SOLUTION BRIEF

Software Supply Chain Security with the Aqua Platform

Key Benefits

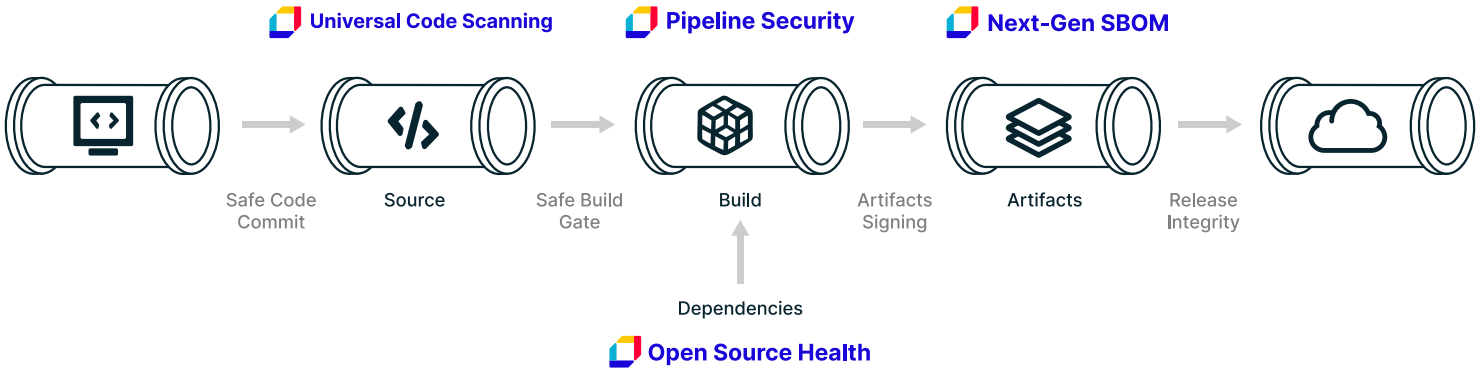
- **Secure your code**
  Integrate security scanning into application lifecycle and dev workflow to maintain development velocity.
- **Empower teams to take security ownership**
  Save time for DevSecOps and application security teams by eliminating benign issues or false positives.
- **Fix vulnerabilities quickly**
  create a pull request to fix a vulnerability quickly and reduce MTTR with one simple click, eliminating the multiple steps required to connect the vulnerability to a fix.
- **Gauge risk and open source health quickly**
  Track the security and maintenance of open source packages across ecosystems.
- **Secure the tool chain**
  Scan for vulnerabilities and license issues on every build and establish a zero-trust environment.
- **Risk prevention**
  Prevent the affected code from progressing through your development pipelines by applying robust assurance policies.
- **Gain visibility into 3rd party components and track dependencies**
  Automate SBOM creation for every release and utilize direct and transitive dependency mapping.

A single breach in the software supply chain can have far-reaching consequences, impacting not only the targeted organization but also countless downstream entities. An alarming 82% of CIOs admit to feeling unprepared to face software supply chain threats. Recent threat research conducted by Aqua's Team Nautilus reveals a staggering 300% increase in attacks targeting software supply chains.

The attack pane is affected directly from the risks introduced in the code like misconfigurations, vulnerable dependencies, and secrets. Risk at any stage of the application lifecycle—code, build, deploy, and run—can result in the weaponization of the application by hackers. Aqua provides full, real-time dependency analysis that gives you full visibility so that you can detect a zero-day supply chain attack as soon as it is discovered.

Aqua's Software Supply Chain Security solution is designed to safeguard against potential attacks by fortifying all four layers of the software supply chain: code, infrastructure, development environments and CI/CD pipelines. Aqua's code to cloud approach prevents known vulnerabilities and risks from being introduced during development and enables rapid response when zero-day risk arises. With Aqua, development teams automate the monitoring and tracking of component changes. The Aqua platform traces risk back to the specific code and developer responsible for enhanced accountability and remediation.

CI/CD Posture Management



Securing your software supply chain from day one

Acting earlier in the SDLC is associated with lower costs to fix and allows for a shorter feedback loop for developers. The Aqua Software Supply Chain Security solution, part of the Aqua Cloud Native Application Protection Platform (CNAPP), integrates with your build environment in minutes and allows you to scan code at the point of commit to a repository when the author of the affected software is known and can be traced back easily. With Aqua, security can become an integral part of the development life cycle itself from the very start.

Key Features

Pipeline Visibility

Get full visibility and control across all CI/CD pipelines so you can easily secure thousands of release tracks that lead directly to your production environment (GitHub Actions, Bitbucket Pipeline, GitLab CI, Jenkins, CircleCI, etc.) Ensure proper configurations and continuously monitor pipeline behavior.

SAST (Static Application Security Testing)

Analyze source code to find security risks that make you organization's applications susceptible to attack. SAST availability is based on industry standards set by OWASP and NIST.

CI/CD Posture Management

Easily spot and fix dangerous misconfigurations of your DevOps platform (e.g., GitHub, Jenkins, and Nexus) and establish a zero-trust DevOps environment.

Open source license detection

Identify and analyze licenses associated with open source software. Support proper usage and deployment of open source code repositories and license agreements.

Best in class SCA (Software Composition Analysis)

Manage and scan any open source component used in your application with Software Composition Analysis (SCA) to detect vulnerabilities. Aqua Trivy is the industry-leading cloud native scanner that supports dozens of coding languages.

LLM (Large Language Model) code security

Implement protective measures to address potential risks and challenges associated with advanced natural language processing models, both public and custom and data sets. Gain comprehensive protection from code to cloud using the OWASP Top 10 recommendations.

Open-Source Health

Explore and analyze open source dependencies used by your organization. Set and enforce company-wide quality controls ensuring that any newly added open source code meets the approved standards.

Policies enforcing custom code hygiene at build time

Maintain clean, well-structured, and optimized code in software development. Ensure that custom code meets certain standards and best practices, while preventing new risks from being introduced to the customer environment.

Intelligent SBOM

Go beyond basic SBOM generation and record every step and action from the moment a developer has committed code, through the build process up until the new final artifact is generated.

Aqua Security sees and stops attacks across the entire cloud native application lifecycle in a single, integrated Cloud Native Application Protection Platform (CNAPP). From software supply chain security for developers to cloud security and runtime protection for security teams, Aqua helps customers reduce risk while building the future of their businesses. Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL protecting over 500 of the world's largest enterprises.
For more information, visit https://www.aquasec.com

Schedule demo ›