Sonatype

PRODUCT OVERVIEW

CLM FOR RISK

Use Component Lifecycle Management (CLM) for Risk to Quickly and Precisely Identify Security, License and Quality Risk Across Your Applications

Research shows that 90% of an average application is assembled from third party components, most of which are open source downloaded from public repositories, such as the (Maven) Central Repository.

While component based application development has fueled a lot of innovation in recent years, the increasing usage of third party components can be difficult to manage and may introduce risk into your organization.

Sonatype's mission is to make it easy to leverage component based development in a secure way - and keep your applications secure over time. As your trusted partner for component and open source governance, risk management, and compliance, Sonatype helps you leverage the benefits of component based development while minimizing the risk associated with security, licensing, and quality issues.

Sonatype understands that you have applications both in production and in active development and maintenance. These applications consist of components that may not have been properly vetted or new vulnerabilities may have been discovered after the initial approval process. Combining the high number of applications that organizations use with the volume, variety, complexity and release cadence of components, it's not surprising that organizations are exposed. Organizations struggle to create and maintain an accurate and up-to-date list of their component inventory across appplications. Developing a complete risk profile based on component security, licensing and quality issues is beyond the reach of most organizations. This reality is not simply an "IT issue" - vulnerable applications can place the entire business at risk.

CLM for Risk is optimized to manage the risk across your existing application portfolio. CLM for Risk provides the visibility you need to monitor and assess application risk in real-time. CLM for Risk allows you clearly assess component security, license and quality risk against application and organization-based security, licensing and architecture policies. Not only will CLM for Risk provide an initial assessment to triage and prioritize your response; CLM for Risk provides ongoing monitoring to ensure continuous trust of your production applications.

CLM for Risk answers these common questions:

- What components are used in each application?
- What is my full component inventory across applications?
- Which components pose the highest degree of security, quality or licensing risk?
- Which applications are impacted?
- Where should we focus our remediation efforts?
- How can we know if a threat status changes over time?
- What new vulnerabilities have been reported that affect my applications?

CLM for Risk helps you:

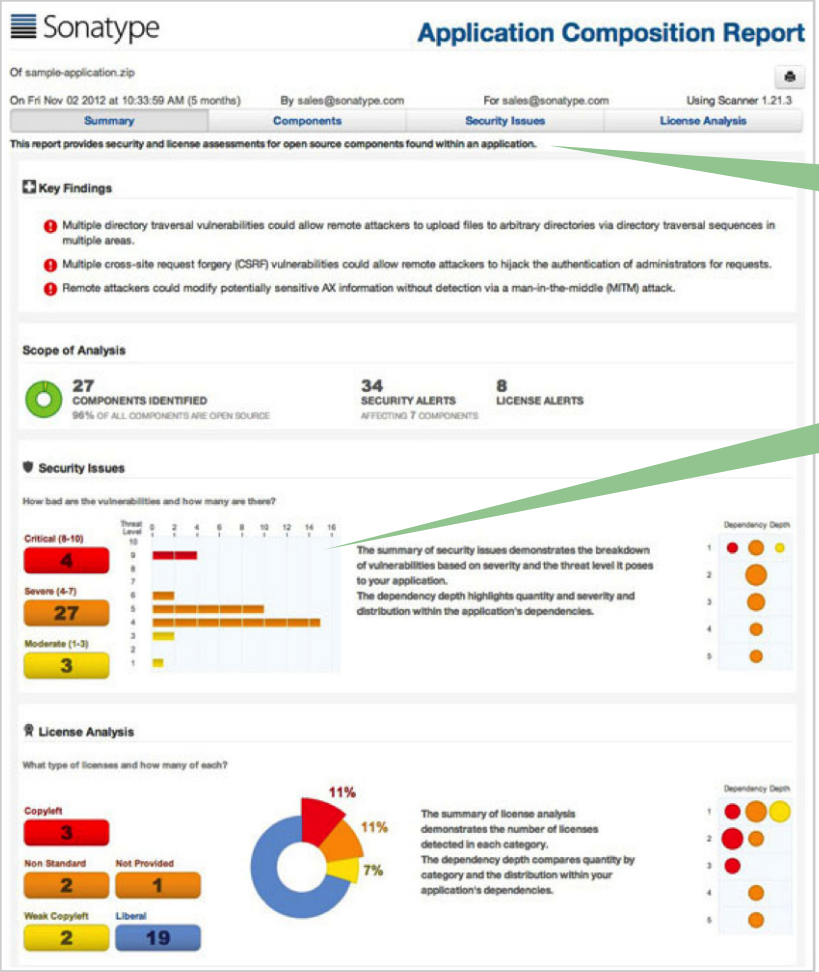
- **Build and maintain an accurate and timely component inventory** that serves as the foundation for assessing and managing application risk.
- **Visualize component risk** with real-time executive dashboards that assess all components in use across both development and production applications.
- **Identify use of open source components with known vulnerabilities** including security, licensing and quality risks in all components and their many dependencies.
- **Prioritize risk** and response using automated policies that reflect your organization's unique risk profiles.
- **Continuously monitor** and be alerted proactively for newly discovered threats.
- **Easily expand** to full component lifecycle management (CLM for Risk & Remediation) which encompasses both managing risk and quickly remediating concerns.

WHY CLM FOR RISK?

Accurate, Timely, and Comprehensive Component Inventory (Bill of Materials)

Sonatype employs a unique, binary fingerprinting approach that instantaneously produces an accurate inventory complete with comprehensive security, licensing and usage intelligence. This Bill of Materials can be used to assess application risk and is the basis for the following capabilities:

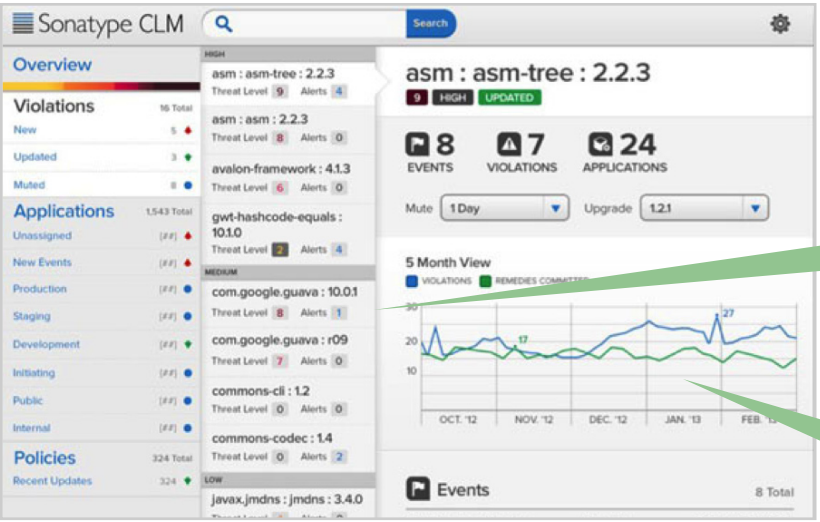
- **Pinpoint discovery** – if a component vulnerability is discovered, CLM for Risk identifies all of the applications that are infected by the flawed component.
- **Application analysis** – the Bill of Materials allows organizations to assess individual applications using the security, licensing and architecture characteristics of all related components, including dependent components.



Detailed component information is available for overall inventory, security and license analysis risk.

Security and licensing summary for your application inventory allows you to quickly assess overall application risk.

Visualize Risk Across the Entire Organization



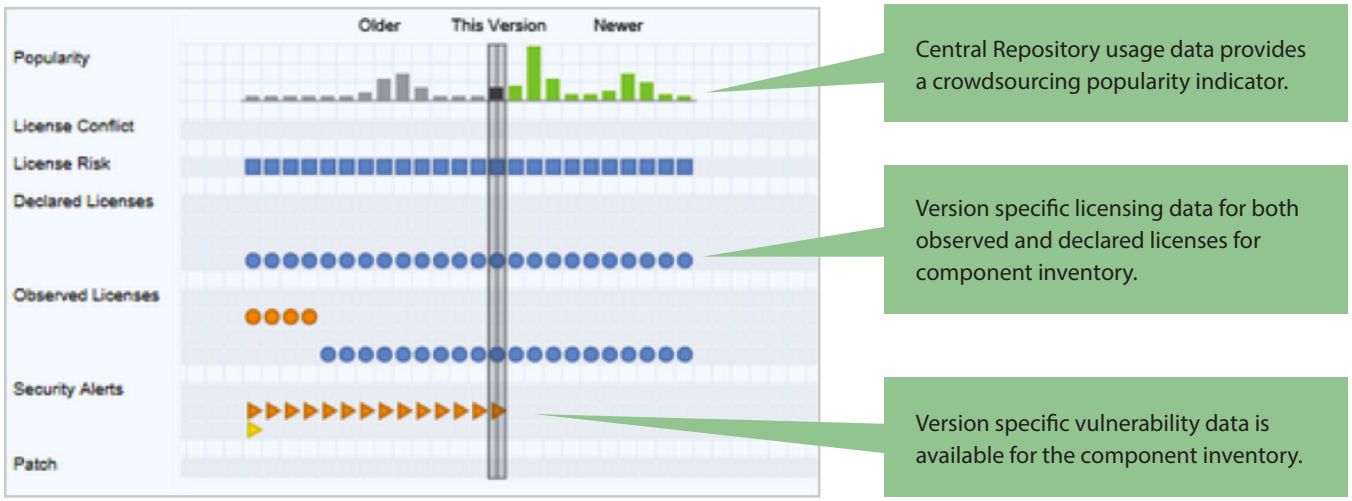
Security, licensing and architecture policy violations are prioritized by threat levels defined for your organization.

Violations and events can be trended over time to assess enterprise risk.

Sonatype dashboards enable you to visualize risk across the entire organization. Intuitively presented inventory and component intelligence provides a summary assessment and detailed information is available via drill-down reports. These dashboards provide the following value:

- **Newly reported threats** are continuously reported through dashboards with prioritization based on impact.
- **Proactive notification** allows you to respond to policy violations that need immediate attention.
- **Comprehensive analysis capability** including historical trend data helps assess the overall risk posture of your applications and drives your risk mitigation strategy.
- **Global risk management view** helps assess risk and supports regulatory and compliance initiatives.

Rich Security, Licensing and Usage Intelligence



Sonatype is uniquely positioned to provide rich component intelligence for binary artifacts that are hosted in the Central Repository. This component intelligence spans security, licensing and usage data providing the following capabilities:

- **Continuous security vulnerability discovery** is provided that leverages public security vulnerability data. Sonatype provides version specific detail allowing you to determine if your application is impacted by the security vulnerability.
- **Comprehensive licensing intelligence** spans both declared and observed license data for all component and component dependencies.
- **Usage information for components in Central** provides an indication of component popularity and developer acceptance.

Policy-based Risk Assessment

Component violations are driven by hierarchial organization and application specific policies.

Risk profiles provide context for analyzing your overall risk profile and responding to new violations.

Sonatype leverages policies so that risk can be assessed based on your organization and application requirements. This approach accommodates specific risk profiles associated with different application types and departmental needs. The policies are the basis for the automated alerting that occurs when new component vulnerabilities are discovered. Sonatype uses automated policies to provide the following value:

- **Hierarchical organization and application specific policies** support diverse security, licensing and architecture concerns. Automated policies can be easily administered by your CISO team, legal/compliance, and enterprise architects, eliminating the need for time-intensive coordination.
- **Risk profiles** can be uniquely built into policies for departmental or application-specific requirements.
- **Customized dashboards** intuitively display your application and component violations using visual cues that make it easy to assess and prioritize the most important risk factors.
- **Policy management** across the entire software lifecycle to report on violations. (Note: with CLM for Risk & Remediation these policies can be automated to provide guidance and enforce action at each stage in the software lifecycle.)

Extending the Value of CLM for Risk

Once your organization begins to automate policy, management and governance of OSS components using CLM for Risk, you can easily upgrade to CLM for Risk & Remediation for these additional benefits:

- Prevent problems from the start by providing intelligence that allows developers to select optimal components within the IDE, when they begin the development process.
- Integrate into Repository Manager, Integrated Development Environment (IDE) and Continuous Integration (CI) Servers provides guidance and enforcement throughout the entire software lifecycle.
- Easily remediate flawed applications with version replacement recommendations and one-click component migration.
- Effectively manage the application delivery process using policy-driven Nexus Pro release management capabilities.

If your organizations struggles to answer basic questions like "what components are used in each application," or "what is my full component inventory across applications," or "which components pose the highest degree of security, quality or licensing risk?" then CLM for Risk was designed with you in mind. Identify your application vulnerabilities and prioritize fixes before an external event forces you to. With CLM for Risk, you'll always have an eye on your risk in real-time – and over time.

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