产 品 技 术 白 皮 书

安企神

上网行为审计系统

白 皮 书

让每一条网络足迹

看得见 · 可追溯 · 能取证

石家庄安企神网络科技有限公司

2026 年 11 月 · V1.0

序 言 5

一、行业现状 5

1.1 效率损耗：隐性成本持续侵蚀组织效能 5

1.2 网络通道：数据外泄的主路径 6

1.3 合规压力：日志可查成为法定要求 6

1.4 治理困境：现有方式为何力不从心 6

二、技术介绍 7

2.1 方案概述 7

2.2 核心功能详解 8

2.2.1 网页浏览审计 8

2.2.2 搜索关键词审计 8

2.2.3 上传下载行为审计 8

2.2.4 程序使用审计 9

2.2.5 文件操作审计 9

2.2.6 时间画像与行为分析 9

2.2.7 屏幕审计：实时、录像与快照 9

2.2.8 带宽流量审计 10

2.3 从审计到管控：闭环治理 10

2.4 协同关系 11

三、方案创新与价值 12

3.1 结构性创新 12

3.1.1 从"多套系统"到"一套事实" 12
3.1.2 从"一刀切"到"组织授权" 12
3.1.3 从"事后追溯"到"事前预警" 13
3.2 工程性价值 13
3.3 运营性价值 13
四、落地方法论 14
4.1 阶段划分 14
4.2 合规与隐私边界 15
4.3 常见顾虑与回应 15
五、典型应用场景与服务保障 16
5.1 行业应用场景 16
5.2 服务保障 16
六、资质与认证 17
6.1 公司概况 17
6.2 资质与认证 17
6.3 服务客户（部分） 17
七、未来展望 17
7.1 行为分析正在与人工智能合流 17
7.2 从"工具"走向"可运营的能力" 18
7.3 我们的判断 18
版权说明 18

免责声明 18

序 言

近几年，企业数据安全事件的复盘结论高度一致：风险大多不是从网络边界突破的，而是从内部终端走出的——一次随意的文件上传、一个个人网盘的后台同步、一段占用整个下午的视频娱乐，都可能成为效率损耗与数据外泄的起点。终端上的网络行为，既是业务运转的载体，也是风险滋生的通道。

与此同时，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，等级保护 2.0 体系亦将安全审计列为重要控制项。法律法规对企业提出了一个明确的要求：能够回答"谁、在什么时间、访问了什么、做了什么操作"，并且相关记录可查询、可导出、可取证。

上网行为审计，正是回答这个问题的技术底座。它让每一条网络足迹看得见、可追溯、能取证，是效率管理、数据防泄密与合规审查的共同前提。

本白皮书共七个章节。第一章分析企业上网行为治理面临的现状与短板；第二章说明安企神上网行为审计系统的技术构成与核心功能；第三章讨论方案的创新点与价值；第四章给出一条可以照着走的落地路径，并明确合规与隐私边界；第五章呈现典型应用场景与服务保障；第六章说明公司资质与认证情况；第七章是对未来的判断。

一、行业现状

1.1 效率损耗：隐性成本持续侵蚀组织效能

行业公开报道的数据显示，企业员工每个工作日平均有超过 2.5 小时用于与工作无关的上网活动，炒股、购物、短视频与追剧占据主要份额。以 50 人规模的团队测算，由此产生的隐性生产力损失每年可达数十万元。更值得警惕的是，这类行为高度隐蔽：员工删除浏览器历史记录、使用隐身模式或切换窗口，都足以让目视巡查失效，管理者既发现不了，也难以量化。

1.2 网络通道：数据外泄的主路径

终端上的每一次文件上传、网盘同步、邮件外发与即时通讯传输，都是潜在的数据出口。员工离职前批量拷贝资料、通过个人网盘外传客户数据、使用未经授权的传输工具等行为，若缺乏完整的审计留痕，企业往往在损失发生后仍无法还原事件全貌，更难以界定责任。

1.3 合规压力：日志可查成为法定要求

《中华人民共和国网络安全法》对企业网络日志留存提出明确要求，等级保护 2.0 体系将安全审计列为重要控制项。在监管检查与客户审计中，企业需要证明自身具备完整的行为记录能力。没有体系化的上网行为审计，合规审查将无从谈起。

1.4 治理困境：现有方式为何力不从心

必须承认，多数企业并非没有做管理，而是管理方式存在问题。以下四个短板在实践中反复出现：

- 制度无法落地为策略：《员工上网管理规定》写得清楚，但"工作时间不得从事无关活动"在终端上没有对应的技术动作，制度停留在纸面；
- 单点堆叠，彼此不通：上网管控、桌管、DLP 各自成体系，各自有客户端与后台，数据互相孤立，无法形成完整的行为视图；
- 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，安全和管理团队每天面对海量记录，最终只能选择不看；
- 无记录，即无证据：事件进入调查或仲裁阶段后，缺少终端侧的行为记录，无法形成有效证据。

这四个短板的共同点，是把上网行为治理当作"采购问题"而不是"治理问题"。而行为治理的本质，是一项需要长期运营的管理工作，其起点是一套完整、可信的审计体系。

二、技术介绍

2.1 方案概述

安企神上网行为审计系统是安企神软件终端安全管理体系的组成部分。安企神软件由石家庄安企神网络科技有限公司研发，打造全生命周期一站式信息安全整体解决方案平台，集文档加密、电脑行为审计、终端安全管理、网络准入控制、敏感内容识别、IT 运维管理等 200 余项功能于一体。在整体体系中，上网行为审计是数据基座：它完整记录终端的上网行为信息，形成可检索、可分析、可导出的行为档案，向上支撑上网权限管控、数据防泄密与终端安全管理，构成"审计—管控—防护—响应"的闭环。

系统采用"终端客户端 + 管理控制台"的集中式架构，支持 B/S、C/S 双重模式：C/S 架构侧重底层安全防护，保障系统自身安全性；B/S 架构便捷易用，网页即可登录管理，无需安装管理端。终端侧客户端轻量驻留，采集网络行为、应用行为与屏幕画面；管理侧完成策略下发、数据汇聚、检索分析与报表输出，支持计算机、用户双重管理模式，管理员在统一后台即可完成全网策略配置与审计审查。



图 1　系统技术架构

在部署与运行方面，系统具备以下工程特性：

- **本地私有化部署**：业务数据留存于用户自有环境，保障数据可控；服务器数据库一键式安装，轻量部署，使用 MySQL 数据库，大型用户支持对接 Oracle 数据库；
- **终端资源占用低**：客户端安装包约 80M，标准环境下安装约 10 秒；测试环境中 CPU 占用约 5%、最高不超过 8%，策略全开内存占用一般不超过 100MB，对终端整机资源消耗控制较好；
- **系统兼容性好**：兼容 Windows、Linux、Mac 及信创系统；
- **运维成本低**：界面简洁、功能划分清晰，降低管理员学习成本；版本按市场需求按需迭代，通常 1-2 个月发布一版。

2.2 核心功能详解

2.2.1 网页浏览审计

解决什么问题：企业需要知道员工上班时间访问了哪些网站、停留了多久，事后能否还原访问内容。

功能价值：系统完整记录每台终端访问的每一个网站，包括 URL 地址、页面标题、访问时间、停留时长与访问频率，支持直接点击 URL 还原访问内容；每项审计记录配备对应的实时屏幕截图，做到"有图有真相"。所有浏览行为自动归档，支持按部门、人员或时间段快速检索。

2.2.2 搜索关键词审计

解决什么问题：搜索行为往往先于违规动作发生，是企业洞察员工意图的重要信号。

功能价值：员工在浏览器中执行的每一次搜索，其关键词均被完整记录；高频关键词可生成词云统计，帮助管理者掌握员工关注焦点，及时发现异常意图，如大量搜索求职、兼职相关内容。

2.2.3 上传下载行为审计

解决什么问题：文件经由网络通道外传，是数据泄露最直接的形态。

功能价值：系统精准记录通过浏览器、网盘、FTP 等通道进行的文件上传下载行为，包括文件名、大小、时间与来源路径。任何经网络通道外传文件的操作均有完整留痕，一旦发生数据泄露事件，可快速定位外发文件、外发通道与责任人。

2.2.4 程序使用审计

解决什么问题：管理者需要客观依据判断员工是在专注办公，还是长时间运行与工作无关的程序。

功能价值：系统实时记录所有应用程序的启动时间、关闭时间、累计使用时长与窗口活动状态，自动分类统计生成报表，为绩效考核与行为管理提供数据支撑。

2.2.5 文件操作审计

解决什么问题：敏感文档在终端上的流转需要全程可溯。

功能价值：系统对文件的新建、修改、复制、删除、重命名及外发行为进行全维度审计，自动记录文件名、路径、操作时间及目标位置；发现敏感文档异常流转时立即触发告警，与数据防泄密能力形成联动。

2.2.6 时间画像与行为分析

解决什么问题：零散的审计记录需要汇聚为管理者可读、可用的决策依据。

功能价值：系统整合每日操作数据，为每位员工生成"时间画像"，图形化展示各时间段计算机使用情况，精确到秒，直观呈现工作活跃度、应用使用分布与网络行为规律；在此之上自动生成工作效率报告、风险行为统计等多维报表，并结合异常行为（如大量下载公司资料、频繁访问求职网站）辅助识别离职风险。

2.2.7 屏幕审计：实时、录像与快照

解决什么问题：文字日志之外，企业还需要可视化的证据层。

功能价值：

- 实时屏幕：管理员可远程实时查看员工屏幕画面，最多可同时查看 16 台设备；

- 屏幕录像：支持 7×24 小时录制终端操作过程，关键事件自动存档，支持按时间线回放与检索；
- 屏幕快照：按设定时间间隔自动截屏，或在检测到敏感操作时即时抓拍。

一旦发生数据泄露或违规操作，管理者可通过回溯画面还原事件全貌，为追责取证提供直观依据。

2.2.8 带宽流量审计

解决什么问题：带宽被谁占用、是否存在异常大流量传输，需要实时可见。

功能价值：系统实时抓取并可视化展示每台终端的上传、下载流量，支持按部门、按应用、按时间段分类统计；当某台终端出现异常大流量传输时即时告警，帮助管理员第一时间发现数据外泄或 P2P 下载占用带宽等问题。

2.3 从审计到管控：闭环治理

审计记录的价值最终要落在治理动作上。安企神提供与审计数据深度联动的管控能力：

管控能力	机制说明
网站黑名单	自定义禁止访问的网址或网站类别（购物、游戏、短视频等），内置海量网址库，尝试访问即被拦截并记录告警
网站白名单	仅允许访问企业指定网站，支持分时段策略：工作时段严格管控，休息时段适度放开
程序黑名单	禁止运行与工作无关的程序，程序启动时从操作系统层面直接拦截
程序白名单	仅允许使用指定办公软件，杜绝私自安装程序带来的效率与安全隐患

管控能力	机制说明
敏感词报警	内置智能敏感词库并支持自定义关键词，员工在聊天、邮件、文档编辑或搜索中输入敏感内容时实时推送报警并保存上下文日志
流量管控	支持全局网速上限、按角色差异化带宽分配与日/月流量限额，超限自动断网，保障核心业务畅通

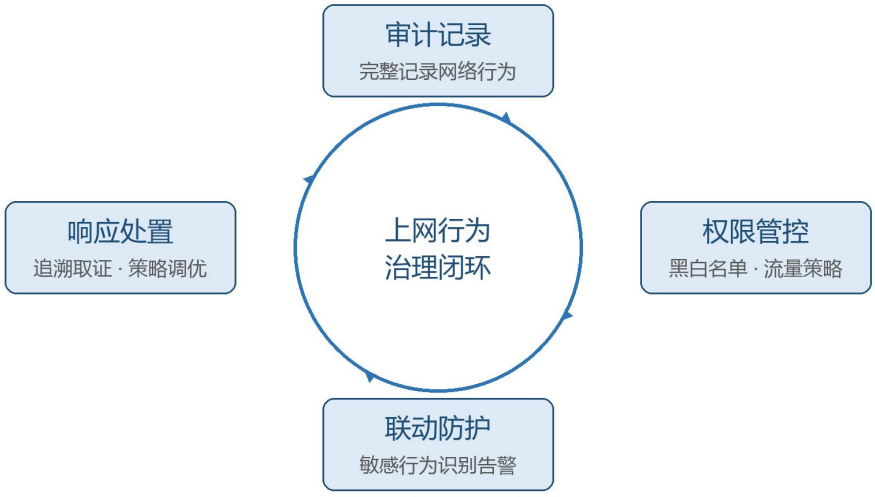


图 2　上网行为治理闭环

2.4 协同关系

上述能力不是并列的功能清单，而是有明确分工的层次结构：

第一层，审计记录：完整、真实地记录网络行为，形成全网统一的行为档案；

第二层，权限管控：基于审计数据实施黑白名单与流量策略，从源头阻断高风险访问与违规程序运行；

第三层，联动防护：与数据防泄密、终端安全管理协同，通过敏感行为识别与实时告警，在风

险演变为损失之前完成干预。



图 3　审计—管控—防护三层协同关系

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"

不少企业的上网治理建设是加法：缺审计加审计，缺管控加管控。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数据。安企神把行为审计、权限管控、数据防泄密收敛到同一套底座，同一台终端在审计视图、策略视图、告警视图中是同一个对象，字段一致、时间线对齐，管理者面对的是"一套事实"。

3.1.2 从"一刀切"到"组织授权"

策略的载体不是"全公司"，而是部门、岗位与时段。安全或管理团队配置的不是"是否允许上网"，而是"研发部门仅允许访问指定站点、市场部门审批后放开、休息时段适度开放"。审计数据按组织维度聚合，报表与考核口径天然对齐。

3.1.3 从"事后追溯"到"事前预警"

审计能力不止用于事后。批量下载公司资料、非工作时段的异常活跃、连续多日的求职类搜索，这些组合行为本身构成风险信号。系统对敏感行为做实时识别与告警，把干预动作提前到损失发生之前。

3.2 工程性价值

低干扰的终端体验。

客户端安装约 10 秒、CPU 占用约 5%、策略全开内存一般不超过 100MB，员工在日常办公中几乎无感，这是审计策略能够全网落地、长期运行的前提。

数据可控的私有化部署。

全部业务数据留存于用户自有服务器，客户端仅保留必要缓存；审计数据这种高敏感度的企业资产，从一开始就留在企业自己的边界之内。

可验证的证据链。

每条记录对应到具体的人、具体的终端、具体的时间，浏览行为可还原页面内容，屏幕审计提供可视化佐证，事件复盘不再依赖回忆与推测。

3.3 运营性价值

- 合规可举证：策略配置、审计记录、告警处置形成完整闭环，可直接支撑等保测评、行业监管检查与客户方审计；
- 风险可量化：违规访问次数、敏感词命中数、异常流量次数，管理工作的价值第一次可以被度量；
- 效率可提升：审计数据让排班、考核与带宽分配有据可依，隐性工时损耗被显性化；
- 责任可归属：每一次外发、每一条访问都对应到人，跨部门的争议复盘有了客观依据。

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：制度先行。 先完善员工上网管理制度并完成告知程序，再启用技术手段，确保审计行为于法有据、于规有依。这一阶段不部署，只做事实收集：梳理终端总量与分布、确认组织架构与岗位职责、明确合规约束。

阶段二：试点观察。 选择一个有代表性的部门做试点，第一阶段仅开启审计记录（观察期），不启用任何拦截类策略，积累基线数据，统一配置流程与实施经验。

阶段三：策略调优与固化。 依据试点数据实施黑白名单、敏感词与流量策略。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。系统支持委托审批、批量审批，并可免费对接钉钉、企业微信、飞书进行审批。

阶段四：分批推广。 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；按部门、角色与时段配置差异化策略，避免"一刀切"影响业务与士气。

阶段五：常态化运营。 上线不是终点。建议建立三项固定动作：月度行为复盘（查看告警分布、误报率与业务投诉，调整策略）；季度合规输出（导出审计报表与处置记录，供内审与外部检查）；定期策略复核（明确审计数据保存期限、查看权限与导出审批流程）。



图 4　五阶段落地路径

4.2 合规与隐私边界

上网行为审计记录可导出为合规报告与法律证据，满足《网络安全法》日志留存要求与等级保护审计控制项，帮助企业建立"可验证的责任链"。同时，行为审计涉及员工个人信息处理，企业在部署时应遵循以下原则：

- **知情同意**：通过规章制度、员工手册或入职责工协议明确告知监控行为的存在、范围与用途，取得员工知情确认；
- **最小必要**：审计范围限定于工作时间、工作设备与工作相关行为，避免采集与企业管理目的无直接关联的私人信息；
- **权限分立**：审计数据查看权限仅授予经授权的管理角色，操作日志本身同样纳入审计，防止审计能力被滥用；
- **用途限定**：审计数据仅用于安全管理、合规审查与绩效评估等声明过的目的，不得挪作他用。

规范部署的上网行为审计系统，不仅是企业合规义务的履行者，也应当是员工个人信息的守护者。

4.3 常见顾虑与回应

会不会影响业务效率？ 不会。审计在后台自动进行，策略自动化执行，无需员工手动操作；客户端资源占用低，实测不影响正常办公。

员工会不会抵触？ 抵触的来源通常不是审计本身，而是"被突然阻断且没有解释"。因此建议上线前做一次面向全员的说明，所有阻断类策略都配置申请通道，阻断的同时告知原因与申诉路径。

外包与驻场人员怎么管？ 为外包团队建立独立账号与独立策略区域，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？ 系统兼容 Windows、Linux、Mac 及信创系统；对确不具备

安装条件的设备，可通过网络层手段做访问限制，不强行安装客户端。

五、典型应用场景与服务保障

5.1 行业应用场景

行业 / 场景	核心诉求	安企神应对
制造 / 设计企业	图纸等核心资产防外泄、外发留痕	上传下载审计 + 文件操作审计 + 敏感行为告警
电商 / 客服中心	服务过程可回溯、工时透明	实时屏幕 + 屏幕录像 + 时间画像
金融 / 律所	严格合规审查、日志可取证	全量行为归档 + 合规报告导出 + 权限分立
通用办公型企业	提升效率、遏制无关上网	网页 / 程序审计 + 黑白名单管控 + 效率报表

典型成效示例：某美术外包工作室曾将项目延期归因于人力不足，经软件使用情况与交付记录比对后发现，部分人员每日在绘图软件上的有效时长不足三小时，其余工时散落在短视频与购物页面。部署行为审计后，管理层得以基于数据优化排班与考核，交付准时率显著回升。

5.2 服务保障

- **实施部署**：按照分步实施原则开展，先试点、后推广；针对采购的功能模块提供专项培训，包含平台操作使用与数据防泄漏实践经验分享；
- **售后响应**：为每个客户指定 1 名专属工程师，提供长期电话、QQ、Email 等多种方式的远程技术支持，工作日响应时间不超过 5 分钟；周一至周六技术支持到晚上 21:00，周日及节假日各岗位均有值班；
- **版本升级**：提供软件版本升级与新功能发布通告服务，通常 1-2 个月发布一版，按客户

业务需求持续迭代；

- **灵活采购**：支持模块化灵活采购，单台被管理终端 60 元起，最终价格根据所选功能模块与部署规模综合确定；提供 7 天免费试用。

六、资质与认证

6.1 公司概况

石家庄安企神网络科技有限公司成立于 2015 年，是一家以研发信息安全类产品以及提供相关服务为主营业务的技术驱动型公司。安企神软件深耕终端安全与数据防泄密领域十余年，拥有 300 余家合作伙伴，服务万余家政企客户，累计覆盖终端超 2 亿台，广泛应用于政府、金融、运营商、制造、能源、教育、医疗等行业。

6.2 资质与认证

- 已通过 ISO9001 质量管理体系认证、ISO27001 信息安全管理体系认证；
- 河北省软件协会会员单位，获评纳税信用 A 级纳税人；
- 已入围多家中央及地方国有企业信息化供应商采购目录。

6.3 服务客户（部分）

苏州华为技术研发有限公司、清河县中心医院、重庆大学、韩国产业银行支行、太极计算机股份有限公司等。

七、未来展望

7.1 行为分析正在与人工智能合流

随着人工智能技术在行为分析领域的深入应用，上网行为审计将从事后追溯进一步走向事前预警：基于行为基线的异常检测、离职风险预测与自动化响应，将成为下一代上网行为管理体系的标配能力。

7.2 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：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、审计数据能否直接转化为管理与合规产出。

7.3 我们的判断

上网行为审计是企业内网安全治理的基础设施：它让每一条网络足迹有迹可循，让效率管理有数据可依，让合规审查有证据可查。安企神将持续投入相关方向的产品研发，以上网行为审计为数据基座，联动权限管控、数据防泄密与网络准入控制，帮助企业在数字化时代实现"安全中自由生长"。

版权说明

版权所有：石家庄安企神网络科技有限公司，保留全部权利。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。

免责声明

本白皮书由石家庄安企神网络科技有限公司编制，用于向客户及合作伙伴说明上网行为审计系统的技术立场、能力框架与实施方法，所载内容仅供参考。文中引用的行业数据来源于行业公开报道与公开统计资料，具体数值因统计口径与年份不同可能存在差异；产品功能描述基于产品当前版本整理，可能随版本迭代调整。文中引用的法律法规与标准以发布时点的公开文本为准。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。

石家庄安企神网络科技有限公司

客服热线　400-666-2563

二〇二六年十一月