Datasheet

Developer-first secrets detection across your workflow with SonarQube

Stop credentials from ever reaching your repository. SonarQube for IDE catches hard-coded secrets—like database passwords and tokens—as you write code, while SonarQube Server and SonarQube Cloud provide automated checks in your PRs. This integrated approach helps you commit with confidence. By delivering actionable code intelligence in the IDE and enforcing rigorous guardrails in CI/CD, SonarQube ensures your code is production-ready and secure by design.

Challenge

Leaked secrets are one of the fastest paths to a major security incident, granting attackers direct access to your most sensitive systems. Once a secret reaches a Git repository, the damage is already done. Remediation becomes a costly, cross-team fire drill involving credential rotation, access audits, and complex Git history cleanup to ensure the secret is no longer available in the version history.

Traditional repository scanning and perimeter tools are inherently reactive—they only alert you after the secret has already been exposed to your version control system. By the time these tools trigger a notification, the secret is already compromised and the "burn and rotate" process must begin. This approach forces security teams and platform engineering into a state of perpetual cleanup rather than prevention. To truly protect the codebase, organizations must shift their focus from finding leaks in the repository to preventing them at the source—the moment code is written in the IDE.

How SonarQube’s secrets detection works

To move beyond the cycle of reactive remediation, organizations must empower developers to stop secrets from ever entering the codebase.

- **Shifts left to the IDE:** Catches secrets the moment they are written using SonarQube for IDE, allowing for an immediate fix before the code is ever committed.
- **Powered by deep analysis:** Combines regular expressions with semantic analysis to accurately identify secrets within the context of your source code.
- **Enforces quality gates:** Automatically applies quality gates in the CI/CD pipeline to block risky changes from merging into your main branch.
- **Extensive rule library:** Covers 340+ rules identifying 450+ secret patterns across 248 cloud services and thousands of APIs.
- **High-precision results:** Engineered for accuracy with a false positive rate below 5%, reducing alert fatigue and maintaining developer trust.
- **Pre-commit protection:** SonarQube’s secret CLI allows developers to scan local files and directories before they are even staged,providing an additional layer of pre-commit protection

Key benefits

Benefit	What you get with Sonar
Prevention-first coverage	Catch secrets in the IDE and block them via quality gates, ensuring they never reach your Git history.
Fast, low-friction scanning	Secrets detection is built into your regular analysis, providing deep insights without impacting scan times.
Comprehensive workflow integration	Consistent policies and protection across the IDE, SonarQube Server, and SonarQube Cloud.
Low total-cost-of ownership	Included in all commercial editions of SonarQube Server and SonarQube Cloud; available for free in SonarQube for IDE.