SOFTWARE SECURITY DELIVERED IN THE CLOUD

HP Fortify on Demand: The quickest, most affordable way to accurately test and score the security of any application

Solution guide
Table of contents

Executive summary 3
Testing third-party software 3
Testing internally developed software 3
How HP Fortify on Demand works 4
Correlation of static and dynamic results 6
Workflows 6
Three levels of dynamic testing 6
Security controls for HP Fortify on Demand 7
Product specifications 8
Integration with HP Fortify Software Security Center 8
Appendix: Fortify’s five-star security rating 8
Executive summary

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 applications licensed 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 team. Users simply upload their application binaries 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 interface and report.

HP Fortify on Demand leverages the market-leading static analysis technology, HP Fortify Static Code Analyzer (SCA) software, and the award-winning dynamic analysis technology, HP WebInspect software. Organizations can view security vulnerabilities in one single dashboard, without installing software on-premise. HP Fortify on Demand is a highly secure SaaS environment with robust security controls that assure all sensitive uploads and other intellectual property remain uncompromised.

Figure 2: HP Fortify on Demand won the “Best Security Solution” CODiE Award.

This document describes in detail how HP Fortify on Demand works and what it can accomplish for companies seeking to test the security of their software.

Testing third-party software

HP Fortify on Demand helps address two key scenarios:

1. Vendor security management: Assessing third-party software
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. While improved vendor contracts can provide some remedy in the case of a breach, ultimately it’s better to avoid the problem altogether. 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. HP Fortify on Demand provides an easy-to-use SaaS-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. HP Fortify on Demand serves as an independent third-party and system of record for conducting a consistent, unbiased analysis.

2. Enterprise assessment management: Assessing internal applications

With internally developed applications, HP Fortify on Demand helps in two ways. For companies with a secure development lifecycle already in place, HP Fortify on Demand can provide a final test before deployment. For organizations new to security, HP Fortify on Demand can provide a quick and accurate test to baseline applications and prioritize efforts to improve application security.
“HP technology identifies potential security threats in software through very deep analysis that ensures the software is safe to deploy and the sensitive data and application behavior cannot be compromised by hackers. HP Fortify on Demand is very easy to use and gives great pointers on where a vulnerability is rooted in the code so it can be quickly fixed.”

Anurag Khemka, President and CEO, RightWave, Inc.

How HP Fortify on Demand works
HP Fortify on Demand tests the security of in-house or third-party applications in four easy steps:

1. Login and upload applications
A new HP Fortify on Demand customer is given a private account with secure login credentials. Role-based access control allows administrators to see all projects and individual contributors to view only their projects. In the case of testing a vendor’s application, HP gives the vendor an entirely separate account.

The user has the ability to kick off a static scan of the application code or a dynamic scan of a running web application.

For static analysis, the user uploads the executable version of an application. HP Fortify on Demand doesn’t require source code. Examples of what may be uploaded include:
- A WAR or EAR file for Java
- A zip file of MSILs for .NET
- A zip file of the source files for PHP

HP Fortify on Demand supports 16 different languages—see “product specifications” on the last page for the complete list.

For dynamic analysis the user provides the URL for the application and any credentials necessary to access the site. If the application is not externally facing, HP Fortify on Demand can install a satellite appliance onsite, from which the testing can run. HP can use a VPN client to gain access to the internal site.

2. Comprehensive testing
HP Fortify on Demand provides comprehensive and accurate testing. The static analysis leverages the solution’s extensive Secure Coding Rulepacks, six analysis engines, and patented X-Tier Dataflow analysis to cover 100 percent of the code. The dynamic analysis leverages HP WebInspect. Dynamic testing experts from HP combine automated and manual testing on a web application that’s up and running. When the power of both whitebox and blackbox security testing is applied to a web application, it results in a comprehensive analysis of an application’s security posture.

Figure 3: Shown are the three key steps of the HP Fortify on Demand process.
After testing is complete, a software security auditor with a background in development and security reviews the result set for accuracy. If there are any false positives, the auditor removes these issues. If custom rules can be written to tailor the analysis to each individual application, the auditor will write these rules and then re-test the application.

3. Results released quickly
HP Fortify on Demand releases results as soon as they are ready. Static analysis results typically finish in one day, regardless of the application’s size. Dynamic analysis results may take longer, depending on the size and complexity of the application.

Once testing and reviews are complete, HP Fortify on Demand emails the user and communicates that the results are ready. A user can login and view correlated and prioritized results.

Figure 4: This executive summary page of the report provides an overview of the security test.

### Executive Summary

<table>
<thead>
<tr>
<th>Company</th>
<th>SCA</th>
<th>Fortify Security Rating</th>
<th>Static: ✓ Dynamic: ✗</th>
</tr>
</thead>
<tbody>
<tr>
<td>Projects</td>
<td>Walmart, Java</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>8.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static Analysis Date</td>
<td>July 22, 2019</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Analysis Date</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Most Prevalent Categories**

- Cross-Site Scripting: Reflected: 183
- SQL Injection: 10
- Directory of Service: Passive Disclosure: 4
- Cross-Site Request Forgery: 2
- Insecure Interception: 2
- Other: 5

**Issues by Priority**

- High: 109
- Medium: 0
- Low: 0
- Total: 109

**Issues by Attack Vector**

- Database: 0
- Network: 0
- Web: 105
- Web Services: 0
- Other: 5

**Remediation Roadmap**

- Vulnerability details includes a complete list of all vulnerabilities, with details about each. HP Fortify on Demand provides helpful details about each vulnerability, including the filename and line of code (if the vulnerability was found statically), and the URL, request, response and parameters (if the vulnerability was found dynamically).

- Remediation guidance describes how each vulnerability could be exploited and how to remediate it.

- PCI report helps companies demonstrate compliance with the Payment Card Industry (PCI) Data Security Standards (DSS).

- OWASP Top 10 shows all issues that fall in the OWASP Top 10.
Correlation of static and dynamic results

HP Fortify on Demand is the only SaaS-based solution to offer true correlation of static and dynamic results. If a customer selects both a static and dynamic scan of an application, all results will be correlated in order to help prioritize issues and reduce the time to investigate and fix issues.

If the same type of vulnerability is found at the same URL both statically and dynamically, HP Fortify on Demand automatically puts these results together, helping users investigate issues more easily and prioritize efforts.

The HP Fortify on Demand dashboard also provides summary correlation information, showing which vulnerabilities were found only statically, only dynamically, or with both analysis techniques. This summary information helps present the relative importance and value of each technique. In some cases the overlap between the two testing methodologies is very high, while at other times the overlap is minimal.

Only HP Fortify on Demand provides true correlation, helping a company understand what the tests are finding and speed the time to remediation.

Workflows

HP Fortify on Demand has two core uses cases—working with third parties to assess third-party code and working with internal developers or security managers to ensure internally developed code is secure. The workflow is very similar in both cases. Below is an overview of both workflows:

• Working with third parties to assure that their software is secure:
  – The vendor and the procurer receive separate HP Fortify on Demand accounts and establish a secure link between their accounts.
  – The vendor uploads its executable and/or provides a URL.
  – HP conducts thorough testing and works with the vendor to resolve issues.
  – When ready, the vendor publishes a summary report to the procurer, demonstrating the security posture of the application.
  – Working with internal developers, quality assurance (QA) professionals or security managers to ensure internally developed code is secure:
    – Security managers provide logins to all HP Fortify on Demand users (most likely developers or security auditors).
    – Each user logs in and uploads the application and/or provides a URL.
    – HP conducts thorough testing and releases results.
    – All results are summarized in one core dashboard.

To speed the process and keep customers informed of status, HP Fortify on Demand sends email notifications whenever an application has been uploaded and when results are ready for viewing.

Three levels of dynamic testing

HP Fortify on Demand offers multiple options for licensing. For both static and dynamic analysis, a user can purchase individual scans or one-year subscriptions for unlimited scanning per application. For dynamic analysis, a user can choose among three different testing levels (Premium, Standard or Baseline). Each is designed for different use cases and offers varying levels of testing. A description of each is below:

• Premium
  – An automated and manual testing solution for websites that are permanent, mission-critical, have rigorous compliance requirements, and in which the company relies on serving its customers or business partners and has multi-step form-based processes
  – Includes testing for both technical and business logic vulnerabilities
Uncovering 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. All results are manually reviewed by security experts to remove any false positives.

**Standard**

- An automated solution for websites that are a permanent fixture in a customer’s online experience and have multi-step form-based processes, but are not necessarily mission-critical
- Includes testing for technical vulnerabilities
- Includes the use of multiple automated and manual testing solutions
- All results are manually reviewed by security experts to remove any false positives

**Baseline**

- An automated solution for websites that are seasonal or temporary in nature
- All results are manually reviewed by security experts to remove any false positives

### Security controls for HP Fortify on Demand

HP Fortify on Demand was designed and developed following industry best practices for secure SaaS solution deployment.

The solution is physically housed in a Tier 4 A+ datacenter featuring multiple redundant power and network feeds and “five nines” uptime. The datacenter is compliant with SAS 70 Type II, ITIL, ISO-17799 and SunTone. It has 24x7x365 security using closed-circuit television (CCTV). All datacenter employees are background-checked and all access is supervised. All doors require PIN, magnetic card and biometric retina scans before granting access. The datacenter has redundant power systems with backup generators and double-conversion uninterruptible power supplies (UPSs).

HP Fortify on Demand features world-class software security built with the same technology as HP Fortify Software Security Center, including hardened operating systems and open-source components. Independent third-party consulting firms conduct code reviews and pen tests on every major release.

HP Fortify on Demand has browser-to-system Secure Sockets Layer (SSL) encryption for data protection. All data, including intellectual property and analysis results, is encrypted with data-at-rest encryption technologies. All hard drives and storage systems are useless outside the HP Fortify datacenter environment.

A virtual private database is used to ensure separation between customers. The database is setup as a virtual per-client relational database management system (RDBMS) instance with database encryption, ensuring that users can only access their own data in their own database.

For more information on the security of HP Fortify on Demand, please see the whitepaper, “HP Fortify on Demand: Security Controls in Place,” available upon request (taylor.mckinley@hp.com).

---

**HP FORTIFY ON DEMAND KEY ADVANTAGES**

- Best-of-breed static and dynamic analysis
- True correlation between static- and dynamic-analysis results
- All results manually reviewed by application security experts
- Flexibility for customers to easily migrate to on-premise solution
- Experienced security research team

---

**Figure 6:** This table shows a comparison of the three testing levels of dynamic analysis available via HP Fortify on Demand.

<table>
<thead>
<tr>
<th>HP Fortify on Demand Dynamic</th>
<th>Baseline</th>
<th>Standard</th>
<th>Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Kickoff</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planning objectives</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Credentials</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Prepare environment</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td><strong>Prepare</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create login script</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Scan configuration</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Application discovery</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Application discovery with manual crawl</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td><strong>Execute</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automated application scanning</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>False positive removal</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Bypass client controls</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Attack authentication</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Attack session management</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Attack access control</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Injection attack</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Attack server, or hijack user privileges</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Advance fuzzing</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Application logic</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Manual penetration test</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td><strong>Report</strong></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Summary</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommendations</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Product specifications

• Language support
  – For static analysis:
    – Any applications written in Java, ASP.NET, C#, VB.NET, PHP, COBOL, ColdFusion, Classic ASP, VB6, VBScript, JavaScript/Ajax, JSP, Python, PL/SQL, T-SQL and XML/HTML
  – For dynamic analysis:
    – Any web application
    – Externally facing applications can be accessed directly
    – Internally facing applications can be accessed using client VPN, HP Appliance, or HP software sensor

Integration with HP Fortify Software Security Center

To ensure a secure development process throughout the software development lifecycle, a company may elect to bring this testing technology in-house, using it as early and as often as needed. This approach allows users to integrate software security assessment into their build systems, bug-tracking systems, integrated development environments (IDEs) and more. At any point in time, HP Fortify on Demand customers can migrate their data over to HP Fortify Software Security Center, the market-leading suite of solutions for Software Security Assurance (SSA). HP Fortify Software Security Center helps integrate security into the software development lifecycle. In most cases, customers who choose to use HP Fortify on Demand over time transition some or all of these licenses to HP Fortify Software Security Center for use as a complete solution in-house for application development teams. If a company chooses to do this, all data is easily migrated via a quick download.

Conclusion

HP Fortify on Demand helps users achieve their software security assessment objectives by providing a robust application-testing environment. Internal and third-party software becomes subject to comprehensive security reviews that are quick, accurate and affordable. This fully hosted SaaS offering uses the same award-winning analysis technology as the market-leading HP Fortify Software Security Center, making it easy for customers to graduate from assessment to remediation and prevention as part of a robust software security assurance program.

Appendix: Fortify’s five-star security rating

HP Fortify on Demand prioritizes all identified issues into four risk quadrants: critical, high, medium and low. Membership in each quadrant is determined by whether the finding has a high or low impact and high or low likelihood.

Impact is the potential damage rendered to assets upon vulnerability exploitation. This damage may be in the form of, but not limited to, financial loss, compliance violation, brand/public-relations damage or loss of life.

Likelihood is a measure combining the accuracy of the result and the potential for exploit.

The HP Fortify on Demand Rating provides summary information on the nature of risk inherent in the application. A perfect rating within this system would be five stars, indicating that no vulnerabilities were uncovered.

• 1 Star: HP Fortify awards one star to projects that undergo an HP Fortify security review, which analyzes a project for a variety of software security vulnerabilities.

• 2 Stars: HP Fortify awards two stars to projects that undergo an HP Fortify security review that identifies no high-impact/high-likelihood issues. Vulnerabilities that are trivial to exploit and have a high business or technical impact should never exist in business-critical software.

• 3 Stars: HP Fortify awards three stars to projects that undergo an HP Fortify security review that identifies no high-impact/low-likelihood issues and meets the requirements needed to receive two stars. Vulnerabilities that have a high impact, even if they are non-trivial to exploit, should never exist in business-critical software.

• 4 Stars: HP Fortify awards four stars to projects that undergo an HP Fortify security review that identifies no low-impact/high-likelihood issues and meets the requirements for three stars. Vulnerabilities that have a low impact, but are easy to exploit, should be considered carefully as they may pose a greater threat if an attacker exploits many of them as part of a concerted effort or leverages a low-impact vulnerability as a stepping stone to mount a high-impact attack.

• 5 Stars: HP Fortify awards five stars to projects that undergo an HP Fortify security review that identifies no issues.