Hewlett Packard Enterprise



# Certify security of third-party software

## HPE Security Fortify on Demand

**Risk in acquired software**

For most organizations, software purchased from vendors represents a large percentage of deployed software and therefore a substantial area of potential risk; yet vendors provide no visibility into its security state. While improved contracts can provide some remedies in the case of a breach, ultimately it is better to avoid the problem if possible. Today, this means analyzing the software for vulnerabilities during the procurement or upgrade process and demanding that significant problems be addressed prior to acceptance.

The challenge in this situation is that software vendors are, for a variety of reasons, resistant to having their software analyzed. Vendors are concerned about the potential for information about specific vulnerabilities being leaked and causing havoc. Likewise, providing their most precious intellectual property, their source code, is also seen as too risky. It is with this challenge in mind that Fortify on Demand has created the Vendor Security Management Program, a hosted, security-as-a-service offering built around the HPE Fortify award-winning analysis and application security testing capabilities.

Fortify on Demand's Vendor Security Management Program enables companies to verify the security of their third party acquired applications while providing capabilities that let the vendor stay in control of the process. Software vendors simply upload their binaries, source or byte code, have a scan conducted, and address any issues before publishing a report summarizing the security of their application. Fortify serves the role of an independent third party and system of record, conducting a consistent, unbiased security testing and analysis of the application and providing a detailed tamper-proof report back to the security team.

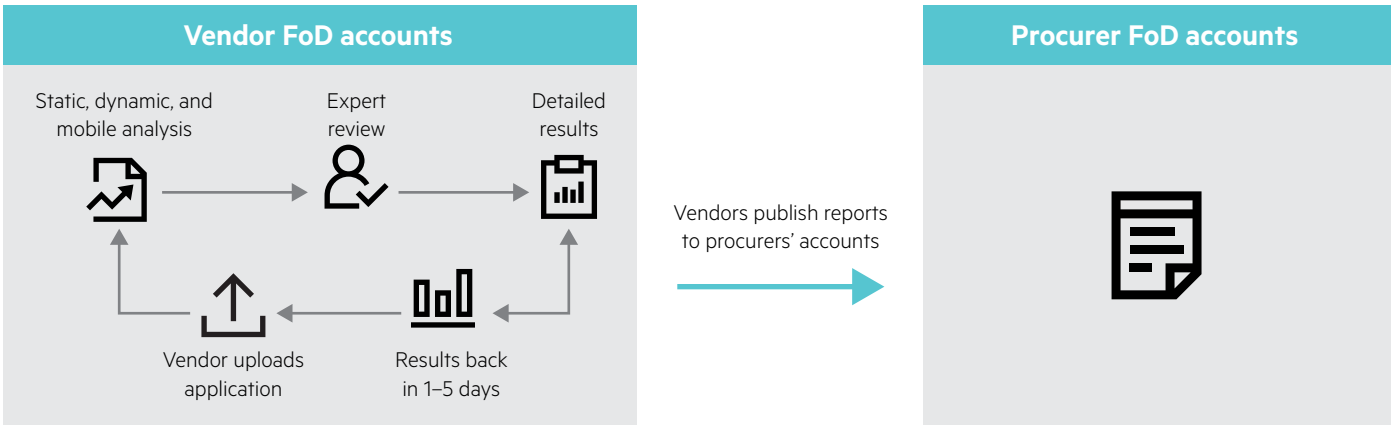


**Figure 1:** The Vendor Security Management Program process

## Key features

### For Vendors

- Provides a standard way of demonstrating security of your software
  - Shows you take security seriously
- Allows for a simple contract clause
  - Negates need for open-ended contractual commitments
- Eliminates repetition—do once for all your customers
  - Reduced cost
- Safeguards proprietary code
  - No need to release code to your customers
- Enhances the security of your software
  - Software developers benefit from line of code details and remediation suggestions
- Reduces the risk of a breach that could damage your reputation

### For Procurers

- Reduces risk
- Outlines a consistent approach for all vendors
  - Can be tailored based on risk profile of application
- Sets out a standard clause that can be included in contracts
  - Clear standard, not contentious
- Eliminates effort on your part
  - Fortify on Demand does it all
- Provides a single view of compliance across all your applications regardless of source

Learn more at
**hpe.com/software/fod**

**Sign up for updates**

★ Rate this document

Hewlett Packard Enterprise



4AA6-1026ENW, February 2016, Rev. 1