FEATURE SHEET

Aqua Dynamic Threat Analysis (DTA)

Detect and Stop Malicious Attacks Before Production

Key Benefits

- **Prevent security incidents** by stopping malicious behavior before deployment.
- **Enable fast development** by empowering developers to safely use third-party images.
- **Reduce the attack surface** by addressing hidden risks early in the app life cycle.
- **Minimize the impact of a potential attack** by tracing and visualizing the entire kill chain.
- **Simplify forensics and investigation** by automatically classifying detected malicious behaviors per the MITRE ATT&CK framework.

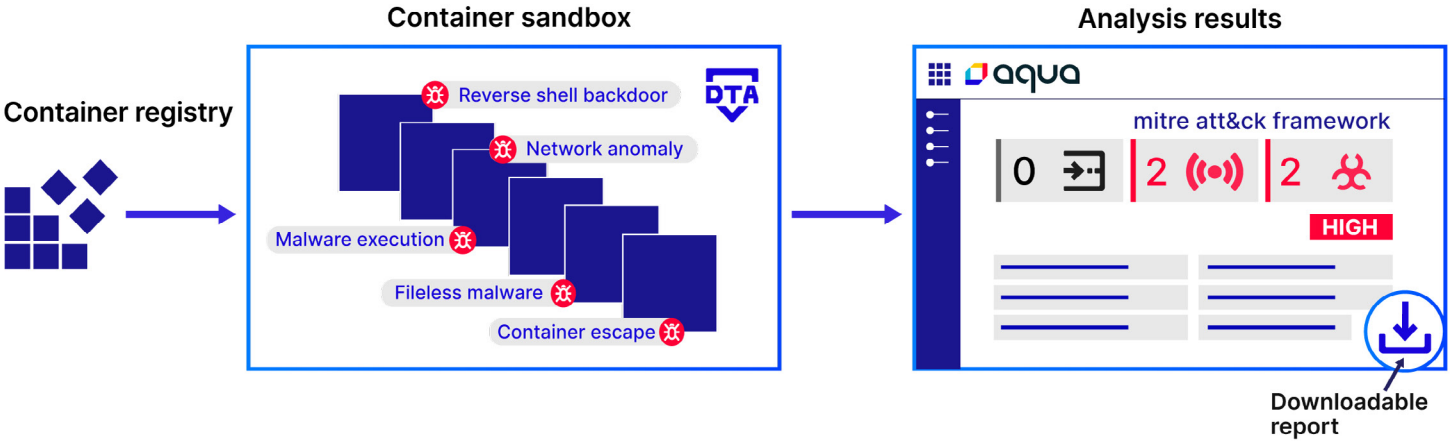
Going Beyond Vulnerability Scanning

The rising popularity of container-driven development has made it a focus area for adversaries who continually refine their techniques to exploit container images. On top of known vulnerabilities, risks in container images commonly involve malware and other malicious components. These threats often remain hidden within images, evading detection by traditional scanning tools until they're activated at runtime. In addition to vulnerability scanning, comprehensive assessment of container image risks must include evaluation of their runtime behavior prior to the deployment.

This is where Aqua Dynamic Threat Analysis (Aqua DTA) comes into play.

Powered by real-world threat intelligence of Aqua Nautilus Research Team, Aqua DTA analyzes runtime behavior of container images before they're pushed to production. Built specifically for cloud native environments, it runs an image in a safe, isolated sandbox and monitors the running instance for dozens of types of suspicious behavior. This allows teams to detect and mitigate malicious threats early in the application life cycle, helping organizations effectively reduce their attack surface while enabling secure development and preventing costly breaches.

Aqua DTA: How it works



1. Aqua DTA pulls a container image from your container registry or CI/CD pipeline and runs it in a safe and isolated VM environment (sandbox) in the cloud. This ensures that if an image is malicious, it won't cause any damage to your environment, preventing breaches and allowing you to contain and investigate it.

2. The dynamic analysis runs for several minutes and monitors how the container images behave: what files are running, what resources are being used, their network activity, and more.

3. Aqua DTA displays the analysis results and detected malicious behaviors, classifies the findings by severity, and maps them to the MITRE ATT&CK framework.

4. Aqua DTA generates a detailed breakdown of the entire attack kill chain, summarizing the findings of the malicious potential of the image in a downloadable report for forensics and investigation.

Summary

As part of Aqua's comprehensive container security solution, Aqua Dynamic Threat Analysis offers a robust and proactive approach to container security, enabling teams to detect and mitigate advanced malicious threats before deployment. By leveraging Aqua DTA, organizations can proactively prevent security incidents, avoid financial costs, enhance their security posture, and maintain the trust of their customers.