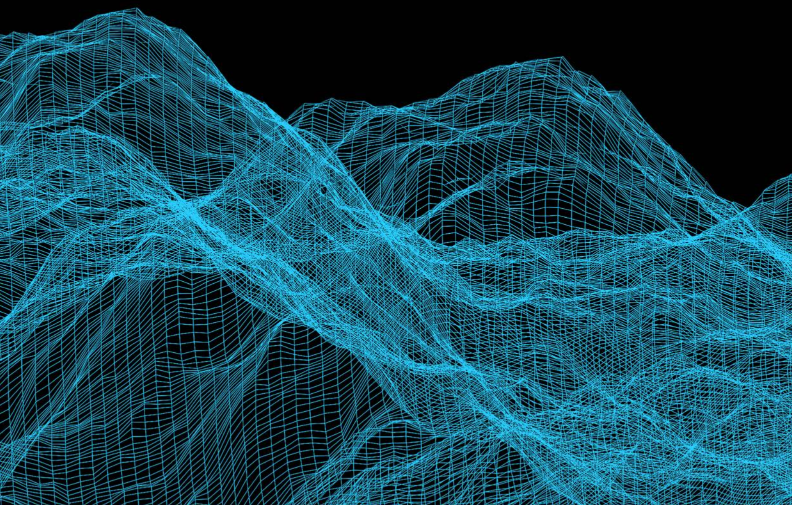
Fortify and Sonatype Deliver

360 Degree View of Application Security

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



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

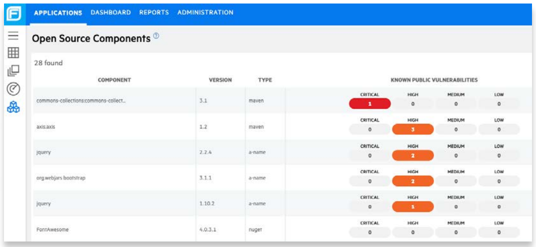
estimated cost of a data breach on a per-incident basis.

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.

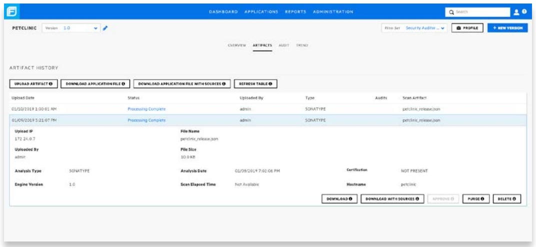
With integration to Fortify, precise open source intelligence provides a 360-degree view of application security issues across the custom code and open source components.



Open Source Components

28 found

COMPONENT	VERSION	TYPE	CRITICAL	HIGH	MEDIUM	LOW
commons-collections:commons-collect...	3.1	maven	1	0	0	0
axis:axis	1.2	maven	0	3	0	0
jquery	2.2.4	a-name	0	2	0	0
org.webjars bootstrap	3.1.1	a-name	0	2	0	0
jquery	1.10.2	a-name	0	1	0	0
FontAwesome	4.0.3.1	nuget	0	0	0	0



ARTIFACT HISTORY

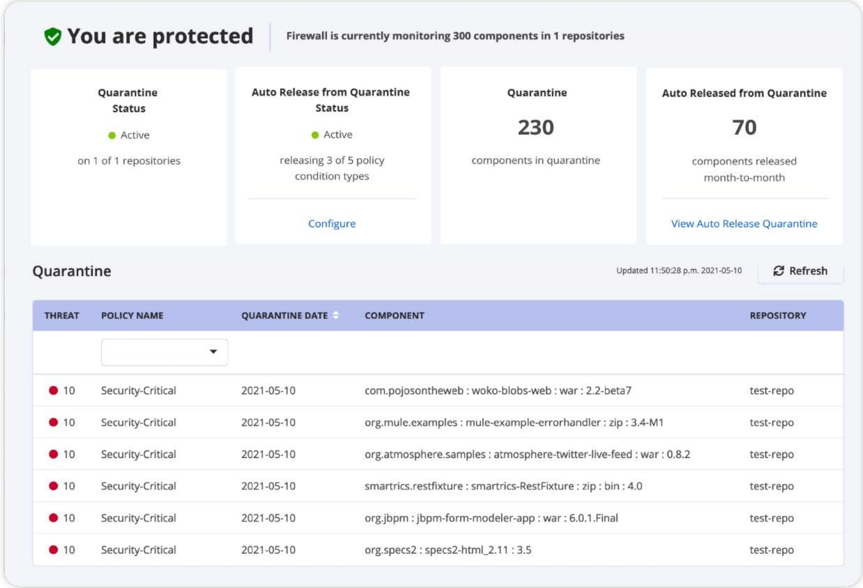
Upload Date	Status	Uploaded By	Type	Audits	Scan Artifact
01/10/2019 1:00:01 AM	Processing Complete	admin	SONATYPE		petclinic_release.json
01/09/2019 5:21:07 PM	Processing Complete	admin	SONATYPE		petclinic_release.json

Upload IP: 172.24.0.7
File Name: petclinic_release.json
Uploaded By: admin
File Size: 10.0 KB
Analysis Type: SONATYPE
Analysis Date: 01/09/2019 7:02:06 PM
Certification: NOT PRESENT
Engine Version: 1.0
Scan Elapsed Time: Not Available
Hostname: petclinic

Open Source Software Composition Assessments

Third party components make up a significant portion of many applications' codebase, making Software Composition Analysis a "must-have" for code security and a strong application security posture. Fortify's Software Composition Analysis, powered by Sonatype, goes beyond a simple comparison of declared dependencies against the National Vulnerability Database (NVD). Using natural language processing, it dynamically monitors GitHub commits, open-source projects, advisory websites, Google search alerts, Index, and several vulnerability sites. Additionally, a dedicated team of security experts regularly discovers new vulnerabilities and adds them to the proprietary knowledge base.

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 security bill of materials (SBOM), including security vulnerabilities and license details, is delivered as a fully integrated experience for security professionals and developers alike.



You are protected

Firewall is currently monitoring 300 components in 1 repositories

Quarantine Status
● Active
on 1 of 1 repositories

Auto Release from Quarantine Status
● Active
releasing 3 of 5 policy condition types
Configure

Quarantine
230
components in quarantine

Auto Released from Quarantine
70
components released month-to-month
View Auto Release Quarantine

Quarantine

Updated 11:50:28 p.m. 2021-05-10

Refresh

THREAT	POLICY NAME	QUARANTINE DATE	COMPONENT	REPOSITORY
● 10	Security-Critical	2021-05-10	com.pojosontheweb : woko-blobs-web : war : 2.2-beta7	test-repo
● 10	Security-Critical	2021-05-10	org.mule.examples : mule-example-errorhandler : zip : 3.4-M1	test-repo
● 10	Security-Critical	2021-05-10	org.atmosphere.samples : atmosphere-twitter-live-feed : war : 0.8.2	test-repo
● 10	Security-Critical	2021-05-10	smartrics.restfixture : smartrics-RestFixture : zip : bin : 4.0	test-repo
● 10	Security-Critical	2021-05-10	org.jbpm : jbpm-form-modeler-app : war : 6.0.1.Final	test-repo
● 10	Security-Critical	2021-05-10	org.specs2 : specs2-html_2.11 : 3.5	test-repo

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, the pioneer in software supply chain management. Sonatype empowers developers and security professionals with intelligent tools to innovate more securely at scale. The Sonatype platform addresses every element of an organization's entire software development life cycle, including third-party open source code, first-party source code, and containerized code. Additionally, 60% of the data that Sonatype ingests comes from public sources like the National Vulnerability Database. Sonatype corrects and curates that public data augmenting 97% of it to make it more precise. This curation process involves sophisticated ingestion tools, AI, and machine learning, along with a team of 65+ data security researchers with 500+ years of experience working nonstop.

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.