opentext™ | Cybersecurity

Brochure

Fortify on Demand Mobile Application Security Testing

Mobile Application Security Testing

Fortify on Demand 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. Fortify on Demand supports **Secure Development** through continuous feedback to the developer's desktop at DevOps Speed and scalable **Security Testing** embedded into the development tool chain.

Protect Mobile Applications throughout the Software Development Lifecycle

Organizations are faced with rapidly expanding application portfolios, both in size and complexity. Securing applications from risk and vulnerabilities has become a business imperative in order to protect the business and protect customers. Applications must be protected across all phases of the Software Development Lifecycle (SDLC) to make a Software Security Assurance program successful. Application security begins when code is developed, code is validated through testing, and is continuously monitored once the application moves into production. Application security programs embedded throughout the SDLC have proven to be the most cost-effective way to ensure policy execution, compliance, and on-going enforcement; however, only 13% of technology influencers and decision makers say all their applications are covered under their current application security program.* Mobile Application Security Testing (MAST) is essential in identifying software vulnerablilities in the development, Quality Assurance (QA) and production phases.

Protect Your Mobile Applications in Development and Production

There are billions of active mobile applications globally with continued exponential growth fueled by the Internet of Things. Insecure mobile applications represent a pervasive threat to enterprises and individuals. The pressure to develop more applications faster continues to intensify.

*"The State of Application Security in the Enterprise"

Fortify on Demand by OpenText mobile application security testing is purpose-built for speed and ease-of-use combined with the most comprehensive mobile application security testing methodologies available. Fortify on Demand, as a cloud-based service, will span the threat landscape across the mobile attack surface and provide the expertise to help you keep your applications secure—spanning from the Software Development Lifecycle (SDLC) and throughout the production environment. We provide the expertise, tools and training to do all of the application security heavy lifting so that your business can focus on innovation.

Application Security Testing across All Mobile Attack Vectors

Fortify on Demand Mobile Assessments by OpenText are often performed during the integration and test phases, complementing Fortify on Demand Static Assessments (SA) by OpenText of client and server source code during early development. Similar to dynamic testing for web applications, Fortify on Demand mobile assessments utilize the compiled application binary to simulate attacks during runtime. More than simple behavioral and reputation analysis, the Fortify on Demand approach to mobile security assessments spans the entire technology stack—client, network, and server—and is capable of identifying over 300 unique vulnerability categories. This holistic approach is used so that vulnerabilities found in one component (the client, for example) can be used while testing another (the server) to identify complex attack vectors, a similar methodology a hacker would employ. As a Fortify on Demand customer, all you have to do is provide the mobile application binary (IPA files for iOS or APK files for Android) to the Fortify on Demand portal.

Fortify on Demand Mobile Application Security Testing Covering Client, Network and Server Components

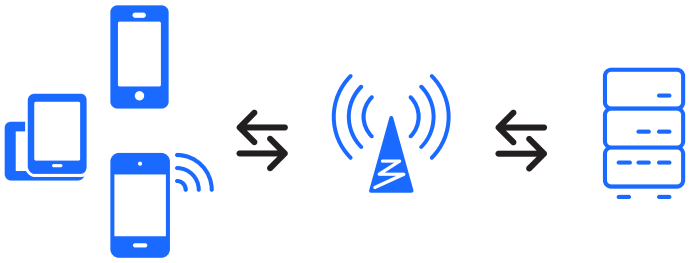

Figure 1. Fortify on Demand Mobile Application Security Testing Covering Client, Network and Server Components.

Perform Automated Assessments of the Mobile Application Binary in Minutes

Mobile developers often fail to harden mobile binaries. Fortify on Demand scans mobile app binary files using a proprietary framework to detect issues in minutes. When a mobile binary is uploaded to Fortify on Demand, it is automatically scanned for packing issues, privacy concerns, and endpoint URL reputation analysis. Fortify on Demand's Mobile Binary Analysis helps identify vulnerabilities that are embedded within the mobile app package such as:

- Hard-coded sensitive information
- Weak Code-signing Certificates
- Weak SSL Certificates
- Libraries with known vulnerabilities
- Misconfigured security options (Disabled App Transport Security)
- Web endpoints with questionable reputation

WebInspect Provides Industry-Leading Assessments for Web Services

Fortify WebInspect is the industry-leading web application security assessment solution designed to thoroughly analyze today's complex web applications, mobile applications, and web services for security vulnerabilities. WebInspect can report more vulnerabilities and in more web application environments than any other AppSec provider—including risks that often go undetected by black-box security testing technologies.

Fortify on Demand utilizes Fortify WebInspect by OpenText's Mobile Scanning to detect web vulnerabilities in backend components of mobile applications. Fortify on Demand's mobile device web scanning starts by running the mobile app on a physical Android or iOS device, recording the backend web traffic with Fortify WebInspect , and identifying the hosts and RESTful endpoints to include in web analysis. Fortify WebInspect is then used to scan the specified workflows for vulnerabilities.

Capability highlights of Fortify WebInspect include:

- Coverage across 300+ unique vulnerability categories
- Advanced mobile macro recording and flexible authentication handling for improved session management, particularly with more complex applications
- Spans both internal and externally facing web applications based on Authentication Level desired (none, VPN, whitelist, multi-factor)
- Native Mobile Application Device Scanning
- Broad client side language support such as HTML5, Flash, JavaScript among others
- Coverage across virtually all server-side languages including HTTP/native, XML, PHP, Visual Basic, C++, JavaScript and JSP, Python, Ruby on Rails, JSON, .Net, AJAX
- Built-in support for scan blackout periods to save time and resources during the assessment
- Simplified integrations via XML data export file patch with leading Web Application Firewalls (WAFs) such as Imperva, F5, Citrix, Barracuda, Radware, and Fortinet

Manual Security Testing For Complex Vulnerabilities across All Attack Vectors

With Fortify on Demand manual testing for Mobile+ assessments, expert mobile security testers will manually analyze the target mobile app and backend web traffic for up to 8 hours using Fortify on Demand's testing methodology. The expert manual analysis is conducted on physical devices, meaning your apps will be analyzed in a real-world, runtime context. This is a live application execution, web traffic capture, and runtime observation. The analysis includes manual inspection of the app's binary, advanced web application testing, and behavioral analysis of on-device/runtime issues. Fortify on Demand's mobile security experts help identify vulnerabilities that can only be detected through human interaction with the mobile app including, but not limited to:

- Sensitive information stored insecurely on-device (passwords, credit cards, API tokens, etc.)

- Insecure app interactions such as insecure intents, application registered URL schemes.
- The ability to harvest user accounts and other authentication flaws
- Access to other users' data or sensitive content through horizontal or vertical privilege escalation
- The ability to access unintended development, debug or admin areas of the application
- Unique business logic flaws due to faulty developer assumptions

Fortify On Demand Offers Flexible Licensing Models

Fortify on Demand Mobile Assessments are available in two licensing models to address specific application security objectives. Customers can mix and match these offerings for each application in their portfolio based on factors including risk profile, appsec maturity, development cadence, compliance requirements. Most customers prefer subscriptions, which allow for unlimited assessments of an application throughout the term.

1. **Fortify on Demand Mobile Assessment Subscriptions** are ideal in more mature AppSec and DevOps environments that are optimized for automation, speed and agility. With the Mobile service level, users can choose between a manual review of the results by our security experts or a fully automated scans that process in a few minutes. Most customers request an expert review for the initial onboarding assessment and then use automated Mobile assessments for subsequent integration with continuous integration and continuous deployment (CI/CD) tools.
2. **Fortify on Demand Mobile+ Assessment Subscriptions** incorporate Fortify WebInspect DAST assessments of backend web services and up to 8 hours of manual testing by a Fortify security expert to complement mobile binary assessments. Mobile+ subscriptions are ideal for supporting business-critical mobile applications since Fortify experts provide a comprehensive security review not possible with an automated scanning solution.

Both Mobile and Mobile+ Assessments are also available as single, standalone scans for applications with limited lifecycles or infrequent releases.

Mobile Or Mobile+? Which Assessment Type Is Right For You?

Both Mobile and Mobile+ assessments provide valuable insight about the security posture of assessed applications, and the two main differences between the two models are the turnaround times and the additional manual checks conducted on the Mobile+ service level. A simplified comparison of Mobile and Mobile+ types is:

Connect with Us

www.opentext.com

	Fortify on Demand Mobile Assessment	Fortify on Demand Mobile+ Assessment
Platforms Supported	iOS, Android	iOS, Android
Automated binary assessment	Yes	Yes
Endpoint reputation analysis	Yes	Yes
Security expert review (Including false positive removal)	Optional	Yes
Fortify WebInspect DAST assessment of web services	No	Yes
Manual vulnerability testing of binary, network & web services	No	Yes
Typical turnaround	<24 hours (with expert review) Minutes (without expert review)	3-5 days (with expert review)

Let's Get Started

Fortify offers the most comprehensive static and dynamic application security testing technologies backed by industry-leading security research.

Fortify Application Security Solutions can be deployed on-premise or with Fortify on Demand, as a service to build a scalable, agile application security program that meets the evolving needs of today's IT organization.

Learn more at
www.microfocus.com/en-us/cyberres/application-security/fortify-on-demand

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

763-000006-003 | O | 11/23 |