Hewlett Packard Enterprise

Data sheet

HPE Security Fortify Static Code Analyzer

Build better code and secure your software

What is static code analysis?
Static code analysis identifies security vulnerabilities efficiently in source code. Static code analysis should be done early in the development lifecycle and also continuously used throughout the life of the application. It provides immediate feedback to developers on issues introduced into code during development.

Statistics

- Over 84 percent of security breaches occur at the application layer[1]
- Critical Web security vulnerabilities impact almost half of all Web applications[2]
- 52 percent of Web applications experience issues with input validation, cross-site scripting, and SQL injection[3]
- 33 percent of applications are never tested for security vulnerabilities[4].

Applications bring risk and security exposure

Life of a software developer

- Building new features and functionalities
- Increasing complexity
- Numerous
- Deadlines
- Shrinking budgets
- Product Delay

These words resonate with software developers because these are the demands they face when creating critical business applications. Building applications today is compounded by countless requirements and developers are so overwhelmed that security is an afterthought. Meanwhile, threats are evolving and adversaries are specializing on exploiting the weak link—applications. HPE Security Fortify Static Code Analyzer (SCA), helps protect organizations from today's greatest security risk, the applications that run their business.

HPE Security Fortify Static Code Analyzer
HPE Security Fortify SCA is a static application security testing (SAST) offering used by development groups and security professionals to analyze the source code for security vulnerabilities. It reviews code and helps developers identify, prioritize, and resolve issues with less effort and in less time.

HPE Security Fortify SCA empowers developers to:

- Scan source code early and often
- Pinpoint the root cause of vulnerabilities down to the line of code
- Correlate and prioritize the results
- Accelerate development and shorten scan times
- Remediate security vulnerabilities quickly
- Review best practices to help developers code more securely

Why HPE Security Fortify SCA is for you

Comprehensive
Fortify SCA supports a wide variety of development environments, languages, platforms, and frameworks to enable security reviews in mixed development and production environments.

- 23 programming languages
- Over 839,000 component-level APIs
- Detects over 700 vulnerability categories
- Supports all major platforms, build environments, and IDEs

Accurate
Fortify SCA provides accurate results and detects a breadth of issues unmatched by other static testing technologies. Fortify SCA prioritizes vulnerabilities to provide an accurate action plan, delivering risk-ranked and categorized issues. It is guided by the largest and most complete set of security coding rules that are expanded and updated by HPE Security Fortify Software Security Research group.

Flexible
Fortify SCA fits into your existing development environment. It is a flexible command line static code analyzer that can integrate into any environment through scripts, plugins, and GUI tools so developers can get up and running quickly and easily.

[1] Gartner Magic Quadrant Report

[2], [3] HPE Cyber Risk Report 2015, February 2015

[4] Study: Mobile Application Developers Not Investing in Security March 20, 2015

Supported languages

- ABAP/BSP
- ActionScript/MXML (Flex)
- ASP.NET, VB.NET, C# (.NET)
- C/C++
- Classic ASP (w/VBScript)
- COBOL
- ColdFusion CFML
- HTML
- Java (including Android)
- JavaScript/AJAX
- JSP
- Objective-C
- PHP
- PL/SQL
- Python
- T-SQL
- Ruby
- Swift
- Visual Basic
- VBScript
- XML

Supported IDEs

- Eclipse
- IntelliJ Ultimate
- IntelliJ Community Android Studio
- IBM Rational Application Developer (RAD)
- IBM Rational Software Architect (RSA)
- Microsoft® Visual Studio

Supported Build Tools

- Ant
- Jenkins
- Maven
- MSBuild
- Xcodebuild

Sign up for updates

Hewlett Packard Enterprise

Efficient

Organizations needing to accelerate their application security program will benefit from faster scan times. Fortify SCA helps developers improve their programming productivity by offering incremental scanning. Incremental scanning reduces the time required to run a scan by only analyzing parts of the code that have changed since the last full scan. It dramatically shortens scan times so developers get results faster, it improves productivity by enabling more frequent scans, and accelerates the time it takes to get software into production faster.

Scalable

Applications come from multiple sources, in-house, outsource, third party, open source, mobile, and with the sheer number and complexity of applications being created, testing and maintaining the security integrity of all these application types across the enterprise is a challenge. With support for the most programming languages in the industry, Fortify SCA can identify the risk in all types of applications and scale with the growing demands of the business.

On Premise or On Demand

Fortify SCA is offered in multiple delivery models designed to accommodate changing needs and requirements.

- On Premise—HPE Security Fortify SCA for deployment, management, and running static application security testing programs onsite.
- On Demand—HPE Security Fortify on Demand is a managed application security testing service that offers an easy and accurate way to initiate static, dynamic and mobile testing without upfront investment, additional resources and time.

Fortify taxonomy of software security vulnerabilities

Vulnerability categories

When it comes to software security, there are no agreed upon standard of what is and isn't a critical vulnerability. Many organizations publish their own interpretation of the top vulnerabilities, leading to discrepancies and confusion. To help developers understand the common types of coding mistakes that lead to security vulnerabilities, Fortify created The Seven Pernicious Kingdoms that unifies the organization of vulnerabilities and maps them to standards such as OWASP, SANS, CWE, and FISMA.

HPE Security Fortify Software Security Research Group is a global team recognized by the industry as one of the top security organizations for monitoring emerging threats. Their collection of knowledge is funneled into the HPE Security Fortify suite of offerings in the form of vulnerability checks that stay on top of the latest threats. The team created the Vulnerabilities Category Taxonomy, a set of rules to help developers understand the types of security vulnerabilities that affect applications.

Learn more: Evolution of a Taxonomy
vulncat.hpefod.com

About HPE Security

Hewlett Packard Enterprise is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE Security ArcSight, HPE Security Fortify and HPE Security—Data Security, the HPE Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn more about HPE Security Products at **hpe.com/software/esp**.

For more information

HPE Security Fortify solutions help you build trust in the software you depend on to run your business. To learn more about HPE Security Fortify Static Code Analyzer, Visit **hpe.com/software/sca** or contact an HPE Security Fortify representative by calling +1 (877)686-9637.

Learn more at
hpe.com/software/fortify

4AA5-6055ENW, December 2016, Rev. 3