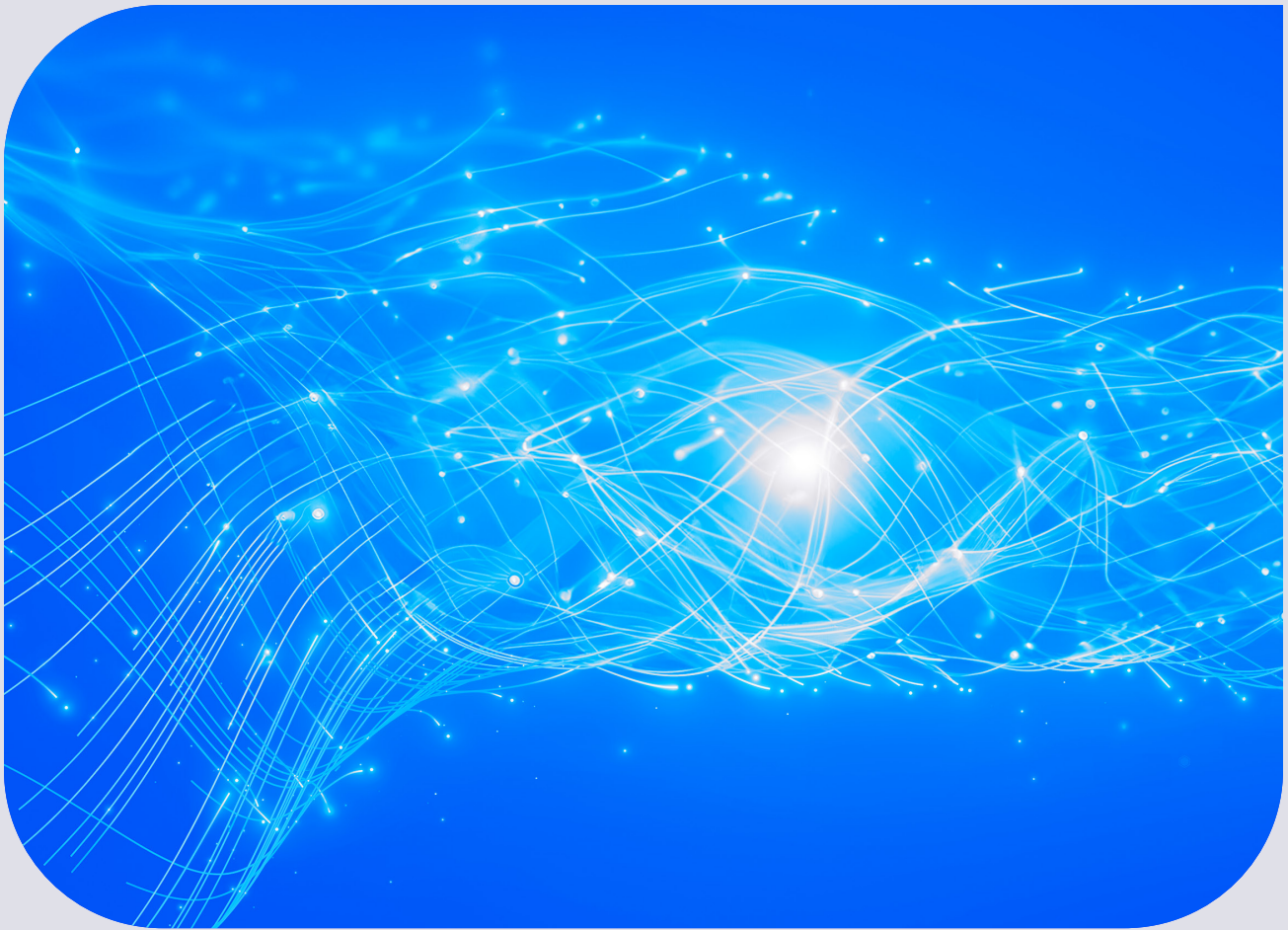


Compliance and Security Benefits

Enterprise Grade Security & Compliance





Enterprise Grade Security & Compliance

ISO 27001 & SOC 2 Certified

Qwiet AI adheres to the highest security and compliance standards, ensuring organizations confidently meet regulatory requirements.

Tenant-Specific Data Security

Your data is kept separate in your tenant and is not used to train models for other customers or shared across environments.

Strict Governance & Audit Controls

Role-based access, encryption, and logging ensure comprehensive security oversight.

AI-Powered Security & Compliance: Faster Scans, Fewer False Positives, Smarter Fixes

Qwiet AI ensures strong security and compliance by leveraging Code Property Graphs (CPGs) and advanced AI models to create a highly secure application security framework.

Agentic AI: Reinforcing Security Guardrails

Qwiet AI's Agentic AI approach is a unique feature that integrates seven specialized security agents as AI Security Code Assistants, embedding security directly into the development lifecycle. This framework automates critical security tasks, streamlines workflows, and enhances collaboration between development and security teams while reducing cognitive load for AppSec professionals.

Key Benefits of Qwiet AI's Agentic AI Approach:

- **Automated Security & Compliance:** The agents provide real-time vulnerability detection, enforce secure coding practices, and ensure compliance with OWASP, NIST, and ISO 27001.
- **Intelligent Threat Prioritization:** AI-driven analysis minimizes false positives, allowing teams to focus on real threats instead of manual triage.
- **Enhanced Developer Productivity:** Qwiet AI's security Code Assistants manage complex security tasks, empowering developers to focus on coding while ensuring security is seamlessly integrated, thereby improving productivity.
- **Contextual Security Insights:** The agents deliver actionable intelligence specific to an organization's risk landscape, improving response times and prioritization.

Qwiet AI enhances overall security efficiency without slowing software development by eliminating manual security processes and reducing unnecessary alerts. Organizations leveraging this approach improve secure software delivery, reduce developer workload, and maintain strong security postures at every stage of development.

Relief from Security Bottlenecks & Compliance Gaps

Traditional security testing tools generate excessive false positives, slow development cycles, and miss complex vulnerabilities. Organizations need a solution that is both precise and efficient without sacrificing compliance. As the only Agentic AI-driven application security platform, Qwiet AI has been AI-first and mathematics-based since its inception in 2017. It addresses these challenges by combining CPG-based security insights with AI-driven automation, ensuring:

- Speed up development by allowing security teams to quickly and accurately find and fix vulnerabilities, reducing time wasted on false alarms.
- Analyzing the entire code structure, control flow, and data dependencies helps to identify and mitigate potential threats before deployment, thereby reducing risk exposure.
- The CPG aligns policy enforcement and actionable compliance reporting with security frameworks such as OWASP, NIST, ISO 27001, and SOC2.



Code Property Graph (CPG) for Security & Compliance

Qwiet AI's platform leverages CPG technology, which stands for Code Property Graph. This technology transforms source code into a graph structure, providing deep insights into code behavior. This approach enables security teams to trace vulnerabilities across multiple code layers, identify exploitable paths, and prioritize high-risk threats more accurately, reducing manual review and remediation time.

- Accelerate secure coding with real-time, AI-driven security insights.
- Enhance developer productivity through automated vulnerability detection, remediation suggestions, and proactive security recommendations.
- Ensure compliance with security standards like OWASP, NIST, ISO 27001, and SOC 2.

By streamlining complex security tasks, Qwiet AI enables developers and security teams to focus on innovation rather than manual security triage. Organizations using this approach have reduced vulnerability remediation time by 40% and significantly decreased manual security efforts, allowing teams to ship secure code faster with fewer disruptions.

CPG vs. Traditional SAST Tools

Qwiet AI's CPG-based approach provides key advantages over traditional Static Application Security Testing (SAST) solutions:

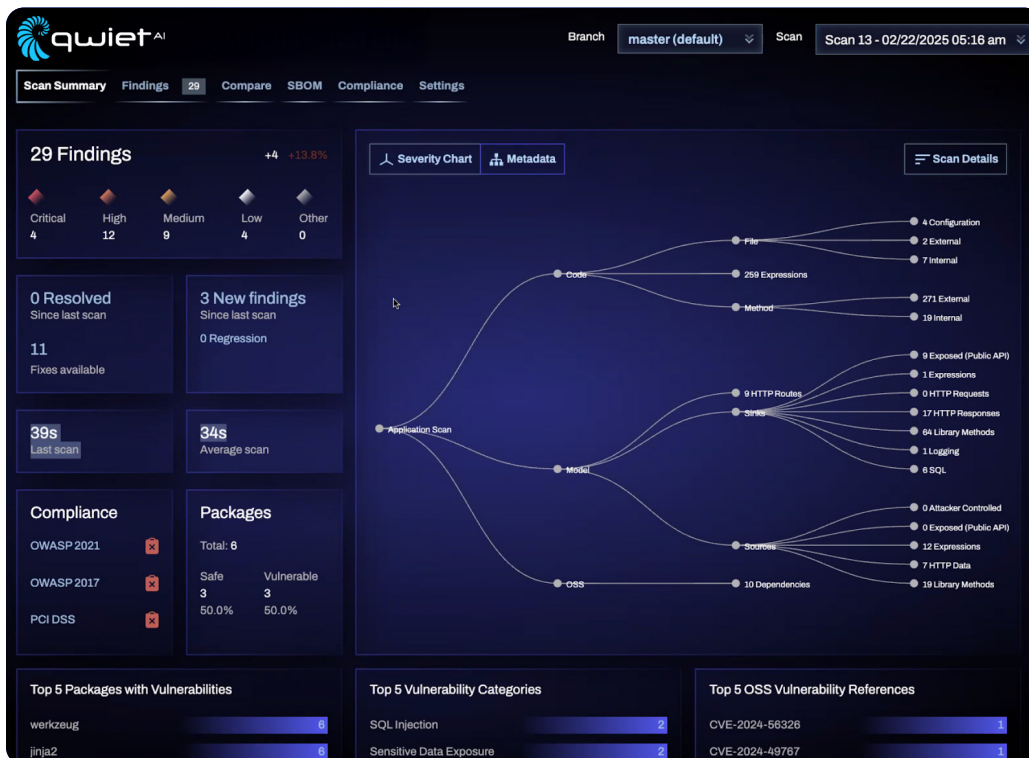
- **Unified Representation:** Combines syntax trees, control-flow graphs, and program dependence graphs into a single structure for deeper security analysis.
- **Enhanced Accuracy:** Reduces false positives by leveraging deep-code context mapping.
- **Scalability & Speed:** Delivers results up to 5x faster than conventional SAST tools.


Qwiet AI's CPG-based approach identifies multi-step exploits, data flow risks, and business logic vulnerabilities often missed by traditional SAST solutions, ensuring comprehensive protection for your organization.

Secure AI Models for Code Analysis

Qwiet AI integrates Large Language Models (LLMs) to enhance security analysis, leveraging their ability to process vast amounts of code, detect patterns, and generate contextual security insights. Using multiple LLMs ensures:

- **Targeted & Explainable Results:** AI-driven recommendations provide traceable, actionable insights.
- **Secure AI Training & Execution:** Enforced data governance with encryption and access controls ensures data security.
- **Minimized False Positives:** Precision-driven AI reduces security report noise, allowing teams to focus on critical issues.



<div>  </div> <div> Severity Select... </div> <div> Status Open x </div> <div> Assigned To Select... </div> <div> Exploitability <input type="checkbox"/> Exploitable <input type="checkbox"/> No Exploits </div> <div> CVSS Score Min: 0, Max: 10 </div> <div> EPSS Score Min: 0, Max: 1 </div>	<div> <input type="checkbox"/> </div>	<div> Finding ID 613 </div>	<div> Status Open </div>	<div> Severity Critical </div>	<div> Unreachable No Exploits </div>	<div> pkg:maven/org.springframework/spring-core@4.3.6.RELEASE </div>	<div> GMS-2022-559 + CVSS 10 + CWE 1035 + CWE 78 + CWE 937 + No Exploits + </div>
	<div> <input type="checkbox"/> </div>	<div> Finding ID 592 </div>	<div> Status Open </div>	<div> Severity Critical </div>	<div> Unreachable No Exploits </div>	<div> pkg:maven/org.springframework/spring-beans@4.3.6.RELEASE </div>	<div> GMS-2022-558 + CVSS 10 + CWE 1035 + CWE 78 + CWE 937 + No Exploits + </div>
	<div> <input type="checkbox"/> </div>	<div> Finding ID 496 </div>	<div> Status Open </div>	<div> Severity Critical </div>	<div> Reachable Exploitable </div>	<div> pkg:maven/org.apache.logging.log4j/log4j-api@2.9.1 </div>	<div> CISA KEV + CVE-2021-44228 + CVSS 10 + CWE 20 + CWE 400 + CWE 502 + CWE 917 + EPSS 0.95 + Exploitable + </div>
	<div> <input type="checkbox"/> </div>	<div> Finding ID 488 </div>	<div> Status Open </div>	<div> Severity Critical </div>	<div> Unreachable Exploitable </div>	<div> pkg:maven/org.apache.logging.log4j/log4j-core@2.9.1 </div>	<div> CISA KEV + CVE-2021-44228 + CVSS 10 + CWE 20 + CWE 400 + CWE 502 + CWE 917 + EPSS 0.95 + Exploitable + </div>

Qwiet AI AutoFix: Agentic AI-Driven Secure Code Remediation

Qwiet AI's AutoFix feature delivers secure, AI-powered code fixes through a multi-agent AI remediation approach, ensuring precise, efficient, and compliant vulnerability resolution with minimal manual intervention. Key capabilities:

- **Context-Aware Remediation:** Code Property Graph (CPG) analysis and Agentic AI reasoning generate fixes that integrate into modern development workflows.
- **Few-Shot Prompting for Precision:** AI-driven fixes leverage real-world vulnerability patterns for accurate and effective patching.
- **Audit-Ready Fixes:** Ensures compliance with OWASP, NIST, and ISO 27001 while maintaining development velocity.
- **Data Security & Compliance:** AutoFix operates within Qwiet AI's virtual private cloud, safeguarding organizational data.
- **Asynchronous Processing:** Prioritizes and suggests fixes for critical vulnerabilities, reducing manual remediation time.
- **Multi-Agent AI Remediation:** Specialized AI agents analyze, generate, validate, and refine fixes, improving accuracy and eliminating redundant security alerts.

By automating remediation with a layered AI approach, Qwiet AI enhances AppSec team productivity, reduces cognitive load, and ensures vulnerabilities are efficiently addressed, allowing developers to code confidently.

See the Difference in Action

Discover how Qwiet AI's Code Property Graph (CPG) technology significantly reduces false positives and enhances scan speeds for AI-powered AutoFix. Learn how our solution can accelerate vulnerability remediation with unmatched accuracy.

Check it out here: [Qwiet AI AutoFix](#)

Request a Demo Today: [Get Started with Qwiet AI](#)

For more details, visit: [Qwiet AI CPG Technology](#)

