Sonatype

EXECUTIVE BRIEF

We Make It Easy to Build Trusted Software– and Keep It That Way Over Time

THE NEW SOFTWARE SUPPLY CHAIN

If your organization develops applications, you're probably using third party software components. In fact, research shows that 90% of an average application is assembled with components instead of source code, the majority of which are open source software downloaded from public repositories, such as the (Maven) Central Repository.

Much like a traditional "supply chain" is used to manufacture products, your software is built with a supply chain of components from all over the globe. The challenge is knowing exactly which components you are using, where they are used and which ones are known to have vulnerabilities or license and quality issues.

Even though applications have become the number one vector of attack[1], application security hasn't kept pace with the speed and scale of modern application development. This leaves a big trust gap. Third party and open source vulnerabilities have become an inherited – but avoidable – risk. Most organizations struggle with the trade-off between going fast and being secure along the way. Sonatype believes you can have both. However, to make application security effective, new approaches have to be significantly simpler, developer friendly and ensure continued trust.

[1]Source: The State of Application Security August 2013, Ponemon Institute & Security Innovation

Are we really securing our applications? A few eye-opening facts.

Open source usage is exploding. **13B downloads in 2013**

90% of the typical application is comprised of open source or 3rd party components

Only **57% of organizations** have policies governing open source usage and 29% of those policies don't address security

71% of all applications contain at least one critical flaw in at least one component

Nearly **2/3 of organizations** don't know which components are used in their applications

60% of developers aren't concerned about security

One year after a security alert: **6,916 organizations** downloaded a high-risk component **66,284 times**. (And this is true of many components!)

Less than 1 percent of security budgets are spent on application security

90% of cyber attacks are focused on applications

Sources: Ponemon Institute, Verizon 2013 Data Breach Investigations Report, Open Source Developer Survey, and Sonatype Application Health Check

SECURITY AT THE SPEED OF DEVELOPMENT– AND THROUGHOUT THE SOFTWARE LIFECYCLE

In many organizations, Agile—and increasingly DevOps—have replaced the traditional waterfall development and delivery approach. This requires that application security is also agile and re-thought in the context of modern development methods, continuous integration, and continuous delivery. Current application security can't scale to meet the demands of modern software development. To secure modern applications, approaches must be:

- Streamlined and built in to development tools
- Effective throughout the entire software lifecycle
- Highly accurate and produce evidence that it is working
- Continuous to address ongoing threats in real-time, ensuring sustaining trust

SONATYPE'S UNIQUE APPROACH IS DESIGNED TO WORK IN THE REAL WORLD

Sonatype allows organizations to automate policies that support component-based development and then delivers relevant information in context throughout the software lifecycle. This ensures that you are using the best components during consumption, development, integration, build and staging. Developers and security professionals get immediate feedback on security in context so they can act on it in real-time.

SIMPLIFY THE COMPLEXITY OF COMPONENT-BASED APPLICATION DEVELOPMENT

Sonatype Repository Managers

Nexus repository managers enable development teams to enjoy the benefits of agile component-based development in a streamlined and structured environment.

Nexus OSS

Nexus OSS is a basic repository manager to improve developer productivity offering the ability to:

- Reduce build times
- Use a central location to store, manage and share components across developers and teams
- Observe, manage and govern components using a repository-centric model

Nexus Professional Repository Manager

Nexus Professional is an enterprise class repository manager featuring technical support, plus enhanced features enabling you to:

- Get increased visibility into security, license and architectural risk associated with components in your repository
- Leverage a proxy-based architecture to store, share and manage components across the enterprise
- Ensure the quality of your production releases with build promotion and staging
- Secure the contents of your repository with access controls and secure connectivity

Nexus Professional CLM Edition

Nexus Professional CLM Edition is an upgrade to the Nexus Pro Repository Manager for organizations who want to move one step closer to full component lifecycle management (CLM). With this upgrade, you can:

- Govern component usage in your build and release process
- Augment Nexus Pro staging and promotion support with policy enforcement that ensures applications meet security, licensing and architecture standards before they advance through the release management process

What Makes Sonatype Different?

As the stewards of the Central Repository, the creators of the Apache Maven project and the distributors of the Nexus open source repository manager, Sonatype has played a significant role in the adoption of open source used by more than 10 million developers in millions of applications.

Our unique history and years of open source experience gives us a unique vantage point to understand both the benefits and risks of open source. That's why our solutions are always designed to empower developers to make better component decisions. Unlike other forms of application security, component security is managed by developers early in the development cycle and yields large security gains for comparatively low cost and effort.

Sonatype Component Lifecycle Management (CLM)

Component Lifecycle Management (CLM) provides a new way to identify, manage and monitor every component and its dependencies throughout the software lifecycle. CLM enables organizations to realize the promise of agile, component-based software development while avoiding security, quality and licensing risks.

Sonatype CLM for Risk

Helps you quickly and proactively identify the component security, licensing and architecture risk of your current applications—especially applications that are already in production, including the ability to:

- Create a full "bill of materials" (BOM) for every applications and a consolidated inventory of all components used in every application
- Identify and visualize overall security, license and quality risk at both the component level and at the application level
- Continuously and automatically monitor for new risks or a change in existing risk level, including risk alerts and an inventory of precisely which applications are at risk.

Sonatype CLM for Risk & Remediation

This is a complete Component Lifecycle Management (CLM) solution to achieve comprehensive and lasting governance across the entire software lifecycle. Includes Nexus Pro and CLM for Risk, plus the ability to:

- Find and fix risky components early in the development process using the tools developers use every day
- Centralize, automate and enforce policies to ensure license and security risks are managed throughout the software lifecycle
- Precisely identify and track all components used in your organization, from consumption to production
- Truly achieve defense-in-depth by enforcing policy across multiple points throughout the entire software development lifecycle
- Streamline DevOps efforts with release management policies
- Manage a complete component inventory in development & production applications
- Proactively and continuously monitor applications for new vulnerabilities to ensure sustained trust

Every day, developers rely on millions of third party and open source building blocks—known as components—to build the software that runs our world. Sonatype ensures that only the best components are used throughout the development lifecycle so that organizations don't have to choose between going fast and being secure. Policy automation, ongoing monitoring and proactive alerts makes it easy to have full visibility and control of components throughout the software supply chain so that applications start secure and remain that way over time.