

Advanced Secrets Detection

Protect Your Codebase with Qwiet AI's
Advanced Secrets Detection



Sensitive information such as API keys, authentication tokens, and private encryption keys can be exposed in modern development environments, creating significant security risks. Qwiet AI's advanced Secrets Detection proactively identifies and mitigates these risks, effectively securing your applications.

Advanced Secrets Detection

- Leverages Qwiet AI's patented Code Property Graph (CPG) and proprietary AI/ML models.
- Qwiet AI's Secrets Detection swiftly and accurately identifies exposed secrets, surpassing traditional pattern-matching techniques with its advanced capabilities.

Integrated Security Platform

- Combines Secrets Detection with Static Application Security Testing (SAST)
- Comprehensive security assessment with a single, efficient scan.

Developer-Friendly Workflow Integration

- Rapid scans averaging around 90 seconds, directly integrating into your existing CI/CD pipelines, ensuring efficient management of security risks without disrupting your workflow.
- Minimizes workflow disruption, significantly reducing false positives and enabling developers to focus on genuine security issues.

Educational Insights

- Provides detailed insights and context around identified risks, enhances developer awareness, and promotes proactive risk management practices.

Integrating **Qwiet AI's Secrets Detection** into your security strategy safeguards your development lifecycle and promotes a proactive security culture within your team. Explore our [Secrets Detection Platform](#) or [review our comprehensive guide on mitigating exposure risks](#) for detailed insights.

Benefits

Strengthened Security Posture

Proactively identifies and mitigates vulnerabilities to prevent data breaches and leaks.

Increased Productivity

Enables developers to address real vulnerabilities without unnecessary distractions efficiently.

Continuous Protection

Provides ongoing scanning and security assessments, ensuring sustained codebase security.

