SOLUTION BRIEF

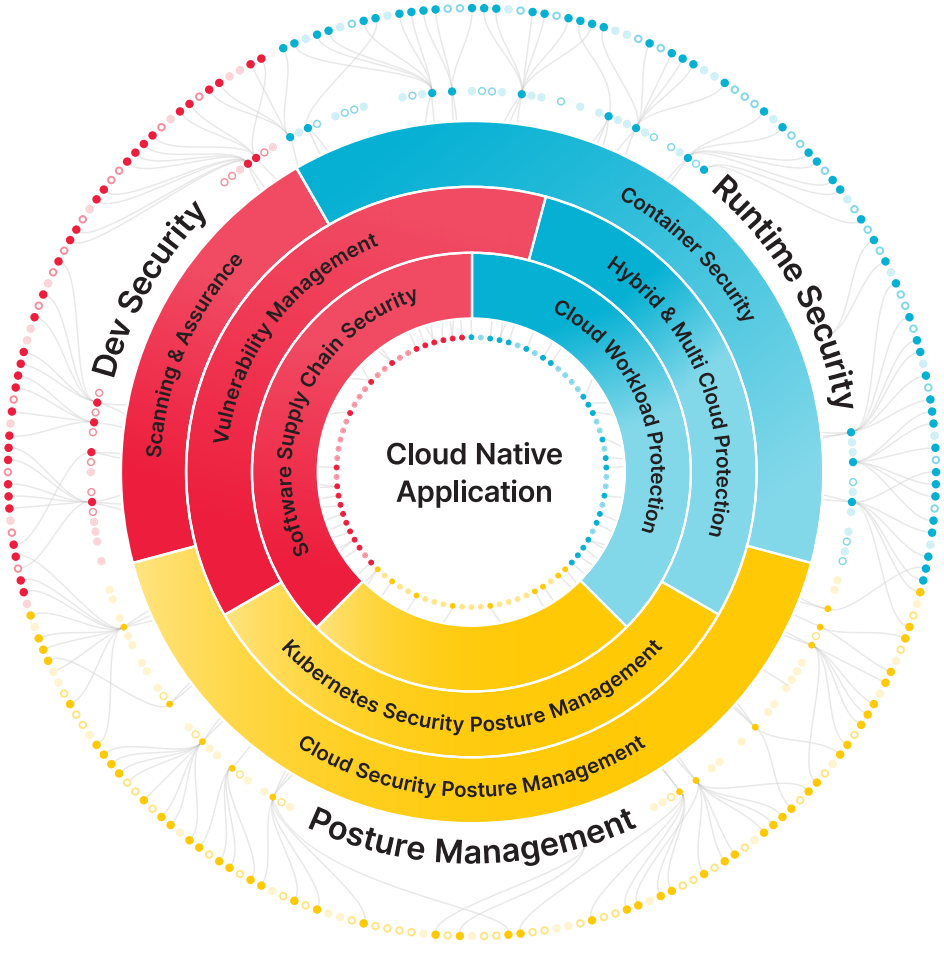
Aqua CNAPP
Go beyond visibility to true cloud native application protection

Aqua's Cloud Native Application Protection Platform (CNAPP) unifies key security capabilities to protect your cloud native applications across their entire lifecycle with a single, unified solution. Unlike CNAPP solutions that only focus on visibility and posture management, Aqua CNAPP actually protects cloud native applications against both known and unknown threats, from code to cloud and back, using a combination of runtime and shift-left protection as well as posture management.

How Aqua CNAPP Secures Cloud Native Applications

Organizations have realized the need for a purpose-built security approach to match the unique demands of a cloud native approach i.e. high velocity lifecycles, micro-services architecture, broad use of open source building blocks and DevOps-driven infrastructure-as-code.

Aqua CNAPP aligns with the dynamic and scalable nature of cloud native applications. The platform proactively keeps bad out to protect from known and unknown threats with shift-left capabilities and protects in real-time with robust runtime protection capabilities. All of this, while maintaining a safe and secure environment across on-prem, multi-cloud and hybrid configurations.



Keep Bad Out: Securing the Code and Build Stages

With a "shift left" approach to cloud native security that stops threats and vulnerabilities in their tracks, Aqua empowers DevOps teams to detect issues early and fix them fast. From the moment developers begin writing code to when the code moves to the build stage, Aqua's CNAPP scans for both known and unknown vulnerabilities and misconfigurations, ensuring only secure, compliant artifacts make it through. This proactive approach fortifies applications against potential threats, catching issues early to save time and resources down the road.

Code and Build Security

Unify security scanning

Automate 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 using a single, universal scanner. Periodic scans keep you alerted to new risks as your code changes.

Go beyond basic SBOM

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.

Fix vulnerabilities fast

Identify and fix the code at the point of origin of the vulnerability using Aqua's detailed dependency tree. Leverage Aqua's auto response functionality that goes beyond prioritization to provide precise instructions and directed communication to asset stakeholders on fixing the vulnerability.

Set boundaries and risk thresholds

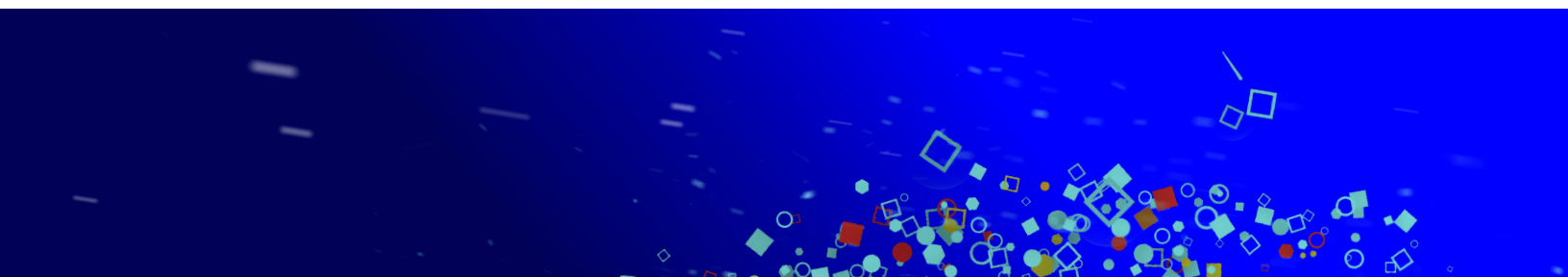
Ensure that the packages and images you deploy are trusted and have passed all security checks before deployment. Aqua's Assurance policies are customizable at different security thresholds to provide the necessary perimeters instrumental in establishing and maintaining a secure runtime environment without stopping development.

Accelerate remediation with cloud-to-code tracing

Aqua automatically links cloud risks in production to the development pipeline and exact line of code as well as relevant developer, enabling you to dramatically simplify and accelerate the remediation process and ensure priority issues are resolved quickly.

Protect against sophisticated threats

Evaluate risk from unknown and hidden threats that evade detection from traditional scanning tools by assessing runtime behaviour of images prior to deployment with Aqua's Dynamic Threat Analysis capability.



Protect in Real-Time: Runtime Security with Aqua

Aqua CNAPP protects applications across container, serverless and VM-based workloads, using multiple layers that include both out-of-the-box threat protections and fully customizable and granular policies. By combining a zero-trust approach to ensure immutability, behavioral detections based on real-world attack analysis, and signature-based malware prevention, Aqua defends applications against both known and zero-day threats. Security teams can automate granular mitigations to stop attacks, as well as view and analyze complex incidents for orchestrated response and forensics.

Advanced Runtime Protection

Optimize application stability and security

Enhance application security with eBPF technology, designed to provide low-friction, less intrusive, robust protection without impacting performance.

Catch what others miss

Identify suspicious activity and Indicators of Compromise (IoCs) mapped to the MITRE ATT&CK framework, based on real-world intelligence from Aqua Nautilus threat research team.
Identify in-memory and evasive attack vectors missed when using only agentless and signature-based methods.

Stop malware attacks in real time

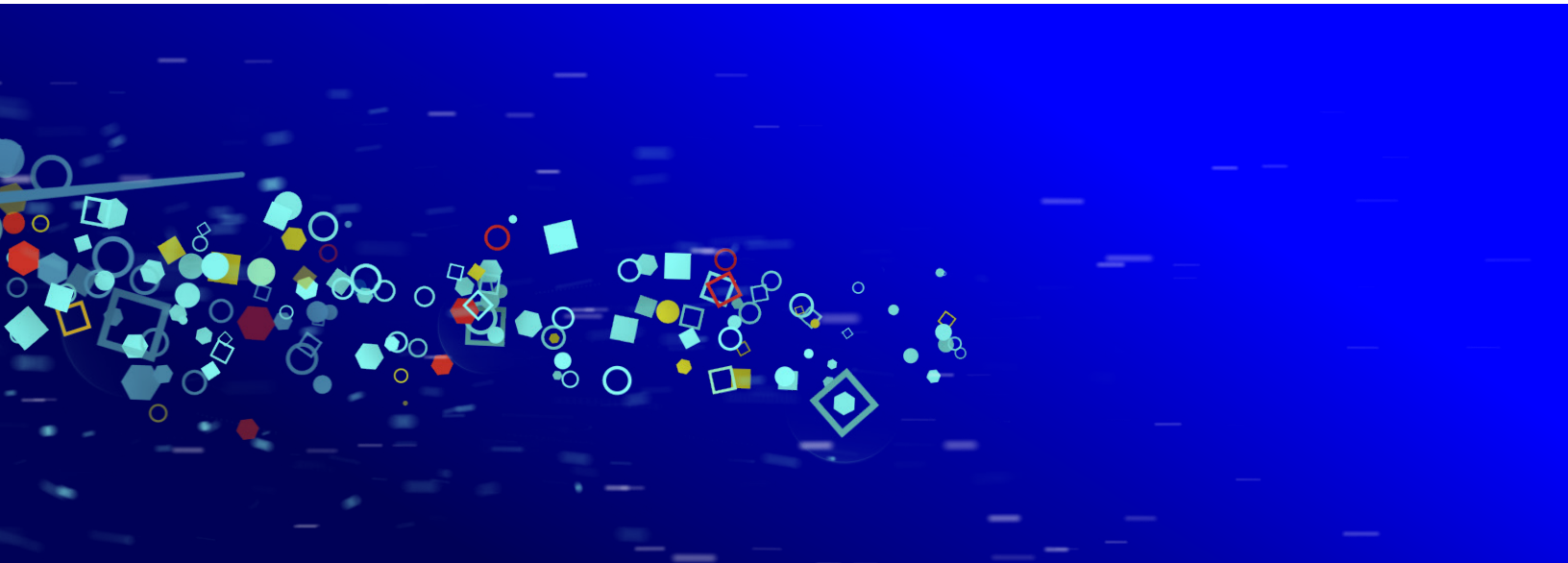
Enhance runtime security by automatically alerting, blocking, or deleting known and unknown malware upon download or execution, also enabling regulatory compliance where malware protection is required.

Ensure workload immutability

Preserve container integrity by automatically blocking unauthorized activities with cutting edge drift prevention technology, ensuring only original image executables and commands run, offering protection against zero-day attacks without stopping the container.

Defend against vulnerability exploits

Protect instantly against vulnerabilities that do not have a fix with vShield, a targeted defense mechanism that precisely prevents exploitation of a known vulnerability, safeguarding your workloads without waiting for patches.



Maintain a Safe Environment: Cloud Infrastructure Security with Aqua

Aqua CNAPP ensures that security is embedded from the very beginning of the cloud and Infrastructure-as-Code (IaC) infrastructure lifecycle, preventing potential security breaches and compliance issues before infrastructure is provisioned.

IaC Security

Integrate security into the CI/CD pipeline: Detect and remediate risks from misconfigurations in the IaC by automatically scanning IaC templates and hardening your application artifacts within CI/CD workflows. Also scan for sensitive data and secrets in the IaC files, ensuring your cloud infrastructure is robust and resilient against the evolving threat landscape, without compromising agility.

Cloud Security Posture Management (CSPM)

Create a unified view of all cloud resources

Quickly connect your cloud accounts and discover all your cloud resources running in AWS, Azure, Google Cloud, Oracle Cloud and Alibaba. Easily see, search, and drill down into specific cloud resources or risks with the unified cloud inventory.

Prioritize top risks and reduce noise

Focus on fixing the top issues with smarter insights correlated across hundreds of checks instead of chasing false positives.

Manage privileges and identities

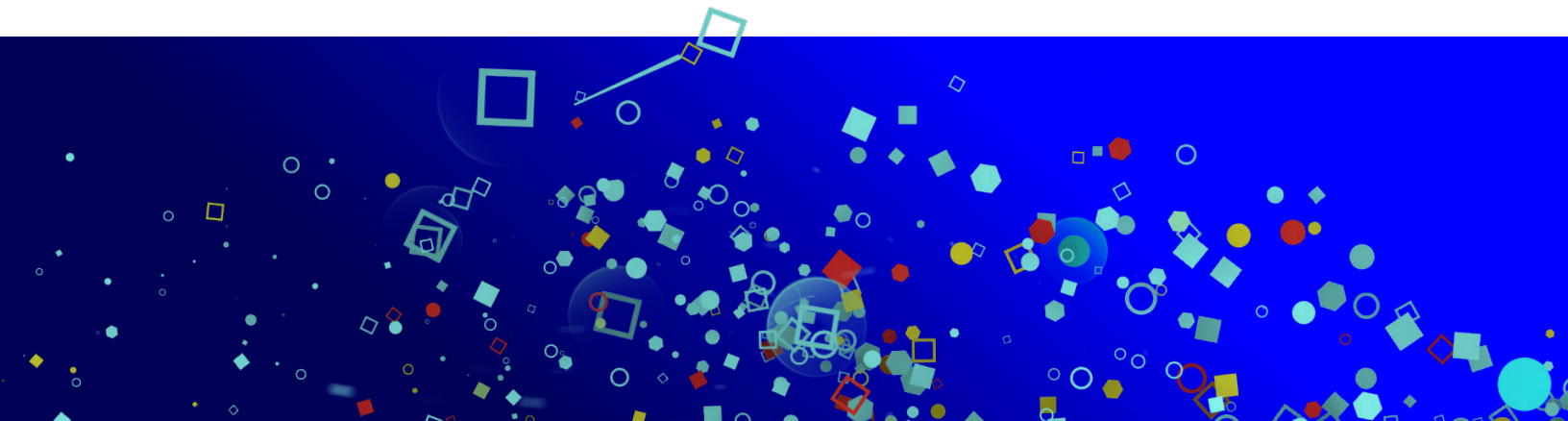
Effectively manage, monitor, and audit who can access specific resources, for the most up-to-date visibility into your cloud environment and security posture.

Quickly assess risk posture

Scan workloads with Aqua's out of the box agentless workload scanning to quickly assess your basic risk posture against various industry standards and benchmarks.

Remediate the most critical issues and reduce risk fast

Focus on fixing the most important cloud security issues, instead of chasing low-priority findings with smarter insights, enabling faster and more efficient remediation.



Kubernetes Security & Posture Management

Ensure compliance

Ensure that your Kubernetes clusters are properly configured according to best practices such as NIST and CIS benchmarks, ensuring compliance and preventing configuration drift.

Protect high-risk workloads

Use advanced admission controls to detect and prevent deployment of high-risk workloads onto Kubernetes clusters, based on flexible policies that enforce user permissions, resource limits, network and files access, and more.

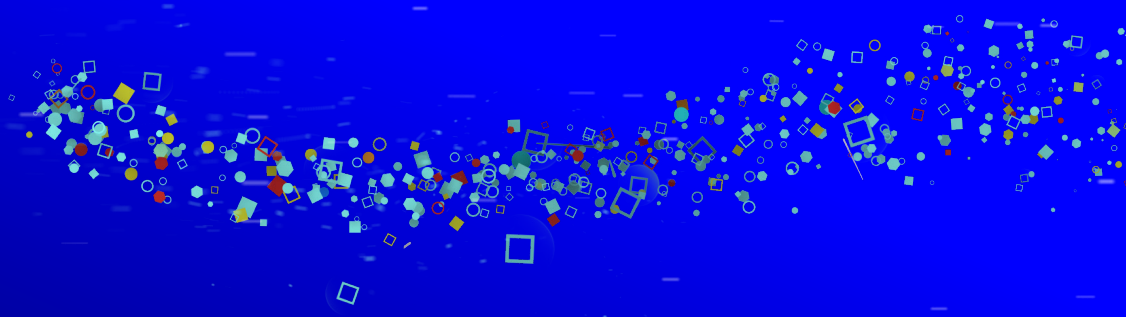
Protect in hybrid environments

Protect Kubernetes clusters across on-prem platforms and public cloud against known attack vectors and threats.

Aqua CNAPP: Enterprise-grade protection powered by real-world threat intelligence

Aqua's unified platform is purpose-built to keep up with the dynamic and ephemeral nature of cloud native applications. The solution is built for unmatched enterprise-grade scale, proven in some of the world's largest container-based and serverless deployments. Many of the world's largest financial institutions use Aqua to power their cloud native security in highly regulated environments and 41 of the Fortune 100 trust Aqua to secure their cloud native applications.

Aqua's cutting-edge threat research team, Nautilus, powers our CNAPP with innovative, research-driven insights specific to cloud native environments, empowering you to truly understand your security posture, make better security decisions, and confidently report compliance to auditors and management.



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 ›