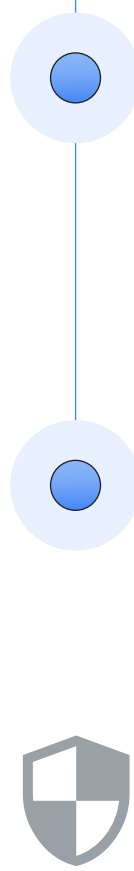
Securing your open source dependencies

5 practical steps for developers, architects, and industry leaders



Google Cloud

Google Cloud

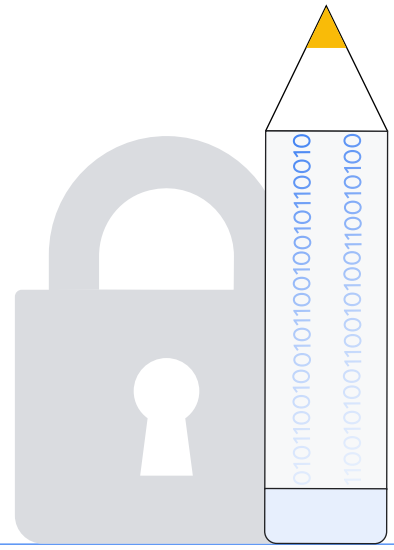
Open source software (OSS) offers a wealth of libraries, frameworks, and tools that can be used to build applications quickly.

However, OSS use also comes with challenges, including security risks.

Securing open-source software dependencies is a multifaceted effort that requires the involvement of developers, architects, and industry leaders. By taking these steps, we can strengthen the security of open-source software and build more resilient and trustworthy systems.

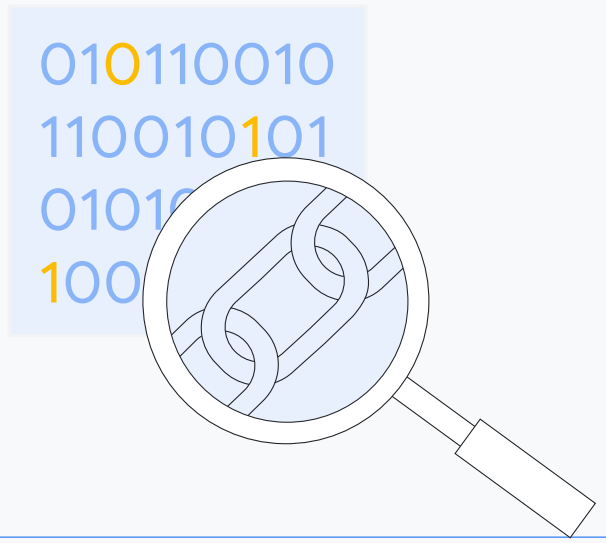
Google Cloud

Developers



- Understand your full inventory of open source software and transitive dependencies.
- Follow CISA guidance and use a known and trusted supplier to obtain components with assured software bills of materials (SBOMs) and tamper evident provenance.
- Regularly update dependencies to the latest version which includes security patches and bug fixes.
- Implement strong access controls and authentication mechanisms to limit access to dependencies.
- Adopt the SLSA framework and both assess your current software development security state and prioritize the steps to progress to the next SLSA level.

Google Cloud

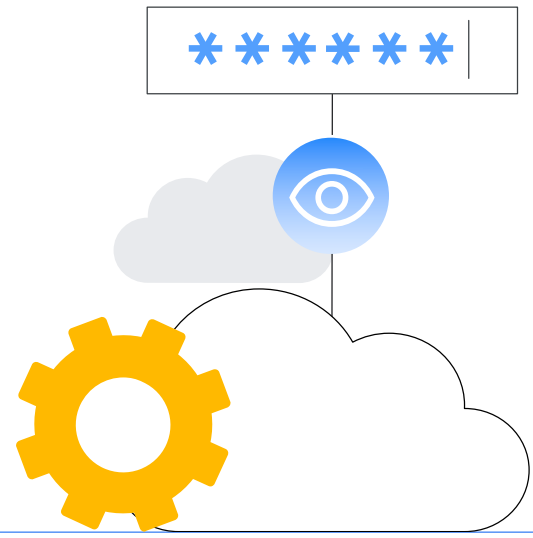


Architects

- Use software composition analysis (SCA) tools to identify and track open-source software dependencies.
- Understand risk levels and implement policies / controls matched to the sensitivity and importance of each of your projects and workloads.
- Evaluate and monitor the security of third-party libraries and components before and after they are integrated into a system.
- Create tooling to generate, consume and combine SBOMs to have a clear understanding and control of components in your applications.
- Establish and enforce secure coding standards, conduct security reviews, and assess system design and architecture to identify and mitigate potential security risks.

Google Cloud

Industry Influencers and Leaders



- Encourage the adoption of SBOMs to increase transparency and accountability in the software supply chain.
- Support the development of open-source software vulnerability databases and the creation of standards for reporting and sharing security issues.
- Support flagging malicious packages / versions by the community and blocking them for all.
- Provide funding and resources to the developer communities to empower maintainers to build securely, proactively find and fix security issues in their code, and build assured SBOMs.
- Promote/mandate the use of existing standard tools like OpenSSF Scorecard.

Google Cloud

Get started with Assured OSS: your trusted source for OSS packages for Java and Python ecosystems.

Leverage the security and experience Google applies to open source dependencies by incorporating the same OSS packages that Google secures and uses into your own developer workflows.

Google Cloud

Using Assured OSS, you can:

- Obtain your OSS packages from a trusted and known supplier,
- Know more about your ingredients with Assured SBOMs provided in industry standard formats like SPDX and VEX,
- Reduce risk - as Google is actively scanning, finding, and fixing new vulnerabilities in curated packages,
- Increase confidence in the integrity of the ingredients you're using through signed, tamper evident provenance,
- Choose from 1000+ most popular Java and Python packages, including common ML/AI projects like TensorFlow, Pandas, and Scikit-learn.

Google Cloud

Sign up to use Assured OSS for free!