MICRO FOCUS
Government Solutions

Data Sheet
Security

Fortify on Demand: FedRAMP Application Security as a Service

Understanding risk is an important first step in any application security initiative. Application security begins at the start from the moment that code is developed. The pace of application development will continue to intensify.

Product Highlights

Micro Focus® Fortify on Demand is a complete application security as a service solution that offers "defense in depth" spanning coverage across more languages and more vulnerability categories. Moreover, Fortify on Demand stays ahead of the changing threat landscape with its quarterly Software Security Research updates.

Fortify on Demand for the U.S. Federal sector is the first and leading application security as a service solution to achieve FedRAMP authorization and is a JAB certified, FedRAMP authorized, cloud accessible managed application security testing platform. This means your government agency can perform application security testing easily and confidently while adhering to internal risk management policies.

Key Benefits

- Enables government programs, security organizations, and application development teams to extend and scale their Software Security Assurance Programs quickly and efficiently
- Combines the most advanced, comprehensive application testing methodologies with manual expert review
- Centralized portal provides intuitive, userfriendly and comprehensive application dashboards, vulnerabilities, and work streams for a single application or across your entire portfolio
- Integrates on-premises and cloud-based application security testing and program management solutions, specifically for U.S. government agencies

Key Features

Code Scan Initiation

Fortify on Demand static assessments can span web, mobile, embedded, or thick-client applications. Scans can be initiated quickly and easily. Developers can upload the application source code from their integrated development environment (IDE), repository, build, or CI server. Developers can also upload code for assessments through the Fortify on Demand portal or automatically using our ecosystem of integrations and flexible application programming interface (API).

Fortify on Demand at a Glance:

- Enables government programs, security organizations, and application development teams to extend and scale their Software Security Assurance Programs quickly and efficiently
- Combines the most advanced, comprehensive application testing methodologies with manual expert review
- Centralized portal provides intuitive, user-friendly and comprehensive application dashboards, vulnerabilities, and work streams for a single application or across your entire portfolio
- Integrates on-premises and cloud-based application security testing and program management solutions, specifically for U.S. government agencies

FedRAMP
Federal Risk Authorization Management Program

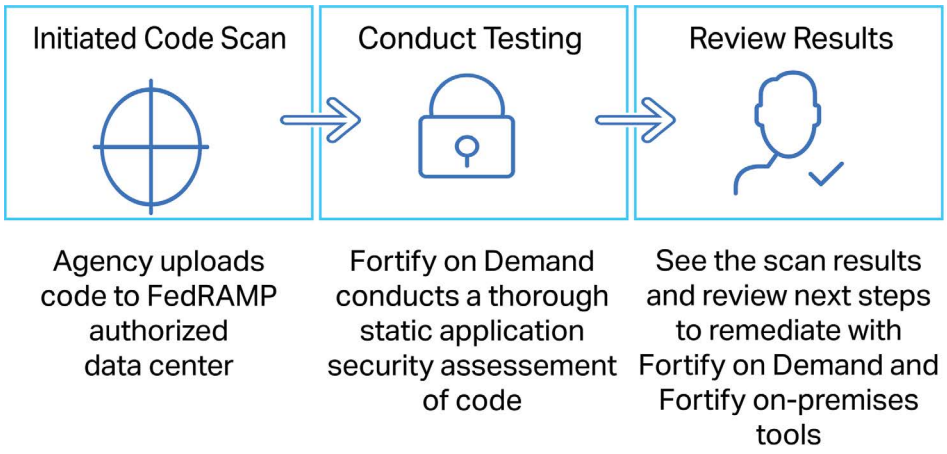

Figure 1. Fortify on Demand for U.S. Federal Application Security Process

Conduct Testing with Fortify on Demand Static Assessments

With Fortify on Demand, developers have the intelligence at their fingertips to build better and more secure software—right from the start. Our comprehensive static scan assessments help developers identify and eliminate vulnerabilities in source or byte code—all to help your business build more secure software. Powered by Micro Focus Fortify Static Code Analyzer (SCA), Fortify on Demand static assessments detect over 763 unique categories of vulnerabilities across 25 programming languages that span over 911,000 individual APIs.

Static assessment capabilities with Fortify on Demand are among the most comprehensive and flexible available worldwide. Fortify on Demand is designed to meet the needs of AppSec leaders for comprehensive application risk management, plus the desire of developers for speed and ease of use. Capability highlights include:

- Support for ABAP/BSP, ActionScript, Apex, ASP.NET, C# (.NET), C/C++, Classic ASP (with VBScript), COBOL, ColdFusion CFML, HTML, Java (including Android), JavaScript/AJAX, JSP, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Scala, Swift, T-SQL, VB.NET, VBScript, Visual Basic, and XML
- Comprehensive scanning coverage across source code, byte code, or object code for any type of application: web, mobile, embedded or thick-client
- Flexible static assessment licensing models with single scan or subscriptions available

Detailed Reporting of Static Scan Results and Vulnerability Management

Fortify on Demand users have the ability to access detailed information behind scan results, particularly as it relates to vulnerability management. Our static scan results include detailed information about each vulnerability detected, guidance on remediation, and links to industry sources with details about the specific vulnerability identified. When coupled with Fortify on-premises licensing, your agency is armed with a proven approach to efficiently identify and then eliminate vulnerabilities in Federal Government applications. An example of the Fortify on Demand Application Issues experience is shown in the screen shot provided.

Our vulnerability management is purpose-built for the FedRAMP environment and spans:

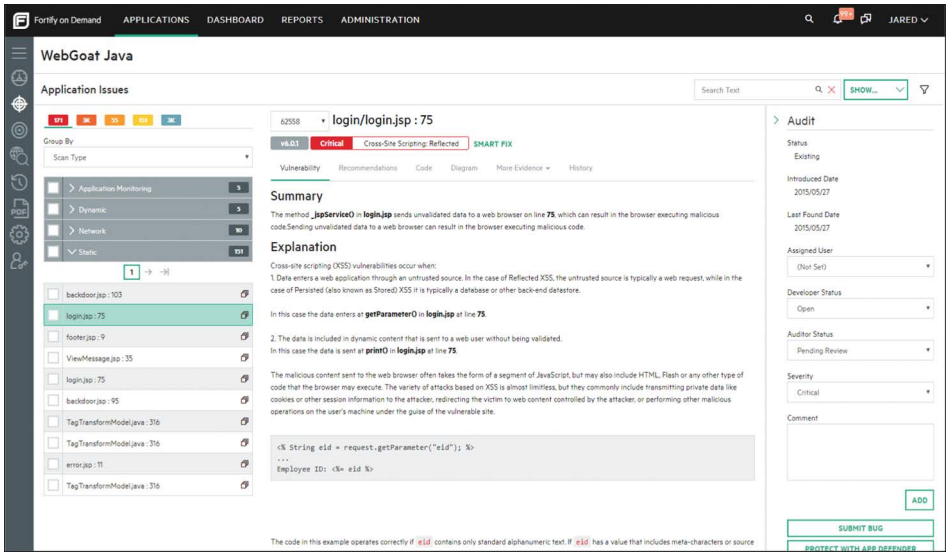

Figure 2. Fortify on Demand Application Issues Page

- Mapping to required and relevant vulnerability frameworks, including FISMA (NIST 800.53), DISA Application Security and Development STIG, MITRE CWE, OWASP, PCI, and many others.
- Reporting in detail of the application against the DISA Application Development STIG in support of the Risk Management Framework (RMF) controls. This reporting provides a "pass/fail" score of the application vs. the DISA Application STIG and thereby the RMF controls.
- Submitting vulnerability reports as part of the documentation packages for the Authority to Operation (ATO), Certification and Accreditation (C & A), Command Cyber Readiness Inspection (CCRI), and other Department of Defense (DoD) or federal certification milestone reports. Such documentation packages provide the artifacts required to demonstrate that automated source code analysis has been completed per the mandatory DISA Application Security and Development STIG requirement.

Faster Remediation with Smart Fix

The Smart Fix issue flow diagram offers enhanced display and navigational functionalities for better usability, particularly around highlighting shared data flows to quickly identify optimal remediation strategies to fix multiple static issues at once. This is driven by a toggled heat map that enables or disables the complete data flow path. Developers can isolate, identify, and remediate vulnerabilities across functional relationships within the application. Shown in the Smart Fix screen shot as indicated, AppSec leaders and developers can visually identify critical vulnerabilities (in red) and determine how these code streams impact other elements of the application.

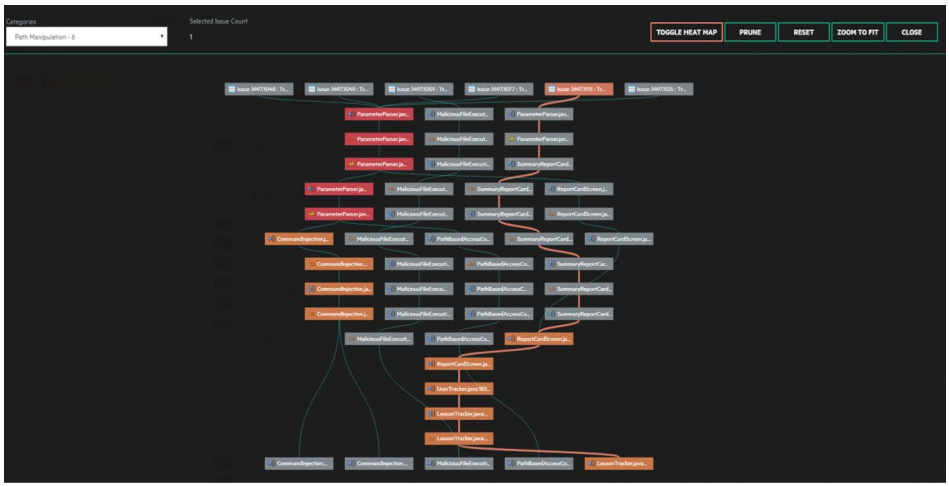

Figure 3. Fortify on Demand Smart Fix Example

Fortify on Demand Assessment Units

Fortify on Demand application security testing services are available by purchasing and redeeming Assessment Units. Fortify on Demand Assessment Units are prepaid credits that are redeemed for single assessments or application subscriptions, offering flexibility to allocate your investment throughout the year.

Assessment Units are valid for 12 months and may be redeemed individually. An application subscription allows for one application to be assessed an unlimited number of times for basic Static service, or monthly for Static+ service, during the 12 month period commencing on date of purchase.

Fortify on Demand Service Levels for U.S. Federal Agencies

We offer three service levels to meet your business objectives:

1. **Single Static + Application Security Assessment** (Single Assessment, 2 Assessment Units)

   Fortify on Demand will perform a Single Static+ Assessment which consists of the following activities:

   – Perform static code analysis using Fortify Static Code Analyzer (SCA) of the application source, byte and/or object code uploaded by the Customer
   – Review of prioritized results by a Fortify on Demand security expert, including false positive removal
   – One (1) remediation validation within thirty (30) days of the assessment

   Recommended for baseline audits of application portfolios as well as baseline/update audits for individual applications subject to periodic development activity (examples: legacy or maintenance applications).

2. **Subscription Static + Application Security Assessment** (Subscription, 6 Assessment Units)

   Fortify on Demand will perform Monthly Static+ Assessments during the Subscription Term. A Static+ Assessment consists of the following activities:

   – Perform static code analysis using Fortify Static Code Analyzer (SCA) of the application source, byte, and/or object code uploaded by the Customer

Contact us at:
www.microfocus.com

Like what you read? Share it.

- For each assessment, Customer may choose one (1) of the following:
- Review of prioritized results by a Fortify on Demand security expert, including false positive removal
- Automated audit of prioritized results using the standard Fortify on Demand issue filter

Recommended for individual applications subject to ongoing development activity, managed development teams separate from uniform SDLC integration and/or without skilled source code security audit support.

3. **Subscription Static Application Security Assessment, Automatic Option**
(Subscription, 4 Assessment Units) Fortify on Demand will perform unlimited Static Assessments during the Subscription Term. A Static Assessment consists of the following activities:
   - Perform static code analysis using Fortify Static Code Analyzer (SCA) of the application source, byte, and/or binary code uploaded by the Customer
   - For the initial assessment, Fortify will provide a review of prioritized results by a Fortify on Demand security expert, including false positive removal
   - For all subsequent assessments during the Subscription Term, Fortify will provide an automated audit of prioritized results using the standard Fortify on Demand issue filter

   Recommended for individual applications subject to ongoing development activity, managed development teams participating in uniform SDLC integration and skilled source code security audit support.

Security Expertise and Account Support

We are committed to the successful adoption of application security within your agency. All accounts include access to a dedicated technical account management team to help drive the success of a customer's application security program. The team manages contract issues, renewals, and support requests; and coordinates Fortify on Demand resources including system and process experts as necessary to drive adoption and customer success.

Let's Get Started

Fortify on Demand offers the most comprehensive application security testing technologies, backed by industry-leading security research. We have a team dedicated to the application security needs within the U.S. Federal sector. Let us share how we can help your agency meet its business objectives.

Learn more at
www.microfocus.com/fod

MICRO FOCUS
Government Solutions