Sonatype

EXECUTIVE BRIEF

DELIVER BETTER, SAFER SOFTWARE EVEN FASTER

WITH SONATYPE SOFTWARE SUPPLY CHAIN SOLUTIONS

In everything we do, Sonatype's mission is simple. We transform software development to promote greater speed and efficiency, while also delivering software that is more secure, higher in quality, and more maintainable over time.

Sonatype has been one of the key enablers of modern, component-based development over the last 15 years. Our team has been a driving force behind the creation and adoption of Maven, the Central Repository, the Nexus Repository Manager, and Nexus Lifecycle. With millions of developers relying on at least one of our innovations every day, Sonatype has established itself at the nexus of all things critical to today's continuous software delivery.

DID YOU KNOW ...
A typical application has 24 critical or severe known security vulnerabilities and 9 known restrictive licenses?

One of the most remarkable changes to software development has been the dramatic rise of open source. Open source projects have become mission critical suppliers, delivering millions of incremental innovations (components), to development processes that are increasingly 'Lean' and 'Agile'. Indeed, modern software development looks remarkably similar to traditional industries where supply chain management has brought enormous business benefit by streamlining the relationships between suppliers, supply, assembly, and distribution.

We apply the transformational and proven principles of traditional supply chain management to the world of software development.

No matter what business you are in, software is your business.

Marc Andreessen, entrepreneur and venture capitalist, once said, "Software is eating the world." Indeed, software has become the primary path to competitive differentiation in many, if not most industries. Since innovation is mission critical, it is not uncommon to see manufacturing, finance and even entertainment/media organizations invest billions per year on software development.

Speed has fueled innovation, but at what cost?

Organizations are embracing new approaches and practices to speed development, such as agile, DevOps, continuous integration, continuous delivery, and component-based development. But is speed all we should be thinking about? By emphasizing speed over all other things, organizations are building up enormous levels of technical and security debt, the vast majority of which is

Hidden speed bumps on the road to continuous.[2]

Open source usage is exploding:
17.2B download requests in 2014

80%-90% of a typical application
is comprised of open source or 3rd party components

51,000 components
in the Central Repository have a known security vulnerability

283,000 components
in the Central Repository have known restrictive licenses

43% of companies
don't have policies to manage component quality

75% of those with policies
don't enforce them

27 different versions
of the same component (on average) are downloaded by the same organization

63% of organizations
keep an incomplete software Bill of Materials

1 in every 16
component downloads in 2014 included a known security vulnerability

23% of the components
in a typical application have critical or severe known vulnerabilities

There are 9 restrictive licenses
in a typical application, critical or severe

31% have had
or suspect a breach in an open source component

hidden from view. From a strategic standpoint, maximizing net innovation, that is, raw innovation minus technical debt, is the ultimate measure that will drive business benefit long term.

The importance of fewer and better suppliers, quality parts and visibility.

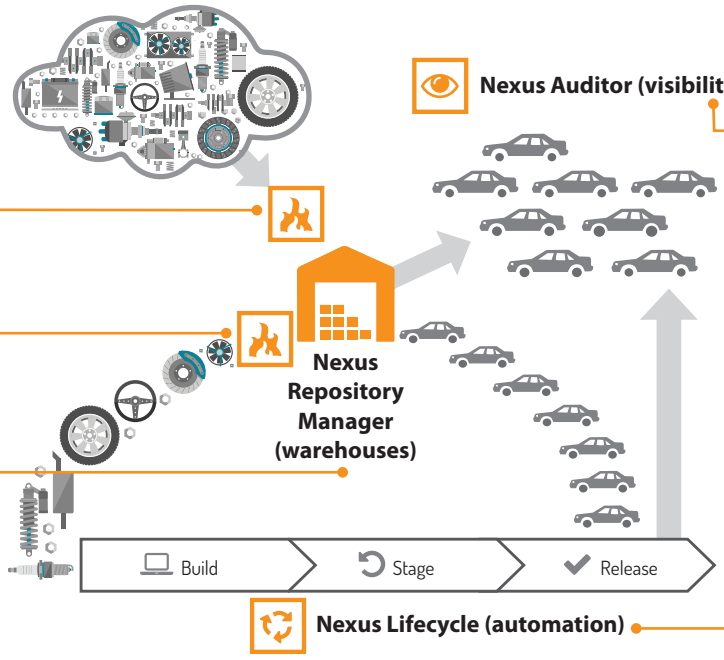
Today 80-90 percent of a modern application is assembled using modular open source or proprietary 'parts' (binaries, artifacts, components). Despite pervasive use, this 'parts' ecosystem remains incredibly complicated and highly opaque.

Without software supply chain solutions, there is no linkage between the suppliers of these 'parts' and the developers who use them – nor is there adequate visibility to where those parts have been deployed into production applications. Without this linkage, a host of issues arise which have long been solved in traditional manufacturing organizations.

For example:

- **Supplier decisions are made without adequate information** – Architects and developers make supplier decisions in isolation, without access to supplier quality and release history information.
- **Given the lack of visibility, all parts generally look the same to a developer** – Most organizations are simply unaware of known vulnerabilities or potential license risks in the components chosen for their applications. As a result, development teams inadvertently use defective or outdated parts long after better versions are released. In 2014 alone, an outdated Bouncy Castle (cryptography library) version with a level 10 security vulnerability, was downloaded 42,124 times by thousands of organizations.[1]
- **Remediation can be hard, yet defective components lead to technical debt** - If vulnerable components are inadvertently chosen, manual processes make it harder to upgrade to a less vulnerable component after-the-fact. Many outdated or vulnerable components remain in applications and build up technical debt over time.
- **Manual processes are too inefficient** - Speed is imperative for development teams. Manual processes or even automated human workflows introduce significant delays for developers driving up costs or leading to circumvention.

[1] Source: Sonatype analysis of the Central Repository.
[2] Sources: 2014 Open Source Developer Survey, Sonatype Application Health Check, and Sonatype analysis of the Central Repository.



Nexus Firewall - Automate policies to block undesirable components from entering or leaving your repository manager.

Nexus Repository OSS - Faster, more reliable builds. Improve open source component downloads, storage, and retrieval.

Nexus Repository - Improve the speed, distribution, and control of component parts and finished goods from development to production.

Nexus Auditor - included with Nexus Lifecycle or can be purchased as a stand-alone product. Monitor the quality and integrity of application components in production applications.

Nexus Lifecycle - Component insight and automated policies provide rapid feedback to prevent defects across your SDLC. Includes Nexus Auditor.

Let's embrace the principles of modern manufacturing. Again.

Lean and Agile software development methodologies both have their roots in Toyota's manufacturing innovations. Now, it's time to borrow Toyota's supply chain management innovations to optimize raw innovation and drive substantial increases in 'net innovation' to deliver better, safer software – even faster.

By leveraging extensive automation, Nexus software supply chain solutions help organizations choose better and fewer suppliers, use the highest quality parts, and track what components are used and where. You can use Nexus to improve the selection, use, sharing and deployment of open source and third party components, as well as other build outputs.

Toyota's process innovations brought enormous gains in productivity, predictability and long-term competitive advantage. Our mission is to ensure that development and operations teams use software supply chain solutions to make more informed decisions, efficiently share and consume components, and track and manage what is used and where—to accelerate innovation without risk. Organizations on the front end of this transformation improve developer productivity by 15-40%, eliminate unplanned work, technical and security debt, and maintainability issues by 96%, and remediate newly discovered defects in minutes, versus days, weeks or months.

Sonatype helps organizations build better software, even faster. Like a traditional supply chain, software applications are built by assembling open source and third party components streaming in from a wide variety of public and internal sources. While re-use is far faster than custom code, the flow of components into and through an organization remains complex and inefficient. Sonatype's Nexus platform applies proven supply chain principles to increase speed, efficiency and quality by optimizing the component supply chain. Sonatype has been on the forefront of creating tools to improve developer efficiency and quality since the inception of the Central Repository and Apache Maven in 2001, and the company continues to serve as the steward of the Central Repository serving 17.2 Billion component download requests in 2014 alone. Sonatype is privately held with investments from New Enterprise Associates (NEA), Accel Partners, Bay Partners, Hummer Winblad Venture Partners and Morgenthaler Ventures. Visit: www.sonatype.com

Sonatype Inc. • 8161 Maple Lawn Blvd, Suite 250 • Fulton, MD 20759 • 1.877.866.2836 • www.sonatype.com
Sonatype Copyright 2015. All Rights Reserved.