Qwiet AI vs. Legacy AppSec Tools: A Head-to-Head Evaluation

How a Fortune 100 technology company saved over 9,600 developer hours

qwiet AI

Table of Contents

Overview

A Fortune 100 technology company recently conducted a comparative analysis of Qwiet AI's preZero platform and its legacy application security solution. The internal legacy tool was evaluated against Qwiet AI using 10 real-world production applications that varied in size and programming language.

The results were definitive. Qwiet AI delivered:

- **10x** faster scan times
- Over **70 percentage points** fewer false positives
- **Thousands** of developer hours saved
- **More** actionable, **prioritized** vulnerabilities
- **Faster remediation** through AI-powered Autofix
- **Easier** user experience for newly onboarded engineers and developers

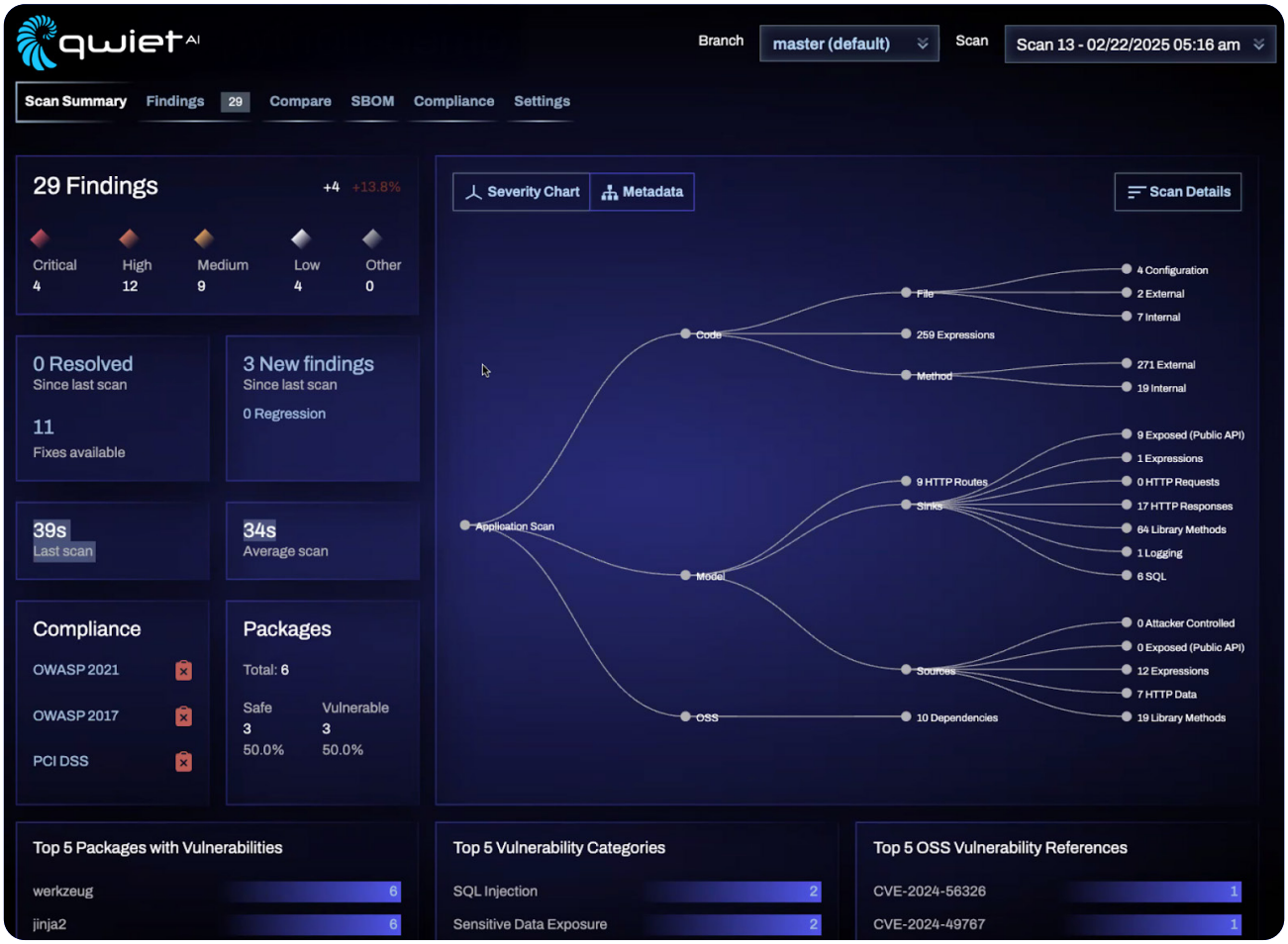
Qwiet AI's patented **Code Property Graph (CPG)** analysis proved critical in surfacing only reachable, exploitable risks, while AI Autofix helped developers resolve them faster and with greater confidence.

Understanding “Legacy” AppSec Tools

At Qwiet AI, we define “legacy” AppSec tools as earlier-generation solutions that lack deep insight into how applications truly function. These platforms typically suffer from:

- **Fragmented scanning** based on code blocks instead of full context
- **Multiple scan passes** are needed to achieve full SAST, SCA, and secret detection.
- **Frequent false positives**, often over 70%
- **Performance degradation** due to bolt-on acquisitions and outdated architecture
- **Surface-level AI integrations** limited to dashboards or queries

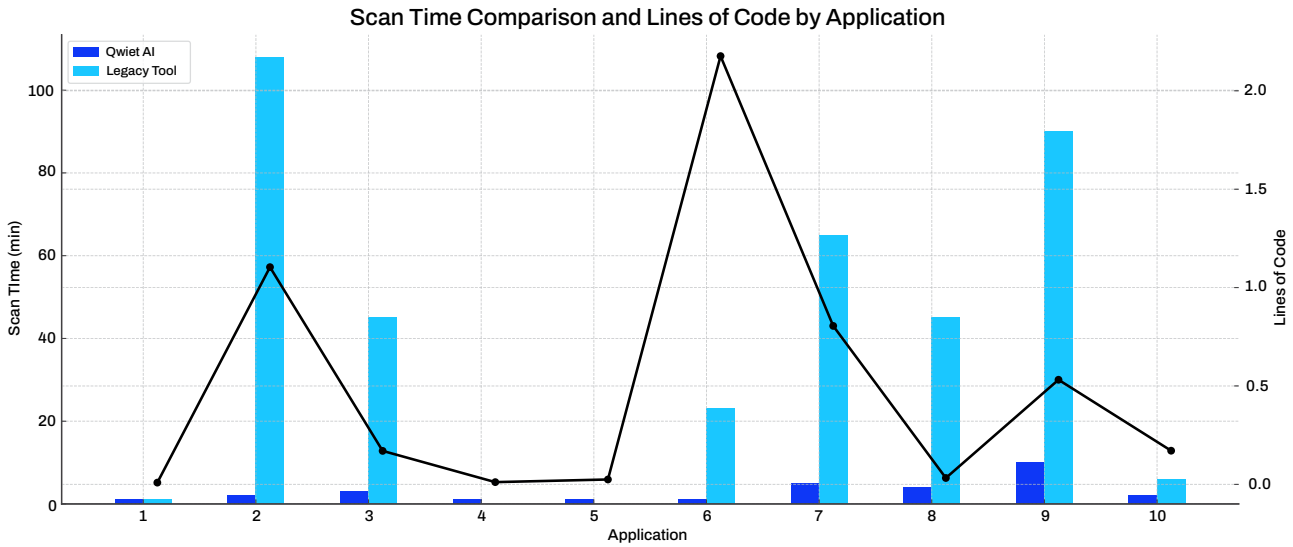
In contrast, Qwiet AI’s modern scanning engine leverages **graph-based analysis with our Code Property Graph (CPG)** to evaluate fundamental data and control flow, dramatically improving accuracy, speed, and prioritization.



The Evaluation

The customer selected 10 production applications to serve as a representative cross-section of their portfolio. Together, these apps totaled nearly 5 million lines of code. The goal is to assess scanning speed, detection accuracy, and real-world remediation burden with Qwiet AI versus their incumbent solution. Neither tool was subject to tuning or policy customization to maintain impartiality.

Scan Times



Total Lines of Code: 4,968,150

Average Qwiet AI Scan Time: 4 minutes

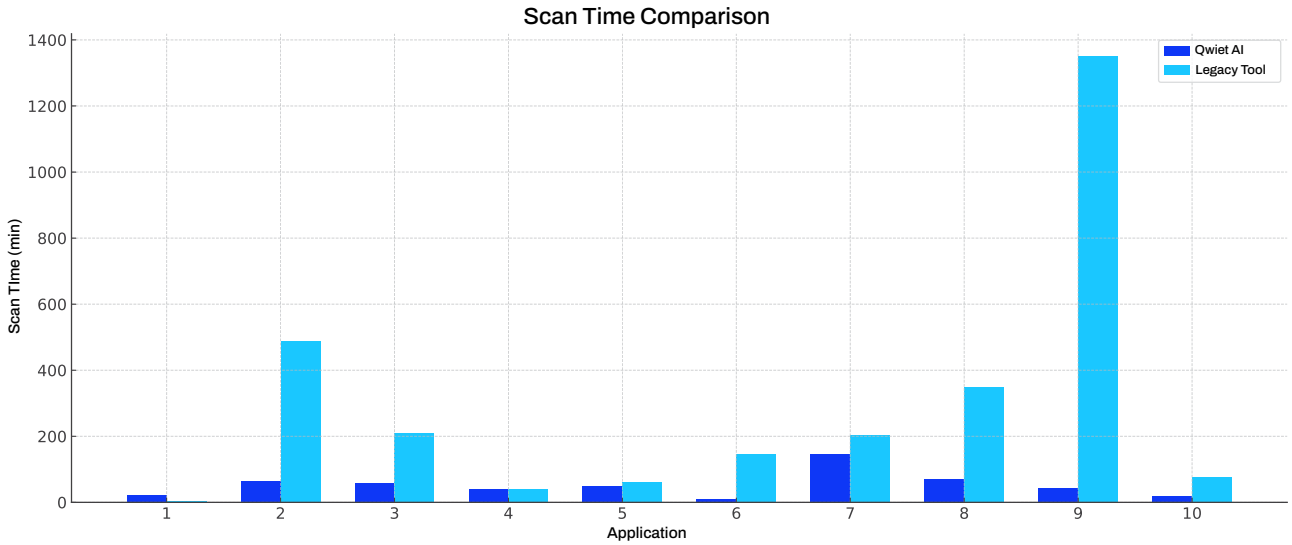
Average Legacy Tool Scan Time: 48 minutes

Industry benchmarks show that legacy static analysis tools frequently require **30 to 90+ minutes** per scan. Qwiet AI completed scans more than **10x faster** without tuning or queuing.

5M+ Lines of Code Tested

10x Faster Scans

Findings and Detection Volume

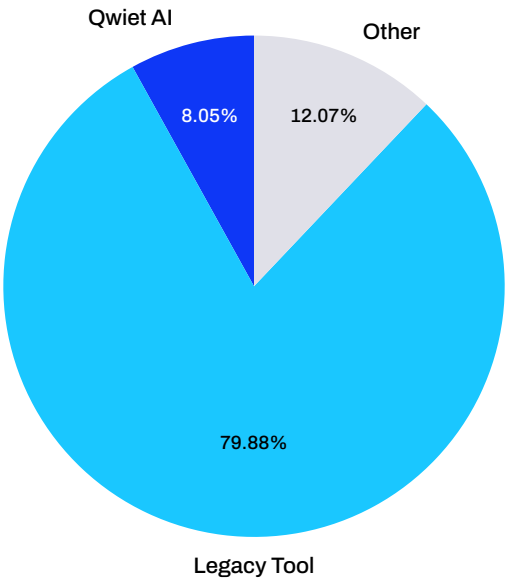


Total Findings

Qwiet AI: 522 | **Legacy Tool:** 2,928

Legacy tools often surface large volumes of low-confidence or unreachable vulnerabilities. Qwiet AI's reachability analysis reduced detection noise by more than **80%**, allowing developers to focus on actionable issues.

False Positive Rate Distribution



False Positives

Validated by the customer's security team, Qwiet AI reported fewer false positives than the legacy tool.

False positive rates from traditional tools typically fall between **50–80%**. Qwiet AI's **8%** rate reflects its context-aware analysis, eliminating unnecessary triage cycles.

92% Fewer False Positives

Remediation Speed with AI Autofix

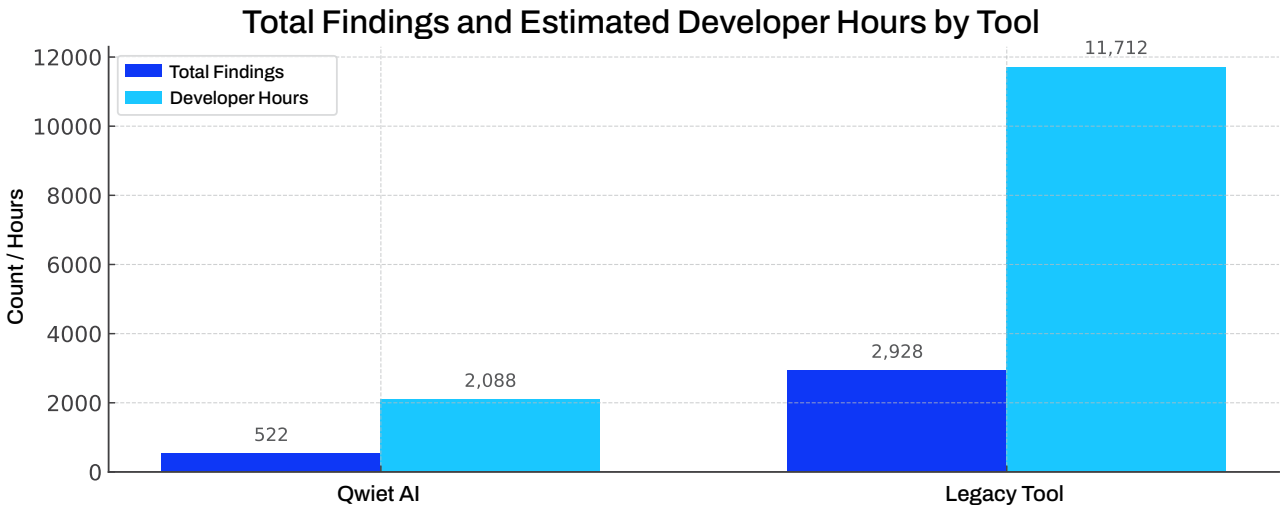
Finding vulnerabilities is only part of the equation. Resolving them without slowing development is where Qwiet AI's **AI Autofix** significantly impacts. Qwiet AI generates **context-aware fix suggestions** based on full data flow, control flow, and syntax. Autofix recommendations are offered directly in the developer's IDE, reducing handoff time and eliminating guesswork. Developers reported that Autofix helped resolve issues significantly faster, with fewer back-and-forth cycles between security and engineering teams.

Key benefits of AI Autofix:

- Code suggestions are **informed by real application flow**, not just templates
- Developers can **apply fixes with confidence**, supported by full trace context
- Manual research and patchwriting time **is significantly decreased**

Developer Productivity Impact

The customer estimated that each true or false finding requires approximately **4 hours** of developer time to research and resolve.



Total Time Saved with Qwiet AI: 9,624 hours

Equivalent to **5 full-time developers** annually freed from low-value triage and remediation efforts.

Over **9,600** Developer Hours Saved

Conclusion

Fast scans. Accurate results. Actionable fixes. This is what Qwiet AI delivers.

Qwiet AI outperformed the legacy solution in every category:

10x Faster Scan Times

82% Reduction in Findings

Between **$960K–$1.4M** in Estimated Cost Savings*

Over **70%** Reduction in Findings

Thousands of hours saved through focused remediation

AI-powered **Autofix** to close the loop faster

Modern security tools should not just find issues; they should help developers fix them efficiently. Qwiet AI enables AppSec teams to deliver absolute protection without **slowing development** or **burning out engineering resources.**

*Estimated Cost Savings: $960,000 (at $100/hour blended rate) and up to $1.4M (at $150/hour for senior developers in high-cost regions)

Experience the Difference

See how Qwiet AI helps teams find and fix vulnerabilities faster, with fewer false positives and less manual effort.

Request a Demo | Try It Free | Learn More

qwiet AI