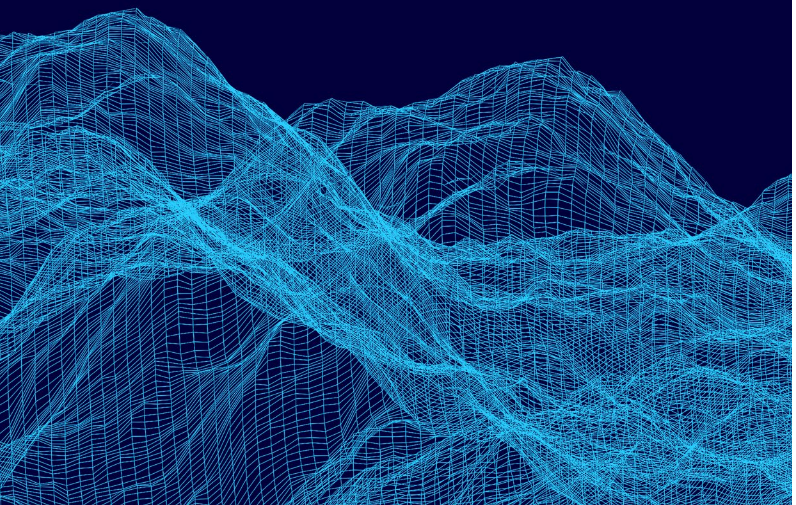
Micro Focus Fortify and Sonatype Deliver

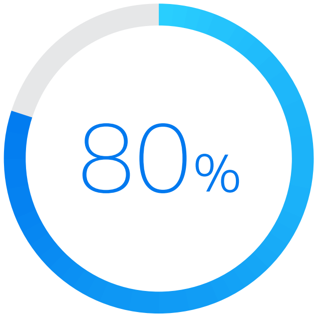
360 Degree View of Application Security

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

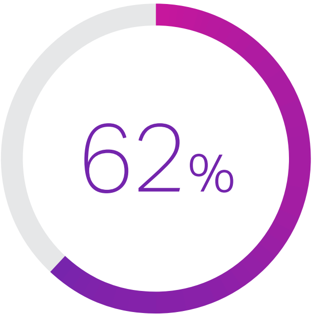


Enterprises Need a Holistic View of Application Security

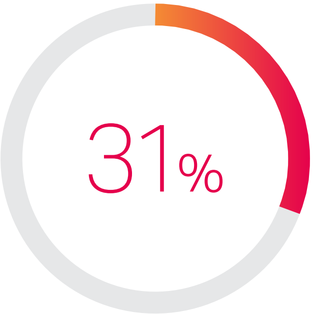
Open source use is common and problematic.



of application code comes from open source libraries.



of organizations do not have any control over what components are used in their applications.



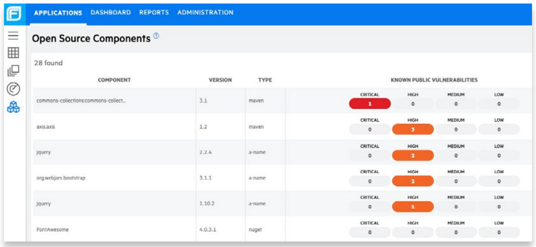
of organizations experienced a breach related to vulnerable open-source components.

Source: 2020 DevSecOps Community Survey, SonaType

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 projects. That's why many are using Nexus Lifecycle to automate open source governance at scale across the entire SDLC, shifting security left within development and build stages.

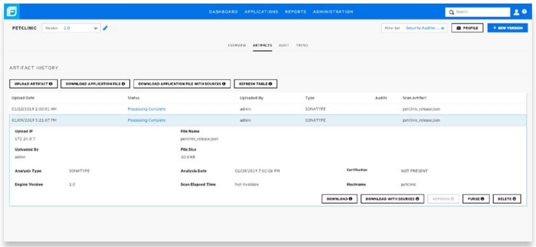
With integration to Fortify, Sonatype's precise open source intelligence provides a 360-degree view of application security issues across the custom code and open source components.



Open Source Components

28 found

COMPONENT	VERSION	TYPE	KNOWN PUBLIC VULNERABILITIES 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



PETCLINIC Version 1.0

Filter Set Security Auditor ...

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	01/08/2019 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" AppSec capability. Fortify on Demand's Software Composition Analysis, powered by Sonatype, goes beyond a simple comparison of declared dependencies against the National Vulnerability Database (NVD) by using natural language processing to dynamically monitor every GitHub commit to every open source project, advisory websites, Google search alerts, Index, and a plethora of vulnerability sites.

Additionally, new vulnerabilities are regularly discovered by a dedicated team of security researchers and added to the proprietary knowledge-base. Fortify on Demand 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 bill-of-materials including security vulnerabilities and license details is delivered as a fully integrated experience for security professionals and developers alike.

Features

- Provide code once for both SAST and software composition analysis
- Supports Java, .NET, JavaScript and Python
- Integrated results deliver one platform for remediation, reporting and analytics
- Examines fingerprints of 65M components for high accuracy—not just file names and package manifests
- Detects 70% more vulnerabilities than the NVD database alone
- 10M unique vulnerabilities to Sonatype

Why Sonatype?

When it comes to managing the constantly evolving security threats within open source, speed is critical. That's why Sonatype Nexus Intelligence works 24×7×365 to keep organizations abreast of the changing threat landscape.

- 70% more vulnerability coverage than alternative databases
- More than 60 world-class Data Security Researchers with 500+ years experience
- 118,000 hours of data security research over 10 years
- 10× faster than National Vulnerability Database