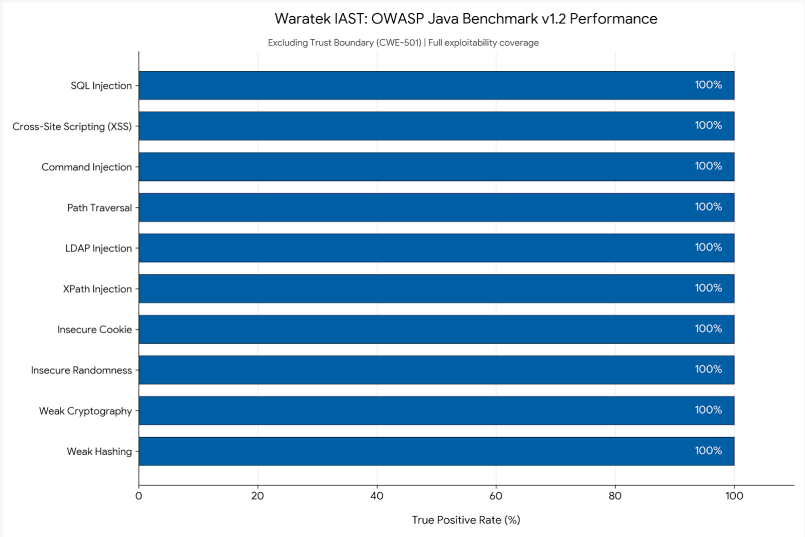
Waratek Redefines Secure Development with Launch of Waratek IAST at JavaOne 2026

AI-assisted code speeds development, but introduces vulnerabilities at an alarming rate. Waratek IAST reports flaws that are exploitable with 100% accuracy.



Waratek's new IAST runtime solution achieved the highest level of accuracy using the OWASP Benchmark Test for Java.

REDWOOD CITY, CA, UNITED STATES, March 18, 2026 /EINPresswire.com/ -- Waratek, a leader in next-generation application security, today announced the official launch of Waratek IAST (Interactive Application Security Testing). The announcement was made during the JavaOne 2026 conference, where Waratek CEO Doug Ennis delivered a featured session on securing the software development lifecycle (SDLC) in the age of AI-generated code.

The launch addresses a critical and growing risk for enterprises relying on Large Language Models (LLMs) to accelerate Java development. While AI boosts productivity, new data from industry leaders reveals that this increased code volume comes with a significant security trade-off, specifically for the Java language.

> We must move beyond trying to scan code after it's written and start instrumenting the applications as they are built. This is a mandatory control for the modern, high-velocity, and AI-driven SDLC."
>
> *Doug Ennis, Waratek CEO*

The AI-Generated Code Risk: Java Leads in Failure Rate

A recent analysis by Veracode highlights that code generated by LLMs has surprisingly low pass rates when it comes to standard security testing. Among the four most common programming languages, Java was identified as the language with the single lowest security pass rate for AI-generated code snippets. According to the analysis, the security failure rate for Java was a staggering 72% (derived from a 28.50% pass rate). Compared

to other popular languages like Python (61.69% pass rate), JavaScript (57.34% pass rate), and C# (55.27% pass rate), Java is the most vulnerable at the moment of generation.

Waratek logo

"The shift toward AI-assisted development is a double-edged sword; we are shipping more code than ever, but we are also shipping more vulnerabilities than ever," said Doug Ennis, CEO of Waratek. “The data clearly indicates that when organizations ask AI to write Java code, they are inherently accepting a massive spike in risk. This isn't just about a few mistakes; a 72% failure rate is a catastrophic failure of security-by-design.”

"With the launch of Waratek IAST, we are providing teams with the 'truth at runtime,'" Ennis continued. "By proving exactly how an exploit interacts with the JVM before it ever hits production, we eliminate the friction between security and dev teams. We must move beyond trying to scan code after it’s written and start instrumenting the applications as they are built. This is a mandatory control for the modern, high-velocity, and AI-driven SDLC."

Key Features of Waratek IAST Include:
100% OWASP Benchmark Accuracy: Achieve a perfect score across all OWASP vulnerability categories with zero manual fine-tuning or custom rulesets. Waratek IAST delivers out-of-the-box precision that eliminates the "noise" typically associated with legacy scanning tools.

Low to Zero False Positives: By analyzing code execution within the runtime environment, Waratek IAST identifies real, exploitable vulnerabilities with precision, eliminating the need for manual triaging.

AI-Ready Security: Specifically designed to catch injection vulnerabilities, deserialization gadgets, and logic flaws often introduced by GenAI coding assistants and which are prevalent in the low-performing Java samples.

Seamless Integration: Works within existing CI/CD pipelines without requiring changes to the application source code or complex configuration.
Unified Platform: Waratek IAST, paired with Waratek’s award-winning RASP (Runtime Application Self-Protection), provides a "Detect-to-Protect" loop from development through production.

The launch coincides with Ennis’s JavaOne 2026 presentation, "When Code Has No Author: Securing Java Apps Through the SDLC," where he demonstrated how IAST plus RASP serves as the primary defense against the unique risks of fragmented code ownership.

Waratek IAST is available immediately for Java applications. For more information or to request a demo, visit www.waratek.com.

About Waratek
Waratek is the industry pioneer making Java security achievable for every mission-critical application and API using innovative runtime protections. Headquartered in Chicago and Dublin, Waratek's patented technology is trusted by enterprises around the world to develop, secure and patch applications in real-time without downtime or code changes.

Doug Ennis
Waratek
+1 872-469-8605
email us here
Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/899612982

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.