SOLUTION BRIEF

Reduce Risk with Advanced Code-to-Cloud Vulnerability Management

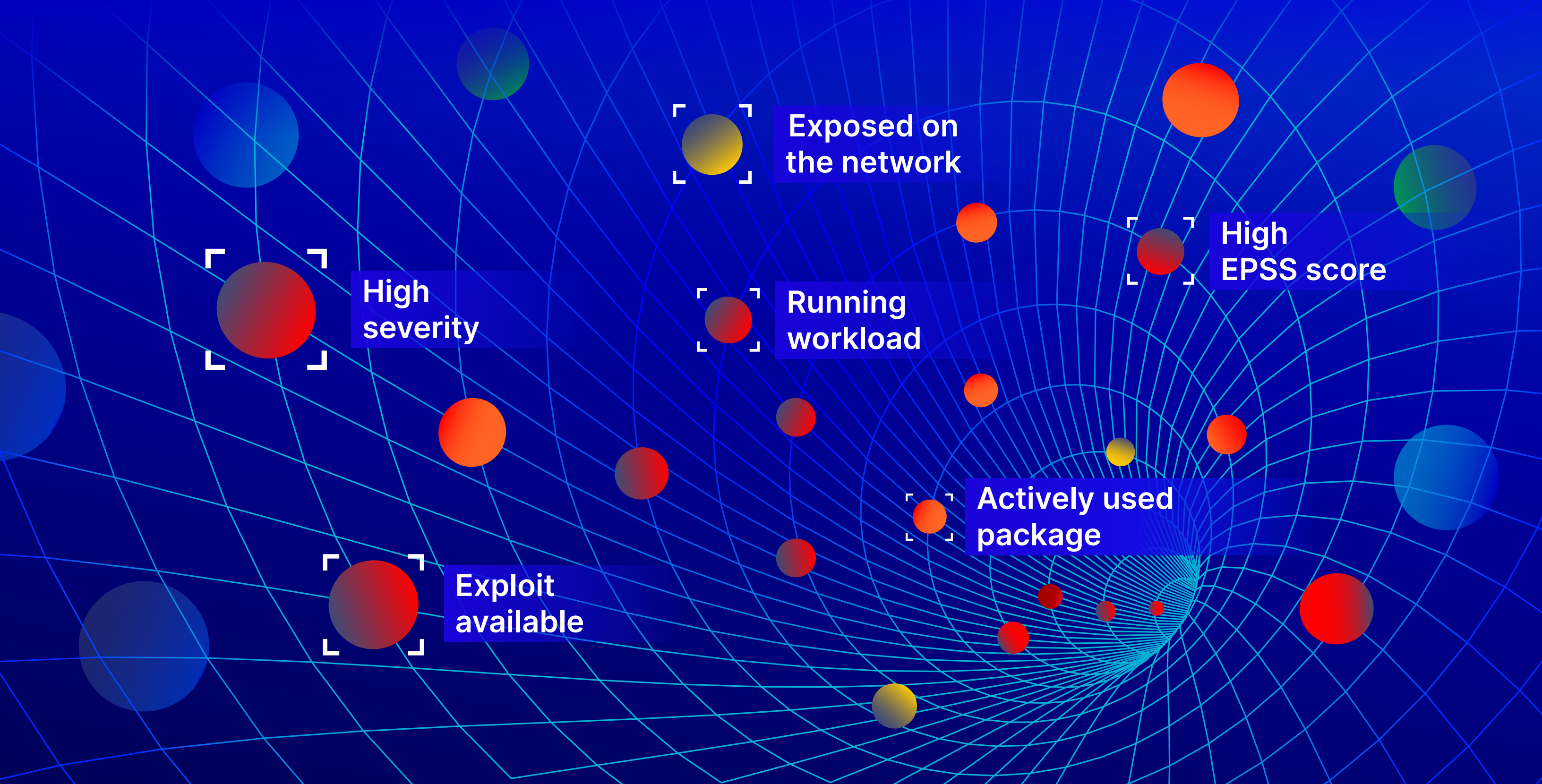
Key Benefits

- ✓ Prevent vulnerabilities from reaching production with comprehensive code scanning
- ✓ Filter top-priority issues that pose the highest risk using deep runtime context
- ✓ Easily trace vulnerabilities back to code to remediate issues quickly
- ✓ Mitigate vulnerabilities at runtime with compensating controls
- ✓ Track and manage your vulnerability posture across the full application life cycle

Cloud native applications rely heavily on open source components, comprising up to 90% of their code. These components often come with numerous direct and indirect dependencies, resulting in a continual influx of vulnerable code into production. This overwhelming volume of vulnerabilities leaves DevSecOps, vulnerability management, and AppSec teams struggling to chase down and address the most critical issues to efficiently reduce the attack surface.

To meet the demands of a dynamic and rapidly evolving cloud environment, an effective vulnerability management strategy must employ a risk-based approach throughout the entire application life cycle. Aqua's advanced Code-to-Cloud Vulnerability Management leverages deep runtime insights to make vulnerability findings actionable, dramatically reducing CVE noise. It empowers teams with the full application context to easily address the most critical vulnerabilities, quickly tracing issues back to the source for remediation or mitigating them in runtime with robust compensating controls.

Risk-Based Insights for Reducing Vulnerability Noise



Advanced Code-to-Cloud Vulnerability Management

Speed up the vulnerability remediation cycle and reduce mean time to resolve (MTTR) by empowering teams with full context of the risks in the specific application. On the left side, provide developers with deep runtime insights, enabling them to accurately prioritize threats and fix issues fast without leaving their workflows. On the right side, equip AppSec teams with detailed code and risk insights, allowing them to easily trace issues back to the source and find responsible owners.

Empower Developers to Own Security

Empower developers to prioritize and easily resolve issues by providing the full context of where their code runs, ensuring that vulnerabilities won't cause damage to running applications. By tracing the CVE back to the code and understanding the risks in the specific application, developers can address issues efficiently and with confidence.

Fix issues easily

Get the full runtime context to prioritize and resolve identified vulnerabilities in your own workflows – either by fixing the CVE in the code, changing to a more updated container image, or using compensating controls to block its exploitation at runtime.

Save time

Spend less time fixing CVEs by easily tracing issues back to code to find the exact line where vulnerabilities originated. Automatically generate a pull request to the responsible owner and use Aqua's or AI-guided remediation advice to resolve issues quickly.

Shift Left and Embed Security from the Start

Help AppSec and DevSecOps teams to secure applications throughout their life cycle, from development to runtime, by integrating security scanning into the DevOps process to accurately detect and fix vulnerabilities and other risks right from the start.

Prevent vulnerabilities from production

Set up assurance policies to define risk level for accepting artifacts for deployment, reducing the attack surface and preventing vulnerabilities from reaching production.

Speed up remediation

Reduce remediation time and make it easy for developers to fix issues by automatically generating a pull request to the responsible owner.

Detect and fix vulnerabilities early

Integrate automated scanning into the software development lifecycle to continually uncover known vulnerabilities in application code, container images, third-party components, open source packages, and more, using Aqua Trivy, the most accurate and universal scanner.

Reduce Vulnerability Noise Across the Full Application Life Cycle

Enable vulnerability management teams to identify and focus on the vulnerabilities that are actually exploitable and clearly prioritize them for remediation based on a unique mix of contextual insights. For non-fixable vulnerabilities, use compensating controls and enforce robust runtime policies to protect applications against threats.

Assess your vulnerability posture

Gain a comprehensive risk picture through contextualization by combining vulnerability findings with secrets, misconfigurations, and various other data points by using Aqua Trivy, the most accurate and universal scanner.

Report on vulnerabilities

Assess and track the status of vulnerabilities and remediation efforts, and regularly communicate them to stakeholders. Report key vulnerability metrics, such as the average age of vulnerabilities and MTTR, or export vulnerability findings into internal systems.

Mitigate in runtime

Close exploitation paths and attack vectors for specific vulnerabilities that can't be fixed by applying compensating controls such as vShield, a virtual patch that provides immediate protection.

Focus on the biggest risks

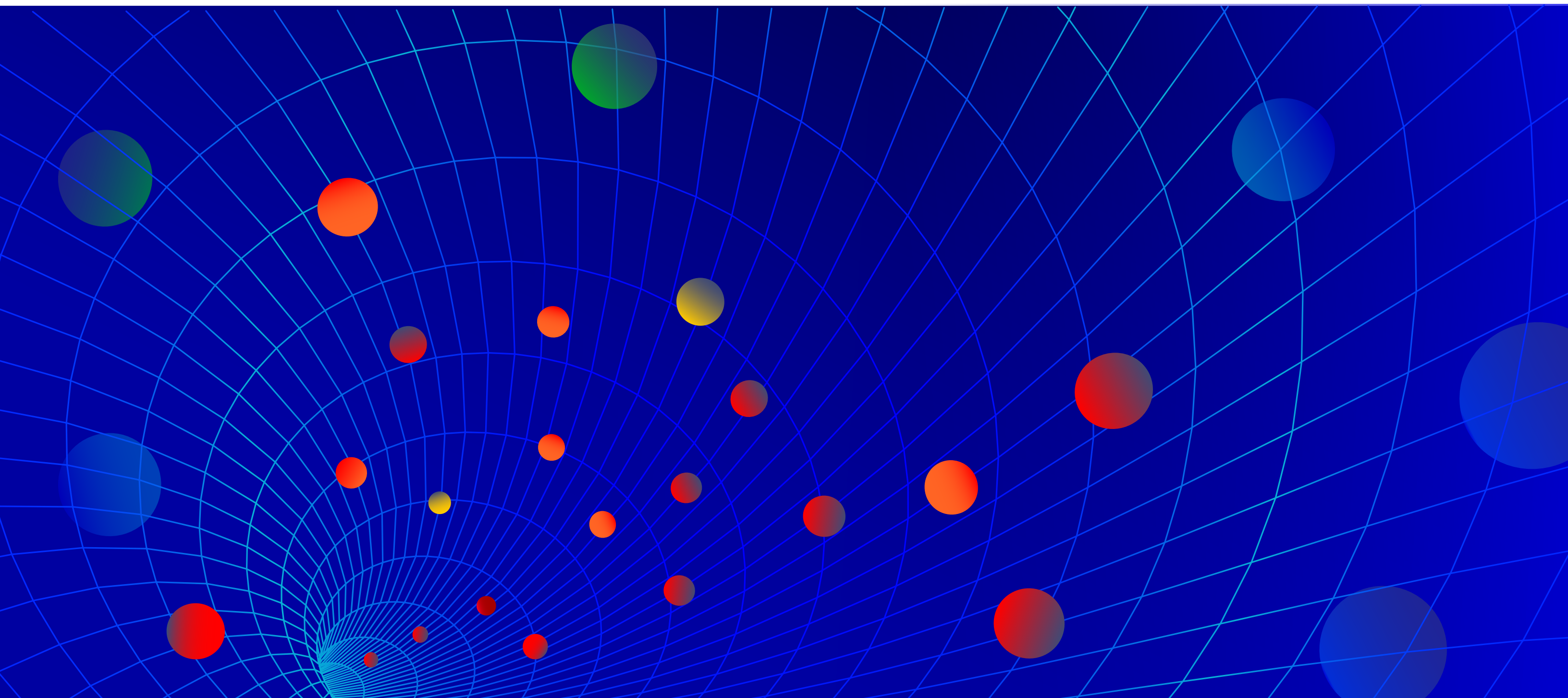
Use a risk-based approach to automatically filter thousands of vulnerabilities and determine top-priority issues that pose the greatest risk and require action. Analyze the impact of CVEs by a variety of granular factors such as reachability, EPSS, actively running packages, available exploits, and more.

Ensure compliance

Ensure that vulnerability management practices comply with internal policies, industry standards, and regulatory requirements.

Enhance runtime protection

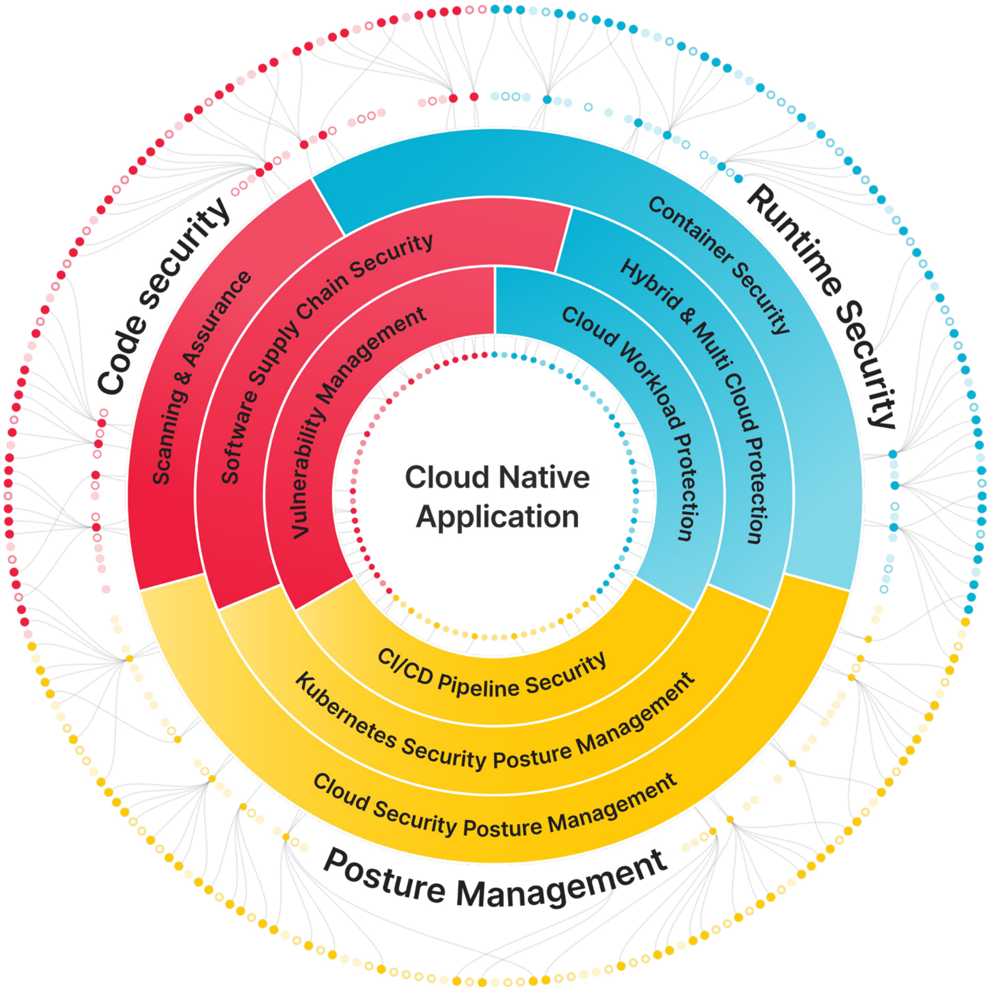
Protect against exploitable vulnerabilities by enforcing granular runtime policies to detect and alert on zero-day attacks, drift, cryptocurrency mining, malware, and other threats in real time.



Aqua CNAPP

Leading Platform for Code-to-Cloud Vulnerability Management

Aqua provides comprehensive end-to-end vulnerability management for cloud native workloads, regardless of where they are deployed. Track vulnerabilities from development to production, leveraging runtime insights to drive efficient prioritization and remediation efforts. Continually manage, assess, and report on vulnerabilities at scale and throughout the entire application life cycle, across your multi-cloud environment, leading to better resource allocation and enhanced security posture.


Cloud Native Application
Code security
Scanning & Assurance
Software Supply Chain Security
Vulnerability Management
Runtime Security
Container Security
Hybrid & Multi Cloud Protection
Cloud Workload Protection
Posture Management
CI/CD Pipeline Security
Kubernetes Security Posture Management
Cloud Security Posture Management

qua Security is the pioneer in securing containerized cloud native applications from development to production. Aqua›s full lifecycle solution prevents attacks by enforcing pre-deployment hygiene and mitigates attacks in real time in production, reducing mean time to repair and overall business risk. The Aqua Platform, a Cloud Native Application Protection Platform (CNAPP), integrates security from Code to Cloud, combining the power of agent and agentless technology into a single solution. 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 ›