Frequently Asked Questions

What are HP and Sonatype announcing?

Sonatype and HP announced on February 24th, 2014, that Sonatype's Component Lifecycle Management (CLM) analysis technology has been integrated into HP's cloud-based software security solution – HP Fortify on Demand. HP Fortify on Demand customers will have access to an Open Source Application Scan using the Sonatype CLM analysis technology from directly within the Fortify on Demand user experience.

HP Fortify on Demand delivers comprehensive, accurate and affordable security assessments that identify vulnerabilities in any application —web, mobile, infrastructure or cloud. Sonatype provides analysis and identification of third party and open source components commonly used as building blocks in modern applications – with a focus on security, license, quality, and policy issues. Together, these capabilities deliver a new level of visibility and analysis into overall application security and risk.

Why should I care?

HP and Sonatype provide you with the next level of application visibility

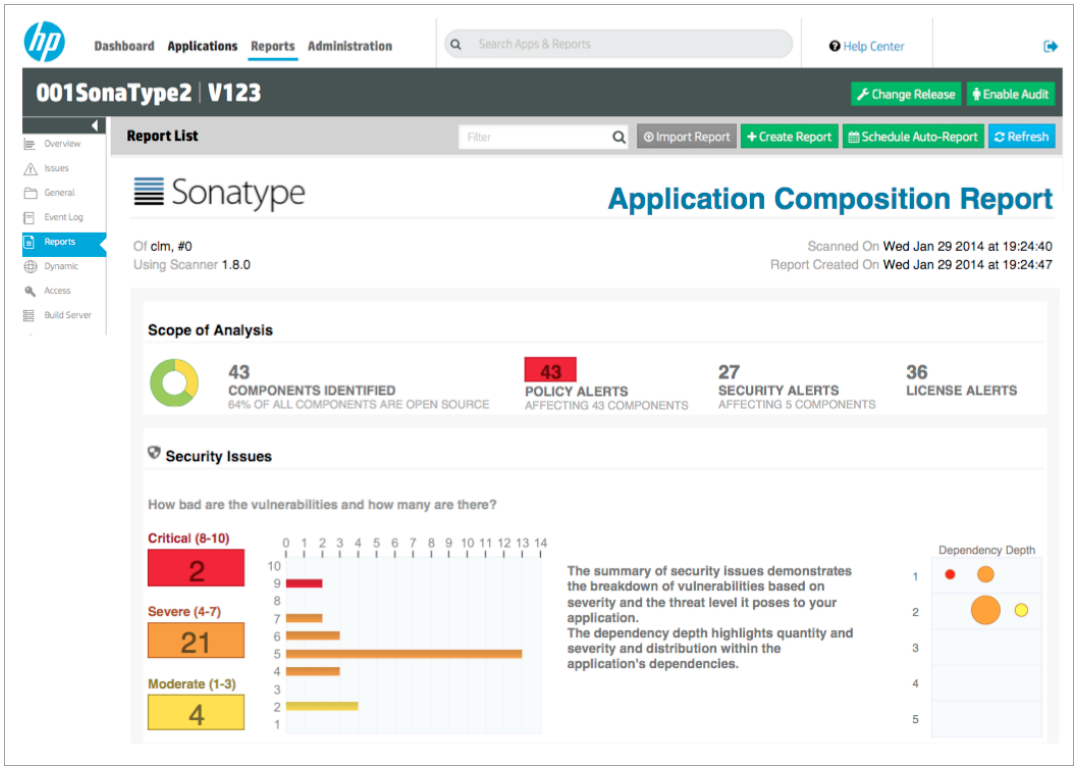
- The unified HP and Sonatype solution delivers on-demand (cloud-based) security testing for any application and deeper visibility into its open source components.
- This represents the industry's first on-demand application security solution providing a combination of Static, Dynamic, and Open Source Risk analysis.
- HP Fortify on Demand now offers a new risk analysis report for open source and third party components.

The new Fortify on Demand "Sonatype Open Source Report" provides visibility into 3rd party and Open Source component risk in just 5 minutes.

- Simply upload, test, and review.
- The Sonatype report outlines potential security, licensing, quality and policy problems in open source and third party components within minutes.
- In addition to Fortify on Demand's application security testing solutions to identify vulnerabilities leveraging mobile, static and dynamic testing, the Sonatype Open Source Report complements those results with the addition of known open source vulnerabilities and the identification of open source components in your application.

If you are using risky components, your applications are at risk

- With 90% of a typical application being composed with open source and third party components, we recognize that the open source component risk vector is growing.
- In 2013, there were 13 billion downloads of open source components from the Central Repository, one of the largest web repositories, for use in application development. 46 million vulnerable components were downloaded. If you are using one of these components anywhere, your applications are at risk.
- Visibility into the vulnerabilities in these components is a top concern of Security, DevOps, Developers, Risk/Compliance, and Legal professionals.
- Concerns over component vulnerabilities are now high on the priority list for standards bodies, such as the Open Web Application Security Project (OWASP), Payment Card Industry (PCI) and the Financial Services Information Sharing and Analysis (FS-ISAC) whose guidelines now state that components with known vulnerabilities must be avoided.



HP Fortify on Demand delivers deeper application analysis with the Sonatype Open Source report by Sonatype. A sample of the complete eight page report is shown above.

When was the announcement?

A Sonatype press release, with HP's full participation, was issued announcing the partnership at the RSA Show on February 24, 2014. Find the press release here.

HP Fortify on Demand's expanded security solution was highlighted throughout the RSA 2014 Conference including in the HP booth theater, at the Fortify pod within the HP booth, at the Sonatype booth, within several RSA sessions led by Sonatype experts, and through a variety of HP and Sonatype online media channels (e.g., LinkedIn, Twitter, Facebook, and Blogs).

Where and when can I find information online?

You can find information on the announcement and the new Fortify on Demand capabilities on the HP Fortify on Demand (beginning March 15) and Sonatype (available now) solution web pages.

Information will also be posted across these Sonatype social channels: LinkedIn, Twitter, Facebook, and Blogs.

When will this integration be available and what will be delivered?

The first phase of the integration is available now within HP Fortify on Demand.

Fortify on Demand customers will have access to the Sonatype Open Source report through HPFOD.com. This is a value added offering only available to Fortify on Demand customers.

A copy of a sample report with callout descriptors of the data provided is available for your review here.

Will there be a cost for the announced Sonatype functionality to HP Fortify on Demand customers?

No. The Open Source report using the Sonatype CLM analysis functionality will be included in the price of the HP Fortify on Demand scans.

What problem are HP and Sonatype solving?

Organizations want visibility into both the security vulnerabilities that exist in their application code, as well as known security and license vulnerabilities in open source components used within their applications. to ensure their applications are trustworthy.

Ninety percent of a typical application is developed using third-party and open source components pulled from the web with little visibility to security vulnerabilities, licensing constraints, policy violations or quality of the components.

Concerns over component vulnerabilities are now high on the priority list for standards bodies, such as the Open Web Application Security Project (OWASP), Payment Card Industry (PCI) and the Financial Services Information Sharing and Analysis (FS-ISAC) whose guidelines now mandate that components with known vulnerabilities must be avoided.

For organizations that need to launch a security program quickly, scale to get all applications tested, and want to manage risk for applications, HP and Sonatype provide a new breed and depth of application security testing to help them.

Who is Sonatype?

Sonatype has been on the forefront of creating tools to manage, organize, and better secure third party and open source application components since its founder created Maven and the (Maven) Central Repository in 2001. More than 20,000 customers rely on Sonatype's Nexus Repository Manager and Component Lifecycle Management (CLM) to manage their open source and third party components across software development and production environments.

In 2013, over 70,000 companies downloaded more than 13 billion open source components from the (Maven) Central Repository for use in their custom-developed applications. Approximately 90% of today's typical application is built using these third party or, open source components, demonstrating the explosive growth of their use in software development.

Sonatype is the leader in Component Lifecycle Management, helping companies pick the best components from the start to make it easy to create trusted applications and keep it that way over time. 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.

Is the Sonatype CLM functionality within Fortify on Demand all that Sonatype sells?

No, the Sonatype Open Source Report is a subset of their overall CLM product offering. While important, as it shows the potential vulnerabilities in open source / third party components at a single point in time, the core of Sonatype's solution addresses the remediation and monitoring of these components throughout the software lifecycle.

What is Component Lifecycle Management (CLM)?

Every day, millions of developers build software applications from open source building blocks, known as components. Businesses and government organizations rely on Sonatype software to select and use the best components (the least vulnerable, highest quality, most compliant licenses) from the start of the development lifecycle to ensure that trustworthy applications can also meet fast-paced release deadlines. Policy automation, ongoing monitoring, and proactive alerts ensure these applications remain secure over time—throughout the software development and production lifecycles.

You can learn more about Sonatype CLM in this whitepaper and eBook.

Who is HP Fortify / Fortify on Demand?

In 2013, HP was recognized as an IT leader in the Application Security Testing (AST) market by Gartner. By bringing together SPI Dynamic and Fortify Software, HP was instrumental in the creation of a combined category that includes both static and dynamic application security testing.

Additional information about HP Fortify as a leader in the 2013 Magic Quadrant for Application Security Testing can be found here.

HP Fortify on Demand is "security as a service" that enables organizations to assess and remediate vulnerabilities quickly without spending time and resources building in-house security and threat expertise. HP Fortify on Demand is easy to manage, fast, and compliant offering the greatest flexibility for the security of all of your application assets. Secure your applications in the cloud, quickly kick off assessments, pass compliance like PCI, HIPPA, FISMA, and more, for unlimited users for all of your desktop, web, and mobile applications. Your security team of experts, HP Fortify on Demand offers a single cloud access view into the security of all of your application assets with complete dash-boarding, executive level reporting, issue-by-issue details including

remediation information. HP Fortify on Demand helps you know what to secure within your applications and how to better secure the application, as early in your development lifecycle possible.

Want to learn more about HP Fortify on Demand?
Take a look at this SlideShare presentation.