opentext™ | Cybersecurity

Data Sheet

Fortify Static Code Analyzer: Static application security testing

Pinpoint the root cause of security vulnerabilities in the source code, prioritize the most serious issues, and get detailed guidance on how to fix them

Build better code with static testing

Static application security testing (SAST) identifies security vulnerabilities during early stages of development when they are least expensive to fix. It reduces security risks in applications by providing immediate feedback to developers on issues introduced into code during development. SAST also helps educate developers about security while they work, enabling them to create more secure software.

Fortify Static Code Analyzer by OpenText™ uses multiple algorithms and an expansive knowledge base of secure coding rules to analyze an application's source code for exploitable vulnerabilities.

This technique analyzes every feasible path that execution and data can follow to identify and remediate vulnerabilities.

Find security issues early

To process code, Static Code Analyzer works much like a compiler, which reads source code files and converts them to an intermediate structure enhanced for security analysis. This intermediate format is used to locate security vulnerabilities. The analysis engine, which consists of multiple specialized analyzers, uses secure coding rules to analyze the code base for violations of secure coding practices.

Manage results with Fortify Software Security Center

Fortify Software Security Center (SSC) by OpenText™ is a centralized management repository providing visibility to an organization's entire application security program to help resolve security vulnerabilities across the software portfolio. Users can review, audit, prioritize, and manage remediation efforts, track software security testing activities, and measure improvements via the management dashboard and reports to optimize static, dynamic, and software composition analysis results.

Fortify SSC correlates and tracks the scan results and assessment results over time and makes the information available to developers through Fortify Audit Workbench by OpenText™, or through IDE plugins, such as the Fortify Plugin for Eclipse, the Fortify Extension by OpenText™ for Visual Studio, and others.

Users can also manually or automatically push issues into defect tracking systems, including OpenText™ ALM Octane, Jira, Azure DevOps Server, and Bugzilla.

- Audit Workbench
  - Smart View—Visualization makes auditing and fixing easier:
    - Quickly understand how multiple issues are related from a data flow perspective

Integration ecosystem includes:

- Flexible deployment options: AppSec-as-a- Service, on-premises, or in the cloud
- Integrated development environments (IDE): Eclipse, Visual Studio, JetBrains (including IntelliJ)
- CI/CD tools: Jenkins, Bamboo, Visual Studio, Gradle, Make, Azure DevOps, GitHub, GitLab, Maven, MSBuild
- Issue trackers: Bugzilla, Jira, ALM Octane
- Open source security management: Sonatype, Snyk, WhiteSource, BlackDuck
- Code repositories: GitHub, Bitbucket
- Swaggerized API for unlimited customization
- Developer-friendly language coverage:
  - Support for Java, Kotlin, Scala, C#, VB.NET, TypeScript, JavaScript, C/C++, Python, PHP, Go, COBOL, Swift, Objective C/C++, Salesforce Apex, Dart/Flutter, Bicep, Solidity, Ruby, SAP ABAP, PL/SQL, T-SQL, ColdFusion, ActionScript, Visual Basic 6, VBScript, Ruby, HTML, XML, JSON, YAML, HCL. Supported languages are detailed in the "Fortify Software System Requirements" documentation.
- Integration into CI/CD tools (IDEs, Bug Trackers, Open Source)
  - Support for all major IDEs: Eclipse, Visual Studio, JetBrains, including IntelliJ.
  - Defect management integrations provide transparent remediation for security issues.
  - Open Source Security integration: Sonatype and Debricked.
  - The combination of swagger supported rest APIs, open source GitHub repo, with plugins and extensions for Bamboo, Azure DevOps and Jenkins are the types of tools to leverage to automate the CI/CD pipeline.

> **"Fortify allows us to analyze a greater volume of code in a much more agile and rapid way. Now, our pipelines usually reach me without vulnerability errors because they've already been detected up front in the development process."**
>
> **Wilson González**
> DevOps manager
> Location World

Connect with Us
www.opentext.com

- Apply Smart View filters to begin triaging or fixing issues at most efficient point

Get fast and accurate scanning

Static application security testing (SAST) captures the majority of code-related issues early in development, allowing you to identify and eliminate vulnerabilities in source, binary, or byte code. Fortify detects 1,627 unique categories of vulnerabilities across more than 33 programming languages and spans more than one million individual APIs with accuracy as demonstrated by a true positive rate of 100% in the OWASP 1.2b Benchmark.

Automate security in the CI/CD pipeline

Fortify reduces risk by identifying and prioritizing which vulnerabilities pose the greatest threat and integrates with CI/CD tools including Jenkins, ALM Octane, Jira, Atlassian Bamboo, Azure DevOps, Eclipse and Microsoft Visual Studio (see Fortify Integrations). Review scan results in real time with access to recommendations, line-of-code navigation to find vulnerabilities faster and collaborative auditing.

Reduce development time and cost

When embedded within the SDLC, development time and cost can be reduced by 25 percent. The production/post release phase is 30 times more costly to fix than vulnerabilities found earlier in the lifecycle. Fortify enables secure coding practices by educating developers about static application security testing while they work.

Choose from flexible deployment options to suit the environment your team is developing in:

- Fortify On Demand by OpenText™ allows teams to work in a fully SaaS-based environment
- Fortify Hosted gives you the best of both SaaS and on premises by working in an isolated virtual environment with complete control of the user data.
- Fortify OnPrem allows a team to have absolute control over all aspects of the Fortify solution.

Get real-time security analysis and results for developers

Security Assistant provides structural and configuration analyzers which are purpose-built for speed and efficiency to power our most instantaneous security feedback tool. It only finds high confidence (all true positives or with very low false positive rates) findings with immediate results in the IDE (Microsoft Visual Studio, Eclipse, and IntelliJ).

Fortify on Demand with Security Assistant is suggested to be used as an additional job aid for developers and used in conjunction with full static scans for a more comprehensive view of security issues. All current Fortify Static Code Analyzer and Fortify on Demand Static Assessments customers are entitled to use Security Assistant with no additional licenses/cost.

Decrease manual audit time

Fortify Audit Assistant by OpenText™ saves manual audit time with machine learning to identify and prioritize the most relevant vulnerabilities to your organization. Automation with applied machine learning reduces manual audit time to amplify ROI of your static application security testing initiative. Fortify Audit Assistant:

- Provides automated audit results in minutes.
- Minimizes auditor workload.
- Prioritizes issues with confidence level.
- Creates accurate and consistent audit results throughout projects.
- Delivers results at the speed of DevOps.
- Reduces the number of issues needing deep manual examination.
- Identifies relevant issues and removing false positives sooner.
- Scales application security with existing resources.

Get a centralized scanning infrastructure

ScanCentral enables lightweight packaging on the build server and provides a centralized scanning infrastructure to meet the growing demands of modern development needs from within Fortify Software Security Center It is scalable, with on-premises, on demand, or hybrid approaches. ScanCentral provides flexibility to achieve desired coverage by adjusting scan, as well as improved scanning performance; tune for fast scans; and tune for comprehensive, more accurate, and restful API/ Swaggerized API.

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

760-000015-006 | O | 06/24 |