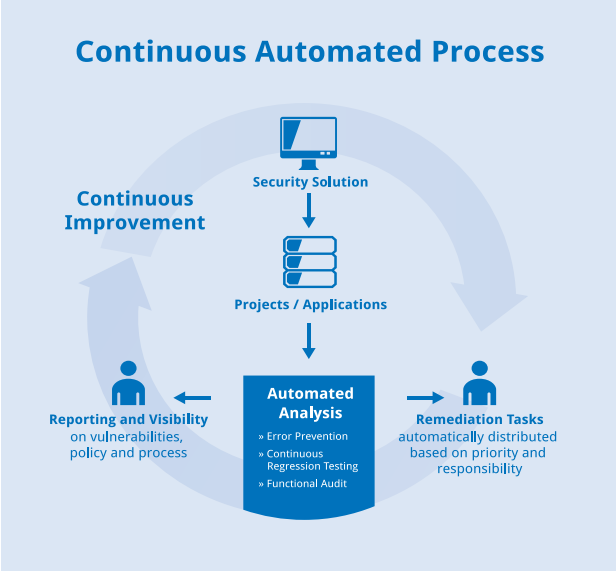
Parasoft Application Security Solution

A Continuous Process for Enterprise Application Security

Parasoft's Application Security Solution helps organizations ensure that security verification and remediation tasks are deployed across every stage of the SDLC by engraining software quality practices into the team's workflow. The solution automatically monitors policy compliance at all layers of the application stack, identifies vulnerabilities, and collects process metrics.



Automate Compliance with Software Security Standards

Rapidly reduce security risk by preventing common—and not-so common—application security vulnerabilities. Static code analysis rules that ensure compliance with OWASP Top 10, CWE/SAN, FDA, MISRA, PCI DSS, and more are built into the solution. As part of Parasoft Development Testing Platform, organizations can also meet traceability requirements mandated by regulatory agencies.

Apply Security Practices throughout the SDLC

Perform comprehensive security assessments using Parasoft's automated system that applies state-of-the-art analyses throughout all stages of the SDLC. Test the application from the inside-out and outside-in to identify potential vulnerabilities and drive the process to ensure that it remains on track without disrupt the team's workflow. Moreover, Parasoft provides real-time visibility into overall security status and processes, documents improvements, and helps you determine what additional actions are needed to safeguard security.

Shift Application Security Left

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. By preventing security-related defects from touching the code, organizations lower downstream costs associated with debugging, as well as market-related costs associated with releasing vulnerable software.

Proud Contributor to DHS SWAMP

Parasoft proudly contributes to the Software Assurance Marketplace (SWAMP), an initiative from the Department of Homeland Security's Cyber Security Division. SWAMP helps protect the nation's critical infrastructure by improving software used for essential functions, such as electrical power, gas and oil, and banking and finance. As part of Parasoft's Development Testing Platform (DTP) family of automated defect prevention and continuous testing solutions, Parasoft's Application Security Solution identifies potential risk at the code level while helping organizations comply with known software quality guidelines.

About Parasoft

With over 25 years of experience empowering organizations to deliver better business applications faster, Parasoft is the leading provider of software quality and application security solutions. By helping organizations, including over half of the Fortune 500 companies, implement static analysis, dynamic flow analysis, runtime error detection, peer code review, and other core verification methods, Parasoft makes security and reliability practical and sustainable throughout the SDLC—not just QA.

Parasoft delivers 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 provides 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:** Continuous regression testing immediately alerts you when modifications impact application behavior, which enables rapid and agile responses to business demands while reducing the risk of change.
- **Functional Audit:** 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 typically fragmented across systems, such as requirements, build, and source control management. Parasoft aggregates and correlates data from disparate development infrastructure components, enabling a comprehensive view of development processes. This visibility facilitates continuous process improvement, increasing productivity and reducing cost.

Supported Languages and Technologies

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 / 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

Analysis Capabilities

- **Rule-based static code analysis:** Verifies that your organization's security policy is implemented in your code and 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.

PARASOFT

USA PARASOFT HEADQUARTERS / 101 E. Huntington Drive, Monrovia, CA 91016
Phone: (888) 305-0041 / Email: info@parasoft.com