Hewlett Packard Enterprise

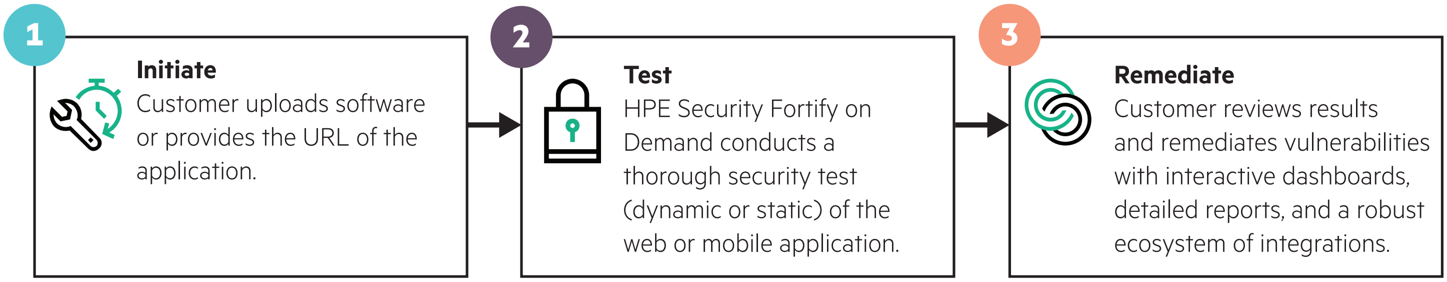
Data sheet

HPE Security Fortify on Demand

Application security as a service

HPE Security 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.

Top 3 reasons customers choose FoD over similar products in the market:
- Deployment flexibility
- Ease of use
- Quality and accuracy of scan results



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

2 **Test**
HPE Security 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 integrations.

Enterprise application risk management

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.

Understanding risk is an important first step in any application security initiative. Organizations must also take steps to build security in points along the software development lifecycle. Fortify on Demand can help build a program that includes secure development, preproduction testing, and production monitoring. Mature programs employ full "defense in depth" across all of these areas, but security teams can start from any point and grow.

Secure development

Finding and fixing application security issues early, during development, is far less costly than waiting until after an application has been deployed. Integrating **static scanning** during the build phase can quickly identify coding errors and oversights, providing immediate feedback to the developer. Open source component analysis 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 available.

Preproduction testing

A **dynamic scan** of the running application in a QA, test, or staging environment simulates the actual attacks used by the bad guys. Fortify on Demand offers three levels of fast and thorough dynamic analysis, backed by a large team of the industry's elite application penetration testers. We believe that in order to have a truly successful application security program, there must be both automated and manual components. Strictly automated application security testing solutions can miss critically important issues including authentication, access control, input validation, session management, web services, and business logic vulnerabilities—not to mention produce excessive false positives.

For those customers purchasing third-party code, HPE Security 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.

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 risk profile changes, discovery of rogue applications, 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.

Service descriptions

Static application security assessments

Static assessments help developers identify and eliminate vulnerabilities in source, binary, or byte code to build more secure software. Powered by HPE Security **Fortify Static Code Analyzer (SCA)**, every Fortify on Demand static assessment also includes a review by our security experts 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, build server, continuous integration, and bug tracker integrations.

Features

- Supports 23+ languages covering web and mobile applications
- Source, byte, and binary scanning
- False positive removal
- Unlimited file size at no additional charge or change to target turnaround
- Includes open source component analysis (powered by Sonatype)
- Target turnaround < two days

Supported languages for static basic assessments are ABAP/BSP, ActionScript/MXML (Flex), ASP.NET, VB.NET, C# (.NET), C/C++, Classic ASP (with VBScript), Java (with Android), COBOL, ColdFusion CFML, Microsoft® T-SQL, Swift, Objective C/C++, PL/SQL, JavaScript/AJAX, Classic ASP, JSP, PHP, Python, Ruby, VBScript, Visual Basic, XML, and HTML.

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 **HPE Security 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. Simply provide a URL and our team will handle the rest.

Service features and benefits

- Get started in one day
- Most accurate, comprehensive scan results on the market
- Easy-to-use management platform
- Flexible delivery—on premise or on demand
- Robust application program interface (API)
- 24x7 personalized support
- **Ecosystem** of out-of-the-box integrations

Table 1. Dynamic assessment service levels

Assessment type	Dynamic basic	Dynamic standard	Dynamic premium
WebInspect scan	Yes	Yes	Yes
False positive removal	Yes	Yes	Yes
Continuous vulnerability scanning*	Yes	Yes	Yes
Continuous risk profile scanning*	Yes	Yes	Yes
Manual testing	-	Yes	Yes
Business logic testing	-	-	Yes
Static code analysis	-	-	Yes
Application Defender*	-	-	Yes
Web services**	-	-	10 endpoints
Target turnaround	< 3 days	< 5 days	< 7 days

* Included with dynamic subscriptions only.

** Web services assessments are offered in buckets of 30 endpoints and can be purchased for an additional cost.

Continuous Application Monitoring

Monitoring applications in production is an increasingly common challenge for security teams. Continuous Application Monitoring combines application discovery with continuous dynamic vulnerability scanning and risk profiling in a subscription service that provides visibility and insight into the risk facing customers' entire application portfolio. The automated discovery scans identify new externally facing applications on a monthly basis and results are presented in a risk-ranked list with confidence scores (up to twelve per year). Confirmed applications can then be enrolled in production-safe continuous vulnerability and risk profile scanning (up to four scans per month). Continuous Application Monitoring serves as both an ideal first step in launching a Software Security Assurance program and as a complement to dynamic and static testing of applications once they are deployed.

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, FoD 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, FoD assessments provide true security testing for companies serious about securing their mobile applications.

Table 2. Mobile assessment service levels

Assessment type	Mobile standard	Mobile premium
Platform	iOS, Android	iOS, Android, Windows®
Mobile binary analysis	Yes	Yes
Reputation & behavioral analysis	Yes	Yes
WebInspect scan	Yes	Yes
False positive removal	Yes	Yes
Manual testing	-	Yes
Business logic testing	-	Yes
Mobile static analysis	-	Yes
Target turnaround	< 2 days	< 7 days

Assessment units

HPE Security Fortify on Demand dynamic, static, and mobile application security testing services are available by purchasing Assessment Units.

HPE Security 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 starting at the purchase order (PO) effective date and may be redeemed individually.

Table 3. Redeeming HPE Security Fortify on Demand Assessment Units

Assessment type	Single assessment	Application subscription
Dynamic basic or static analysis	2 Assessment Units	6 Assessment Units
Dynamic or mobile standard	4 Assessment Units	12 Assessment Units
Dynamic or mobile premium	8 Assessment Units	25 Assessment Units
Dynamic web services	4 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 HPE Security 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.

Operational services

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

Account management
All accounts include access to a dedicated technical account management team to help drive the success of a customer's application security program. The team liaises with the customer 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.

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 technical support for HPE FoD. Customers may contact Hewlett Packard Enterprise through a variety of methods such as in-portal chat, support tickets, telephone, or email. The severity of the request determines the response and resolution time.

For additional details, customers can visit the Help Center within the **HPE Security Fortify on Demand portal**.

Capacity and performance management
All tiers of the SaaS infrastructure are proactively monitored for capacity and performance. The architecture allows for addition of capacity to applications, databases, and storage.

Change management
HPE Security Fortify on Demand follows a set of standardized methodologies and procedures for efficient and prompt handling of changes to SaaS infrastructure and application, which enables 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. These may or may not include new features or enhancements. HPE determines whether and when to develop, release, and apply any SaaS. Upgrade customers are notified through in-portal messaging and product update emails.

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 or the following exceptions:

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks
- Force majeure events as described in the HPE SaaS terms
- Actions or omissions of customer (unless undertaken at the express direction of Hewlett Packard Enterprise) or third parties beyond the control of HPE
- Unavailability due to customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of HPE
- Scheduled upgrades or maintenance

Assumptions

- Customer must have Internet connectivity to access the Fortify on Demand portal.
- HPE FoD is performed remotely and delivered in English only.
- The service commencement date is the date on which customer's PO is booked within the HPE order management system.
- The import of customer data into HPE FoD during the implementation requires that the information is made available to Hewlett Packard Enterprise at the appropriate step of the solution implementation and in the HPE-designated format.
- A subscription is valid for a single application, which cannot be changed during the subscription term purchased.

Furthermore, HPE FoD is provided based on the assumption that customer will implement and maintain the following controls in its use of HPE FoD:

- Configuring customer's browser and other clients to interact with HPE FoD
- Configuring customer's network devices to access HPE FoD
- Appointing authorized users
- Configuring HPE FoD account such that end user passwords are sufficiently strong and properly managed
- Performing validation activities related to implementation and external application setup during the service initiation and ongoing phases
- Performing procedures for access approvals, modifications, and terminations

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 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. HPE endeavors to help minimize disruptions to the application and/or 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 will be responsible for all data cleansing and data accuracy as part of any assessment request. Hewlett Packard Enterprise is not responsible for the accuracy of the data provided by the customer.
- 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 a solution in team foundation server for a .NET application).
- 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. Customer will provide port 80/443 access to all applications that are to be assessed for remote testers. If they are internal applications, VPN access will be provided for the HPE FoD testing team.
  - User logins may not be **daisy chained** within the application
  - Up to one (1) user login
  - Must be the same domain name:
    - HPE.com is a domain name.
    - hpe.com/news is the same domain as HPE.com.
    - community.hpe.com is a different domain name and considered a different application.
    - hpe.it is a different domain name and considered a different application.
    - For web service assessments, Representational State Transfer (REST), Simple Object Access Protocol (SOAP), and standalone web services are supported.
  - For REST, an endpoint is a combination of a uniform resource identifier (URI) and HTTP method. All endpoints in the bucket must be for the same FQDN. For example, all of the following are endpoints for a single **bucket**:
    - GET https://api.hpe.com/api/v1/Accounts
    - GET https://api.hpe.com/api/v1/Accounts/{AccountId}
    - PUT https://api.hpe.com/api/v1/Accounts/{AccountId}
    - GET https://api.hpe.com//api/v2/orders/{orderId}/items/{itemId}
    - POST https://api.hpe.com//api/v2/orders/{orderId}/items/{itemId}
  - For SOAP, an endpoint is an individual method provided by a web service. All endpoints in the bucket must be defined in a single SOAP Web Services Description Language (WSDL) file. In the WSDL, the service is indicated by the <service> tag and the method by the <operation> tag.
  - For standalone web services, an endpoint is a combination of URI with an associated WSDL and method. All URIs in the bucket must be for the same FQDN. In the WSDL, the method is indicated by the <operation> tag.
    - For mobile assessments, an application is a single installable application for a single hardware platform. Mobile applications submitted for testing must be in the form of a compiled IPA (iOS), Android Package Kit (APK) (Android), or the source code, which must be able to be successfully compiled prior to submission of the application.

- For mobile and static analysis, an **application** must meet the HPE Security Fortify **SCA** minimum requirements for currently supported languages.

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

About HPE Security Fortify
HPE Security 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
hpe.com/software/fod

Hewlett Packard
Enterprise