Parasoft Application Security Solution

Improve Security without Impeding Development Productivity—Establish a Continuous Security Process

Parasoft, the industry-leader in development-driven quality solutions, is now delivering the next generation of application security solutions. These solutions establish a continuous process that identifies and remediates security vulnerabilities across every stage of the SDLC—as well as ingrains security tasks into the team’s workflow. Rather than impact productivity, you actually improve it.

- For teams ready to embrace the ideal policy-based approach to security, Parasoft establishes a system that automatically monitors whether your security policies are implemented in the code, applied at all layers of the application stack, operate correctly in the context of realistic scenarios, and persist as the application evolves.

- For teams who need to rapidly reduce their security risk, Parasoft delivers a “jump start” solution for preventing the most likely application security vulnerabilities (OWASP Top 10, PCI, CWE, DISA STIG etc.)

- For teams tasked with performing a comprehensive security assessment, Parasoft provides an automated system that applies state-of-the-art analyses throughout all stages of the SDLC—testing the application from the inside-out and outside-in to identify potential vulnerabilities.

In all cases, Parasoft’s unique automated infrastructure drives the process to ensure that it remains on track and does not disrupt the team’s workflow.

To promote rapid remediation, each vulnerability detected is prioritized, automatically correlated to the developer who introduced it, then distributed to his or her IDE with direct links to the problematic code.

Moreover, Parasoft’s Development Testing Platform provides real-time visibility into overall security status and processes, documents improvements, and helps you determine what additional actions are needed to safeguard security.
Comprehensive Analysis within a Continuous Process

### Analysis Capabilities

- **Rule-based static code analysis**: Verifies that your organization's security policy is implemented in your code. Also identifies common security vulnerabilities. Parasoft’s rule set is the most comprehensive in the industry, and is constantly being extended.

- **Peer code review process automation**: Facilitates peer review for a high-level analysis of security, design, etc.—even for geographically-distributed teams and outsourced development.

- **Data flow analysis**: Detects injection vulnerabilities, XSS, exposure of sensitive data, and other vulnerabilities without test cases or application execution.

- **Unit-level security test generation and execution**: Starts testing validation methods and verifying security functionality before the complete system is ready, reducing the length and cost of downstream security verification.

- **Penetration testing**: Verifies that the security policy operates correctly at the messaging/protocol level. Also identifies common security vulnerabilities via “outside-in” testing.

- **Runtime analysis/monitoring**: Exposes security vulnerabilities that manifest themselves only at application runtime.

- **Continuous regression testing**: Ensures that the application remains secure as it evolves in response to changing business demands.

### Process/Workflow Capabilities

- **Security policy development**: Ensures that security requirements are clearly defined, visible, and enforceable.

- **Centralized policy management**: Ensures consistent, automated application of all relevant policies—from security, reliability, performance, and maintainability, to SOA governance, to regulatory compliance (SOX, PCI, HIPAA, etc.).

- **Automated infrastructure**: Makes security tasks an unobtrusive part of the team's existing workflow. It analyzes the code and application nightly, then notifies the appropriate team members if action is needed. Interactive desktop testing is also available for immediate feedback.

- **Centralized reporting**: Ensures real-time visibility into security status and processes. This helps managers assess and document trends, as well as determine if additional actions are needed to safeguard security.

- **Integration with development infrastructure**: Correlates results with requirements, bugs, and source code changes.

- **Error assignment and distribution**: Promotes fast remediation. Each vulnerability detected is prioritized, assigned to the developer who wrote the related code, and distributed to his or her IDE with direct links to the problematic code.

### Technologies Supported

Java / C/C++ / .NET languages (C#, Visual Basic, Managed C++) / SOA / Web services / Web applications / Web 2.0 / RIA / AJAX / SOAP / BPEL / Multiple message protocols / JSP / XML / HTML / JavaScript / WSDL / EJB / CSS / VBScript/ASP

### Frameworks/Standards/Regulations Supported

OWASP / PCI / DHS / NIST / SOX / HIPAA / ISO/IEC / Others

### Compatible Software and Platforms

Eclipse / Rational Application Developer (RAD) / Microsoft Visual Studio Wind River / Borland / IntelliJ / Oracle / BEA / Software AG/webMethods / IBM MQ-Series / TIBCO / Sonic / IONA / HP / Other leading platforms
Quality = Reliability + Security

Security and reliability are inextricably intertwined in today’s complex applications. You can’t rest assured that your application security efforts will protect you unless you know that the application will operate reliably. After all, your “secure” login process will be inconsequential if the application happens to skip it under exceptional conditions. And you can’t be confident that the application will operate reliably unless you know that security attacks can’t hijack or crash it.

Without a Continuous Process, Security and Reliability Efforts Decay

Although security and reliability problems have distinctly different manifestations and impacts, the underlying methods used to identify and prevent them have much in common—static and dynamic analysis, runtime analysis, and other testing technologies are hardly new.

With the same methods comes the same main obstacle to sustained adoption: they tend to disrupt the development process, overwhelm the team, and inevitably decay—leaving the team with a long list of known problems, but little actual improvement. This is especially pronounced with security because most developers aren’t trained in it and don’t think it’s their concern.

Parasoft—Industry Leader in Quality as a Continuous Process—Makes Security + Reliability Practical and Sustainable

With over 25 years of experience helping over half of the Fortune 500 companies implement static analysis, dynamic analysis, runtime analysis, peer code review, and other core verification methods, Parasoft knows what it takes to make security and reliability practical and sustainable.

Parasoft engineered a process for ingraining security tasks across the SDLC in a way that improves rather than impacts productivity—as well as an automated infrastructure to drive this process.

The same system that is established for safeguarding security can also be leveraged to improve reliability.

The result is a continuous quality process that delivers:

- Confidence—and evidence—that all development activities adhere to policies and meet uniform expectations.
- More rapid and agile responses to business demands.
- Reduced risk of business downtime, ensuring business continuity. Continuous process improvement, increasing productivity and reducing cost.
Parasoft—Leader in Delivering Quality as a Continuous Process

About Parasoft
For 25+ years Parasoft has been empowering organizations to deliver better business applications faster. We achieve this by delivering quality as a continuous process throughout the SDLC not just QA. The result is a sustainable process that delivers greater productivity at the same time that it improves software quality.

Parasoft Development Testing Platform deliver an end-to-end quality process that begins with a requirement and ends with the audit of a business process. They support the following components:

- **Error Prevention:** Parasoft delivers an automated framework to ensure all software development activities meet uniform expectations around security, reliability, performance, and maintainability. We provide a foundation for producing solid code by exposing structural errors and preventing entire classes of errors. This initiates the continuous quality process, delivering greater productivity and significantly fewer software defects.

- **Continuous Regression Testing:** Parasoft’s continuous regression testing immediately alerts you when modifications impact application behavior. By providing a safety net that alerts the team when modifications impact application behavior, it enables rapid and agile responses to business demands, reducing the risk of change.

- **Functional Audit:** Parasoft’s continuous quality practices promote the reuse of test assets as building blocks to streamline the validation of changing business requirements. This enables your team to execute a more complete audit of your business application. The result is a reduced risk of business downtime, ensuring business continuity.

- **Process Visibility and Control:** SDLC quality metrics are fragmented across key systems such as requirements, build, and source control management. Parasoft aggregates and correlates this system data, delivering a comprehensive view of your development processes. This process visibility facilitates continuous process improvement, increasing productivity and reducing cost.

About Automated Defect Prevention
Interested in Automated Defect Prevention? Parasoft wrote the book on it. Parasoft CEO Adam Kolawa, who was recently recognized by eWeek as one of the 100 Most Influential People in IT, co-authored Automated Defect Prevention: Best Practices in Software Management (Wiley-IEEE, 2007).

To learn more, visit http://www.parasoft.com/adp.

“In their authoritative new book, Dorota Huizinga and Adam Kolawa have done an admirable job defining a realistic methodology for implementing infrastructure for automatically preventing defects from getting into software. Is it simple? No, of course not. There’s no silver bullet. But when the software industry is ready to journey toward zero-defect applications, the road will look like Huizinga and Kolawa’s “Automated Defect Prevention.”

Alan Zeichick – Editorial Director, BZ Media’s SD Times