CyberRes

Brochure

Fortify on Demand Static Application Security Testing

Static Application Security Testing

CyberRes 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.

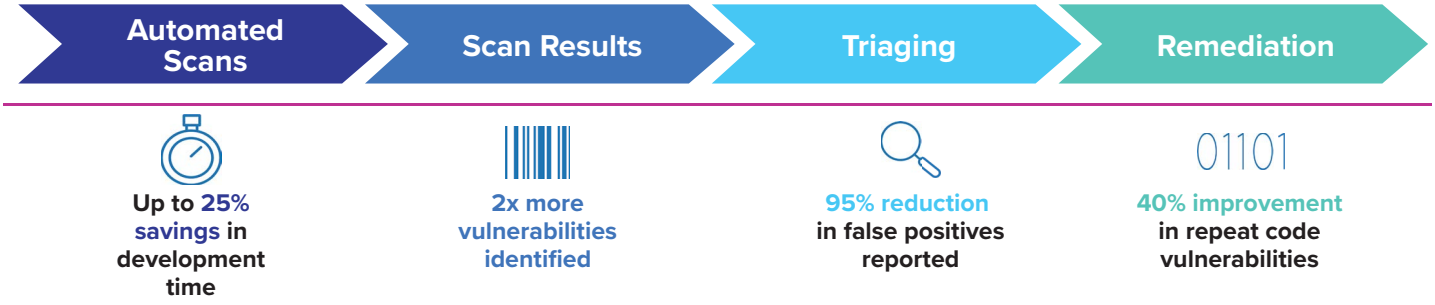
Protect Applications throughout the Software Development Lifecycle

Organizations are faced with rapidly expanding applications portfolios, both in size and complexity. Securing applications from risk and vulnerabilities has become an imperative in order to protect the business and protect customers. Applications must be protected across all phases of the Software Development Lifecycle (SDLC) in order for a Software Security Assurance program to be successful. Application security begins when code is developed. Code is validated through testing. Application security programs embedded throughout the Software Development Lifecycle (SDLC) have been proven to be the most cost-efficient way to ensure policy execution, compliance, and ongoing enforcement; however, only 13% of technology influencers and decision makers say all their applications are covered under their current application security program.[1]

Fortify on Demand: Proven in Finding and Fixing Vulnerabilities

Fortify on Demand is a complete, proven application security solution as a service that is scalable to the needs and various application loads of your business. Fortify on Demand can save up to 25% in development time as code scans can be configured to run automatically. Risks can be identified through Fortify on Demand static scans within minutes[2], often revealing 2x more vulnerabilities in source code than other vendors. Fortify on Demand can also reduce false positives by up to 95% which can expedite triaging. Furthermore, it can help reduce repeat code vulnerabilities by up to 40%, resulting in faster development of applications with fewer production risks.

1. "The State of Application Security in the Enterprise"
2. Fortify Internal Assessments—October 2020
3. "Continuous Delivery of Business Value with Fortify"—June 2017



Fortify on Demand Static Assessments Secure Code Right from the Start

Fortify on Demand finds and fixes application security risks as code is being written. The Fortify on Demand solution is fully integrated within the Integrated Developer Environment (IDE). This means developers receive real-time insights and recommendations on code vulnerabilities as the code is being written. With Fortify on Demand, developers have the intelligence at their fingertips to build better and more secure software—right from the start. Our comprehensive static scan assessments help developers identify and eliminate vulnerabilities **in source, binary, or byte code**—all to help your business build more secure software. Powered by **Fortify Static Code Analyzer (SCA)**, Fortify on Demand static assessments detect over 781 unique categories of vulnerabilities across 27+ programming languages that span over 1 million individual APIs.

Static assessment capabilities with Fortify on Demand are amongst the most comprehensive and flexible available worldwide. Fortify on Demand is designed to meet the needs of AppSec leaders for comprehensive application risk management plus the desire of developers for speed and ease-of use. Capability highlights include:

- Support for ABAP/BSP, ActionScript, Apex, ASP.NET, C# (.NET), C/C++, Classic, ASP (with VBScript), COBOL, ColdFusion CFML, HTML, Java (including Android), JavaScript/ AJAX/Node.js, JSP, Kotlin, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Scala, Swift, T-SQL, VB.NET, VBScript, Visual Basic, and XML
- Developer tools to accelerate AppSec integration across existing agile or DevOps processes including: IDE plug-ins, code uploads from build or Continuous Integration (CI) servers, and native integration to bug trackers
- Open source component analysis, powered by Sonatype, to identify publicly disclosed vulnerabilities and license risks
- Comprehensive scanning coverage across source code, byte code or object code for any type of application: web, mobile or thick-client
- Flexible static assessment licensing models with singlescan or subscriptions available
- Real-time vulnerability identification and reporting with Fortify Security Assistant (with subscription only)
- Actionable results in <1 hour for most applications with DevOps automation

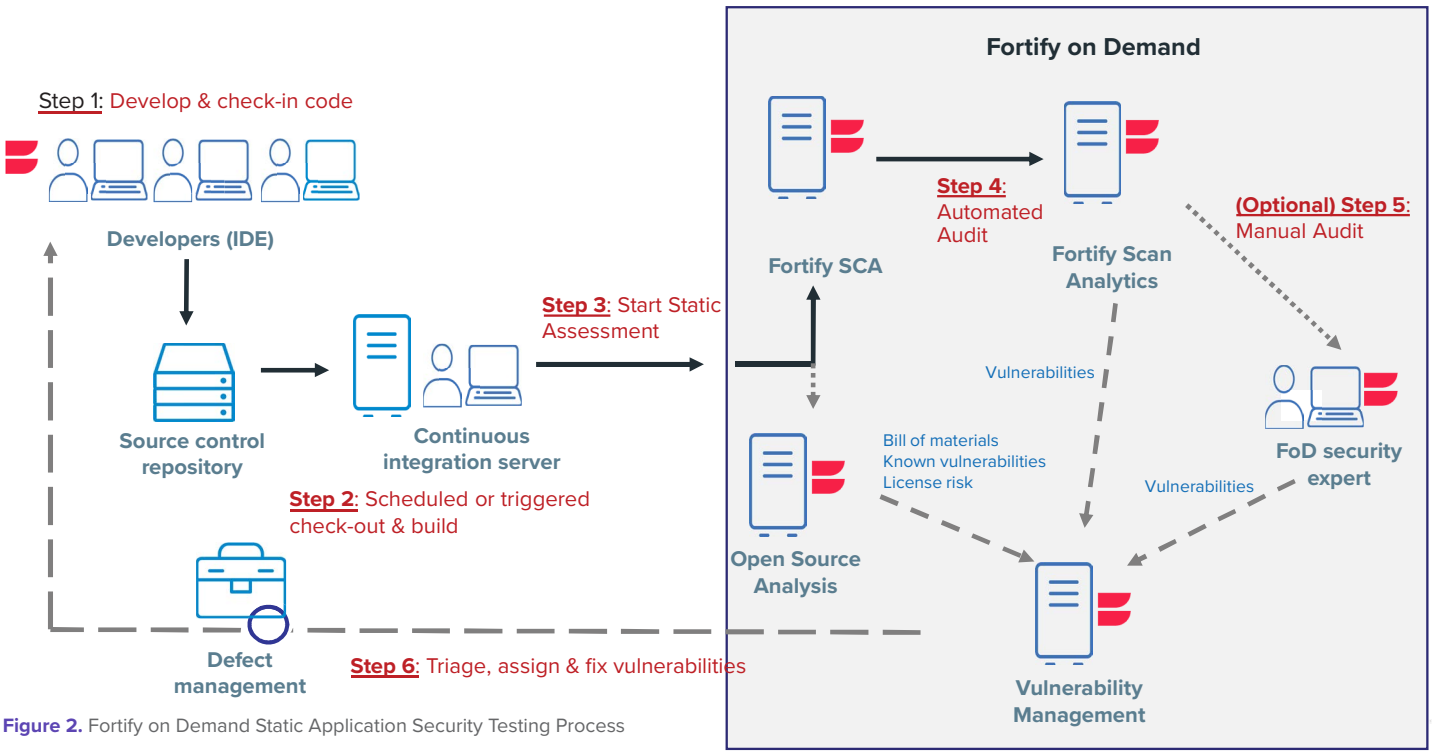


Figure 2. Fortify on Demand Static Application Security Testing Process

Before the Static Assessment (Pre-Fortify on Demand)
Fortify on Demand subscriptions include **Fortify Security Assistant** to accelerate DevOps speed and security.

Fortify Security Assistant is a plug-in within the integrated development environment (IDE) that notifies the developer of potential security vulnerabilities as code is being written. Fortify Security Assistant also offers recommendations on how the developer can remediate identified vulnerabilities. This empowers the developer to learn how to catch application risks early while saving the developer time in remediation across later SDLC phases.

When the software is ready to advance in a DevOps or continuous delivery environment, it is passed through to build or the CI server. Fortify on Demand static assessments can be initiated quickly and easily. Developers can upload the application source, binary and/or bytecode from the IDE, repository, build or CI server. Developers can also manually upload code for assessments through the Fortify on Demand portal or automatically using our ecosystem of integrations.

During the Static Assessment (with Fortify on Demand)
Upon code upload, **Fortify Static Code Analyzer (SCA)** immediately begins scanning the application using an optimized configuration chosen based on the unique characteristics of each application. The first time an application is submitted, our team of security experts provides further tuning to both maximize quality and minimize scan time. With an optimal configuration established, development teams can move at DevOps speeds knowing that quality is not being compromised.

Once the Fortify SCA scan completes, the prioritized results are processed by **Fortify Scan Analytics**. Fortify Scan Analytics utilizes patent-pending machine learning technology to distinguish between the most relevant vulnerabilities and false positives based on millions of historical audit decisions by Fortify on Demand experts.

Continuously incorporating new intelligence, the predictions turn a large volume of security information into a small set of high confidence, actionable results in the span of seconds. Depending on the assessment type, users choose whether to have these predictions automatically applied and published or if a further manual audit by a security expert is desired.

Because nearly all applications are built with a combination of custom and open source code, static assessments also include an optional open source analysis of the application. Open source analysis happens in parallel to the Fortify SCA scan and no code leaves the Fortify on Demand environment. Powered by **Sonatype's** software composition analysis, the identified components provide a bill of materials with known public vulnerabilities and license information.

All results are delivered through the centralized Fortify on Demand platform. Each vulnerability includes all of the information a developer needs to understand and fix the underlying issue: a detailed description, line of code, data flow diagram, guidance on how to remediate the vulnerability, consequences if it's not addressed, and best practices to help developers code more securely. Fortify on Demand makes it easy to integrate remediation into each team's workflow, whether that's managed through Fortify on Demand or our native integrations into the leading defect management systems. Using full-featured plugins for the major IDE, development teams can triage, assign issues, track progress and collaborate in real-time as the code is written.

Fortify on Demand Secures DevOps

DevOps is as much about automating repetitive, error-prone tasks to improve overall development effectiveness, as it is about a new process or organizational principle. There is the myth that application security adds more work and time to the SDLC and can be an inhibitor to the DevOps model. Fortify on Demand is purpose-built to make security an integral part of development, particularly by building and automating secure code practices within the SDLC.

Fortify on Demand is fully integrated into the DevOps toolchain in order to accelerate automation and integration within the SDLC. This makes it faster and easier for developers to build security into the SDLC, whether that's on a set release cadence, reoccurring schedule or even every build. As a result, your business is able to move toward automated AppSec programs, embed security into the SDLC and reduce risk in the production environment. Currently available DevOps toolchain integrations with Fortify on Demand include:

- Eclipse, Microsoft Visual Studio, IntelliJ developer IDE plug-ins
- GitHub and Atlassian Bitbucket source control repositories
- All major build and CI systems including Jenkins, Microsoft Visual Studio Team Services (VSTS)/Team Foundation Server (TFS), Bamboo, TeamCity, Travis, CircleCI through native plug-ins or our easy-to-use universal uploaded utiliy

- Application Lifecycle Management with ALM Octane/Quality Center (QC), Atlassian Jira, Microsoft VSTS/TFS, Bugzilla bug tracking and defect management systems

Fortify Static Assessment Scans Can Take Minutes within a Mature DevOps Environment

Fortify, a leader and innovator in AppSec, has worked with hundreds of organizations to accelerate application security as a service within DevOps environment. Mature security organizations have capitalized on the proven success of Fortify on Demand to automate and integrate application security as demonstrated through static assessment times.

Approximate Fortify on Demand SCA Scan Times[4]

Application Size	Average Fortify SCA Scan Time	Total Lines of Code (TLOC)
Extra Large	12.6 hours	>1M TLOC
Large	2.8 hours	>400K TLOC
Medium	40 minutes	>100K TLOC
Small	9 minutes	<100K TLOC

Note: Average Fortify SCA scan time Fortify on Demand static assessments with standard onboarding process for new applications. Actual scan time for an application will vary based on code structure, complexity and related factors. Changes to submitted application structure may require manual intervention to re-tune Fortify SCA configuration.

Fortify on Demand Offers Flexible Licensing Models

Fortify on Demand Static Assessments are available in two licensing models to address specific AppSec objectives. Customers can mix and match these offerings to each application in their portfolio based on risk profile, AppSec maturity, development cadence, compliance requirements, etc.

1. **Fortify on Demand Static Assessment Subscriptions** are ideal in more mature AppSec and DevOps environments that are optimized for automation, speed and agility. A manual audit of vulnerabilities by our security experts during the onboarding scan establishes a high quality baseline with unlimited subsequent automated scans that are ideal for continuous integration.
2. **Fortify on Demand Static+ Assessment Subscriptions** allow for the choice of manual audits on each scan. Static+ subscriptions are appropriate when an existing application is expected to undergo significant changes throughout the subscription term. Another scenario is when your AppSec program requires flexibility to re-baseline an application multiple times during the subscription. New or developing application security programs frequently prefer Static+ assessments so development teams can ramp up using a measured scanning cadence with the absolute minimum chance of false positives. Static+ assessments are also designed for business-critical applications for any business, no matter the maturity of its AppSec program. Business-critical applications can span financial, compliance or other high priority initiatives.

Fortify on Demand also offers licensing models for application software security without a subscription. Both Static and Static+ assessments can be purchased with the Fortify on Demand Single Scan option, which is attractive for applications that require two or fewer scans annually, meeting compliance requirements on legacy applications, or time-bounded applications (industry event app, marketing promotion app, etc.)

4. Fortify Internal Assessments—October 2020

Comparison: Fortify on Demand Static vs. Static + Assessment

	Static	Static+
Application Type	Web, mobile, thick-client	Web, mobile, thick-client
Files Supported	Source, binary, byte	Source, binary, byte
Open Source Analysis	Yes*	Yes*
Fortify Static Code Analyzer	Yes	Yes
Fortify Scan Analytics	Yes	Yes
Audit Methodology (single scan)	Automated	Automated + Manual
Audit Methodology (subscription)	Manual for initial scan then Automated	Automated + Manual
Fortify Security Assistant (available by subscription only)	Yes	Yes

*Added Sonatype subscription needed

Close the Loop with Secure Development Training

Fortify offers comprehensive AppSec training, research and insight—accessible anytime, anywhere. Our mission is to be your valued partner and accelerate the success of your Software Security Assurance program. Resources available include:

- Real-time access within Fortify on Demand to Secure Code Warrior, a leading gamified training platform helping programmers learn and expand their cybersecurity skills
- Guidance and recommendations, built within Fortify on Demand, on how to remediate code vulnerabilities
- Integration of the latest Fortify Software Security Research (SSR) rule packs for coverage, remediation and insights on the new code vulnerabilities
- Extensive Fortify on Demand Training curriculum, focused on secure code development, embedded within the Fortify on Demand solution.

Let's Get Started

Fortify offers the most comprehensive static, dynamic and mobile 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 with Fortify on Demand to build a scalable, nimble Software Security Assurance 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

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes
A Micro Focus line of business