Sonar

How a global luxury car manufacturer gained control over unpredictable code risks with SonarQube

A global luxury car manufacturer's dedicated technology and software team manages risk and governance for over 550 active projects. Their primary environment consists of sprawling, multi-module Java codebases, supporting critical platforms from sales to logistics and finance.

The challenge: Unpredictable security risks, low visibility, and delivery disruptions

Recently, a significant industry shift increased complexity for engineering leadership: rapid growth in software supply chain complexity, a continuous increase of newly reported CVEs, and escalating expectations for transparency and governance. Dependency risk was no longer solely a technical issue—it became a strategic threat to customer trust and delivery velocity.

Like many modern engineering organizations, the team faced challenges with hidden dependency risks in complex builds, unpredictable delivery pipelines, and persistent gaps in portfolio-level vulnerability visibility. Their internally developed Software Composition Analysis (SCA) tool supported SBOM generation and identification of known open source vulnerabilities. However, as their dependency trees deepened and post-build threats emerged, limitations became clear:

- Transitive (indirect) dependencies were nearly impossible to trace
- Newly disclosed vulnerabilities led to sudden, unexpected build failures
- Leadership struggled to gain real-time insight across the portfolio, resulting in time-consuming manual reviews
- Security and platform teams identified these blind spots as "the biggest pain point" of their governance model

Company

A global luxury car manufacturer

Company size

Enterprise

Industry

Automotive manufacturing

Key Results

- Faster signal and reduced overhead across 550+ projects
- Predictable software delivery
- Accelerated response to weaponized vulnerabilities
- Unified portfolio intelligence for rapid, governed remediation

Mounting vulnerabilities force urgent governance modernization

For years, the organization maintained the status quo until rising risks created a tipping point. Vulnerabilities discovered after builds exposed business-critical pipelines. Unplanned outages caused missed deadlines, and developers devoted substantial time to manual triage, slowing progress across teams.

"They needed to know, instantly and at scale, where they were exposed—and what mattered most," explained an engineering leader. A search began for a solution built to address velocity, scale, and cross-team collaboration in governance and security.

The Solution: SonarQube Advanced Security delivers instant portfolio coverage

The global luxury car manufacturer's technology team selected SonarQube Advanced Security to modernize their SCA workflows. The transition, spanning hundreds of projects, was described by engineers as "as easy as it could be." No custom configuration was required, and scan speeds surpassed their previous tools, saving time and reducing manual overhead.

Engineers cited SonarQube as a "big time saver," freeing both developer and security resources for higher-impact work. Onboarding was straightforward, scaling effortlessly across projects.

Three SonarQube Advanced Security capabilities that power secure, predictable software delivery:

1. Exploit-aware risk prioritization

Rather than relying only on CVSS scores, SonarQube's SCA risk signals incorporate sources such as the CISA Known Exploited Vulnerability list and EPSS scores. This enables teams to prioritize remediation for vulnerabilities with known exploits, accelerating the response to those presenting genuine risk.

2. Actionable, clear triage

SonarQube's intuitive dashboard presents rich vulnerability context, even for deeply nested dependencies. Engineers noted, "The dashboard made everything clear. We could understand the issue, right down to the specific library affected, and take action confidently." Unified, real-time reports replaced manual mapping of exposure across the portfolio. The unique data from SonarQube also includes deeper reviews of CVEs to provide actionable guidance, directly from Sonar's contractual partnership with open source maintainers. This human-curated intelligence promises to significantly reduce the noise often associated with dependency scanning.

3. Stable, predictable pipelines

Importantly, SCA findings are now decoupled from quality gates. Previously, newly disclosed vulnerabilities could automatically fail builds; SonarQube allows teams to remediate at their own pace, eliminating surprise failures and enhancing delivery consistency.

The result: Governance and compliance scaled across apps with unified SBOM and SCA intelligence

With SonarQube Advanced Security, the organization standardized SBOM and SCA intelligence across applications and shared services, bringing code quality and security together in one workflow. Leaders can manage license compliance, monitor vulnerability exposure, and enforce code standards via both quality gates and SCA dashboards.

Platform and AppSec teams report reduced developer toil, improved velocity, and a framework for repeatable incident response. Their transformation highlights actionable insights, developer empowerment, and measurable business impact at scale.

What's next: Preparing for next-gen governance and closing remaining risk blind spots

The next step involves addressing outstanding governance gaps. With upcoming portfolio- and application-level component search in SonarQube, leadership will gain the unified cross-project visibility needed, transforming blind spots into best practices.

By implementing SonarQube Advanced Security, this Global Luxury Car Manufacturer has achieved scalable governance, a developer-centered approach, and alignment with the velocity and risk demands of modern software development. This journey offers a practical blueprint for any platform or AppSec leader seeking to modernize code security while preserving speed and control.

About Sonar

Sonar helps developers accelerate productivity, improve code security and code quality, and supports organizations in meeting compliance requirements while embracing collaboration with AI technologies. The SonarQube platform, used by 7M+ developers worldwide, analyzes all code – developer-written, AI-generated, and third-party open source code – supercharging developers to build better applications, faster.

Sonar provides automated code review and assurance, inherently applies secure-by-design principles, fixes issues in code before they become a problem, and enforces policy standards – all while improving the developer experience. Sonar is trusted by the world's most innovative companies and is considered the industry standard for integrated code quality and code security. Today, Sonar is used by 400K organizations, including Mastercard, Barclays, Ford Motor US, and T-Mobile.