WILLKIE

SYNOPSYS®
Silicon to Software™

Open Source Challenges for Clients

…and how to manage

Spencer Simon, Willkie Farr & Gallagher LLP
Phil Odence, Black Duck Audit, General Manager

Jan 2023

Agenda

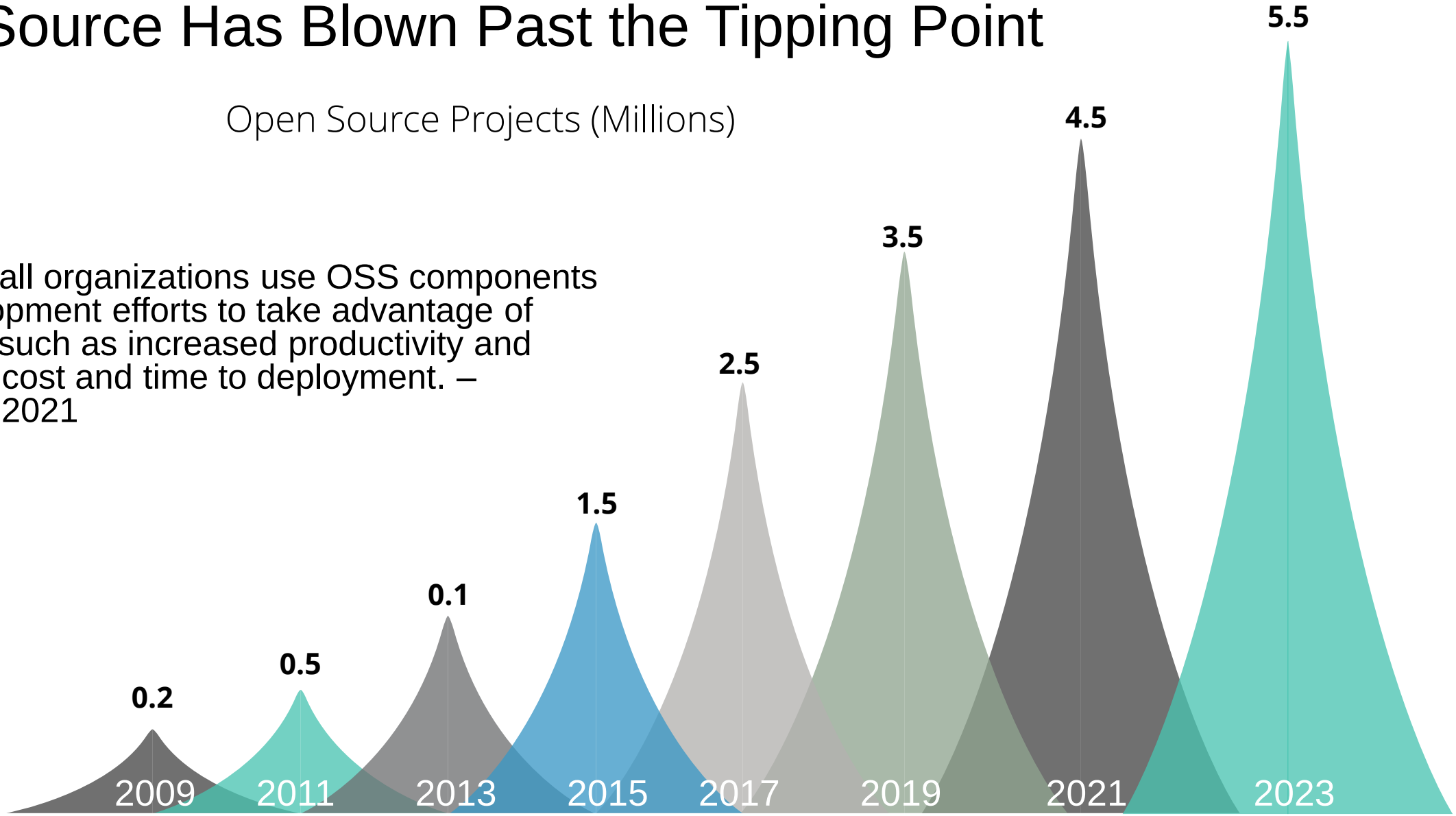
- The Rise and Challenges of Open Source
- What is Open Source Code
- Risks of Using Open Source Code
- Helping Clients Manage / Working with Synopsys
- Q&A

The Rise and Challenges of Open Source

The good news and the (not so) bad news

Open Source Has Blown Past the Tipping Point

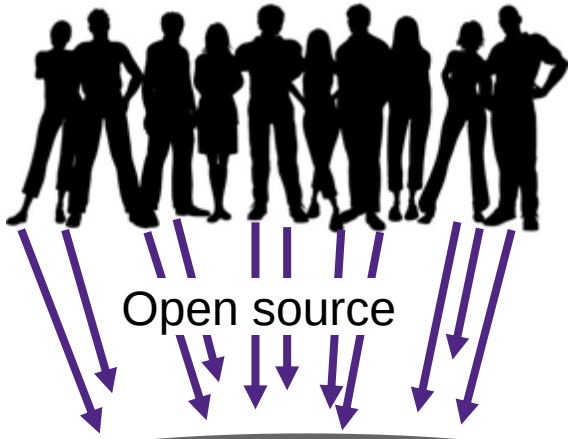
- Virtually all organizations use OSS components in development efforts to take advantage of benefits such as increased productivity and reduced cost and time to deployment. – Gartner, 2021



Source: Black Duck KnowledgeBase

So open source is often unchecked, resulting in risks

"OSS brings a variety of risks, including the long-term viability of projects, security vulnerabilities and unfavorable license terms
-Gartner, 2021



Commercial third-party code

Purchasing
- Licensing?
- Security?
- Quality?
- Support?

Codebase

Management visibility—not!

SECURITY RISK
Which components have vulnerabilities, and what are they?

LEGAL RISK
Which licenses are used, and do they match anticipated use of the code?

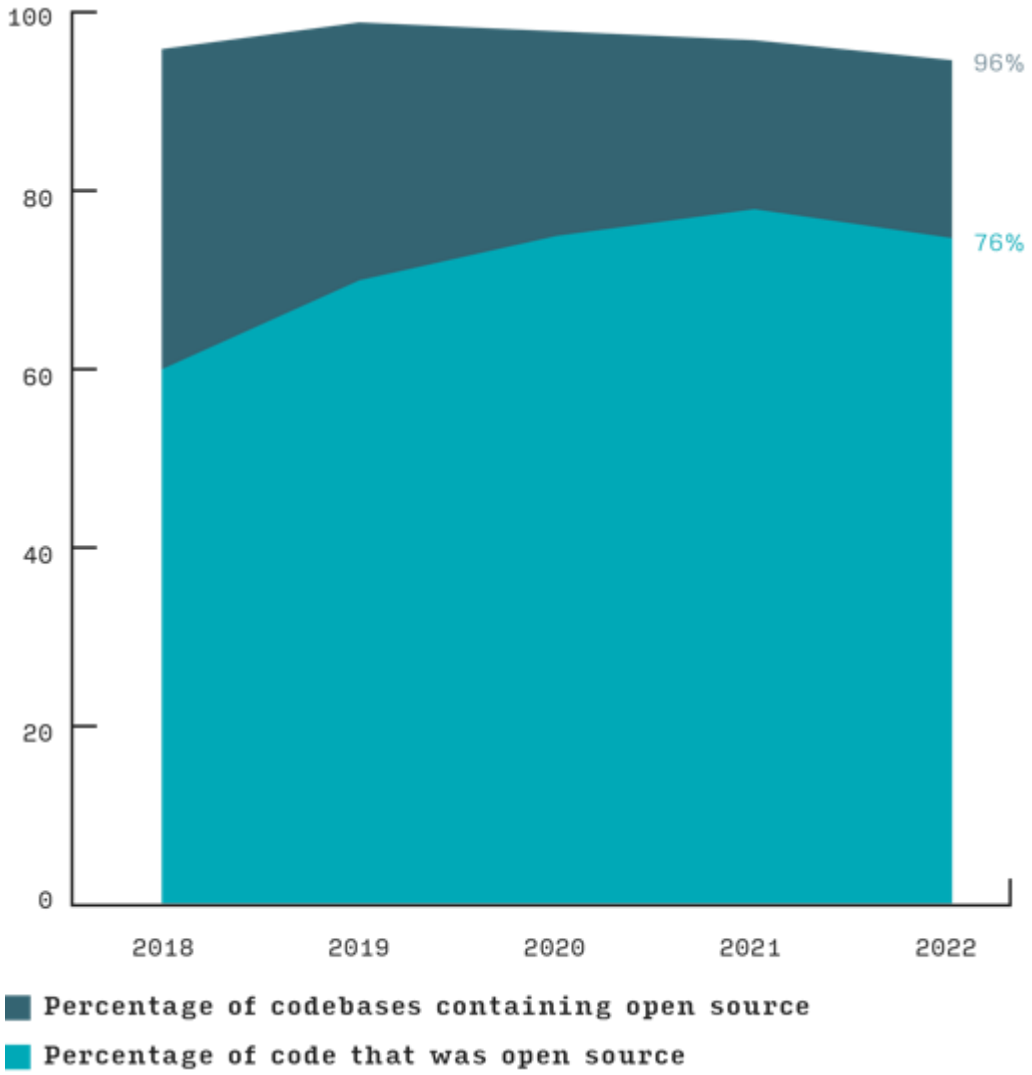
OPERATIONAL FACTORS
Which versions of code are being used, and how old are they (dead projects)?

Open Source Security and Risk Assessment

Quantifying usage and the risks

- Eighth Edition
- With Synopsys CyRC (Cybersecurity Research Center)
- Software of
  - Tech companies
  - Vast majority M&A-related
- 100s of transactions; 1000s of “code bases”
- Data anonymized and aggregated

Audited tech companies rely heavily on open source



Lots of components to manage

595

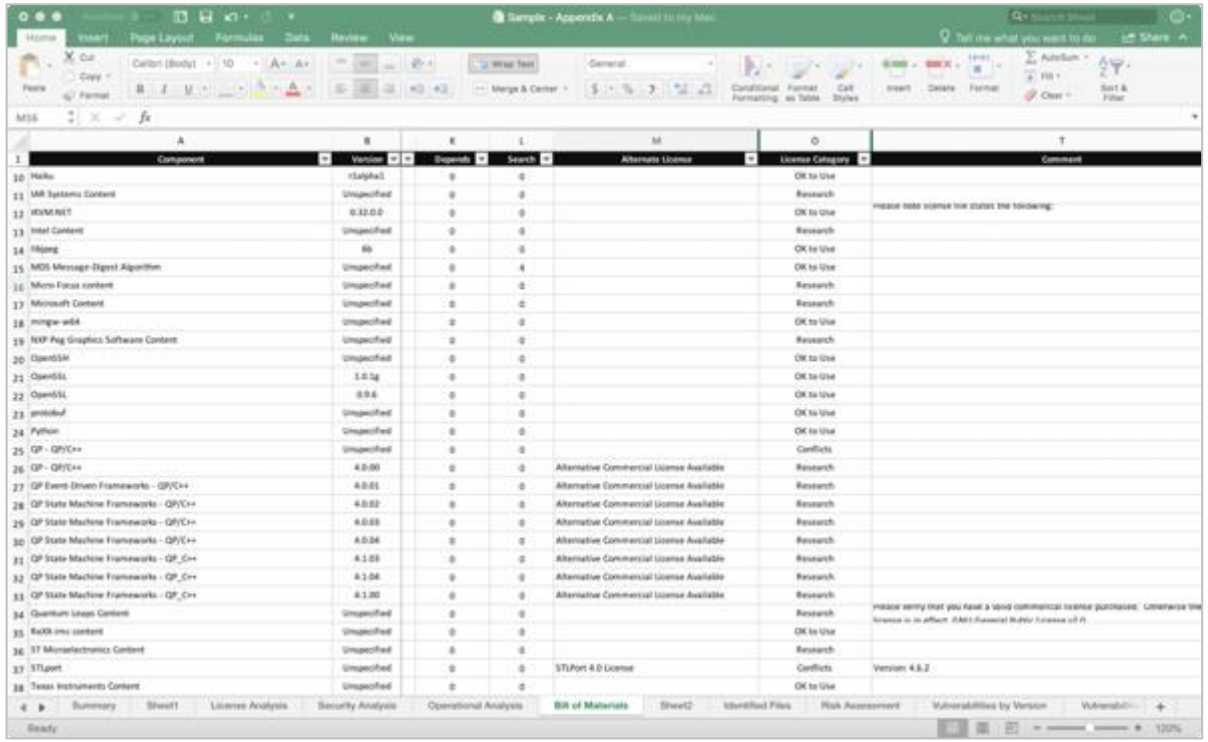
Components per application

1906

Components per transaction

…and companies rarely know how much…

- Few targets are able to easily produce a list with any confidence
- When they do, it tends to be ~50% accurate
  - Sometimes vague
  - High-level
  - Incomplete

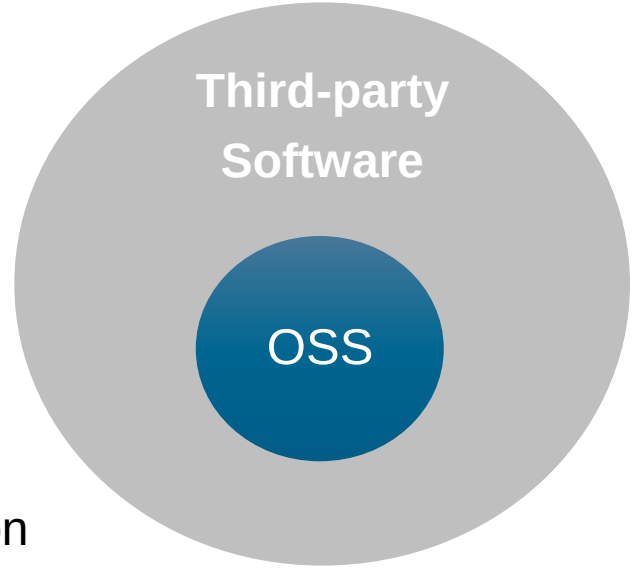


What is Open Source?

A license type and but not just

What is OSS?

- Third party code available as source code on the Internet offered to all on standard terms
- “OSS” is software licensed under an “open source license”
  - Source available, free distribution, derivative works
- Licenses support a collaborative development methodology
- Two main types of licenses:
  - Permissive/Attribution-style – Very developer friendly; just maintain attribution
  - Copyleft/Viral/Reciprocal – Can compromise proprietary intellectual property

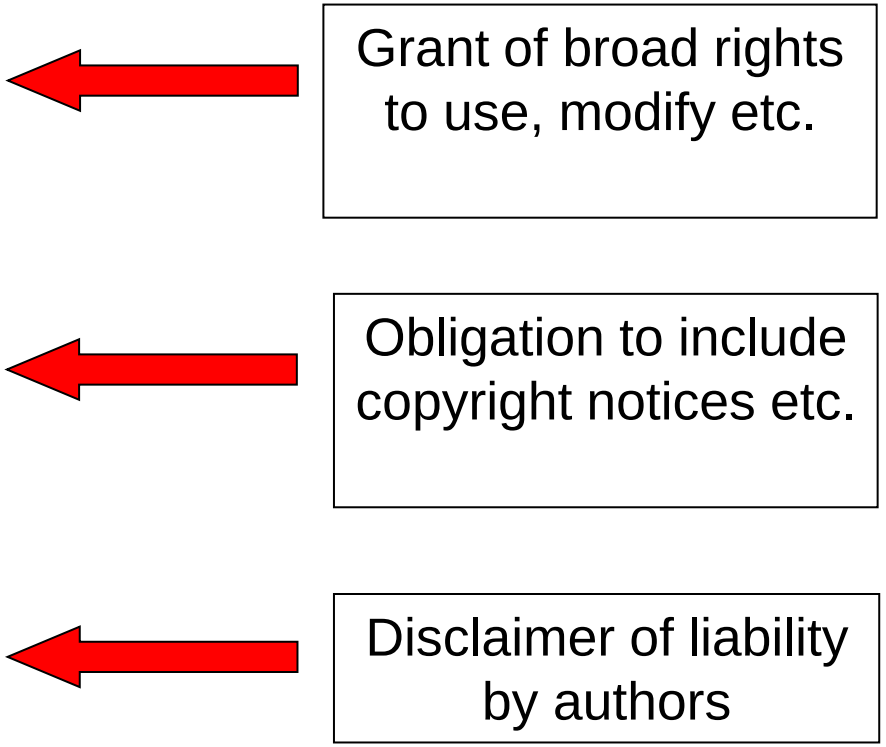


Permissive License Example: The MIT License

Permission is hereby granted, free of charge, to any person obtaining a copy of this 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

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 … IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY … ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE



Note: License terms have been edited for these purposes

GPL Provisions

GPL v.2
(Section 2. b.)

You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties ***under the terms of this license****.*

GPL v.2
(Section 3)

You may copy and distribute the Program (or a work based on it) in object code or executable form … provided that you also do one of the following:

- *accompany it with the complete corresponding machine-readable source code … on a medium customarily used for software interchange; or,*
- *accompany it with a written offer … to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code.*

Increase in SaaS accounts for some of license risk trend

Top 20 Open Source Licenses

Ranked according to number of open source projects using the license:

- Top 10 licenses account for 93%, same as in 2013
- Top 20 licenses account for 97%, same as in 2013
- GPL family of licenses account for 32%, down from 53%
- Apache+BSD+MIT licenses account for 52%, up from 31%

	Open Source License	%
1.	MIT License	32%
2.	GNU General Public License (GPL 2.0)	18%
3.	Apache License 2.0	14%
4.	GNU General Public License (GNU) 3.0	7%
5.	BSD License 2.0 (3-clause, New or Revised) License	6%
6.	ISC License	5%
7.	Artistic License (Perl)	4%
8.	GNU Lesser General Public License (LGPL) 2.1	4%
9.	GNU Lesser General Public License (LGPL) 3.0	2%
10.	Eclipse Public License (EPL)	1%
11.	Microsoft Public License	1%
12.	Simplified BSD License (BSD)	1%
13.	Code Project Open License 1.02	1%
14.	Mozilla Public License (MPL) 1.1	< 1%
15.	GNU Affero General Public License v3 or later	< 1%
16.	Common Development and Distribution License	< 1%
17.	DO WHAT THE F**K YOU WANT TO PUBLIC LIC.	< 1%
18.	Microsoft Reciprocal License	< 1%
19.	Sun GPL with Classpath Exception v2.0	< 1%
20.	zlib/libpng License	< 1%

Source: Black Duck KnowledgeBase

Many unknown and fringe licenses (>2500)

- Beer-ware
- Fender Stratocaster
- WTFPL
- Chicken Dance
- JSON

JSON: The subtlety of a custom license

Copyright (c) 2002 JSON.org

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 shall be used for Good, not Evil.

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.

Software Licensing Violations: Shift from Non-profit to B2B

Software Freedom Law Center

- Cisco
- Verizon
- Monsoon Multimedia
- Xterasys
- High-Gain Antennas
- Bell Microproducts
- Super Micro Computer
- Westinghouse Digital

gpl-violations.org

- Sitecom
- Fortinet
- Motorola
- Acer
- Skype
- D-Link
- BT
- Fantec

Businesses

- Jacobsen v Katzer
- ASUS PC laptop
- Diebold
- Oracle v Google
- Twin Peaks v Red Hat
- Versata/Ameriprise/XimpleWare
- Hellwig v. Vmware
- McHardy v. everyone
- Wix and Wordpress
- Artifex v. Hancom
- Co-Kinetic Systems v. Panasonic Avionics
- Software Freedom Conservancy v. Vizio
- Hermes Center v. ANAC
- Class action v. Msft, Github, OpenAI (Copilot)

Infringement

Valuation

Negative publicity

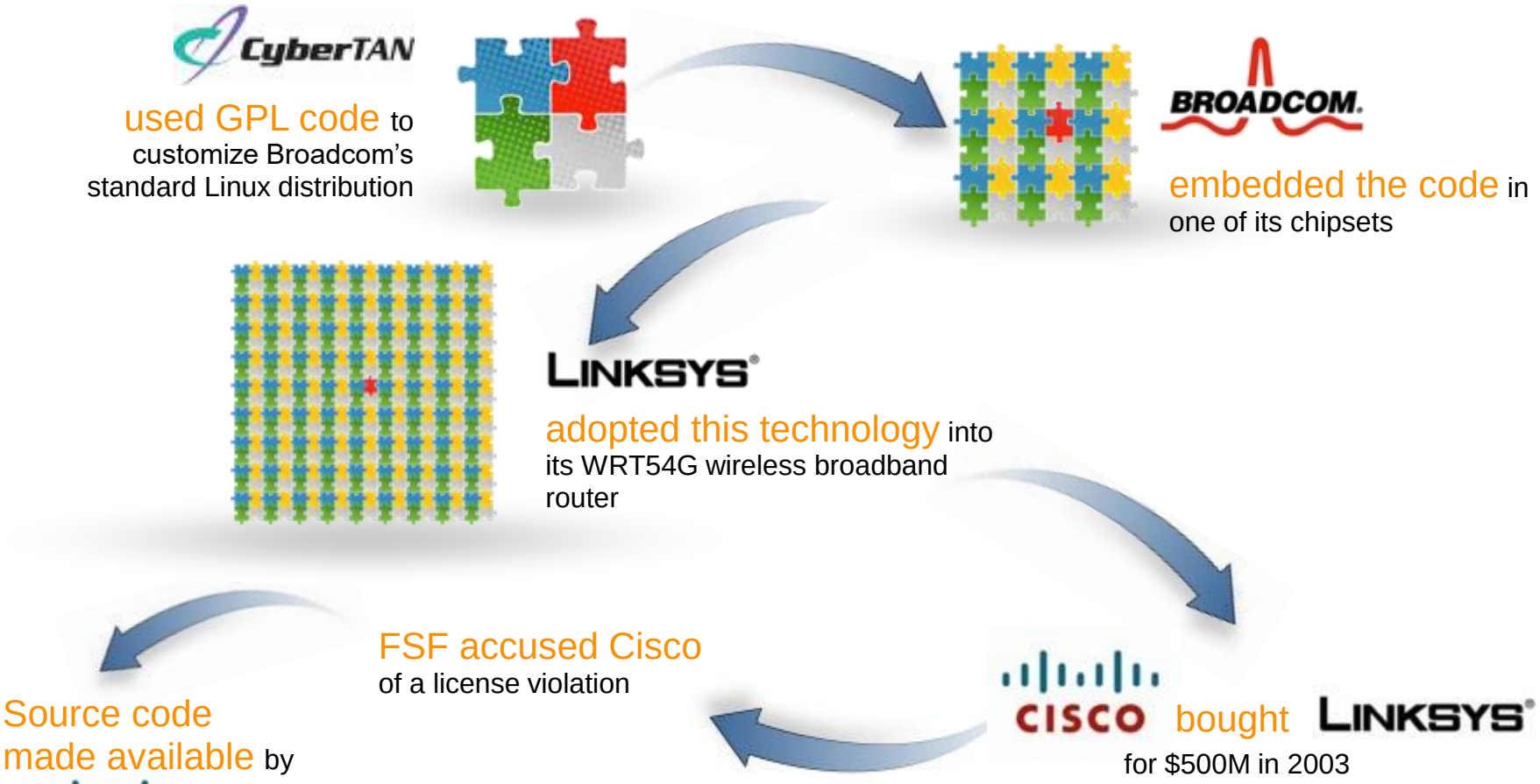
Revenue Loss / Injunctions

Support costs

Who is Next?

Risks and Open Source

Even the Best of Companies…original M&A wake up call

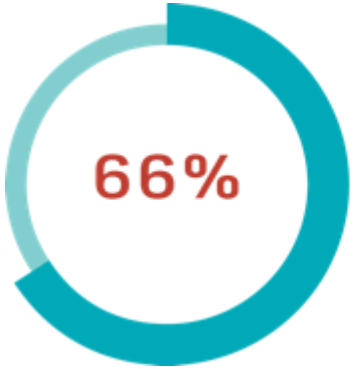


The story continues...

Developers modified firmware turning a low-end ($60) device into a high-function router

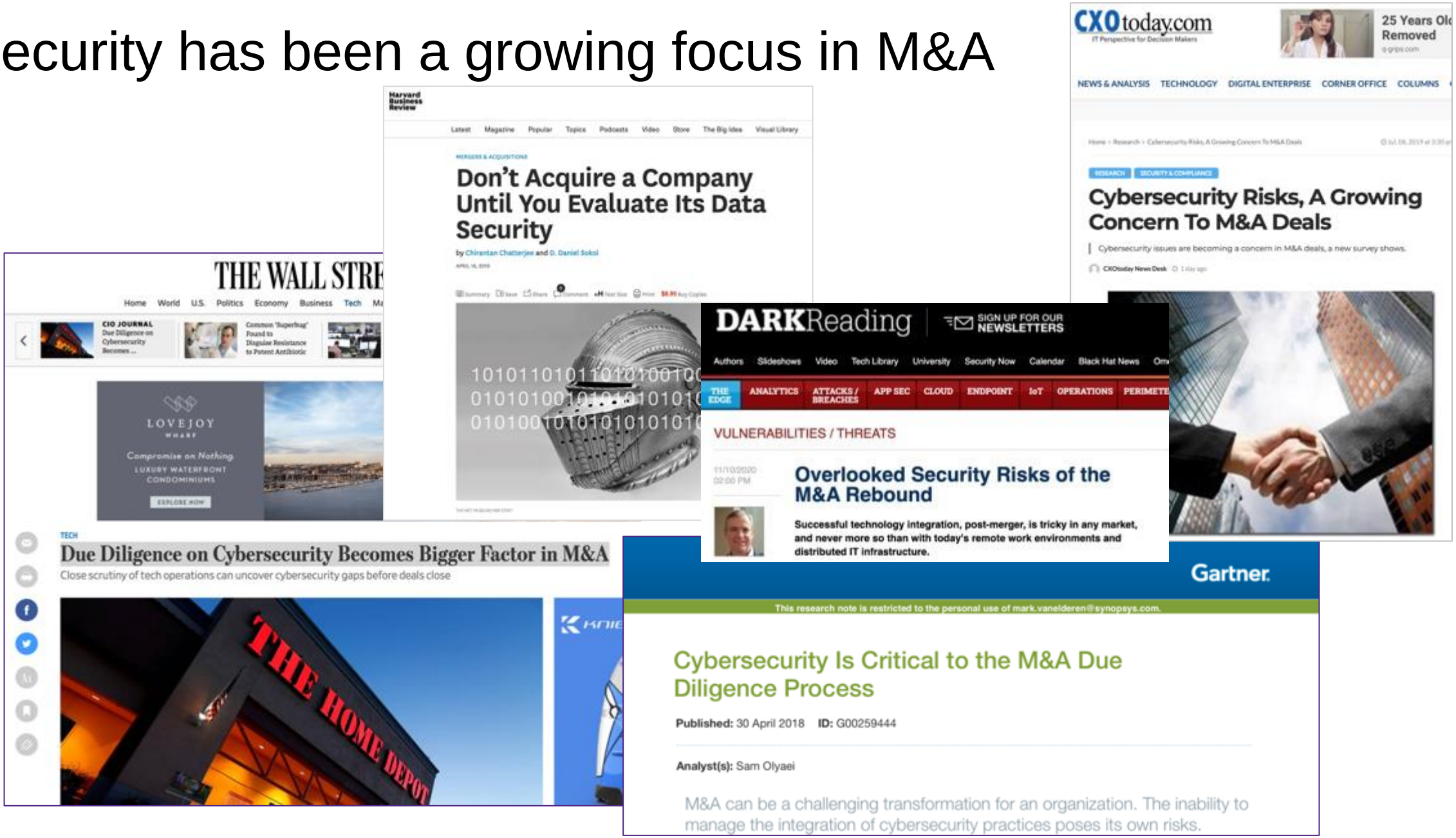
License Issue Frequency

of transactions had license conflicts



of transactions contained open source with no license or a custom license

Security has been a growing focus in M&A



High profile vulnerabilities focus attention on open source security

Over 5000 new vulnerabilities discovered in open source components each year.

OpenSSL Ships Patch for High-Severity Flaws

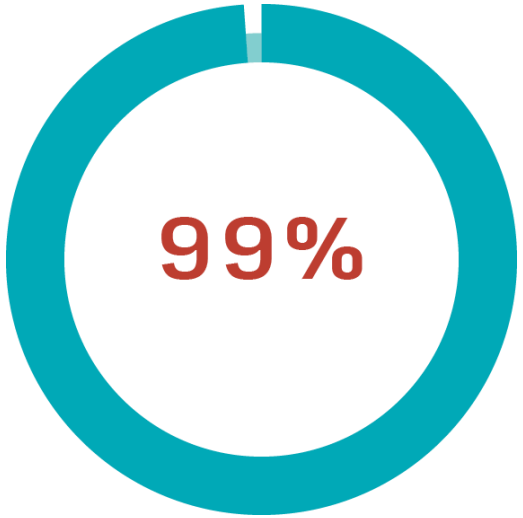
The most serious of the vulnerabilities may allow an attacker to read memory contents or launch denial-of-service exp

By Ryan Naraine
February 7, 2023

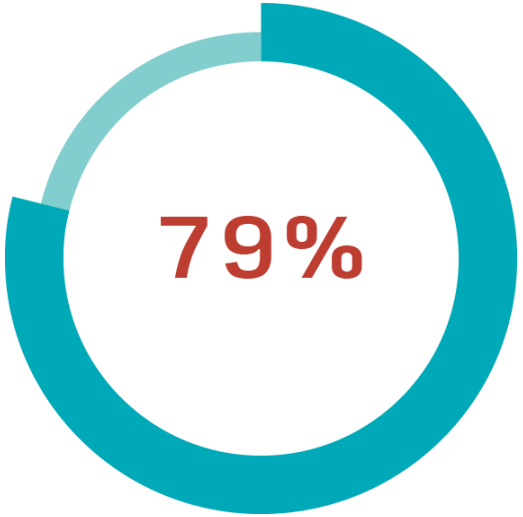
The Cybersecurity 202 • Analysis

Cyber world is starting 2022 in crisis mode with the log4j bug

Frequency of Vulnerabilities



of transactions involve code with at least one vulnerability



of transactions involve code with high-risk vulnerabilities

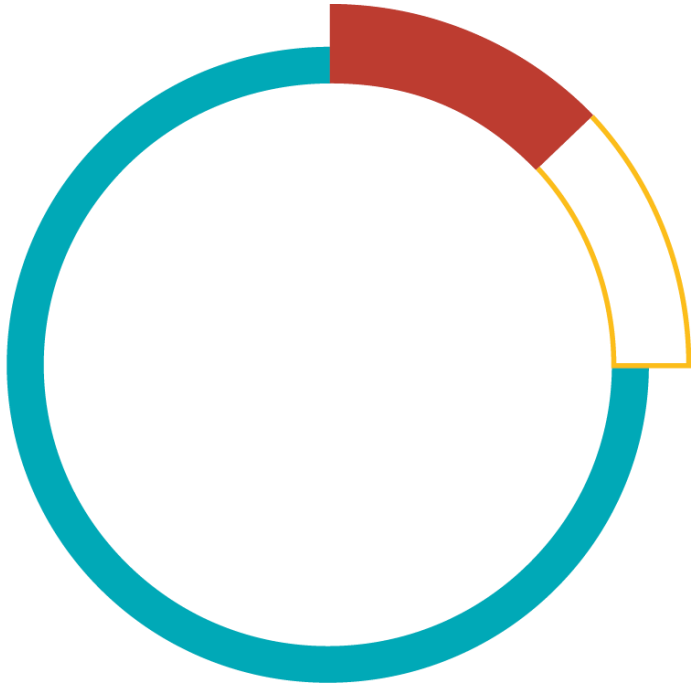
Extent of Vulnerabilities

483

Vulnerabilities per transaction

2022 started with Log4j

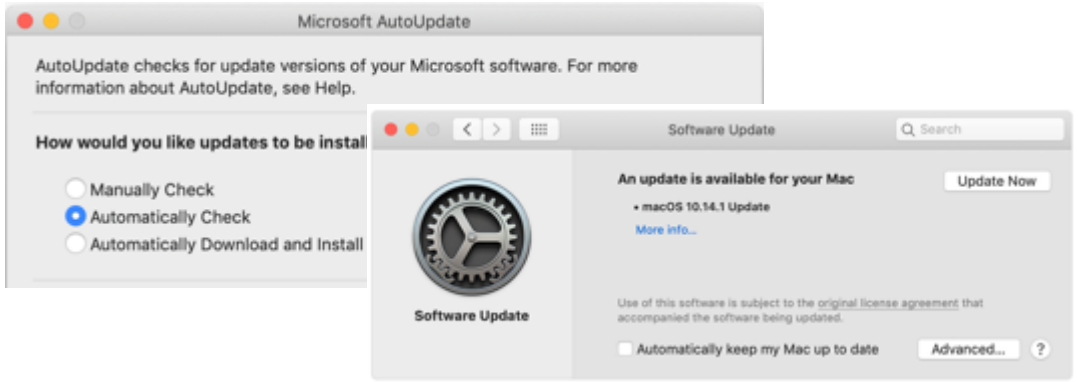
568 transactions included Java language codebases. **13%** contained a vulnerable Log4J component, down from **25%** last year.



Who’s responsible for open source maintenance?

Commercial Code - Push

- Dedicated security researchers
- Alerting and notification infrastructure
- Regular patch updates
- Dedicated support team with SLA



Open Source Code - Pull

- Community based code analysis
- Monitor newsfeeds yourself
- No standard patching mechanism
- Ultimately, you’re responsible

[MediaWiki-announce] MediaWiki Maintenance Releases: 1.26.2, 1.25.5, 1.24.6 and 1.23.13

Chad innocentkiller at gmail.com
Mon Dec 21 20:37:34 UTC 2015

- Previous message: [MediaWiki-announce] Security Release: 1.26.1, 1.25.4, 1.24.5 and 1.23.12
- **Messages sorted by:** [date] [thread] [subject] [author]

We would like to announce the release of MediaWiki 1.26.2, 1.25.5, 1.24.6, and 1.23.13.

These are maintenance releases to fix regressions introduced in the previous release.

Download links are given at the end of this email.

== Maintenance fixes ==
(T121892) Various special pages resulted in fatal errors.

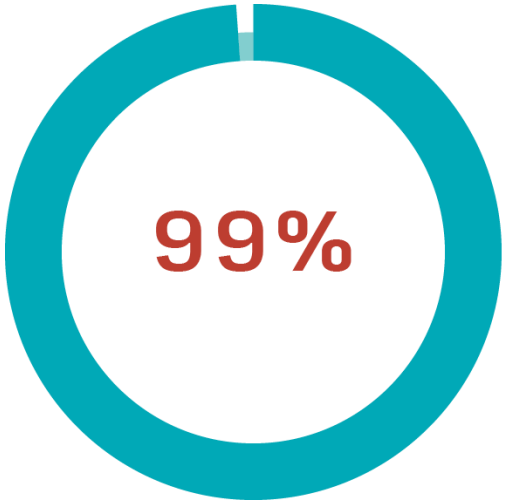
== Note about EOL of 1.24.x ==

Please note that 1.24.6 marks the end of support for the 1.24.x series of releases. Technically this ended a few weeks ago with the release of 1.26.0.

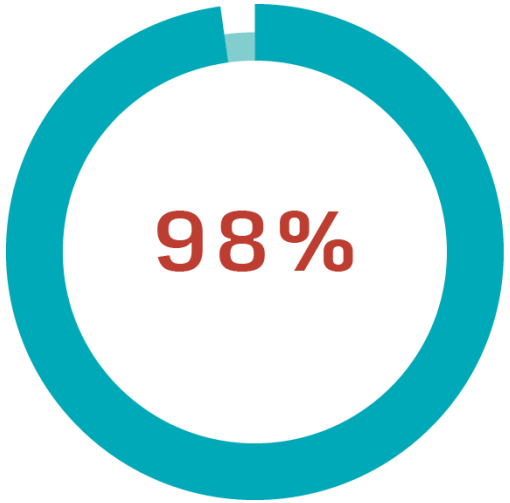
However, 1.24.5 had issues (along with other versions), so it was thought fair
to fix them.

Operational factors to consider

Maintenance tends to be weak



of transactions contained components that had no new development in the past two years



of transactions contained open source more than four years out-of-date

Manage, Don’t Fear

Helping clients manage

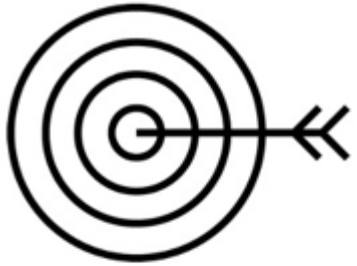
- Code analysis
- Internal
- M&A

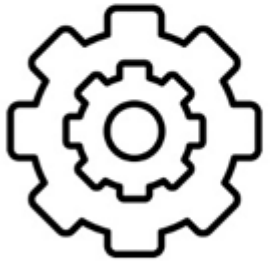
Using OSS is Not a Free Lunch…

…internal governance maximizes OSS benefits while managing the risks

Requirements for World-Class OSS Management

- Strategy
  - The business objectives for use of OSS
- Policy
  - Usage rules
- Process
  - How managed
- Technology
  - Automated governance and compliance





To manage OSS risks, clients need an end-to-end approach

DETECT

Inventory & track all open source components in your code

PROTECT

Identify & remediate known open source vulnerabilities & license issues before you ship

MANAGE

Set, verify, & enforce open source security and use policies across supply chain

MONITOR

Actively monitor & fix new vulnerabilities that impact deployed software

Integrate & automate with your DevOps tools and processes

Supply Chain / SBOMs are re-raising the issue

- Another use case for audits

- Recent SBOM interest is driven by security concerns
  - NTIA, now CISA
  - Executive Order

- Consumers need to understand what's in the code
  - SBOMs are great for sharing
  - Credibility of data also an issue
  - 3rd party audits from trusted suppliers can close the gap

Positioning Spectrum of Open Source Analysis

Automated Tool

Human Expert w/tools

Just right for DevOps

Perfect for M&A

Scan (product or MS)

Black Duck Open Source Audit

Why acquirers worry

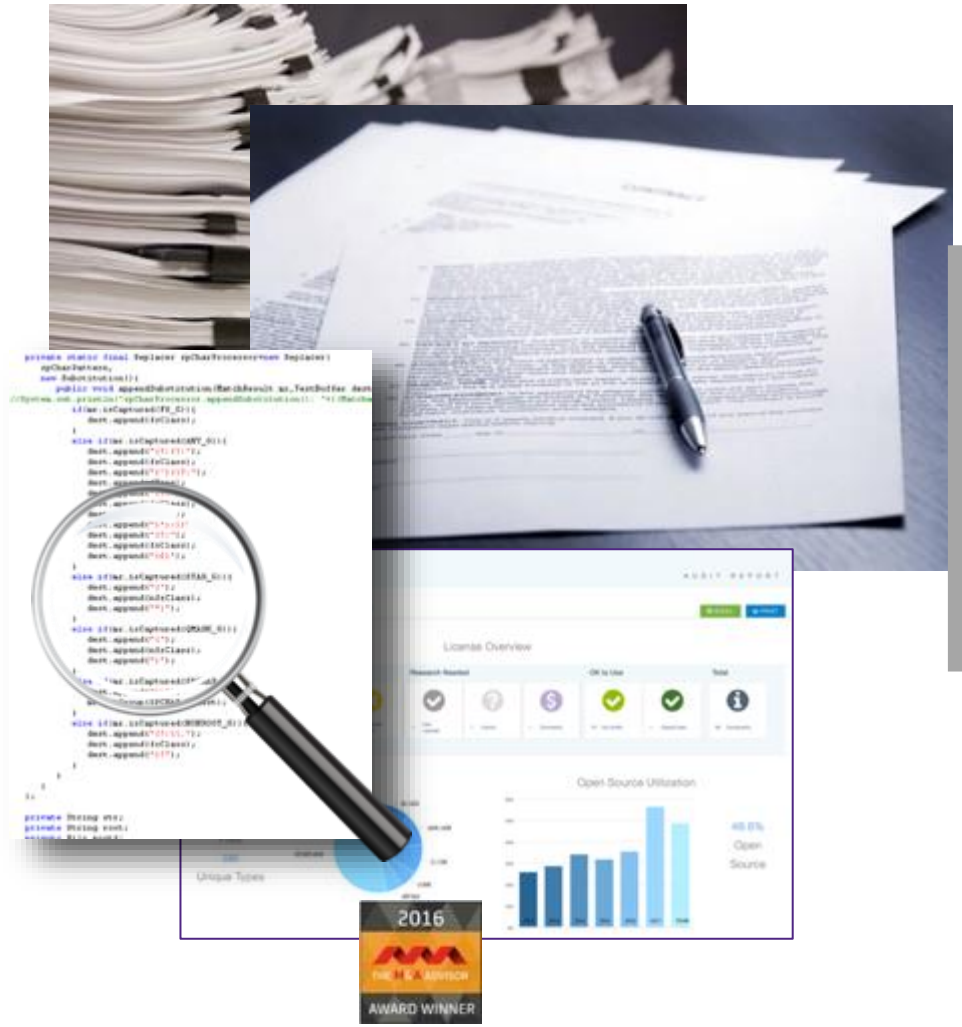
- Unmanaged open source can be risky

  Many open-source assets are either undermanaged or altogether unmanaged once established within an IT portfolio. — Gartner

- M&A considerations
  - Above is especially true for smaller companies
  - Deeper pockets may draw fire
  - Divestment anticipation
  - Business case / Integration planning
- OSS as part of software due diligence has gone from unusual to being the norm in tech deals

Software Due Diligence

Managing Open Source Risks in Tech Deals



OSS DD

Confirmation
Information
”Surprises”

The Deal

Valuation

Terms

Integration &
Remediation Plans

Example Software Reps and Warranties

Seller provided all inbound and outbound licenses

No third-party infringement of Seller IP or of others' IP by Seller

Seller owns all IP Listed in Disclosure Schedules

Sellers: Manage Before the Event

- One year out…
    - Be prepared to provided open source Bill of Materials
    - Work with IP attorney
    - Implement open source strategy, policy, process and tools
    - May be simple depending on organization
- Weeks/months out
    - Organize a pre-diligence audit
    - Remediate any issues and rescan
    - Provide report as a sales tool

Remediating Open Source Issues

Remove	A minor feature may not be worth the risk.
Replace	Perhaps with a similar open source or commercial component. For common capabilities, there may be similar components under compatible licenses.
Rewrite	Recreate the functionality with proprietary code.
Renew	Move to an patched version for security vulnerabilities/old components
Relicense	Some copyright holders are willing to license software under different terms, perhaps another open source license or some commercial arrangement.
Respect	As usage matters, there are cases, particularly with medium-risk licenses, that the way the component is used may be easily modified and allow you to respect the terms of the license.

Black Duck Audits for M&A Due Diligence

More than 15 years' experience, thousands of audits

- Hyper-Responsive
- Trusted Reputation
- Expertise/Quality of Work
- World Class Tools

"With the capabilities that Synopsys brings to the table, we are able to consolidate into one vendor which makes it a lot easier for us to manage. Working with Synopsys is easy and they provide results we can trust and rely on."

-Grant Chang, VP of Corp Dev, Point Click Care

Summary

- Developers use open source…for great reason
- There are many paths for unknown components into a code base
- Unmanaged use of open source can be risky
- Any company developing software needs a strategy, policy, processes and tools for consuming open source
- Open source diligence should be part of every tech acquisition

Next Steps

Other free resources for lawyers

- Legal webinar series on Brighttalk
- Open Hub free project directory: **https://www.openhub.net/**
- Blog posts tagged “legal”: **www.synopsys.com/blogs/software-security/category/legal/**
- https://www.synopsys.com/software-integrity/resources/white-papers/legal-resources.html

Register for Next Course

Questions?
Ask the Black Duck Audit team!

Phil Odence, podence@synopsys.com

blackduckaudits@synopsys.com