

SOFTWARE SUPPLY CHAIN RISK MANAGEMENT

Son Nguyen

Email: SonNV@mi2.com.vn

Mobile: +84977585651



AGENDA





Why Are So Many People Talking About Software Supply Chain Security?

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

Presentation content source: Synopsys

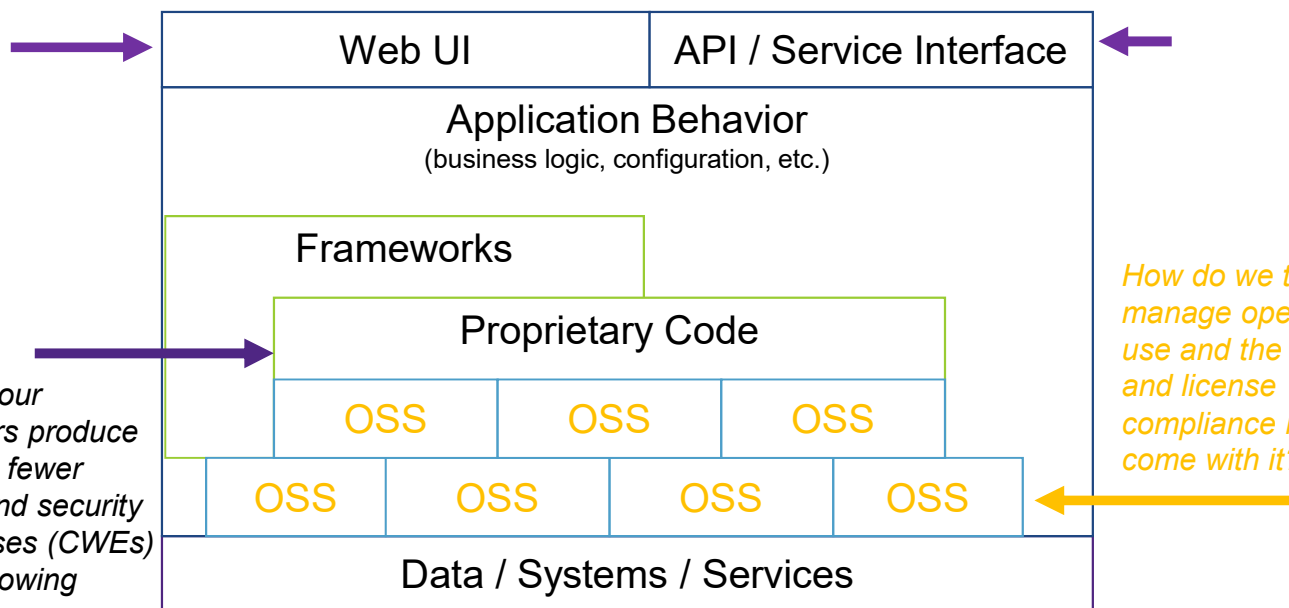
APPLICATIONS & SECURITY ISSUES

How do we know we've addressed runtime vulnerabilities and data protection issues before we deploy?

How do we ensure the protocols & APIs our software exposes aren't vulnerable to common hacks?

How can our developers produce code with fewer defects and security weaknesses (CWEs) without slowing down?

How do we track and manage open source use and the security and license compliance risks that come with it?



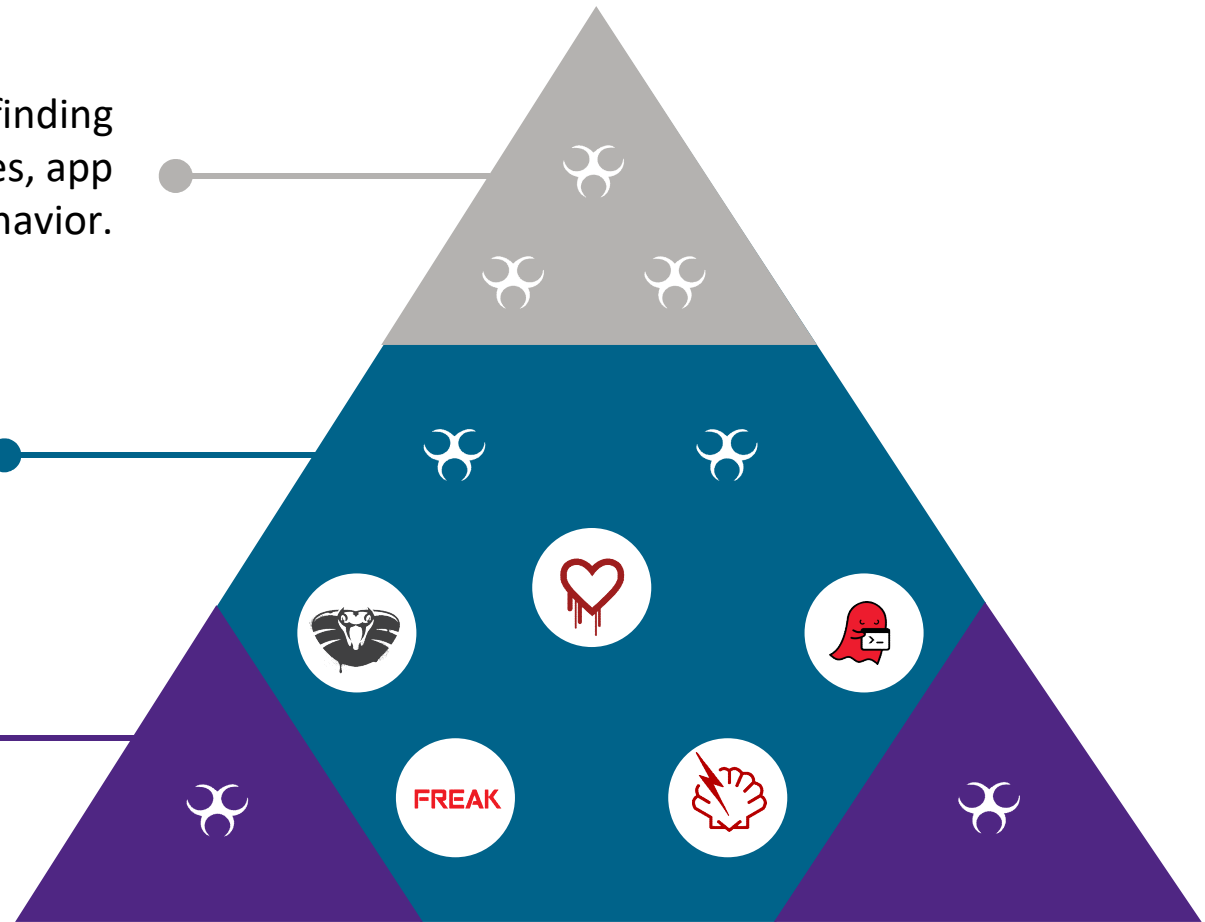
Presentation content source: Synopsys

APPLICATIONS & SECURITY ISSUES

SAST and DAST tools are good at finding security weaknesses in coding practices, app configuration, and behavior.

But most open-source vulnerabilities are too complex and too deep in the code to be found by SAST or DAST alone.

Library dependencies are often opaque to developers and open doors to vulnerabilities not in custom code.

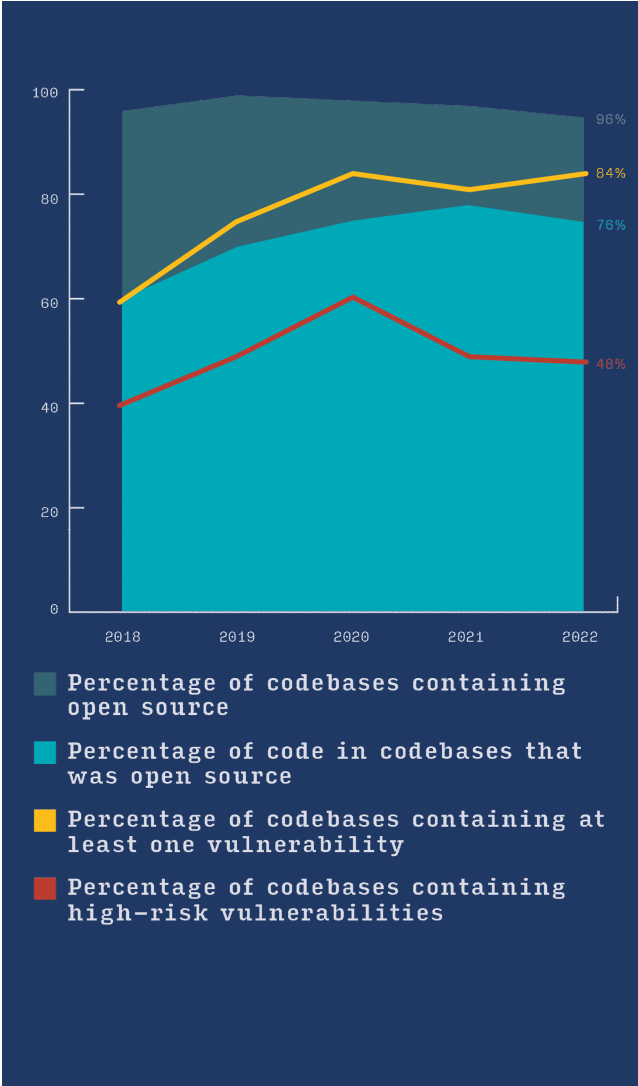


Presentation content source: Synopsys

SYNOPSYS OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT 2023

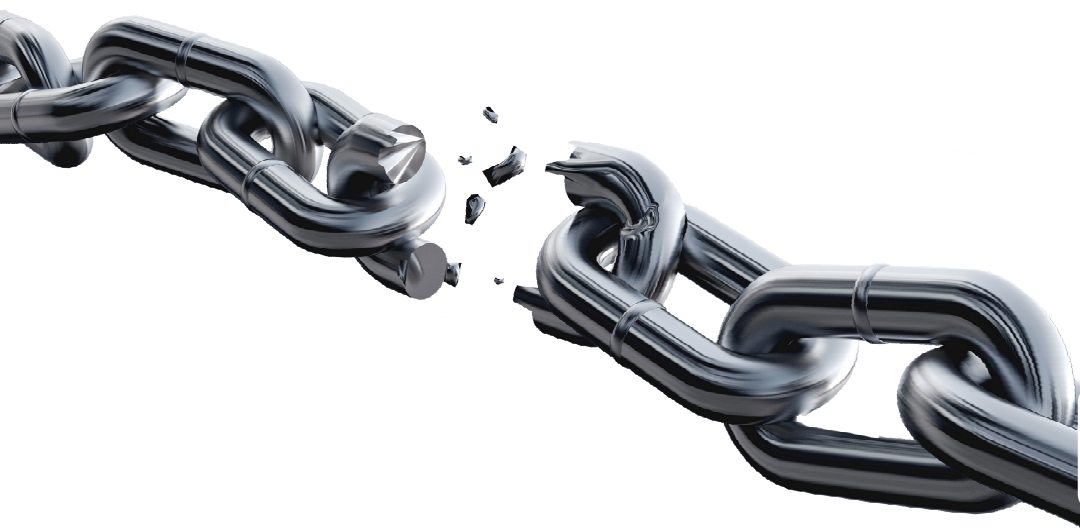
> 1703 Applications Assessed

- Almost All Codebases Contain OSS (96%)
 - Most Applications are Mostly OSS (76%)
- Most Codebases Were Vulnerable (84%)
 - High-Risk Vulnerabilities (48%)



Presentation content source: Synopsys

OPENSOURCE & SOFTWARE SUPPLY CHAIN RISKS



Zero-Day Exploits

Public Vulnerabilities

License Risk

Malware

Information Leakage

Presentation content source: Synopsys

LEGAL RISK

All Software Should Be Licensed

- Liability
- Trademarks
- Patents
- Ownership

MIT License

Copyright 2020, Synopsys Ltd.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Gnu GPL v3

FreeBSD

This GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to allow them to be shared and copied with the greatest freedom. By contrast, the GNU General Public License is intended to ensure that the users of a program have the freedom to change the program and to share their modified versions. In other words, the license grants users the freedom to copy and to modify the program and to redistribute copies. However, it does not allow users to remove their responsibility for the changes they make. When you speak of free software, you mean freedom: freedom to use the software, freedom to change it, freedom to share it, and freedom to improve it. For the software to be free, the user must be able to do these things: use the software for any purpose; study and change the source code of the program; redistribute copies of the software; and improve the program, and release your improvements to the public, so that the whole community benefits from your changes.

By contrast, if you place a program under a license that grants other kinds of freedoms, you do not have freedom of distribution. You may, for instance, place a program under a license that permits only certain users to run it, while forbidding others to run it. Or you may restrict how someone can use the software. A program that contains a restriction like this is not free software. We tell you it is not free software because you have not exercised all the freedoms that are required for it to be free software. You may still use and redistribute copies of the software if you wish, but you must also make sure that everyone who receives a copy of the software is also given the freedoms that you were given. You must make sure that you, too, are free to change and share the software.

You are not allowed to claim that the software is your own work, or that you have not received the software from the original author. To protect the rights of those who have received the software, you agree to pass on any freedom that you have. You must make sure that anyone who receives a copy of the software is also given the freedoms that you were given. You must make sure that you, too, are free to change and share the software.

You are not allowed to claim that the software is your own work, or that you have not received the software from the original author. To protect the rights of those who have received the software, you agree to pass on any freedom that you have. You must make sure that anyone who receives a copy of the software is also given the freedoms that you were given. You must make sure that you, too, are free to change and share the software.

TERMS AND CONDITIONS

0. Definitions.

This License refers to either the GNU General Public License or the GNU Lesser General Public License.

The "Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensee" and "recipient" refer to anyone who holds a copy of the Program. "You" also refers to any entity that controls the distribution of the Program, whether it is an individual, a corporation, a partnership, a government, or any other kind of organization. "You" also refers to any entity that controls the distribution of the Program, whether it is an individual, a corporation, a partnership, a government, or any other kind of organization.

The "Source Code" for a program means the preferred form of the program for making modifications to it. "Object code" means any form of a program that is not source code. "Executable" means a program that can be run on a computer. "Derivative work" means any work that is based on the Program or any part of it, including modifications, additions, deletions, and other changes, and any work that is based on the Program or any part of it, including modifications, additions, deletions, and other changes.

The "Copied and Modified Version" of the Program means any version of the Program that is based on the Program or any part of it, including modifications, additions, deletions, and other changes, and any work that is based on the Program or any part of it, including modifications, additions, deletions, and other changes.

The "Copied and Modified Version" of the Program means any version of the Program that is based on the Program or any part of it, including modifications, additions, deletions, and other changes, and any work that is based on the Program or any part of it, including modifications, additions, deletions, and other changes.

1. Copying and Distribution.

You may copy and distribute copies of the Program in any form, and by any means, without restriction, provided that you comply with the following conditions:

a) You must retain the copyright notice for this Program and any notices of copyright for any other programs included in the Program.

b) You must retain the text of this License and any notices of copyright for any other programs included in the Program.

c) You must retain the text of any other notices of copyright for any other programs included in the Program.

d) You must retain the text of any other notices of copyright for any other programs included in the Program.

2. Proprietary Software.

You may copy and distribute copies of the Program in any form, and by any means, without restriction, provided that you comply with the following conditions:

a) You must retain the copyright notice for this Program and any notices of copyright for any other programs included in the Program.

b) You must retain the text of this License and any notices of copyright for any other programs included in the Program.

c) You must retain the text of any other notices of copyright for any other programs included in the Program.

d) You must retain the text of any other notices of copyright for any other programs included in the Program.

3. Patenting.

You may copy and distribute copies of the Program in any form, and by any means, without restriction, provided that you comply with the following conditions:

a) You must retain the copyright notice for this Program and any notices of copyright for any other programs included in the Program.

b) You must retain the text of this License and any notices of copyright for any other programs included in the Program.

c) You must retain the text of any other notices of copyright for any other programs included in the Program.

d) You must retain the text of any other notices of copyright for any other programs included in the Program.

4. Conveying Modified Versions.

You may copy and distribute copies of the Program in any form, and by any means, without restriction, provided that you comply with the following conditions:

a) You must retain the copyright notice for this Program and any notices of copyright for any other programs included in the Program.

b) You must retain the text of this License and any notices of copyright for any other programs included in the Program.

c) You must retain the text of any other notices of copyright for any other programs included in the Program.

d) You must retain the text of any other notices of copyright for any other programs included in the Program.

5. Conveying Source Code.

You may copy and distribute copies of the Program in any form, and by any means, without restriction, provided that you comply with the following conditions:

a) You must retain the copyright notice for this Program and any notices of copyright for any other programs included in the Program.

b) You must retain the text of this License and any notices of copyright for any other programs included in the Program.

c) You must retain the text of any other notices of copyright for any other programs included in the Program.

d) You must retain the text of any other notices of copyright for any other programs included in the Program.

6. Conveying Executable Versions.

You may copy and distribute copies of the Program in any form, and by any means, without restriction, provided that you comply with the following conditions:

a) You must retain the copyright notice for this Program and any notices of copyright for any other programs included in the Program.

b) You must retain the text of this License and any notices of copyright for any other programs included in the Program.

c) You must retain the text of any other notices of copyright for any other programs included in the Program.

d) You must retain the text of any other notices of copyright for any other programs included in the Program.

7. Additional Terms.

You may add additional terms to the Program, but only if you do so in a way that does not conflict with the terms of this License. Any additional terms you add must be clearly marked as such, and must not be intended to restrict the freedoms that are granted by this License.

8. Disclaimers.

You may make any disclaimer you wish, but you must not attempt to disavow or limit your liability for the damage caused by the Program.

9. Acceptance of Terms.

You may accept the terms of this License by using the Program, or by copying or distributing copies of the Program.

10. Termination.

You may terminate the Program if you wish, but you must not attempt to disavow or limit your liability for the damage caused by the Program.

11. Liability.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

12. Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

13. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

14. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

15. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

16. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

17. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

18. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

19. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

20. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

21. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

22. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

23. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

24. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

25. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

26. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

27. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

28. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

29. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

30. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

31. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

32. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

33. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

34. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

35. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

36. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

37. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

38. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

39. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

40. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

41. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

42. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

43. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

44. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

45. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

46. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

47. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

48. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

49. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

50. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

51. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

52. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

53. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

54. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

55. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

56. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

57. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

58. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

59. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

60. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

61. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

62. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

63. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

64. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

65. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

66. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

67. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

68. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

69. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

70. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

71. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

72. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

73. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

74. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

75. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

76. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

77. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

78. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

79. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

80. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

81. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

82. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

83. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

84. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

85. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

86. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

87. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

88. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

89. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

90. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

91. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

92. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

93. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

94. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

95. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

96. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

97. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

98. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

99. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

100. No Warranty.

You may not attempt to disavow or limit your liability for the damage caused by the Program.

OSS LICENSE OBLIGATIONS

MIT License
Status: Approved | Family: Permissive

Required	Forbidden	Permitted
> Include License	> Hold Liable	> Distribute
> Include Copyright		> Private Use
> Conditions of Use For Globally Approved Components		> Modify
		> Commercial Use
		> Sub-License

GNU General Public License v3.0 only
Status: Unreviewed | Family: Reciprocal

Required	Forbidden	Permitted
> Include Copyright	> Hold Liable	> Place Warranty
> Disclose Source	> Sub-License	> Commercial Use
> State Changes	> Anti DRM Provision	> Modify
> Include Install Instructions	> Patent Retaliation	> Distribute
> Include License	> Fees	> Use Patent Claims
> Distribute Original		
> Reverse Engineer		
> Right to Copy		
> License Back		

Copyleft/ Reciprocal

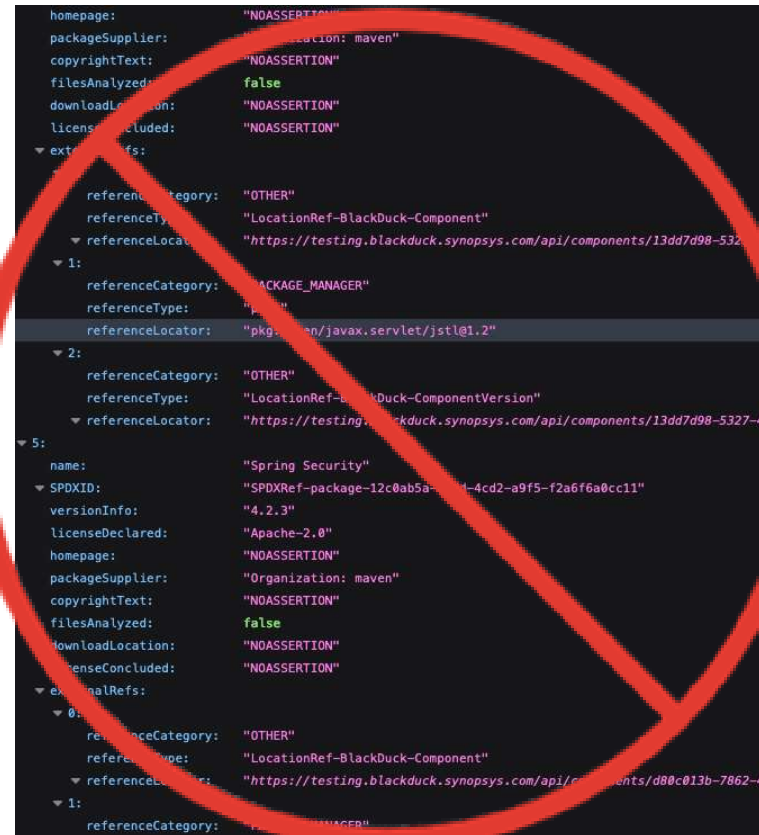


Presentation content source: Synopsys

SBOM TO SOLVE SUPPLY CHAIN RISK

WHAT IS SBOM ALL ABOUT *REALLY?*

A software Bill of Materials (SBOM) is a list of all the open source and third-party components present in a codebase. An SBOM also lists the licenses that govern those components, the versions of the components used in the codebase, and their patch status, which allows security teams to quickly identify any associated security or license risks



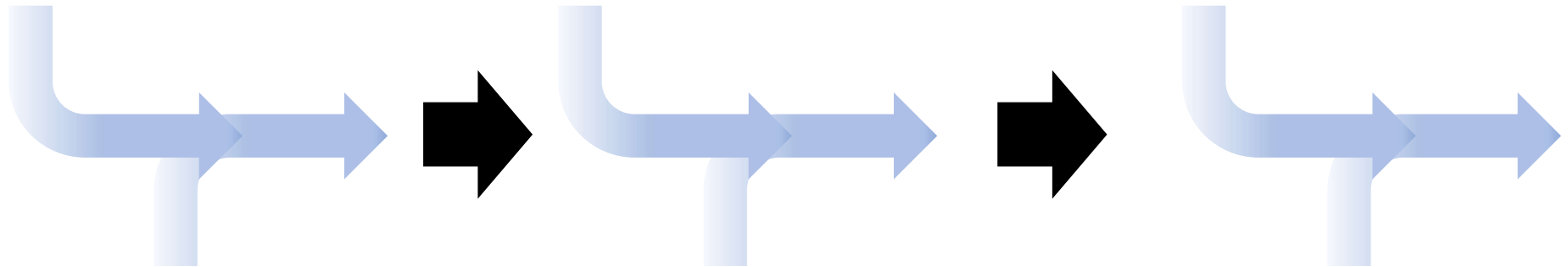
```
homepage: "NOASSERTION"
packageSupplier: "Organization: maven"
copyrightText: "NOASSERTION"
filesAnalyzed: false
downloadLocation: "NOASSERTION"
licenseConcluded: "NOASSERTION"
externalRefs:
  - referenceCategory: "OTHER"
    referenceType: "LocationRef-BlackDuck-Component"
    referenceLocator: "https://testing.blackduck.synopsys.com/api/components/13dd7d98-5327-4..."
  - 1:
    referenceCategory: "PACKAGE_MANAGER"
    referenceType: "PackageManager"
    referenceLocator: "pkg:maven/javax.servlet/jstl@1.2"
  - 2:
    referenceCategory: "OTHER"
    referenceType: "LocationRef-BlackDuck-ComponentVersion"
    referenceLocator: "https://testing.blackduck.synopsys.com/api/components/13dd7d98-5327-4..."
  - 5:
    name: "Spring Security"
    SPDXID: "SPDXRef-package-12c0ab5a-1-4cd2-a9f5-f2a6f6a0cc11"
    versionInfo: "4.2.3"
    licenseDeclared: "Apache-2.0"
    homepage: "NOASSERTION"
    packageSupplier: "Organization: maven"
    copyrightText: "NOASSERTION"
    filesAnalyzed: false
    downloadLocation: "NOASSERTION"
    licenseConcluded: "NOASSERTION"
    externalRefs:
      - 0:
        referenceCategory: "OTHER"
        referenceType: "LocationRef-BlackDuck-Component"
        referenceLocator: "https://testing.blackduck.synopsys.com/api/components/d80c013b-7862-4..."
      - 1:
        referenceCategory: "PACKAGE_MANAGER"
```

LIFE CYCLE-CENTRIC VIEW

First-Party
Code

Compiled
Binaries

Complete
Firmware



Third-Party
Dependencies

Supporting
Packages

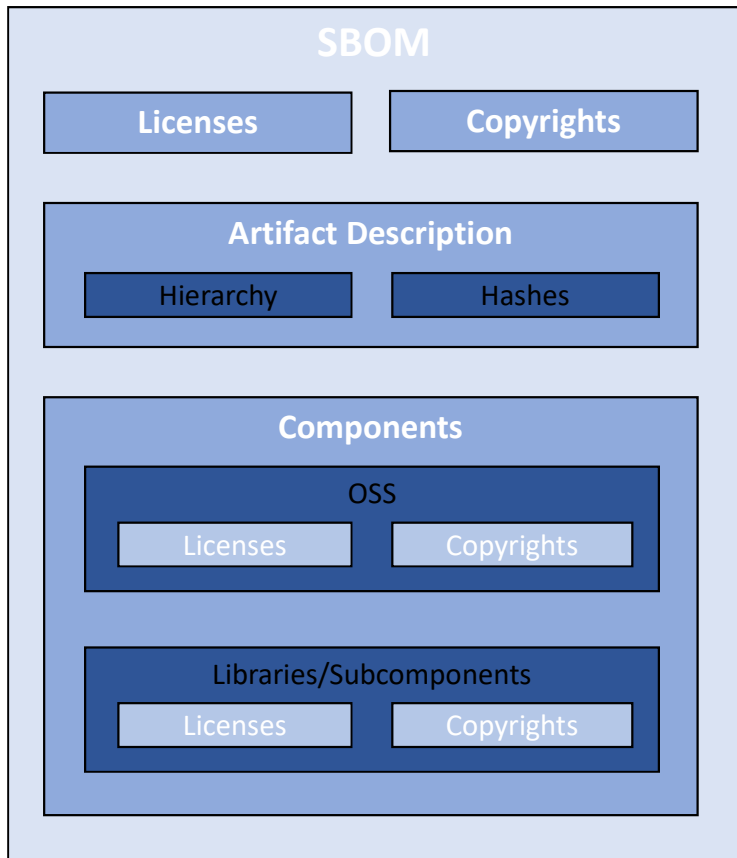
Runtime
Environment

Source

Binary

Presentation content source: Synopsys

SBOM STRUCTURE

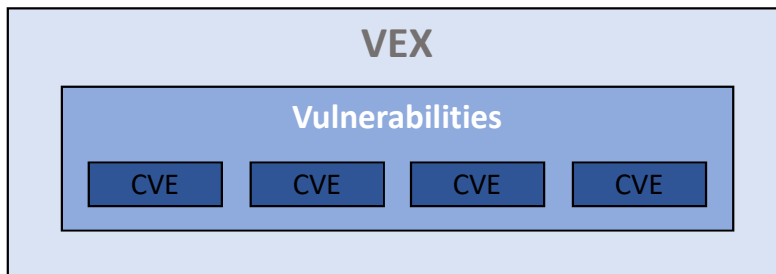


Standards

- SPDX
- CycloneDX
- ~~SWID~~

Formats

- JSON
- RDF
- Tag Value
- XML

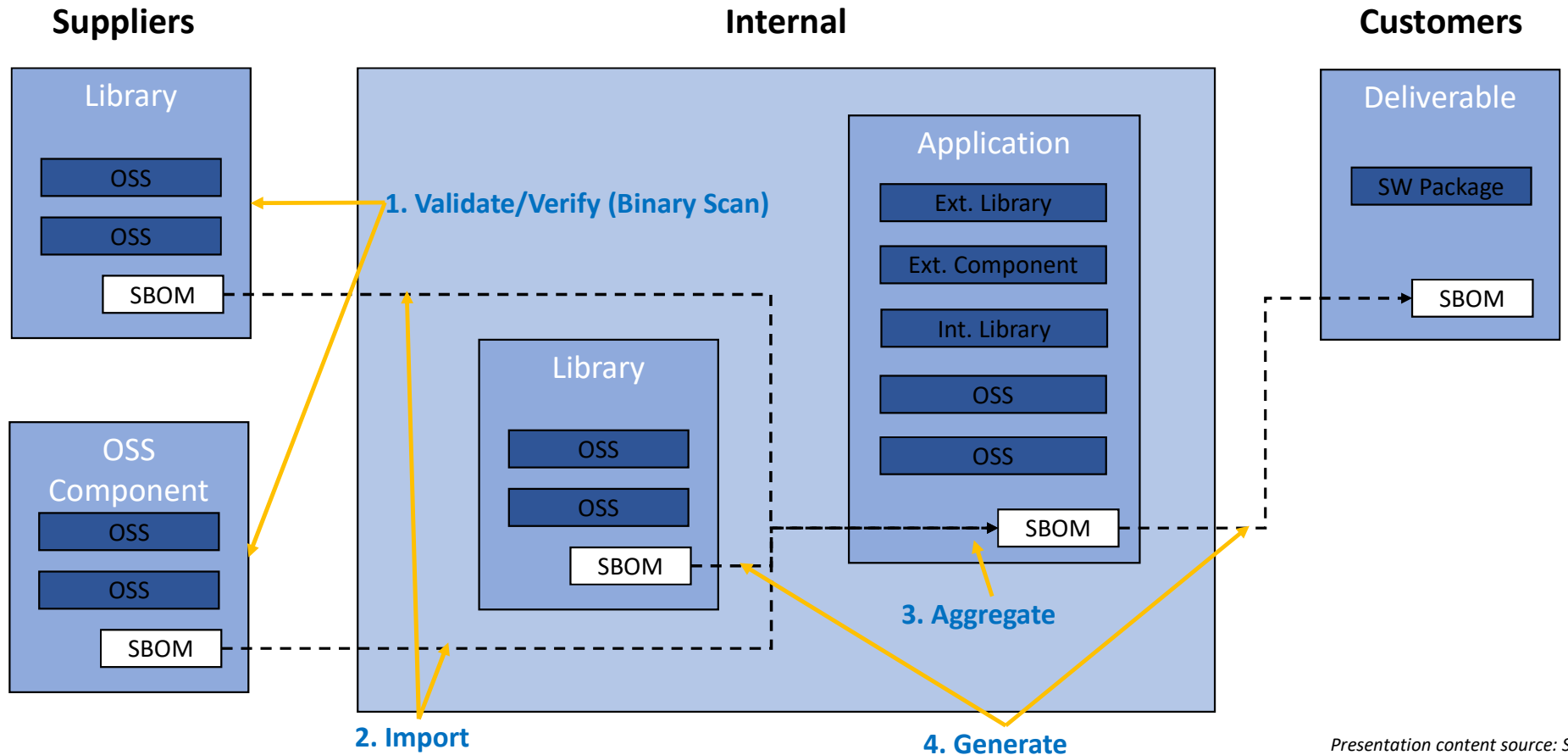


Vulnerability Exchange (VEX)

- Supported in CycloneDX 1.4
 - (Not compliant with NTIA?)
- Not Yet Supported in SPDX

Presentation content source: Synopsys

SBOM WORKFLOW



Presentation content source: Synopsys

SBOM GAPS

- Developing Standard: Stream of New Requirements
- Multiple Standards
 - CycloneDX, SPDX, SWID
- Inconsistent Aggregation
 - Package
 - Component
 - Subcomponent
 - File
 - Artifact
- Inconsistent Package Identification
 - CPE: Common Platform Enumeration
 - PURL: Package URL

CPE

Wildcards

```
cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:  
<update>:<edition>:<language>:<sw_edition>:<target_sw>:  
<target_hw>:<other>
```

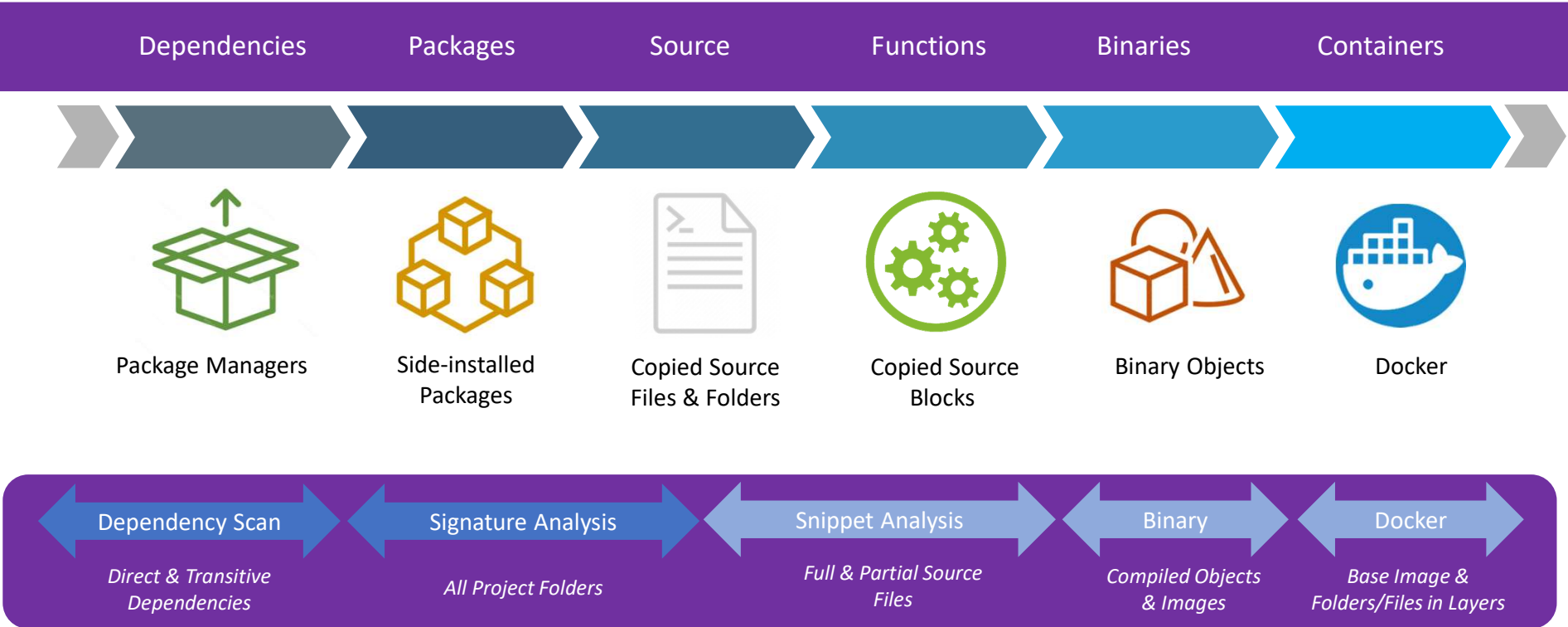
PURL

Origin Specific - Inconsistent

```
• gem:jruby-launcher@1.1.2?platform=java  
• github:package-url/purl-spec@244fd47e07d1004f0aed9c  
• golang:google.golang.org/genproto#googleapis/api/annotations  
• maven:org.apache.xmlgraphics/batik-anim@1.9.1?repository_url=repo.spring.io
```

SBOM CHALLENGES ACCURATE IDENTIFICATION AND VALIDATION WITH BLACKDUCK

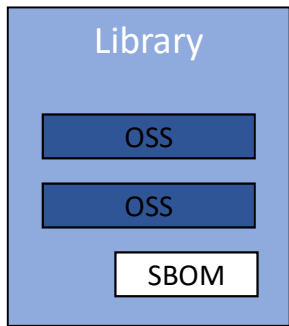
IDENTIFYING OSS AND THIRD-PARTY SOFTWARE



Presentation content source: Synopsys

VALIDATION

Suppliers



SBOM

- Apache Commons Lang 3.6
- Apache Commons Logging 1.2
- Apache HttpClient 4.4.1
- Apache HttpComponents Core 4.4.5
- Apache Neethi 3.0.3
- Apache POI 3.16

Binary Scan

- Apache Commons Lang 3.6
- Apache Commons Logging 1.2
- Apache HttpClient 4.4.1
- Apache HttpComponents Core 4.4.5
- Apache Log4j 1.2.15
- Apache Log4j API 2.9.1
- Apache Neethi 3.0.3
- Apache POI 3.16

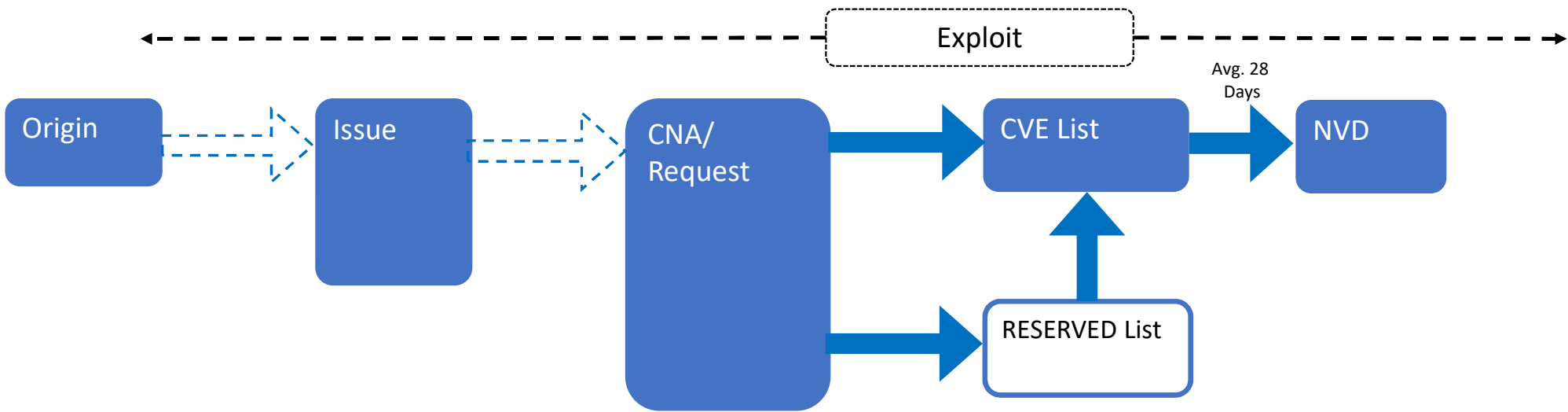


>	BDSA	BDSA-2019-4008 (CVE-2019-17571)	9	Critical
		Zero-click RCE		
>	BDSA	BDSA-2021-4371 (CVE-2020-9493)	8.5	High
		Zero-click RCE		
>	BDSA	BDSA-2022-0118 (CVE-2022-23307)	8.5	High
		Zero-click RCE		
>	NVD	CVE-2023-26464	7.5	High
>	BDSA	BDSA-2021-3764 (CVE-2021-4104)	7.4	High
		Zero-click RCE		
>	BDSA	BDSA-2022-0117 (CVE-2022-23302)	7.1	High
		Zero-click RCE		
>	BDSA	BDSA-2022-0119 (CVE-2022-23305)	6.7	Medium
>	BDSA	BDSA-2020-1398	4.6	Medium

Presentation content source: Synopsys

SBOM CHALLENGES PRECISE VULNERABILITY GUIDANCE WITH BLACKDUCK

PUBLIC SECURITY WORKFLOW



Presentation content source: Synopsys

PUBLIC SECURITY WORKFLOW

4 YEARS

Vulnerabilities go undetected before being identified

4.4 WEEKS

for the community to code and release a fix after a vulnerability is identified

10 WEEKS

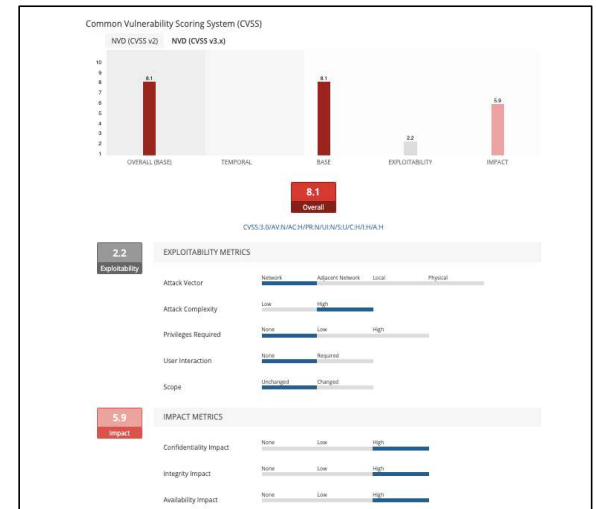
to alert the community on the availability of a security update

SLOW!

INCOMPLETE

POOR REVIEW

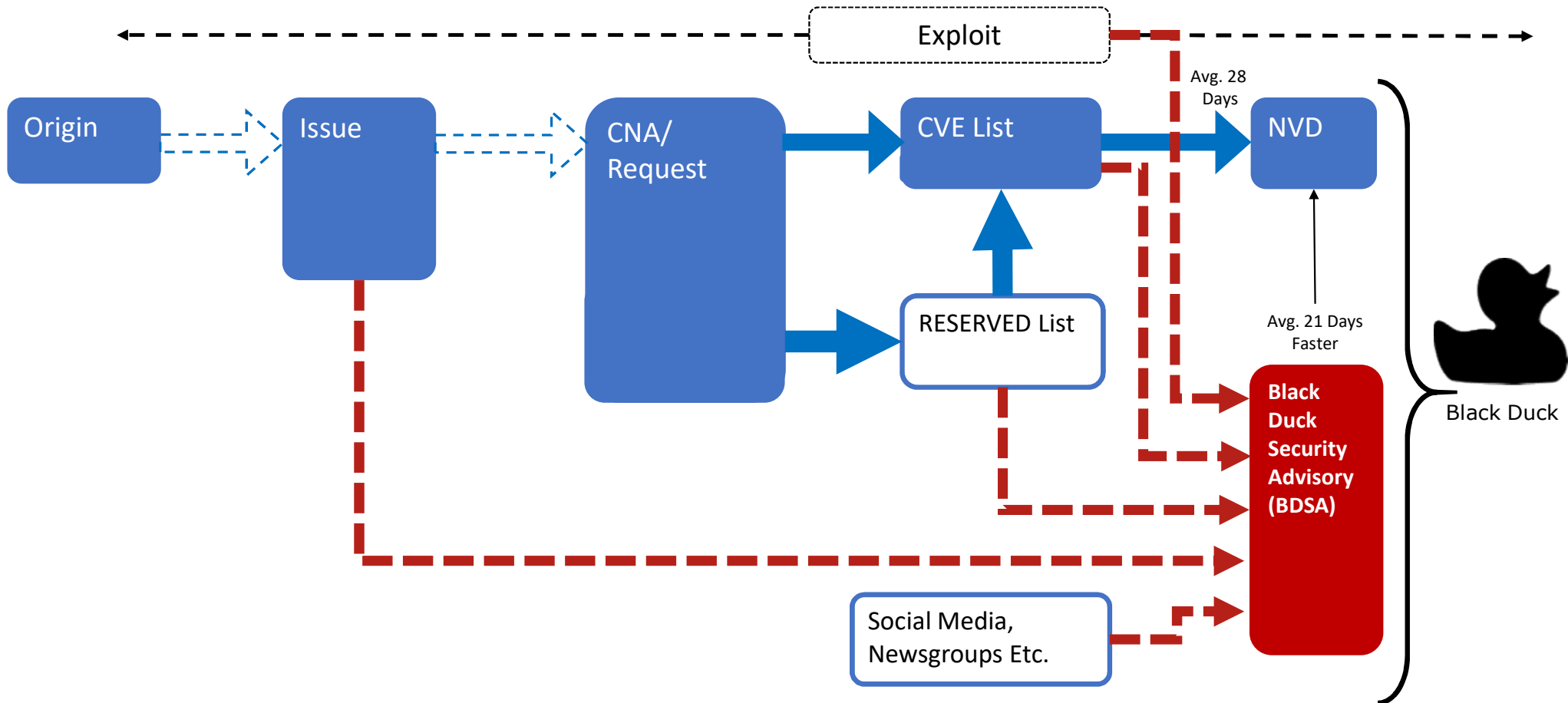
NO GUIDANCE



CVE-ID	
CVE-2019-0232	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
<p>When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulfstange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/).</p>	

Presentation content source: Synopsys

ENHANCED SECURITY WORKFLOW WITH BLACKDUCK



Presentation content source: Synopsis

SCA & SBOM – SUMMARY



Multi-Factor Scanning

Source, Dependencies, Binaries, Snippets etc.



Advanced Vulnerability Data

Public Data Not Reliable



Scalable, Mature SCA Capabilities

Reduce Rework



SBOM

Does not Replace Full AppSec Process
Developing Standard
Trust but Verify

Presentation content source: Synopsys

BLACK DUCK BY SYNOPSYS

Unparalleled OSS Coverage

Full Multi-Factor Identification

Declared License

Component ^	Source	Match Ty	Usage	License	Security Risk
<input checked="" type="checkbox"/> Adobe Flash Player 11.4.402.265	1 Match	Binary	Dynamically Linked	M Basic Proprietary Commercial License	36 179 18
<input checked="" type="checkbox"/> adobe/XMP-Toolkit-SDK ?	1 Match	Binary	Dynamically Linked	BSD-3-Clause	9 9 4
<input checked="" type="checkbox"/> antlr 2.7.7	3 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	ANTLR-PD	
<input checked="" type="checkbox"/> AOP Alliance (Java/J2EE AOP standard) 1.0	3 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Public Domain	
<input checked="" type="checkbox"/> Apache Bean Validation :: bval-core 1.1.2	1 Match	Exact Directory	Dynamically Linked	Apache-2.0	

Full BOM Curation

SBOM Generation

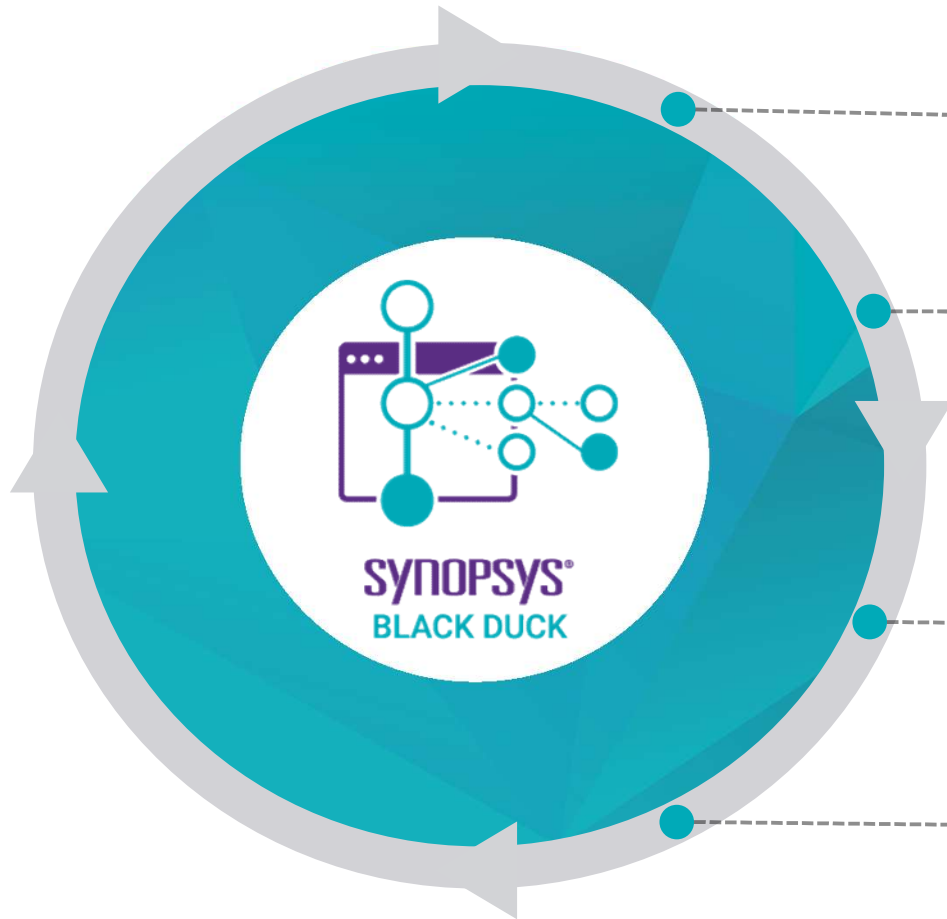
SBOM Import

Deep License

Expert, Private Vulnerability Feed

Presentation content source: Synopsys

BLACK DUCK BY SYNOPSYS



Detect

Identify and track all open source in apps and containers



Protect

Find and fix known open-source vulnerabilities in development and production



Comply

Verify and comply with open-source license terms and conditions

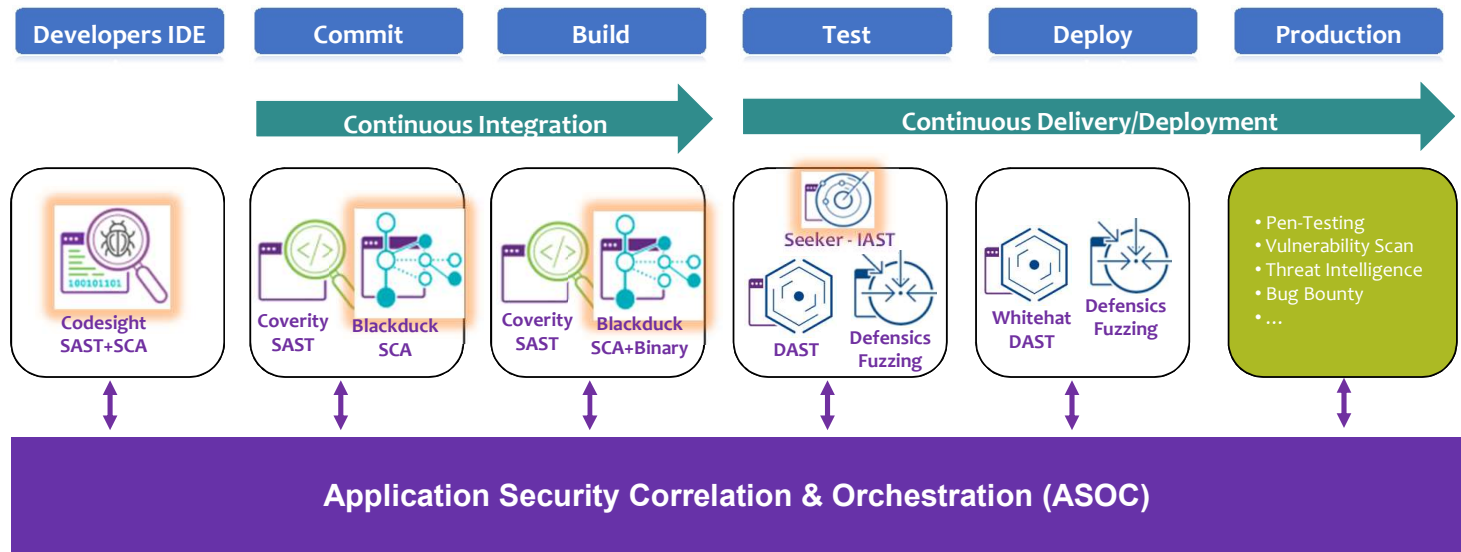


Manage

Integrate and automate open source risk policy enforcement end-to-end

Presentation content source: Synopsys

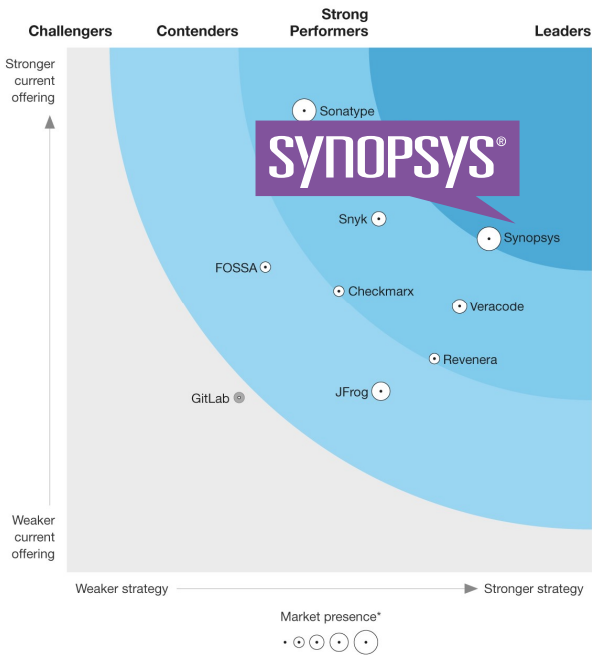
BLACK DUCK IN DEVSECOPS PIPELINE



Presentation content source: Synopsys

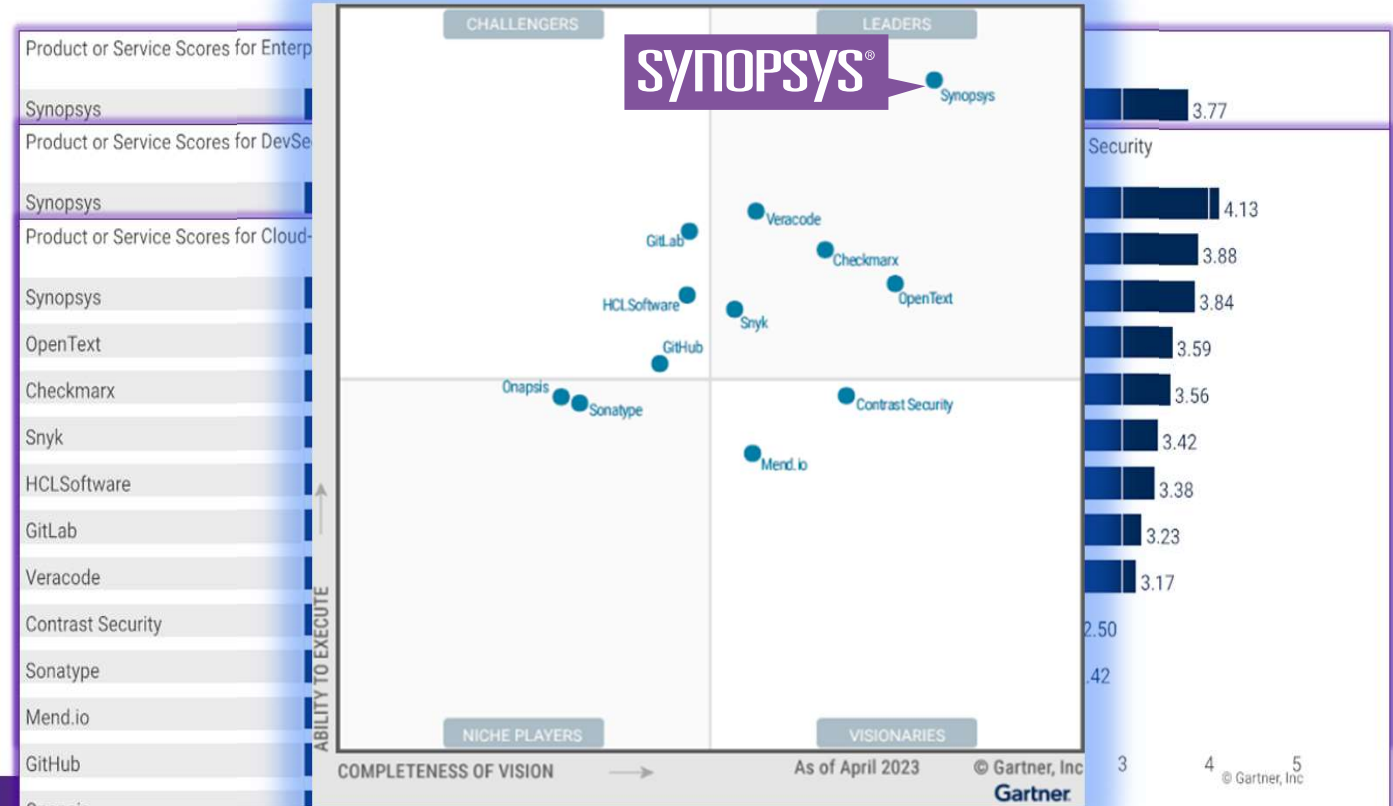
BLACK DUCK BY SYNOPSYS

THE FORRESTER WAVE™
Software Composition Analysis
Q3 2021



*A gray bubble or open dot indicates a nonparticipating vendor.

161636 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.



Presentation content source: Synopsys

WITH SYNOPSYS, YOU CAN...



Build a holistic AppSec program

- Align people, processes, and technology
- Understand your AppSec gaps, risks, and objectives
- Ensure you have the skills and resources to succeed

Secure your software supply chain

- Secure and manage OSS dependencies
- Comprehensively test any type of software
- Identify weaknesses in DevOps infrastructure



Build security into DevOps

- Enable developers to build better software
- Maintain velocity while ensuring security
- Focus teams on the issues that matter most

Presentation content source: Synopsys



Thank you

✉ mi2jsc@mi2.com.vn 🌐 www.mi2.com.vn