

# HP Fortify on Demand

## Software security testing in the cloud



### Hosted software security

HP Fortify on Demand is a Security-as-a-Service (SaaS) testing solution that allows any organization to test the security of software quickly, accurately, affordably, and without any software to install or manage. This automated on-demand service helps organizations with two key challenges:

- Ensuring the security of custom built software applications as well as those from third parties
- Increasing the speed and efficiency of building security into a development lifecycle

HP Fortify on Demand serves the role of an independent, third-party system of record, conducting a consistent, unbiased analysis of an application and providing a detailed tamper-proof report back to the security and development teams. Users simply upload their application source code and/or provide a URL for testing. HP Fortify on Demand can conduct a static and/or dynamic test, verify all results, and present correlated findings in a detailed web-based interface and report. HP Fortify on Demand solutions can scale to meet the needs of any size organization.

The HP Fortify on Demand highly secure SaaS environment is easy to use—no hardware, software or expertise required. Get started with HP Fortify on Demand in three easy steps.

### How HP Fortify on Demand works

#### 1. Initiate

Upload your source code or point us at your URL and receive a comprehensive application layer test that encompasses static and dynamic analysis. Leverage HP Fortify on Demand with your build server to make uploads more frequent and automated for all applications.

- In-house - Collaborate with your developers to test in-house applications before you deploy into production.
- Commercial - Protect your investments by ensuring all commercial software is secure before licensing.
- Outsourced - Guarantee that your outsourced code is written securely.
- Open source - Ensure that any open-sourced software is compatible with your security expectations.

#### 2. Test

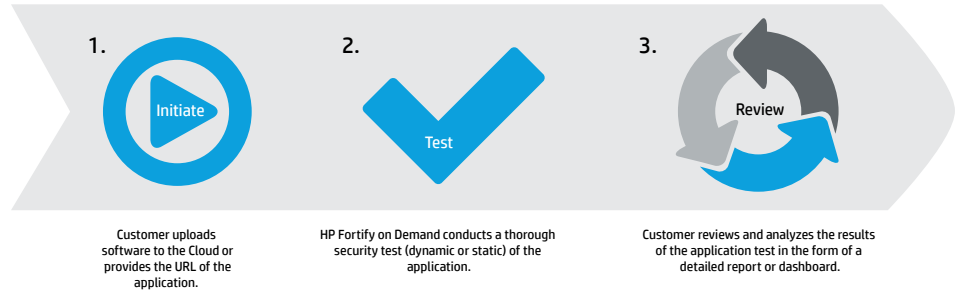
Our SaaS expert team will conduct a thorough audit of your application for security vulnerabilities.

- Static analysis - Users simply and securely upload, byte, or source code, and HP Fortify on Demand completes award-winning static analysis.
- Dynamic analysis - Users provide the URL of any application either in QA or production, and HP Fortify on Demand can be scheduled to test automatically at one of three levels of service.
- Expert review - All results are reviewed manually by a software security expert to ensure the highest degree of accuracy.

“Almost half of tested applications in 2012 were vulnerable to Cross-Site Scripting vulnerabilities.”

-HP 2012 Cyber Security Risk Report

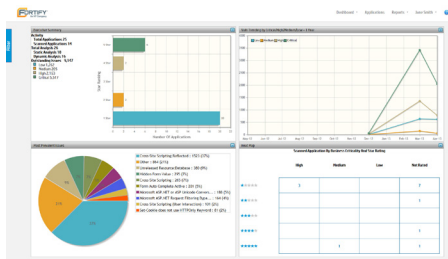
**Figure 1.** Shown are the three key steps of the HP Fortify on Demand process.



**3. Review**

Review detailed and correlated results.

- Executive dashboard - Monitor and manage all your application testing projects from a single point of record. Development and security teams can save time, effort, and headaches by communicating and collaborating through a central location.
- Technical dashboard - View the top 5 worst performing projects, OWASP top 10 category trending, outstanding remediation project in the last 4 weeks, and issue assignment vs. unassigned by criticality.
- Detailed reporting - Assessments are delivered in a report featuring a consistent five-star rating system typically in one day. Results are correlated and prioritized by severity and exploitability. Issues identified include line of code-level details with suggestions on how to fix.



**HP Fortify on Demand Executive Dashboard**

The Executive Dashboard shows key results for your application testing projects from a single screen.

**HP Fortify on Demand use cases**

HP Fortify on Demand can secure any application, whether it’s developed internally or by third-party organizations. Typically, it’s used in these scenarios:

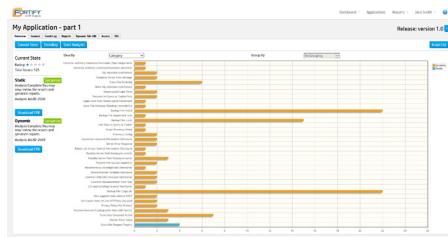
**Security testing for internal applications**

This enables any organization to test the security of all in-house software-whether in development or deployed in production. HP Fortify on Demand establishes a security baseline across the entire software portfolio. With no hardware or software to deploy or maintain, customers can test more applications-hundreds or even thousands-efficiently and effectively. Short on staff? The HP Fortify team of experts provides all the testing and triaging necessary. With an annual subscription, HP Fortify on Demand users can enjoy unlimited assessments.

**Security testing for third-party applications**

HP Fortify on Demand provides an independent review of third-party applications, allowing organizations to test software before purchasing, and also allowing software vendors to demonstrate the security of their software. Third-party vendors can upload the source code and/or provide a URL, review the results, and then publish a report back to their customer. This service compels commercial vendors to take action to proactively fix vulnerabilities, while allowing them to remain in control of their applications. Security professionals can demand that high-priority problems be addressed and verified during the procurement or upgrade process, prior to acceptance. HP Fortify on Demand serves as an independent third-party solution to conduct unbiased analysis of applications and provide a detailed tamper-proof report back to the security team.

**Figure 2.** Detailed reporting: Fortify on Demand reporting can correlate the results from different forms of testing and prioritize them by severity to present the truest representation of application risk. screenshot named fod detailed reporting



## Selecting the right solution for you

How do you choose between an on-premise or on-demand solution?

HP Fortify doesn't lock you into your investment. We offer both an on-premise and an on-demand solution.

- Some companies start with HP Fortify on Demand due to the low cost of ownership and the luxury of quickly jumpstarting their software testing. Later, they may decide to bring the technology in-house, once the expertise has ramped up.
- Other companies select a hybrid model, with some applications sent to the cloud for testing and others analyzed in-house during development.
- Companies also find that Fortify on Demand is incredibly easy to use and determine the ROI for them is higher when utilizing FoD for all their applications.

With HP Fortify, customers have the flexibility to adopt either or both an on-demand and an on-premise solution. Our on-demand and on-premise solutions leverage the same analysis techniques, vulnerability categorizations, and application rating systems. HP is the only company that offers this flexibility in deployment.

## About HP Fortify on Demand

### HP Fortify on Demand features

- Best-of-breed analysis
  - Market-leading static and dynamic capabilities
  - Analysis capabilities tested across Fortify customers since 2001
  - Largest, most experienced security research team
- Correlated static and dynamic results with detailed priority guidance
- Accurate results, tailored to each application
- Supports Web, mobile, and thick-client apps
- All results manually reviewed by application security experts
- Central testing program management for all applications

### HP Fortify on Demand benefits

- Easy to manage: no hardware, no software, and no maintenance
- Fast: results typically in less than 24 hours for static assessments
- Flexibility to migrate easily and quickly to the HP Fortify on-premise solution and vice versa
- Easy to get started - no need to wait for lengthy procurement, approvals or deployments
- Quickly pass compliance with PCI, HIPAA, FISMA, and many other standards
- Custom solutions that can fit any size organization
- Detailed reporting including correlated results prioritized by severity to present the truest picture of application risk

### HP Fortify on Demand specifications

- Static analysis - byte, or source code for 21 different languages
- Dynamic Analysis - All Web languages
- Mobile Analysis - Android, Apple iOS, Blackberry, and Microsoft

## “Mobile application vulnerabilities increased 68% from 2011 to 2012”

-HP 2012 Cyber Security Risk Report

### HP Fortify on Demand integrations

- HP Application Lifecycle Management (ALM) - HP Fortify on Demand results can be imported into ALM, letting organizations track security vulnerabilities like other software defects.
- Archer - HP Fortify on Demand results can automatically be exported into Archer to help prove compliance.
- Build server - customers can set up an automated process for uploading applications from a build server.

## Static Languages

### Languages Supported

ABAP/BSP	COBOL	Python
ASP.NET	JavaScript/Ajax	Ruby
C	Java (with Android)	T-SQL
C#	JSP	VB6
C++	Objective C	VBScript
Classic ASP	PHP	VB.NET
ColdFusion	PL/SQL	XML/HTML

## HP Fortify on Demand Dynamic

HP Fortify on Demand offers three Dynamic assessment types. Most customers choose an assessment type based on the risk profile of the application being testing. Typically Marketing applications are tested with Basic while PCI and HIPAA applications are tested with the Premium dynamic assessment

<b>Basic</b>	<ul style="list-style-type: none"> <li>• An automated solution for Web Applications</li> <li>• Baseline includes an assessment via HP WebInspect security scanner</li> <li>• All results are manually reviewed by security experts to remove false positives</li> </ul>
<b>Standard</b>	<ul style="list-style-type: none"> <li>• An automated solution for Web Applications that are a permanent fixture in a customer’s online experience and have multi step form-based processes, but are not necessarily mission-critical</li> <li>• Standard manual testing for technical vulnerabilities</li> <li>• Standard includes the use of multiple automated and manual testing solutions</li> <li>• All results are manually reviewed by security experts to remove any false positives</li> </ul>
<b>Premium</b>	<ul style="list-style-type: none"> <li>• An automated and manual testing solution for Web Applications that are permanent and mission-critical, have rigorous compliance requirements and, in which, the customer relies on serving its clients or business partners and has multi step form-based processes</li> <li>• Premium includes testing for both technical and business logic vulnerabilities</li> <li>• Uncovering the business logic vulnerabilities requires manual review by website security experts who are capable of understanding things like account structures and the contextual logic in Web applications</li> <li>• Includes Web services for up to 10 endpoints</li> <li>• Premium includes a static assessment as well if customer has access to the source or byte code for the applications being assessed. This is optional</li> <li>• All results are manually reviewed by security experts to remove any false positives</li> </ul>

## Mobile assessment offerings

Mobile Analysis	Basic	Standard	Premium
App Risk Level	Low Marketing App	Medium Personally Identifiable	High Credit Card/SSN
Client Layer - Source	√	√	√
Client Layer - Dynamic		√	√
Client Layer - Binary			√
Network Layer - Dynamic		√	√
Server Layer - Static & Dynamic			√
Remediation Scan	√	√	√

## About HP Fortify Software Security Center

HP Fortify on Demand is a part of the HP Fortify Software Security Center suite, a comprehensive solution for automating and managing an application security program in the enterprise. HP Fortify Software Security Center proactively eliminates the immediate risk in legacy applications, as well as the systemic risk in application development processes.

## About HP Enterprise Security

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market leading products from HP ArcSight, HP Fortify, and HP TippingPoint, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats. Find out more at [hp.com/go/SIRM](http://hp.com/go/SIRM)

## About HP Fortify

HP Fortify offers comprehensive SSA solutions featuring the broadest line of products and services in the market today. HP Fortify solutions help you build trust in the software you depend on by helping you find, fix, and fortify applications in less time and for less cost than comparable tool-centric strategies.

Learn more at  
[hp.com/go/Fortify](http://hp.com/go/Fortify)

Sign up for updates  
[hp.com/go/getupdated](http://hp.com/go/getupdated)



Share with colleagues



Rate this document

© Copyright 2012-2013 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Java is a registered trademark of Oracle and/or its affiliates.

4AA4-0664ENW, July 2013, Rev. 1

