Saltworks
An Orasi Company

Securing the SDLC: Micro Focus Fortify Leads the Way

Software security has never been more important, given that software is the number one attack vector implicated in successful cyberattacks. For application developers, the stakes are especially high. According to research firm Gartner, nearly 80 percent of security breaches occur at the application layer. Yet, even decade-old vulnerabilities are still being exploited, because software teams don't have powerful, proactive tools—and an end-to-end program for security—in place.

To reduce the odds of having applications exploited, developing organizations must focus on security, not only at the end of the development cycle, and certainly not solely as a response to issues found in production. Rather, security must be built into the entire SDLC, from secure development through robust security testing and swift action on identified vulnerabilities. Once applications are released to production, ongoing monitoring and further remediation are imperative to assure end-to-end security. With every code change or periodic release, the cycle begins anew.

Shift Left—to Integrated Security Testing

Solutions now exist that facilitate application security (AppSec) by automating some of the most important tasks, which are often difficult and time-consuming to accomplish manually. One example we frequently recommend—and help organizations deploy effectively—is Micro Focus Fortify, a vulnerability scanning platform that offers two different scanning models: static and dynamic.

Static and dynamic scanning are not opposites, with one scrutinizing existing applications and the other examining code under development. Rather, they are complementary.

Static code analysis: Purpose-designed to identify security vulnerabilities efficiently in source code, providing immediate feedback on issues that might create vulnerabilities as they are introduced into code during development activities. For static code analysis, Orasi recommends Micro Focus Fortify Static Code Analyzer (SCA).

Fortify SCA is a static scanning solution that can integrate into any environment through scripts, plugins, and GUI tools. It prioritizes the vulnerabilities it discovers, delivering them categorized and ranked by risk to provide developers with a functional action plan. Micro Focus security experts continually expand and update the security coding rules incorporated into Fortify SCA, giving it the most comprehensive rule set of any static code analysis tool on the market.

Fortify Scan Results

Static Scans

35%
Issues Resolved
0-30 Days
(1st scan range)

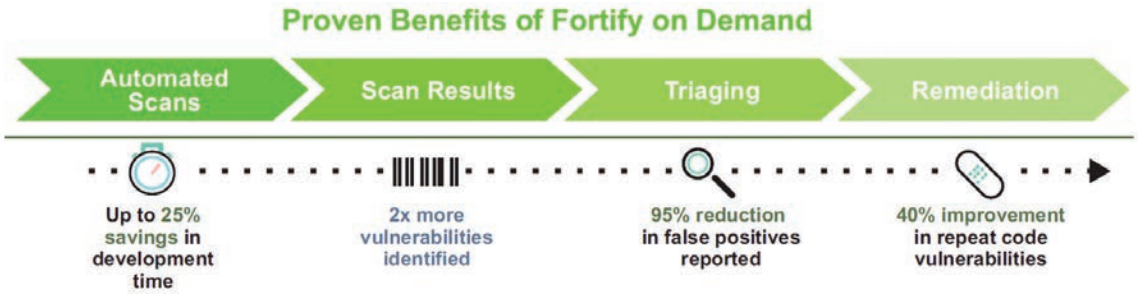
90%
Issues Resolved
0-120 Days
(1st four scan ranges)

Dynamic Scans

32%
Issues Resolved
0-30 Days
(1st scan range)

79%
Issues Resolved
90-120 Days
(End of 4th scan range)

Most critical-severity issues were addressed by the second range of scans (6 to 11 scans, or 31 to 60 days).



Dynamic analysis: Used primarily for pre-release testing and for post-release monitoring, dynamic analysis tools explore the attack surface of running applications to identify new types of vulnerabilities that are difficult to detect solely through source code analysis. For dynamic code analysis, Saltworks recommends Micro Focus WebInspect.

WebInspect is designed not only to find vulnerabilities in existing applications but also to identify them in application updates and other releases. This type of analysis can be invaluable, since release cycles are often time constrained, encouraging teams to bypass security checks.

The WebInspect agent crawls each application, searching for new types of vulnerabilities that are more readily detectable in a runtime environment. Through the use of sophisticated algorithms, it can also detect web services and capture URL rewrites (a rule-based rewriting mechanism for modifying request URLs before they are processed by a web server).

Application Security as a Service

For companies that seek a comprehensive application security solution but prefer a SaaS platform, Saltworks recommends Micro Focus Fortify on Demand (FoD). FoD allows any organization to test an application's security quickly, accurately, affordably, and without any software to install or manage. This automated, on-demand service helps organizations surmount two key challenges:

- Ensuring the security of third-party applications;
- Building security into the product at maximum speed and efficiency.

Taken as a whole, the Fortify family is the premier option for embedding end-to-end protection into software across the entire SDLC. There is no application security suite like it.