Sonatype

PRODUCT OVERVIEW

FROM NEXUS TO COMPONENT LIFECYCLE MANAGEMENT

Extend Your Repository Strategy to Full Component Governance

As a Nexus user, you are hopefully realizing the many benefits of a repository manager, such as using Nexus to proxy open source components from the Central Repository and hosting custom components like proprietary JDBC drivers. And once this dependable cache of components is in Nexus Pro, it is accessible to all of your developers and continuous integration server nodes.

By leveraging third party components, you are building and delivering applications faster than ever. However, there's a downside: you're taking on responsibility for potential security vulnerabilities, license issues or even quality deficiencies in those components. Eventually, your organization will want to manage the risks associated with your open source usage, whether it be internally or externally driven.

The road to component security.

Developers need to be empowered with information, not burdened with a set of inflexible rules. While it looks good on paper, a locked down repository consisting only of pre-approved components can slow down development. Turning Nexus into a 'Golden Repository' of only pre-approved components sounds like an optimal solution, but in reality it's too extreme and can have negative consequences. For instance, waiting for approval for those soon-to-be golden components slows project momentum. When development stops because of policy constraints, there is a good chance the process will be circumvented. Developers are problem-solvers by nature; workarounds are to be expected.

The key is providing your developers with the component intelligence they need to make the best decisions at the start -- and build it into the tools they use every day. This early visibility goes a long way since developers make choices on component usage throughout the development process.

The road to policy management.

Written and approved policies are needed not only at the beginning of the project, but also throughout the entire development lifecycle to avoid or remediate vulnerable components or complicated licenses. Ultimately, this provides the assurance that satisfies security, compliance and legal interests.

As a Nexus user, you've probably also come to the conclusion that flexible, automated policies providing guardrails that propel development would add significant value, as opposed to those confining policies limited to strictly blacklist or whitelist components at the repository level. Policy approaches that are manual or workflow heavy fall short because they can't keep pace with the volume, variety, complexity and release cadence of components. Challenges with process-laden approvals are exacerbated by the sheer number of applications and the need for short, agile-based delivery cycles.

Since protecting your production applications is the ultimate goal, monitoring within the production environment should also be on your radar. The ability to proactively identify, triage and remediate new vulnerabilities as they happen may also be very appealing.

CLM is the next logical step. Here's why.

Hopefully you've taken advantage of the Nexus Repository Health Check and have seen that components downloaded from the Central Repository have a relatively large number of security vulnerability and license issues. Keep in mind that these issues affect components that have been proxied to your local Nexus instance. That does not necessarily mean that any of your own applications include these components.

If you're a Nexus Pro user, you have detailed information about the components, which allows you to assess the health of your overall repository. Analyzing your repository contents is a starting point for managing component usage, but you also need to extend management throughout the software lifecycle. The good news is that Nexus provides a good starting point and Sonatype Component Lifecycle Management (CLM) allows you to expand your governance in a non-linear approach. It's a method that's designed to fit into your team's work style. It let's you focus on the stage you're currently working on, not taking you back to a point you've already been.

Think of it more as a natural path of applying policies that provide stage-appropriate guidance throughout the software lifecycle. You define the policies and the actions, and Sonatype CLM automates the guidance and enforcement directly in the tools that are used by your developers.

- You can start by applying policies to the staging and promotion process within Nexus Pro, ensuring applications meet your security, licensing, and architecture standards as part of the release process.
- You can guide your developers with component intelligence directly in the IDE to select optimal components from the beginning, eliminating downstream issues. And if flaws are discovered, your developers can select the best replacement and migrate to that component using "one click migration" support.
- You can use the Sonatype CLM for CI plugin to manage your build and continuous integration efforts, including the ability to fail a build so that applications that don't meet your standards are not promoted to production.
- Or, you can start by assessing the risk for applications in production. Sonatype CLM can analyze your application inventory, create a 'bill of materials' to show what components are used where, identify risk based on policies appropriate to your organization and application type, triage and prioritize action, fix the flaw by migrating to a new component, and help manage the release process.

All of these scenarios are enabled with automated policies that provide appropriate guidance and enforcement to protect your production environment – with up-front flexibility for your developers. The need for manual review or an approval-laden process that can't keep pace with your development efforts is eliminated, allowing your precious human resources to focus on defining policies and managing exceptions.

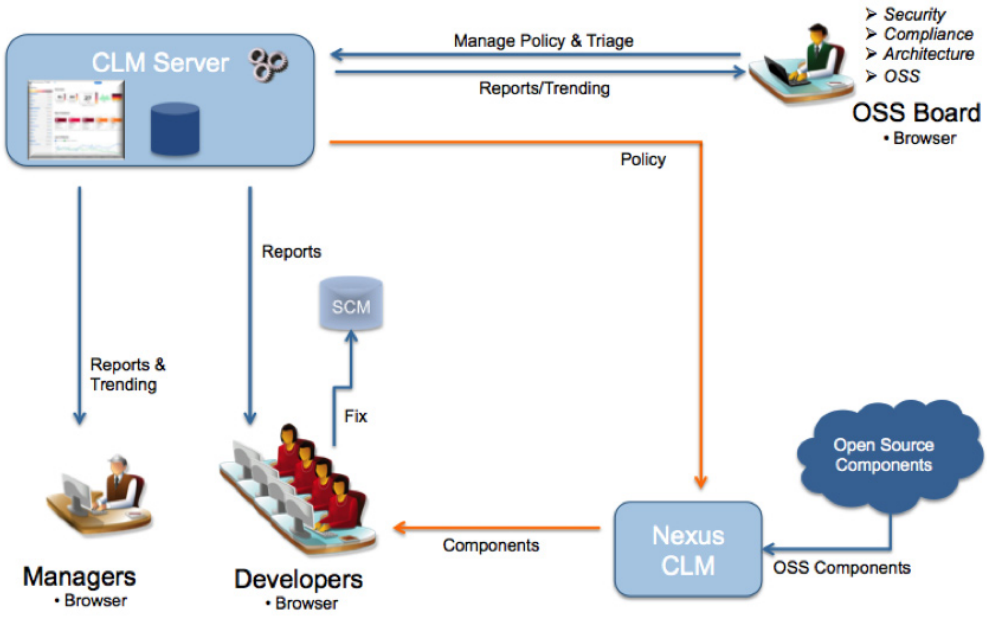
Nexus Pro CLM Edition extends the value of your Nexus investment

Nexus Pro CLM Edition is an upgrade for Nexus Pro that improves the visibility and control of your component-based development by analyzing the content of your application builds and automatically controlling the release process using security, licensing and quality criteria. Security, licensing and architecture policies codify your organization's standards and security profiles for distinct applications. These policies are automatically enforced during the build promotion and staging process to ensure that only trusted applications are released to production.

This approach ensures that any release you produce is actively and automatically validated against up-to-date information regarding security vulnerabilities and license characteristics for all the components you use. You can establish a policy that notifies you or stops the staging process if any components in your software have known security vulnerabilities or use a license that is incompatible with your policies.

Nexus Pro CLM Edition makes it easy for existing Nexus users to extend the value of their repository manager investment.

This diagram shows how the Nexus Pro CLM Edition uses policies to manage components in your repository and to manage the release process based on your security, licensing and architecture concerns.



Sonatype CLM provides complete lifecycle management

Developer-friendly guidance at the beginning of a project is great – extending that governance throughout the Software Development Lifecycle (SDLC) is what makes it most effective. We've established that policies that allow for independent decision-making based on a set of criteria are more likely to be accepted and therefore more easily incorporated into the development lifecycle.

Our mission is simple. We make it easy to build trusted application and keep them that way over time. We do this by adhering to the following principles:

Developer-friendly guidance and enforcement supported throughout the software lifecycle.

What makes guidance "developer-friendly"? The answer is to integrate component intelligence and policy guidance directly in the tools that developers use, such as the Repository Manager, IDE and Build/CI environment. This integrated guidance prevents problems and identifies flaws early in the process. And it's not just problem discovery – Sonatype CLM makes it easy to fix problems by providing advice about ideal component replacements which can be implemented with one click migration support.

This combination of capabilities speeds development and doesn't get in the way of developer deadlines.

Security, legal/compliance, and architecture concerns are addressed to enable effective CLM throughout the entire software lifecycle.

CLM begins when your security, legal and architecture teams codify their specific requirements in the policies. Hierarchical organizational requirements and application-specific requirements are supported to simplify policy administration and ensure policies are applied with the right context and consistently enforced.

When policy enforcement is automated, your human resources are freed up to focus on the work of policy definition and exception management.

Comprehensive application & component inventory intelligence including a "bill of materials".

Nexus provides an inventory at the repository level – Sonatype CLM extends this so that you can see a complete inventory across your enterprise, including an application inventory. This inventory capability is based on unique matching that ensures fast, accurate and up-to-date inventory data. Unlike approaches that rely on slow, batch-based scans, Sonatype provides inventory data instantaneously so it can be integrated naturally into development tools.

This complete inventory capability provides the foundation for providing security, licensing and usage information that drives the automated policy actions.

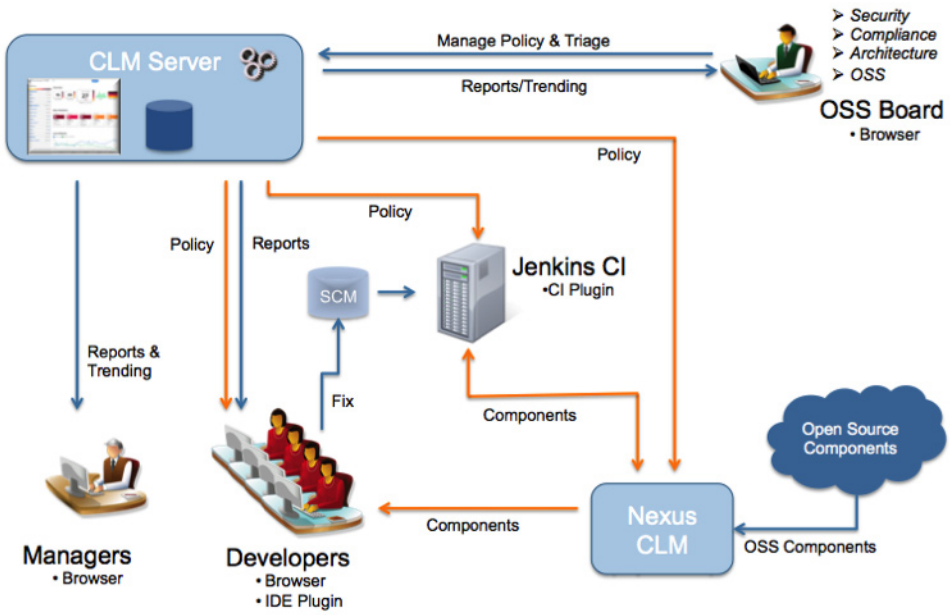
Monitor applications even after they move into production and assess risk across the enterprise.

Ultimately, this is all about protecting applications – it's ideal to start with CLM as you develop new applications, but you also have protection for those applications already in production.

Production application usage is dynamic, components are not static and hackers are not complacent. Sonatype CLM continuously monitors the application inventory for new vulnerabilities and proactively alerts appropriate constituents. Vulnerabilities can be mitigated easily since Sonatype CLM prioritizes the risk. Sonatype CLM makes it easy to select the best replacement version, migrate the application to the new version using one-click migration, and helps manage the release process so the new application version can be deployed to production quickly.

Sonatype CLM provides dashboards that allow you to assess the entire application portfolio. If a flawed component is discovered, the Sonatype CLM inventory allows you to determine what applications are affected – or you can look at an individual application or set of applications to see components that violate your policies.

This diagram shows how Sonatype CLM guides and enforces action throughout the entire SDLC. Sonatype policies are defined with different actions based on the stage of the development lifecycle. IDE guidance provides developers with instant, actionable data during the normal activities of their job. CI support enables validation and enforcement of policies in your continuous integration environment:



Where do I start and how do I deploy Sonatype CLM?

Here are some simple steps:

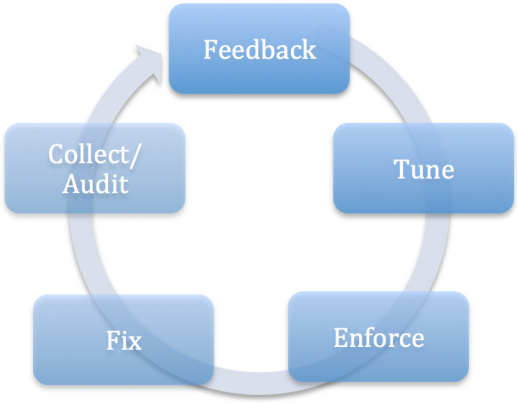
- Install the Sonatype CLM Server
- Create a CLM Policy
- Set initial enforcement points to information gathering only
- Install the appropriate plugins
- Validate and tune policy using real data
- Over time, adjust enforcement points

Sonatype CLM gives you a tremendous amount of control over component usage. Like all enforcement technologies, it is easy to over enforce. The goal is to go fast and be secure. Allowing developers to experiment with new technologies, while giving them early notice of policy violations, enables them to be proactive in component choice and interactive with policy decisions.

Start simple, iterate and improve. Incremental change is the key to a successful effort. As with any significant initiative, it's critical to show short-term success.

It's best to leverage an approach to management/governance where you iterate over time, advancing incrementally. This goes double for policy creation - even if you start with default or generic policies that provide a foundation on component usage, you will likely have to tune the policies over time to achieve an optimal balance. Not all applications are equal in regards to risk and not all policies are applicable to all applications. Starting with an iron-fisted policy applied to all applications is the quickest way to failure.

If you iterate, you can start with your greatest common denominator policies in "audit" mode vs. "enforcement" mode. In audit mode, policies are set to manage risk based on your organization's risk tolerance. Audit mode can also be considered as collection or inventory mode. Once you feel good about the policy design, you can start turning on enforcement actions (e.g., stop builds, stop promotion to production, etc.) without the resistance you'd get by starting with too many policies. Over time, policies can be adjusted to lower risk issues and improve code quality. The iterative process of policy tuning, enabling lifecycle stage enforcement per policy, and early issue notification gives an organization unprecedented control over component risk without creating the traditional antagonistic relationship between governance and efficient software construction.



For most organizations the "big bang" approach – where all teams, all individuals, all departments, and all applications are introduced to component management at the same time – is not feasible. Like other technology or policy rollouts, it makes sense to start small and expand over time.

The nice part about good component management is that you can start with your critical applications. It is often easier to see the ideal future direction by understanding the mistakes of the past. CLM does not impact an application's performance and since it is not invasive, it is best to start first with the core applications first where the greatest positive impact can be made.

Get Started Today

If you're considering the transition to full CLM, try it for 20 days. We'll walk you through the process, and at the end of 20 days, you'll have a detailed situational analysis and risk report.

With Sonatype CLM in your integrated development environment, your continuous integration server and enhanced support in your repository manager, you will be able to ensure that security vulnerabilities and license issues are detected and avoided early on in the development lifecycle and get to production. As a Nexus user, you have the flexibility to upgrade policies to drive the release management process. You can upgrade to full IDE integration when you and your team are ready for full CLM.

Sonatype CLM greatly reduces the security and license risks from your software development while at the same time reducing the effort required. Sonatype CLM allows you to take care of the 80 - 90% of your application, that originates from using components and provides tools specifically catered to your developers construct applications.

For more information about Sonatype CLM check out our website (www.sonatype.com/CLM) or contact us directly.

Sonatype's software protects the world's enterprise software applications from security, compliance, and licensing threats. Every day, millions of developers build software applications from open source building blocks, or components. Customers rely on the Sonatype family of products to accurately identify and analyze component usage and proactively fix flawed components throughout the software development lifecycle so applications are secure and comply with licensing and regulatory requirements. Sonatype is privately held with investments from New Enterprise Associates (NEA), Accel Partners, Bay Partners, Hummer Winblad Venture Partners and Morgenthaler Ventures.

Sonatype Inc. • 8161 Maple Lawn Drive, Suite 250 • Fulton, MD 20759 • 1.877.866.2836 • www.sonatype.com