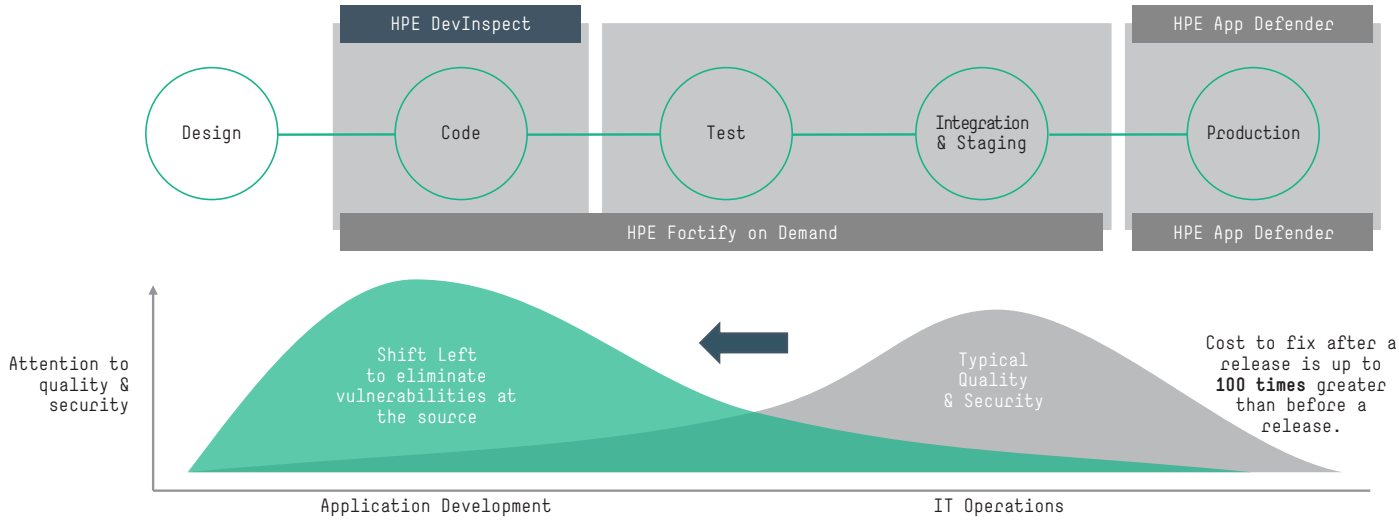
Hewlett Packard Enterprise

HPE DevInspect

Secure code development at the speed of DevOps

Application security embedded in development

Eliminate security vulnerabilities as you code



Fundamental application security errors in coding are still occurring

- 52 percent of Web applications experience issues with input validation, including cross-site scripting, SQL injection, and other vulnerabilities
- 48 percent mobile applications with input validation vulnerabilities

Critical Web security vulnerabilities impact almost half of all Web applications

- 48 percent have cross-frame scripting
- 37 percent have cross-site scripting

See the **2015 HPE Cyber Risk Report** for more details.

Instant application security for the developer

HPE DevInspect brings the full power of market-leading application security technologies directly to the developer, ensuring more secure code as you "shift left" in your development processes. By providing immediate and continuous feedback to the developer on security vulnerabilities, DevInspect improves the security of software by identifying and removing application security vulnerabilities as code is written. DevInspect, drastically reduces the effort to find and remediate vulnerabilities by giving developers instant and frequent feedback on the security of their code before they ever think about deploying it. Designed to be a natural part of the developer environment, DevInspect assesses software from inside the developer's environment (IDE) as they type and when they build. DevInspect brings the power of HPE Fortify's industry-leading security static, dynamic and interactive application testing technologies[1] to provide deep, accurate and actionable security results. Results can be seamlessly integrated into existing application security programs for enterprise-wide application security management.

[1] Gartner Magic Quadrant 2015

Secure and agile development
Agility tops business leaders' list of priorities, as they prepare for the fast-paced, hypercompetitive future. IT departments find that in order to support escalating business technology needs, they must streamline processes, reduce resource consumption, and reduce time-to-market. Development organizations can save time and money by identifying and correcting security defects even earlier in the agile development process than before; however, most developers are not security experts and require help to find and fix security defects. HPE DevInspect solves this by pinpointing application security defects and providing remediation while the developer is coding. With this immediate and continuous feedback, developers can take quick, decisive action to remediate vulnerabilities, within their agile development process.

Integrated with development tools
HPE DevInspect features intuitive integration with the Eclipse integrated development environment (IDE). You can safeguard your applications and improve your security expertise without ever leaving your IDE.

Find and fix security defects at the source

HPE DevInspect combines instant and frequent feedback with deep and comprehensive security analysis to find security defects early, fixing them quickly and preventing potential attacks in production.

Find vulnerabilities instantly
HPE DevInspect includes Fortify's Security Assistant feature that helps the developer fix security defects in real time as he or she is producing the code. It highlights vulnerable code and suggests changes much the same way a spell-checker identifies potential errors and suggests alternatives. The recommendations and examples crafted by the market-leading HPE Security Research team provide accurate and detailed information that you can use to correct your code.

Frequent testing feedback
For high quality applications to be delivered at a rapid pace, it is important to continuously assess and monitor them at every stage of the lifecycle. By applying powerful automated application security testing, you can speed up cycles and reduce errors.

Fix vulnerabilities with accuracy
The in-depth analysis of HPE DevInspect includes the full capabilities of HPE Fortify Static Code Analyzer (SCA) to accurately identify security defects during development. Fortify SCA performs deep and comprehensive analysis of an entire application. Issue evidence and remediation guidance is provided on an issue-by-issue basis and assists developers with locating the root cause of the problem down to the line of code.

Integral part of a full lifecycle SSA solution
HPE DevInspect is a stand-alone secure coding tool for developers, but is also an integral part of a full-lifecycle software security assurance (SSA) solution. HPE DevInspect can be used seamlessly with the cloud-based HPE Fortify on Demand to couple developer testing with cloud-based managed services for complete portfolio coverage. When you are ready to expand and scale, it integrates with the full suite of HPE Fortify Software Security Center and Fortify on Demand for enterprise-wide, distributed assessment capabilities. Both provide a scalable, organization-wide view of application security with centralized control over user permissions, security policies, and remote scanning administration.

Get comprehensive security assessment during application development

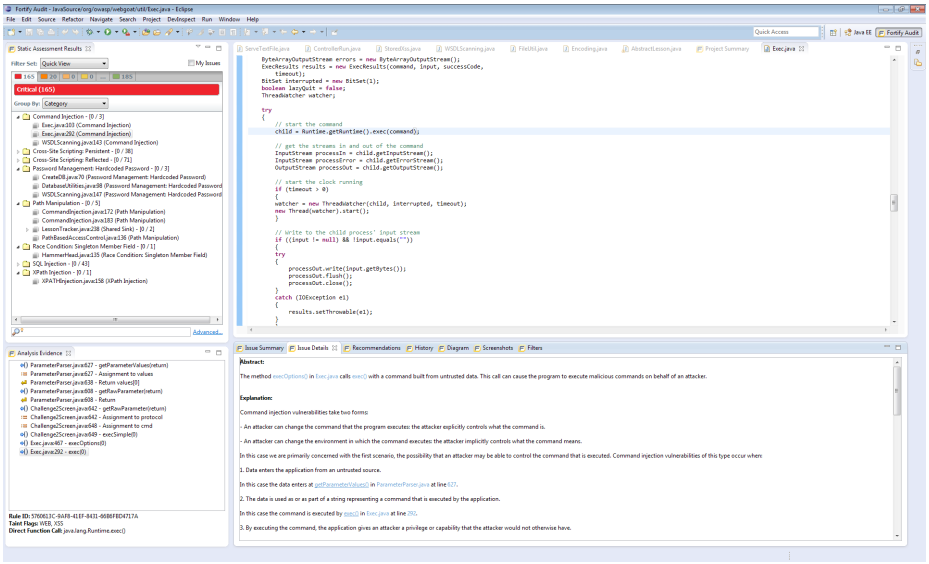


Figure 1. Powerful security advice at your fingertips

HPE DevInspect finds application security defects right at the source—when the developer is coding. Eliminate downstream efforts and streamline your agile development efforts.

Key features and benefits

Instant security results

- Inline analysis of the source code as the developer types
- Removes vulnerabilities at their source avoiding remediation efforts later
- Out-of-the-box-results—no configuration required

Continuous security feedback

- Continuously assesses source code and updates security findings as code is written
- Tracks findings and remediation

Natural part of developer environment

- Fully integrated into the native development environment (IDE) and the DevOps work flow
- Use seamlessly in conjunction with cloud-based managed security testing in Fortify on Demand
- Connected with full suite of Fortify software security assurance solutions

Deep and accurate analysis

- Fewer false positives; more accurate assessment
- Leverage the leading HPE Security Fortify Static Code Analyzer[2] right at the desktop
- The user has the option to run HPE Security Assistant or other more in-depth analysis methods

Matures with your security program

- Use stand-alone for developers and, when you are ready, seamlessly integrate with industry-leading HPE Security Fortify Software Security Center and Fortify on Demand[2] for centralized management of your application security program

[2] **Forrester Wave: Application Security, Q4 2014**

Specification

Multiple analysis approach

- Real-time static code analysis testing as you type
- In-depth, comprehensive static code analysis as you build/compile
- Improve accuracy and results using this in-depth approach
- Receive vulnerability risk ratings based on **Fortify Priority Order**
- Obtain remediation guidance tailored to your target environment
- Download vulnerability test updates from expert HPE security researchers
- Find vulnerabilities exposed through third-party components

Table 1: Minimum specifications

RAM • 8 GB of random access memory (RAM) • 40 GB available • 4 cores 1 GHz processor or better
Eclipse 4.5.x IDE
For use with Java applications

Learn more at
hpe.com/software/devinspect

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-2975ENN, December 2015