



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

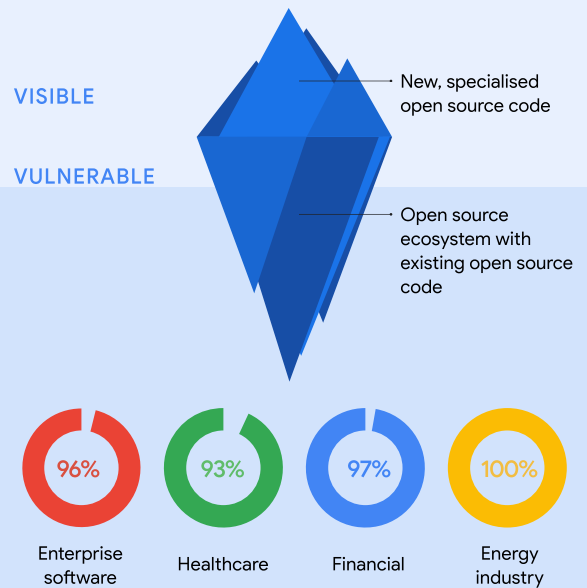
The open source development community, built on transparency and sharing, contributes an enormous amount of code to the majority of applications we use today. From medical equipment to the power grid, people rely on open source software (OSS) virtually every hour of every day—making open source projects a prime target for cyber attacks. The last three years saw a **742% year-over-year increase¹** 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 standards³

PERCENTAGE OF INDUSTRY SOFTWARE THAT CONTAINS OPEN SOURCE CODE²



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. That's why we welcome efforts by the U.S. Government to advance OSS security, such as the Securing Open Source Software Act introduced in the Senate in 2022.

- 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



Applications

Google OSS-Fuzz

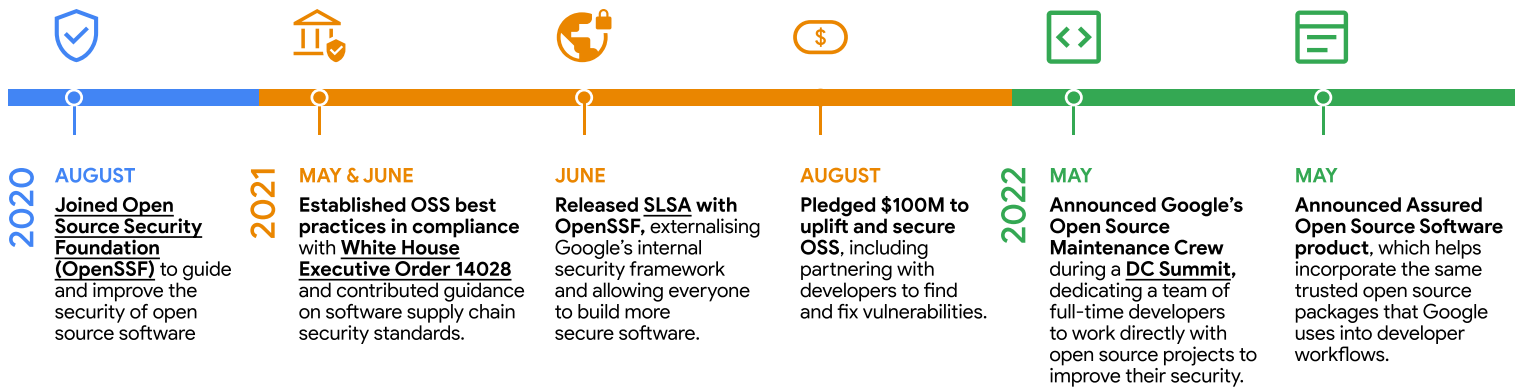
Our response to the Heartbleed bug

The [Heartbleed bug](#) was a serious open source vulnerability, a weakness with the potential to affect nearly every Internet user. In 2014, hackers stole the names, addresses, birth dates, phone numbers, and social security numbers of **~4.5M patients** from the database of one of the largest U.S. hospitals

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



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 believes 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.