Nexus Auditor
Monitor production and third-party apps for open source risk.

Open source components age more like milk than wine. With 1 in 10 open source component downloads containing a known security vulnerability, how do you manage risk in your production or third-party applications?

Organizations that outsource their development efforts to third parties must first understand what open source is included in those applications and if it poses any security or legal risk, before they put it in production.

Additionally, legacy applications no longer going through development must be analyzed to understand risk exposure relative to outdated open source components.

Manual verification methods don’t scale. Visibility into open source usage is a requirement to mitigate risk.

Generate a Software Bill of Materials
Nexus Auditor automatically generates a software bill of materials to identify open source components used within third-party or legacy applications.

Get a complete list of open source components included within your app to quickly identify components that violate your open source policies.

“I would give this product a nine out of ten. I’ll have a full report of artifacts—including those that are not secure—that would have been ingested into our organization. That information is priceless.”

—C. CHANI (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW

www.sonatype.com
Continuously Monitor Apps for New Vulnerabilities

An open source component might be free of security vulnerabilities today, but that doesn’t mean it will stay that way forever. Nexus Auditor continuously monitors your production applications to identify newly disclosed vulnerabilities.

You’ll receive an email or alert when a new vulnerability is found, so you can immediately take action to eliminate any threat from outside attackers.

Key Benefits of Nexus Auditor

✓ Protect third-party or legacy applications from vulnerable open source components.
✓ Continuously monitor applications for new risk and take action before it’s too late.
✓ Feel confident that outsourced development teams are not using restrictive open source licenses, eliminating potential legal issues.
✓ Sleep better at night knowing that open source risk is being actively managed, even in applications no longer being developed.

There is a feature called Continuous Monitoring. Because of this feature, as time goes on we’ll be able to know whether a platform is still secure or not. It’s integrated, it’s proactive, it’s exactly what you want for a security product.”

—C. CHANI (FINANCIAL SERVICES), IT CENTRAL STATION REVIEW