

# FortiDevSec

Available in



Hosted

## Continuous Application Security Testing in CI/CD Pipelines

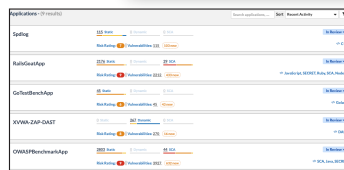
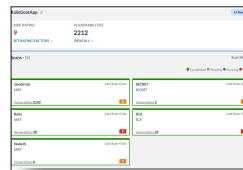
Software applications are everywhere, and the success of every business depends on its ability to develop and deploy business software applications faster and faster.

Since time-to-market is crucially important, businesses simply cannot afford to follow the traditional slower waterfall method of application development anymore. The waterfall model is a sequential approach where changes to the application are deployed perhaps once in many months, and the development team moved to the next phase of development or testing only if the previous step completed successfully.

Application development teams are now adopting agile and DevOps methodologies for rapid application development and deployment. In the agile model, development and testing activities are concurrent and continuously iterated. The application changes are deployed very frequently to the cloud, and so the development, functional, and application security (AppSec) testing teams have tighter collaboration and communication with faster turnaround times. This condition has led to the need to automate the workflow involved in building and deploying applications to the cloud, and subsequently, to the rise of the DevOps role, wherein continuous integration/continuous deployment (CI/CD) tools are used to enable this automation.

Application Security (AppSec) testing needs to be automated as well and made to work in this CI/CD paradigm and be incorporated in the earlier stages of the development cycle (commonly referred to as shift-left). This scenario is where many AppSec testing products may fall short when they are not natively built to support the user experience of developers and DevOps, who typically do not have much AppSec expertise and are unable to use such products effectively. Quite simply, they are not DevSecOps enabled.

DevSecOps is short for development, security, and operations. It refers to automating the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery.



### Key Benefits

- **Automate DevSecOps.** Embed application security into your DevOps process natively, without requiring much application security expertise
- **Gain visibility across the entire attack surface.** Understand all the security risks in web apps, including source code, open-source components, and run-time attack vectors
- **Consolidated Dashboard.** An easy to use portal normalizes, aggregates, and consolidates security risks found across many types of scan types
- **Get intelligently prioritized issues.** See security issues in a ranked list with intelligent analyses of scans across all scan types
- **Easy and manageable.** Eliminate setup and management overhead. No need to set up or update scanners. The latest scanners get set up automatically. Unified configuration for all your scans with no need for siloed plugins

## FEATURE HIGHLIGHTS

### Innovative Product Offering

AppSec testing is also very fragmented. There are many types of AppSec scans that need to be done on an application to figure out all its vulnerabilities, and these are usually offered by separate products. A multi-product solution creates fragmentation and hinders DevSecOps enablement of AppSec.

The industry needs an innovative AppSec product that has DevSecOps in its DNA. It should be easy to use by developers and DevOps without requiring specialized security expertise. It should also be a comprehensive offering covering all types of AppSec scans, including SAST, DAST, SCA, Secrets, and more.

FortiDevSec is Fortinet's DevSecOps product. FortiDevSec offers a Cloud/SaaS-based continuous application security

testing built from the ground up to natively focus on software developers and DevOps. FortiDevSec enables the shift-left architecture for application security by finding security vulnerabilities in applications right in the early stages of the development lifecycle, thus allowing the developers to find and fix issues quickly before even the application goes to production.

FortiDevSec integrates and sits natively in the application's DevOps CI/CD pipeline. It offers comprehensive application scanning, including scanning source code, third-party libraries, secrets, and live web application URLs. It then aggregates the security issues and presents them in an easy-to-use web portal. Intelligent noise reduction enables developers to prioritize working on the most critical vulnerabilities without overwhelming them.

### Simple Security for Modern App Development

Modern application development is a combination of rapid application development using agile methodologies, being cloud-native, using microservices and container-based architectures, using CI/CD to automate build and deployment, and the need to automate application security testing in CI/CD.

FortiDevSec orchestrates and automates continuous application security testing for developers and DevOps directly into the application CI/CD DevOps lifecycle. DevOps can integrate FortiDevSec just by copying a few lines of code into their CI/CD and without requiring any AppSec expertise. This feature allows AppSec to work at the speed of DevOps. FortiDevSec supports all major CI/CD tools, languages, and frameworks.

For DevOps, it provides a single automation layer for all application security scan types through a unified yaml configuration. There is no need for DevOps to include multiple plugins for multiple scanners. The scanners come in dockerized images and are always updated to the latest version, providing overall easy manageability.

### Easy integration into CI/CD platforms


```

SAST scan:
  docker login --username $DOCKERHUB_USERNAME --password
  $DOCKERHUB_PASSWORD
  docker run --rm --mount type=bind,source=$PWD,target=/code
  registry.fortinet-us.com/fortidevsecops/fortidevsecops-sast
  orgid: your-org-id-here


DAST scan:
  docker login --username $DOC
  $DOCKERHUB_PASSWORD
  docker run --rm --mount type=bind,source=$PWD,target=/code
  registry.fortinet-us.com/fortidevsecops/fortidevsecops-dast
  appid: your-app-id-here
  # Optional param section starts
  buildtool: jenkins. # Optional param, values=jenkins,travis
  scaanner: sast,dast,sca # Optional param, default is All
  language: python, javascript # Optional param, default is Auto Detect

variables:
  DAST_URL: https://your.url.com # Optional param


# Optional param section end
# end of file
    
```




Jenkins  
(with plug in)




Harness  
CI




GitHub  
Action



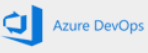
Circle CI



Bamboo



Travis CI



Azure DevOps



## FEATURE HIGHLIGHTS

### Comprehensive Vulnerability Management

Applications need to be secured from multiple attack vectors, and in order to do that, they need to be security tested using many types of scanners.

Static or source code testing (SAST) scans the application's own source code, SCA/OSS scans the third-party libraries (typically open-source libraries) included in the application, Secrets scans for open password texts in the code, DAST or dynamic testing analyzes a web application through the front-end to find vulnerabilities through simulated attacks.

FortiDevSec provides comprehensive vulnerability management by including multiple types of testing, including SAST, SCA/OSS, Secrets, and DAST.

FortiDevSec introspects each application and automatically selects the types of scanning that are needed and relevant for that application based on the application's attributes like languages and frameworks. Scanners are automatically downloaded or updated as dockerized images in the FortiDevSec agent.

**RailsGoatApp** In Review

RISK RATING: **9** | VULNERABILITIES: **2212**

SET RATING FACTORS → | VIEW ALL →

Scans - (5) Scan History

- JavaScript SAST: Last Scan 4 Jan, Vulnerabilities: 2143
- Ruby SAST: Last Scan 4 Jan, Vulnerabilities: 30
- NodeJS SAST: Last Scan 4 Jan, Vulnerabilities: 8
- SECRET: Last Scan 4 Jan, Vulnerabilities: 2
- SCA: Last Scan 4 Jan, Vulnerabilities: 29

**ZulipPythonApp** In Review

RISK RATING: **9** | VULNERABILITIES: **1850**

SET RATING FACTORS → | VIEW ALL →

Scans - (5) Scan History

- Python SAST: Last Scan 4 Jan, Vulnerabilities: 1399
- SCA: Last Scan 4 Jan, Vulnerabilities: 0
- JavaScript SAST: Last Scan 4 Jan, Vulnerabilities: 37
- SECRET: Last Scan 4 Jan, Vulnerabilities: 105
- NodeJS SAST: Last Scan 4 Jan, Vulnerabilities: 309

### Consolidated Dashboard

FortiDevSec offers an easy-to-use portal where users can log in and view all the issues across all their applications and all the different scan types. There is no more need to use multiple portals for numerous different and fragmented scanners.

Scan results are first normalized across multiple scan types. The risk rating, risk category, and descriptions are all normalized. The results are then aggregated and presented with various filters so the user can prioritize on fixing the most critical items first.

Developers usually get overwhelmed when there is a very high number of issues reported. To mitigate that scenario, FortiDevSec intelligently correlates these results across multiple scan results and manipulates the risk ratings accordingly. This result aids in the noise reduction of the reported issues and makes the developer focus on fixing the most critical issues first.

Filters (433 results)

- Calculated Risk Rating: Critical (13), High (361), Medium (53), Low (6)
- Status: New (433), Confirmed (0), In Review (0), Reviewed (0), Reopened (0), Fixed (0), Risk Accepted (0), False Positive (0), Removed (0)
- Category: Files, Directory

**RailsGoatApp** In Review

Vulnerabilities 433 active, 0 closed MARK ALL AS REVIEWED | EXPORT

- JavaScript SAST: Vulnerabilities: Total - 2143, Unique - 395
- Ruby SAST: Vulnerabilities: Total - 30, Unique - 17
- NodeJS SAST: Vulnerabilities: Total - 8, Unique - 8
- SECRET: Vulnerabilities: Total - 2, Unique - 2
- SCA: Vulnerabilities: Total - 29, Unique - 11

Vulnerable dependency: jquery\_min.js  
Severity: High

Vulnerable dependency: scan/Gemfile.lock:activerecord  
Severity: Critical



## ORDER INFORMATION

The FortiDevSecOps offers licenses based on the number of users. This group typically includes all the developers who work on the applications that are security tested by FortiDevSec. Other users like DevOps, security, and management would also need access to the FortiDevSec portal, and those need to be counted too. Currently, FortiDevSec offers a SKU that includes up to five users. The SKU is also stackable, so a greater number of users can be included. These users have access to onboard an unlimited number of applications (that these users are directly working on) and scan them unlimited times on FortiDevSec.

PRODUCT	SKU	DESCRIPTION
FortiDevSec	FC1-10-DEVSC-513-01-12	FortiDevSec - Standard functionality Tier - Unlimited scans and unlimited apps for all scanners for up to 5 developer users (all developers working on the target apps to be scanned are counted) - Annual Subscription.



[www.fortinet.com](https://www.fortinet.com)

Copyright © 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA (<https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf>) and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy ([https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower\\_Policy.pdf](https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf)).