Fortify on Demand: FedRAMP Application Security as a Service

Fortify on Demand is uniquely designed to help government agencies adhere to internal risk management policies and government mandates. Developers confidently build security throughout the entire software development life cycle, and security professionals review findings and achieve required compliance reporting.

FedRAMP CyberRes Fortify on Demand for the U.S. Federal sector is the first and leading cloud-accessible managed application security testing platform. It is the only application security managed vendor that is operating on AWS GovCloud. It is JAB certified and FedRAMP authorized. With access to Fortify on Demand, Government agencies and programs can quickly, easily, cost-effectively and confidently perform application security testing and obtain the fastest, most accurate results available.

Product Highlights

Identify and Eliminate Vulnerabilities Earlier
With Fortify on Demand, developers can 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. Powered by Fortify Static Code Analyzer (SCA), Fortify on Demand static assessments detect over 781 unique categories of vulnerabilities across 27 programming languages that span over 1 million individual APIs.

- **Static assessment capabilities** with Fortify on Demand are among the most comprehensive and flexible available worldwide. That includes support for ABAP/BSP, ActionScript, Angular, Apex, ASP.NET, C# (.NET), .NET Framework and .Net Core, C/C++, Classic ASP (with VBScript), COBOL, ColdFusion, Go, HTML, Java (including Android), JavaScript/AJAX, JSP, Kotlin, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Scala, Swift, T-SQL, TypeScript, VB.NET, VBScript, Visual Basic, and XML.
- **Quick and Easy Scan Initiation**
  Upload application source code from IDE, repository, build or CI server. Manual upload via the FoD portal and automatic upload via our ecosystem of integration and flexible API.

Access Detailed Reporting of Static Scan Results and Vulnerability Management
Our vulnerability management is purpose-built for the FedRAMP environment and spans:

- 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.

Key Features

Leader in Gartner Magic Quadrant
Fortify has been named a leader in application security testing for the 8th year in a row.

Comprehensive Assessments
FoD static assessments detect over 781 unique categories of vulnerabilities across 27 programming languages that span over 1 million individual APIs.

Achieve Compliance Requirement
JAB Certified, FedRAMP authorized.

Quick and Easy Scan Initiation
Get your AppSec program started in a day. Upload application source code from IDE, repository, build or CI server. Manual upload via the FoD portal and automatic upload via our ecosystem of integration and flexible API.

Save Time with Smart Fix
Access a flow diagram for better usability to isolate, identify, and remediate vulnerabilities across functional relationships within the application.

Flexible Scanning Options
AppSec testing services available by purchasing and redeeming Assessment Units for single assessments or application subscriptions.

Security Expertise and Account Support
Access to a dedicated technical account management team 24/7.

- 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.

Conduct Dynamic Application Security Testing

Fortify on Demand Dynamic Application Security assessments mimic real-world hacking techniques and attacks using automated techniques to provide a comprehensive analysis of complex web applications and services. Featuring Fortify WebInspect for automated dynamic scanning, Fortify on Demand provides a full-service experience as all scans include macro creation for authentication and a full audit of results by our experts to remove false positives and for overall quality—a level of service you don't get with other providers.

Assessment includes:

- Ability to recognize over 250 unique vulnerability categories for web applications in QA, staging or production.
- Expanded coverage, accuracy, and remediation details with IAST runtime agent.
- Assess public-facing and internal web sites and web services.
- Generate virtual patches for all leading web application firewalls (WAFs).

Flexible Plans to Fit Your Business' Mission

- 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.

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.
- Provides access to a centralized portal with intuitive, user-friendly and comprehensive application dashboards, vulnerabilities, and work streams for a single application or across your entire portfolio.
- Integrates on-premise and cloud-based application security testing and program management solutions, specifically for U.S. government agencies.
- Over 27 programming languages covered: ABAP/BSP, ActionScript, Angular, Apex, ASP.NET, C# (.NET), .NET Framework and .Net Core, C/C++, Classic ASP (with VBScript), COBOL, ColdFusion, Go, HTML, Java (including Android), JavaScript/AJAX, JSP, Kotlin, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Scala, Swift, T-SQL, TypeScript, VB.NET, VBScript, Visual Basic, and XML.
- Automate security in the CI/CD pipeline with Swagger-supported RESTful APIs, GitHub repository, and plugins for Azure DevOps, VSTS, and Jenkins.
- Integrates with defect management tools and covers security issues caused by open source components with software component analysis tools integration.

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

Contact us at **CyberRes.com**
Like what you read? Share it.

CyberRes
A Micro Focus Line of Business