

Integrated code quality and security at enterprise scale with SonarQube Enterprise

AI agents now write more code than any team can review by hand. Pull requests that once ran 300 lines routinely reach 3,000, and the model that generated the code cannot catch what it was already blind to. Empowering your development teams with the tools to **deliver high-quality, secure software at speed** is paramount, while simultaneously ensuring your tool infrastructure meets the rigorous demands of enterprise operations.

SonarQube Enterprise is designed precisely for this. By equipping developers with an enterprise-ready automated code review platform, you enable high-performing teams to deliver mission-critical software at scale and speed, with verification that stays independent of the system that produced the code.

Elevate your development teams

SonarQube Enterprise provides advanced functionality that enables your development teams to achieve unparalleled levels of code quality and security and elevate them to an elite level:

- **Comprehensive code intelligence:** Gain **in-depth code analysis** across more than 45 programming languages including support for additional enterprise languages (ABAP, Ansible, Azure Pipelines, C, C++, Dart, GitHub Actions, Groovy, Jupyter Notebooks, JSON, Objective-C, PL/SQL, PostgreSQL, PowerShell, Shell, Swift, TSQL, YAML not in Community Build) (Apex, COBOL, Gosu, JCL, MuleSoft DataWeave, PL/I, RPG, and VB6 not in Developer edition).
- **Agentic code verification and remediation:** AI code generation increases output volume faster than humans can review it, and the defect rate scales with it. SonarQube Enterprise closes that gap with **organization-wide quality gates** that catch bugs and vulnerabilities in AI-generated code at the pace of creation. The **SonarQube Remediation Agent** autonomously clears technical debt by opening pre-scanned, verified pull requests before a developer reviews them, while the **SonarQube Hunter Agent** surfaces broken access control, business logic flaws, and authentication vulnerabilities that traditional static analysis isn't designed to catch. **Sonar Vortex** extends governance upstream, feeding agents your architecture rules, security standards, and compliance constraints before they write a single line. It then verifies agentic output in real time to reduce defects, build failures, and token consumption across agentic workflows before code reaches the PR.

- **Protecting enterprise codebases:** Large businesses face a unique challenge, protecting expansive, intricate codebases. SonarQube Enterprise is built for this complexity, detecting sophisticated bugs and vulnerabilities that other tools miss. With features like advanced secrets detection—now redacted by default—advanced dataflow bug detection, a unified vulnerability model that consolidates SAST, software composition analysis, and secrets findings into a single view, and cross-functional taint analysis, your teams can release stable, secure, and enterprise-ready applications with confidence.
- **Optimized developer workflows:** Analyzes branches and pull requests and supports multiple integrations into DevOps platforms. This means that **different teams with different workflows are all supported** with a single tool that governs your single set of code quality and security standards across all types of DevSecOps teams.
- **Enterprise LLM governance:** As teams integrate large language models into their development workflows, managing which models are in use and under what terms becomes an operational risk. SonarQube Enterprise gives security and platform teams a centralized control point for LLM access across the organization, replacing per-team credential sprawl with consistent, auditable policy enforcement.
- **Meet your compliance needs:** Enterprise includes security, regulatory, and audit reports so you can prove compliance with, for example, PCI, OWASP, CWE, STIG, CASA, and EU CRA standards. Teams in safety-critical industries can generate an audit-ready **MISRA C/C++ Compliance Report** directly from analysis results, and a **WCAG Accessibility Compliance Report** gives teams exportable evidence of accessibility conformance—without manual evidence assembly.
- **SonarQube Advanced Security:** Available to purchase with SonarQube Enterprise, strengthens your application security with:
 - **Software Composition Analysis (SCA)** analyzes software supply chains, identifying vulnerabilities, generating SBOMs, and ensuring license compliance, so teams can proactively secure their codebase and reduce risks associated with third-party dependencies.
 - **Advanced SAST** goes beyond traditional SAST to discover deeply hidden security vulnerabilities with fewer false positives. Advanced SAST identifies deeper and more complex vulnerabilities due to the interaction of your application code with third-party (open-source) code.

Operate with confidence in an enterprise environment

SonarQube Enterprise provides the robust foundation, scalability, and security necessary to manage complex, large-scale software portfolios across multiple teams and business units:

- **Single unified instance:** Consolidate your several separate SonarQube instances into one central instance for reduced overhead, centralized oversight, and standardization of your policies that apply to all teams and business units.
- **Unmatched scalability and performance:** Experience **fast, accurate analysis scalable to billions of lines of code**, ensuring that your integrated code quality and security efforts keep pace with your organization's growth—including the exponentially larger volumes generated by AI agents.
- **Enterprise-grade speed and reliability:** Benefit from parallel processing of analysis results so **developers are never waiting for results and can continue innovating**. The solution is **hardened to the U.S. Department of Defense (DoD) standards**, providing a trusted and secure platform for your most critical assets.
- **Portfolio management:** Generate executive-level reports for a consistent and comprehensive source of truth for code health across all your projects.
- **Self-managed and air-gapped deployment:** Agentic verification and governance capabilities run entirely inside the infrastructure of your choice—no source code crosses your perimeter. For teams in regulated, air-gapped, or VPC-restricted environments, this means you no longer have to choose between agentic development velocity and data sovereignty.
- **Trusted by industry leaders:** Join the ranks of organizations, including **over 75% of Fortune 100 companies**, that **trust SonarQube** for their integrated code quality and security needs.
- **Additional licenses** included for testing and staging environments, to minimize disruption of your development teams during updates and maintenance.
- **Premium Support available:** Ensure operational continuity and peace of mind with 24x7 Premium Support, **providing expert assistance whenever you need it**.

SonarQube Enterprise deeply integrates into your enterprise environment, putting the power of integrated code quality and security directly into your developers' hands. It is the strategic choice for organizations committed to deploying the highest application standards across their entire digital landscape—adopting agentic development at scale, governing AI model usage with confidence, and maintaining the verification layer that makes it all safe.