AquilaX AI

Application Security Co-Pilot

https://aquilax.ai

Top tier AppSec Engineer

Understands Business Logic

Runs on cloud and on-prem

Runs on CPU and self-learns

Trained on 300M+ Projects

Expertise in 10+ scanning types

Detected 150M+ vulnerabilities

Scans in under 60s

Code is the language of technology, and security is the grammar that ensures it communicates only what you intend

About AquilaX

— — — — — — — —

Established by seasoned professionals formerly with Goldman Sachs, HSBC, and Visa, AquilaX Ltd emerged as an academic endeavor, focused on simplifying Source Code, Infrastructure, and Container Security scanning within the Software Development Life Cycle (SDLC). As a Software as a Service (SaaS) solution, it seamlessly integrates into Git-based pipelines, such as GitHub and GitLab, demanding zero prior knowledge of Application Security, emphasizing accessibility and inclusivity in code security practices.

Scanner
— — — — —

→ **Secret & PII Scanner** – Conduct real-time source code analysis for the identification of API keys, passwords, certificates, encryption keys, and PII.

→ **Static Application Security Testing (SAST)** – Conduct thorough scans on your first-party code to identify vulnerabilities introduced, such as SQL Injection, XSS, and more.

→ **Software Composition Analysis (SCA)** – Dependency scanning on open-source libraries in use, cross-referencing against public and private databases to identify and mitigate known vulnerabilities.

→ **Container & Software Scanning** – Examining Docker images to identify and rectify security vulnerabilities, ensuring robust and secure deployment environments.

→ **Infrastructure as a Code (IaC) Scanning** – Scanning programmatic infrastructure, minimizing human error, ensuring consistency, and enhancing overall security measures in IT resource deployment (in the cloud).

→ **API Security** – Conduct code-based API security testing to continuously identify and assess risks in API services and functionalities over time, tracking risk transitions for enhanced security measures

→ **Backdoor and Malware Identification** – Conduct scans on both first-party and third-party code to pinpoint malicious functionalities, such as malware or backdoors

→ **AI Generated Code** – Scan first party code for identification of source code created by AI models.

GenAI
— — — — —

AquilaX AI models are designed to optimize application security through automation and contextual intelligence. These proprietary models enhance security workflows, reduce false positives, and streamline remediation efforts.

Key Values:
➔ **High Accuracy & Noise Reduction** – AquilaX Securitron leverages AI trained on 300M+ open-source projects to minimize false positives and deliver precise vulnerability detection

➔ **Efficient & Scalable Performance** – Optimized for CPU compatibility and real-time security analysis, ensuring fast execution with minimal resource consumption

➔ **Actionable AI Insights** – Provides automated classification, contextual vulnerability explanations, and remediation recommendations, eliminating the need for manual security triage

AquilaX credo, loud and proud
— — — — —

DevSecOps, as we know it, is about to get bulldozed. Why? Because it's based on rule sets written by humans, for humans, to be reviewed endlessly by humans. Companies like Semgrep, Snyk, and BlackDuck have done a bang-up job, but let's face it—security-by-rules is like using a flip phone in a smartphone era. It's a noble effort, sure, but far from scalable or revolutionary.

Why AquilaX?

— — — — —

Feature	AquilaX AI	Other Vendors
Auto False Positive Removal	*Yes*	No
Security Scanners	*Yes (Full suite – 9 in parallel)*	Limited Capabilities
Review and Triaging	*Yes (Free of charge)*	No (or extra cost)
AI Models	*Yes (Bespoke, pre-trained, and context aware)*	No (or Using public services, or generic models)
Scanning Time	🚀 **83% Faster (under 60sec)**	🐌 Slow & Time-Consuming
Deployment Options	*SaaS, Private Cloud, On-Prem*	Mostly SaaS-Only

Integrations

— — — — — —

Initiating source code scanning with AquilaX is straightforward— an engineer has to just provide permission to AquilaX to access the code, simply as that! No integration, no customization, no security knowledge!

Subsequently, AquilaX clones the code, initiates comprehensive assessment through various scanners using the AquilaX worker, aggregates results, and delivers a consolidated output on the dashboard (we support GitHub, GitLab and BitBucket).
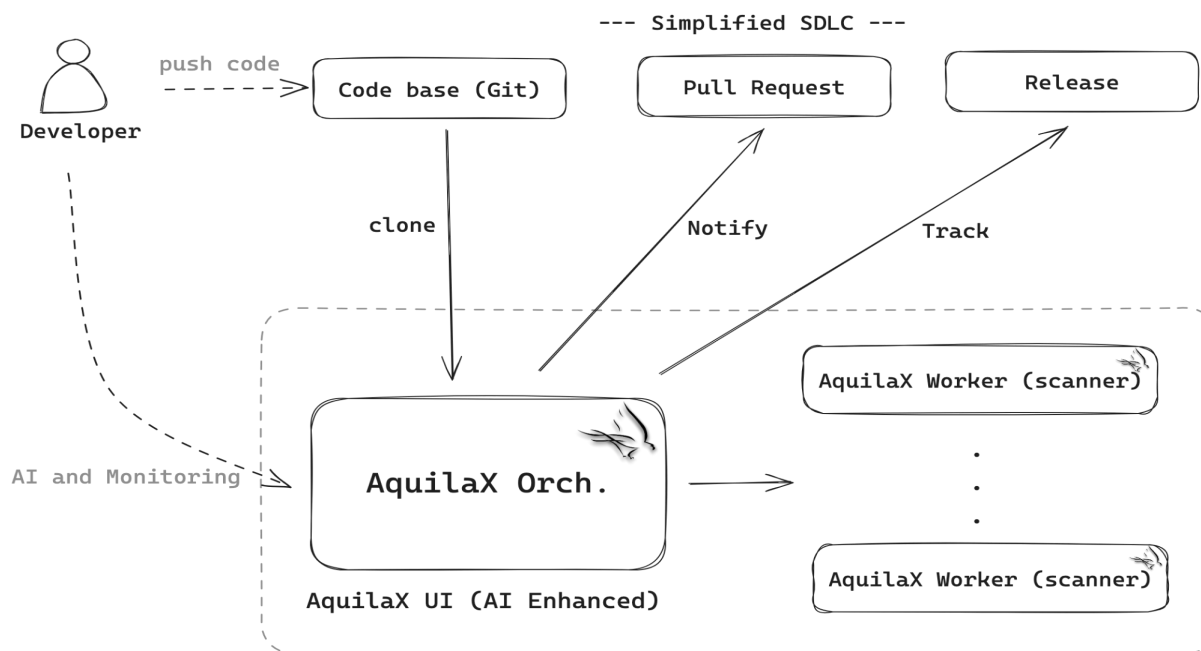
Not Your Average Scanners: AquilaX, Making Security Look Cool!

We harness AI to present results seamlessly, reducing noise, minimizing evidence risk. Our system suggests prioritized vulnerabilities, detailing necessary fixes and estimating the associated remediation costs.

License

— — — — — —

AquilaX operates on a user-based subscription model, with select scanning functionalities offered for free. This approach aims to foster a thriving community by encouraging more engineers to join our security initiatives.

Price list per developer

Free	Premium	Ultimate
$0/m	$19/m	$59/m
☑ **Secret Scanner** ☑ **PII Scanner** ☐ IaC Scanning ☐ SAST ☐ SCA ☐ Container Scanning ☐ API Security ☑ **Monitoring** ☐ AI Integration ☐ Backdoor Scan ☐ Fix Feeds	☑ **Secret Scanner** ☑ **PII Scanner** ☑ **IaC Scanning** ☑ **SAST** ☑ **SCA** ☑ **Container Scanning** ☐ API Security ☑ **Monitoring** ☐ AI Integration ☐ Backdoor Scan ☐ Fix Feeds	☑ **Secret Scanner** ☑ **PII Scanner** ☑ **IaC Scanning** ☑ **SAST** ☑ **SCA** ☑ **Container Scanning** ☑ **API Security** ☑ **Monitoring** ☑ **AI Integration** ☑ **Backdoor Scan** ☑ **Fix Feeds**

All our services include comprehensive online documentation, technical support, and access to on-call security experts for an added layer of assistance and guidance.

For on-premises installations of the AquilaX engine, an additional one-time cost is applied. This covers expenses associated with the Engineering team's support for the on-prem installation and ensures meticulous monitoring of the system's correct functionality.