



Klocwork: Software Security Through Source Code Analysis

Klocwork provides enterprise source code analysis tools that identify critical software security vulnerabilities in both code and architecture.

Klocwork provides developers, software architects and security specialists with tools to identify, assess, remediate and measure security vulnerabilities as an integral part of the software development lifecycle.

Through Klocwork source code analysis, security organizations can establish secure coding best practices across the development team through consistent, policy-based deployment and ongoing education capabilities.

“Overall, the combination of early defect and vulnerability identification within the IDE, the integrated architecture capabilities and Klocwork’s breadth of analysis across key quality concerns and security vulnerabilities in C, C++ and Java contributed to its selection by BMC.”

– from Klocwork’s BMC Case Study



// SECURITY VULNERABILITY IDENTIFICATION

Programming bugs can lead to serious security vulnerabilities. To eliminate code vulnerabilities and reduce the need for post-release security patches, organizations need to discover and remove vulnerabilities early in the development process.

Klocwork provides development organizations with comprehensive visibility into the security and reliability of their code bases and software architectures. By connecting developer source code analysis to the overall system context, Klocwork tools prevent critical software vulnerabilities from ever entering the code stream.

Klocwork products help developers fix security vulnerabilities as they work by identifying critical defects before unit test or code check-in. This ensures that potentially crippling coding errors never make it to market and that security and QA functions can focus on comprehensive testing.

// COMPREHENSIVE SOURCE CODE ANALYSIS

Klocwork’s source code analysis tools let organizations:

- » Analyze C, C++ and Java code
- » Provides support for major Java frameworks including J2EE, J2ME, J2SE, Google Web Tool Kit, and Hibernate
- » Identify, understand and repair vulnerabilities before they become problems
 - Run Klocwork tools within developers’ native IDE, text editor or command line environments
 - Reported vulnerabilities include explanations on the nature of the risk along with mitigation recommendations
- » Review more code in less time
 - Run automatic source code analyses during the software build process
 - Better understand the software through architectural visualization tools
- » Customize source code analyses to suit the needs of particular projects or environments

PROVEN IN SERIOUS ENVIRONMENTS

Klocwork offers a proven, scalable source code analysis solution used by more than 250 customers, including global leaders in networking equipment, silicon chips, computer and Internet software, aerospace and defense, and finance and insurance.



// EMPOWERING THE DEVELOPER

Klocwork offers the first source code analysis solution to combine the productivity benefits of desktop source code analysis with the power and accuracy of system-wide analysis. Klocwork tools let developers identify and remediate security vulnerabilities at the point of creation – within their IDE. Klocwork offers plug-ins for the following leading IDEs:

- » Microsoft Visual Studio
- » Eclipse and Eclipse-based IDEs
- » Wind River
- » QNX
- » IBM Rational Application Developer
- » JetBrains IntelliJIDEA

Klocwork IDE plug-ins include comprehensive documentation explaining each vulnerability, its risk and recommendations for mitigation.

// ADVANCED VULNERABILITY DETECTION

Klocwork detects serious, exploitable security vulnerabilities and code defects in C, C++ and Java environments. Klocwork tools identify coding issues such as:

Java:

- » Null reference exceptions
- » Code injection vulnerabilities
- » SQL injection vulnerabilities
- » Cross site scripting flaws
- » LDAP spoofing
- » Denial of service vulnerabilities

C & C++:

- » Buffer overflows and code injection vulnerabilities
- » DNS spoofing
- » Tainted data propagation and usage

// COMPREHENSIVE REPORTING

Klocwork products reveal the critical security issues identified by leading security groups and publications including:

- » The Open Web Application Security Project (OWASP) Top 10 Project
- » The US Department of Homeland Security's Common Weakness Enumeration (CWE) dictionary
- » The National Institute of Science and Technology and the US Department of Commerce's Software Assurance Metrics and Tools Evaluation (SAMATE) project

Eliminate Programming Errors

A 2006 SANS report found that three programming errors are responsible for more than 85% of critical security vulnerabilities.

Klocwork products eliminate these:

- » Accepting input from users without validating and sanitizing the input
- » Allowing data placed in buffers to exceed the length of the buffer
- » Handling integers incorrectly

Klocwork products also support policy definition to ensure better, more secure coding practices across the development team.

With Klocwork, organizations can ensure the quality and security of mission-critical software across millions of lines of code and provide comprehensive guidance on software security to distributed development teams.

Contact Klocwork today for a [free trial](#).