

清源 CleanSource

软件成分分析 (SCA) · Software Composition Analysis

开源组件安全漏洞

开源许可证合规风险

软件出口合规

使用开源软件面临的挑战

开源应用规模激增，安全与合规风险加剧



漏洞普遍且定位低效

84% 代码库至少含 1 个漏洞，74% 含高危漏洞，人工定位普遍耗时。



治理体系建设滞后

开源治理战略与人力投入不足，全生命周期管控薄弱，合规审查机制不健全。



AIGC 时代新挑战

LLM 等技术加速创新，同时放大开源漏洞与许可证合规的潜在风险。

84% 代码库至少含 1 个漏洞

74% 代码库含有高危漏洞

数据来源：行业开源安全研究报告

清源 CLEANSOURCE SCA

高效管理开源组件安全与许可证合规

提供多种先进探测技术、全面的数据库与灵活的部署方式，助力企业快速建立准确、全面的 **软件物料清单 (SBOM)**，保证开源组件与库的可见性；依托强大的**漏洞可达 / 不可达性分析**与漏洞治理能力，降低并管理因引入开源及第三方代码带来的**安全、质量与许可证合规风险**。



安全风险防控

漏洞精准识别、恶意代码检测



合规性管理

许可证合规、供应链透明化



开发效率提升

自动化检测、基线管理



成本优化

修复成本降低、审计成本减少



安全体系建设者

OSPO、安全架构师等



开发流程优化者

DevOps、CI/CD 流水线负责人



合规风险管控者

法务、知识产权顾问



安全运营执行者

安全运营工程师、漏洞管理专员

CSSA · 独家漏洞情报体系

从 GitHub Oday 源头生产高质量漏洞情报

传统 CVE / NVD 视角已滞后 —— 将漏洞感知前移到 Issue 与 PR 级别，多源富化让漏洞情报「更早 · 更全 · 更可用」。

70-80
条/日 稳定产能30+
天提前预警

Issue + PR 双源感知

同时覆盖最早风险线索与修复行为，比只看 CVE 更早一步

大模型辅助 + 人工核验

语义识别安全信号，人工确认保证结构化情报可用、稳定

命中当前版本研判

关联 GHSA / CVE / CSSA 情报，判断版本影响与利用条件

多源富化：GitHub Issue · Security PR · Mailing List · Apache · oss-security · CNA / Vendor

八大核心功能 · 数据库实力 · 核心优势

产品能力

清源 SCA 八大核心功能

01
多维度
全面检测

02
识别组件
安全与合规风险

03
CSSA 独家
漏洞体系

04
漏洞可达&
不可达分析

05
二进制
软件包扫描

06
AI 风险
治理能力

07
安全审计
能力

08
可视化的
数据总览

数据库实力

覆盖全球全面准确的开源软件数据库

1 开源引入场景

2 识别技术 & 算法

3 SCA 知识库

4 生成 SBOM

依赖引入 源码引入 二进制引入

构建 / 非构建扫描 精确目录匹配 文件匹配 代码片段匹配 反编译 函数相似度匹配

3 万亿行 开源代码 3.2 亿个 组件信息 27 万+ 漏洞信息 200+ 开源组件源 604 种 编程语言 千亿级 文件信息

支持主流格式 SPDX · CycloneDX · SWID；含提供者、组件名称与版本、唯一标识符、依赖关系、创建人与时间戳等。

提高供应链透明度 高效管理供应链风险 方便跨组织共享交换 统一输出格式建立生态

核心优势

五大维度，业界领先的 SCA 能力

组件识别

- 604 种语言全覆盖
- 组件/文件/依赖/片段/二进制扫描
- Linux 内核约 40 分钟

知识库

- 3.2 亿组件信息
- 27 万+ 漏洞信息
- NVD / CNVD / CNNVD / CAVD / GitHub Advisory
- CSSA 提前 30+ 天预警

合规

- 许可证检出率 98%+
- 风险等级/兼容性/篡改告警
- 权利义务追溯与解读

集成性能

- CLI / API / Jenkins / LDAP / ...
- 主流代码仓库兼容

灵活部署

- SaaS / 本地 / 混合部署
- 支持并行扫描
- 提供服务器配置建议

部分服务客户

互联网 & ICT 腾讯 · 阿里巴巴 · 百度 · 蚂蚁集团 · 字节跳动 · 中兴通讯

汽车 宝马 · 蔚来 · 博世 · 延锋 · 零束 · 零跑汽车

高校 & 社区 公安部三所 · 上海交通大学 · 复旦大学 · OpenAnolis · OpenSDV

高端智造 小米 · vivo · OPPO · 荣耀 · 新华三 H3C · 大华

半导体 & 软件 壁仞科技 · 紫光展锐 · 江波龙 · 全芯智造 · 航盛 · 统信软件

基金会 & 机构 Linux 基金会 · 中国信通院 · 工信安全 · OpenChain · OpenSSF · 开放原子开源基金会

