SOLUTION BRIEF

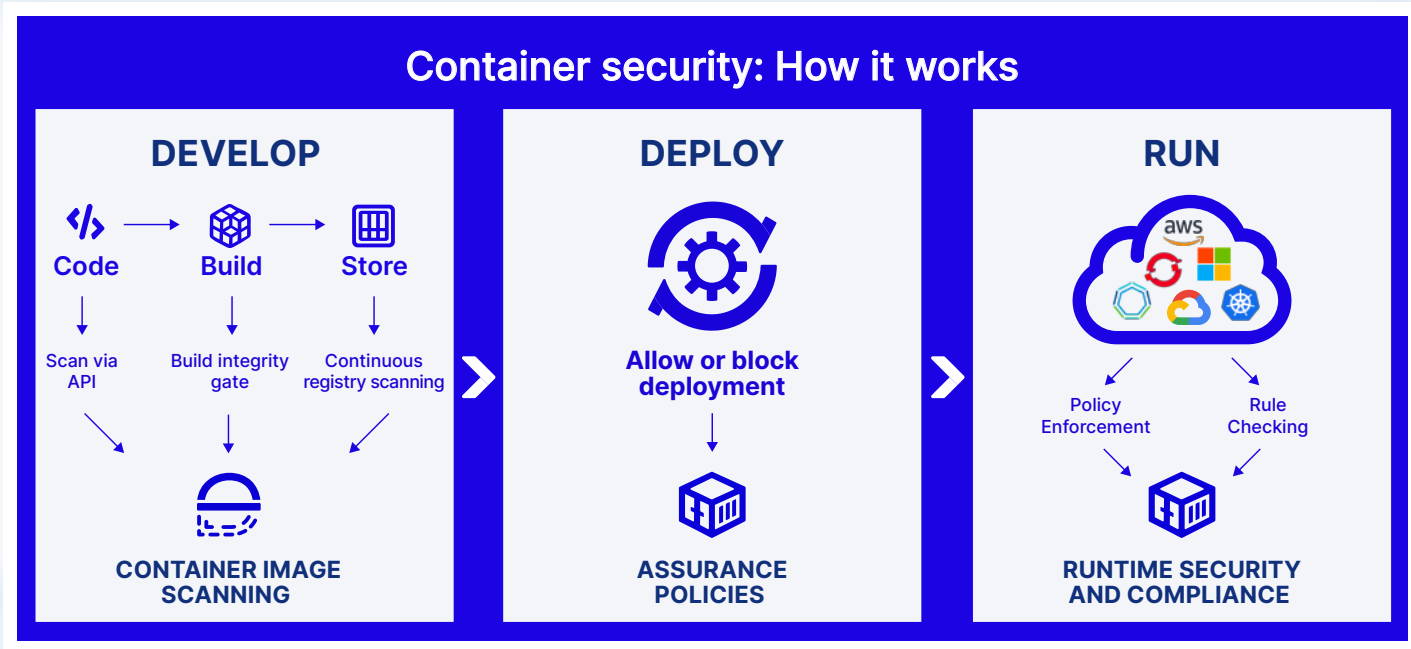
Automate container security across the full application life cycle

Containers represent a dramatic shift in software development, creating a new attack surface and introducing unique security challenges. The ephemeral and elastic nature of containers, the distributed network and the complex architecture of container-based applications that run in dynamic multi-cloud and hybrid environments require a different kind of protection than traditional VMs.

Effective container security relies on deploying automated controls throughout the entire software development life cycle (SDLC), unifying teams across development and security. Starting in the early stages of development, a comprehensive approach involves rigorous image scanning to prevent as many known risks as possible. This process seamlessly extends through assurance gates, allowing only scanned and approved artifacts to proceed to deployment. The life cycle culminates in active runtime controls to block any malicious activity while ensuring robust protection of the workload.

Key Benefits

- Detect and remediate risks early without slowing down development
- Automate regular security scanning across the SDLC
- Ensure container integrity across the full life cycle
- Continuously track and monitor container behavior at runtime
- Detect and stop attacks in progress
- Secure your hybrid and multi-cloud environments with a single policy engine



Find and remediate risks early in the SDLC

Enhance container security and minimize vulnerabilities by integrating automated image scanning into your DevOps pipeline. This enables quick identification and prioritization of critical security risks before deployment, saving time and resources by reducing the need for manual security checks and allowing teams to focus on development.

Accurately detect risks

Comprehensively scan container images for known vulnerabilities, hidden malware, embedded secrets, open source license issues, configuration issues, and more with a premium version of the award-winning cloud native security scanner Aqua Trivy.

Uncover sophisticated malware

Discover hidden malware by running a container image in an isolated sandbox to check its runtime behavior before it goes to production. Aqua DTA (Dynamic Threat Analysis) monitors behavioral patterns and detects multiple indicators of compromise (IOCs), such as container escapes, malware, cryptominers, code injection backdoors, network anomalies, and more.

Prioritize issues efficiently

Automatically generate a prioritized list of vulnerabilities based on various risk-based contextual factors such as exploitability, severity, and whether the workloads are running, helping to clearly prioritize vulnerabilities for remediation.

Consolidate scanning tools

Streamline security and risk management by leveraging Trivy across all application life-cycle stages. This unified approach boosts scanning accuracy and consistency, replaces multiple tools with one, and facilitates early issue detection and resolution, empowering your organization to scale efficiently in the cloud.

Run only trusted images with assurance policies

Ensure a secure and compliant production environment by enforcing guardrails that permit only container images that meet all security and compliance standards to pass through. DevSecOps teams can tailor assurance policies with flexible rules to define specific risk thresholds, catering to the unique needs of various pipelines and environments.

Establish acceptance gates

Prevent unapproved container deployments and mitigate operational errors, image sprawl, and rogue deployments with Aqua assurance policies, which set clear tolerance levels for your environment's security posture.

Control your risk tolerance

Speed up your DevOps processes and manage risk effectively by setting the level of accepted risk and having multiple policies for different circumstances and different requirements.

Tailor policies and rules

Set up highly flexible assurance policies based on the security needs of different applications or pipelines. The rules can apply to various factors, such as risk score, vulnerability severity, root privileges, embedded secrets, malware, and more.

Improve collaboration across teams

Streamline communication of security requirements between development and security teams, ensuring alignment on risk thresholds and action plans.

Detect and stop container attacks in real time

Gain complete workload visibility and enforce robust runtime policies across hybrid and multi-cloud environments. Instantly detect and address threats in real time without disrupting containers in production, enhancing security, maintaining operational efficiency, and avoiding costly downtimes to preserve customer trust.

Protect workloads faster

Quickly protect runtime workloads with user-friendly, out-of-the-box protection against advanced threats, eliminating the need for specialized cloud native expertise.

Protect against the unknown

Discover emerging and zero-day threats with Aqua's advanced kernel-level behavioral detection, which uses real-world indicators and in-depth research from Aqua Nautilus threat research team for highly accurate cloud native threat detection.

Optimize application stability and security

Improve application stability and performance with eBPF technology for less intrusive, lightweight security, enhancing user experience and efficiency.

Define once and run anywhere

Establish a universal set of granular runtime security rules to save time and ensure consistency across hybrid and multi-cloud environments, enhancing your overall security posture and reducing the risk of threats due to inconsistent enforcement.

Ensure consistent visibility and enforcement

Achieve consistent, granular control over container environments, ensuring that security policies are applied uniformly and reducing vulnerability risks.

Stop malware

Enhance your cybersecurity by automatically alerting, blocking, or deleting advanced malware upon download or execution. This comprehensive detection approach catches elusive threats and ensures protection against fileless and in-memory attacks.

Detect and stop zero-day attacks

Secure cloud workloads from known and emerging threats with patented drift prevention, automatically blocking unauthorized internal movements or privilege escalation, stopping zero-days.

Investigate incidents

Collect comprehensive forensics data at the kernel level, providing detailed incident timelines and supporting integration with SIEM, analytics, or monitoring tools for enhanced visibility and analysis.

Aqua CNAPP: Leading platform for container security

As the pioneer and recognized leader in container security, Aqua provides complete end-to-end protection for your container workloads, regardless of where they are deployed. We help you shift left to comprehensively scan your container images in the build, empowering your developers to fix risks early on where it costs less. With key acceptance gates set up in the CI/CD pipeline, reduce the attack surface before deployment by allowing only authorized images to run. In production, ensure real-time protection of your container workloads, prevent drift, detect malware, and stop known and sophisticated zero-day attacks as they happen.

Aqua Security sees and stops attacks across the entire cloud native application lifecycle in a single, integrated platform. 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.
The Aqua Platform is the industry's most comprehensive Cloud Native Application Protection Platform (CNAPP).
Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL with Fortune 1000 customers in over 40 countries.
For more information, visit https://www.aquasec.com

Schedule a demo ›