

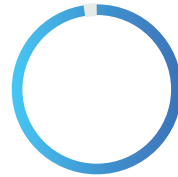
Fortify and Sonatype Deliver

# 360 Degree View of Application Security

Discover the integrated, best-in-class solution for custom code and open source code security vulnerabilities.

## Enterprises Need a Holistic View of Application Security

Open source use is common and problematic.



**97%**

of code comes from open source libraries



**633%**

increase in malicious software supply chain attacks in one year.



**4.5M**

estimated cost of a data breach on a per-incident basis.

Source: Sonatype State of the Software Supply Chain Report 2022

## Open Source + Custom Code Vulnerabilities in a Single Dashboard

Enterprises need to secure not just the code they write, but also the code they consume from open source components. That's why many are using Sonatype's solutions to accelerate digital innovation without sacrificing security or quality across the software supply chain.

With integration to Fortify, precise open source intelligence provides a 360-degree view of application security issues across the custom code and open source components.

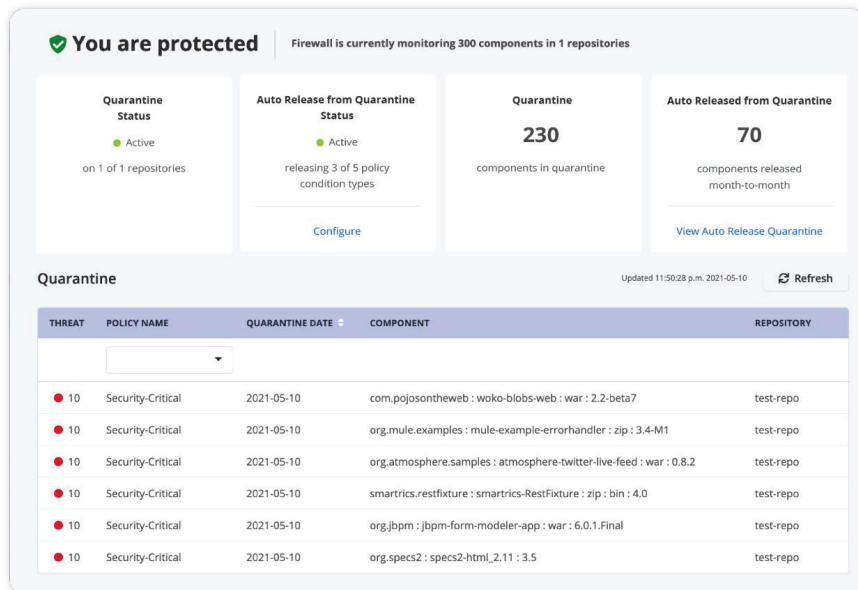
COMPONENT	VERSION	TYPE	KNOWN PUBLIC VULNERABILITIES
commons-collections:commons-collections	3.2	JAR	Critical: High, Medium, Low
hibernate	5.2	JAR	Critical: High, Medium, Low
spring	5.2.4	JAR	Critical: High, Medium, Low
spring-security	5.2.1	JAR	Critical: High, Medium, Low
spring	5.0.2	JAR	Critical: High, Medium, Low
spring-security	4.0.1	JAR	Critical: High, Medium, Low

ARTIFACT	VERSION	TYPE	STATUS	SEVERITY	MITIGATION
spring-security	5.2.1	JAR	High	Critical	Upgrade to 5.2.4
spring	5.0.2	JAR	High	Critical	Upgrade to 5.2.4

# Open Source Software Composition Assessments

Third-party components constitute a significant portion of federal agency applications, making Software Composition Analysis (SCA) critical for maintaining compliance and ensuring robust cybersecurity. Fortify's Software Composition Analysis, powered by Sonatype, offers comprehensive security insights beyond standard dependency checks against the National Vulnerability Database (NVD). Utilizing advanced natural language processing, it continuously scans GitHub commits, open-source repositories, security advisories, Google alerts, and multiple vulnerability databases to proactively detect emerging threats. Furthermore, a dedicated team of security experts actively identifies new vulnerabilities, maintaining an up-to-date proprietary knowledge base tailored specifically to support the unique security requirements of U.S. federal agencies.

Fortify simplifies the onboarding and scanning process by combining static and composition analysis into a single integration point, whether that's in the IDE or CI/CD pipeline. The comprehensive software bill of materials (SBOM), including security vulnerabilities and license details, is delivered as a fully integrated experience for security professionals and developers alike.



## Features

- Over 108K+ malicious packages were discovered and blocked
- Manage components, binaries, and build artifacts across your entire software supply chain.
- 20x faster searches and downloads of OSS components by developers
- 99% reduction in time spent reviewing and approving OSS components
- 26x faster identification and remediation of OSS vulnerabilities

## Why Sonatype?

Sonatype is the software supply chain security company, empowering organizations to build secure, high-quality software at scale. Our comprehensive platform provides proactive protection against malicious open-source software, advanced SBOM management, and industry-leading dependency management solutions. As founders of Nexus Repository and stewards of Maven Central—the world's largest repository of Java open-source software—we leverage unmatched expertise, AI-driven analytics, and precise data curation to enhance public vulnerability information. Trusted by numerous federal organizations and 70% of the Fortune 100, Sonatype ensures compliance, mitigates risks, and optimizes software development efficiency. To learn more, visit [sonatype.com](https://sonatype.com).

## Why Fortify?

The Fortify Software Security Research team translates cutting-edge research into security intelligence that powers the Fortify product portfolio. Today, **Fortify Software Security Content** supports 1,286 vulnerability categories across 30+ programming languages and spans more than one million individual APIs.

## Why MFGS, INC.?

MFGS, Inc. is the trusted advisor to the U.S. Government, its partners and system integrators for achieving optimal efficiency throughout an agency's enterprise software architecture. We bring a comprehensive portfolio of enterprise-grade software and a deep understanding of how DOD agencies operate to support your entire software development lifecycle, enabling you to safely plan, build, deliver and run your mission.

Learn more at [mfgsinc.com](https://mfgsinc.com)

