Points of Contact

USAF & MDA Account Directors

Scott Snowden, Scott.Snowden@mfgs.carahsoft.com
Bryan White, Bryan.White@mfgs.carahsoft.com

Fortify DOD Sales Specialist

John Farrell, John.Farrell@mfgs.carahsoft.com

Fortify DOD Solution Architect

Haleh Nematollahy, Haleh.Nematollahy@microfocusgov.com
Jamie Delco, Jamie.Delco@mfgs.carahsoft.com

Application Security Summary

Static Analysis SAST (Fortify): analysis of computer software that is performed without actually executing programs (i.e. run on source code)

Dynamic Analysis DAST (WebInspect): analysis of computer software that is performed by executing programs on a real or virtual processor (Pentesting against a running web application)

Real-time Application Self Protection RASP (Application Defender): software agent protects and monitors production systems.

Open Source security scanning (Sonatype): performs Software Composition Analysis by scanning third party open source software included in your application, identifying CVEs and other risks.

Fortify

Static Code Analyzer (SCA) – this is the component that scans the source code and generates a Fortify Project Report (fpr) which contains the scan results

Audit Workbench (AWB) – a stand-alone thick client to audit and review scan results. AWB can also be used to scan application source code.

IDE Plug-ins – plug-ins for Developer IDEs such as Eclipse and Visual Studio that allow developers to run scans on their desktops and/or interact directly with scan results to facilitate quick and efficient remediation.

Security Assistant – plug-in for Visual Studio and for Eclipse that delivers real time, as you type code, security analysis and results. Alerting developer to common security issues without having to run a full scan.

Software Security Center (SSC) – A centralized repository for all of the scan results. It provides tracking, trending, reporting and dashboards for your entire portfolio of applications. This is a web based application that you install and maintain on your network

FedRAMP Fortify on Demand (FOD) – A SaaS application security testing service. Customers upload their source code to our FedRAMP FISMA Moderate approved AWS GovCloud (IL2) data center where our US security team scans the application, audits the results and provides the finding back through the online portal.

WebInspect

WebInspect (WI) – a Windows based dynamic application security testing tool that identifies application vulnerabilities in deployed web applications and services. WebInspect scans modern frameworks and web technology with the most comprehensive and accurate dynamic scanner. The product is easily deployable in enterprise environments, has exhaustive REST APIs to benefit integration and has the flexibility to manage security risks either through intuitive UI or run completely via automation.

Important References

Fortify Support – online Fortify support portal for submitting and working tickets
https://softwaresupport.softwaregrp.com/

Fortify Chat Support – Questions orders, SAID, downloads, support access, etc
https://softwaresupport.softwaregrp.com/web/softwaresupport/chat-language-selection

Licensing and Software Download – portal for license management and software download
https://entitlement.mfgs.microfocus.com/

Documentation – location for all product documentation
https://www.microfocus.com/support-and-services/documentation/

Rulepack Download – portal for SCA static rulepack downloads and premium content download
Support.Fortify.com

Product Announcements – subscribe to product and rulepack release announcements
https://community.softwaregrp.com/t5/Fortify-Product-Announcements/bd-p/Fortify_PA

VULCAT – List of all security categories covered by Fortify and WebInspect
https://vulncat.fortify.com/en

Protect 724 – online user community. Contains documentation, training videos, user forum, etc.
https://community.softwaregrp.com/t5/Protect724/ct-p/Protect724

Fortify Unplugged – YouTube channel with training videos and demonstrations of new features
https://www.youtube.com/channel/UCUDKcm1wIfE6EWk_SyK0D4w/videos

Fortify Marketplace – online source for plug-ins and other integration tools https://marketplace.microfocus.com/fortify

Fortify Engineering – online resource to access source code for plug-ins and REST API samples https://fortify.github.io/

Sonatype: https://marketplace.microfocus.com/fortify/content/sonatype-nexus-lifecycle-integration-with-ssc