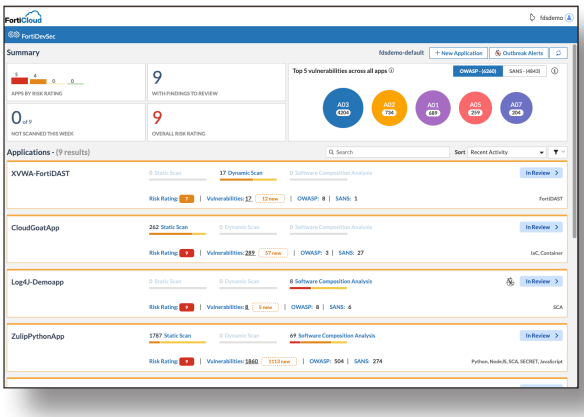
DATA SHEET

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 security risks in web apps, including source code, open-source or third party components, container images, IaC, 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. Filter and priortize on OWASP Top 10 and CWE/SANS Top 25 vulnerabilities
- **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, Secret, Container images, and IaC files.

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.

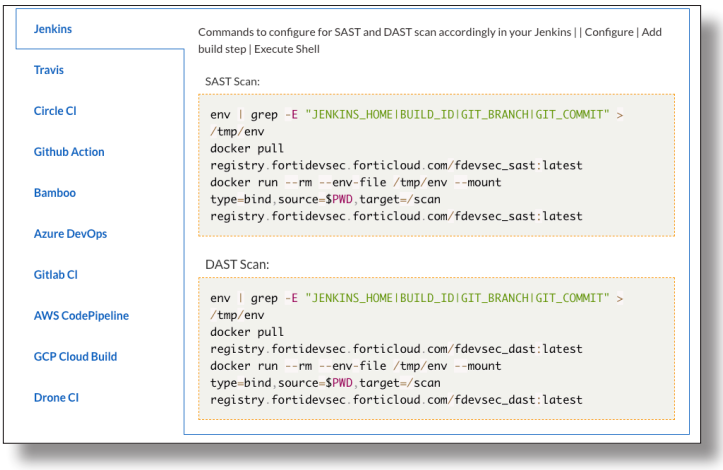
FortiDevSec integrates and sits natively in the application's DevOps CI/CD pipeline. It offers comprehensive application scanning, including scanning source code, open-source/third party libraries, secret, container images, IaC - Infrastructure as Code files and live web application URLs. It then aggregates 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.

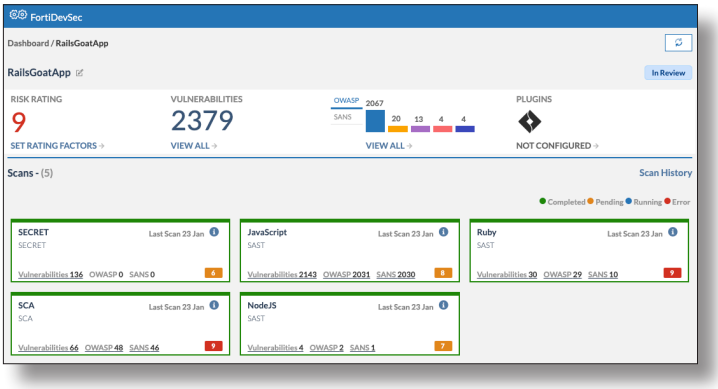


FEATURE HIGHLIGHTS

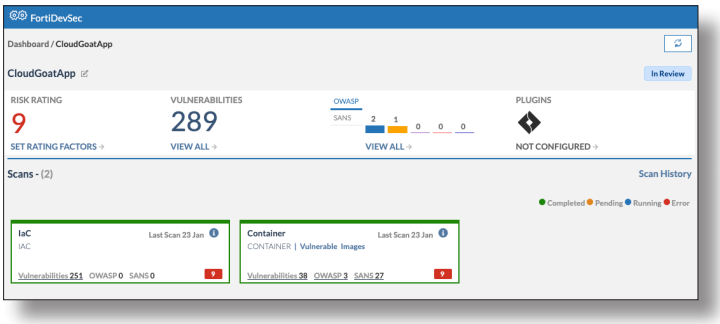
Comprehensive Vulnerability Management

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. Container scanning finds vulnerabilities in container images created during the build. Infrastructure-as-Code IAC scanning finds misconfigurations in infrastructure before it is even created.



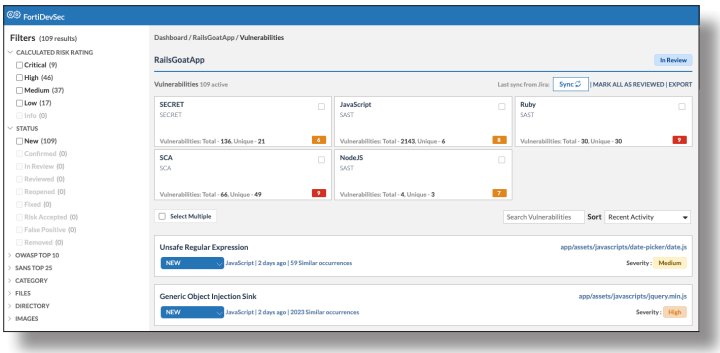
FortiDevSec includes all the above types of scanning to provide comprehensive vulnerability management. DAST scanning alone is provided through another Fortinet product - FortiDAST but FortiDevSec is seamlessly integrated into and includes FortiDAST.



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.

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. OWASP Top 10 and CWE/SANS Top 25 vulnerabilities are highlighted and can be filtered by users to prioritize.

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.

ORDER INFORMATION

The FortiDevSecOps offers licenses based on the number of users, i.e., developers.

This number includes all the developers who work on and across all the applications that are security-tested by FortiDevSec for a customer. Typically, these developers would have an account and check-in code on the application source code repository (like GitHub).

First, count the number of developers who check-in/commit code into the repo of an application scanned by FortiDevSec. Second, do this across all the applications scanned by FortiDevSec to get the total count at a customer license level. Of course, if the same developer works in more than one application, they don't have to be counted twice.

This number of developers/users is not the same as the number of users that login to the FortiDevSec portal. In most cases, the latter would be smaller than the total number of developers calculated using source code repos.

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 for SAST, Secrets, Container, and IaC scans.

The only limitation for number of applications scanned is for DAST scanning. DAST scanning is provided internally by another product called FortiDAST. Every five-user FortiDevSec license comes included with a five-application scanning for DAST. If more than five applications are needed for DAST scanning, there is a separate add-on SKU/license that can be purchased.

PRODUCT	SKU	DESCRIPTION
FortiDevSec	FC1-10-DEVSC-513-01-12	FortiDevSec - Standard functionality Tier - Unlimited scans and unlimited apps for all scanners (SAST, SCA/OSS, Containers, IaC and Secrets) for up to 5 developer users (all developers working on the target apps to be scanned are counted). This also includes DAST or WebApp Vulnerability scanning provided by FortiDAST but limited to 5 apps. Use add on SKU to add more apps for DAST. - Annual Subscription. FortiCare support included.
FortiDAST add-on to FortiDevSec	FC1-10-DEVSC-216-02-12	Add on FortiDAST web vulnerability scanning / DAST functionality to FortiDevSec. Both products are to be used in SAAS version. This SKU provides access for scanning 5 apps using FortiDAST. This is on top of 5 apps for DAST that get included by default for each FortiDevSec license.

FDS-DAT-R03-20230127