Sonatype

SOLUTION OVERVIEW

NEXUS AUDITOR

Sonatype's Nexus platform helps organizations build better software, even faster. Similar to a manufacturing production line with a supply chain of parts, applications are built by assembling open source and third party components from a wide variety of public and proprietary sources. Assembling software from existing components enables teams to deliver great features faster and more cost effectively. However, the management of components is complex, time-consuming, and can leave organizations vulnerable to security and licensing risks.

In fact, due to the lack of visibility in current development tools, it is not uncommon for an organization to unknowingly use components with critical security defects or license issues, which then require time and money to update or replace them later.

Nexus Auditor provides exceptional visibility, identifying which components are used in your applications and continuously monitoring and reporting on known and newly discovered security vulnerabilities and licensing risks. If your organization 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 Nexus Auditor was designed with you in mind. Identify your application vulnerabilities and prioritize fixes before a breach occurs. With Nexus Auditor, you'll always have an eye on components in real-time—and over time.

KEY BENEFITS

Continuous Visibility

Bill of Materials

In just minutes, Nexus Auditor generates a complete and precise inventory of all open source and third-party components used during builds or in applications. All components are identified by advanced binary fingerprinting and are listed with attributes such as version, age, popularity, potential license issues and known security vulnerabilities. Nexus Auditor eliminates the time-consuming and error prone process of manually inventorying components - including their dependencies – in an effort to determine if you're impacted by a new security vulnerability alert or to check for license issues.

Continuous Monitoring
Nexus Auditor stores the complete inventory of components in your applications and constantly monitors them for newly found security vulnerabilities. When issues are identified, there is an immediate understanding of impact and exposure across the application inventory.

Customizable Dashboards
Sonatype dashboards enable you to visualize risk across your entire organization's application portfolio. Intuitively presented inventory and component intelligence provides a summary assessment and detailed information is available via drill-down reports.

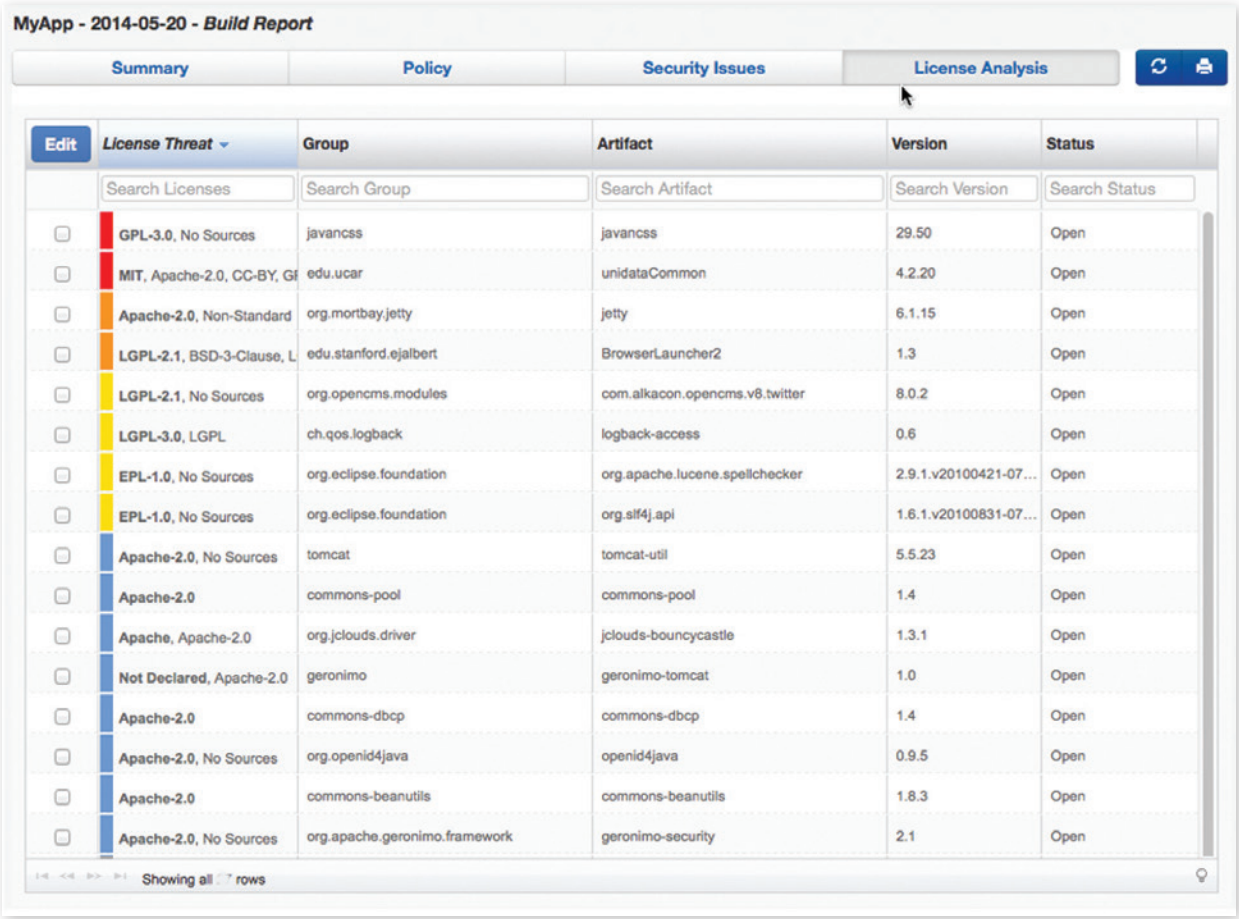
- Newly reported threats are continuously reported in dashboards with prioritization based on impact.
- Proactive notification allows you to respond to policy violations that need immediate attention.
- Comprehensive analysis capabilities include historical trend data, helps assess the overall risk exposure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

Component Identification and Intelligence Data Feed
A key strength of Nexus Auditor lies in its ability to precisely identify your components and match those components against known security vulnerabilities, as well as other data regarding license, component age and most current versions.

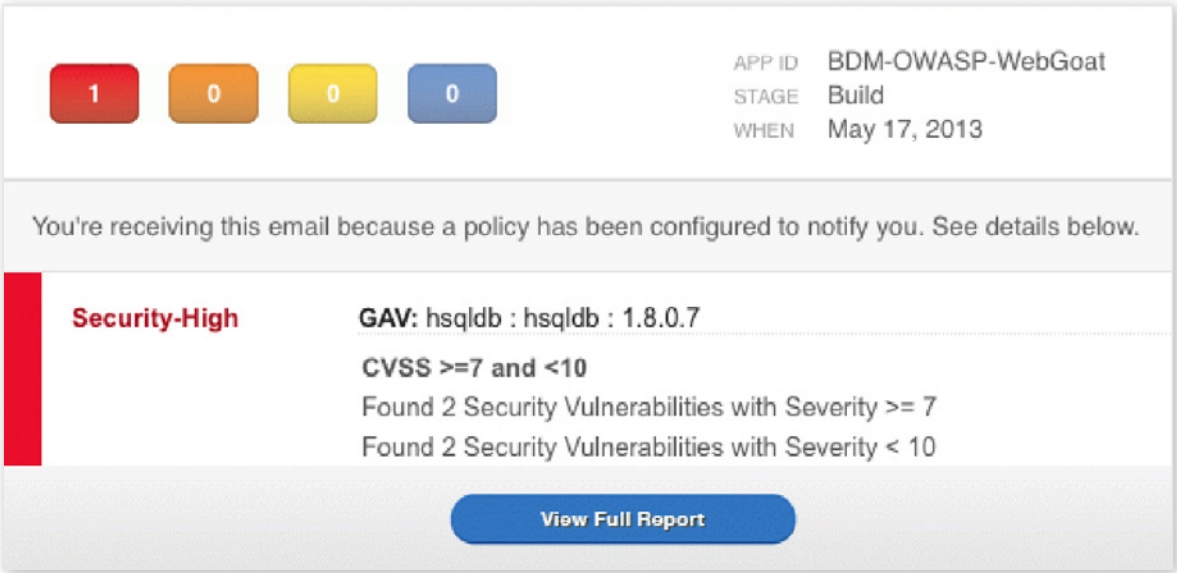
- Unique advanced binary fingerprinting is used to precisely identify your components, including partial/modified matches. This highly accurate process minimizes false positives and false negatives to give you trusted, high quality information without wasted time or effort.
- Sonatype's component intelligence is based on an in-depth, multi-step process for analyzing new security vulnerabilities announced through public and private sources, and identifying the specific component that is impacted.
- Comprehensive licensing intelligence spans both declared and observed license data for all components and component dependencies.

Tailor Policies to Trigger Alerts
Nexus Auditor leverages custom or out-of-the box policies to meet your unique requirements based on application types and departmental needs. The policies are the basis for the automated alerts you receive 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 security team, legal/compliance team, or enterprise architects, eliminating the need for time-intensive coordination.
- Risk profiles can be uniquely built into policies for departmental or application-specific requirements.
- With our other product, Nexus Lifecycle, these policies can be automated to provide guidance and enforce action at each stage in your software life cycle.



With the Bill of Materials feature, Nexus Auditor eliminates the time-consuming and error prone process of manually inventorying components—including their dependencies—in an effort to determine if you're impacted by a new security vulnerability alert or to check for license issues.



Nexus Auditor leverages custom or out-of-the box policies to meet your unique requirements based on application types and departmental needs. The policies are the basis for the automated alerts you receive when new component vulnerabilities are discovered.

NEXUS SOLUTIONS AT-A-GLANCE

Nexus Auditor is one of Sonatype's Software Supply Chain Automation solutions and features the Sonatype IQ Server. To meet the needs and priorities of all organizations, Sonatype offers different integration points so that component intelligence and policy management can be leveraged in different ways across the life cycle. Please use the chart below to compare our various solutions, or for more detailed information go to www.sonatype.com/nexus/try-compare-buy/compare

	Repository Management	Software Supply Chain Automation							
	Repository Manager	IQ Server	Key Integration Points				Additional Integrations		
	Full-featured component warehouse & distribution manager	*Software supply chain intelligence & policy management*	*Repository*	*IDE*	*CI Server*	*Staging/ Release*	*SonarQube*	*Command Line (CLI)*	*Custom (API)*
Nexus Repository	●								
Nexus Auditor		●						●	
Nexus Firewall		●	●			●			
Nexus Lifecycle		●		●	●	●	●	●	●

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