On the Radar: Sonatype

Managing components in the software lifecycle

Reference Code: IT016-001548
Publication Date: 12 Dec 2013
Author: Chandranshu Singh

SUMMARY

Catalyst

Sonatype is a component lifecycle management (CLM) vendor that provides CLM to help organizations create secure component-based applications and keep them secure over time. CLM is aimed at mitigating the security, license, and quality risk associated with the usage of open source components in the application lifecycle. As applications have evolved over time, so has the risk associated with them, with applications the primary vector of attack in most reported security incidents. Attackers often succeed in overcoming application security because development teams don't have a handle on existing security vulnerabilities in third-party code or open source components.

Key messages

- Sonatype helps limit consumption to secure, certified, open source components.
- It integrates with development tools to provide developer-relevant information without switching context.
- It supports faster development of trusted applications by preventing problems early in the development lifecycle
- It provides application vulnerability maps and risk-exposure profiles.
- It automates policy creation and enforcement, and production monitoring for new threats.
- Dashboards provide visibility of overall component risk including a full component inventory by application with an associated risk profile.

Ovum view

The Sonatype solution has grown organically, and the vendor is well positioned to identify, enumerate, and evaluate the risks associated with open source component usage. Sonatype CLM enables organizations to combat these vulnerabilities by managing and monitoring open source component usage, enforcing policy, and enabling fixes for compromised components. In Ovum's view, Sonatype CLM is a must-have tool for DevOps, pure software development, IT security, and legal departments.

RECOMMENDATIONS FOR ENTERPRISES

Why put Sonatype CLM on your radar?

Sonatype CLM is a comprehensive component lifecycle management solution that provides visibility into open source and custom component usage in the organization. It helps identify flawed components and associated risk, as well as providing mitigation paths by providing fixes or suggestions for alternative components. Sonatype CLM follows a lifecycle approach to managing open source component usage. The solution focuses on steps such as secure consumption of components, policy enforcement during development, creating and updating exposure profiles for applications, risk remediation, and threat monitoring in production environments.

Sonatype manages a secure repository of open source components from which development teams can source components as required for development needs. By safeguarding the source of component consumption, Sonatype eliminates a significant amount of risk from the development process. The repository also enables application vulnerability mapping by creating an application composition report that contains details of all components used in the application and their associated vulnerabilities.

In the development workflow, developers start by choosing secure components for their applications from a component intelligence dashboard (integrated with the IDE) that provides detailed information about the selected components, and suggests alternatives for components with significant threat levels. If the developer chooses to remediate risk by choosing an alternative component, the solution automates the migration process.

At the policy governance and enforcement level, Sonatype's approach is non-intrusive. Information required to take action is available in the development tools used by the team. The Nexus Professional repository manager provides application-level risk profiles, and threat summaries for architectural, licensing, and security policies. Threat monitoring in production environments provides a realtime view, as well as a historical trend analysis through an executive dashboard, which is also useful for monitoring policy compliance by the development team.

HIGHLIGHTS

Background

Sonatype was formed in 2008 with the Nexus development team at its core. However, the work in this direction had already begun with the launch of Maven and Maven Central (now The Central Repository) in 2001. The Sonatype team has a strong basis in development focused open source software. By 2006, Maven and Maven Cental had a strong installed base and an active community of contributors. Nexus repository manager was released in 2008, and Sonatype was formed soon after. The company raised capital in rounds of funding that received participation from several leading venture capitalist firms. The latest round raised $25m, with investment led by NEA. In 2012, Sonatype announced the Component Lifecycle Management solution, which was formally released in March 2013.

Current position

Ovum believes that vulnerabilities introduced by open source component usage are on the rise. Furthermore, these vulnerabilities have a cascading effect due to the nature of software development in modern enterprises. Most software is assembled from reusable components rather than developed from scratch, which was the case a couple of decades ago. Predictably, the usage of open source components and third-party code libraries has also grown over time. Therefore, the open source dependencies have multipled, as well as the vulnerabilities when the flawed components are transferred to application software worldwide using the components.

With a growing focus on application security, which has now come to mean building secure applications by incorporating security concerns early in the development lifecycle, products such as Sonatype CLM will be increasingly relevant to enterprise development teams. Organizations need to identify security vulnerabilities in the code itself and remove them before the code is shipped or deployed to production. With the changing nature of software development, IT leaders have come to realize that introducing secure development practices is only the tip of the iceberg because it covers custom-developed code and/or vendor supplied code. However, most of the vulnerabilities reside in open source components extensively used by development teams, and organizations often have no coherent strategy for governing the usage of these components in the development process. In Ovum's opinion, Sonatype fills this gap quite well.

From a market perspective, Sonatype targets the components layer in an application's architecture. These components could be proprietary (custom-developed) or sourced from third parties (frameworks, libraries, utilities, and so on) as well as open source. The vendor collects metadata on a wide range of components used in the development lifecycle, and assesses the threat level associated with each component. This component level information is then used to generate exposure profiles for applications in an organization's portfolio. The metadata is collected from the Central Repository as well as from third party sources including several vulnerability tracking and testing tools, from open source communities, and also directly from customer environments. With such extensive data gathering, Sonatype CLM is well positioned to provide actionable intelligence on component usage throughout the lifecycle; from limiting consumption to certified components to providing remediation advice downstream, as well as monitoring for new threats in production environments.

The product has been launched recently, and field deployment examples are awaited.

DATA SHEET

Key facts

Table 1: Data sheet

Product name	Sonatype CLM	**Product classification**	Component lifecycle management, ALM, software development, DevOpsSec
Version number	1.6	**Release date**	March 2013
Industries covered	All industries, all organizations with development teams (in-house or vendor-supplied)	**Geographies covered**	All
Relevant company sizes	All	**Licensing options**	On-premise, PaaS
URL	http://www.sonatype.com	**Route(s) to market**	Direct sales
Company headquarters	Fulton, Maryland US	**Number of employees**	60+

Source: Ovum

APPENDIX

"On the Radar"

"On the Radar" is part of Ovum's series of research notes that highlights up-and-coming vendors that bring innovative ideas, products, or business models to their markets. Although "On the Radar" vendors are not always ready for prime time, they bear watching for their impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

Code Analysis for Reliable and Secure Aplication Development, IT016-001449 (June 2012)

Author

Chandranshu Singh, Senior Analyst (Ovum Software – IT Solutions)

chandranshu.singh@ovum.com

Disclaimer

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions, and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.