opentext™ | Cybersecurity

Data Sheet

Fortify Static Code Analyzer (SCA) Static Application Security Testing

Fortify Static Code Analyzer (SCA) pinpoints the root cause of security vulnerabilities in the source code, prioritizes the most serious issues, and provides detailed guidance on how to fix them so developers can resolve issues in less time with centralized software security management.

Static Testing Helps Build Better Code

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. Static Application Security Testing also helps educate developers about security while they work, enabling them to create more secure software.

Fortify Static Code Analyzer (SCA) 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, Fortify SCA 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. Fortify SCA also provides a rules builder to extend and expand static analysis capabilities and be able to include custom rules. Results are viewed in a number of ways depending on the audience and task.

Manage Results with Fortify Software Security Center (SSC)

Fortify Software Security Center (SSC) by OpenTextis 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 and dynamic application security test results. Fortify SSC helps to provide an accurate picture and scope of the application security posture across the enterprise. The Fortify SSC server resides in a central location and receives results from different application security testing activities, such as static, dynamic, and real-time analysis.

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.

Integration Ecosystem Includes:

- Flexible Deployment Options: AppSec-as-a-Service, On Premise, 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

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

Key Benefits

Fast and Accurate Scanning

- Static application security testing (SAST) captures the majority of code related issues early in development.
- Identify and eliminate vulnerabilities in source, binary, or byte code
- Fortify SCA detects 815 unique categories of vulnerabilities across 27 programming languages and spans over one million individual APIs
- Accuracy as demonstrated by a true positive rate of 100% in the OWASP 1.2b Benchmark

Automate Security in the CI/CD Pipeline

- Reduces risk by identifying and prioritizing which vulnerabilities pose the greatest threat
- Fortify 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 & Cost

- When embedded within the SDLC, development time and cost can be reduced by 25%. The production/post-release phase is 30 times more costly to fix than vulnerabilities found earlier in the lifecycle.
- 2X as many vulnerabilities found with up to 95% reduced false positives (reference: Mainstay Continuous Delivery of Business Value with Fortify by OpenText™ 2017))
- Enables secure coding practices by educating developers about static application security testing while they work

Key Features

- Developer-friendly language coverage
  - Support for ABAP/BSP, ActionScript, Apex, ASP.NET, C# (.NET), C/C++, Classic, ASP (with VBScript), COBOL, ColdFusion CFML, Go, HTML, Java (including Android), JavaScript/AJAX, JSP, Kotlin, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Swift, T-SQL, VB.NET, VBScript, Visual Basic, and XML
  - 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 integration: Sonatype, WhiteSource, Snyk, BlackDuck
  - 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.
- 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-prem by working in a isolated virtual environment with complete control of the user data.
  - Fortify On-Prem allows a team to have absolute control over all aspects of the fortify solution.
- Security Assistant provides real time, as-you-type code, security analysis and results for developers.
  - It provides structural and configuration analyzers which are purpose built for speed and efficiency to power our most instantaneous security feedback tool.
  - Security Assistant 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.
- 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.
  - Provides automated audit results in minutes
  - Minimizes auditor workload
  - Prioritizes issues with confidence level
  - Creates accurate and consistent audit results throughout projects
  - Audit results at the speed of DevOps; this makes it possible to integrate SCA to build servers, source code management servers and scan more often with immediate results.

"We can identify, analyze, and resolve possible issues far more efficiently with Fortify Static Code Analyzer than we ever could before."

Brenton Witonski
Senior IT Security Engineer
Acxiom

Connect with Us
www.opentext.com

  - Reduces the number of issues needing deep manual examination
  - Identifies relevant issues and removing false positives sooner
  - Scales application security with existing resources
- ScanCentral enables lightweight packaging on the build server, and provides a scalable, centralized, Fortify by OpenText™ scanning infrastructure to meet the growing demands of modern development needs from within Fortify Software Security Center.
- Flexibility to achieve desired coverage by adjusting scan.
  - Improved scanning performance
  - Tune for fast scans
  - Tune for comprehensive, more accurate
  - Restful API/ Swaggerized API
- Scalable with on-premise, on demand, or hybrid approaches

Accurately Assess the Security State of Your Applications

Fortify offers the broadest set of software security testing products spanning the software lifecycle:

- **Fortify Static Code Analyzer (SCA) for Static Application Security Testing (SAST):** Identifies vulnerabilities during development, and prioritizes those critical issues when they are easiest and least expensive to fix. Scanned results are stored in Fortify SSC. Learn more about Fortify SCA at: **www.microfocus.com/en-us/cyberres/application-security/static-code-analyzer**.
- **Fortify WebInspect for Dynamic Application Security Testing (DAST) by OpenText™:** Identifies and prioritizes security vulnerabilities in running web applications and web services. Integrates Interactive Application Security Testing (IAST) to identify more vulnerabilities by expanding coverage of the attack surface. Scanned results can be stored in Fortify SSC.
- **Fortify Software Security Center by OpenText™:** An AppSec platform that enables organizations to automate an application security program. It provides management, development, and security teams a way to work together to triage, track, validate, and manage software security activities.
- **Fortify on Demand for Security as a Service:** Easy and flexible way to test the security of your software quickly, accurately, and without dedicating additional resources, or having to install and manage any software.

System Requirements

For detailed product specifications and system requirements, visit: **www.microfocus.com/documentation/fortify-static-code/**.

Company Overview

At Cybersecurity we help you run your business and transform it. Our software provides the critical tools you need to build, operate, secure, and analyze your enterprise. By design, these tools bridge the gap between existing and emerging technologies—which means you can innovate faster, with less risk, in the race to digital transformation.

Fortify offers the most comprehensive static and dynamic application security testing technologies, along with runtime application monitoring and protection, backed by industry-leading security research. Solutions can be deployed in-house or as a managed service to build a scalable, nimble Software Security Assurance program that meets the evolving needs of today's IT organization.

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.

760-000015-005 | O | 10/23 | © 2023 Open Text