进

程管控、透明加密等基础模块，完成基础权限策略下发，验证专业业务软件正常运行，确认终端日常打开、编辑、打印等业务操作无异常，保障安全策略对业务无感，夯实端点统一管控底座。

阶段三：小范围试用

选取 1-2 个核心部门开展试点验证，逐步叠加高级能力，包括敏感内容识别、邮件外发审批、受控外发包、屏幕水印、行为审计告警等模块，测试策略联动效果，校验审批流程、拦截规则、告警机制是否贴合企业真实业务流转，收集业务部门反馈，迭代优化策略阈值与例外规则，验证系统稳定性与业务适配性。

阶段四：推广固化

试点验收通过后，按照组织架构分批次全量推广至全部终端，完善全维度安全策略体系，形成常态化端点安全运营体系，持续迭代优化，保障体系长期稳定运行。



图 1-11 产品落地方法

七、实践案例

某综合性集团企业面临终端分散，资产底数不清，终端安全策略各自独立，缺乏统一管控平台，存在违规软件安装、非法外设接入、办公文档外泄、运维远程操作无审计等问题，需要一套统一端点安全管理平台，实现资产可视化、办公安全管控、运维工具集成一体化。



部署域智盾统一端点安全管理系统，完成全集团终端资产盘点分组，启用桌管工具、软件管家等模块，同时叠加外设管控、行为审计能力；先在总部职能部门试点，再分批次向下属分支机构推广，建立分级权限管理，按部门差异化下发安全策略。

建设成效

实现集团终端资产统一视图，终端身份信息可在线查看，标准化桌管运维工具统一下发，软件资产可盘点管控，远程协助、水印、备份等运维安全能力一体化落地，提升集团终端标准化管理与办公数据安全管控能力，降低分散运维成本。

八、未来展望

- 一体化将进一步向业务侧延伸

端点管理平台正在成为企业 IT 的基础设施之一，与身份系统、业务系统、审计系统联动。它的价值不再只是安全，还包括资产准确性、运维效率与合规输出，这三项恰好都是业务部门关心的事。

- 数据的可用不可见

在保护个人信息的前提下使用数据做分析，是《个人信息保护法》实施后的现实课题。方向是通过脱敏、去标识化与权限隔离，让数据在被使用时尽量少暴露原始信息，这将成为端点管理产品的新能力项。

- 我们的判断

统一端点安全管理的下一步，不是继续增加功能项，而是把端点产生的数据真正变成可用的治理资产。域智盾软件将在识别能力、跨平台覆盖与运营效率三个方向持续投入、与时俱进，让系统成为客户长期依赖的工作方式，而不是一次性交付的软件。

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，用于说明统一端点安全管理系统的技术立场、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修订本文件的权利，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