Securing the foundation for software development

With the dramatic rise of state-sponsored cyber attacks and malicious actors online, we believe our products and services are only as helpful as they are secure. At Google, we are more focused than ever on protecting people, organisations and governments by sharing our expertise, empowering society to address ever-evolving cyber risks and continuously working to advance the state of the art in cyber security to build a safer world for everyone.

Open source software — code that is made freely available for anyone to use, modify, and build upon — is the foundation of the modern Internet. The world of open source software development allows collaboration and rapid innovation by sharing solutions freely. Yet the very openness that makes the digital world accessible to everyone also leaves it uniquely vulnerable to security threats.

Challenge

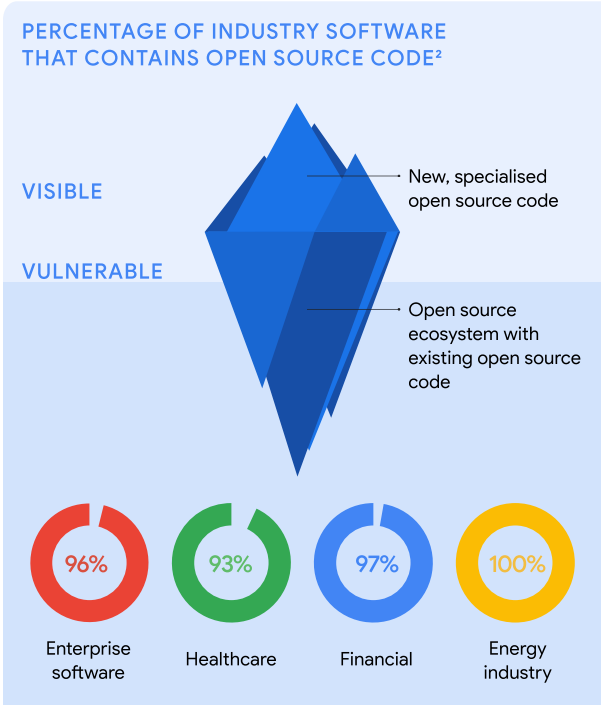
Open source software is a concern for everyone

The open source development community, built on transparency and sharing, contributes an enormous amount of code to the majority of applications we use today. From medical equipment to the power grid, people rely on open source software (OSS) virtually every hour of every day—making open source projects a prime target for cyber attacks. The last three years saw a 742% year-over-year increase[1] in software supply chain attacks.

The open source ecosystem is intricately layered, where hidden indirect dependencies can contain security flaws. These layers make vulnerabilities hard to detect manually, and securing this portion of software development has become an urgent security issue globally.

Additional focus is required at all levels:

- Open source developers need knowledge and resources to secure their projects
- Organisations need to understand supply chain risks and vulnerabilities to develop mitigation plans
- Governments and industry must partner to ensure robust, effective security standards[3]



[2] Source: 2022 Synopsys Open Source Security and Risk Analysis Report

Our solution

Securing open source software for everyone

At Google, we've been working on this challenge for years. In fact, each year over 10% of Googlers contribute to open source software projects. Our experience leads us to conclude that modern digital security can actually come through embracing openness. Open approaches ensure we can rapidly adopt the latest innovations and allow more people to solve security challenges. But to fully unlock the value of open source, we need stronger public-private partnerships and dynamic policy frameworks to shore up security for everyone.

- We're leading the community with next-level security frameworks, such as Supply-chain Levels for Software Artefacts (SLSA),[4,5] and developing advanced security tools.
- We've developed Graph for Understanding Artefact Composition (GUAC), which brings together software security information from different sources into a single queryable database. GUAC will democratise the availability of security information by making it freely accessible and useful for every organisation.

Our commitments:

- Invest $100 million in open source security, leadership roles in the Open Source Security Foundation, and direct collaboration with developers
- Define and share actionable security standards, guidance, free tools and best practices we use internally with the entire open source community
- Advance detection, automated triaging, and ways to build security into the earliest development stages
- Automate tooling to make enterprise-level security free and accessible for everyone

Google OSS-Fuzz
Our response to the Heartbleed bug

In response, Google launched OSS-Fuzz as a free community service. Fuzz testing pinpoints unknown security weaknesses in minutes, unlike manual testing, which can take months. We invested in building an infrastructure to automatically test hundreds of open source projects. OSS-Fuzz now runs regular code scans and is innovating constantly to find more classes of bugs.

800+ critical open source projects are scanned by Fuzz testing in six languages.

Our industry investments and milestones

2020

AUGUST
Joined Open Source Security Foundation (OpenSSF) to guide and improve the security of open source software

2021

MAY & JUNE
Established OSS best practices in compliance with **White House Executive Order 14028** and contributed guidance on software supply chain security standards.

JUNE
Released SLSA with OpenSSF, externalising Google's internal security framework and allowing everyone to build more secure software.

AUGUST
Pledged $100M to uplift and secure OSS, including partnering with developers to find and fix vulnerabilities.

2022

MAY
Announced Google's Open Source Maintenance Crew during a **DC Summit,** dedicating a team of full-time developers to work directly with open source projects to improve their security.

MAY
Announced Assured Open Source Software product, which helps incorporate the same trusted open source packages that Google uses into developer workflows.

Google recommended practices that can help public and private organisations stay safe today:

- Implement SLSA to harden software supply chain security
- Cryptographically sign and verify the authenticity of your software using Sigstore
- Automate vulnerability discovery, tracking, and triaging with OSS-Fuzz and OSV.dev
- Use Scorecards to automatically evaluate security risk with your dependencies

Our approach

Software is only as secure as the weakest link. We're investing our expertise and financial resources to raise the security of the entire open source ecosystem. Our team of development and security experts believe we can protect more public and private organisations in the following ways:

Our team audits every stage of the product life cycle, continuously scanning, analysing, and fuzz testing for vulnerabilities

We support the open Internet, sharing what we know with the developer community and keeping it secure for the public and businesses

We're future-proofing security by detecting sophisticated threats, providing advanced automated tooling, and staying a step ahead of whatever comes next

Securing open source software is a shared responsibility, and we are committed to continued collaboration on this urgent, critical problem. g.co/security/gosst

Sources: 1.2022 State of the Software Supply Chain. 2. 2022 Synopsys Open Source Security and Risk Analysis Report. 3. CISA Goes on Tour to Get Feedback on Cyber Incident Reporting Rules. 4. Sharing our knowledge (i.e., releasing SLSA, guiding OpenSSF) means that everyone who makes software, not just Google, can benefit from Google's experience and time-tested security practices. 5. SLSA is a set of practices that can help organisations improve the security of their software development process. It helps meet the US government's Secure Software Development Framework, requirements laid out by the government in response to the Executive Order on cyber security. That means organisations will have guidance on how to comply with federal guidelines to make software more secure for everyone.