好的，作为360安全产品技术分析专家，我已根据您提供的用户反馈数据，生成以下技术分析周报。

360安全产品用户反馈技术分析周报

统计周期：2025-12-01 至 2025-12-31 **生成时间**：2026-01-03 22:32 **分析专家**：360安全产品技术分析中心

---

1. 执行摘要（核心发现）

本周共收集有效用户反馈 **135** 条，整体用户情绪偏向**负面**，主要矛盾集中于**安全工具的“强干预”特性与系统稳定性、用户体验之间的失衡。**

- **核心风险**：出现 **1例高风险** 反馈，用户在执行漏洞修复后导致双硬盘系统中的Deepin国产操作系统无法启动，暴露出底层修复功能在**多系统/特定硬件环境**下存在严重的兼容性与稳定性风险。
- **主要矛盾**：**误报与过度拦截**问题突出（如游戏文件被查杀、正常软件操作被阻），直接影响了用户对产品“智能性”的信任，可能导致用户关闭核心防护功能，引入真实安全风险。
- **体验痛点**：**资源占用异常**（C盘突增24G）、**核心工具缺陷**（手心输入法词库逻辑问题）等非安全类问题引发强烈用户不满，影响产品整体口碑。
- **运营压力**：超过60%的反馈附带文件（`has_attachment: 82`），对样本分析、人工鉴定及响应效率提出了更高要求。

2. 详细数据分析

2.1 反馈分类分布

类别	数量	占比	关键问题简述
问题反馈	78	57.8%	输入法缺陷、误拦截、资源占用异常等核心体验问题。
人工服务	13	9.6%	寻求人工帮助，多与复杂问题或样本鉴定相关。
样本举报	8	5.9%	用户提交疑似误报文件请求鉴定。
软件管家/苏打办公等	12	8.9%	关联工具的功能或兼容性问题。

类别	数量	占比	关键问题简述
系统急救箱/驱动大师	4	3.0%	系统修复、驱动管理相关反馈。
其他/未分类	20	14.8%	包含解决方案咨询、网址举报等。

分析：“问题反馈”占比最高，表明产品在**功能实现、交互逻辑和资源管理**等基础体验层面存在较多优化点。

2.2 情感与内容分析

- **整体情绪**：**负面。**用户主要表达了对功能缺陷、系统被影响、资源被占用的困扰与不满。
- **关键诉求**：
    1. **稳定性**：安全操作不应破坏现有系统（尤其是多系统环境）。
    2. **精准性**：防护应更智能，区分恶意行为与正常软件操作，减少误报。
    3. **可控性**：用户需要清晰、便捷的途径管理防护规则和产品资源占用。
    4. **透明度**：对于安全警告，用户希望获得更明确的解释和可操作的选项。

2.3 处理状态分析

- **已答复/已解决**：133条（98.5%），表明客服响应覆盖率高。
- **待跟进 (`need_followup`)**：2条，需确认是否为上述高风险或中风险事件的深度处理。

3. 风险等级评估

风险等级	数量	具体描述	可能影响
高风险 (High)	1	漏洞修复/清理功能导致双系统（Win10+Deepin）中Deepin无法启动。	系统不可用，数据丢失风险，严重损害用户信任与产品声誉。
中风险 (Medium)	1	安全防护过度拦截“模拟鼠标操作”的正常软件。	妨碍用户正常工作流，可能导致用户禁用关键防护模块，引入安全盲区。
低风险 (Low)	0	-	-
潜在风险			

风险等级	数量	具体描述	可能影响
	多项	C盘异常占用24G（引发强烈不满）、高频输入法功能缺陷（影响日常体验）。	导致用户卸载，负面口碑传播，影响产品整体市场评价。

4. 改进建议

4.1 对测试开发团队

1. **强化兼容性测试矩阵**：立即将**多操作系统共存（特别是Windows + Linux双启动）** 的场景纳入高风险功能（如系统修复、驱动更新、深度清理）的强制测试流程。
2. **建立资源监控与告警机制**：在产品中内置对临时文件、日志、隔离区等磁盘占用的监控，异常增长时主动提醒用户或自动清理。
3. **优化“智能”防护策略**：针对游戏修改器、自动化办公软件等常见“灰色”软件，**细化行为识别规则**，并提供更灵活的“信任此程序”或“创建规则”的选项，减少一刀切拦截。

4.2 对安全运营团队

1. **建立风险反馈闭环**：将用户反馈的严重系统兼容性问题，**同步至安全研究与漏洞挖掘团队**，分析是否为安全工具自身引入了新的系统脆弱点。
2. **提升样本处理与用户沟通效率**：
    - 对用户提交的样本，利用AI初筛后，可在产品端提供更快的初步结果（如“暂未发现恶意行为，建议添加信任”）。
    - 丰富知识库，针对“如何恢复误报文件”、“如何调整拦截强度”制作清晰的图文/视频指南。
3. **优化反馈分类标签**：当前存在未分类（“”）反馈，建议优化反馈提交界面或后台分类规则，确保问题能被准确归口。

5. 下周重点

1. **【紧急】 成立专项小组**，复现并彻底解决**漏洞修复导致Deepin系统无法启动**的高风险问题，发布修复方案或临时规避指南。
2. **【高优】 分析C盘异常占用案例**，定位具体模块（如日志系统、备份机制）的问题根源，准备热修复或下版本优化方案。
3. **【持续】 梳理“误报/误拦截”高频场景**，由安全运营团队牵头，协同算法与开发团队，启动1-2个典型场景（如特定游戏、办公软件）的防护规则优化试点。
4. **【流程】** 召开一次 **【测试】&【安全运营】跨部门会议**，基于本周报案例，同步风险，对齐在“兼容性测试”和“用户风险反馈”方面的协作流程。

报告结束

生成时间: 2026-01-03 22:33:49 | 机密文件