MEND

Open Source Audit

In the high-risk world of M&A, speed and accuracy are critical. Assessing software assets requires both the expertise of seasoned auditors and strong Software Composition Analysis (SCA) technology. Mend Open Source Risk Assessment Audit leverages Mend's technology, combined with an actionable report by expert auditors, to deliver a trusted on-demand solution that provides a comprehensive risk profile of a software asset. The audit process is swift, requiring no on-premises support. We present a complete and accurate picture of open source license compliance, application security, and code compatibility risks, to help organizations make informed decisions before an acquisition or an investment.

The audit helps teams to

Mitigate potential open source license violations by listing all of the open source and third-party components, and highlighting any license conflicts. components, and highlighting any license conflicts. Detect known open source security vulnerabilities that might affect the value of the asset. Identify out-of-date versions and multiple versions of the same open source component. Remediate any issues found, swiftly, based on recommendations from the open source community.

How it works

Using a quick and simple process, analysis is performed on all open source libraries, including direct and transitive dependencies. Detailed information about license compliance, security vulnerabilities, and compatibility risks created by open source libraries, are presented.

Audit Deliverables

1. Open source audit report

Includes an executive summary, dashboard views of overall risk composition, Open Source License Risk analysis, Security Vulnerability analysis, and Compatibility Risk analysis which highlights components which are multi-versioned or out-of-date. The report also provides the added value of detailed comments from the auditor, annotating the report with observations regarding usage and actual risk presented by the library.

2. Due diligence report

A detailed report that lists the libraries detected during the analysis (BOM). Additional information such as licenses, risk score, copyright and references to the home of the library can also be found in this report.

3. Secrity vulnerabilities report

This report lists all of the known open source security vulnerabilities that were discovered in the audit, with detailed information about the vulnerabilities, their location in the projects, and a suggested fix for faster remediation.

4. License text abd attributions report

A report that lists the various licenses for this project, their license texts, and copyright information when available.

5. Compatibility risk report

A list of outdated and multi-versioned libraries and update recommendations.

6. Audit report walkthrough

This hands-on consultation session helps all parties understand the data presented in the reports. It also includes a walkthrough of the report sections, high-risk areas, and other items highlighted during the audit.

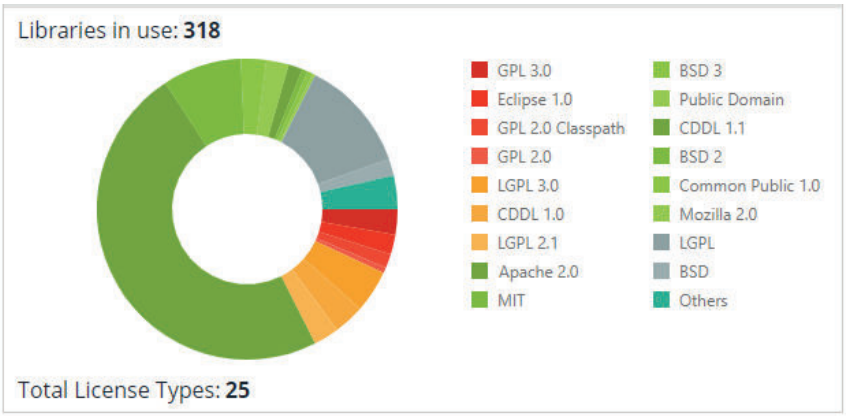
The Anlysis Dashboard

The license risk distribution chart (left) and the Vulnerability Severity distribution chart (right), describe the overall risk status of an organization's codebase.

Licenses Risk & Severity Distribution

License Distribution Overview

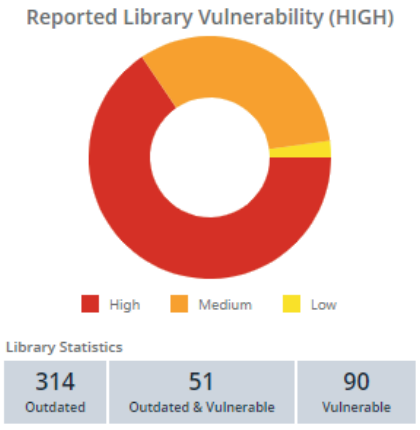
This chart is part of the License Risk Analysis Overview. It presents the total number of open source license types used in the organization's codebase, and their distribution.



Licenses Analysis

Reported Security Vulnerabilities Chart

This chart is part of the Security Risk Analysis Overview and presents the overall distribution of high, medium, and low severity open source security vulnerabilities discovered in an organization's code base.



Library Vulnerability