Nexus Flow 用户手册

Windows 实时网络流量监控、PCAP 分析与报告导出

项目	信息
适用产品版本	1.0.31
手册版本	1.1
发布日期	2026-06-11

目录

1. 产品定位与核心能力

Nexus Flow 是 Windows x64 免安装网络流量监控工具。它使用 WinDivert 捕获本机数据包，将数据包汇总为 flow，并按主机、服务与程序显示下载、上传、包速率、活动连接、DNS、国家、ASN 与风险信息。

主要使用场景

1. 实时查看本机与远程主机之间的 TCP、UDP、ICMP、IPv4 与 IPv6 流量。
2. 按网卡、方向、端口、IP/CIDR、程序名称或 PID 缩小观察范围。
3. 查看 Top Hosts、Top Services、Top Programs 与 SQL Server TDS 等重点流量。
4. 导入 classic PCAP/CAP 做离线汇总，或将实时数据包持续写入 PCAP。
5. 用 CSV、JSON、Excel、HTML 或 PDF 交付 flow 明细或摘要。

支持范围

项目	当前支持
平台	Windows x64；WPF / .NET 8；Portable EXE
实时捕获	WinDivert；需要管理员权限
数据源	实时捕获、classic .pcap、.cap
分析维度	Flow、主机、服务、程序、DNS、国家、ASN、风险、告警
输出	PCAP、CSV、JSON、XLSX、HTML、PDF

2. 工作方式与数据流程

Nexus Flow 将数据包捕获、flow 汇总、名称解析、风险判断与界面显示分为不同阶段。理解数据流程有助于判断筛选条件何时生效，以及 DNS、程序名称或 GeoIP 字段为何可能稍后才补齐。

阶段	输入	主要工作	输出
捕获	本机网卡数据包或 classic PCAP	WinDivert sniff mode 或离线读文件	数据包样本
汇总	数据包样本	按方向、地址、端口与协议建立 flow	Flow 记录与统计
补充信息	远端 IP、Port、PID	服务名称、程序、DNS、国家、ASN、组织	可读字段
显示	Flow 与摘要	总览、Inspect、Hosts、Services、Programs	实时界面
交付	当前累积数据	CSV、JSON、Excel、HTML、PDF、PCAP	报表或捕获文件

6. 核心捕获、汇总、搜索与报表生成均在本机执行。
7. 只有用户主动更新 GeoIP/ASN 数据或启用 Webhook 时，才会使用网络连接。
8. 左侧 Port、IP 与程序条件会影响保留或显示的 flow；上方搜索主要筛选界面，不会改写原始捕获文件。
9. DNS、程序与 GeoIP/ASN 解析受缓存、权限、数据库版本与数据包时序影响，可能暂时显示未知。

3. 系统要求、部署与启动

正式交付包为单一 ZIP。程序自带 .NET 运行环境，不需要另外安装 .NET、Microsoft Office 或 PDF 软件。

项目	要求
操作系统	Windows 10 / Windows 11 x64；建议使用仍受支持且已更新的版本
权限	必须以管理员身份运行，以加载 WinDivert 驱动
磁盘	为程序、日志、GeoIP/ASN 数据、PCAP 与报告预留空间；需求随流量与保留时间增加
网络	实时捕获不需要外部服务；在线更新 GeoIP/ASN 时需要互联网

部署与启动

10. 将 NexusFlow_Portable_v1.0.31_WinDivert_KapsekSelfSigned.zip 解压到可信的本地文件夹；不要直接从 ZIP 内运行。
11. 确认 NexusFlow.exe 与包内第三方授权声明存在。
12. 右键单击 NexusFlow.exe，选择“以管理员身份运行”。
13. 如果 Windows SmartScreen 或终端防护提示，请按组织流程验证来源、签名与哈希。
14. 首次启动时选择语言，输入正式授权，或单击“使用试用版”。

4. 授权、试用版与产品信息

授权窗口支持繁体中文、简体中文与英文。正式授权通过 Email 与 25 位授权码离线验证；授权数据使用 Windows DPAPI 保护并保存在当前 Windows 用户设置中。

1. 授权窗口可选择语言、输入 Email 与授权码，或进入五分钟试用模式。

功能	试用版	正式授权

功能	试用版	正式授权
实时捕获	累计最多 5 分钟	不受试用时间限制
PCAP 持续写入 / 导出	禁用	可用
CSV / JSON / Excel / HTML / PDF	禁用	可用
PCAP 导入与界面查看	可用	可用

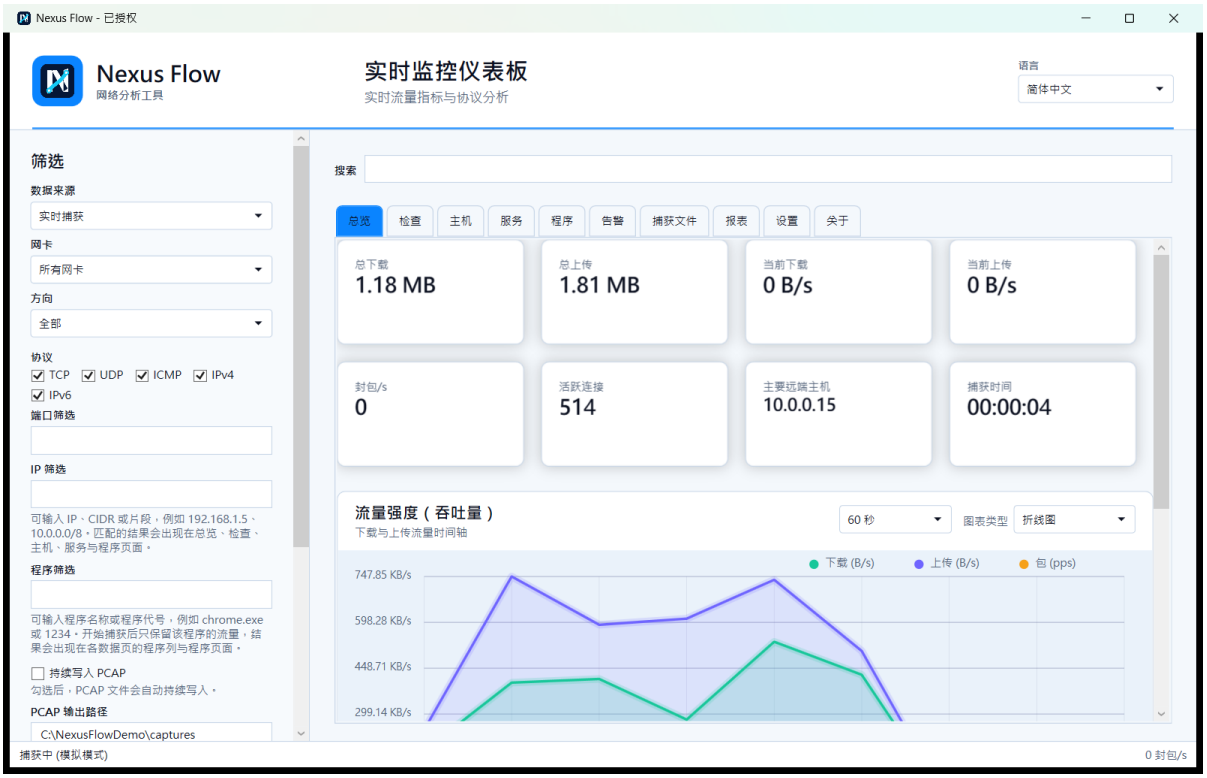
激活正式授权

15. 在授权窗口选择所需语言。
16. 输入购买授权时使用的 Email。
17. 输入格式为 XXXXX-XXXXX-XXXXX-XXXXX-XXXXX 的授权码。
18. 单击“激活”。成功后主窗口标题栏显示“已授权”。
19. 如只需评估，单击“使用试用版”；试用时间只在开始实时捕获后累计。

2. 关于页说明产品、第三方授权与试用版限制；界面版本文字可能与正式交付版不同。

5. 主界面与操作区域

主窗口由 Header、左侧筛选与操作区、搜索栏、十个功能页签及底部状态栏组成。语言可在右上角即时切换；主题固定跟随 Windows。



3. 总览页同时显示八项实时指标、流量时间轴、Top Hosts 与 Top Services。

区域	用途
Header	产品名称、仪表板标题、语言切换
左侧面板	数据源、网卡、方向、协议、端口/IP/程序筛选、PCAP 与捕获操作
搜索	跨 flow、主机、服务、程序、告警与捕获文件匹配关键字
页签	总览、检查、主机、服务、程序、告警、捕获文件、报告、设置、关于
状态栏	捕获状态、模拟/正式模式与当前包速率

6. 第一次捕获：快速开始

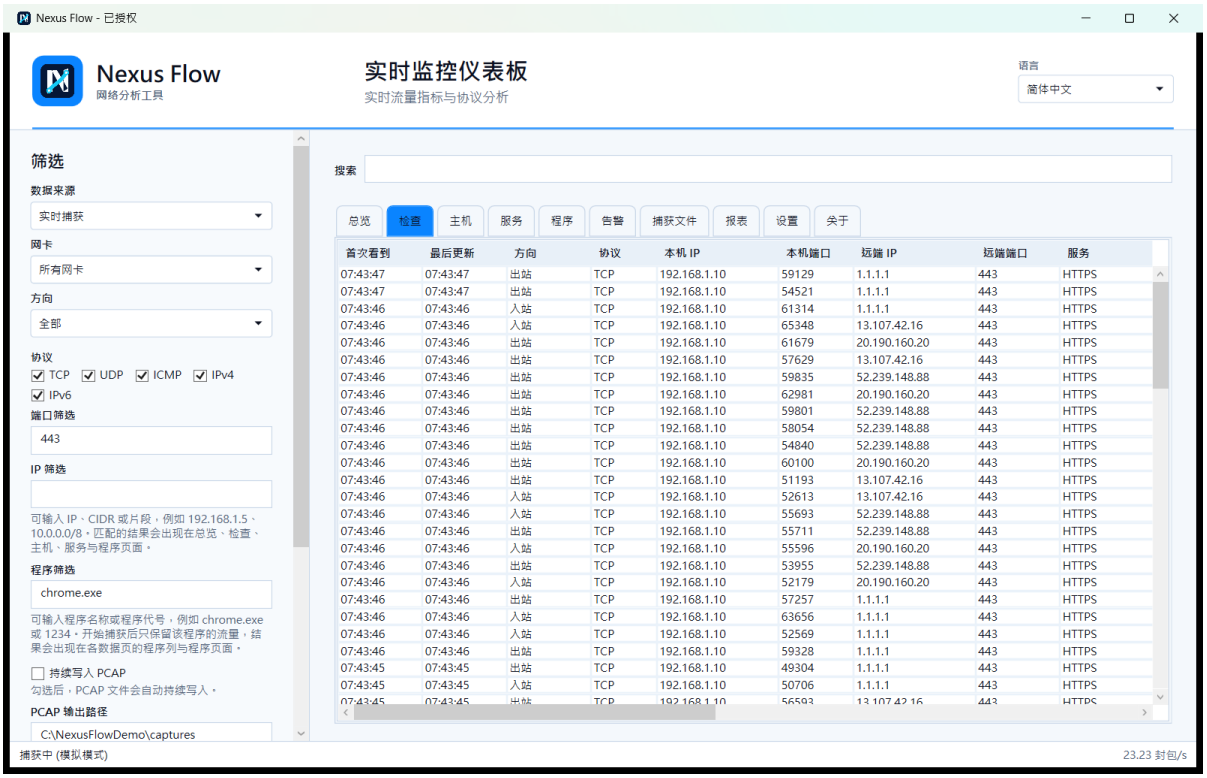
20. 以管理员身份启动并完成授权或选择试用版。
21. 在“数据源”选择“实时捕获”。
22. 选择所有网卡或指定网卡，并设置方向与协议。

23. 需要时输入端口、IP/CIDR、程序名称或 PID。
24. 如需保存原始数据包，正式授权用户可先勾选“持续写入 PCAP”。
25. 单击“开始捕获”，确认底部状态栏显示正在捕获。
26. 在总览、检查、主机、服务或程序页确认数据。
27. 完成后单击“停止捕获”；再按需要导出报告或检查 PCAP。

重要：“暂停界面”只停止界面刷新，后台捕获与统计仍会继续；要停止驱动使用与试用计时，必须单击“停止捕获”。

7. 实时捕获、筛选与暂停界面

控件	用法与示例
数据源	实时捕获；或切换 PCAP 导入并选择文件
网卡	所有网卡，或指定物理/虚拟接口
方向	全部、入站、出站
协议	TCP、UDP、ICMP、IPv4、IPv6，可多选
端口	443；80,443；10000-10100
IP	192.168.1.5；10.0.0.0/8；或地址片段
程序	chrome.exe；sqlservr.exe；或 PID 1234



4. Port 443 与 chrome.exe 筛选场景；Inspect 只保留匹配条件的 HTTPS flow。

控件	实际行为
开始捕获	按当前网卡、方向、协议与筛选条件开始；捕获中修改部分选项会重新开始并清空统计
停止捕获	停止 WinDivert、结束试用计时并关闭持续 PCAP writer
暂停界面	停止界面更新，但底层捕获仍可能继续；再次按下可恢复显示
清除统计	清空当前 flow、摘要与图表，不等同删除已写入的 PCAP 文件
导出 CSV	导出当前累积的完整 Flow 集合；上方搜索不会自动限制导出集合
导出为 PCAP	捕获中切换持续写入的开始或停止，并非真正的一次性快照

28. 开始捕获前确认条件。捕获中更改网卡、方向或协议会重新启动捕获并清除现有统计。

29. 端口、IP 与程序文本条件会影响后续汇总与界面；如需干净的比较基准，请先停止并清除统计。

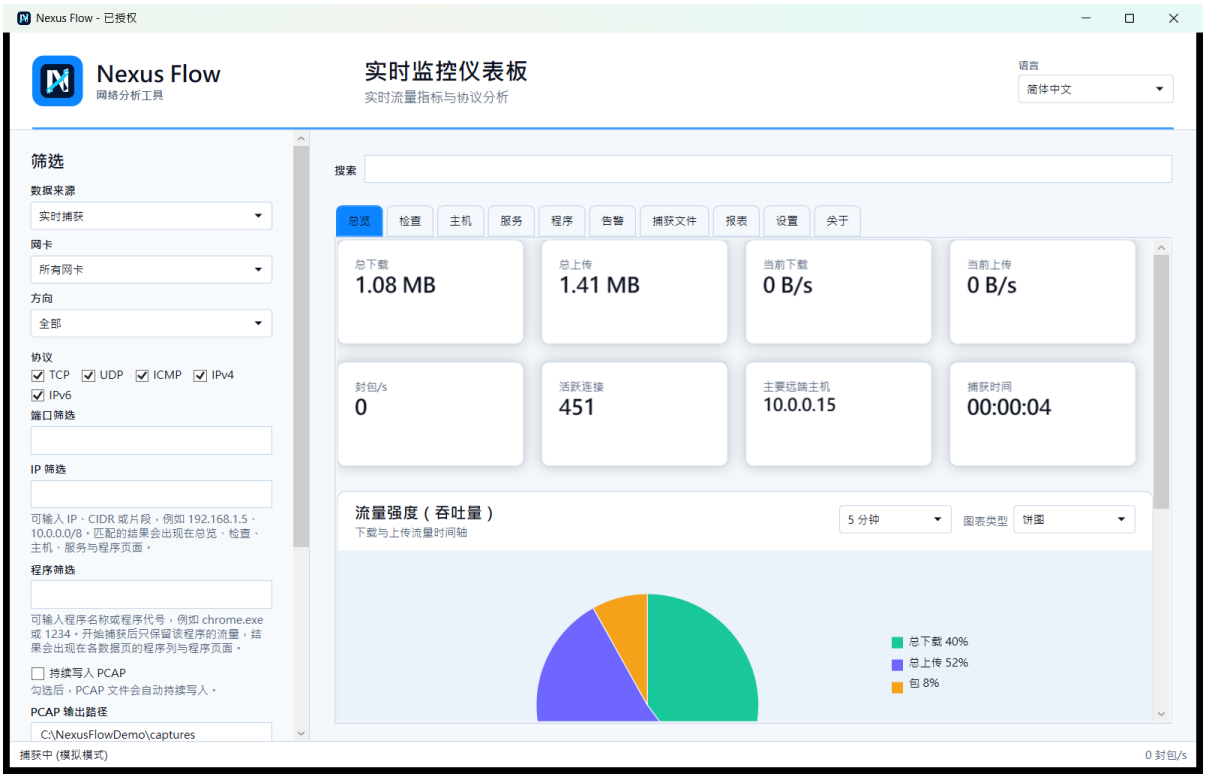
30. “清除统计”会清除当前 flow 与图表，但不会自动停止正在运行的捕获。

31. “暂停界面”适合暂时冻结界面阅读；再次单击可恢复刷新。

8. 总览指标与流量图表

指标	解读方式
总下载 / 总上传	自本次统计起点累积的字节，按方向换算
当前下载 / 当前上传	最近采样区间的实时速率
数据包/s	最近采样区间每秒数据包数
活动连接	当前汇总器内仍视为活动的 flow 数
主要远端主机	当前累积流量最大的远端 IP
捕获时间	自捕获开始或统计重置后的经过时间

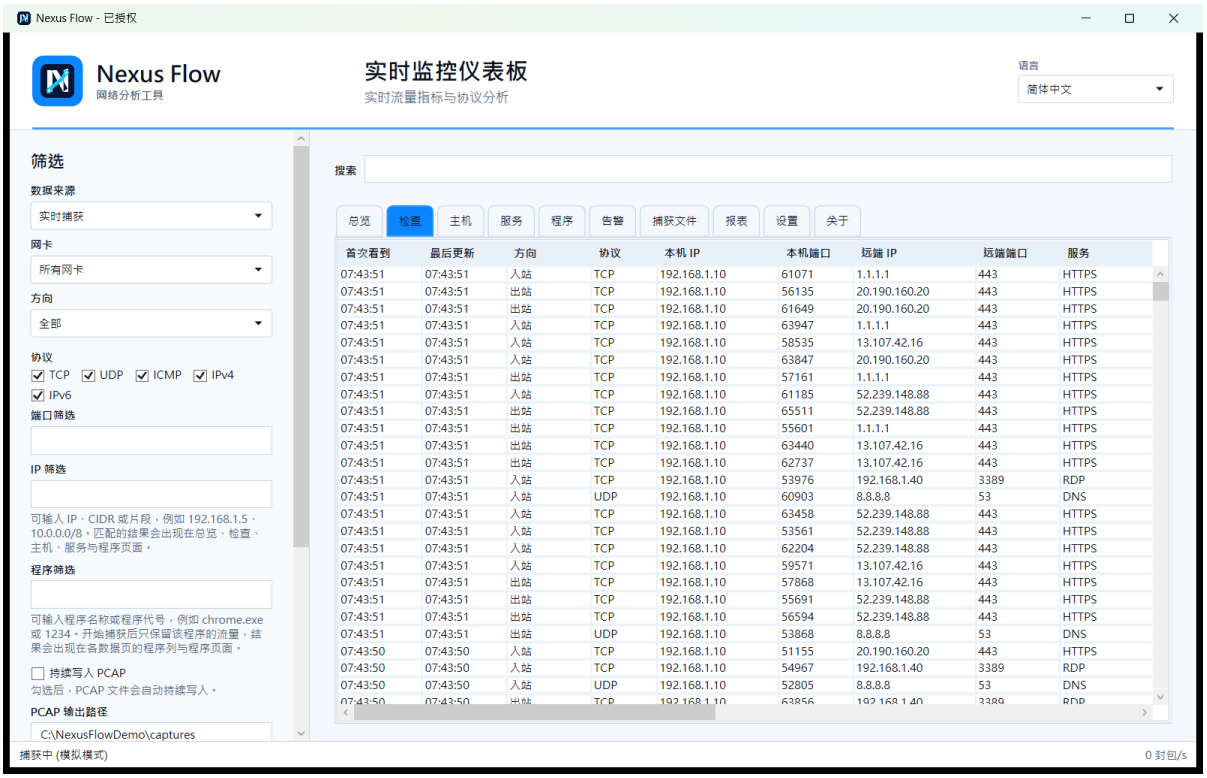
设置	选项与用途
时间范围	60 秒、5 分钟、15 分钟、30 分钟
折线图	适合比较下载、上传与数据包率的变化趋势
面积图	强调流量量级与时间分布
柱状图	适合逐采样点比较下载与上传
饼图	比较当前累积下载、上传与数据包的占比



5. 饼图以当前累积的下载、上传与数据包量显示流量组成。

9. 检查明细与全局搜索

“检查”页逐行显示 Flow。画面字段依次包括“首次看到”、“最后更新”、“方向”、“协议”、“本机 IP”、“本机端口”、“远端 IP”、“远端端口”、“服务”、“程序”、“程序代号”、“国家”、“自治系统”、“域名”、“包”、“流量”、“状态”与“风险”；可使用水平滚动条查看后续字段。

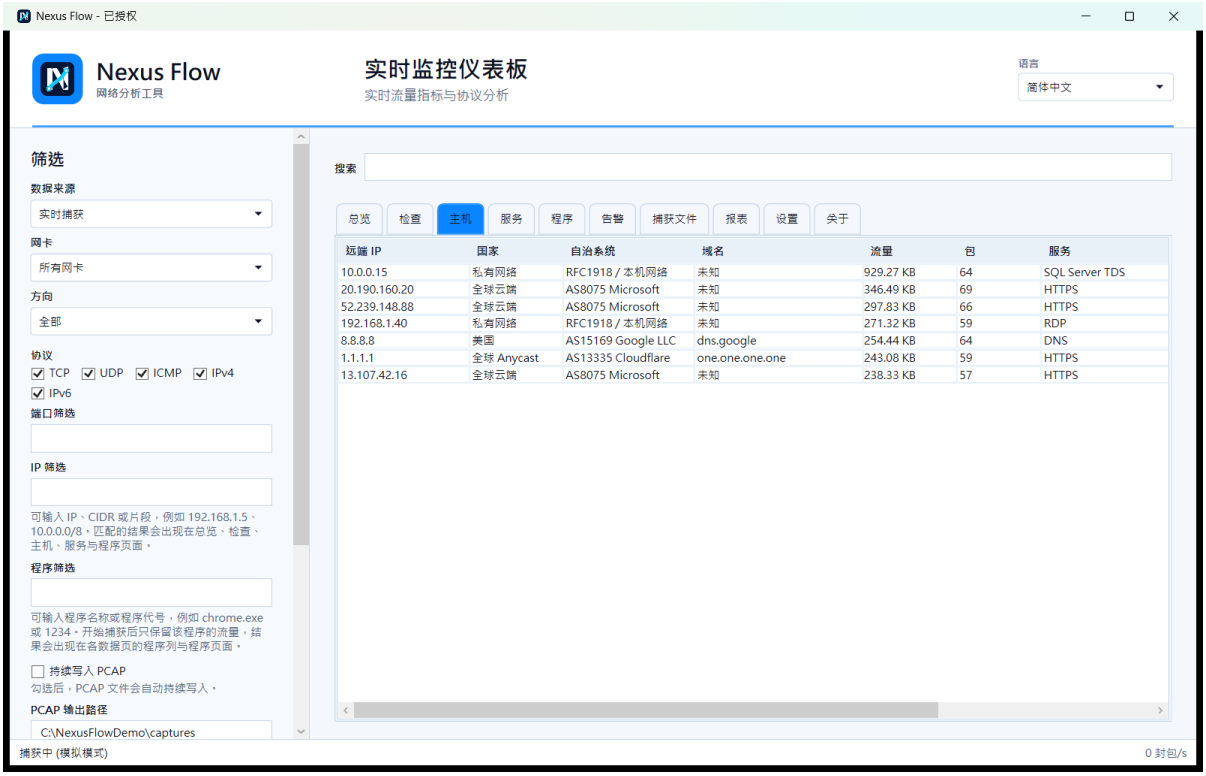


6. “检查”页按 Flow 显示时间、方向、端点、服务、程序与流量等字段。

字段组	包含内容	使用重点
时间	首次看到、最后更新	定位流量发生区间与持续时间
网络	方向、协议、本机 / 远端 IP 与端口	确认通信双方与服务端端口
应用	服务、程序、程序代号、域名	找出通信用途与发起程序
识别	国家、自治系统、域名	识别网络归属与名称解析；需先准备 GeoIP/ASN 数据
统计	数据包、流量、状态、风险	按数据量与风险进行排序和调查

重要: 上方“搜索”会过滤当前界面与摘要视图；CSV/Excel 的导出实现使用完整 Flow 集合，因此不要把界面搜索结果误认为报表导出范围。需要交付特定子集时，应对导出文件另行筛选。

10. 主机分析



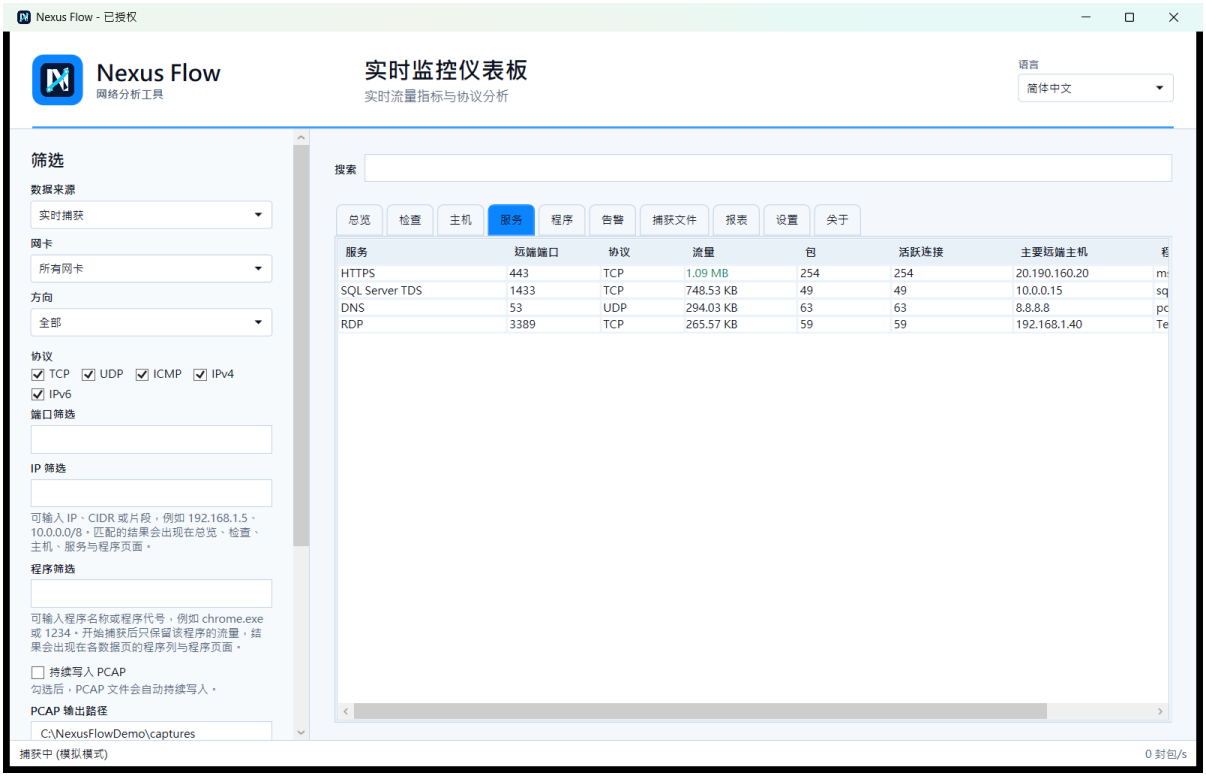
7. “主机”页按远端 IP 汇总国家、自治系统、域名、流量、包、服务与程序。

字段	说明
远端 IP / 国家 / 自治系统	远端端点及其地理与网络归属
域名	由 DNS 缓存或反向解析取得；未知不代表没有连接
流量 / 包	此远端 IP 在当前统计期间的累积量
服务 / 程序	曾与该主机通信的服务与本机程序摘要
风险	“正常”或“黑名单”；黑名单数据由产品设置加载

1. 先使用上方“搜索”缩小数据，再按“流量”、“包”或“活动连接”排序。
2. “主机”适合从可疑 IP 出发；“服务”适合从端口或协议出发；“程序”适合从本机应用程序出发。

3. 三个摘要页都会受左侧“端口筛选”、“IP 筛选”与“程序筛选”影响，但各页的汇总维度不同。

11. 服务分析



8. “服务”页按服务、远端端口与协议汇总流量、包与主要端点。

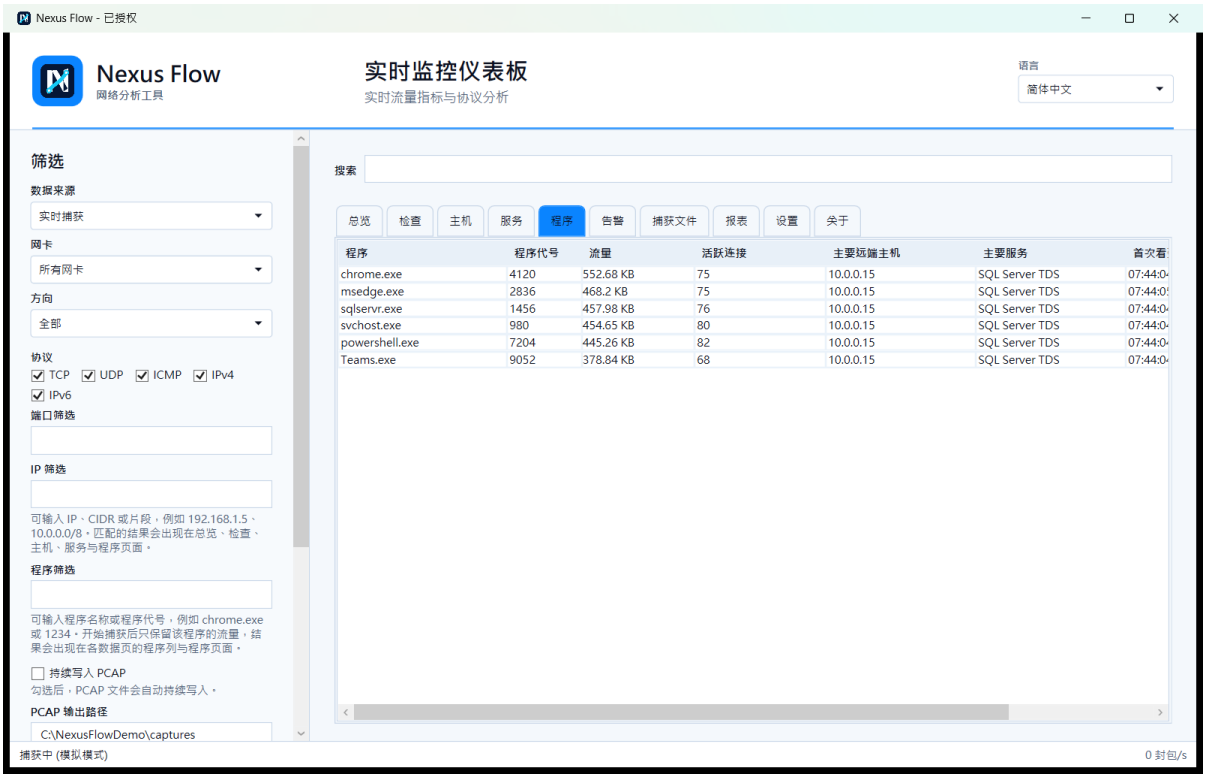
字段	说明
服务 / 远端端口 / 协议	例如 HTTPS 443/TCP、DNS 53/UDP、SQL Server TDS 1433/TCP
流量 / 包	同一服务与协议在当前统计期间的总量
活动连接	当前仍活动的相关 flow 数
主要远端主机	该服务累积流量最大的远端 IP
程序	使用该服务最多的本机程序

1. 先使用上方“搜索”缩小数据，再按“流量”、“包”或“活动连接”排序。

2. “主机”适合从可疑 IP 出发；“服务”适合从端口或协议出发；“程序”适合从本机应用程序出发。

3. 三个摘要页都会受左侧“端口筛选”、“IP 筛选”与“程序筛选”影响，但各页的汇总维度不同。

12. 程序分析



9. “程序”页按程序与程序代号汇总流量、连接数、主要远端主机及服务。

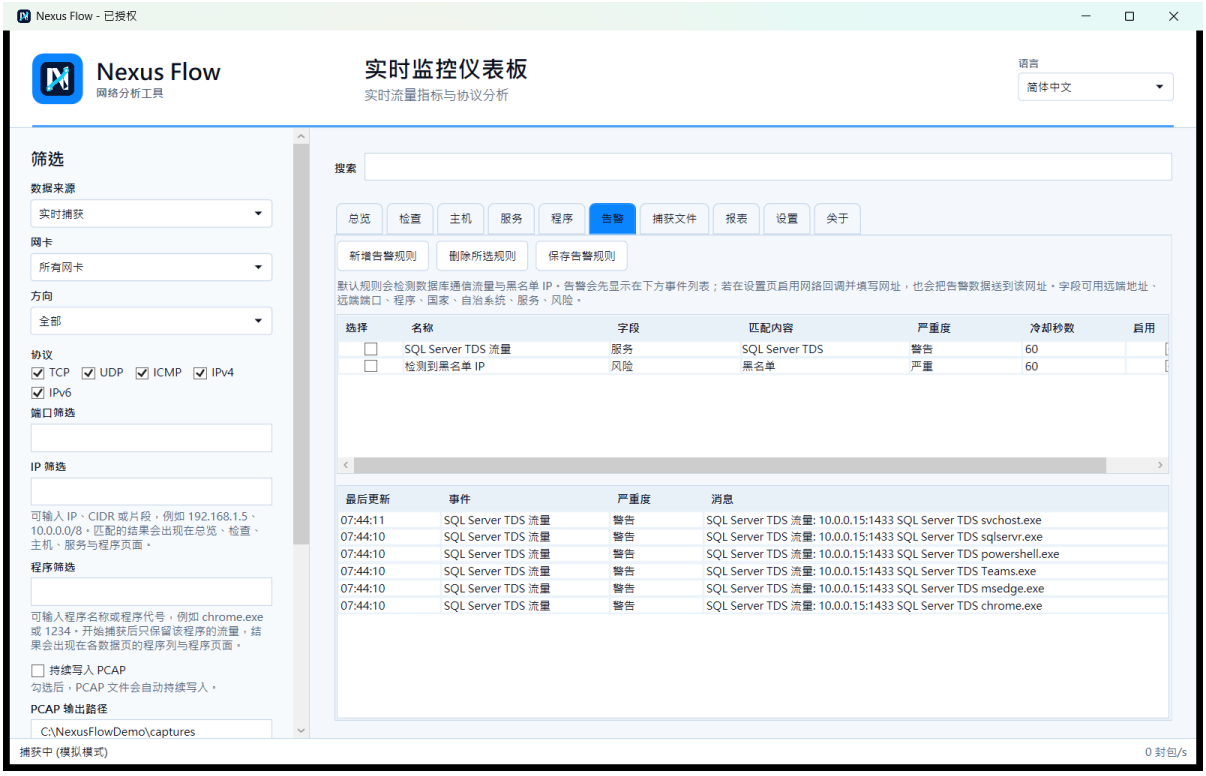
字段	说明
程序 / 程序代号	由 Windows 连接所有者数据推定；短连接可能显示“未知”
流量 / 活动连接	该程序累积流量与当前活动 flow 数
主要远端主机 / 主要服务	快速识别程序主要连接目标与用途
首次看到 / 最后更新	程序在当前捕获期间的活动时间范围

1. 先使用上方“搜索”缩小数据，再按“流量”、“包”或“活动连接”排序。

2. “主机”适合从可疑 IP 出发；“服务”适合从端口或协议出发；“程序”适合从本机应用程序出发。
3. 三个摘要页都会受左侧“端口筛选”、“IP 筛选”与“程序筛选”影响，但各页的汇总维度不同。

13. 告警规则、事件与 Webhook

“告警”页包含可编辑规则与事件列表。默认规则检测 SQL Server TDS 服务与黑名单 IP；命中规则时先添加界面事件，启用网络回调后再通过 HTTP POST 发送 JSON。



10. “告警”页上半部分管理规则，下半部分显示匹配规则的事件记录。

1. 选择“新增告警规则”，在新行填写“名称”、“字段”、“匹配内容”、“严重度”、“冷却秒数”与“启用”。
2. “字段”可使用“远端 IP”、“远端端口”、“程序”、“国家”、“自治系统”、“服务”或“风险”。

3. 按“保存告警规则”将规则写入设置；如需删除规则，先勾选“选择”，再单击“删除所选规则”。未保存的表格修改不应视为正式配置。
4. 事件匹配规则时会出现在下方事件表；相同规则在冷却期间不会重复产生大量通知。
5. 若“设置”页打开“启用网络回调”，事件也会通过 HTTP POST JSON 发送；失败只记录在日志中，不会阻塞捕获。

字段	说明
名称	规则名称
字段	可用值：远端 IP、远端端口、程序、国家、自治系统、服务、风险
匹配内容	不区分大小写的包含匹配；空白不触发
严重度	例如信息、警告、严重；作为事件标记与 Webhook 字段
冷却秒数	相同规则、远程端点与程序再次触发前的冷却秒数
启用	取消后不评估该规则

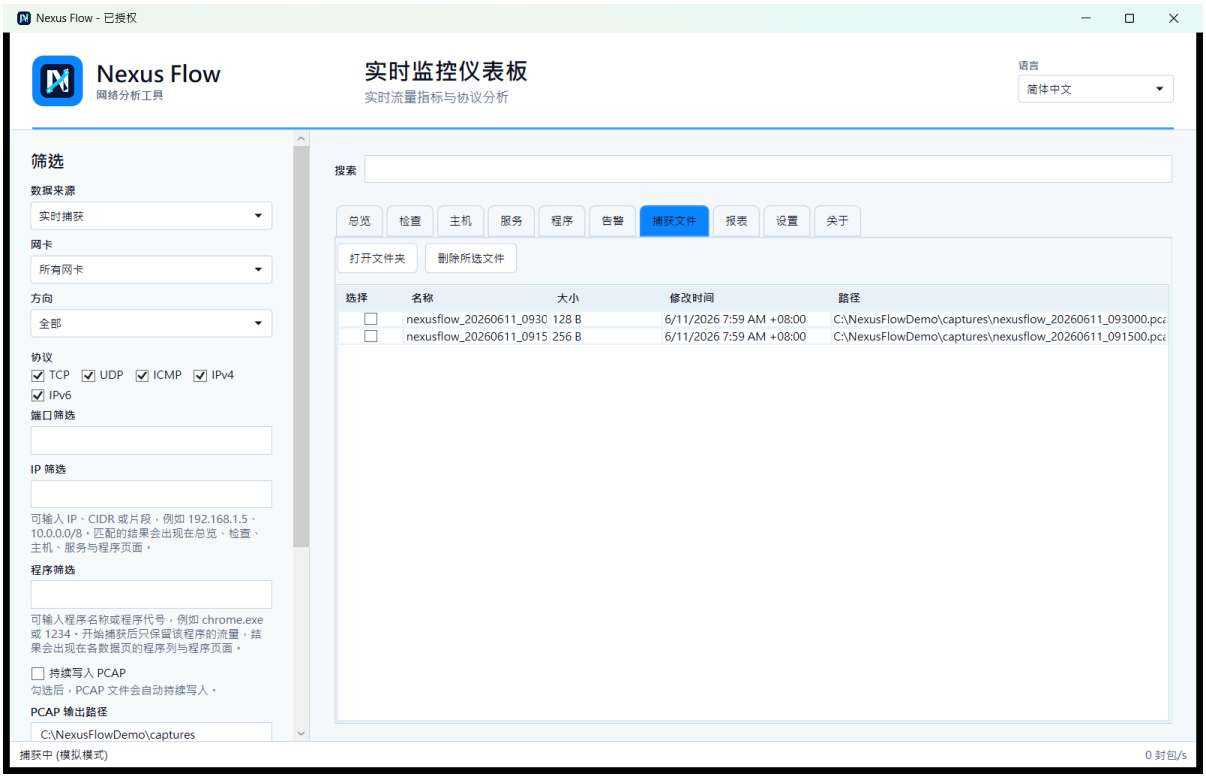
注意: Webhook JSON 包含 product、eventType、severity、time、remoteAddress、remotePort、process、country、asn。产品不提供签名或重试队列；接收端应使用 HTTPS、验证来源并容忍重复/丢失事件。

14. PCAP 导入、持续写入与捕获文件管理

Nexus Flow 可在正式授权下持续写入实时数据包，也可导入现有 classic PCAP/CAP。PCAP 可能包含敏感网络数据，应按组织保留策略处理。

任务	操作	注意事项
导入离线文件	“数据来源”选择“PCAP 导入”，再选择 .pcap 或 .cap	文件选择器会显示 .pcapng，但当前读取器不支持 PCAPNG
开始实时写入	开始捕获前勾选“持续写入 PCAP”，或捕获中按“导出为 PCAP 文件(一次性保存当前记录)”	试用版停用；文件名为 nexusflow_yyyyMMdd_HHmmss.pcap
停止写入	停止捕获，或再次按“导出为 PCAP 文件(一次性保存当前记录)”	停止后才会完整关闭文件并刷新捕获文件列表

任务	操作	注意事项
管理文件	在“捕获文件”页单击“打开文件夹”，或选择文件后单击“删除所选文件”	删除操作不可恢复；使用中的文件可能无法删除



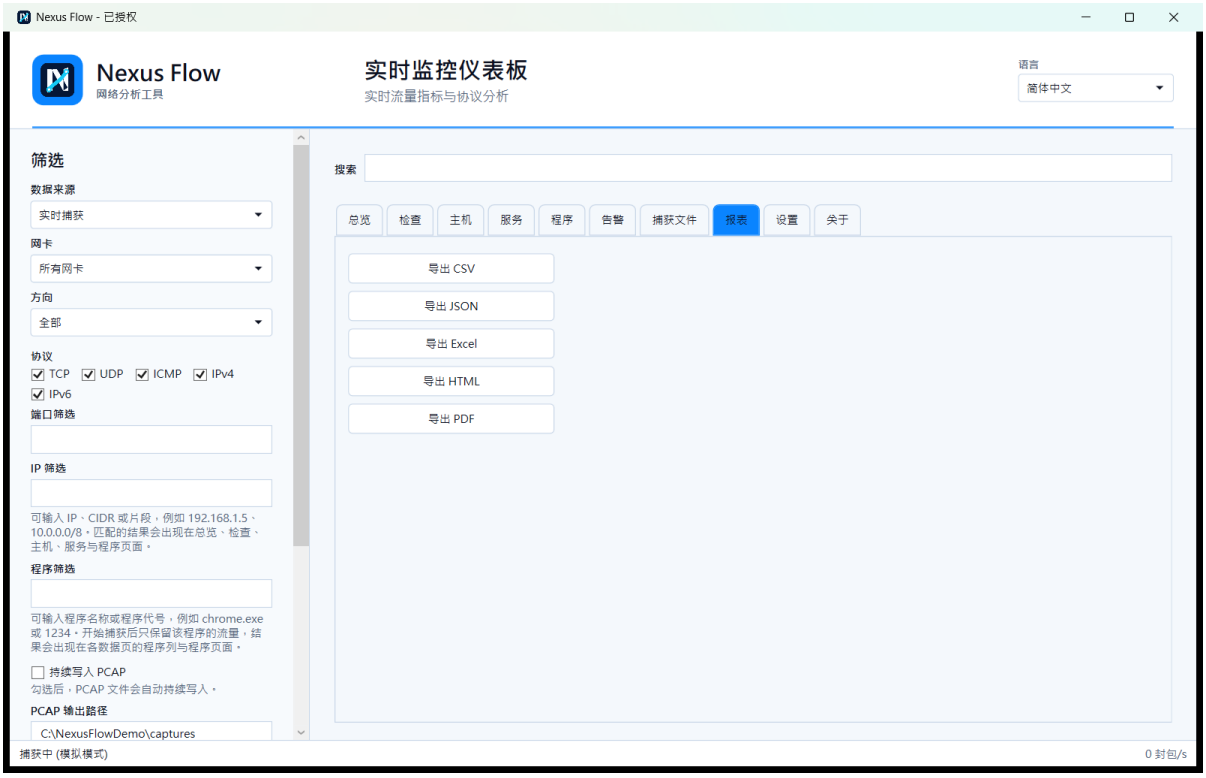
11. “捕获文件”页列出 PCAP 名称、大小、修改时间与完整路径。

功能	操作与结果
捕获前持续写入	勾选“持续写入 PCAP”并开始捕获，自动创建 nexusflow_yyyyMMdd_HHmmss.pcap
捕获中切换写入	捕获期间单击左侧“导出为 PCAP 文件(一次性保存当前记录)”；当前实际行为为开始/停止持续写入
“捕获文件”页	列出默认 captures 目录的 .pcap，可使用“打开文件夹”或“删除所选文件”
PCAP 导入	“数据来源”选择“PCAP 导入”，再选择 classic .pcap 或 .cap
格式	classic PCAP，LINKTYPE_RAW 101

警告: 文件选择器会显示 .pcapng，但当前版本不解析 PCAPNG，会显示不支持消息。请先用 Wireshark/tshark 转为 classic .pcap。

15. 报表导出与交付

正式授权用户可从“报表”页导出五种格式。完成后产品显示文件路径，并在文件资源管理器中选中输出文件。



12. “报表”页提供“导出 CSV”、“导出 JSON”、“导出 Excel”、“导出 HTML”与“导出 PDF”五种输出。

1. 先完成捕获或 PCAP 导入，确认“检查”与摘要页已有数据。
2. 切换到“报表”页，选择“导出 CSV”、“导出 JSON”、“导出 Excel”、“导出 HTML”或“导出 PDF”。
3. 输出完成后产品会显示文件路径，并打开文件所在文件夹。
4. 交付前抽查时间、端点、程序、DNS、国家/ASN 与报表编码，并按数据分级遮罩敏感信息。

格式	内容	默认子目录
CSV	全部 flow 明细；UTF-8	reports\csv
JSON	snapshot、前 50 条主机 / 服务 / 程序、前 100 条告警	reports\json
Excel	全部 flow 明细；.xlsx，不需要 Office	reports\excel

格式	内容	默认子目录
HTML	可用浏览器打开的摘要	reports\html
PDF	简要摘要与热门主机	reports\pdf

警告: 报告可能包含内外部 IP、程序名称、域名、国家、ASN 与告警信息。PDF 生成器偏向 ASCII 文本；如需完整中文显示，请优先使用 HTML、Excel、CSV 或 JSON。

16. 设置、GeoIP/ASN 与后台监控

“设置”页集中管理“PCAP 输出路径”、“地理位置与自治系统数据库”、“网络回调网址”及“默认启用实时捕获文件写入”。设置保存在当前 Windows 用户的 settings.json。

13. “设置”页管理 PCAP 路径、GeoIP/ASN、网络回调与默认实时捕获文件写入。

设置	作用
PCAP 输出路径	设置持续写入与按钮启动写入的目标文件夹
地理位置与自治系统数据库	指定 ip2asn-v4-u32.tsv；可在线更新或导入 .tsv/.tsv.gz

设置	作用
网络回调网址 / 启用网络回调	将告警事件以 JSON POST 到指定端点
默认启用实时捕获文件写入	保存后，下次开始捕获时自动写入 PCAP；试用版禁用
保存设置	写入 settings.json，并同步左侧 PCAP 路径

1. “PCAP 输出路径”会同步到左侧捕获控制区。
2. “地理位置与自治系统数据库”可使用“从网络更新数据”，或通过“导入本地数据文件”导入 IPtoASN TSV/TSV.GZ；更新后现有 Flow 会在后续刷新时补充信息。
3. “网络回调网址”应使用受控 HTTPS 端点，接收端需自行处理验证、保留期限与重试策略。
4. “默认启用实时捕获文件写入”只对正式授权有效；试用模式会自动取消。
5. 最小化时主窗口可隐藏到系统托盘；托盘菜单可使用“显示主窗口”、开始/停止捕获、“迷你窗口”或退出。

17. 故障排除

问题	可能原因	处理方式
程序要求管理员权限	WinDivert 驱动需要提升权限	以管理员身份重新启动；确认 UAC 与终端策略
无法开始捕获	驱动被阻止、签名/权限问题、无效条件	查看错误码与 nexusflow.log；确认 WinDivert runtime 与安全策略
界面没有数据	条件过窄、选错网卡/方向、当前没有流量	选择“所有网卡”与“全部”方向；清除筛选后重试
试用版自动停止	累计实时捕获已达到 5 分钟	激活正式授权；PCAP 导入仍可用
PCAPNG 无法导入	当前版本不支持 PCAPNG	先转换为 classic .pcap
告警没有发送到 Webhook	未启用、URL 错误、TLS/防火墙阻止	检查设置与接收端日志；使用 HTTPS 测试端点
报告按钮不可用	试用模式	完成正式授权
国家/ASN 未更新	尚未下载或导入数据库	在“设置”页更新或导入 IPtoASN TSV/TSV.GZ
最小化后找不到窗口	已隐藏到系统托盘	双击 Nexus Flow 图标或使用“显示主窗口”

18. 安全、隐私与已知限制

安全与隐私

1. 实时捕获、汇总、授权验证与报告生成都在本机运行；只有用户启用的 GeoIP 更新与 Webhook 会连接外部端点。
2. license.dat 与 trial.dat 使用 Windows DPAPI，通常只能由相同 Windows 用户解密。
3. WinDivert runtime 位于 ProgramData，正式程序会限制目录 ACL，并在退出时清理相关驱动服务。
4. PCAP、flow、域名、程序与告警可能属于敏感或个人数据；捕获前应获得授权并按策略保留。
5. 删除产品文件夹不会自动删除 LocalAppData、ProgramData、桌面 PCAP 与报告。

已知限制

1. 产品是监控与分析工具，不会阻止、修改或注入数据包，也不是防火墙。
2. 当前不提供 PCAPNG 解析、地图、云账号、集中管理、Windows Service 或 MSI/MSIX。
3. 程序映射与 DNS/GeoIP 结果受系统权限、缓存、数据库版本与数据包时序影响。
4. 主界面搜索只影响查看，不会自动把报告导出限制为可见行。
5. “关于”页文字版本可能与 1.0.31 交付包不一致，应以正式交付信息为准。