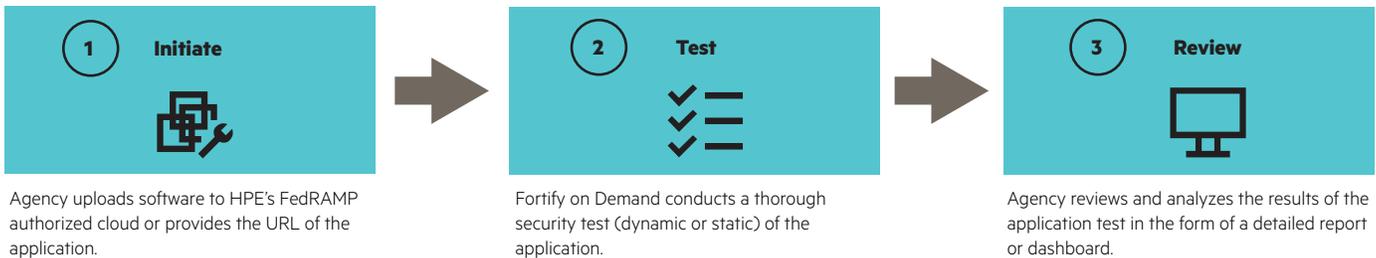




HPE Security Fortify on Demand

Managed application security testing for U.S. Public Sector



HPE Security Fortify on Demand is an application security testing and program management solution that enables government agencies to easily create, supplement, and expand a Software Security Assurance program through a managed service dedicated to delivery and customer support. Combining the most advanced application testing technologies with expert review and dedicated account management, HPE Security Fortify on Demand is part of an end-to-end software security suite delivered through a global infrastructure for true 24/7 operation.

Application risk management

Software underlies every piece of critical agency information. Yet, throughout government, there are hundreds of thousands of applications (both proprietary and third party) being used that have never been checked for vulnerabilities. Meanwhile, exploitation of widely deployed client-side and server-side applications are still commonplace (HPSR Cyber Risk Report 2015). This lack of software security assurance leaves gaping security holes throughout government networks, allowing attackers to evade detection and gain access to our country's most critical assets.

For government agencies, securing software is no longer a "nice to have"—something that can be done reactively when an error is discovered in passing. Rather, software security has become a "must have." Agencies must proactively secure and monitor their software and applications from development through deployment, whether native, legacy, mobile, third party or open source.

However, doing so is often easier said than done. For most agencies, actively securing their software is not only a budgetary challenge, but also a personnel challenge. Across government, there is a critical skills gap in software security.

The first Security software as a service (SaaS) offering to achieve FedRAMP authorization, HPE Security Fortify on Demand allows government agencies to perform fast and accurate security assessments of more than 600 vulnerability categories and services, regardless of where the application resides and without any software to install or manage. It further allows agencies to easily and confidently test any outsourced, third-party, or open source software.

Software must become a new priority layer of security if agencies are to ensure the integrity of their networks and information. Through Fortify on Demand, agencies can easily and affordably take the first steps needed to achieve software security assurance and protect America's most important data and information.

**FedRAMP Authorized**

The Joint Authorization Board (JAB) of the Federal Risk and Authorization Management Program (FedRAMP) granted HPE Security Fortify on Demand a FedRAMP Provisional Authorization (P-ATO) for use by the government community on February 4, 2015. Fortify on Demand for the USPS system leverages the HPE Helion for Public Sector cloud for both hosting of the services and management of the underlying operating systems that support the software. The HPE Helion P-ATO was granted June 5, 2013. For additional information, visit fedramp.gov.

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 agency 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.

Software security research

Access to real-time threat intelligence updates from HPE 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 HPE Software Security Center and HPE 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 HPE 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
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

	BASIC	STANDARD	PREMIUM
Dynamic assessments			
Technique	Full automated	Full automated + manual	Full automated + manual
False positive removal	Yes	Yes	Yes
Authentication	Yes	Yes	Yes
Logic	No	No	Yes
Source code	No	No	Yes
Web services	No	No	10 endpoints
Target turnaround	< 3 days	< 5 days	< 7 days
Static assessments			
Languages	21 ⁺	N/A	N/A
Upload file size	All sizes	N/A	N/A
Vulnerability categories	All categories	N/A	N/A
Audit review	Yes	N/A	N/A
False positive removal	Yes	N/A	N/A
Target turnaround	< 2 days	N/A	N/A
Mobile assessments^{**}			
Platforms	iOS, Android, Windows [®] , BlackBerry	iOS, Android	iOS, Android, Windows, BlackBerry
Client: Automated binary	No	Yes	Yes
Client: Manual binary	No	OWASP top 10	All categories
Client: Source code	Yes	No	Yes
Network	No	OWASP top 10	All categories
Server: Web services (dynamic)	No	OWASP top 10	All categories
Server: Web services (source code)	No	No	Yes
False positive removal	Yes	Yes	Yes
Target turnaround	< 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.

** Mobile Standard and Premium level assessments only available in Commercial (non-FedRAMP) environment.

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

Hewlett Packard Enterprise delivers ongoing infrastructure and support services including the following:

Customer support

Hewlett Packard Enterprise 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 HPE through a variety of methods such as support tickets, telephone, or email. HPE support team either provides support to the customer directly or coordinates delivery of HPE 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 HPE 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

Hewlett Packard Enterprise 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 Hewlett Packard Enterprise as part of the service when an upgrade version is ready and has been validated in the data center environment.

**Availability service-level objective**

HPE Security 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 Hewlett Packard Enterprise) or third parties beyond the control of Hewlett Packard Enterprise
- That resulted from the customer’s equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Hewlett Packard Enterprise
- That resulted from scheduled infrastructure maintenance downtime to implement major version upgrades

In the event of a complete outage at our primary data center, a Data Recovery location is at the ready with a 4-hour recovery time objective (RTO) and 15-minute recovery point objective (RPO).

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. Hewlett Packard Enterprise 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 HPE team at the appropriate implementation step and in the HPE 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.
- 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. Hewlett Packard Enterprise 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 HPE 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.).
- Fortify on Demand service commencement date is the date that the customer PO is booked within the HPE order management system.

Contact

fodsales@hpe.com

Additional terms

While Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 HPE and releases HPE from all liabilities arising from such problems.

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

Hewlett Packard Enterprise 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 HPE terms for SaaS. A copy of the terms may be requested.

Learn more at
hpe.com/software/pubsecsecurity



Sign up for updates

★ Rate this document



© Copyright 2015–2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Java is a registered trademark of Oracle and/or its affiliates. Windows is either registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

4AA3-5229ENW, March 2016, Rev. 1