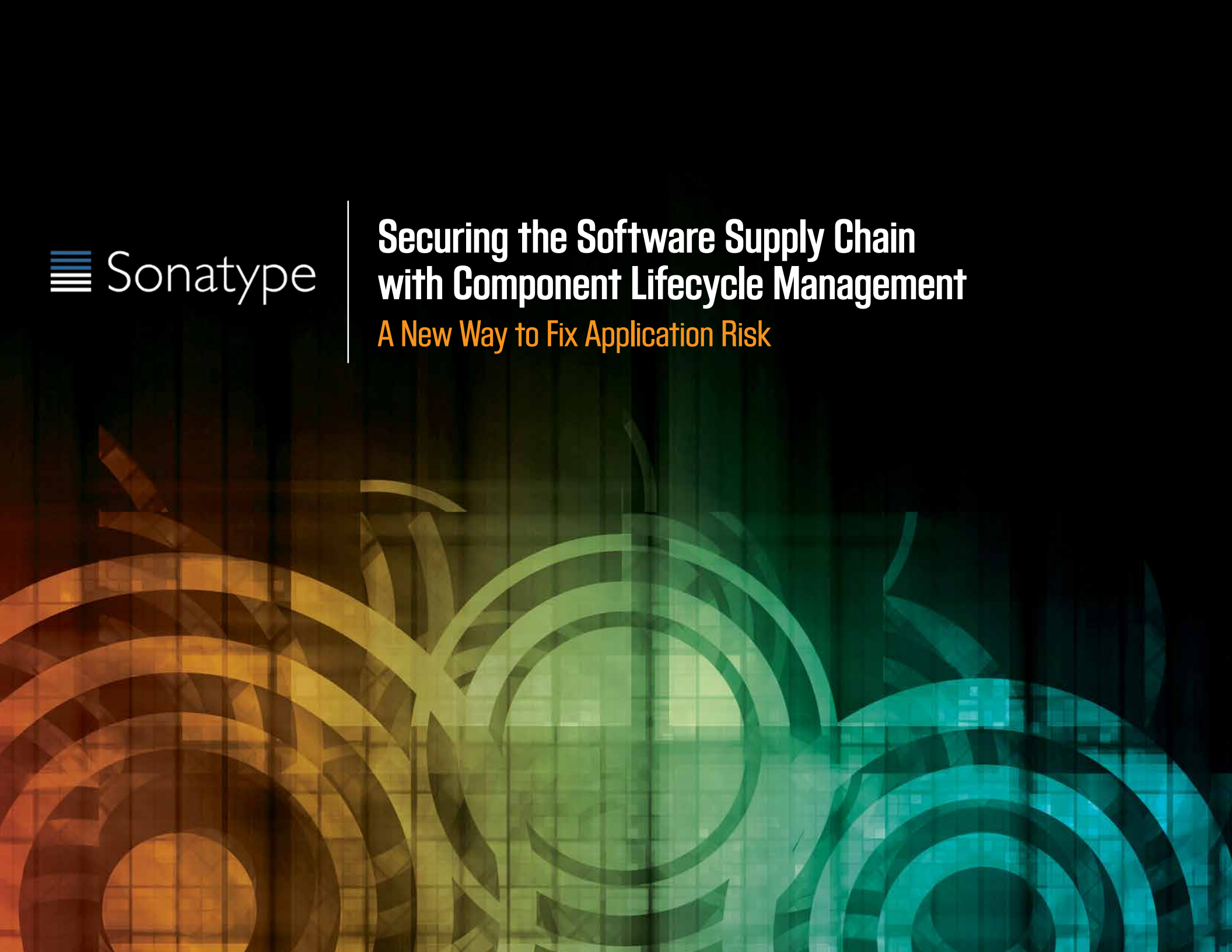
Sonatype

Securing the Software Supply Chain with Component Lifecycle Management

A New Way to Fix Application Risk



Applications Are No Longer Written – They're Assembled

Up to 90% of the typical application is comprised of components, most of which are open source and originate from hundreds of projects outside the enterprise.

Software assembly lets organizations develop faster, reduce costs, and improve efficiency. But a complex supply chain also introduces security, IP and other risks. Component exposures are exceedingly common and today's security tools don't secure the modern software supply chain. It's also too complex and expensive to monitor every component in use.

To make application security matter, new approaches have to be significantly simpler, usable by developers and show real, sustainable results. With the right controls and processes to identify and govern component usage as well as eliminate flaws, organizations can secure the entire lifecycle.

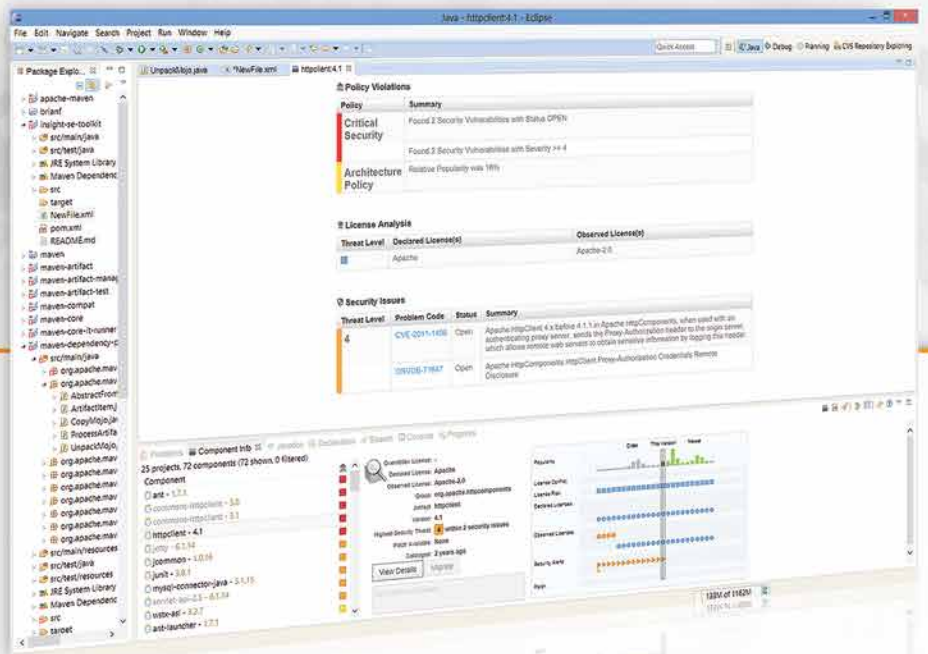
Go Fast and Be Secure

Sonatype Component Lifecycle Management (CLM) is the first and only application security tool to secure component-based applications. CLM tracks usage, enforces policy, and prevents the use of flawed components throughout the modern software supply chain. By natively integrating into the tools developers already use, risk is removed proactively, drastically reducing downstream "fix" costs. This modern approach to software assurance makes it possible to reduce risk and ensure compliance without impeding development velocity.

Sonatype CLM is the first application security solution to:

- Provide a single view of all components, their policy, metadata and promotion model in your repository, IDE, CI Server and CLM Server.
- Improve developer 'component IQ' by providing component intelligence within the IDE so they can make the best component choices early in the development process.
- Automate defect resolution through flexible remediation options at every phase of the development process, creating zero delay for development.
- Support a defense-in-depth strategy with centralized rule management combined with multiple enforcement points. If someone were to subvert a control in one enforcement point, it would be caught at another.
- Make governance simple through user-centric, intuitive design and the belief that if you can't make governance simple, you're creating more barriers to making it secure.

Combining these benefits allows organizations to build security in from the start. . . and enforce it throughout the entire software lifecycle.



Sonatype CLM for IDE in Eclipse lets developers make the best component choices early in the development cycle.

62% of organizations report breaches in the past year due to flaws in their critical applications

The Sonatype CLM Solution

The CLM Server provides a central location for active risk assessment and management across development environments, applications, and teams. Within the CLM Server you can:

- View and manage your comprehensive inventory of components and associated bill-of-materials.
- Define and automate your policy and rules.
- Assess risk globally through comprehensive dashboards.
- Pinpoint risks via drill-down reports and detailed analysis.
- Receive alerts and impact assessments of newly discovered flaws.

CLM Secure Consumption ensures trust in the software supply chain by authenticating and securely delivering components. Sonatype can uniquely provide:

- OSS project validation to ensure high quality, trusted components.
- Secure component delivery to eliminate man-in-the-middle attacks.
- Authentication throughout the software lifecycle eliminates risk of tampering inside the firewall.

CLM for Development provides developers with security, popularity, and licensing information making it easy to detect and prevent flaws early in the development process. This "zero-latency" approach to remediation reduces the impedance for developers that typically drives non-compliance.

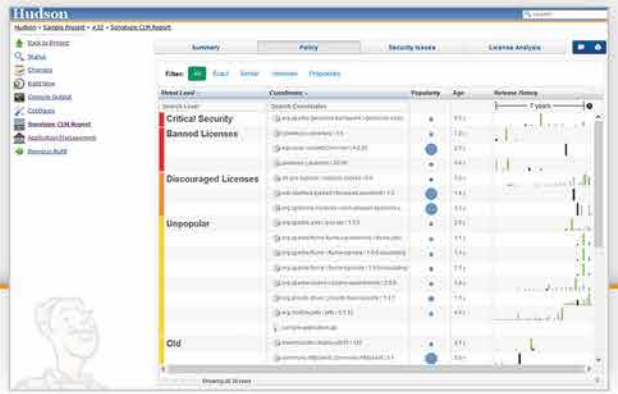
- Rich security, licensing, and popularity metadata informs component selection in the IDE.
- Information and policy enforcement extends across the IDE, repository, and CI server to automate and enforce governance across the entire software lifecycle.

CLM for Continuous Monitoring establishes sustaining trust by monitoring your component inventory for newly identified vulnerabilities. Information is presented in a first-of-its-kind component dashboard designed to be efficiently consumed and to provide visibility of what threats exist, where they are and what actions to take.

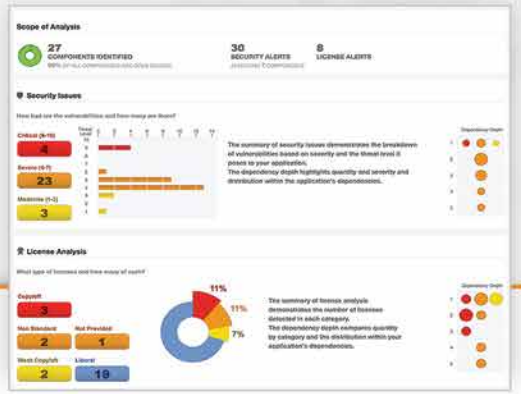
Know Your Components – Throughout the Software Lifecycle

Sonatype CLM enables organizations to accurately identify and analyze component usage, effectively govern the entire software lifecycle, and proactively fix flawed components. By informing component choice, pinpointing flaws early in the software lifecycle, and offering flexible remediation options, Sonatype CLM reduces risk, improves programmer productivity, and increases development velocity.

Dashboards and reports provide a complete view of global risk with drill-down detail to drive action.



Integration with CI servers enforces policy at build time.



Newly discovered threats are continuously reported against your inventory of components to ensures sustaining trust throughout your software supply chain.

About Sonatype

Sonatype has been on the forefront of creating tools to manage, organize, and better secure components since the inception of the Central Repository and Maven in 2001. Today, over 70,000 companies download over 8 billion components every year from the Central Repository, demonstrating the explosive growth in component-based development. Today's software ecosystem has created a level of complexity that is increasingly hard to manage. Partnering with application developers, security professionals and the open source community, Sonatype has introduced a way to keep pace with modern software development without sacrificing security. We call it Component Lifecycle Management (CLM), the new platform for securing the modern software supply chain.

We believe that to achieve application security, the approach has to be simple to use, integrated throughout the lifecycle and ensure sustaining trust. With CLM we're improving the visibility, management and security of component-based development across the entire lifecycle. Together with our customers, we're ushering in a new era of application security.

Sonatype 12501 Prosperity Drive, Suite 350 · Silver Spring, MD 20904 · 1.877.866.2836 · **www.sonatype.com**