



Insignary Clarity

A security and compliance solution for the open source supply chain



Table of Contents

<u>Manage Open Source Software in Your Supply Chain</u>	<u>3</u>
What is Open Source Software?.....	3
Open Source is Everywhere	3
About Open Source Security.....	3
Security Vulnerability Trends	4
Recently Discovered Security Vulnerabilities	4
About Open Source Compliance	4
Why Use Third Party Code?	5
About Third Party Code.....	5
Concerns about Third-Party Code.....	6
Conclusion	6
<u>Get Confidence through Clarity.....</u>	<u>7</u>
About Insignary Clarity.....	7
<u>Insignary Overview.....</u>	<u>9</u>
About Insignary	9
Open Source Community.....	9
Contact Us.....	10

Manage Open Source Software in Your Supply Chain

Open Source Visibility is Everything

What is Open Source Software?

- Open source software is software with source code that anyone can inspect, modify, and enhance.
- By using open source, developers can lower assembly costs and quickly add innovations, saving months or years of originally required development time.

Open Source is Everywhere

- Open Source has become pervasive in every aspect of embedded, mobile and enterprise computing. Today 80% to 90% of every modern application is comprised of open source component parts.
- It exists in every sector and adoption is growing – the Linux Foundation estimates that more than 31 billion lines of code have been committed to open source repositories.



- ☒ 1,906 new open source projects suppliers are introduced daily
- ☒ 10,000 new versions are released every day
- ☒ Each project releases an average of 14 times per year

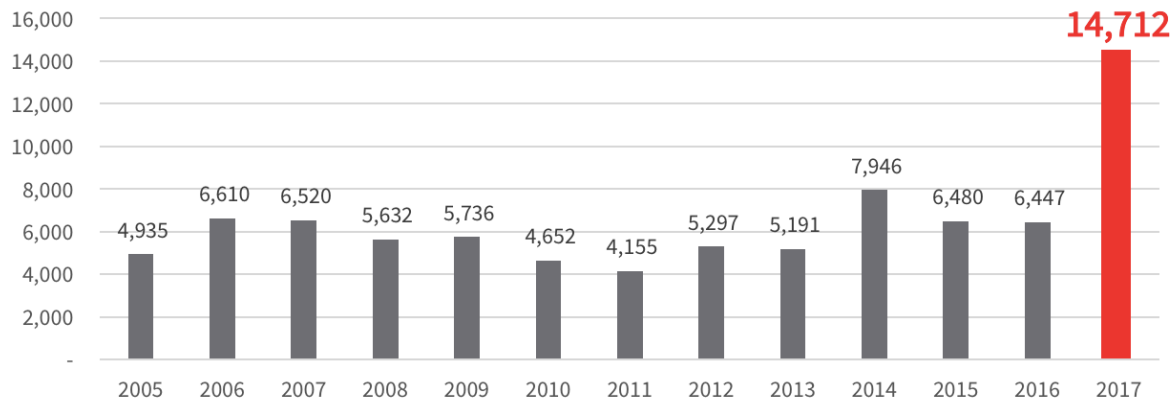
Reference: Sonatype 2017 State of the Software Supply Chain

About Open Source Security

- Significant vulnerabilities have been discovered in popular open source software.
- Because of its inherent flexibility and widespread usage, open source related vulnerabilities are an easy, efficient, and effective target for hackers.

Security Vulnerability Trends

- In 2017, we saw 14,712 new vulnerabilities added to the CVE list.
 - The same year, 4,800 OSS-related security vulnerabilities were reported, with the number of OSS vulnerabilities per codebase having increased by 134%.
- 2018 – on pace to reach 16,500 vulnerabilities, breaking last year’s record.



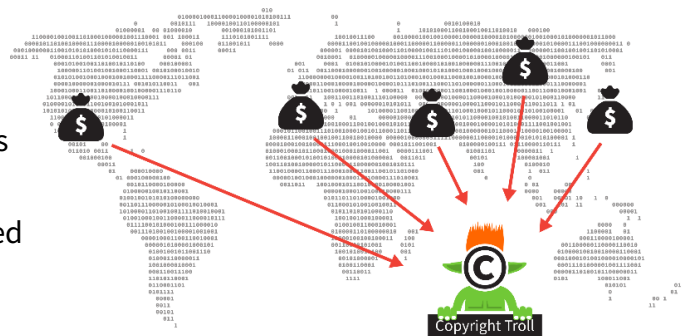
Recently Discovered Security Vulnerabilities



	Heartbleed	Shellshock	Freak	Ghost	DROWN	SambaCry	JAKARTA
Discovery	2014	2014	2015	2015	2016	2017	2017
Release	2011	1989	1990s	2000	1990s	2010	2007
Component	OpenSSL	Bash	OpenSSL	GNU C Library	OpenSSL	SAMBA	Apache Struts

About Open Source Compliance

- Open source has legal obligations when distributed
 - Open Source can only be used under terms granted by the copyright holders
- The rise of copyright trolls
 - Parties know to use open source license terms for profit (rather than for collaboration) have started to impact the market.



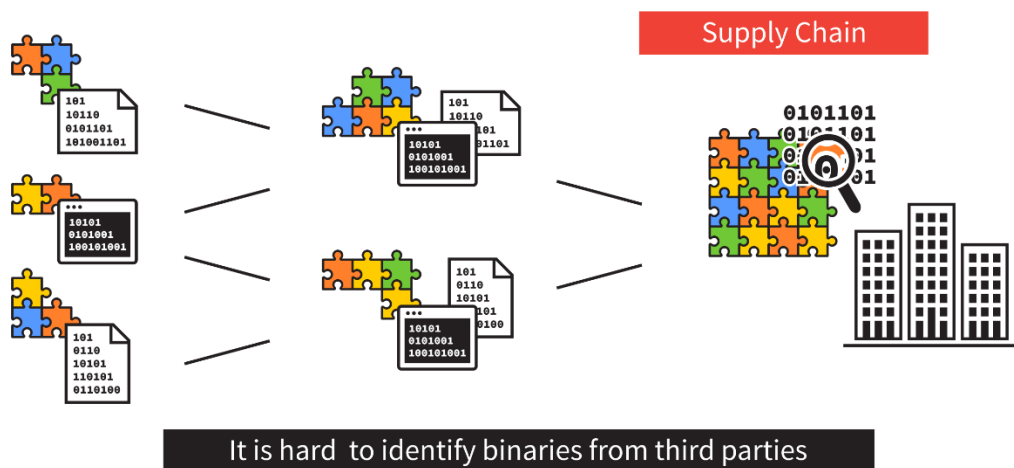
Why Use Third Party Code?

- Third party code allows companies to quickly build on sophisticated components or technology platforms.
- This helps companies to increase efficiency and reduce costs.

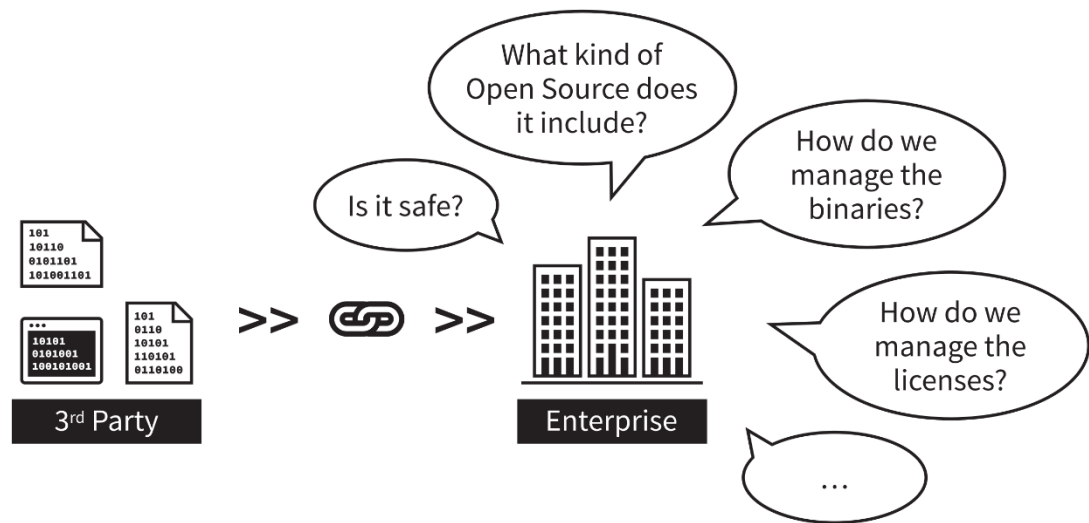


About Third Party Code

- Every company in the supply chain is responsible for the security and legal compliance of third-party code.
- Most third-party code contains open source and is distributed in binary format.



Concerns about Third-Party Code



Conclusion

- Open source software and third-party code are irreversible trends.
- But their growth and advantages are accompanied with security risks and license obligations
- If managed properly, open source and third-party code usage can deliver fantastic benefits

Get Confidence through Clarity

Taking Open Source Binary Analysis to the Next Level

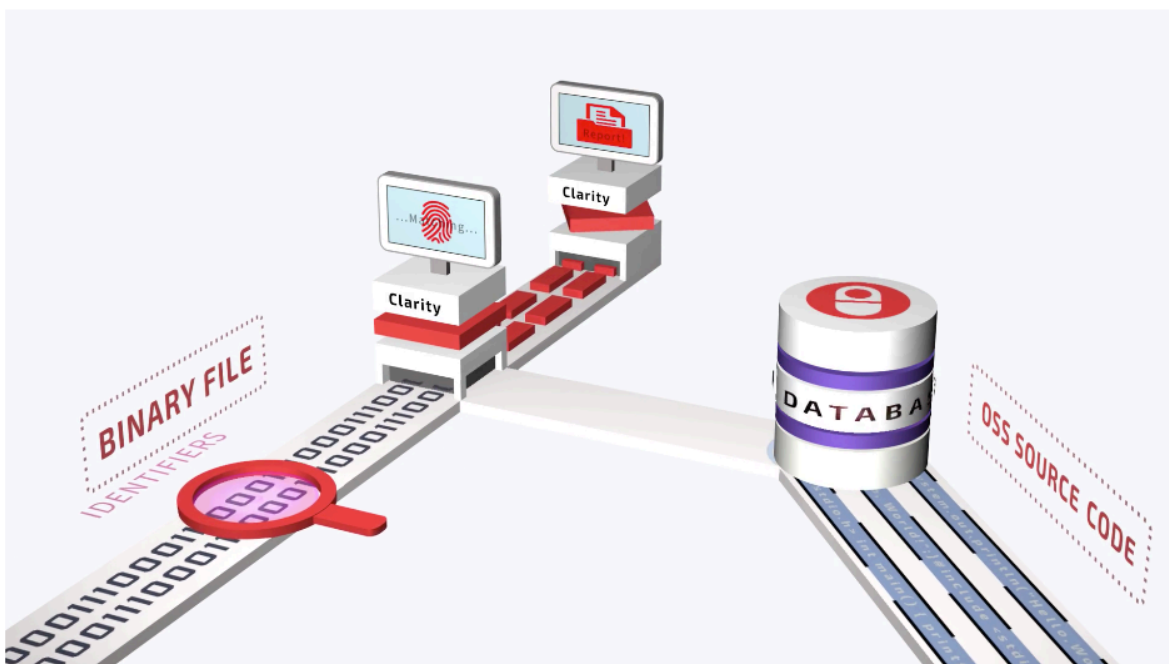
About Insignary Clarity

High Level Overview

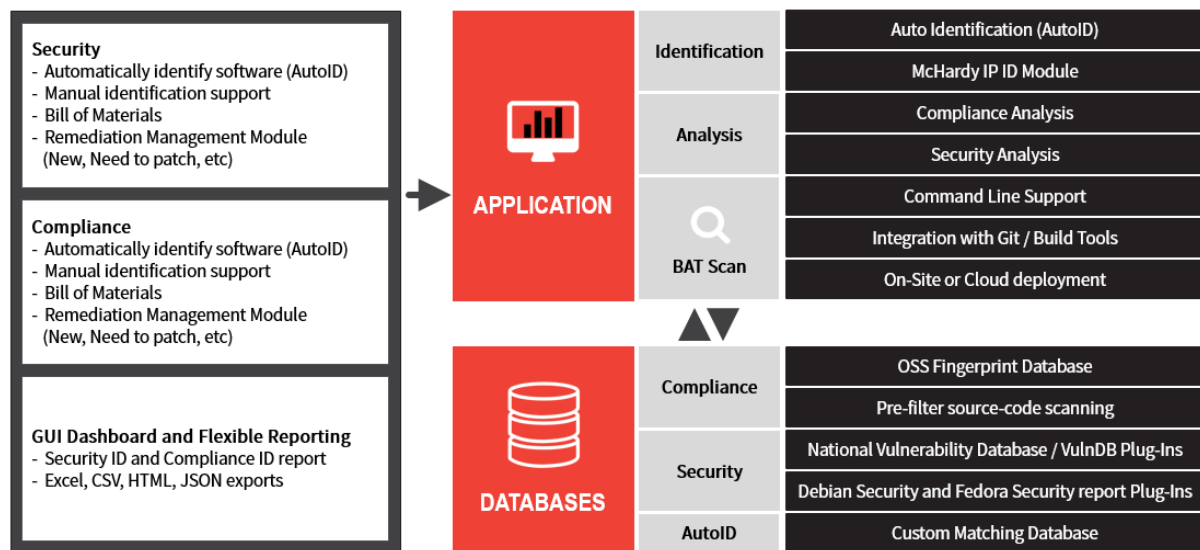
- Insignary Clarity is a specialized software composition analysis solution that can scan binary code without source code or reverse engineering.
- It provides customers with a Bill of Materials designed to show high priority security and associated potential license issues so companies can take quick, effective corrective action.
- Insignary Clarity can be deployed as a cloud-based and on-premise deployment, and supports RESTful API, LDAP, and automation servers like Jenkins.

How It Works

- We leverage unique fingerprint-based technology, which works on the binary-level without the need for source code or reverse engineering.
- Clarity extracts “fingerprints” from the target binary code to examine and then compare against fingerprints stored in our OSS source code database.



Insignary Clarity



Exact Matches and Fuzzy Matches

- Many solutions can do exact matches to known binaries, but in the embedded Linux space there is almost no standard repository for binary components that can be reused.
 - Checksum changes even if one single bit is different, making it difficult to analyze binaries using checksum-based matching.
- Insignary Clarity can do not only exact matches but also fuzzy matches.

Get Confidence Through Clarity

- Insignary Clarity helps companies identify, prioritize, and address potential open source issues in the supply chain. It equips development, operation, and security teams with increased confidence in the deployment of open source products and services.



Insignary Overview

Gain Insight into Your Binary

About Insignary

- Insignary is the developer of Clarity, a specialized software composition analysis solution that helps customers gain visibility into the binary code they use by identifying known, preventable security vulnerabilities, while also highlighting potential license compliance issues.
- We are backed by venture capital and have significant business and technical talent in our executive team, with extensive experience in the IT industry. The founding team specializes in open source software, compliance, and security.

Open Source Community

Insignary is part of a bigger open source community. Through our affiliation, we bridge organizations to the potential of open source software, while interacting and collaborating with the community to accelerate open source development.

- Insignary joined Open Invention Network community in November 2016
- Insignary joined Linux Foundation Silver Membership in January 2017
- Insignary joined GENIVI Alliance in July 2017

openinventionnetwork®



Contact Us

Email: info@insignary.com

Address: Suite 1604, 602 Yeongdong-daero, Gangnam-gu, Seoul 06083, Korea

Phone: +82-2-547-7006

Fax: +82-2-547-7166

Website: www.insignary.com

For product or partner information

Email: sales@insignary.com

Phone: +82-2-547-7167

For technical support please visit Insignary Support Desk System

<https://insignary.atlassian.net/servicedesk>