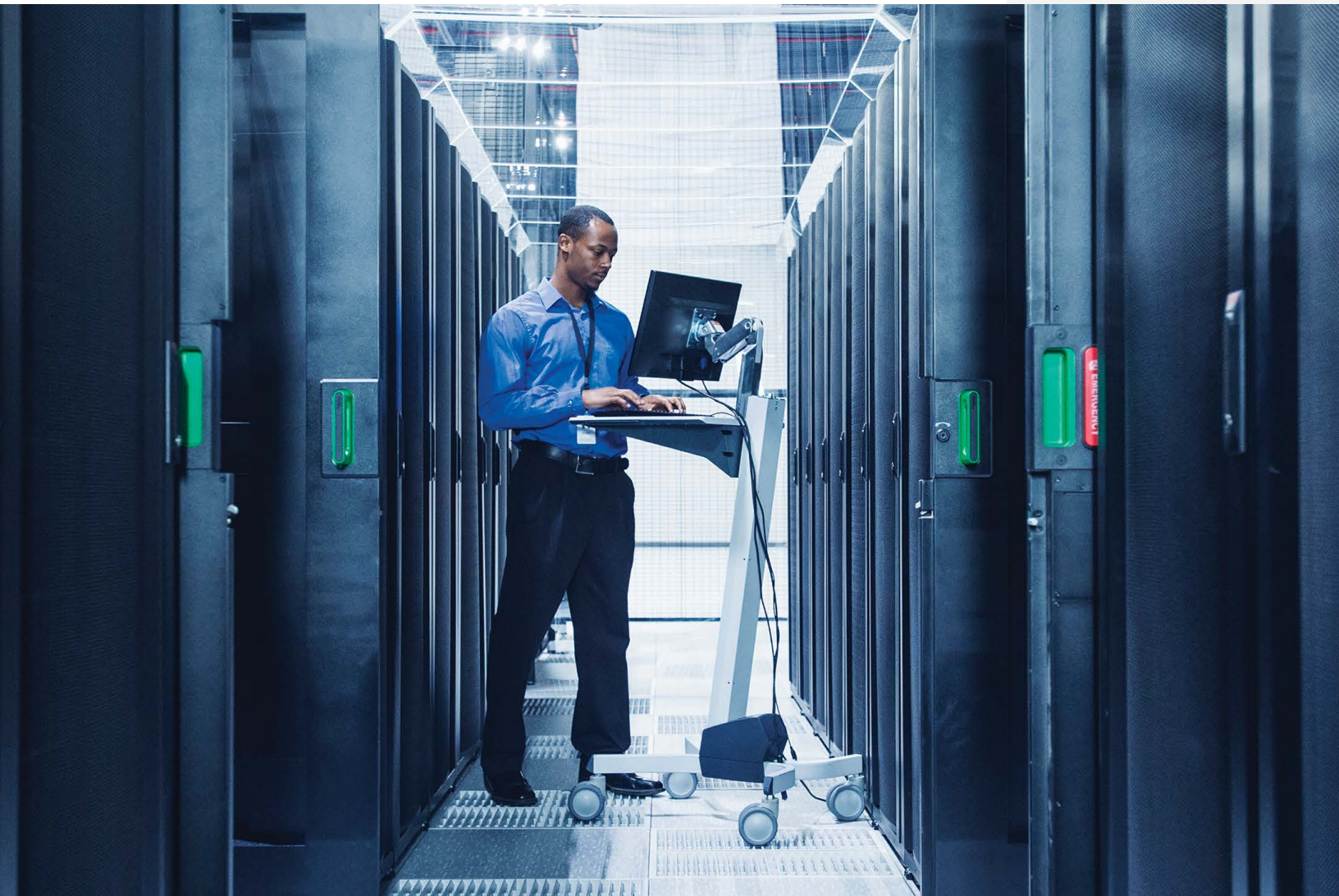
CyberRes

Brochure

Fortify on Demand Dynamic Application Security Testing



Dynamic 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, scalable **Security Testing** embedded into the development tool chain and **Continuous Monitoring** to protect software running in production.

Protect 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 been 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.* Dynamic Application Security Testing (DAST) is critical to identify vulnerabilities in the software in the Quality Assurance (QA) phase.

Fortify on Demand Dynamic Assessments Are Essential to Software Security

Fortify on Demand dynamic assessments complement Static Application Security Testing of source code because they identify vulnerabilities that can be detected only in a live/simulated production environment. Examples of vulnerabilities detected only through dynamic testing range from configuration related vulnerabilities to sophisticated hacking techniques and specific attack vectors against an application's business logic. Our dynamic assessments mimic real-world hacking attacks to ensure that potential vulnerabilities are identified and isolated. Fortify on Demand dynamic assessments can also be integrated into the live production environment through our optional Continuous Application Monitoring solution.

Fortify on Demand Dynamic Application Security Testing (DAST) assessments:

- Mimic real-world hacking techniques and attacks on targeted applications
- Provide comprehensive security analysis of complex web applications and web services
- Crawl the entire attack surface to find exploitable vulnerabilities
- Can test internal applications through site-to-site VPN or whitelisting Fortify on Demand's official data centre IP addresses

Our DAST technologies support web applications, web services, and mobile-browser optimized applications. What makes Fortify on Demand DAST assessments unique is that they integrate four essential components: **WebInspect automated testing, manual analysis, optional active IAST** and **continuous application monitoring**.

* "The State of Application Security in the Enterprise"

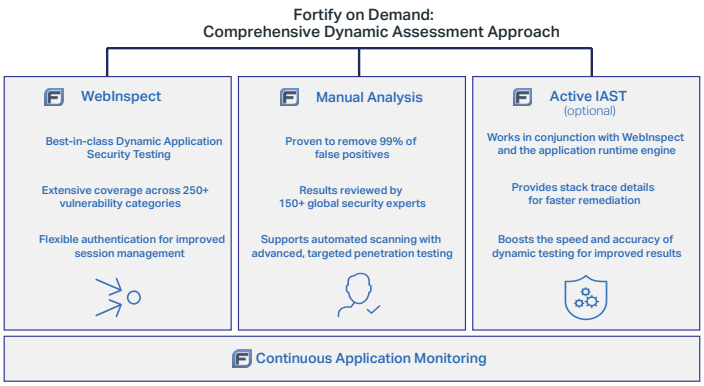


Figure 1. Fortify on Demand: Comprehensive Dynamic Assessment Approach

Fortify on Demand Leverages Webinspect's Leading-Edge DAST Capabilities

WebInspect is the cornerstone of Fortify on Demand DAST and is the industry-leading dynamic web application security assessment solution. WebInspect is designed to thoroughly analyze today's complex web applications and web services for security vulnerabilities. Fortify on Demand discovers potential threats across all web applications and web services as they move across QA, staging, and into production.

Capability highlights of WebInspect include:

- Coverage across 250+ unique vulnerability categories
- Automated scan scheduling and built-in support to pause and resume scans during scan blackout periods to save time and resources
- Flexible authentication handling for improved session management, particularly with complex applications
- Broad client side language support such as HTML5, Flash, JavaScript among others
- Language-agnostic scanning technology covering virtually all server-side languages
- Assessments available for single page applications (SPAs) and web services

Our Dedicated Application Security Experts Manually Analyze Scan Results

Fortify on Demand works as an extension of your in-house application security team. We recognize the significant time and money your time has spent in developing new applications. Your business may not have the time nor the in-house expertise to review extensive reports to validate scan coverage and remove false positives. Fortify on Demand, in its commitment to ensure actionable results, takes the extra step to manually review all initial dynamic scan results with its dedicated team of 150+ global security experts. This includes the isolation and the removal of false positives. Some of the tasks performed by the Fortify on Demand testing team include:

- Development of authentication macros if needed
- Validation of scan coverage
- Remove 99+% of false positive from the results aggregating both manual and automated audits—saving you remediation time and resources

Our team can also manually analyze the target web application or web service for up to 8 hours using Fortify on Demand's testing methodology to augment the WebInspect scan results with advanced, targeted penetration testing. Our experts conduct an in-depth examination of the application's authentication scheme, session management, access control, and a review for logical flaws and faulty developer assumptions. They identify vulnerabilities that can only be detected through human intervention, including, but not limited to:

- The ability to harvest user accounts
- Bypassing multi-step authentication
- Password reset flaws
- Accessing other users' data or sensitive content
- Horizontal or vertical privilege escalation
- Skip key transaction steps such as shopping cart payments
- Abuse of discount or business limit restrictions
- Unique business logic flaws due to faulty developer assumptions

Fortify on Demand Includes an Active IAST Option to Strengthen Dynamic Assessments

Innovation and leadership are among the reasons why customers choose Fortify for their application security solution. An example of this is providing our Fortify on Demand customers the option of integrating our visionary active **IAST (Interactive Application Security Testing) Agent** during the dynamic assessment process. The IAST Agent is installed on the application runtime server and automatically synchronizes with WebInspect during a Fortify on Demand dynamic assessment. Benefits of the IAST Agent include:

- Improved coverage (All major components of the attack surface are tested)
- Greater accuracy (Fewer false positives are generated)
- Faster remediation (Full stack trace provided for each issue identified)

Fortify on Demand Continuous Application Monitoring Protects Applications in Production

Complementing comprehensive security testing before release, Fortify on Demand Continuous Application Monitoring provides valuable information about the ever-changing risk for applications in production. Continuous Application Monitoring combines lightweight, production-safe dynamic vulnerability scanning and application risk profiling to alert when risk-relevant changes occur. Automated, unauthenticated scanning occurs on a weekly basis and focuses on a combination of the most common and critical vulnerabilities across the OWASP Top 10, as well as configuration vulnerabilities that can be introduced at any time in the production environment—and can't be caught in pre-production testing. The risk profile assessment included in each scan examines characteristics that drive attacker interest and internal compliance requirements, including:

- Collecting Personal Identification Information (PII)
- E-commerce functionality
- Authentication methods and restricted content
- Web technologies in the application stack (application server, Javascript libraries, etc)

Fortify on Demand Offers Flexible Dynamic Assessment Service Options

Fortify on Demand Dynamic Assessments are available in two service levels to address specific application security objectives, and both levels can be purchased as a subscription or a single scan. Subscription packages allow for unlimited scans of an application over a 12 month period. Subscriptions offer continuous support for your on-going dynamic application security testing programs.

Which service option is right for your business? It depends on the risk level of your applications.

1. Fortify on Demand Dynamic Assessment Subscriptions are ideal for lower risk applications that have already been deployed or are not as critical to your business. Dynamic assessments can be managed in a more automated fashion and can deliver security testing during iterative releases or new feature enhancements during the subscription period.
2. Fortify on Demand Dynamic+ Assessment Subscriptions are ideal for business-critical, high risk applications. Additional manual analysis by the Fortify on Demand team becomes necessary to identify all potential vulnerabilities, particularly for applications that collect PII or process financial transactions. The higher the potential risk of an application breach to your business, the more manual testing and analysis may be necessary.

Single scans may be preferred for applications that have limited lifecycles or limited compliance requirements. Single scans also include one remediation scan to validate fixes for the vulnerabilities that have been reported earlier as a result of the full scan. Remediation scans must be conducted within 30 calendar days of the original assessment. Web service application testing, which involves significant manual testing, is available as single scans only (no subscriptions).

Comparison: Fortify on Demand "Dynamic" vs. "Dynamic +" Assessment Service Subscriptions

Fortify on Demand Dynamic Assessments are available in two service levels to address specific application security objectives, and both levels can be purchased as a subscription or a single scan. Subscription packages allow for unlimited scans of an application over a 12 month period. Subscriptions offer continuous support for your on-going dynamic application security testing programs.

	Fortify on Demand Dynamic Assessment	Fortify on Demand Dynamic+ Assessment
Application Type	Website	Website OR Web Services
WebInspect DAST	Yes	Yes
Authentication	Yes	Yes
Security expert review (Including false positive removal)	Yes	Yes
Continuous Application Monitoring (Subscriptions only)	Yes	Yes
Active IAST	Optional	Optional
Manual vulnerability testing	No	Yes

Fortify on Demand Offers the Complete Dynamic Scanning Solution

Fortify on Demand is your application security as a service partner to offer complete Software Security Assurance. Testing and monitoring your applications throughout the entire SDLC is essential to preventing exploitable vulnerabilities. Our dynamic assessments go above and beyond the traditional DAST. We recognize today's threat landscape requires a multiple-pronged approach to ensure that your business is protected. Only Fortify on Demand can integrate:

- Comprehensive Dynamic Application Security Testing powered by WebInspect
- Extensive manual review of scan results by a global team of 150+ application security experts
- Leading-edge technologies such as active IAST and runtime application self-protection (RASP with Fortify Application Defender)
- Continuous monitoring of your applications through risk assessment profiles and on-going scans in production

Let's Get Started

Fortify offers the most comprehensive static and dynamic application security testing technologies, along with runtime application monitoring, backed by industry-leading security research.

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