产 品 技 术 白 皮 书

安企神

AI安全合规&网络安全技术

白 皮 书

看得见每一次 AI 对话
管得住每一份核心数据

石家庄安企神网络科技有限公司

2026 年 11 月 · V1.0

序言 3
一、行业现状 3
1.1 网络威胁与内部风险正在叠加 3
1.2 传统防护手段的三个局限 4
1.3 合规要求持续加码 4
二、技术介绍 4
2.1 方案概述：一个平台、两道防线、三层智能 4
2.2 网络安全纵深防护 5
2.3 AI 使用审计：看得见每一次对话 6
2.4 AI Insight：从"看见"到"看懂" 7
2.5 管理协同与部署 8
三、方案创新与价值 9
3.1 从"看不见"到"全程可见"的 AI 使用治理创新 9
3.2 从"单点防护"到"纵深协同"的网络创新 9
3.3 从"合规成本"到"合规资产"的价值创新 9
3.4 客户价值小结 9
四、落地方法论 10
4.1 五阶段实施路径 10
4.2 培训与制度共建 10
4.3 合规与隐私边界 11
4.4 常见顾虑与回应 11
五、典型应用场景与服务保障 11
5.1 行业场景 11
5.2 服务保障承诺 12
六、资质与认证 12
七、未来展望 12
版权说明 13
免责声明 13

序言

当企业的业务全面跑在网络上、当 AI 工具进入每个人的工位，安全问题正在从"防外部"变成"内外同防"：一边是勒索病毒、钓鱼链接、违规外联带来的网络侧威胁，一边是数据经由网络出口与 AI 对话悄悄流出的内部风险。更棘手的是，员工每天都在向各类 AI 提问、上传文件，这些行为超出了传统审计的视野——看得见数据，看不见流向，成为许多企业的真实困境。

安企神给出的答案是：把网络防护做扎实，把员工对 AI 的每一次使用纳入审计视野。当员工向 AI 提问、投喂文件时，企业需要知道问了什么、传了什么、风险有多大。《安企神 AI 安全合规&网络安全技术白皮书》系统阐述安企神软件在网络安全防护、AI 使用审计与 AI Insight 智能洞察方面的技术设计、落地方法与服务体系，帮助企业在"防得住"与"管得住"之间建立一套可持续运转的安全底座，同时守住合规与员工体验的边界。

石家庄安企神网络科技有限公司成立于 2015 年，深耕数据安全与终端管理领域十余年，产品与服务覆盖万余家政企客户，终端管理规模超过 2 亿台。我们希望这本白皮书成为您规划网络安全与智能审计体系时的实用参考。

一、行业现状

1.1 网络威胁与内部风险正在叠加

从外部看，勒索病毒通过漏洞与弱口令渗透进办公网，钓鱼邮件诱导员工点击恶意链接，供应链攻击让一次普通的软件更新成为入口；从内部看，员工私接热点绕开管控、通过网盘与邮箱外发敏感文件、使用未经报备的 AI 工具上传业务数据。外部攻击与内部违规往往相互

交织：攻击者利用内部管理的松懈，内部风险借助网络出口放大。单一维度的防护已经无法应对这种叠加态势。

1.2 传统防护手段的三个局限

其一是"静态"。基于固定规则的黑名单与封端口策略，跟不上应用与攻击手法的快速变化，策略永远慢半拍。其二是"告警疲劳"。全量日志带来的是每天成千上万条记录，管理员根本没有精力逐条翻阅，真正的异常反而被淹没。其三是"事后追溯"。多数方案只能在事件发生后还原过程，缺少事中识别与实时阻断的能力，损失已经造成才被发现。

1.3 合规要求持续加码

《网络安全法》《数据安全法》《个人信息保护法》与等级保护 2.0 对企业提出了明确要求：网络边界要可控、访问行为要留痕、安全事件要可响应、审计记录要可追溯。监管与客户的双重压力，正在把"网络安全+行为审计"从加分项变成准入项。企业需要的不再是一堆单点工具，而是一套既能防护网络、又能智能审计、还能输出合规证据的统一体系。

二、技术介绍

2.1 方案概述：一个平台、两道防线、三层智能

安企神 AI 安全合规与网络安全方案建立在统一的终端安全平台上：服务器端私有化部署在企业内网，客户端常驻每台终端，管理控制台供管理员统一调度。在这个平台上，两道防线并行运转——网络安全防线守住"边界与通道"，AI 使用审计与洞察引擎盯住"AI 用法与数据流向"；三层能力贯穿其中——全量采集让 AI 使用看得见，敏感判定让风险看得清，AI Insight 让处置跑得快。

两道防线的分工非常清晰：

- 网络安全防线负责"控住网"：网络准入、违规外联检测、分区隔离、流量审计、补丁基线，把网络侧的威胁入口逐一封堵；
- AI 使用审计与洞察负责"管住 AI 用法"：采集员工向各类 AI 的提问与投喂文件，识别其中的敏感内容，通过 AI Insight 输出结论与处置建议，把 AI 侧的数据外流风险及时发现、及时拦截。

两道防线共享同一套行为日志与同一个管理控制台，任何一次网络侧的异常都能在行为侧找到上下文，反之亦然。

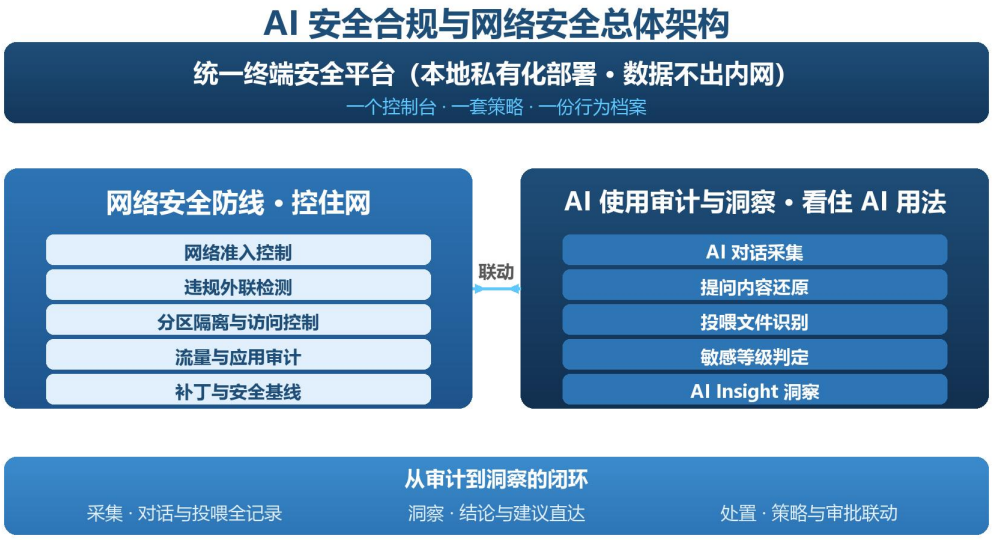


图 1　AI 安全合规与网络安全总体架构

2.2 网络安全纵深防护

网络准入控制。 未经登记的设备接入办公网即被识别并阻断，合法设备按身份与安全基线放行；对不带客户端的访客设备可引导至隔离区域，避免"一台带毒设备瘫痪全网"。

违规外联检测。 实时监测私接热点、随身 WiFi、双网卡桥接、代理翻墙等绕开企业网络边界的行为，一旦发现立即告警并可强制断开，堵住最容易被忽视的"旁路出口"。

分区隔离与访问控制。 内置终端防火墙支持按部门、网段、IP 与端口配置访问策略，研发区、财务区、办公区之间按需隔离；非工作所需的端口与服务默认关闭，把横向移动的空间压到最小。

流量与应用审计。 对网页访问、上传下载、文件传输等网络行为进行应用级识别与记录，支持按应用与网站分类管控带宽，视频、下载、股票类流量可限速或阻断，保障业务系统带宽。

补丁与安全基线。 统一检测系统与常用软件的漏洞缺口，补丁经服务器端审核后分批分发；同时对弱口令、未开启防火墙、杀毒软件缺失等基线项定期核查，不合格终端自动列入整改清单。



五道防线层层嵌套：外挡设备、内限移动、中堵旁路、上管流量、下固根基

图 3　网络安全纵深防线

2.3 AI 使用审计：看得见每一次对话

AI 已经成为办公日常——写方案、改代码、做表格、翻译润色，都离不开它。但每一次提问都可能带出一段业务信息：客户名单、合同条款、设计参数、源代码。安企神的 AI 使用

审计，把"员工向 AI 问了什么、投喂了什么文件"完整记录下来，让 AI 使用从"看不见"变成"可追溯"。

全平台覆盖，网页版与程序版一网打尽。

无论是浏览器里打开的 ChatGPT、DeepSeek、Kimi、豆包、文心一言、通义千问等网页版 AI，还是安装在电脑上的桌面客户端、浏览器插件、AI 写作与绘图类程序，安企神都能通过进程与访问域名自动识别，统一纳入审计范围；企业自建的本地大模型与 API 调用工具同样可以覆盖。

提问内容完整还原。

每一次对话的提问文本、发生时间、使用账号、所在终端、所用的 AI 平台都被完整记录，支持按人员、按部门、按平台、按关键词组合检索。管理者既能回看某位员工在某天向某个 AI 提了什么问题，也能看到某个敏感关键词在哪些部门的提问中出现过。

投喂文件全程留痕。

上传给 AI 的附件（文件名、大小、类型）、复制粘贴进对话框的大段文本、以截图形式提交的画面，都会被记录并与对应的提问关联。哪些文件被投喂给了哪个 AI、什么时间、由谁操作，一目了然——这正是当前最容易被忽视、后果也最严重的一条泄露路径。

敏感等级判定。

系统对提问内容与投喂文件做敏感识别：涉及客户信息、报价成本、图纸参数、源代码、未公开方案的内容自动标注风险等级，高风险对话实时进入预警列表，管理员不必逐条翻阅海量对话记录。

2.4 AI Insight：从"看见"到"看懂"

如果说 AI 使用审计解决"看得见"，AI Insight 解决的是"看得懂、看得快"。它把分散的对话记录、投喂文件与终端行为汇聚成可决策的洞察，让管理者面对 AI 浪潮不再凭感觉。

AI 使用画像。 按部门、岗位、平台维度呈现 AI 使用全貌：哪些部门用得多、偏好哪些平台、集中在什么时段、提问主题如何分布。企业第一次能够清晰回答"我们到底在怎样使用 AI"这个此前无从下手的问题。

风险热力洞察。 敏感投喂的 TOP 文件、高危提问的 TOP 人员、异常时段的使用峰值，以热力图与排行榜直观呈现；同一条泄露路径反复出现时，Insight 会自动标记为"模式化风险"，提示这是流程缺口而非个别现象，需要从制度层面补位。

结论式洞察，而非数据堆砌。 Insight 不止给图表，更直接给出判断与建议："研发部近 30 天向外部 AI 上传图纸类文件 27 次，建议开启图纸外发审批""客服部提问中客户手机号出现频次上升，建议启用脱敏提醒"。管理者看到的是结论，读完即可行动。

洞察驱动处置。 洞察结果可一键转为管控策略：对高风险 AI 站点限制访问、对上传行为强制审批放行、对特定部门开启敏感内容提醒；处置效果再回流到 Insight 中验证，形成"采集—洞察—处置—复盘"的完整闭环。



从一次提问到一条洞察，AI 使用全程可追溯、可处置

图 2 AI 使用审计与 AI Insight 洞察链路

2.5 管理协同与部署

方案延续安企神一贯的轻量路线：服务器端支持本地私有化部署，行为数据全部留存企业内网；客户端安装体积小、资源占用低，对业务软件无干扰；策略在一处配置、全网生效，网

络防护策略与 AI 审计策略在同一控制台协同联动。企业无需组建专职安全团队，一名 IT 管理员即可承担日常运营。

三、方案创新与价值

3.1 从"看不见"到"全程可见"的 AI 使用治理创新

AI 工具的普及让数据出口从"邮箱和网盘"扩展到了"每一次对话"。安企神率先把 AI 使用纳入审计范围：网页版与程序版全覆盖、提问内容与投喂文件全记录，再用 AI Insight 把海量对话记录提炼成结论与建议。企业由此第一次拥有完整的"AI 使用台账"，治理有据可依，风险有迹可循。

3.2 从"单点防护"到"纵深协同"的网络创新

准入、外联检测、隔离、流量、补丁五项网络能力不是五个孤立开关，而是围绕同一套终端身份与同一份策略体系构建的纵深防线：准入挡住非法设备，隔离限制横向移动，外联检测封住旁路出口，流量审计看住数据通道，补丁基线收敛漏洞面。任一环节被突破，下一环节仍有兜底。

3.3 从"合规成本"到"合规资产"的价值创新

等保测评、客户审厂、上市合规都需要提交网络安全与行为审计的证明材料。安企神的审计档案、策略配置、风险处置记录可以直接输出为合规证据，原本"为了过检而做"的投入，变成可持续复用的管理资产。

3.4 客户价值小结

对外，攻击入口被逐一封堵，勒索与钓鱼的成功率显著下降；对内，敏感数据流动全程可见，员工向 AI 问了什么、投喂了什么文件一览无余，高风险行为即时预警；对管理者，AI 使用态势与安全风险一张报表看清；对员工，正常办公几乎无感，管控只发生在真正越界的时刻。

四、落地方法论

4.1 五阶段实施路径

第一阶段"立项调研"：梳理网络拓扑、终端数量与高风险岗位，明确审计范围与管控目标，形成实施方案。第二阶段"部门试点"：选择一两个代表性部门上线，验证准入、隔离与 AI 预警的准确性，收集误报样本。第三阶段"策略调优"：依据试点反馈调整敏感词库、风险阈值与网络分区策略，让 AI 的判断贴合企业实际。第四阶段"分批推广"：按部门分批部署客户端与网络策略，每批稳定运行后再推进下一批。第五阶段"常态运营"：进入日常风险榜单巡查与月度报表机制，安全体系进入自我运转状态。



图 4　AI 安全与网络防护五阶段落地路径

4.2 培训与制度共建

工具只是底座，制度与习惯才是长效保障。实施过程中我们协助企业完成三项工作：一是管理员培训，覆盖策略配置、预警处置与报表解读；二是管理层简报，把风险榜单与合规证据讲清楚；三是员工宣导，用"管数据不管隐私"的透明规则争取理解与配合。

4.3 合规与隐私边界

方案的采集范围严格限定于工作场景下的设备与网络行为，不涉及员工私人通讯内容；AI 使用审计同样只覆盖工作终端上的提问与投喂行为，目的是识别业务数据是否经由 AI 外流，而非审查员工的私人事务；所有行为数据加密存储在企业内网服务器，访问权限分级授权并全程留痕；敏感内容识别仅输出风险判定与脱敏摘要，不落地原文内容。企业应同步在员工手册或保密制度中明确告知审计范围，做到"告知在先、采集在后、最小够用"。

4.4 常见顾虑与回应

"AI 使用审计会不会侵犯员工隐私？"——审计范围严格限定于工作设备与工作场景，并在制度中向员工明确告知；系统关注的是业务数据是否经由 AI 外流，而不是员工的私人事务。"会不会拖慢电脑和网速？"——客户端资源占用经过严格压测，流量管控保障业务带宽优先。"部署要不要专人专岗？"——一名 IT 管理员经培训即可承担日常运营，复杂预警处置可借助安企神服务团队远程支持。"员工会不会抵触？"——管控聚焦于工作行为与数据安全，配合透明宣导，实际落地企业的员工反馈普遍平稳。

五、典型应用场景与服务保障

5.1 行业场景

行业	网络安全重点	AI 使用审计重点
金融与投资机构	交易网段隔离、访问准入	AI 提问留痕、客户信息投喂识别
研发与制造企业	研发区隔离、外联封堵	图纸/代码投喂 AI 识别与外

		发审批
政务与事业单位	等保合规、补丁基线	AI 使用合规审查、敏感提问预警
医疗机构	挂号诊疗网段防护、准入控制	患者数据投喂识别、异常使用洞察
教育与科研单位	机房与办公网隔离	课题与试卷资料投喂管控

5.2 服务保障承诺

安企神在全国拥有 300 余家合作伙伴，提供本地化实施与售后支持：产品支持 7 天全功能试用；单台授权低至 60 元起，按终端数量灵活授权；客服热线 400-666-2563 。工作日 5 分钟内响应；重大安全事件提供专项技术支持通道，保障客户网络与数据安全万无一失。

六、资质与认证

安企神软件已通过 ISO9001 质量管理体系与 ISO27001 信息安全管理体系认证，核心功能模块取得多项计算机软件著作权登记；产品历经万余家政企客户的生产环境验证，终端管理规模超过 2 亿台，在政务、金融、制造、医疗、教育等行业形成了成熟的交付与运营经验。

七、未来展望

AI 使用治理走向深度洞察。

AI Insight 将从"记录与告警"进一步走向预测：基于历史使用模式，预判哪类岗位、哪类操作最可能出现数据外流，把防线从"事后追溯"再次前移到"事前布防"；洞察结论也将以更自然的方式呈现，让每一条建议都可读、可判、可复盘。

网络防护走向零信任。

"默认不信任、持续验证"的零信任架构将与终端准入深度融合，每一次访问都基于设备身份、用户身份与风险评分动态授权，边界内外一视同仁。

合规走向自动化。

等保条款与行业规范将被固化为可校验的策略模板，系统自动比对现状与差距、生成整改清单与测评证据，合规从"项目制"变成"日常态"。

风险治理走向闭环。

网络防护、AI 审计、数据防泄密与保密沙箱将在同一平台上打通，形成"发现—评估—处置—复盘"的完整闭环，让企业的每一分安全投入都可度量、可持续。

版权说明

本白皮书版权归石家庄安企神网络科技有限公司所有。未经书面许可，任何单位和个人不得以任何形式复制、转载、摘编本白皮书的部分或全部内容。安企神及本白皮书中提及的产品名称，是石家庄安企神网络科技有限公司的商标或产品标识。

免责声明

本白皮书内容基于产品当前版本整理，功能与界面可能随版本升级而调整，具体以实际交付版本为准。本白皮书仅用于向客户介绍产品技术与方案，不构成任何形式的合同承诺。因使

用本白皮书内容而产生的任何直接或间接损失，石家庄安企神网络科技有限公司不承担相关责任。

如需了解更多产品信息或预约产品演示，请联系安企神客服热线 400-666-2563。