SOLUTION BRIEF

Detect and stop live attacks with intelligence-driven runtime protection

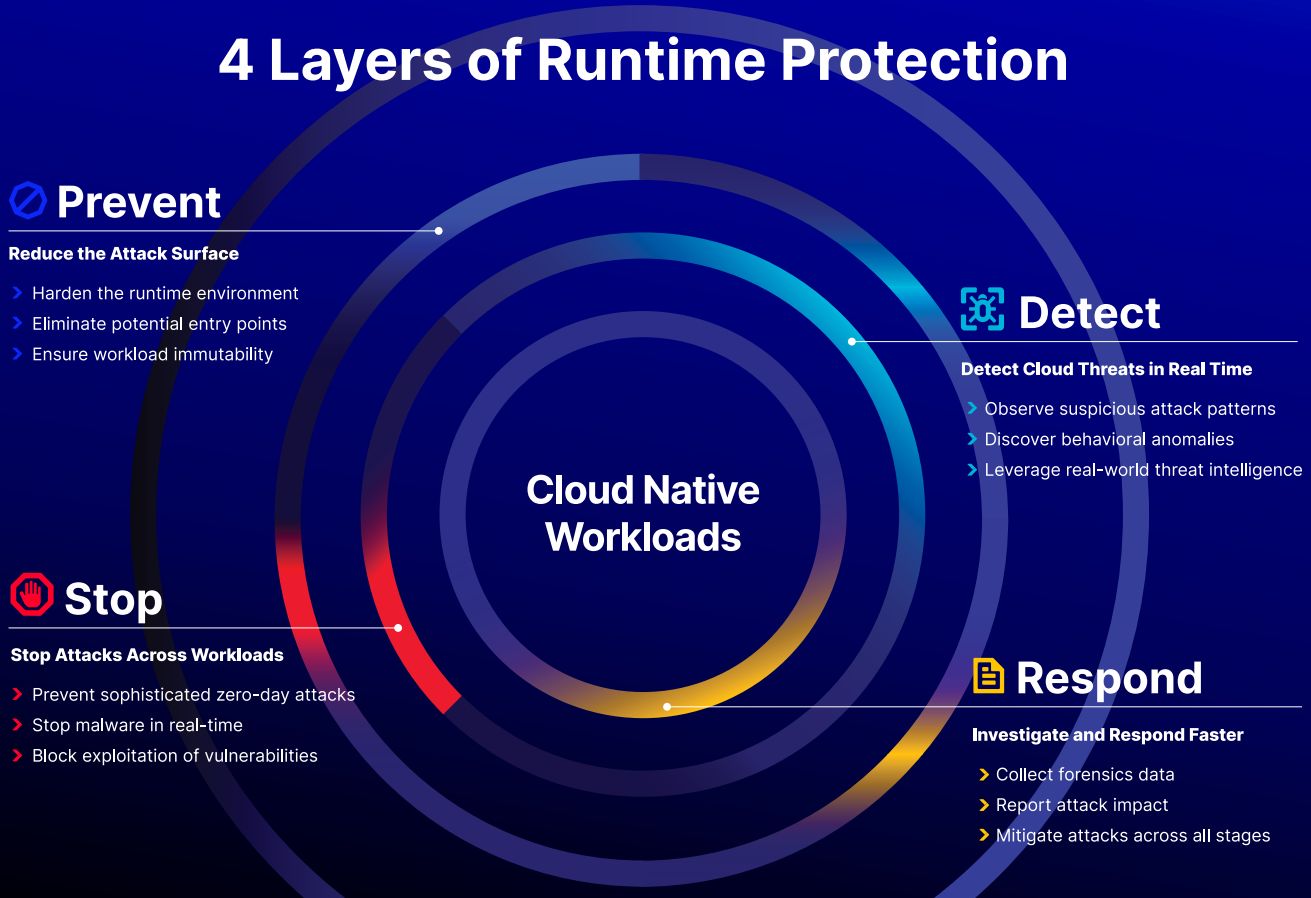
Key Benefits

- ✔ Secure hybrid and multi-cloud workloads at runtime with a single policy engine
- ✔ Reduce the attack surface and eliminate potential entry points for attack
- ✔ Detect and stop attacks in real time with no impact on production
- ✔ Identify and block malware and suspicious behavior in running workloads
- ✔ Protect against the unknown and stop zero-day attacks with ease
- ✔ Investigate incidents and respond faster

In recent years, security teams have mastered cloud visibility, leveraging various tools to improve the security posture and ensure compliance. However, cloud attacks continue to proliferate. While organizations' efforts focused on reducing the attack surface, active runtime protection wasn't given enough attention. As cloud threats intensify both in complexity and volume, the ability to detect and stop attacks in real time becomes more crucial than ever.

It's time to elevate your runtime defense with a powerful, intelligence-driven solution designed for modern, agile security teams. **Aqua Runtime Protection** deploys in minutes to immediately safeguard your cloud native applications where the stakes are the highest. Detect and stop active attacks on your running containers, VMs, and serverless workloads in real time with granular controls to instantly identify known and unknown threats, fileless malware, zero-day attacks, cryptocurrency mining, and more.

4 Layers of Runtime Protection



Prevent potential threats

Anticipate and neutralize threats before they materialize with runtime hardening controls. Implement preemptive measures and restrict workload access to effectively lock down the environment, proactively thwarting potential attacks before they initiate.

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.

Reduce the attack surface

Eliminate potential entry points for threats by hardening the runtime environment ensuring restricted access and preventing any lateral movement or escalation within or between workloads.

Ensure consistent visibility and enforcement

Achieve consistent, granular control over cloud native environments, ensuring uniform security policy application, enforcing immutability, and reducing vulnerability risks.

Protect workloads faster

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

Detect attacks in real time

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, prevent drift, instantly detect malware, known and unknown attacks as they unfold.

Detect threats with precision

Cut through alert noise with high-fidelity detection and smart severity scoring, enabling faster response to legitimate threats and reducing alert fatigue.

Ensure consistent visibility and enforcement

Achieve consistent, granular control over cloud native environments, ensuring uniform security policy application and reducing security risks.

Reduce response times

Detect threats with complete visibility and enhance montioring of advanced threats with detailed kernel-level visibility into each malicious action.

Protect against the unknown

Discover zero-day threats accurately with advanced cloud native detection and response powered by real-world threat intelligence from Aqua Nautilus research team.

Catch threats that others miss

Identify defense evasion techniques missed by agentless scans, using MITRE ATT&CK framework to categorize malware, IOCs, and novel attacks, catching what others overlook.

Observe suspicious behavior and attack patterns

Identify threats using behavior and signature-based detection methods to uncover known and unknown threats before they reach production.

Stop live attacks instantly

Go beyond mere threat detection by quickly addressing and resolving identified threats. Stop sophisticated zero-day attacks and suspicious behavior in production without disrupting running workloads, thereby enhancing security, maintaining operational efficiency, and avoiding costly downtime to preserve customer trust.

Stop attacks with no downtime

Ensure workload immutability by automatically blocking any unauthorized activity, privilege escalation, and zero-days, without killing the container.

Block exploitation of vulnerabilities

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

Stop malware attacks in real time

Enhance runtime security by automatically alerting, blocking, or deleting advanced malware upon download or execution, with the flexibility to choose the best course of action based on the severity of the threat and your preferences.

Prevent zero-day attacks

Elevate your cloud security with cutting-edge drift prevention technology that automatically detects and blocks unauthorized actions, offering proactive protection against zero-day attacks.

Respond faster and simplify the incident investigation

To effectively navigate the demands of digital transformation, it is crucial to ensure the necessary speed and agility of your Security Operations Center (SOC) team. Rapidly determine the impact and see the entire attack kill chain of a security incident, capture every malicious action for investigation, and proactively mitigate attacksacross all workloads and layers.

Investigate incidents faster

Collect comprehensive forensics data at the kernel level to investigate an attack and get to the root cause faster. Get detailed incident timelines and runtime risk data in your SIEM, analytics, or monitoring tools for enhanced visibility and analysis.

Capture malware evidence

Preserve critical malware evidence even in ephemeral environments, ensuring IR and SOC teams can trace attacks, reduce false positives, and meet regulatory requirements.

Optimize application stability and security

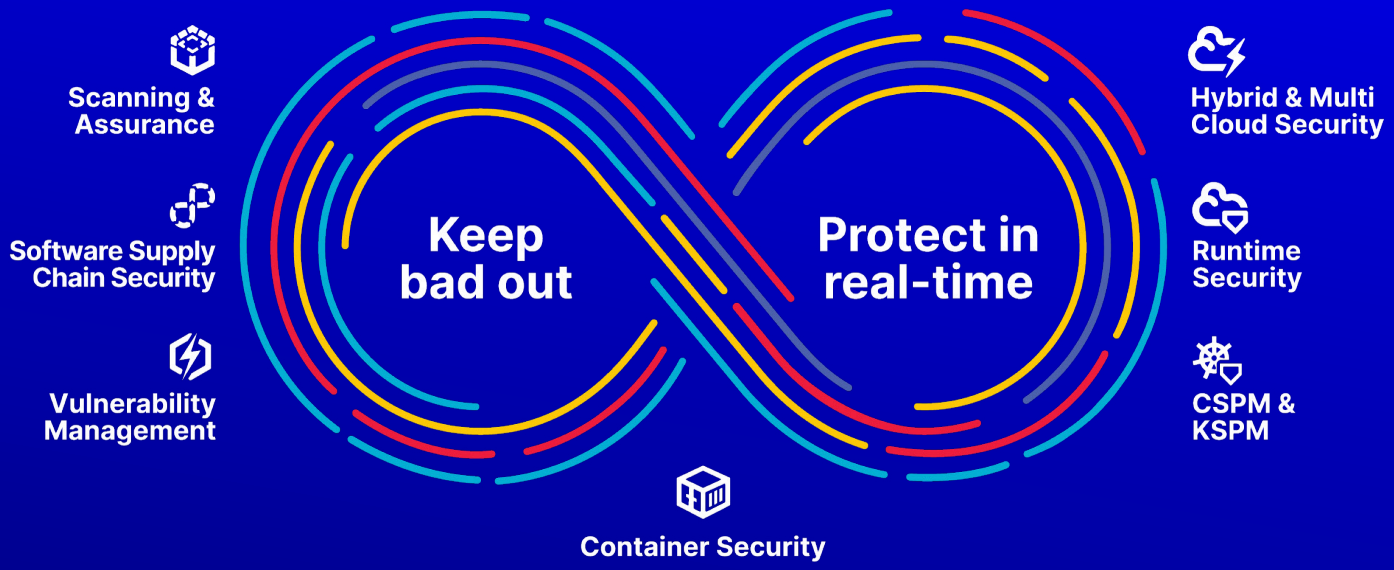
Enhance application security with eBPF technology, designed to provide low-friction, less intrusive protection without impacting performance.

Report attack impact easily

Provide a detailed report of the entire attack timeline by mapping techniques to the MITRE ATT&CK framework and assessing impact during each stage of the attack.

Elevate your runtime defense with Aqua CNAPP

As an integral part of Cloud Native Application Protection Platform (CNAPP), Aqua provides a robust, intelligence-driven solution for active runtime protection of cloud native workloads. To keep up with the velocity of digital transformation, it allows SOC teams to accelerate detection and response by seamlessly blocking any unauthorized activity without causing downtime to running workloads. As the threat landscape continues to evolve, enhance resiliency against escalating cyber threats and zero-day attacks through behavioral detection, which is based on real-world threat intelligence from the Aqua Nautilus research team.



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 ›