

# Software Integrity for Agile Environments

January 2011

# The Pressure is On

---

More than ever before, companies are being asked to do things faster. They need to get products to market faster to remain competitive and capitalize on market opportunity. That time pressure is being felt across all phases of the software development lifecycle. Developers need to deliver more innovation through complex code faster, and time allotted for formal quality control is shrinking. To deal with this pressure, companies are turning to Agile development methodologies for rapid iterative development cycles and the promise of improved efficiency and faster time to market. According to a recent study published by Dr. Dobbs and Forrester Research, over 45% of companies have implemented some form of Agile development.

## **Agile: Not A Panacea**

Agile development is not a panacea. While it's designed to increase efficiency, it can also introduce risk as testing cycles get condensed and serious bugs can get overlooked. As the testing cycles are squeezed, more of the burden for code quality assurance is getting pushed into development. With additional pressure placed on developers, they can not afford the time and effort required for manual testing. They need an automated approach for assuring the quality, security and safety of their code.

## **Code Assurance Through Static Analysis**

Static analysis enables developers to assure the quality, security and safety of their code as it is being written through automated defect detection and resolution. As the code is compiled, it is analyzed for defects. Developers can then quickly address high severity issues without sacrificing time to market. Waiting for QA or Security teams to find defects later in the lifecycle can result in rework and expensive project delays. Issues found in development are significantly cheaper to fix, up to 30% cheaper in time and cost, than those found in QA or worse, found in by the end customer. For a static analysis solution to be effective, it should provide developers with relevant, accurate and actionable information. To maximize efficiencies, it must seamlessly integrate into the existing software development process. For example, if a developer is running a continuous build system where the software is compiled on a regular basis, the static analysis solution should run each time the build is created.

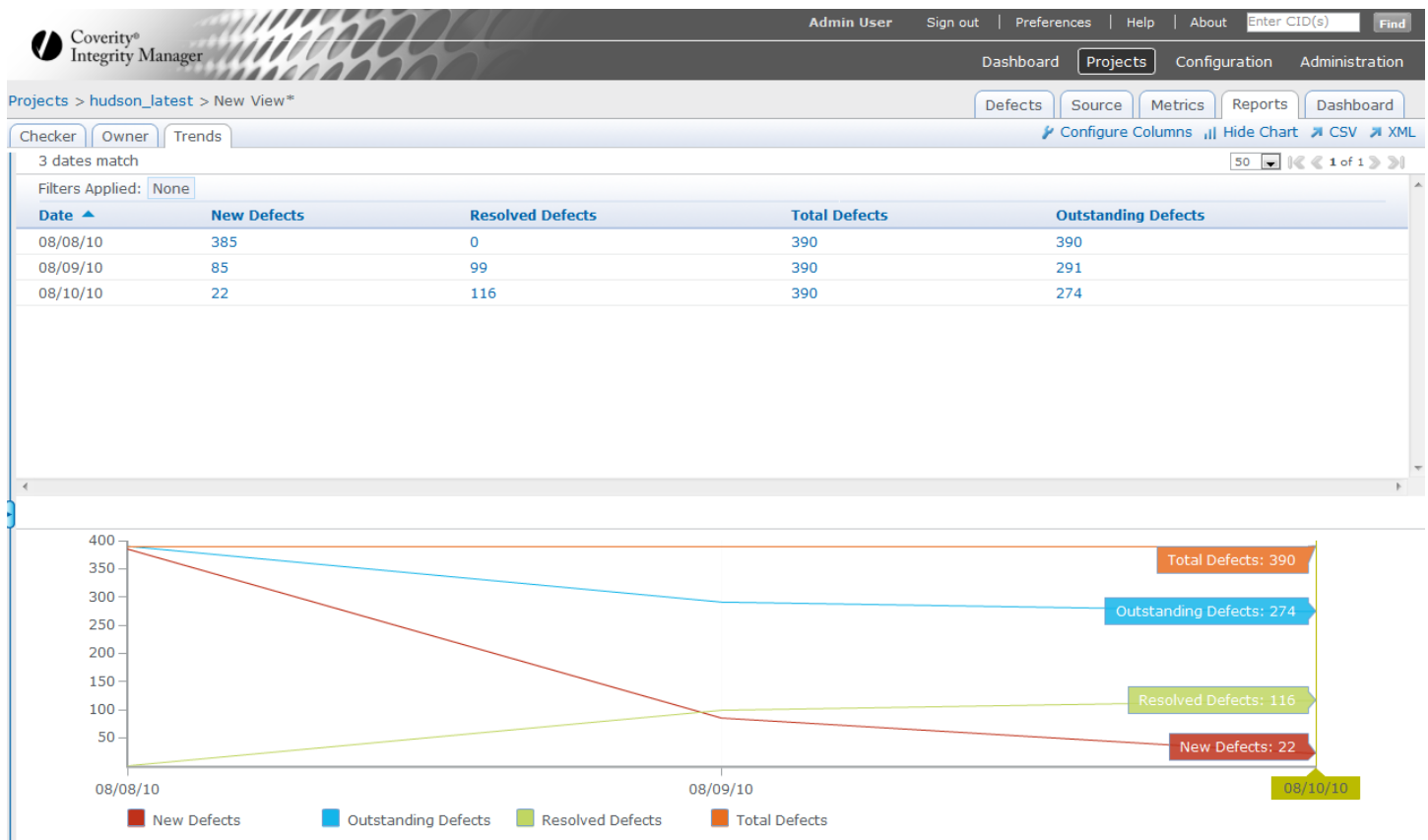
# Coverity Static Analysis

Coverity is the market leader in static analysis with over 1,000 customers and five billion lines of code under analysis. It's specifically designed to help developers save time by allowing them to quickly identify quality, security and safety defects in their code. It utilizes sophisticated algorithms to identify and triage high risk defects that could result in software crashes, security breaches or safety issues. It enables users to find hard to spot issues such as null reference pointers, memory leaks and potentially exploitable security flaws in the largest, most complex code bases. Coverity provides relevant information specifically tailored for the developer. They are presented with accurate and actionable information about the severity of defects, potential impact and where they occur in the code so developers can get to work quickly on resolving the most critical defects while keeping their product schedule on track. Plus, developers can identify all of the places the defect exists in the code base across projects and products so they can fix it once and update it everywhere which saves valuable time.

## Visibility & Control

Through the unified management interface, Coverity Integrity Manager, managers get visibility into overall code quality of internally developed code, third party code and across development sprints. They can quickly see new defects and assign them to the appropriate engineer based on who last made changes to the code.

Deciding when a project is ready for a release is a key principle in Agile. In Scrum, one of the most common types of Agile, teams hold daily meetings to report progress and make decisions. Coverity Integrity Manager provides rich data and metrics about the quality of each sprint. This information is critical when trying to balance the need for rapid time to market with the need for acceptable quality levels.

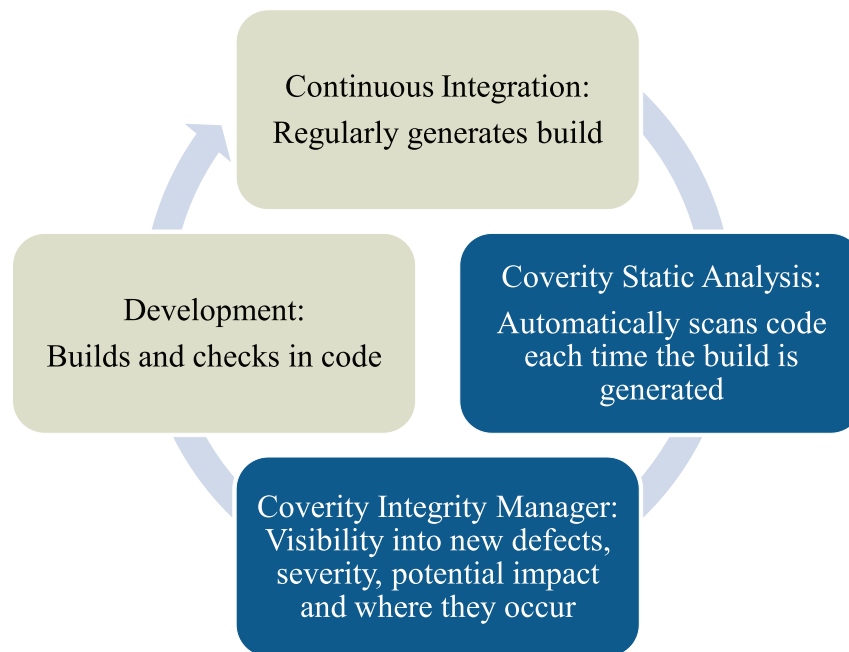


# Integrated Into The Software Development Lifecycle

With so many extra pressures on developers today they need solutions that will tie into their existing software development tools and processes. Coverity Static Analysis integrates seamlessly with common development practices and market leading tools.

## Continuous Integration

One of the most common practices in Agile development is continuous integration. It's been embraced by the majority of the Agile community because it enables a faster, automated central build process. Integration of the code happens every time it gets checked into the source control system so that quality, safety and security issues can be found early. In the traditional waterfall model, teams wait for all of the development to be completed before conducting the integration; which can result in a higher cost of quality. Coverity Static Analysis complements the practice of continuous integration by implementing a continuous process for code assurance. Each time a central build is generated, Coverity can automatically scan the code for high severity defects. Users have the flexibility to tune the scan to conduct the most complete analysis or only identify the highest risk defects. Once defects are identified, they are published to a defect database for tracking and management. Developers can receive automatic notification so they can quickly begin the triage and resolution process. Coverity offers out of the box integration with Electric Cloud Accelerator so every time a build is generated it's checked for quality, safety and security defects.



Other common practices for incorporating Coverity into the development process include the following:

## Clean Before Check In

Developers can run the scan of their source code from their desktop prior to checking it in to a source code repository system; a process often referred to as clean before check in. By scanning the code before checking it in, developers are able to address security and quality issues immediately.

## The Nightly Build

Another common approach is to run the scan on the source code after the nightly build. This approach enables a project administrator to review the overall code quality of the project, triage and assign defects which need resolution to the appropriate developer. This methodology enables users to pinpoint errors which may result from the integration or conflicts in the integrated code streams.

## Seamless Integration

Coverity Integrity Manager easily integrates into existing development infrastructure such as:

- Source Control Systems
- Bug tracking systems
- IDEs including Microsoft Visual Studio 2010 and Eclipse
- Build Systems

## Summary

Companies have adopted Agile development to cope with the market's demand for increased speed. Developers are acutely feeling the pressure and can no longer afford to wait until the end of a formal QA cycle or security audit to be informed of defects which need to be addressed. They need an automated solution for assuring the quality, safety and security of their software. Coverity Static Analysis allows developers to test early and often so they can ensure the quality at each development sprint. By finding and addressing the most critical issues early, defects are cheaper and faster to fix. Seamless integration with existing Agile development methodologies and tools helps maximize development efficiencies.

## For more information

Find out how Coverity can help your organization improve the integrity of your software and enhance your Agile Development initiatives. To learn more, contact your Coverity representative or visit us at [www.Coverity.com](http://www.Coverity.com)

# About Coverity

Coverity ([www.coverity.com](http://www.coverity.com)), the software integrity leader, is the trusted standard for companies that have a zero-tolerance policy for software failures. Coverity's award-winning portfolio of software integrity ([www.coverity.com/products](http://www.coverity.com/products)) products discovers software defects in development before they can impact the business. More than 900 companies and organizations rely on Coverity to help them deliver high-integrity software. Coverity is a privately held company headquartered in San Francisco.

Coverity and Coverity Prevent are trademarks of Coverity, Inc. All other company and product names are the property of their respective owners.

Copyright © 2010, Coverity, Inc. All Rights Reserved.

Visit us at [www.coverity.com](http://www.coverity.com).

## Headquarters

185 Berry St. Suite 1600  
San Francisco, CA 94107  
USA

**General:** (415) 321-5200

**U.S. Sales:** (800) 873-8193

**International Sales:** +1 (415) 321-5237

**Fax:** (415) 541-9521

## Boston

230 Congress St.  
3rd Floor  
Boston, MA 02110  
USA

**General:** (617) 933-6500

## London

Coverity Ltd  
Quatro House  
Lyon Way, Camberley,  
Surrey GU16 7ER

**General:** 01276 804790

**Fax:** 01276 804676

## Israel

Engineering Software Lab  
LTD (E.S.L.)  
Floor 21 Beit Gibor Sport  
7 Menachem Begin St.  
Ramat Gan 52521

**General:** +972 3 6122918

**Fax:** +972 3 6122919

## Japan

Coverity Asia Pacific  
Shinjuku Nomura Bldg.,  
10 Fl.  
1-26-2 Nishi-Shinjuku,  
Shinjuku-ku  
Tokyo 163-0510 Japan

**General:** +81-3-5909-8838

**Fax:** +81-3-5909-8839

## Japan

Hankyu Grand Building,  
20 Fl.  
8-47, Kakuda-cho  
Kita-ku, Osaka-shi  
Osaka, 530-0017

**General:** +81-6-7711-1624

**Fax:** +81-6-6573-1179