SOLUTION BRIEF

Aqua Platform
Accelerate Your Digital Transformation with Trusted Cloud Native Security

Key Benefits

- Reduce risks and minimize the attack surface of container-based applications.
- Secure running applications and instantly detect, stop, and respond to attacks.
- Manage vulnerabilities at scale by detecting, prioritizing, and fixing CVEs from code to cloud.
- Accelerate DevSecOps and automate container security across the full application life cycle.
- Prove and report compliance with confidence.

Unleash the full power of cloud native technologies to drive innovation securely and boost business growth.

As businesses embrace digital transformation and move to the cloud, the need to rapidly build and release new services to meet customer needs has never been more critical. Success in today's competitive landscape requires not only a fast time to market but also the confidence that your applications are secure.

However, traditional security approaches fall short in the new dynamic and complex cloud native environments. Organizations face an overwhelming volume of vulnerabilities without any context, forcing teams to waste time chasing endless alerts and investigating false positives. The reliance on multiple siloed tools leads to gaps and inefficiencies, while the disconnect between development and security teams creates frustration and further slows innovation.

The modern cloud and DevOps-driven world demands that security becomes part of the development life cycle, enabling businesses to move fast, innovate, and maintain a competitive edge.

The Aqua Cloud Native Application Protection Platform (CNAPP) enables organizations to fully realize the benefits of cloud native technologies by securing containers, Kubernetes, VMs, and serverless functions throughout the entire life cycle. By embedding security into every stage of development, deployment, and operations, Aqua empowers businesses to build faster, enhance customer experiences, and confidently deliver new digital services. With Aqua, organizations can seamlessly implement DevSecOps practices, overcome operational challenges, and minimize security risks while accelerating their digital transformation journey.

Reduce the Attack Surface

Efficiently manage and reduce security risk in cloud native environments with comprehensive end-to-end visibility throughout the entire application life cycle.

Unify security scanning

Automate scanning into your build pipeline to detect vulnerabilities in third-party components and your own code, open source license issues, infrastructure as code (IaC) misconfigurations, secrets, malware, and more using Trivy, a universal and comprehensive security scanner for containers and other artifacts.

Secure your CI/CD toolchain

Harden your CI/CD pipeline, including all development infrastructure and tools, by quickly identifying and fixing misconfigurations in various DevOps platforms such as GitHub, GitLab, and Jenkins to mitigate supply chain risks.

Set deployment gates

Ensure that the images you deploy are trusted and have passed all security checks before deployment. Prevent critical issues from reaching production while establishing and maintaining a secure runtime environment without slowing development.

Quickly assess risk posture

Gain visibility across all your environments, discover all your cloud resources, and accurately identify risks quickly and reliably.

Manage Vulnerabilities at Scale

Dramatically cut the number of CVEs, accelerate mean time to resolution, and minimize your overall risk profile using code-to-cloud vulnerability management.

Reduce vulnerability noise

Automatically filter thousands or tens of thousands of CVEs to determine top-priority issues that pose the greatest risk and require action. Track vulnerabilities from development to production, leveraging runtime insights for efficient prioritization and remediation.

Prioritize CVEs efficiently

Focus on the vulnerabilities that are actually exploitable, clearly prioritizing them for smarter remediation based on a unique mix of contextual insights, such as reachability, Exploit Prediction Scoring System (EPSS) score, actively running packages, available exploits, and more.

Report on vulnerabilities at enterprise scale

Track key vulnerability metrics and remediation efforts and communicate them to stakeholders to ensure that vulnerabilities are tracked, mitigated, and reported in line with regulatory obligations.

Speed up remediation with cloud-to-code capabilities

Empower developers to easily trace issues back to the source to find the exact line of code where vulnerabilities originated. Automatically generate a pull request to the responsible owner and use Aqua's AI-guided remediation advice to fix issues quickly.

Mitigate CVEs in runtime

Prevent exploitation of known vulnerabilities that can't be fixed by applying compensating controls in runtime such as virtual patches that provide immediate protection without the need to rebuild the image and with zero downtime.

Accelerate DevSecOps

Enable DevOps speed by embedding comprehensive security scanning and powerful policy-driven controls from the start and across the entire application life cycle.

Enable developers to fix issues fast

Enable developers to adopt a security-first mindset by providing full visibility into where their code runs. Automatically trace issues to the exact code line, generate pull requests, and streamline resolution to save time and effort, ensuring that vulnerabilities don't affect running applications.

Automate security scanning

Embed comprehensive security scanning into the application life cycle and DevOps process to continuously scan every image, artifact, IaC template, and running workloads, automatically reducing risks, and ensuring compliance with internal policies and industry standards.

Shift left and integrate security early

Detect and remediate risks as developers write code, allowing teams to address issues before they reach production, enhancing speed and improving security posture.

Boost operational efficiency

Streamline communication and security processes among Development, Security, and Ops teams by leveraging robust code-to-cloud capabilities, fostering close collaboration across teams, and cultivating shared responsibility and a security-first mindset.

Protect in Runtime

Secure running applications and monitor active container, serverless, and VM workloads in real time, using a layered security approach that includes both out-of-the-box protection and customizable runtime policies.

Detect attacks instantly

Gain complete runtime visibility in minutes and enforce robust security policies across hybrid and multi-cloud environments. Ensure real-time protection of your production workloads against a wide range of threats and instantly detect malware, known, and unknown attacks as they unfold.

Catch what others miss

Identify suspicious activity and sophisticated zero-day attacks based on real-world, continuously updated threat intelligence from the Aqua Nautilus research team. Automatically alert, block, or delete malware upon download or execution, ensuring regulatory compliance where malware protection is required.

Stop attacks with no downtime

Stop sophisticated attacks and suspicious behavior in production without disrupting running workloads. Ensure workload immutability by automatically blocking any unauthorized activity, privilege escalation, and zero-day attacks without killing the container itself.

Respond and investigate incidents quickly

Rapidly determine the impact and see the entire attack kill chain of a security incident, capture every malicious action for investigation, and proactively mitigate attacks across all workloads and layers.

Secure Containers Across the Full Life Cycle

Achieve complete end-to-end protection for container images and running container workloads, regardless of where they are deployed across hybrid, on-premises, and multi-cloud environments.

Prevent security incidents

Detect advanced malicious threats and suspicious behavior in container images by running them in a secure sandbox before they're deployed, effectively preventing any damage to a runtime environment.

Control your risk tolerance

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

Consolidate scanning tools

Streamline security and risk management by leveraging Aqua 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.

Define once and run anywhere

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

Prove and Report Compliance

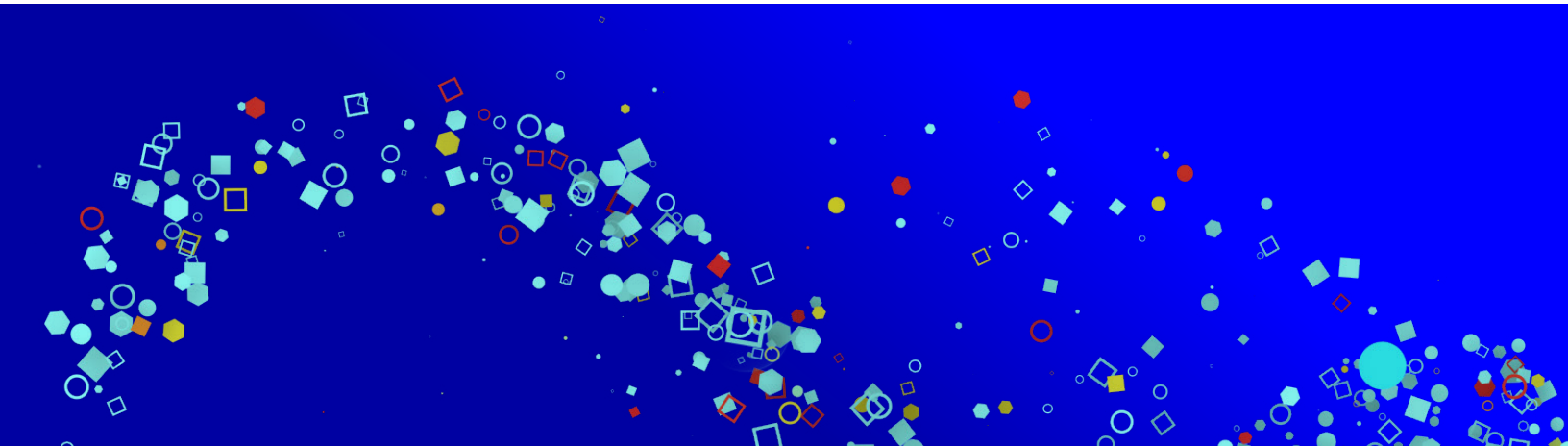
Proactively reduce security risks while meeting regulatory requirements with various industry standards, such as PCI DSS, NIS2, CIS Benchmarks, DORA, and GDPR.

Achieve compliance without compromise

Define policies to manage and maintain compliance of your cloud native applications by automatically auditing your security posture for drifts and violations across dozens of popular industry frameworks and regulatory standards such as NIST, PCI DSS, GDPR, and CIS Benchmarks.

Report compliance with ease

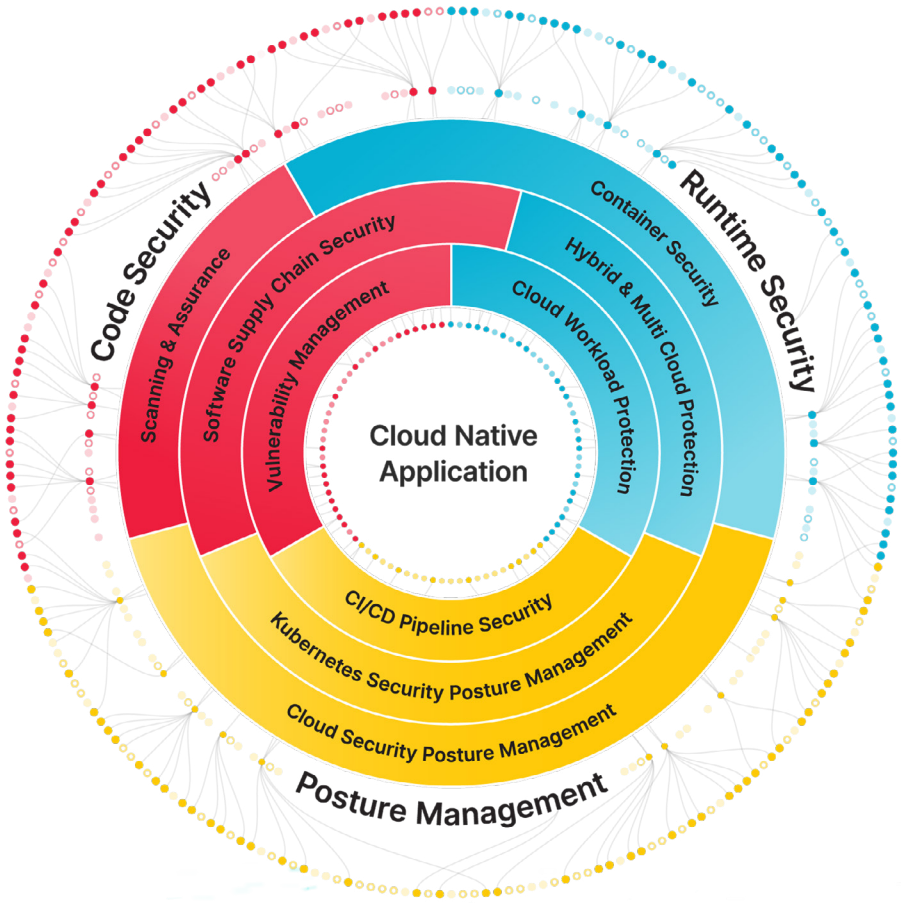
Confidently demonstrate compliance to auditors and management with compliance dashboards and real-time reports while enforcing security policies to ensure continuous compliance throughout the application life cycle.



The Aqua Platform: Securing Every Application Everywhere

Aqua Cloud Native Application Protection Platform (CNAPP) provides end-to-end protection for cloud native applications deployed in containers, serverless functions, and VMs throughout their entire life cycle. A single comprehensive platform proactively secures applications from the first line of code through runtime, across on-premises, multi-cloud, and hybrid environments – no matter where they're deployed. With a quick deployment, Aqua instantly integrates with your existing cloud native stack and seamlessly scales as your needs evolve.

Aqua CNAPP enables secure and faster adoption of cloud native technologies, such as containers, Kubernetes, and serverless functions, empowering businesses to innovate and thrive in the digital age. We help organizations implement DevSecOps so they can build faster, enhance customer experiences, and deliver new digital services with confidence, removing obstacles and minimizing security risks on their digital transformation journey.



aqua

Aqua Security is the pioneer in securing containerized cloud native applications. The Aqua Platform, a Cloud Native Application Protection Platform (CNAPP), enables organizations to secure every cloud native application everywhere, from code commit to runtime. With enterprise scale that doesn't slow development pipelines, Aqua secures your future in the cloud. 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 a demo ›