PeerSpot

PeerPaper™ Report 2024

Increase Developer Velocity While Mitigating Risk With Fortify and Sonatype

sonatype

Fortify by opentext™

Contents

Introduction

Use of open-source software (OSS) has become non-negotiable in software development today. This has not been a risk-free proposition, however. There were twice as many supply chain attacks in 2023 as there were in the years 2019 to 2022 combined. Custom code can also be the cause of security risk, as vulnerabilities get embedded into software making its way through the DevSecOps pipeline. It's not good news for developer teams and their partners in security and quality assurance (QA). Everyone is expected to produce software more quickly than ever before, just as an increased security workload creates a drag on productivity for developers and quality assurance (QA) teams.

Developers, security staffers, and QA stakeholders need a way to speed up software development while getting better at mitigating risks in custom code and OSS. One approach that is gaining traction involves adopting a holistic combination of software composition analysis (SCA), which mitigates security and legal risk in OSS and third-party components, and static application security testing (SAST), which discovers security flaws in custom code.

This paper explores how this joint approach can succeed in accelerating software development while improving risk reduction. It is based on the experiences of PeerSpot members who use Fortify Static Code Analyzer for SAST and Sonatype Lifecycle for SCA. Users describe how the two solutions come together for faster DevOps and mitigate risk.

Maurizio G.
Senior manager at a consultancy with 11-50 employees

Sonatype acts as a mandatory gatekeeper for accessing open-source libraries. Combining Sonatype and Fortify provides an invaluable holistic view of the application code developed by the factory.

READ REVIEW

Overview: A Holistic Solution for Higher Developer Velocity With Less Risk

PeerSpot members are finding that the combination of Fortify Static Code Analyzer and Sonatype Lifecycle comprises a holistic solution that enables them to increase developer velocity as they reduce risks affecting custom and open-source code. Developer velocity is a measure of how much work a developer can perform in a given timeframe.

Regarding risk reduction, the Head of Audit, Compliance & Cybersecurity Practice at a small consultancy explained, "Sonatype acts as a mandatory gatekeeper for accessing open-source libraries. Combining Sonatype and Fortify provides an invaluable holistic view of the application code developed by the factory."

In his case, Sonatype "effectively identifies vulnerabilities lurking within the open-source components." This, he added, "offers significant value to developers who rely on these libraries, as it helps ensure their work is not compromised by unforeseen vulnerabilities. This information acts as a boost for developers, enabling them to leverage the library's functionality with greater confidence. The combination works like a black box for the developer. Sonatype and Fortify complete each other."

An Adjunct Professor at the University of Maryland had a similar experience. He said, "The value that combining Fortify and Sonatype is that we use Fortify as a SaaS analysis tool. We review static code and Sonatype allows you to find vulnerabilities."

In terms of developer velocity, the consultancy's Head of Audit remarked, "We've reduced the time to market of the implementation phase by 50%. We can test the applications faster, and we can support a number of projects with the same number of people."

Speeding up testing with automation is a big time saver, as a Security DevOps Engineer at a financial services firm found. His team can complete a dynamic scan in around 20 minutes. "However," as he said, "this turnaround time is significantly faster than relying on the entire security team to conduct manual testing."

Maurizio G.
Senior manager at a consultancy with 11-50 employees

"

Helps us reduce risk exposure on applications through the discoverability of vulnerabilities and weaknesses.

READ REVIEW

Reducing Risk

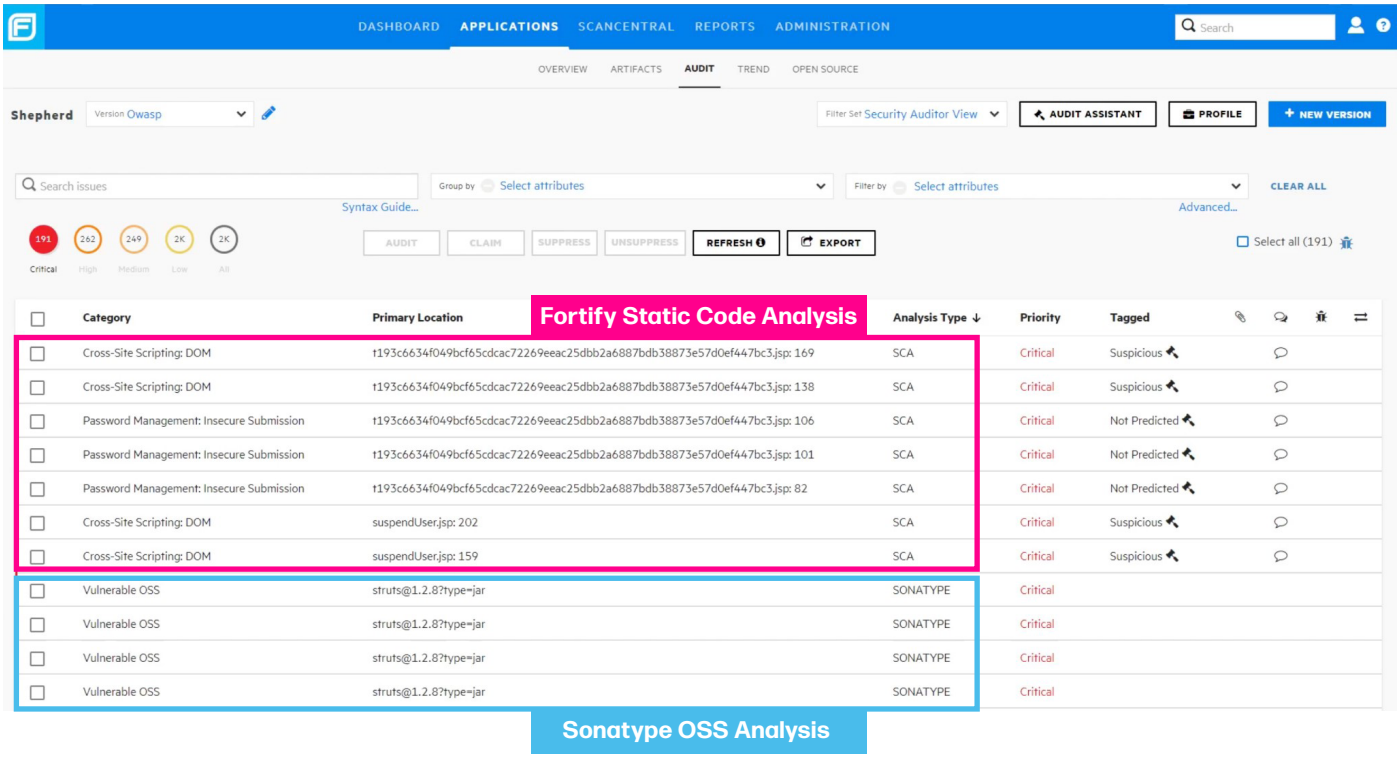
Risk reduction is half the battle of DevSecOps. As users discovered, the joint Fortify/Sonatype solution achieves this aim by providing visibility, identifying vulnerabilities—and then remediating them—while also maintaining compliance. Figure 1, a screenshot of Fortify Software Security Center, illustrates how the solution identifies vulnerabilities in static code and OSS and displays them in a single dashboard for rapid remediation.

Getting better at risk reduction in OSS is necessary because only 11% of open source projects are actively maintained. It's simply imperative to track the health of dependencies over time. To this end, Fortify users like a Software Analyst at a financial services firm revealed that the solution helped them identify vulnerabilities and weaknesses and reduce their risk exposure. The consultancy's Head of Audit similarly stated that Fortify "helps us reduce risk exposure on applications through the discoverability of vulnerabilities and weaknesses."

For a VP of Cybersecurity who uses Fortify Static Code Analyzer at a financial services firm, the Fortify portal "is well-suited for managing and tracking risks associated with the open-source components used in our software projects."

FIGURE 1

Screenshot of Fortify Software Security Center, which identifies vulnerabilities in static code and OSS for rapid remediation.



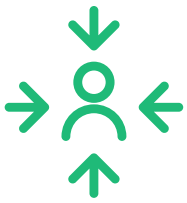
Category	Primary Location	Analysis Type	Priority	Tagged
Cross-Site Scripting: DOM	f193c6634f049bcf65cdcac72269eeac25dbb2a6887bdb38873e57d0ef447bc3.jsp: 169	SCA	Critical	Suspicious
Cross-Site Scripting: DOM	f193c6634f049bcf65cdcac72269eeac25dbb2a6887bdb38873e57d0ef447bc3.jsp: 138	SCA	Critical	Suspicious
Password Management: Insecure Submission	f193c6634f049bcf65cdcac72269eeac25dbb2a6887bdb38873e57d0ef447bc3.jsp: 106	SCA	Critical	Not Predicted
Password Management: Insecure Submission	f193c6634f049bcf65cdcac72269eeac25dbb2a6887bdb38873e57d0ef447bc3.jsp: 101	SCA	Critical	Not Predicted
Password Management: Insecure Submission	f193c6634f049bcf65cdcac72269eeac25dbb2a6887bdb38873e57d0ef447bc3.jsp: 82	SCA	Critical	Not Predicted
Cross-Site Scripting: DOM	suspendUser.jsp: 202	SCA	Critical	Suspicious
Cross-Site Scripting: DOM	suspendUser.jsp: 159	SCA	Critical	Suspicious
Vulnerable OSS	struts@1.2.8?type=jar	SONATYPE	Critical	
Vulnerable OSS	struts@1.2.8?type=jar	SONATYPE	Critical	
Vulnerable OSS	struts@1.2.8?type=jar	SONATYPE	Critical	
Vulnerable OSS	struts@1.2.8?type=jar	SONATYPE	Critical	

VISIBILITY / 360-DEGREE VIEW

Reducing risks starts with being able to spot them. The combined Fortify/Sonatype solution operationalizes this idea with a 360-degree view of the risk environment. The University of Maryland's Adjunct Professor described it like this: "As a security analyst, I like the management view. From there, you can review the code and review findings in order to approve, deny, or recommend."

He went on to say that the Fortify Software Security Center, which acts as a portal, "is quite useful. It's a good overview. You can really see what's happening after you've developed something." On a related, note, the consultancy's Head of Audit found the Fortify on Demand Portal to be "quite useful" because "It helps centrally manage everything and provides us with a 360-degree view of our AppSec team."

The Software Security Center also stood out as the solution's most effective feature to a VP of CyberSecurity in the financial services industry. He said, "This on-premises portal, included with their primary SaaS offering, streamlines the process of triaging our results. With thousands of daily active users, the Software Security Center serves as a



Centralized Management

centralized platform, consolidating results from various tools, including Sonatype, Fortify WebInspect's DAST results, and Pen Test findings from our internal team."

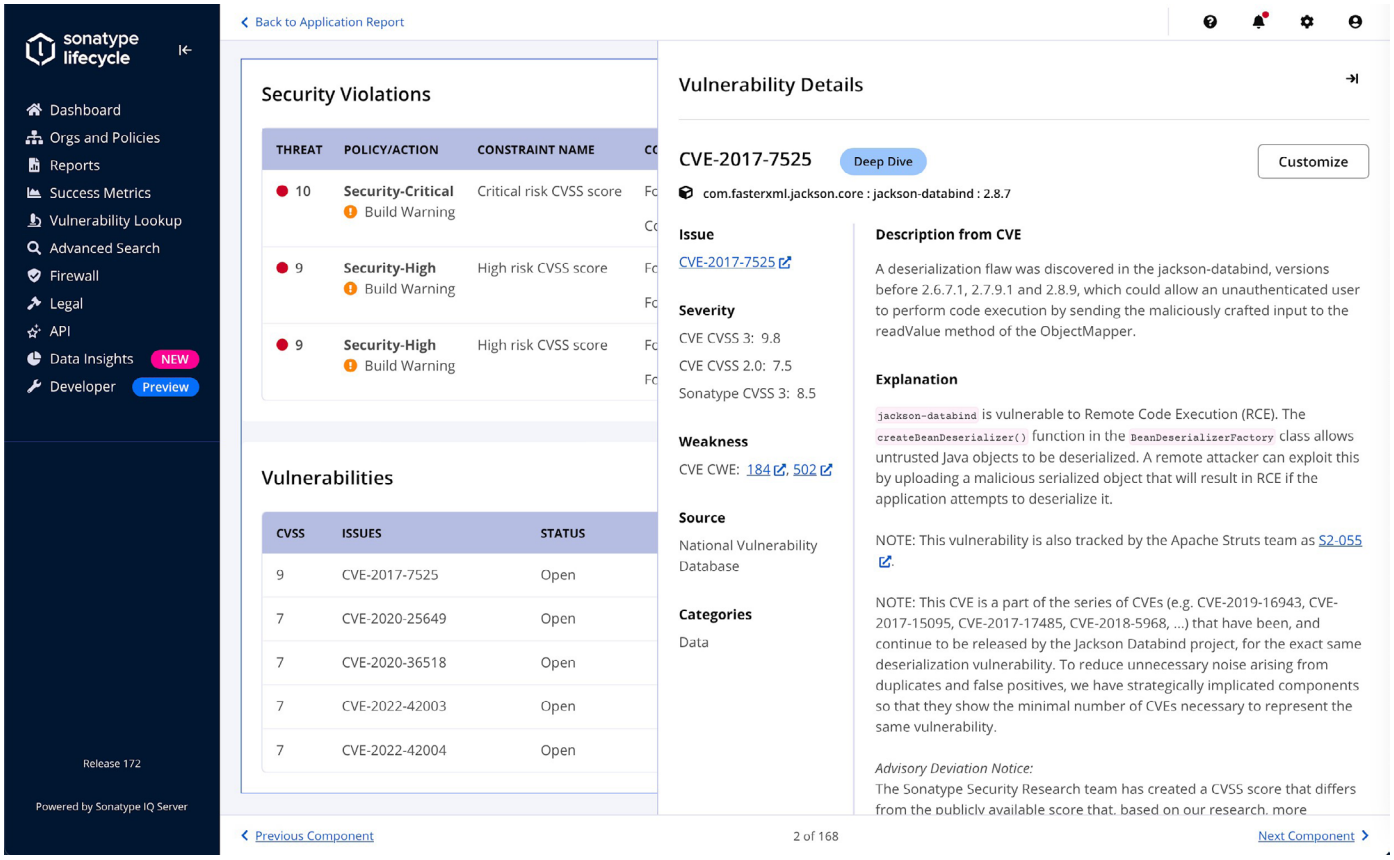
From there, he said, "This unified view eliminates the need for developers to log into multiple portals to access code vulnerabilities, open-source issues, web app scans, and Pen Test results. Instead, they can access everything they need from a single, convenient location."

"I really like Fortify Software Security Center," said a Sr. Cyber Analyst at a power utility. His team can get insights into the security of applications instantly from a single pane of glass, and then "go there straight away and check that information." He added, "We can scan the code and push the results. I can also see all the applications. I know the portfolio of the applications that we have. I can see all the information about the organizations, the code, and the developers in one spot."

IDENTIFICATION OF VULNERABILITIES

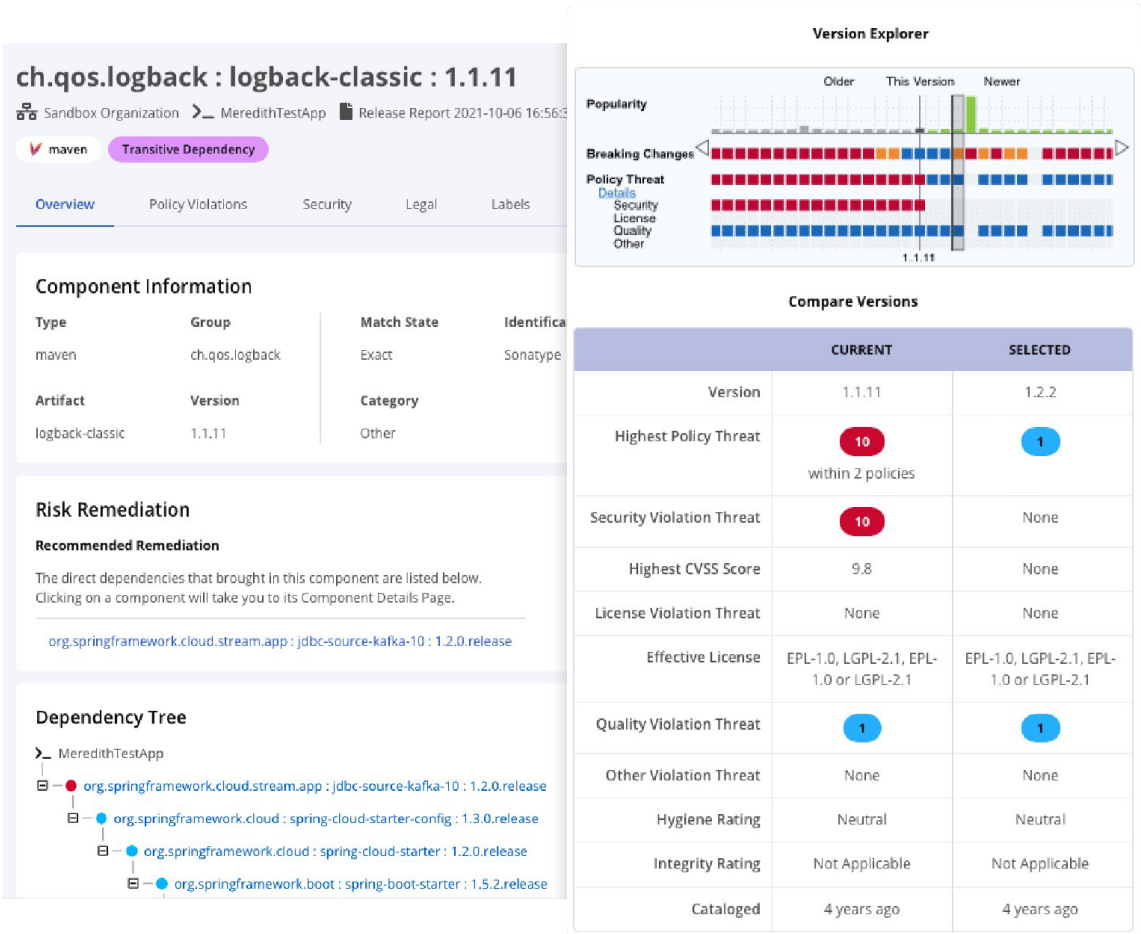
Improving risk reduction outcomes in DevSecOps also relies on the identification of vulnerabilities. After all, it's impossible to remediate a vulnerability without knowing what it is. To this end, Sonatype Lifecycle allows a Technical Manager at a financial services firm with over 1,000 employees to check their third-party code libraries for vulnerabilities. A Technical Consultant at a software company simply stated, "The most important features of the Sonatype Nexus Lifecycle are the vulnerability reports."

A Vice President of Application Security for North America at BNP Paribas, a financial services firm, explained how Fortify SAST reviews the source code or compiled binary code without executing the application, "This helps in identifying vulnerabilities, coding errors, and security issues within the codebase."



The solution's comprehensive set of security rules and patterns further helps identify vulnerabilities, including issues related to the Open Web Application Security Project (OWASP) Top Ten, CWE (Common Weakness Enumeration), and other industry standards. In his case, getting to success requires supporting a wide range of programming languages, including Java, C/C++, C#, and Python. He added, "This broad language support makes it suitable for various development environments."

For a Vice President, Cybersecurity at a financial services firm, visibility manifested as "Fortify provides robust details about the issues, along with comprehensive insights into what needs to be fixed." He then said, "The ability to see all of the different versions in Sonatype results has been particularly helpful as an indicator."



MAINTAINING COMPLIANCE

Becoming compliant with government regulations and industry frameworks is part of the vulnerability mitigation process for software in a range of industries and government use cases. Compliance rules may specify that software makers create software bills of materials (SBOMs). Software purchased by government agencies is one example. The developers need to know what open-source code they've put into the applications and document it. Sonatype Lifecycle solves for this need, offering the ability to build, ingest, monitor, and manage SBOMs.

Users of the Fortify/Sonatype combined solution found it to be helpful with compliance in general. For example, a Vice President, Cybersecurity at a financial services firm said, "Both Fortify and Sonatype have excellent integrations with compliance frameworks such as GDPR, PCI, and DSS, providing comprehensive reporting capabilities that help us meet regulatory requirements."

He then commented that the integrations "enable us to stay abreast of evolving regulatory requirements and ensure that our vendor partners promptly address any changes." He cited the example of OWASP updating its categories, a move that prompted a quick release of support for the new categories by Fortify and Sonatype. This allowed his team "to seamlessly update our reporting without delay."

"Fortify and Sonatype help maintain compliance with the applicable regulations," said the University of Maryland's Adjunct Professor. His team mostly uses Sonatype for compliance and licenses. "By combining both solutions together," he added, "it enables you to solve a lot of issues that may occur in the future.

Vice President
Cybersecurity at a financial services firm with 10,001+ employees

"

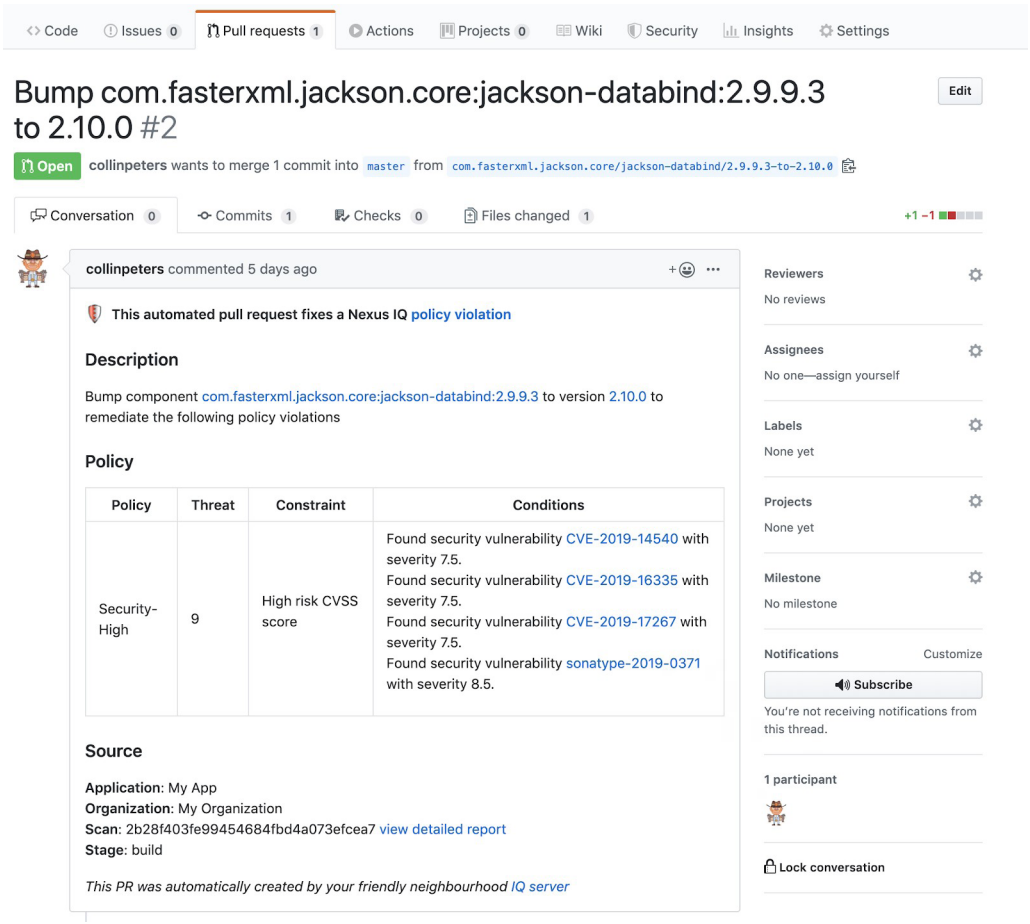
Both Fortify and Sonatype have excellent integrations with compliance frameworks such as GDPR, PCI, and DSS, providing comprehensive reporting capabilities that help us meet regulatory requirements.

READ REVIEW

REMEDIATION OF POTENTIAL VULNERABILITIES

Remediation is the last, critical step in mitigating vulnerabilities. Regardless of whether vulnerabilities are in source code or OSS components and packages, Sonatype and Fortify have teams fully covered. Fortify and Sonatype can help remediate vulnerabilities once they are identified. According to the University of Maryland's Adjunct Professor, the solution provides a level of detail that is "very informative" in this regard. He said, "It provides you with recommendations on how to fix items. And they provide you with other resources available for how to address the issues. You can also see the root cause."

Vulnerability Mitigation



The Sr. Cyber Analyst at the utility explained how Fortify SAST helps remediate potential vulnerabilities by using accurate and reliable results. He said, "I like that they use standards such as OWASP Top 10 or SANS Top 25. They are very good at this. When it finds any vulnerabilities, it shows you by the rank. You can filter by so many standards. It gives you a description of the vulnerability as well as recommendations on how to fix it. It also gives you some references if you want to read more."

Other notable comments about the combined solution's ability to remediate potential vulnerabilities included:

"When Fortify is on-premises with GitHub, remediation is easy. They can suggest and resolve issues directly. Fortify can offer guidance to the development team. So it's not only an identification tool, it's also a tool that can provide remediation for potential vulnerabilities." - Head of Audit, Compliance & Cybersecurity Practice who uses Fortify Static Code Analyzer at a small consultancy

"Fortify mitigates risk exposure in applications by identifying vulnerabilities and weaknesses. It pinpoints all the issues that developers need to address and provides comprehensive guidance for remediation." - Vice President, Cybersecurity who uses Fortify Static Code Analyzer at a financial services firm

Maurizio G.

Senior manager at a consultancy with 11-50 employees

"

It helps centrally manage everything and provides us with a 360-degree view of our AppSec team.

READ REVIEW

Increasing Developer Velocity

Whether it's about time to market or completing internal feature releases, development organizations tend to be interested in improving their developer velocity. Faster is almost always better, assuming no tradeoffs in quality or security. As users of the Fortify/Sonatype combined solution have discovered, it helps with developer velocity.

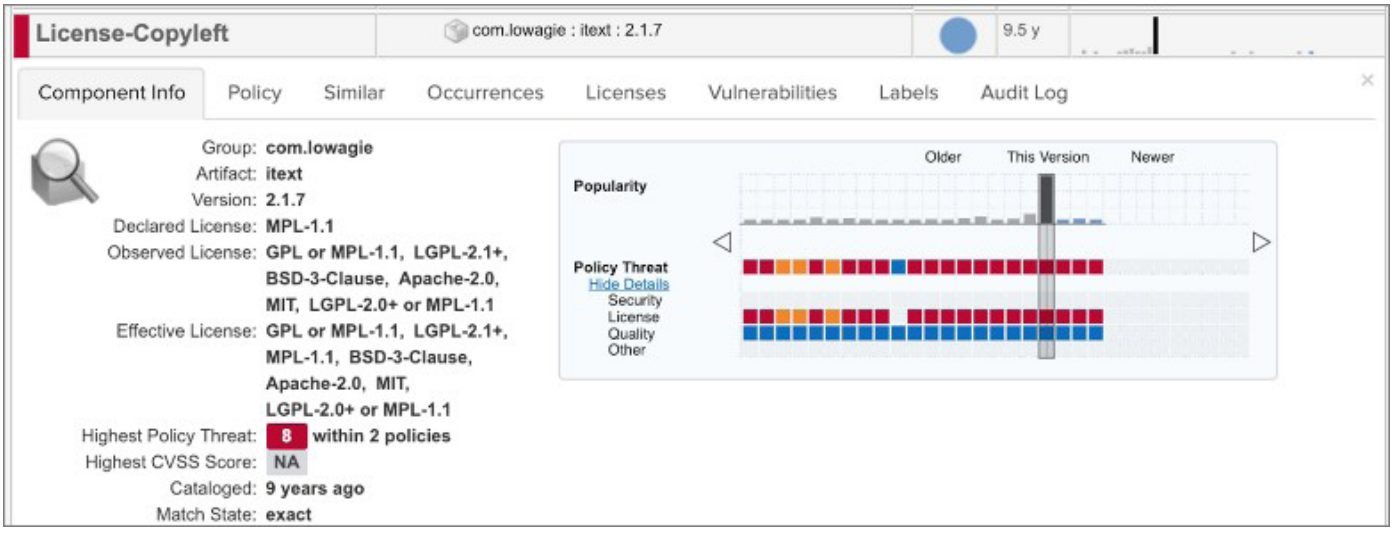
Factors that speed up development, as enabled by Fortify/Sonatype combined solution, include improving developer productivity, integration with other solutions, and real time feedback. Ease of use also helps everyone work more quickly. Securing the software supply chain can contribute to developer velocity as well. The fewer supply chain concerns that developers and QA teams have to deal with, the faster the entire process will go. As all of these elements of developer velocity come together, innovation should improve, too.

IMPROVE DEVELOPER PRODUCTIVITY

A Software Engineer at a manufacturing company felt that the solution "has definitely increased developer productivity." She elaborated, saying, "If you manually download a package, you're not sure if it is the right package because you cannot test it. But now, we can automatically download packages. It's much more effective and more productive for each software developer using it. I would estimate we have seen a 20 percent increase in productivity."

Increases Developer Productivity

Sonatype and Fortify generate synergy that enhances DevSecOps productivity. By integrating Sonatype's advanced component intelligence and dependency management with Fortify's robust SAST capabilities, development teams can be efficient in addressing AppSec challenges throughout the software development lifecycle.



Sonatype excels in providing comprehensive visibility into open-source components. It identifies potential vulnerabilities and license issues early in the development process. Fortify SAST complements Sonatype by performing in-depth static analysis on custom code, uncovering security flaws before they escalate. Together, this powerful combination not only strengthens the security posture of applications but also streamlines the development pipeline.

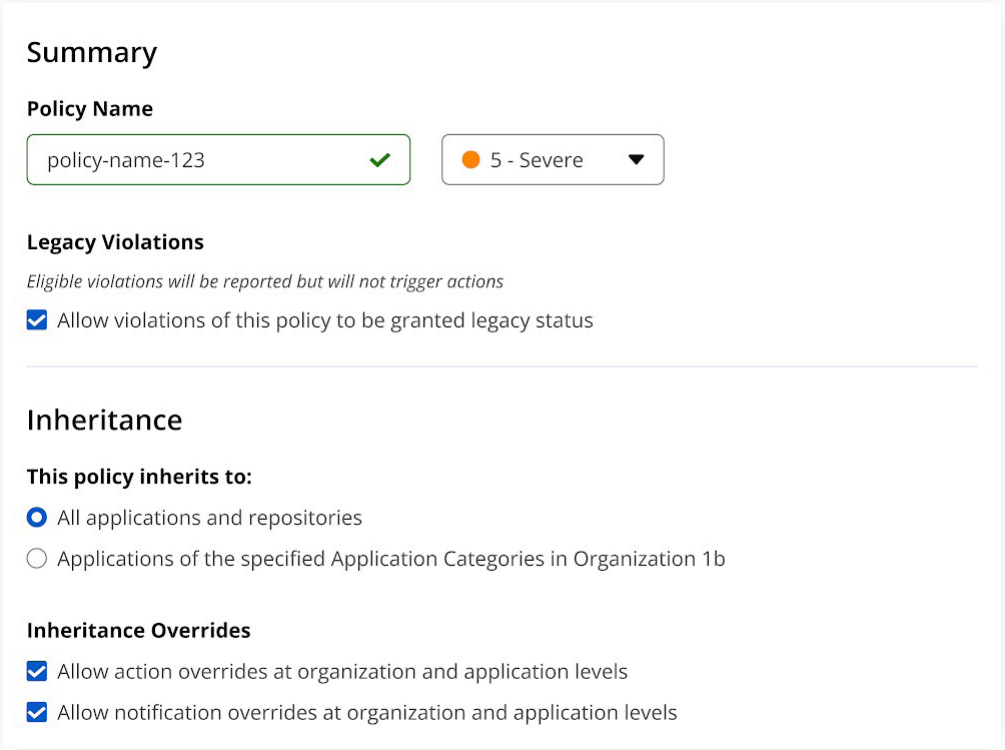
The University of Maryland's Adjunct Professor offered an example, saying, "Fortify helped us to free up staff time since it helps us resolve issues faster." The financial service firm's Software Analyst likewise noted, "Fortify SAST has helped free up around 20 percent of our employees' time to work on other projects."

Jumani B.
Adjunct at University of Maryland

"

Fortify and Sonatype help maintain compliance with the applicable regulations.

READ REVIEW

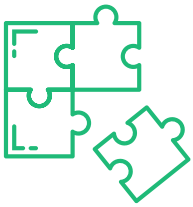


INTEGRATION WITH OTHER SOLUTIONS

DevSecOps, as its name suggests, is highly integrative in nature. To work, the systems underpinning DevSecOps must interoperate. And, developer velocity picks up when it's easy to integrate those systems. Stakeholders do not have to spend as much time setting up integrations and managing them.

The Fortify/Sonatype solution proved itself in this regard. For example, as the manufacturing company's Software Engineer remarked, connecting the solution to the integrated development environment "was quite easy because you just have to download the plugins and then set up the URL and the user and password."

She elaborated, discussing the solution's integration with the Eclipse IDE, the WebStorm Javascript IDE, and Microsoft Visual Studio. She said, "You just need to set up a project or an app and then you just make the connection in all the tools you're using."



Ease of Integration

BNP Paribas' Vice President of Application Security for North America also integrates Fortify with various IDEs, as well as with continuous integration/continuous delivery (CI/CD) pipelines. He said, "This allows developers to scan code seamlessly."

REAL TIME FEEDBACK

The Sonatype/Fortify combination delivers real-time user feedback that helps developers move the DevSecOps process along more rapidly. Sonatype sends out instant alerts about OSS component risks, while Fortify quickly pinpoints security flaws in custom code. As the financial service firm's Software Analyst revealed, "I can perform a scan and immediately see our current situation. This allows me to quickly assess if our coding practices are effective or if we need to stop and address any issues before they become bigger problems."

With real-time feedback, the Sonatype/Fortify solution acts like a "tag team," a sort of "one-two punch" that turbocharges security while also supercharging the development workflow. DevSecOps teams get instant insights, actionable intel, and the power to squash vulnerabilities on the spot. As a result, developers can move more quickly while focusing on innovation.

The financial service firm's Software Analyst revealed, "I can perform a scan and immediately see our current situation. This allows me to quickly assess if our coding practices are effective or if we need to stop and address any issues before they become bigger problems."

Real Time Feedback

Real time feedback helps the consultancy's Head of Audit realize "efficiency in the deployment of the application" because, "It makes code review much easier pre-deployment."

EASE OF USE

Both Sonatype and Fortify are designed with a focus on ease of use. The solution provides development teams with accessible and intuitive interfaces that help stakeholders perform tasks quickly. As a Code Reviewer at HQ USMEPCOM, a small government agency, shared, "The GUI is really easy to navigate through and is very user-friendly." University of Maryland's Adjunct Professor offered a similar take, saying, "It's pretty easy to find vulnerabilities. Then, you go to the source. It is very good at tracking to see where the data or the issue enters into your source code so you can track it or go back to where it started."

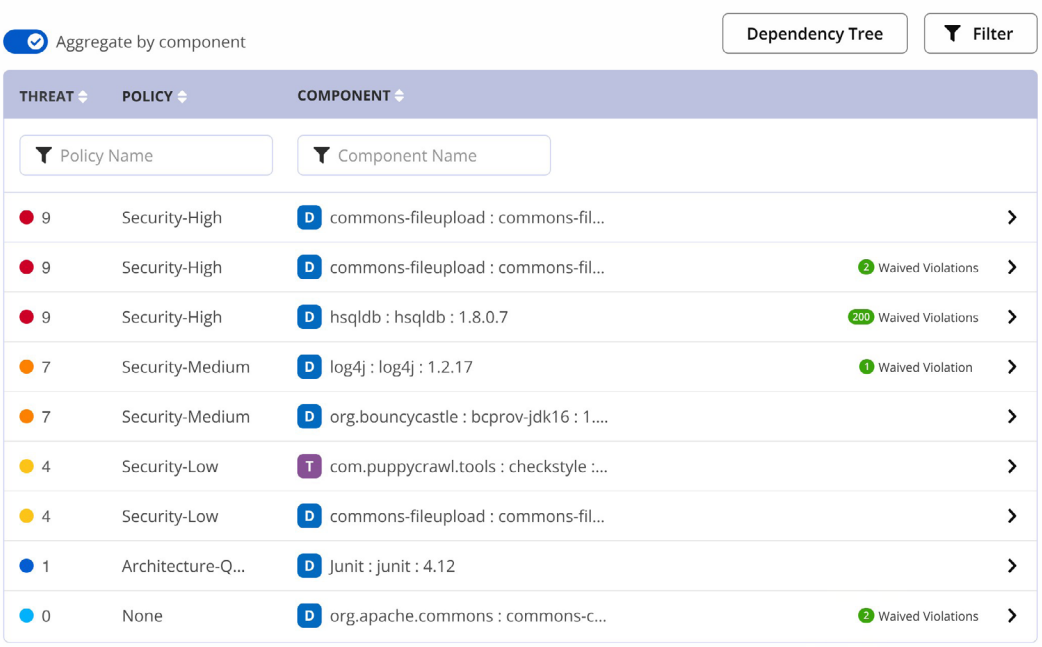
Sonatype simplifies the management of open-source components by offering clear visibility into dependencies and vulnerabilities. Its user-friendly dashboards and actionable insights empower developers to make informed decisions effortlessly. Fortify also maintains a user-friendly environment with straightforward configurations and result interpretations.

Renee S.
Code Reviewer at HQ USMEPCOM

"

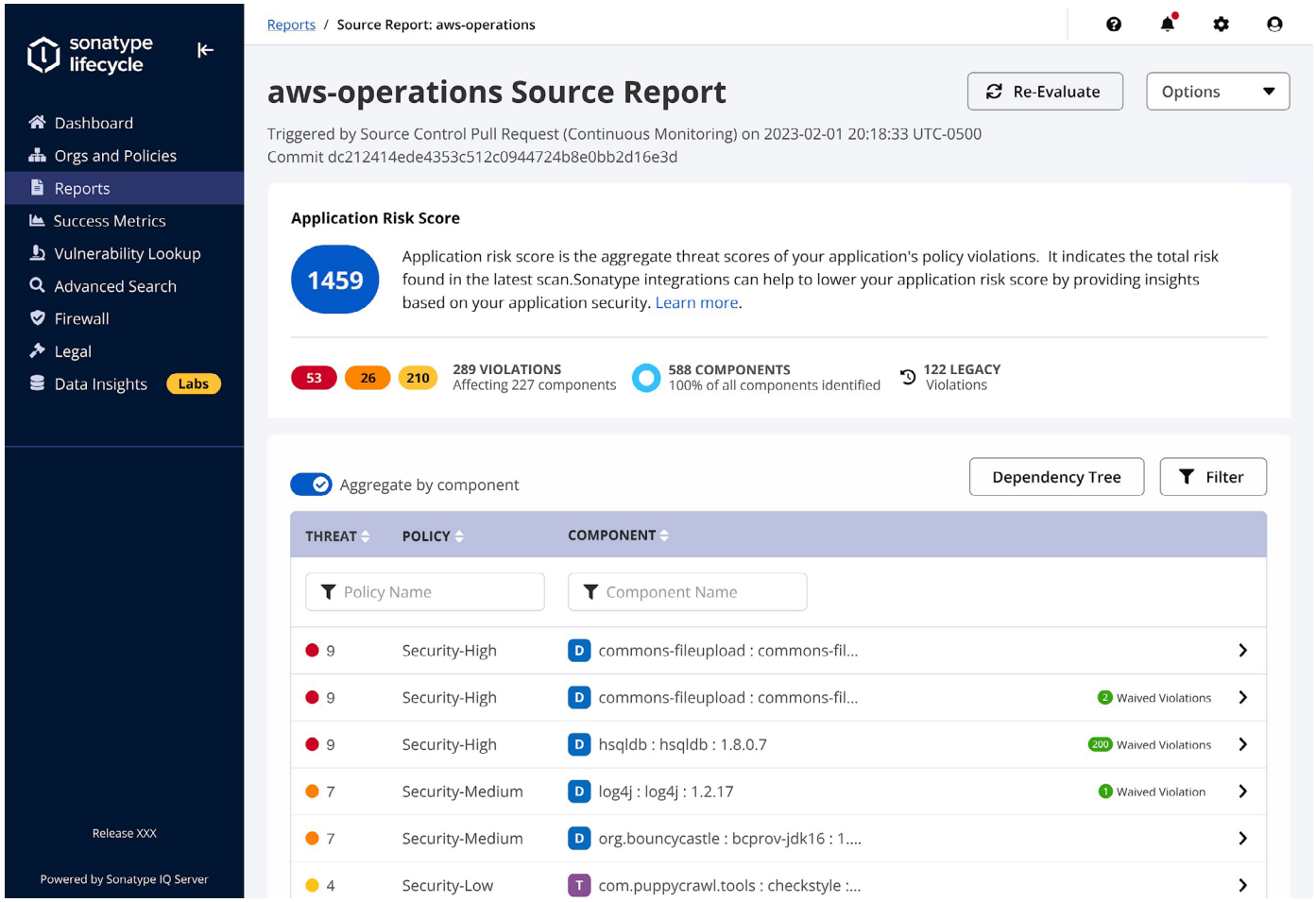
The GUI is really easy to navigate through and is very user-friendly.

READ REVIEW



The seamless integration of Sonatype and Fortify not only enhances security but also prioritizes user-friendly experiences. The combination ensures that developers can navigate through security assessments with ease, promoting collaboration and enabling teams to address potential issues efficiently. This user-centric approach enhances the solution's overall usability. It allows development and security teams to work cohesively toward the goal of building secure software without sacrificing user-friendliness.

The solution's ease of use contributes to its efficiency. A Code Reviewer at HQ USMEPCOM, a small government agency, shared, 8University of Maryland's Adjunct offered a similar take, saying, "It's pretty easy to find vulnerabilities. Then, you go to the source. It is very good at tracking to see where the data or the issue enters into your source code so you can track it or go back to where it started."



ENABLING INNOVATION

The collaborative integration of Sonatype and Fortify forms a dynamic synergy that fosters innovation within the DevSecOps paradigm. Innovation becomes possible, in part, through the use of OSS code. A Managing Director at Digalance, a small tech services company, put it plainly, saying, "Most software innovation happens in an open-source environment, and developers generate only a small amount of code."

As a result, DevSecOps teams become empowered to innovate with confidence. By seamlessly uniting component intelligence and dependency management from Sonatype with the advanced security analysis capabilities of Fortify, the holistic combed solution encourages a culture of continuous improvement. Developers can experiment with new ideas, iterate on code, and implement changes knowing that the integrated solution provides robust security measures.

To this point, Digalance's Managing Director further commented, "Lifecycle integrates everything from IDE down to production. It's a unique solution that helps customers embrace open-source development because that's where the innovation is happening. At the same time, I know the code coming into my environment is clean. A lot of our customers have adopted Azure DevOps, especially on the banking side. Some parts of the solution are in the cloud, while others are on-prem."

Vice President
Cybersecurity at a financial services firm with 10,001+ employees

Fortify provides robust details about the issues, along with comprehensive insights into what needs to be fixed... The ability to see all of the different versions in Sonatype results has been particularly helpful as an indicator.

READ REVIEW

SECURING THE SOFTWARE SUPPLY CHAIN

As major supply chain attacks like the epoch-defining 2020 SolarWinds breach have shown, a vulnerable supply chain can be the source of major delays and distractions that stall developer velocity. Only by diligently tracking OSS in use, identifying vulnerabilities, and then remediating, can a software development organization protect itself from threats in the supply chain.

Sonatype achieves this objective by addressing every element of an organization's software development life cycle (SDLC), including third-party open-source code, first-party source code, and containerized code. To support the process, Sonatype ingests, corrects, and curates a wide range of public data. Sixty percent of the data the platform ingests comes from public sources like the National Vulnerability Database. Sonatype then augments 97% of this data to make it more precise using AI, machine learning, and a team of data security researchers with 500+ years of experience.

Digalance's Managing Director took advantage of these powerful capabilities. For him, it was Sonatype's combination of vulnerability identification and GNU Affero General Public License (AGPL) license issues that made a difference. He said, "[My developers] They can see the associated risk and which version has the lowest risk. Developers can effortlessly migrate the entire project by dragging and dropping the version of the code with the lowest risk."

Conclusion

Developing and releasing high quality, secure software on an accelerated schedule is not a simple matter. Automated testing helps, as exemplified by Fortify Static Code Analyzer for SAST and Sonatype Lifecycle for software composition analysis. By delivering 360-degree visibility, the solution makes it easier to identify and remediate vulnerabilities. Compliance improves, too. Developer velocity increases, along with developer productivity. Working together as a holistic combined solution, Fortify and Sonatype help enable accelerated software development, but with greater risk mitigation.

About PeerSpot

PeerSpot is the authority on enterprise technology buying intelligence. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

About The Vendors

Fortify's Application Security Testing portfolio empowers your team for DevSecOps practices, enabling cloud transformation, and securing software supply chains by constantly innovating, supporting, and collaborating with organizations across the globe. As a code security solution with over two decades of expertise and acknowledged as a market leader by major analysts, Fortify provides the most adaptable, precise, and scalable AppSec platform available, covering the breadth of modern use cases and capabilities. We firmly believe that great code is secure code, and at Fortify, helping customers achieve it runs through everything we do.

Sonatype is a software supply chain management company. We enable organizations to innovate faster in a highly competitive market. Our industry-leading platform empowers engineers to develop software fearlessly and focus on building products that power businesses. Sonatype researchers have analyzed more than 120 million open-source components – 40x more than its competitors – and the Sonatype platform has automatically blocked over 115,000 malicious components from attacking software development pipelines. Enabling high-quality, secure software helps organizations meet their business needs and those of their customers and partners. More than 2,000 organizations, including 70% of the Fortune 100 and 15 million software developers, rely on our tools and guidance to be ambitious, move fast and do it securely. To learn more about Sonatype, please visit www.sonatype.com.

03.25 | 248-000098-001