

Black Duck Accelerates Coverity with AI-Powered Enhancements and EU CRA-Ready Capabilities

New features enable teams to maximize AI-assisted development, streamline vulnerability triage, and meet with emerging security and compliance requirements

BURLINGTON, Mass., July 14, 2026 /PRNewswire/ -- [Black Duck®](#), the leader in AI-powered application security, today unveiled new capabilities across its [Coverity®](#) static analysis solution. The updates advance AI-powered development and security capabilities, support compliance workflows for the EU Cyber Resilience Act (CRA) and other emerging regulations, and deliver a range of user experience enhancements.

Together, the updates mark the arrival of Coverity's first AI-powered features into customer hands, extend Coverity into modern AI-assisted development workflows, and give security and development teams the ability to prioritize findings by security impact, directly supporting conformance with emerging regulatory obligations.

Coverity's new AI capabilities are also designed to run on the customer's own LLM of choice, giving organizations full control over where their code and scan data are processed, a critical requirement for regulated industries and enterprises with strict data governance policies.

Deterministic Static Analysis, Now Amplified by AI

Each of the AI-powered capabilities below is designed to operate with the customer's own LLM, so organizations retain control over model choice, data residency, and audit trails, extending Coverity's long-standing commitment to trust and transparency into the AI era.

- **AI-Assisted Issue Triage:** This feature is optimized for triage of C and C++ findings, which can be prone to higher levels of false positives, while also delivering significantly improved issue triage across all other supported languages.
- **Security Scan MCP Server for AI Coding Agents:** A new Model Context Protocol server enables AI coding agents to run local Coverity scans and surface security and quality issues in-context, bringing Coverity's deterministic, reproducible scan results into agentic workflows so AI coding agents act on verified truth, not probabilistic guesses.
- **New AI-Powered IDOR Vulnerability Detection:** A new security checker that identifies Insecure Direct Object Reference (IDOR) vulnerabilities in JavaScript and TypeScript code. This class of flaw arises when applications expose internal identifiers (e.g., user IDs, database keys, filenames) without verifying authorization before performing an action.

Purpose-Built Capabilities to Support CRA Readiness

With the CRA vulnerability management reporting countdown underway, Coverity is delivering foundational capabilities that help align scan results with regulatory expectations:

- **New Security Impact Lens:** Users can now sort and filter issues by security priority, bringing the same rigor to security prioritization that Coverity has long offered for code quality. This lens directly supports

conformance with the CRA.

- **CRA-Aligned Checker Option:** A new option enables checkers that support organizations' efforts to meet both the vulnerability management and cybersecurity obligations of the new CRA regulations, so scan results are aligned to these requirements out of the box.

Rust Programming Language Support

Coverity now analyzes Rust 1.92, extending quality and security analysis support to one of the fastest-growing systems programming languages.

A Streamlined Experience for Faster, Focused Triage

A new Coverity user interface streamlines the workflows customers use most. Refreshed navigation, smarter issue filtering, and a more efficient triage experience help teams cut through large volumes of findings with less friction.

"Coverity has set the gold standard for static analysis for more than two decades, and we're raising the bar by pairing its deterministic precision with the speed of AI, meeting customers where modern software development is heading," said Dipto Chakravarty, Chief Product & Technology Officer at Black Duck. "Code today is written, reviewed, and shipped by agents, and businesses have to move at machine speed to stay ahead. These updates deliver exactly that: AI that slashes triage time without sacrificing auditability, an MCP server that brings Coverity into agentic developer workflows, and new lenses and checkers that make CRA readiness operational, not aspirational."

AVAILABILITY

All new Coverity capabilities announced today are generally available for customer deployment.

Existing Coverity customers gain these AI-powered capabilities without changing what they rely on most: the deterministic, auditable scan results that make Coverity the standard for regulated industries.

For more information, visit the [Coverity Documentation Portal](#).

About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.

SOURCE Black Duck Software

For further information: Editorial Contact: Liz Samet, Black Duck, 336.414.6753, esamet@blackduck.com

<https://news.blackduck.com/2026-07-14-Black-Duck-Accelerates-Coverity-with-AI-Powered-Enhancements-and-EU-CRA-Ready-Capabilities>