



Fortify and DevOps

Fortify on Demand drives proven results within DevOps toolchain¹



- Complete, proven application security solution as a service
- Scalable to the needs and various application loads of your business.
- Risks can be identified through Fortify on Demand static scans within minutes²
- The impact is faster development of applications with fewer production risks.

¹ "Continuous Delivery of Business Value with Fortify" – June 2017

² Fortify Internal Assessments – June 2017

Fortify on Demand Static Application Security Testing Process

Step 1: Develop & check-in code



Developers (IDE)



Source control repository



Continuous integration server

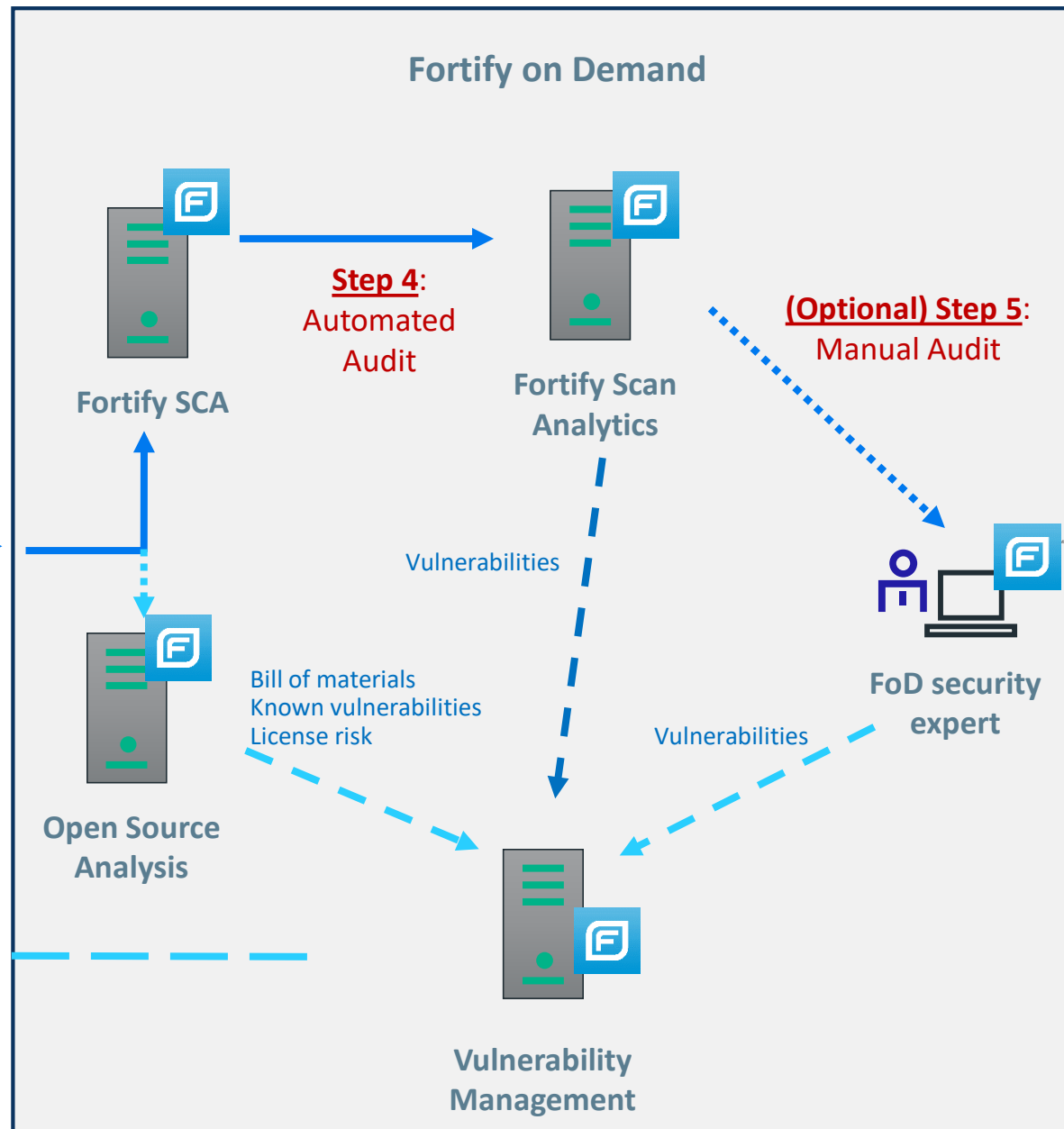
Step 3: Start Static Assessment

Step 2: Scheduled or triggered check-out & build



Defect management

Step 6: Triage, assign & fix vulnerabilities



Fortify on Demand

Step 4: Automated Audit

(Optional) Step 5: Manual Audit

Fortify SCA

Fortify Scan Analytics

Vulnerabilities

Bill of materials
Known vulnerabilities
License risk

FoD security expert

Vulnerabilities

Open Source Analysis

Vulnerability Management

Azure DevOps

Builds Releases Library Task Groups Deployment Groups*

MyFirstProject Save & queue Discard Summary Queue

Tasks Variables Triggers Options Retention History

Process
Build process

Get sources
MyFirstProject \$/MyFirstProject

Agent phase
Run on agent

Install SCA on agent
Fortify Static Code Analyzer Install

Add tasks
Don't see what you need? [Check out our Marketplace.](#)

Search

All Build Utility Test Package Deploy Tool

- Extract Files
Extract a variety of archive and compression files such as .7z, .rar, .tar.gz, and .zip.
- Fortify on Demand Dynamic Assessment
Start Fortify assessment of website
- Fortify on Demand Static Assessment
Submit code for Fortify assessment
- Fortify Static Code Analyzer Assessment
Run Fortify Static Code Analyzer
- Fortify Static Code Analyzer Install
Install Fortify SCA on an agent
- Fortify WebInspect Dynamic Assessment
Run WebInspect dynamic scan
- FTP Upload
FTP Upload

Azure DevOps

MyFirstProject

Save & queue | Discard | Summary | Queue

Tasks | Variables | Triggers | Options | Retention | History

Process
Build process

Get sources
MyFirstProject \$/MyFirstProject

Agent phase
Run on agent

Run Fortify WebInspect dyna...
Fortify WebInspect Dynamic Assessment

Fortify WebInspect Dynamic Assessment

Version 1.*

Display name *
Run Fortify WebInspect dynamic assessment on

Scan Settings: *
Passive

WebInspect API: *
<http://localhost:8083/>

Scan Results: *
c:\agent\scans

Control Options ^

Enabled
 Continue on error

Timeout *
0

Open Source Scanning, Sonatype

Scope of Analysis



32
COMPONENTS IDENTIFIED
91% OF ALL COMPONENTS ARE OPEN SOURCE

11 **12**
POLICY ALERTS
AFFECTING 23 COMPONENTS

77
SECURITY ALERTS
AFFECTING 6 COMPONENTS

5
LICENSE ALERTS

Security Issues

How bad are the vulnerabilities and how many are there?

Critical (7-10)

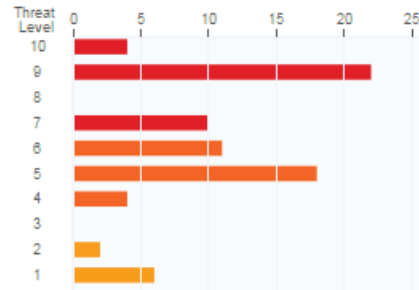
36

Severe (4-6)

33

Moderate (1-3)

8



The summary of security issues demonstrates the breakdown of vulnerabilities based on severity and the threat level it poses to your application. The dependency depth highlights quantity and severity and distribution within the application's dependencies.

Dependency Depth



License Analysis

What type of licenses and how many of each?

Critical (8-10)

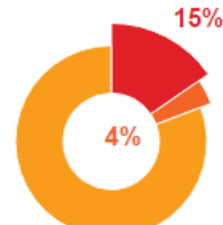
0

Severe (4-7)

4

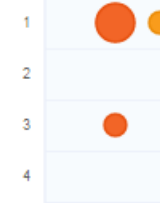
Moderate (1-3)

0



The summary of license analysis demonstrates the number of licenses detected in each category. The dependency depth compares quantity by category and the distribution within your application's dependencies.

Dependency Depth



Expanded developer training with Secure Code Warrior

Interactive training for top vulnerabilities



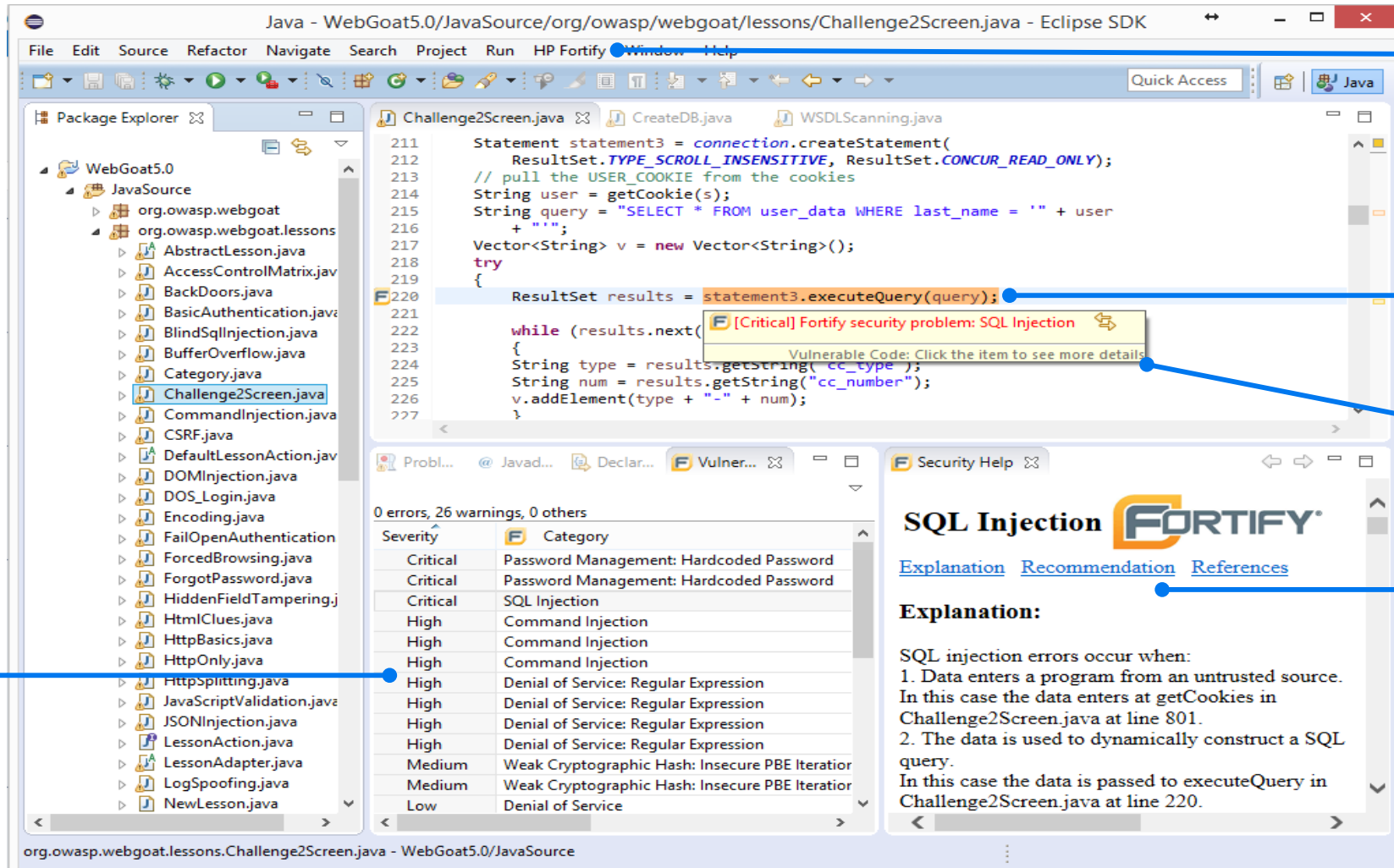
Incorporates a gamified interface for a more interactive, engaging developer training experience

Advantages over Codebashing/Checkmarx

- 1. Offers broader application framework support**
 - JAVA Spring, JAVA Struts, JAVA JSP/J2EE, C# .NET WebForms, Ruby on Rails, Android JAVA, Objective c
- 2. First to offer a live data-driven evaluation of an individual developer's true secure code writing ability**
- 3. AppSec executives are able to see the learning progress of their development team(s) including:**
 - Each developers secure code strength and weakness areas,
 - Allows for evaluation of skills across offshored and external development teams

Source: [Cybersecurity Excellence Awards](#)

Fortify Security Assistant highlights vulnerabilities during coding



Fortify menu for additional options

Vulnerable line of code is highlighted as developer code & provides tips for additional information

Level of criticality

All issues detected in the project

Type of vulnerability, explanation and detailed remediation guidance

Scan Central

Fortify Audit Assistant applies machine learning to identify the vulnerabilities most relevant to your organization

