Micro Focus Security – Security at the core of everything you do: Operations, Applications, Identities and Data

- Application Security
- Security Operations
- Data Security
- Identity and Access management

Application Security: Fortify application security testing protects your entire software development lifecycle (SDLC) with the most automated, integrated, enterprise-scale solution both on-premise and in the cloud.

Fortify: End-to-end AppSec

Fortify is the recognized market leader in application security and is the most comprehensive and scalable application security solution that works with your current development tools and processes. With Fortify, organizations can start securing applications in a single day including custom code, open source or commercial components and scale as needs grow with an on premises, as a service, hosted, or hybrid implementation.

Why Fortify

- Fortify has been a market leader in both Gartner and Forester for application security for almost 10 years and was recognized as a Gartner Peer Insight Customers Choice for 2022
- Fortify is the only comprehensive application security provider to offer SAST, DAST, IAST, and SCA on premise and as a SaaS
- Fortify on Demand is FedRAMP certified Moderate/Impact Level 2 for both SAST and DAST and we are in the process of getting Software Composition Analysis added with Debricked (target Spring ’23)
- Enable compliance of your applications with broad vulnerability coverage, including over 1,137 categories across SAST and DAST that enable compliance with standards such as OWASP Top 10, CWE/SANS, Top 25, DISA STIG, PCI DSS, NIST 800-53, FISMA, OWASP ASVS
- Fortify Software Security Center (SSC) offers a single pane of glass to see your Static, Dynamic, and Open Source vulnerabilities
- Fortify integrates with your current CI/CD tools: https://www.microfocus.com/en-us/cyberres/application-security/ecosystem
- Fortify has a leading Software Security Research team
- Micro Focus Fortify Software Security Content supports 1,137 vulnerability categories across 30+ programming languages and spans more than one million individual APIs

“Buzzwords” to listen for

- Application Security – is the process of making apps more secure by finding, fixing, and enhancing the security of apps.
- Vulnerabilities – weaknesses in code that are susceptible to being hacked. A flaw in your code that creates a potential security risk.
- Static Application Security Testing (SAST) – analyses the source code of an application for security vulnerabilities

- Dynamic Application Security Testing (DAST) — tests for vulnerabilities in Web Applications and Web Services by crawling and performing attacks against the application.
- Software Composition Analysis (SCA) – tests for vulnerabilities in open source components
- Shifting Security Left – an ideology of testing for vulnerabilities earlier in the software development lifecycle (SDLC)
- DevOps – is the combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity
- DevSecOps – the philosophy of integrating security into the DevOps process
- Continuous Integration/Continuous Delivery (CI/CD) Pipeline - helps you automate steps in your software delivery process, such as initiating code builds, running automated tests, and deploying to a staging or production environment
- Automated Scans – the ability to schedule scans with minimal action on the part of a developer
- Machine Learning Auditing Tool - minimizes auditor workload with machine learning to identify the vulnerabilities from Fortify Static Code Analyzer results
- Compliance- the requirement to map to industry security controls standards such as FISMA, NIST 800-53, DISA STIG, OWASP

Target Audience that care about AppSec:
The two main groups that we sell to are the Security Team and/or the Application Development Team
Target Personas:

- CISO, CIO, CSO, Application Security Manager, Lead Developer, IT Director, ISSO, ISSM, Application Development Manager, Director of Security, Security Auditor, Information Assurance, Cybersecurity Lead

Common Pain Points

- Securing the Software Supply Chain; SBOM Requirements
- Data Breach/Security Vulnerabilities
- Compliance/Security Controls
- API Security
- RMF Process / ATO
- Increasing number of applications and releases
- Constantly expanding attack surface, growing number of vulnerabilities
- Vulnerability Management
- Meeting Audit Requirements
- Improved Cybersecurity/security posture

<u>Identify if there is an Opportunity – Prospecting Calls</u>

Probing Questions:
What is your current application security strategy?
Are you responsible for Application Security within your organization? Who is responsible for AppSec?
Do you have applications that your team manages or develops?
Do you have any DevSecOps initiatives?
Is securing the software supply chain top of mind for your team?
Where does AppSec rank in your overall risk environment?
Are there specific compliance requirements that you have regarding application security? NIST, FISMA, DISA STIG?

Are you experiencing or do you anticipate growth in new applications across your business? What types of applications? Web, Mobile?
Do you have a requirement to perform static, dynamic, or software composition analysis on your applications?
What are teams currently doing to scan for vulnerabilities in your applications?
What percentage of your applications are currently being scanned under your AppSec program?
What tools are you currently using? (even if not Fortify tools)
Are you familiar with or currently using Fortify or WebInspect?

Upsell Opportunities with Existing Customers

If the customer is currently using Fortify for Static Analysis of their source code, ask them what they are doing to dynamically scan their web applications, web services, APIs or mobile apps?
Let them know that doing Static and Dynamic Analysis on their applications will give them a more complete view of the vulnerabilities across the entire SDLC.

If the customer is currently using WebInspect for Dynamic Analysis, ask them what they are doing to analyze their source code for vulnerabilities.
Let the customer know that doing Static Analysis can help them identify vulnerabilities earlier in the SDLC and help shift security left.

Sonatype/Debricked Upsell Questions:

Do you have open-source software components that are included in your applications? If yes, do you have a requirement to scan on those components to determine the risk in the application?
Do you have a need to generate a Software Bill of Materials (SBOM)?
Would it be helpful for you to be able to identify risk in your open-source components and identify what is the next non-vulnerable version to upgrade to?
Would it be helpful to have a single pane of view for SAST, DAST and your Open Source results?

Competition:

SAST Competitors- Synopsys, Checkmarx, Veracode, SonarQube, Gitlab, GitHub
DAST Competitors- HCL Appscan, Accunetix, Netsparker, Invicti, OWASP ZAP, Whitehat, Burp Suite
SCA Competitors- Black Duck, Mend (WhiteSource), OWASP Dependency Check

Solution & Benefits of the Fortify Suite for Application Security

- ***Fortify Static Code Analyzer:*** Static Application Security Testing. Deliver secure software fast…Find security issues early in the development cycle while developers are coding and fix at the speed of DevOps.
- ***Fortify WebInspect:*** Dynamic Application Security Testing Software. Find and prioritize web application vulnerabilities. Automate dynamic web application testing across a software portfolio.
- ***Sonatype (SCA):*** Software Composition Analysis. Identify vulnerable open source components within a customer's applications and provide next known non-vulnerable version.
- ***Debricked (SCA):*** Software Composition Analysis. Identify vulnerable open source components within a customer's applications and provide next known non-vulnerable version.
- ***Fortify on Demand (FOD):*** is a complete **FedRAMP certified** Application Security as a Service solution. It offers an easy way to get started with the flexibility to scale. In addition to static and dynamic, Fortify on Demand covers in-depth mobile app security testing, open-source analysis, and vendor application security management. Fortify is the only FedRAMP certified vendor.

- *SBOM:* has emerged as a key building block in software security and software supply chain risk management. A SBOM is a nested inventory, a list of ingredients that make up software components.
- *Software Security Center:* is a centralized management repository that provides security managers and program administrators with visibility into integrations and the entire application security testing program.
- Fortify Hosted: SaaS Based offering of Fortify Portfolio to outsource infrastructure/deployment of customer's Fortify platform in their SaaS environment with customers driving their scans
- *Security Assistant:* for Eclipse or Visual Studio provides real-time-as-you-type security analysis on code. Fix each issue with confidence knowing that only high confidence issues are flagged. Developers can also customize which issues are shown.
- *Audit Assistant:* minimizes auditor workload with machine learning to identify the vulnerabilities from Fortify Static Code Analyzer results. This reduces the number of issues that need deep manual examination and enables teams to scale application security with existing resources.

Scoping Questions

**We will confirm this information on the initial Scoping Call with the Fortify team. However, any details that can be gathered in advance of the first call with the full team would be great.

Fortify Scoping Questions: 2023

Date:
Organization:
POC:
Email:
Phone:

- What agency, organization and program are you supporting?
- Are you looking for SAST, DAST or Open-Source Scanning solutions?
- Does your team have experience using Fortify or other SAST/DAST products? What tools are you currently using?
- Do you prefer a SaaS Solution or On-Premise Solution?
- Which compliance requirements apply (RMF, NIST 800-53, FISMA, DISA App STIG, etc.)?
- When do you need to have your secure coding program operational?
- How many unique code bases (source code required) will need to be scanned?
- How many developers will be leveraging the fortify tools to either runs scans, review results, or remediate issues in the code?
- How many IA staff or security auditors will need to run scans and review findings?
- Which programming languages are the applications developed in?
- Is your development environment centralized or distributed?
- Are you using a Continuous Integration/Build process that this needs to be integrated with? Which one? (CICD / Jenkins, ADO…)
- Do you have a solution in place to scan your open-source software components, libraries and frameworks? If so which tool?
- Do any of the apps have a web component? Web service?
- Do you have a specific budget you can help us understand?
- Is this a funded project?
- Is there a specific contracting vehicle or procurement approach that works best for you?

Sample Virtual Customer Care Visit / Value Check Template:
***Please check with your Fortify team to see if we are actively working any opportunities to send a more tailored message to those customers we are already engaged with. ***

EMAIL 1 Initial Outreach:

We would like to offer your Software Assurance (SwA) team a complimentary Virtual Fortify Customer Care Visit (CCV). This is a 1-hour session where you will meet the full team supporting you for FY23 virtually to talk about your implementation of Fortify SAST and WebInspect, and to answer any questions you have.

The objective is to help you evaluate your use of Fortify SAST and WebInspect, and answer questions that will help you improve and expand your Software Assurance program. If you have any specific support or technical issues, please provide them prior to the CCV and we will make sure to address them during the call.

EMAIL/Call 2 Confirm the Agenda:
Meeting should include the **Account Executive, Fortify Specialist, 1 Fortify Engineer, CSM. Please confirm the topics of interest and add them to the agenda for the meeting. Also, please provide the full team with a summary of what the customer feedback has been, what the customer owns, CSID, PoP date, partner they use etc. so that we can have a productive meeting**

The usual topics for discussion and recommended attendees include -

Implementation Topics -
Deployment model
System configuration and settings
Integration with IDE, CI/CD
Support for Compliance mappings
Security reporting framework
Adoption rate, obstacles and accelerators
Best practices for SwA
Recommendations
General Q&A -
Support and case escalation process
Features and functions
What's new?

Recommended Attendance -
Head of Application Security
Development Leads, ISSOs, and/or System Admin assigned "hands-on" with Fortify SAST/WebInspect
Development Manager(s) responsible for secure development teams and/or Manager responsible for Audit instance(s) of Fortify SAST/WebInspect
Manager i/c Certification and Accreditation, if applicable

In addition to the above, we have new exciting features such as ScanCentral SAST and DAST, additional open source scanning solutions, integration with CI/CD Pipelines, and new language support such as

json/Yaml, secret scanning (IaC). We would like to discuss your goals and demo any new features that can help you achieve your goals.
Please let us know the best way to coordinate the CCV with your team!