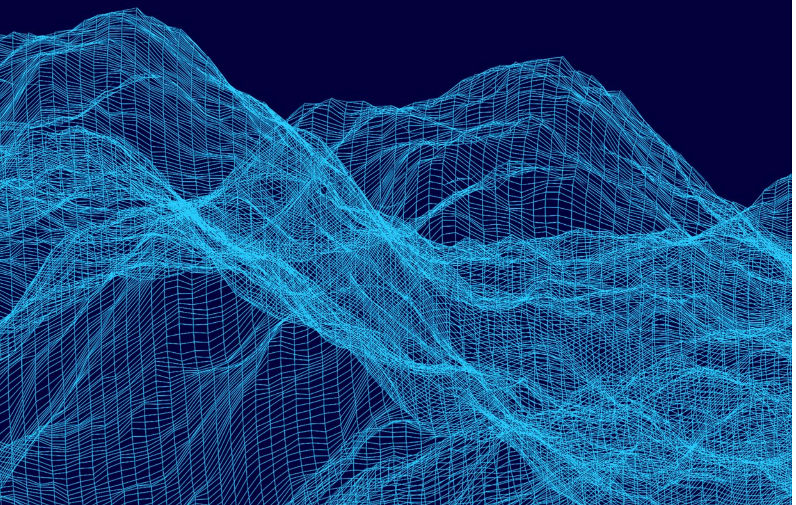
MICRO FOCUS | sonatype

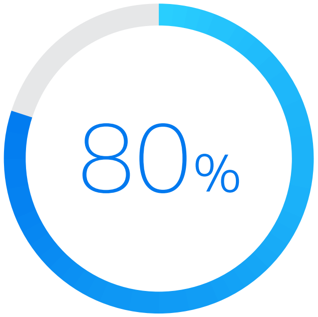
Micro Focus Fortify and Sonatype Deliver 360-Degree View of Application Security

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

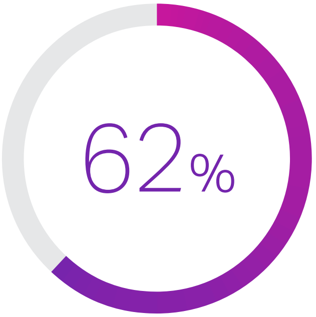


Enterprises Need a Holistic View of Application Security

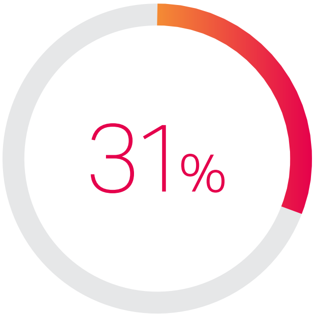
Open source use is common and problematic.



of application code comes from open-source libraries.



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



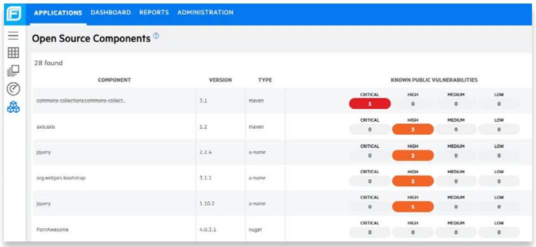
of organizations experienced a breach related to vulnerable open-source components.

Source: 2018 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 components. 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.

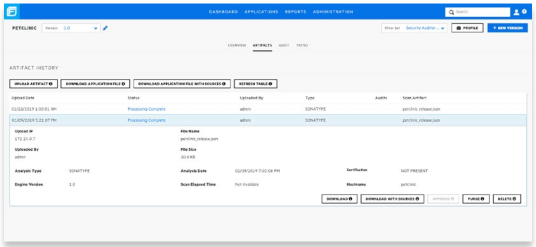
With integration to Fortify, precise open-source intelligence provides a 360-degree view of application security issues across the custom code and open source components.



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



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). 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 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.

Susceptibility Analysis

Once the solution scans for vulnerabilities, developers or security professionals can check whether someone has invoked a vulnerability in your custom code. More importantly, they can see whether attacker-controlled input reaches the code's function. Sonatype research identifies vulnerability signatures containing the method or function responsible for the specific CVE. And Fortify provides the translation model of the application and the rules engine to look for usage or user-controlled input that hits a particular method or function.

This Susceptibility Analysis capability:

- Reduces known vulnerability false positives.
- Eliminates months of effort upgrading a library that has almost no security benefit.
- Saves time on investigating known issues in open source.

You'll avoid the time-consuming headache of auditing vulnerabilities. And ultimately, more accurate data helps organizations make better decisions about which vulnerabilities require attention.

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?

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 working nonstop.

Why Micro Focus Fortify?

The Fortify Software Security Research team translates cutting-edge research into security intelligence that powers the Fortify product portfolio, including Fortify Static Code Analyzer (SCA), Fortify WebInspect, and Fortify Application Defender. Today, Micro Focus Fortify Software Security Content supports 1,032 vulnerability categories across 27 programming languages and spans more than one million individual APIs.