



# Leading European Asset Manager Secures AI-Generated Code with Coverity

## ABOUT THE CUSTOMER

**Industry:** Financial services

### Customer footprint

- Institutional and retail investors across Europe
- One of the region's largest asset managers by assets under management

### Core business areas

- Asset and portfolio management
- Risk and compliance management

### Challenges

- Vulnerability backlog accumulating over time
- AI-generated code outpacing security review
- Regulatory mandate to eliminate all critical- and high-severity vulnerabilities

### Requirements

- Faster mean time to remediation
- DORA and PCI DSS compliance
- Scalable across all development teams

### Solution

- Coverity Static Analysis

A leading European asset management firm that manages trillions of euros in investments chose Coverity® Static Analysis to secure its human- and AI-generated code. The firm is subject to standards including the Digital Operational Resilience Act (DORA) and the Payment Card Industry Data Security Standard (PCI DSS) that demand robust controls and verifiable, continuous evidence that applications are free of critical- and high-severity vulnerabilities.

The firm's development teams have increasingly turned to AI coding agents to accelerate the production of application code. As a result, code is being generated at a pace and volume that would have been unthinkable just a few years ago.

## THE CHALLENGE: Keeping up with AI coding agents

The firm's security and development leaders faced a compound problem. First, a large backlog of vulnerabilities had built up over time, the result of years of rapid development across a sprawling application portfolio. Second, widespread adoption of AI coding agents added significantly more code—and significantly more vulnerabilities. Compliance requirements made the challenge even more pressing. DORA and PCI DSS require the firm to ensure its applications are free of all critical- and high-severity vulnerabilities.

The firm needed a way to identify these vulnerabilities in both human- and AI-generated code, triage them efficiently, and prioritize remediation so the most important issues get fixed first.

## THE SOLUTION: Coverity and AI-assisted triage

The firm integrated Coverity into its agentic development workflows. Coverity operates within the same workflows where code is being produced, so vulnerability detection happens continuously and in context. Then, AI analysis classifies each issue to deliver focused and prioritized remediation plans rather than a raw, undifferentiated list of findings. This means developers can quickly verify the results and prioritize the most important issues to remediate.

The combination of accurate static analysis and intelligent triage allows developers to spend their time on the vulnerabilities that matter. This is a critical advantage, as code is being generated faster than ever.

## THE RESULTS: Improved MTTR and reduced risk

Combining Coverity scans with AI-assisted triage significantly reduced mean time to remediation (MTTR). The firm has been able to drive down its open vulnerability count to levels it had not previously achieved—even as AI coding agents continue to accelerate the volume of code being produced.

Having a verified, prioritized set of issues allows the firm to focus on the issues that matter most, dramatically shortening the path from detection to fix. The accuracy of Coverity's scans played a key role in this. Its low false positive rate improved developer trust in the results and helped contain the cost of the AI analysis layer, since fewer findings had to be processed.

## SUMMARY

AI coding agents continue to be a central part of the firm's development strategy. Coverity's accurate static analysis in combination with AI-assisted triage has become an essential part of how the firm builds secure software. Embedding security into the same agentic workflows that generate the code helped the firm turn a growing backlog of vulnerabilities into a model for secure, high-velocity development.

## 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](https://www.blackduck.com).