# Fortify on Demand

**Micro Focus Fortify on Demand (FoD) delivers application security as a service, providing customers with the security testing, vulnerability management, expertise, and support needed to easily create, supplement, and expand a Software Security Assurance program.**
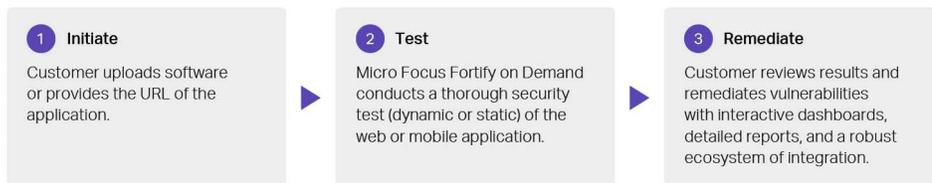


**1 Initiate**
Customer uploads software or provides the URL of the application.

**2 Test**
Micro Focus Fortify on Demand conducts a thorough security test (dynamic or static) of the web or mobile application.

**3 Remediate**
Customer reviews results and remediates vulnerabilities with interactive dashboards, detailed reports, and a robust ecosystem of integration.

**Figure 1.** Fortify on Demand: Application Security for the New SDLC

**Top 5 Reasons Customers Choose Fortify on Demand:**

- Deployment flexibility
- Ease of use
- On-demand experts
- Scalability
- Built for DevSecOps

## Product Highlights

**Enterprise Application Risk Management**
Understanding risk is an important first step in any application security initiative. Organizations must build security along the software development lifecycle. Fortify on Demand helps build a program that includes secure development, preproduction security testing, and production monitoring.

Organizations are faced with rapidly expanding applications portfolios, both in size and complexity. In addition to protecting legacy applications and certifying new releases of software developed in-house using a combination of custom and open source code, ensuring the security of out-sourced and commercial off-the-shelf applications is critical as well. For those customers purchasing third-party code, Fortify on Demand provides an easy-to-use Vendor Security Management service that doesn't require source code, allows the vendor to test applications, resolve issues, and then publish a report to the procurer.

A centralized, online portal enables Fortify on Demand customers to get started quickly and build a comprehensive Software Security Assurance program over time. Dashboards provide visibility to an organization's entire application security portfolio, allowing them to view program risk, address critical security issues early, and prioritize remediation efforts across many teams and applications.

## Key Benefits

**Secure Development**
Finding and fixing application security issues early, during development, is far less costly than waiting until after an application has been deployed, so empowering developers to create secure software from inception is critical. Fully integrated within the IDE where developers work, static assessments provide immediate feedback to the developer. Open source component analysis is available and can be added with a mouse click to avoid including known vulnerable components. Audited scan results, including line of code details and remediation advice, help drive secure coding best practices. As organizations further mature and adopt DevOps principles, Fortify on Demand static assessments are often integrated into the software toolchain as an automatic step in the continuous build and integration pipeline.

**Security Testing**

A dynamic or mobile assessment of the running application in a QA, test, or staging environment simulates the real-world hacking techniques and attacks employed by hackers. For web applications and web services, dynamic assessments employ a combination of automated and manual testing techniques to crawl the application attack surface and identify exploitable vulnerabilities before an application release is deployed to production. Furthermore, interactive application security testing (IAST), with Fortify's runtime agent, supercharges dynamic testing to find more vulnerabilities—and fix them faster.

Similar to dynamic testing for web applications, Fortify on Demand mobile assessments utilize the compiled application binary and employ a combination of automated and manual techniques to identify vulnerabilities across all three tiers of the mobile ecosystem— client device, network, and backend services. More than just simple reputation or behavioral analysis, mobile assessments provide true security testing for companies serious about securing their mobile applications.

**Security Production Monitoring**

Inevitably, not all vulnerabilities can be remediated for every application before it goes live. Misconfigurations in production environments can introduce issues not present in preproduction, and new zero-day vulnerabilities arise in-between release cycles. A robust production monitoring regimen includes continuous dynamic scanning for vulnerabilities and run time detection of security events in the application itself. Fortify on Demand provides all production application monitoring activities in a single, integrated place, ensuring the continuity of application security throughout the entire SDLC..

## Key Features

**Static Application Security Assessments**

Static assessments help developers identify and eliminate vulnerabilities in source, binary, or bytecode to build more secure software. Powered by [Micro Focus Fortify Static Code Analyzer (SCA)](#), static assessments detect over 781 unique categories of vulnerabilities across 27 programming languages that span over 1 million individual APIs. Fortify on Demand static assessments can also include a review by our security experts and our innovative

Fortify Scan Analytics machine learning platform to remove false positives and ensure overall quality so that development teams can maximize their remediation efforts early in the software lifecycle. Fortify on Demand seamlessly fits into customers' existing agile or DevOps processes with out-of-the-box IDE, continuous integration/continuous deployment (CI/CD), and bug tracker integrations.

**Features**

- Supports 27+ languages: ABAP/BSP, ActionScript, Apex, ASP.NET, C# (.NET), C/C++, Classic ASP (with VBScript), COBOL, ColdFusion CFML, GoLang, HTML, Java (including Android), JavaScript/AJAX/Node.js, JSP, Kotlin, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Scala, Swift, T-SQL, VB.NET, VBScript, Visual Basic, and XML
- Microservice licensing model for modern application development
- Real-time vulnerability identification with Security Assistant
- Actionable results in <1 hour for most applications with DevOps automation.

| | Static | Static+ |
|---|---|---|
| Application type | Web, mobile or thick-client | Web, mobile or thick-client |
| Fortify SCA analysis | + | + |
| Fortify Scan Analytics automated audit | + | + |
| Security Assistant | +[1] | +[1] |
| Security expert manual review | [2] | + |
| Open source analysis | +[3] | +[3] |

1. Subscriptions only
2. Security expert review optional for first subscription scan only
3. Added Sonatype subscription needed

**Open Source Software Composition Assessments**

Third party components make up a significant portion of many applications' codebase, making Software composition analysis a "must-have" AppSec capability using natural language processing to dynamically monitor every GitHub commit to every open source project, advisory websites, Google search alerts, OSS Index, and a plethora of

vulnerability sites. Powered by Sonatype, Fortify on Demand's Software Composition Analysis is much more than a simple comparison of declared dependencies against the National Vulnerability Database (NVD). Additionally, new vulnerabilities are regularly discovered by a dedicated team of security researchers and added to the proprietary knowledge-base. Fortify on Demand simplifies the onboarding and

scanning process by combining static and composition analysis into a single integration point, whether that's in the IDE or CI/CD pipeline. The comprehensive bill-of-materials including security vulnerabilities and license details is delivered as a fully integrated experience for security professionals and developers alike.

**Features**

- Provide code once for both SAST and software composition analysis
- Supports Java, .NET, Javascript and Python
- Integrated results deliver one platform for remediation, reporting and analytics
- Examines fingerprints of 65M components for high accuracy—not just file names and package manifests
- Detects 70% more vulnerabilities than the NVD database alone

**Dynamic Web Application Security Assessments**

Dynamic assessments mimic real-world hacking techniques and attacks using both automated and manual techniques to provide 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. Our manual testing focuses on the types of vulnerabilities that skilled hackers exploit, including authentication, access control, input validation, session management, and business logic testing. And once an application is deployed, Continuous Application Monitoring provides production-safe vulnerability scanning for the most critical vulnerabilities across the OWASP Top 10 and risk profile change detection.

**Features**

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

|  | Dynamic | Dynamic+ |
|---|---|---|
| Application type | Website | Website OR web services[4] |
| Fortify WebInspect analysis | + | + |
| Verify URL & authentication | + | + |
| Security expert manual review | + | + |
| Interactive application security testing (IAST) | + | + |
| Continuous application monitoring | +[5] | +[5] |
| Manual vulnerability testing |  | + |

4. Single scans only for web services.
5. Subscriptions only. Includes vulnerability and risk profile scanning; discovery sold separately.

**Mobile Application Security Assessments**

Fortify on Demand delivers comprehensive end-to-end mobile security with real-world mobile application security testing across all three tiers of the mobile ecosystem—client device, network, and web services. Similar to dynamic testing for web applications, mobile assessments utilize the compiled application binary and employ the same techniques hackers utilize to exploit vulnerabilities in mobile applications, whether they are developed internally, outsourced, or acquired. More than just simple reputation or behavioral analysis, Fortify on Demand mobile assessments provide true security testing for companies serious about securing their mobile applications.

**Features**

- Supports iOS and Android mobile applications
- Identifies over 300 unique vulnerability categories from mobile binary to backend services
- Emphasizes security vulnerability identification in addition to behavioral and reputation analysis
- Automated mobile binary assessments in <5 minutes for most applications
- Manual testing performed on physical devices

|  | Mobile | Mobile+ |
|---|---|---|
| Application type | Mobile binary | Mobile binary and backend services |
| Vulnerability analysis (mobile binary) | + | + |
| Endpoint reputation analysis | + | + |
| Security expert manual review | + | + |
| Fortify WebInspect analysis (backend services) |  | + |
| Manual vulnerability testing |  | + |

## Assessment Units

Fortify on Demand static, dynamic and mobile 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.

For each single assessment or subscription requested, customers choose a combination of one assessment type (dynamic, static, or mobile) and one assessment service level. An application subscription allows for one application to be assessed an unlimited number of times during the 12 month period. All assessments include one remediation validation scan within one month of the assessment.

| Assessment Type | Single Assessment | Subscription |
|---|---|---|
| Static Assessment | 1 Assessment Unit | 4 Assessment Units |
| Static+ Assessment | 2 Assessment Units | 6 Assessment Units |
| Dynamic Website Assessment | 2 Assessment Units | 6 Assessment Units |
| Dynamic+ Website Assessment | 6 Assessment Units | 18 Assessment Units |
| Dynamic Web Services Assessment | 2 Assessment Units | 6 Assessment Units |
| Dynamic+ Web Services Assessment | 6 Assessment Units | N/A |
| Mobile Assessment | 1 Assessment Unit | 4 Assessment Units |
| Mobile+ Assessment | 6 Assessment Units | 18 Assessment Units |

**Table 4.** Redeeming Fortify on Demand Assessment Units

## Secure Development Training

Secure Development Training for everybody involved in the software development lifecycle is a cornerstone of any application security program and helps reduce the organizations' exposure to application security risk. Most organization are aware that secure development training is a key security control that helps reduce application security risk. However, all too often, it is only available on an ad-hoc basis.

Fortify on Demand provides over 100 hours of application security training material split into 13 role-based curricula, managed through the Fortify on Demand platform.

### Features

- Mandate training for all development personnel before they are allowed to participate in the application development process

- Provide training appropriate to the individual's needs—no more, no less. For example: a regular Java developer should receive specific training in how to develop secure Java code. A Java developer for an e-commerce application will need more advanced training

- Make training available on-demand to enable easy scheduling and minimize impact on developer productivity

- Offer a scalable solution for everybody involved in development including third-parties if appropriate

- Provide up to date content to ensure new threats and new technologies are understood and addressed

### Support

Fortify on Demand is designed as a self-service platform that includes context sensitive help, video tutorials, chat support, and helpdesk ticketing available 24x7 through a dedicated support team. For larger customers, the service includes a Technical Account Manager (TAM) to help drive adoption of the service and ensure customer success. The TAM is the customer's primary point of contact, proactively supporting the on-boarding of the first development team, managing support issues and holding regularly scheduled service reviews. Additional onsite or remote support services are available at additional charge.

### About Micro Focus Fortify

Fortify offers the most comprehensive static and dynamic application security testing technologies, along with run time application monitoring and protection, backed by industry-leading security research. Solutions can be deployed in-house or as a service to build a scalable, nimble Software Security Assurance program that meets the evolving needs of today's IT organization.

Learn more at
**www.microfocus.com/en-us/cyberres/application-security/fortify-on-demand**

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

**{S} Saltworks**
An Orasi Company

**CyberRes**
A Micro Focus line of business

orasi