itbigtec
艾体宝

艾体宝Mend
应用程序安全检测平台

AI赋能，全面提升软件安全与合规处理

贯穿创建到提交的全生命周期安全

Mend通过双重扫描保障AI代码的安全性：创建阶段提供快速的A1优化检测，提交时进行深度的SAST/SCA分析，实时发现漏洞并验证代码质量，从而确保开发流程不受影响，安全问题在早期得到处理。

应用安全体系的统一可视化

通过单一平台，Mend实现了对AI代码、开源组件、容器及模型的全方位安全可视化，消除了信息孤岛，并在统一的成本模型下简化了运维工作，确保企业在扩展AI应用时依然能够保持安全的可视化管理。

AI 赋能的高效规模化漏洞修复

Mend.io 结合AI和自动化技术，从根本上加速漏洞修复流程。通过实时反馈和智能决策，帮助开发者聚焦核心问题，提升团队在大规模环境中快速响应和修复AI相关漏洞的能力。

保护技术栈中的每一个 AI 组件

Mend AI 平台能够自动发现、扫描、管理并加固每一个 AI 模型、agent 或 prompt，提供全面的安全可视化，并通过智能修复建议引导开发者进行安全操作，有效降低 AI 风险并确保工作流程中的安全性。

itbigtec 艾体宝
itbigtec.com
sales_it@itbigtec.com
400-999-3848
分部：广州 | 上海 | 苏州 | 北京 | 西安 | 成都 | 台湾 | 香港 | 日本 | 韩国
版本：V1.0

联系我们
(T: 135 3349 1614)

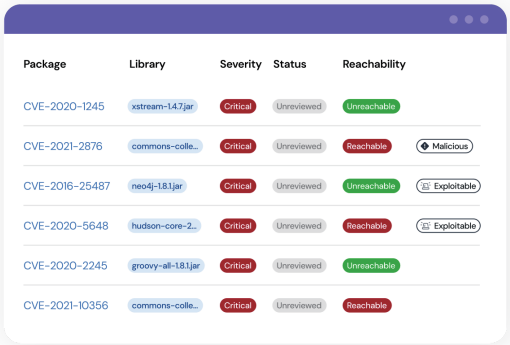
网络安全交流群

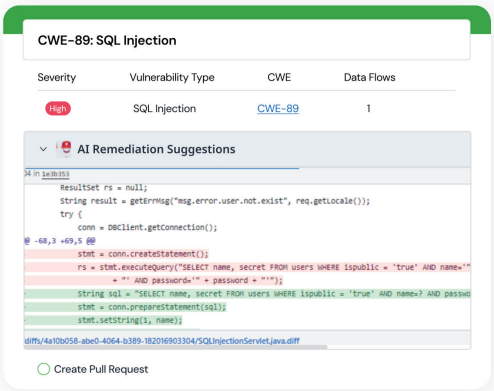
获取更多案例

关键功能解析

Mend SCA(软件组成分析)

- 通过先进的可达性分析技术，精准识别 AI 代码中可能被利用的漏洞，并优先处理实际可被攻击的漏洞。集成 CVSS 4.0 严重性评级，确保漏洞处理优先级清晰。
- 自动生成详尽的软件物料清单（SBOM），包括所有库和依赖项，支持 SPDX、CycloneDX 等国际标准格式，确保 AI 项目中的所有依赖都被清晰记录。
- 提供自动化漏洞修复功能，能够在代码提交前实时发现并修复开源漏洞，减少漏洞暴露的风险。
- 针对 AI 模型和容器环境，自动检测暴露的密钥、证书等敏感信息，并结合可达性分析持续保障容器环境中的安全性。





Mend SAST(静态应用安全测试)

- AI 驱动的漏洞检测聚焦于当前代码的变动，大幅减少误报，提升精确度。AI 的聚类和降噪机制提高了检测的精度，精确率提升 38%，召回率提升 48%。
- 利用 Mend AI 驱动的修复机制，漏洞信息可以直接传递给 AI 代码助手，在 AI 工作流程中自动修复自定义代码缺陷。修复准确率提高 46%，显著降低开发者的工作负担。
- 完全集成 IDE、源代码仓库、依赖注册表及 CI/CD 流水线，实现真正的"安全左移"，保障开发过程中的每一步都能得到安全管控。

Mend AI(AI 安全管理)

- 自动识别 AI 代码和依赖中的模型、框架与智能代理，覆盖 Hugging Face 和 Kaggle 上超过 50 万个 AI 模型。实时生成完整的 AI-BOM(AI 软件物料清单)，确保所有 AI 资产都能得到全面管理。
- 独特的暴露等级评估将 AI-BOM 与已知风险(如许可问题、公开漏洞、恶意包等)关联，提供详细的修复建议，并优先排序，帮助团队有序应对风险。
- 通过 Mend 平台的预置或自定义用例，自动化检测 AI 的潜在行为风险，涵盖 Prompt 注入、上下文泄露、数据外泄等新型攻击手段，确保 AI 应用的安全性。
- 在大规模 AI 部署中，统一管理模型使用、许可证合规及提示安全，强制执行安全规则，并通过审批流程确保 AI 资产在所有环境中的安全可控。