Securing the Software Supply Chain

Argon, Part of the Aqua Security Platform

Argon software-as-a-service extends the Aqua Cloud Native Application Protection Platform (CNAPP) and helps you maintain development velocity while building and running more secure and reliable code. Connect Argon to your development environments and tools to detect and identify risks earlier throughout the SDLC and eliminate risks that could lead to successful supply chain attacks. With Argon, you get a security blueprint that translates industry guidelines and best practices into a pragmatic security enforcement plan, paired with the tools necessary to automate compliance.

Core Capabilities

- Scan artifacts and dependencies to identify security risks, vulnerabilities and malware.
- Enforce security and DevOps policies with real-time alerts, automated remediation, and prevention of vulnerable or malicious code from advancing to production.
- End-to-end visibility across the software supply chain that allows your security and DevOps teams to identify issues and receive actionable information regarding their CI/CD pipeline.

What Makes Argon Different

- Go beyond enforcing quality and security standards for each release and protect both the DevOps processes and the tools against system vulnerabilities, misconfigurations, data theft, tampering, and unauthorized changes.
- Perform automated integrity checks against a software bill of materials to ensure that the code you commit is the code you deploy.
- Leverage the world's most popular open source vulnerability scanner, Aqua Trivy, with more than ten thousand stars on GitHub (roadmap capability).

aqua

What Aqua and Argon Means for You

Together, Argon and Aqua form the strongest solution for supply chain security, enabling you to secure every aspect of your software lifecycle from development, to test, to production. Automate the protection of the CI/CD pipeline across artifacts, infrastructure, and processes to ensure that security gates are implemented and maintained.

- Automate Aqua Dynamic Threat Analysis (DTA) in the CI/CD pipeline to detect malicious or anomalous activity that evades static scanning and only manifests at runtime—from a secure sandbox environment—and block malicious artifacts from being deployed to production.
- Detect anomalies from unknown threats with runtime protection and implement better security controls in the pipeline using consistent behavioral indicators identified by Aqua's dedicated threat research team, Team Nautilus.
- Establish a single source of truth for security in CI/CD pipelines and centralize assurance policies across Argon and Aqua to determine image compliance (roadmap capability).

Go Cloud Native with the Experts!

Get a Demo >

aqua

aquasec.com

contact@aquasec.com

@Aqua Security

@AquaSecTeam

in/Aqua Security

@AquaSecTeam