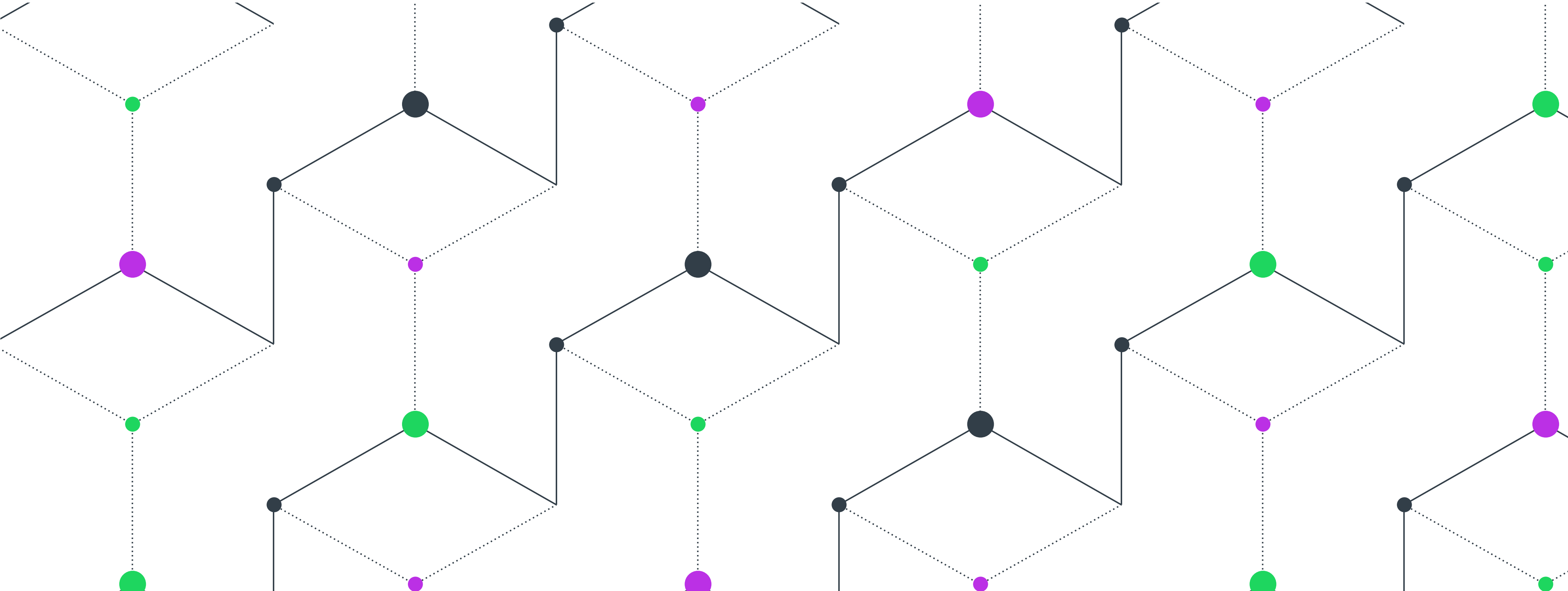
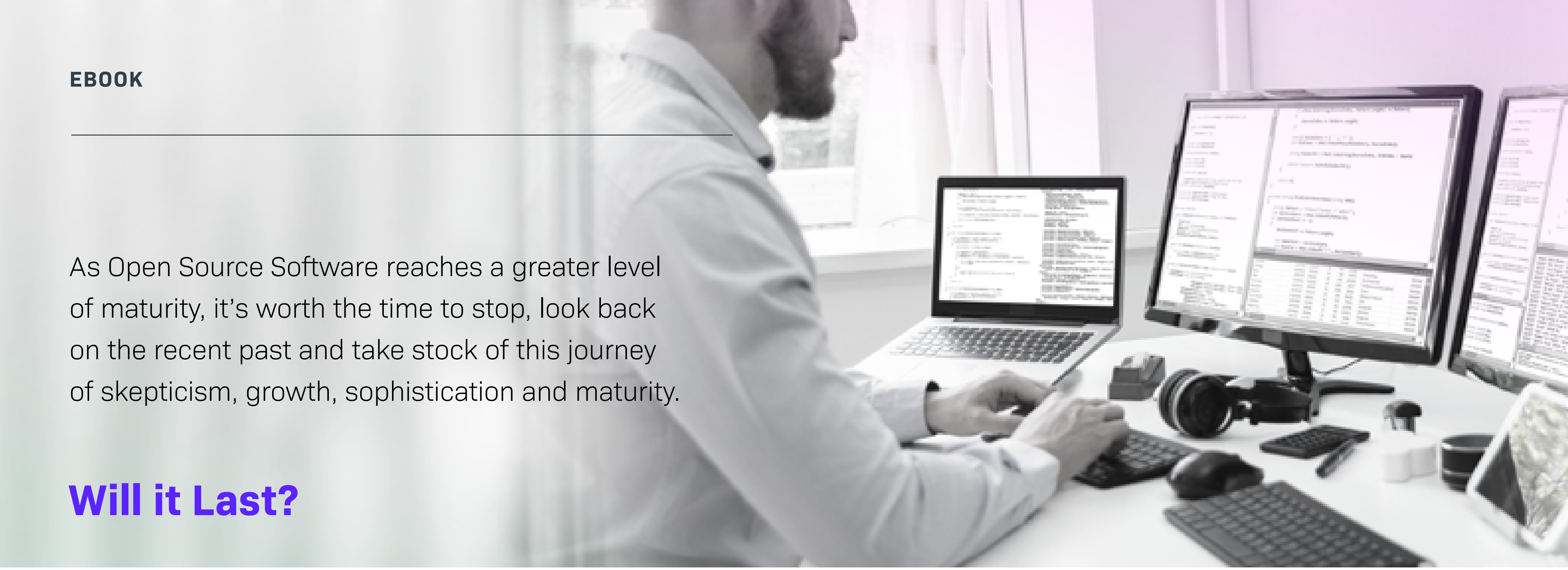
EBOOK

The Maturity of Open Source Software

Trends and Best Next Steps for Software Composition Analysis





As Open Source Software reaches a greater level of maturity, it's worth the time to stop, look back on the recent past and take stock of this journey of skepticism, growth, sophistication and maturity.

Will it Last?

It didn't seem so in the early years of apprehension and doubt. Today, however, open source has reached key milestones:

1

Resilience

The term "open source" has been around for 21 years and counting!

2

Responsibility

With the creation of open source communities the industry promotes collaboration, the enrichment of resources, and provides tools to support license compliance and risk management.

3

Approachability

Open source use continues to deliver on its mission of innovation by helping people work together to leverage existing work, improve it and share it.

4

Growth

Open Source Software is everywhere. It's global, the foundation of the Web and used in all industries. Most companies today use open source internally and in their products.

As open source enters its next step of maturity, what's ahead? Let's take a closer look at its current state and what you need to know to better prepare for open source use, management, and success in the coming future.

Open Source Holds Significant Value for Enterprise Businesses

Heavy Saturation

"Open source software (OSS) industry saturation is complete: today, 95% of mainstream IT organizations leverage nontrivial open-source software assets within their mission-critical IT portfolios—whether they know it or not."

Gartner Hype Cycle for Open-Source Software

When large enterprises embrace Open Source Software, good things can happen and opportunities emerge, especially for building applications on a large scale. Today, those enterprises realize the transformation the industry has gone through and recognize open source as a game changer. Point of proof? 2018 was a year for major acquisitions of open source enterprise players.

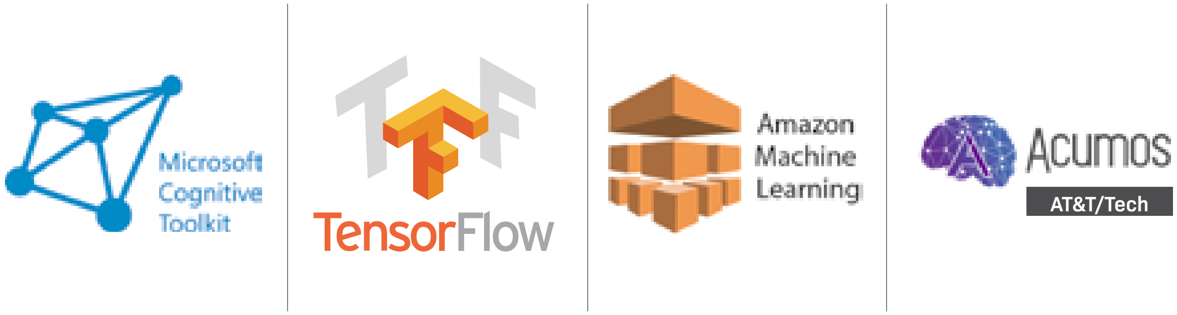
GitHub	Adobe	IBM	salesforce
Microsoft	Magento	redhat	MuleSoft
$7.5B	$1.68B	$34B	$6.5B

Big Tip

Open Source Software is here to stay. Know what your company uses today, plan for positive management, and secure your future.

Growth Continues, Especially with Artificial Intelligence

Artificial Intelligence (AI) and machine learning technologies have tremendous opportunity—going well beyond what was possible over the last decade. Major companies like Google, Microsoft®, and Amazon are embracing open source and making their AI and machine learning systems open source. Why? Because they want to continue to be on the leading edge of technology innovation.



Big Tip

One of the first actions any organization can take is to outline a company policy related to using and managing Open Source Software in applications—both internal and customer facing.

Growing Pains

License Changes for Solution Monetization

Communities that were previously only free and open source are now looking at ways that they can monetize their platforms. Redis, MongoDB and others made license changes to ensure contributions back to the community.

> *"...organizations like Redis, MongoDB, Confluent and others have recently introduced new licenses that make it harder for their competitors to take their products and sell them as rebranded services without contributing back to the community..."*
>
> TECH CRUNCH
>
> **TESTIMONIAL**

License Changes—Easier to Use

Other organizations are recognizing that streamlining licenses offers benefits. OpenSSL, which previously was under two different licenses with different terms of use, is simplifying compliance by switching its platform over to a single license—the Apache 2 license. Additionally, Microsoft announced that its patent portfolio will be based on OSS further demonstrating the acceptance of open source at a enterprise level.

Big Tip

One of the first actions any organization can take is to outline a company policy related to using and managing Open Source Software in applications—both internal and customer facing.

Due Diligence is No Longer Optional

Ten years ago, many companies considered Open Source Software due diligence and management as optional or only a requirement during M&A events. It was only relevant to larger companies. That's no longer the case today. When a startup, for example, goes for another round of funding, they are required to create a highly accurate bill-of-materials regarding all instances of Open Source Software use.

Regular automated scanning and audits of code bases help IT teams—big and small—put proactive protection plans and processes in place to know what's in their code and facilitate the end goal of 100% license compliance and risk management. Many companies are now monitoring open source usage as part of daily operations.

Big Tip

The basics of license compliance management need to be taught at all levels of the organization, not just at the developer level. Senior management must be made aware of license compliance requirements, as well as the need to periodically update products in order to repair vulnerable open source components.

Software is eating the world. Very few acquisitions include no software assets.

Risk is too high to cover potential issues with "reps and warranties."

Due diligence for M&A efforts is key, but start-ups need it for new funding.

More requests for continual scanning with different versions versus one-time scans.

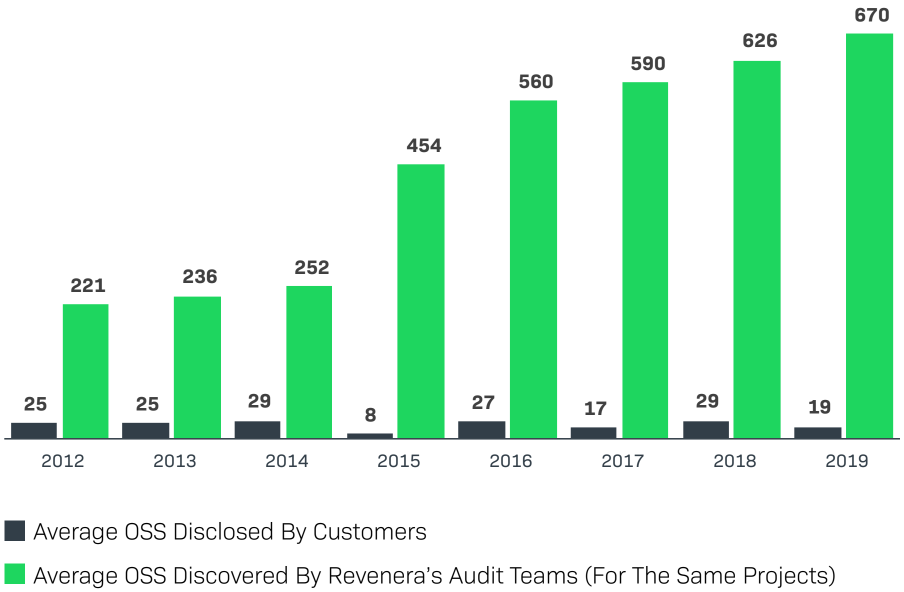
Open source due diligence used to be just about big companies. Now it's start-ups, private equity firms, law firms, etc.

INSIGHT

Companies are Still Underestimating Open Source Software Usage

While some companies attempt to manually monitor what open source is used internally and in products that ship to customers, they often don't know every nook and cranny where open source code can exist. Are you aware, for example, that open source can come into the company through "shadow IT," where someone in the organization manages a IT project or purchases an app without the IT department's knowledge? Third-party software can also include open source code, which would not be known without strict disclosure policies. All this adds up to a significant gap between what companies think they use vs. reality.

The Knowledge Gap – Still Wide



Big Tip

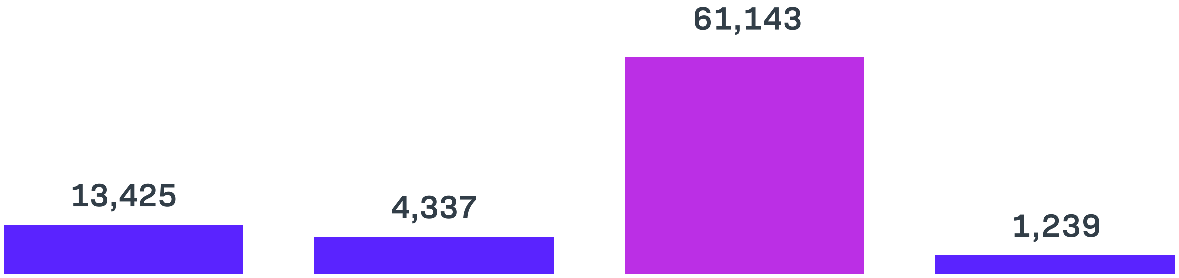
Don't underestimate the open source Bill of Materials (BOM). It's a critical aspect of license compliance and one day you could be asked to provide a complete inventory report of all open source components, including all dependencies and affiliated licenses.

Not All Risks Are Equal

Current data from Revenera customer audits shows that 85 percent of the issues found were identified as a Priority Level 3 (P3). Good news? Depends on how you look at it. While it's true not all license compliance risks related to open source use are equal based on severity, it's also true that what you don't know can hurt you. Data also supports that only 2 percent of issues uncovered during audits were initially disclosed prior to audit start. One unresolved issue is all it takes.

The good news is that the trend is moving in the right direction and the marketplace is becoming more sophisticated. Revenera's data also supports that more requests are being made for varying degrees of analysis versus just baseline audits. There's more understanding that code scanning is an ongoing, incremental process that requires a strategic, collaborative approach.

Revenera Audit Services Data



P1
High severity issues such as strong Copyleft compliance issues involving the APGL and GPL, or other important vulnerabilities.

P2
Secondary priority issues related to commercial and vanity licenses.

P3
Low risk hygiene issues related to permissive license issues such as those under BSD, Apache, and MIT.

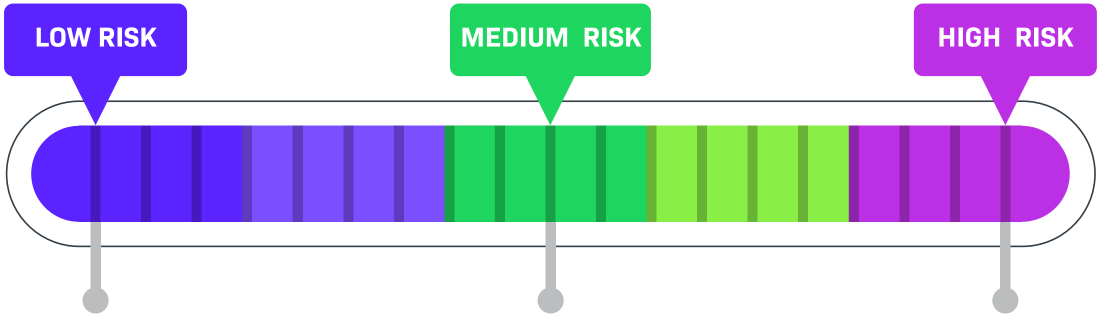
P4
Dual/tri-licensed components with a viral and permissive license option.
For example: jQuery under GPL or MIT.

Big Tip

Not sure where to get started? Engaging with a Software Composition Analysis (SCA) company to perform an independent third-party audit is a great first step to getting you to a compliant and secure state. A SCA audit will identify all major open source and commercial components in your applications.

Varying Levels of Analysis Needed

With the growth in open source use and its market maturity, managing what's used and putting controls in place can seem overwhelming. Some companies are starting to develop a more strategic approach by prioritizing flagship products for scanning, identifying the highest exposure points within the organization, understanding client risks and more. By recognizing what your top needs are, next steps for monitoring can be highly focused for maximum impact.



LOW RISK
Package Analysis
Build Dependencies

MEDIUM RISK
Scan Evidence for
Prioritized Analysis

HIGH RISK
Source Code
Fingerprint Analysis

Big Tip

Plan for a phased approach to getting clean and staying clean.

Actions to Take: A Deep Dive

With open source use comes great responsibility from a variety of stakeholders within the organization. CEOs should align with their CTOs, security officers and engineers to more completely understand their:

- Current state of open source license compliance and security,
- Methods and processes for ongoing monitoring,
- Remediation guidelines, and
- The level of ongoing training and education needed for developers and engineers.

Goal is to always have answers to the following questions:

Who wrote it?

Where is it deployed?

Are there issues with it?

Have the issues been fixed?

DEVELOPERS

- What is being shipped?
- What open source packages are we using?
- Do we have redundant and/or outdated technologies?

LEGAL AND SECURITY

- Which applications contain known vulnerabilities?
- What are the open source disclosures for a product?
- Are we compliant with the open source license obligations?

ENGINEERING MANAGEMENT

- Where are we using open source across the company?
- What is the impact of known vulnerabilities?
- Have scheduled remediation actions been completed?

THIRD PARTIES/SUPPLY CHAIN

- What open source/commercial packages are in these binaries?
- Have known security issues been resolved?
- Is there compliance with all third-party licenses?

Big Tip

Go with the "Rule of Three"— Collaborate, Investigate, and Automate:

COLLABORATE: Form a cross-functional team and put a stake in the ground regarding the importance of establishing open source management policies.

INVESTIGATE: Assess the maturity of your open source analysis capabilities.

AUTOMATE: Engage with a Software Composition Analysis tool to automate scanning for a long-term approach.

Assessing Needs

A recent Gartner report* states that by 2020, DevOps initiatives will cause 50% of enterprises to implement continuous testing, using frameworks and open-source tools. With this trend it's important for companies to assess their current state of Open Source Software management maturity. As usage expands, so does the potential for risk.

Big Tip

Analyze where things stand today with a Software Composition Analysis (SCA) maturity assessment.

How Mature is Your SCA Process?

Process Maturity and Business Value

Optimized **LEVEL 4**	Are we optimized for growth, scalability, digital transformation, and change management?
Automated **LEVEL 3**	Have we automated processes for scale and best user experience?
Enabled **LEVEL 2**	Are we using standard vulnerability management, OSS license compliance and obligation management processes across all products?
Reactive **LEVEL 1**	Are our applications secure, compliant and centrally managing obligations?

Key Software Composition Analysis Business Processes

License Management → Vulnerability Management → Obligation Management → Component Management

* Gartner: Four Steps to Adopt Open-Source Software as Part of the DevOps Toolchain, Manjunath Bhat, Daniel Betts, Christopher Little, 6 February 2019.

Final Big Tip

Some companies lack the insight and awareness to evaluate the effectiveness of their open source management. Discover where you are on your journey by taking the Software Composition Analysis maturity assessment.

NEXT STEPS

Want to know more about Software Composition Analysis and prioritizing your open source management?

LEARN MORE >

Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. **www.revenera.com**

1.800.809.5659 | +44.870.871.1111 | revenera.com