Snyk Secrets

No blind spots. No noise. No exceptions.

Snyk Secrets blocks hardcoded credentials before they reach production — with ML-powered, high-precision detection across your AI coding agents, IDEs, pull requests, and CI/CD, unified with the Snyk AI Security Platform.

Secret sprawl just became an AI problem

AI coding assistants generate credential-laden code at machine speed. Agentic systems pull secrets from wherever they're stored and pass them between services with no human reviewing where they land. Stolen credentials are already the #1 initial access vector in data breaches, and Gartner predicts AI agents will cut the time to exploit an exposed credential in half by 2027.

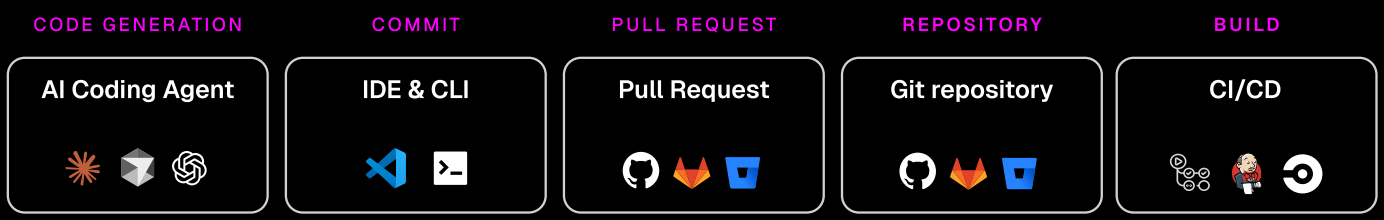
- **Machine-speed generation:** AI assistants and agents write, store, and pass credentials faster than any human review process can catch.
- **Alert fatigue:** Legacy scanners lean on regex and keyword matching alone, generating enough false positives that findings get tuned out.
- **Disconnected tooling:** Point solutions can find a secret, but can't connect that risk to the rest of your security posture.

Detection accurate enough to trust, prevention early enough to matter

Snyk Secrets closes the gap between accuracy, prevention, and platform integration. It reads the code around a candidate secret rather than just matching a pattern, then stops the real ones before they ever reach a repo.

- **High-precision detection:** Identify real secrets from false alarms by reading the file paths, variable names, and comments around it — not just matching a pattern.
- **Prevention at every stage:** Block secrets in your AI coding assistants, IDEs, at commit, in pull requests, and in CI/CD pipelines — including secrets introduced by AI coding agents.
- **Unified governance:** Manage secrets risk alongside code, open source, container, and infrastructure as code issues.

Prevention Across the Agentic Development Lifecycle



PROTECTED BY SNYK

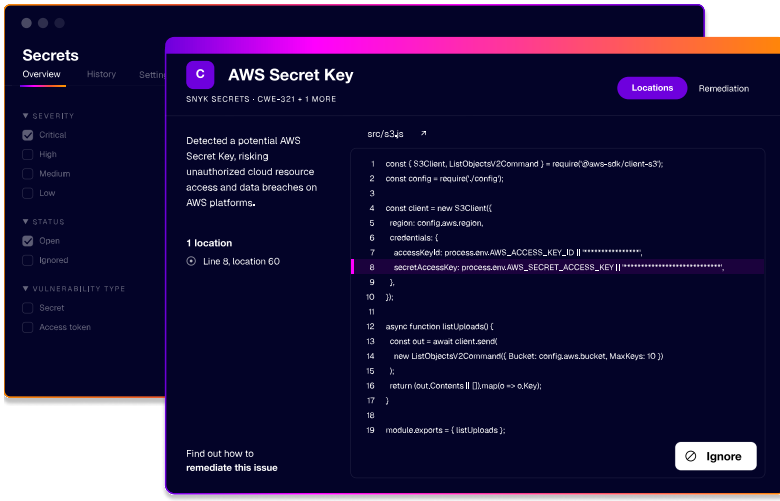
Spotify · ATLASSIAN · snowflake · twilio · Manulife · yalo

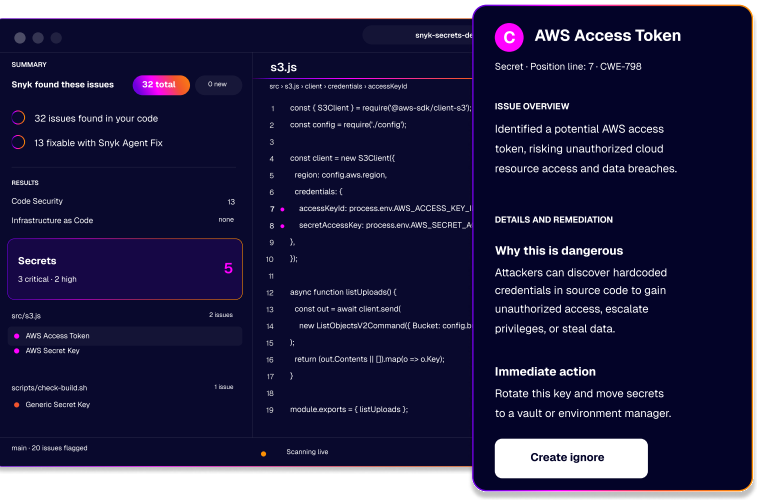
Block secrets before they ship across the ADLC

Snyk Secrets delivers accurate detection, real prevention, and unified governance — directly inside the workflows your teams already use. Its capabilities span the full software development lifecycle, from the first line written to the moment code merges.

High-precision, context-aware detection

ML-powered contextual detection reads the code around a candidate secret — file paths, variable names, comments, neighboring tokens — to separate a live credential from a test fixture. Snyk Secrets combines high-entropy analysis, regex, and ML semantic scoring, and is extendable with custom regex for proprietary secret formats.



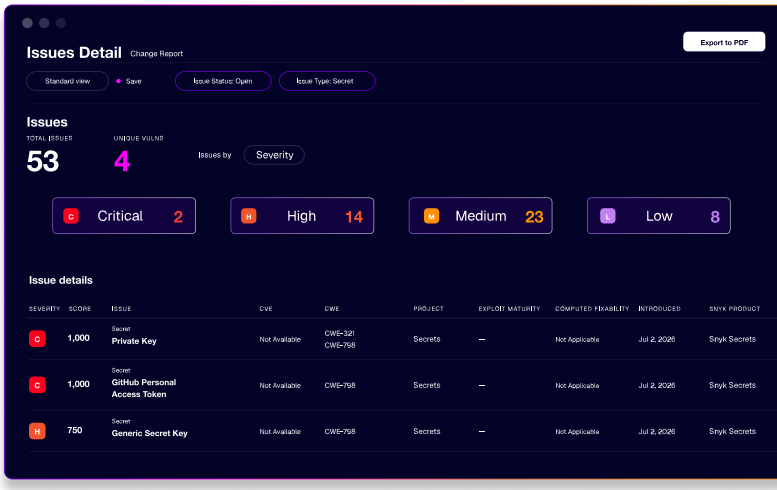


Prevention across the SDLC

Snyk Secrets hooks into agentic workflows to prevent hardcoded secrets from being committed. Real-time IDE feedback flags a secret the moment it's written, PR checks gate merges to protected branches, and scheduled CI/CD and SCM scanning across GitHub, Bitbucket, and Azure Repos catches anything that slips through.

Unified governance across the AppSec program

Unified reporting tracks detection and remediation trends (MTTR) across every repo. Snyk Consistent Ignores centralizes false-positive triage instead of handling it repo by repo. Findings sit alongside Snyk Code, Open Source, Container, and IaC in one interface.



Stop the sprawl before it starts

See how Snyk Secrets blocks hardcoded credentials before they reach production — without slowing developers down.

BOOK A LIVE DEMO

snyk