Solution Brief

Software Supply Chain Security with the Aqua Platform

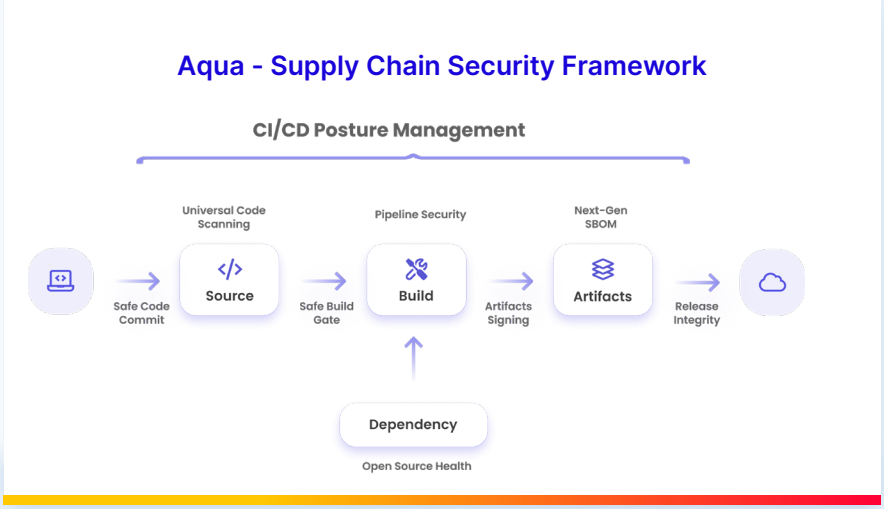
Software Supply Chain risks permeate the application lifecycle and target not just code but also the tool chain itself. That's why the Aqua Software Supply Chain Security solution secures your code, development infrastructure, and pipeline processes so that you can protect your bottom line and safely deliver innovation faster.

The solution prevents successful attacks by helping you fix vulnerabilities and other issues as early as possible in your Software Development Lifecycle (SDLC). It also identifies dangerous misconfigurations in your build tools that could leave the door open to attackers. Then, it helps you establish code integrity and release gates to prevent code manipulation or injection attempts and enable signed, compliant deployments.

The Aqua Software Supply Chain solution is a fully-integrated part of the Aqua Cloud Native Security Platform. It covers all critical software supply chain attack vectors in a single solution for the best visibility and control across your entire SDLC.

Key Benefits

- Comprehensive coverage in one solution across all critical software supply chain attack vectors
- Protects revenue at risk by ensuring only secure and attested artifacts are deployed to production
- Increases productivity by centralizing application security and orchestration and integrating into developer and DevOps workflows
- Reduces the cost of remediation by shortening development feedback loops and integrating vulnerability management
- Deploys in minutes and begins reducing top risks from day one



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 Security Platform, 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. The solution's assurance policies can prevent the affected code from progressing through your development pipelines until it is remediated. With Aqua, security can become an integral part of the development life cycle itself from the very start.

Key Features

Universal Code Scanning

Automate security scanning into your build pipeline to detect vulnerabilities in third-party components (SCA, software composition analysis) and your own code (SAST, static application security testing), open source license issues, infrastructure as code (IaC) misconfigurations, secrets, malware, and more. Periodic scans keep you alerted to new risks as your code changes.

In-Workflow Alerts

Aqua analyzes your code and notifies you wherever the code is: as an alert in your Integrated Developer Environment (IDE), as a comment on your pull request in your Source Code Management (SCM) platform, and as an alert (or build failure notification) in your CI pipeline before release.

Next-Gen 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. With code signing, users can also verify the code history and gain certainty that the code they create is the same code that ends up in the development tool chain.

Pipeline Security

Aqua lets you gain full visibility across all CI pipelines in your organization. Easily navigate thousands of release tracks that lead directly to your production environment.

Apply Static Pipeline Analysis to break down each pipeline (e.g. GitHub Actions, Bitbucket Pipeline, GitLab CI, Jenkins, CircleCI, and more) into its most basic instruction to determine which ones are improperly set up and could put your artifacts at risk.

Simple Deployment and Configuration

SaaS makes deployment of the Aqua Software Supply Chain solution simple. Configuration is also easy; just connect to your SCM and CI/CD tools using their Application Programming Interface (API) keys and initiate a scan to discover all of the assets in your account and begin assessment for risks. For on-premise tools a broker is available to scan assets locally.

Open-Source Health

Explore and analyze open-source dependencies used by your organization. Aqua grades every open-source package used based on: quality, maintainability, popularity, and risk. It then notifies developers of potentially dangerous packages at the moment they introduce them. You can set and enforce a company-wide level of quality that must be met before adding new open-source code to your codebase.

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.

Aqua enforces Least Privilege Access, so you can easily audit privileges across your SDLC, and detect which users have access to code repositories, CI pipelines, or Artifact registries. Then enforce least privilege policies and implement separation of duties to reduce security risks and meet compliance requirements.

Connect Code to Runtime with Unified Cloud Native Security

Software Supply Chain Security is a key component of the Aqua Platform, the most integrated Cloud Native Application Protection Platform (CNAPP). It allows you to realize proactive security across the entire software development life cycle (SDLC) including code, build, deploy, and run phases. For attacks that are discovered in runtime, use the platform to identify what components are affected—down to the line of code where the issue exists—making remediation faster and more precise than ever.

Integrity scanning

Prevent sophisticated software supply chain attacks such as SolarWinds and Codecov by scanning your build pipeline for anomalous behavior and malicious activity with eBPF-based technology. Detect any drifts from the known good baseline like unexpected file modification or establishing communication with a suspicious URL.

Aqua Security stops cloud native attacks, preventing them before they happen and stopping them when they happen. With Aqua, DevOps and Security teams prioritize risk in minutes across the entire development lifecycle while automating prevention to secure their cloud native applications on day one. Real cloud native attacks are stopped immediately without killing workloads. With a platform built on the most loved open source cloud native community and innovation from dedicated threat research, Aqua is a complete solution to cloud native security for transformational teams. Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL with Fortune 1000 customers in over 40 countries.

Schedule demo ›