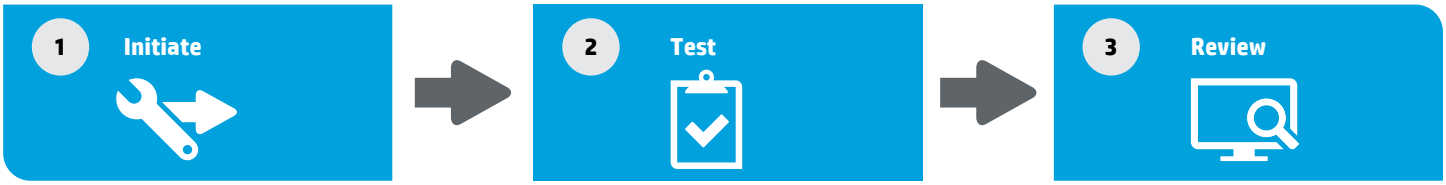
Data sheet

HP Fortify on Demand

Managed application security testing available on demand

HP Fortify on Demand is a managed application security testing service that makes it simple to initiate security tests on a few applications or launch a comprehensive security program without upfront investment of technology and resources. Combining advanced dynamic and static testing technologies (HP Fortify) with HP's experience in evaluating software security, Fortify on Demand brings professional-level software security expertise to organizations of any size.



Customer uploads software to the cloud or provides the URL of the application.

Fortify on Demand conducts a thorough security test (dynamic or static) of the application.

Customer reviews and analyzes the results of the application test in the form of a detailed report or dashboard.

Enterprise application risk management

Assessing internal applications
With internally developed applications, Fortify on Demand helps in two primary ways. For companies with a secure development lifecycle already in place, Fortify on Demand can provide a final test before deployment. For organizations new to security, Fortify on Demand can provide a quick and accurate application security test to baseline applications and prioritize efforts to improve application security.

To accelerate time to market, companies are increasingly relying upon outsourced development resources and open source software. Third party developers may not follow the same best practices instituted with in-house developers while open source code can be filled with known vulnerabilities. Fortify on Demand enables companies to identify and assess the security risk of outsourced or open source content and implement the necessary security control strategies. With Fortify on Demand, companies can maintain fast-paced delivery of secure applications, no matter the source.

Vendor application security testing and management
For most organizations, third-party code represents a large percentage of deployed software, and therefore, a substantial area of potential risk. Yet most vendors provide little or no visibility into the security state of their products. Companies should ensure their third-party software is tested for vulnerabilities during the procurement or upgrade process, and request that critical issues be addressed prior to acceptance.

However, software vendors are, for a variety of reasons, resistant to having their software analyzed by anyone but themselves. Vendors are concerned about providing access to their most precious intellectual property, their source code. Fortify on Demand provides an easy to use security-as-a-service based approach that doesn't require source code, and allows the vendor to test applications, resolve issues, and then publish a report to the procurer. Fortify on Demand serves as an independent third party and system of record for conducting a consistent, unbiased analysis.

Service features and benefits

Cloud-based managed service
Fast and easy to start an application security program with minimal upfront investment that has the flexibility to scale with changing business needs. There is no need to install, procure, and maintain hardware or hire and retain a large staff of application security experts.

Fast results
Accurate, detailed results delivered on many assessments in one to three days.

Centralized portal
User-friendly dashboards and reporting make it simple to manage an application portfolio and collaborate across distributed teams. Assess risk, initiate scans, analyze results, and remediate vulnerabilities based on prioritized recommendations.

Global presence
Data centers in the United States, Europe, and Japan paired with 24x7 testing capabilities to meet the needs of a worldwide customer base. Choose from a growing list of supported languages, including English, Japanese, and Spanish.

Software security research
Access to real-time threat intelligence updates from HP Security Research.

Personalized support
Results are manually reviewed by application security experts. You also receive a technical account manager responsible for ensuring overall customer satisfaction, driving adoption of the service, and providing best practice guidance.

Comprehensive security testing solution
Integrate with security software offerings including HP Software Security Center and HP TippingPoint to build a powerful security program. IDE plug-ins, build server integration, WAF, digital vaccines, and bug tracking are supported as well.

Service descriptions

Application security testing
Fortify on Demand dynamic, static, and mobile application security testing services are available by purchasing HP Fortify on Demand Assessment Units. Fortify on Demand Assessment Units are pre-paid 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 starting at the purchase order (PO) effective date and may be redeemed individually.

Table 1. Fortify on Demand Assessment Units

Assessment service level	Single assessment	Application subscription
Express	N/A	1 Assessment Unit
Basic	2 Assessment Units	6 Assessment Units
Standard	4 Assessment Units	12 Assessment Units
Premium	8 Assessment Units	25 Assessment Units

For each single assessment or subscription requested, the customer chooses a combination of one assessment type (dynamic, static, or mobile) and one assessment service level. Customers that perform a single assessment can request one remediation validation scan within one month of the assessment. An application subscription allows for one application to be assessed an unlimited number of times for a period of 12 months starting at the PO effective date (irrespective of when Fortify on Demand Assessment Units are redeemed).

Customers are also able to purchase multiple years' worth of assessment units on a single PO (two or three years). For multi-year commitments, a set annual allotment of assessment units is purchased and each year's allotments are issued on the anniversary of the PO effective date. Each year's allotment of assessment units must be used within 12 months and are not "rolled over" to subsequent years.

Table 2. Assessment Service Levels

	Express	Basic	Standard	Premium
Dynamic assessments				
Technique	Fast automated	Full automated	Full automated + manual	Full automated + manual
False positive removal	No	Yes	Yes	Yes
Authentication	No	Yes	Yes	Yes
Logic	No	No	No	Yes
Source code	No	No	No	Yes
Web services	No	No	No	10 endpoints
Target turnaround	< 1 day	< 3 days	< 5 days	< 7 days
Static assessments				
Languages	Java, .NET	21+*	N/A	N/A
Upload file size	< 75 megabytes	All sizes	N/A	N/A
Vulnerability categories	Cross-site scripting, SQL injection	All categories	N/A	N/A
Audit review	No	Yes	N/A	N/A
False positive removal	No	Yes	N/A	N/A
Target turnaround	< 1 day	< 2 days	N/A	N/A
Mobile assessments				
Platforms	iOS, Android	iOS, Android, Windows®, BlackBerry	iOS, Android	iOS, Android, Windows, BlackBerry
Client: automated binary	Yes	No	Yes	Yes
Client: manual binary	No	No	OWASP top 10	All categories
Client: source code	No	Yes	No	Yes
Network	No	No	OWASP top 10	All categories
Server: Web services (dynamic)	No	No	OWASP top 10	All categories
Server: Web services (source code)	No	No	No	Yes
False positive removal	No	Yes	Yes	Yes
Target turnaround	< 1 day	< 2 days	< 2 days	< 7 days

* Supported languages for static basic assessments are ABAP/BSP, ASP.NET, C, C#, C++, COBOL, Classic ASP, ColdFusion, FLEX, HTML, Java (with Android), JavaScript/AJAX, JSP, Objective-C, PHP, PL/SQL, Python, Ruby, Transact-SQL, VB.NET, VB6, VBScript, or XML.

Web services assessment

Web services assessments are offered in buckets of 10 endpoints and can be added to any level of dynamic testing. A customer can request a Web services assessment by redeeming four (4) Fortify on Demand Assessment Units.

Digital risk assessment

Fortify on Demand offers an internal or external digital discovery assessment on domains and Internet protocol space assets owned by the customer. This assessment helps the customer determine how many live or unknown websites the company owns, which of those websites house unknown application functionality, and the risk profile of these sites. A customer can request a digital risk assessment by redeeming fifty (50) Fortify on Demand Assessment Units.

Operational services

HP delivers ongoing infrastructure and support services including the following:

Customer support
HP maintains a team of support staff, which will be the single point of contact for all issues related to the infrastructure and support for Fortify on Demand. Customers may contact HP through a variety of methods such as in-portal chat, support tickets, telephone, or email. HP support team either provides support to the customer directly or coordinates delivery of HP software support. The severity of the request determines the response and resolution time. For additional details, customers can visit the Help Center within the Fortify on Demand portal.

Technical account manager
All accounts include the service of a technical account manager (TAM) to help drive the success of a customer's application security program. The TAM serves as the customer's Fortify on Demand liaison via the Help Center; manages contract issues, renewals, and support requests; and coordinates HP resources including system and process experts as necessary to drive adoption and customer success.

Capacity and performance management
All tiers of the Fortify on Demand infrastructure are proactively monitored for capacity and performance. Our architecture allows for addition of capacity to applications, databases, and storage. Capacity is increased as required as the customer's utilization of Fortify on Demand expands.

Change management
HP follows a set of standardized methods and procedures for the efficient and prompt handling of changes to the infrastructure and application, which enable beneficial changes to be made with minimal disruption to the service.

Scheduled upgrades and maintenance
Upgrades and binary patches are performed by HP as part of the service when an upgrade version is ready and has been validated in the data center environment.

Availability service-level objective
Fortify on Demand is designed for an availability service-level objective of 99.5 percent, which starts on the Go Live Date. "The Go Live Date" is the date at which point the customer end users access the production environment with production data. The availability service-level objective shall not apply to performance issues:

- Caused by overall Internet congestion, slowdown, or unavailability
- Caused by unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks, etc.
- That resulted from actions or inactions of the customer (unless undertaken at the express direction of HP) or third parties beyond the control of HP
- That resulted from the customer's equipment or third-party computer hardware, software, or network infrastructure not within the sole control of HP
- That resulted from scheduled infrastructure maintenance downtime to implement major version upgrades

Assumptions

- For dynamic assessments, an application is defined as a fully qualified domain name (FQDN) and has a single authentication management system. Customer must confirm that its Web application and user credentials are functioning prior to the security assessment. In addition, all functional and performance testing should be completed by this time, and the application's code should be frozen for the duration of the security test engagement. Any cancellations or delays of more than two hours require 24-hour notice prior to the scheduled assessment. The customer may be required to confirm authorization to perform a security assessment of the application. HP is not liable for any monetary or technical damages as a result of the assessment on the requested URL.
- For static assessments, an application is defined as a deployable unit of code consisting of a collection of source and/or byte code instruction files that:
  - Can deliver some or all of the functionality of a business application
  - Is written in the same technology family
  - Is built on a single platform
  - Does not include any loosely coupled components
  - Can be configured to run on an application server (e.g., a Web Application Archive [WAR] or Enterprise Archive [EAR] file for a Java application) or, for a .NET application, is defined as a solution in team foundation server. Mobile applications must meet the minimum requirements for the supported language version
- A subscription is valid for a single application, which cannot be changed during the subscription term purchased.
- The import of the customer's data requires that the information is made available to HP team at the appropriate implementation step and in the HP designated format, as defined in the agreed project plan.
- The customer is responsible for maintaining list of authorized users who may access the system, including creation of usernames and passwords and keeping list accurate and confidential according to the customer's internal policies.
- The customer will perform validation activities related to implementation and external application setup during the service initiation and ongoing phases.
- The customer must have Internet connectivity to access the Fortify on Demand instance.
- Fortify on Demand security service will be performed remotely. HP may choose to utilize qualified subcontractors to perform the services.
- The customer agrees to respond in a timely fashion requests for the customer business and technical data, documentation, and other information or assistance needed to provide Fortify on Demand security assessments. The customer is responsible for the accuracy and the completeness of all information it provides.
- The customer will be responsible for all data cleansing and data accuracy as part of any assessment request. These activities are to be completed in a manner consistent with the project timeline. HP is not responsible for the accuracy of the data provided by the customer.
- Fortify on Demand security service does not contemplate the sale of products or support services, which shall require the necessary terms and conditions for such purchase pursuant to separate agreement between the parties. Any software that HP uses to provide Fortify on Demand will not be provided to the customer upon termination of Fortify on Demand (This statement controls over anything to the contrary in the current software-as-a-service [SaaS] terms.).
- HP Fortify on Demand service commencement date is the date that the customer PO is booked within the HP order management system.

Additional terms

While HP performs a review of all pre-assessment information to determine the potential for adverse impact against the network and application, the customer acknowledges that some of the services are designed to test the security of computer software, and the software and/or testing services used may reveal or create problems in the operation of the systems tested. The testing may result in disruptions of and/or damage to the customer's or the customer's third-party service provider's information systems and the information and data contained therein, including but not limited to denial of access to a legitimate system user, automatic shutdown of information systems caused by intrusion detection software or hardware; or failure of the information system. HP endeavors to help minimize disruptions to the application, network while performing any automated scanning, manual validation, or penetration testing. The customer accepts the risk of such possibility and hereby waives all rights, remedies, and causes of action against HP and releases HP from all liabilities arising from such problems.

The customer acknowledges that it has the right to acquire HP services and HP products separately.

HP reserves the right to expire this data sheet according to the expiration date of the accompanying quote, or if unspecified, 45 days from the date this data sheet was delivered.

This data sheet is governed by current HP terms for SaaS. A copy of the terms may be requested.

Learn more at
hp.com/go/FortifyonDemand

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-0664ENW, November 2014, Rev. 2