

Aqua Dynamic Threat Analysis (DTA)

Aqua DTA dynamically analyzes container images before they are deployed, in a secure isolated sandboxed environment, examining and tracing behavioral anomalies to uncover advanced malware that cannot be detected by static scanners.



The Rising Threat of Hidden Malware

As the use of containers continues to grow, malicious actors have been developing attacks that target container infrastructure. An emerging threat, these sophisticated attacks hide malicious code inside images and open source packages, using evasion techniques to avoid detection by static scanners that look for file signatures. Such malware can only be detected in a running container but doing so in live environments poses a high risk to the business.

Aqua DTA addresses these risks by automatically running images in a secure sandboxed environment, then analyzing, tracing, and classifying the detected behaviors. The sandbox prevents the malware from doing any harm to other workloads and resources on the host or network. Using Aqua DTA allows security and DevOps teams to improve the security of their software supply chain and reduce risk to runtime environments.

Identify Hidden Risk in Your Container CI Pipeline

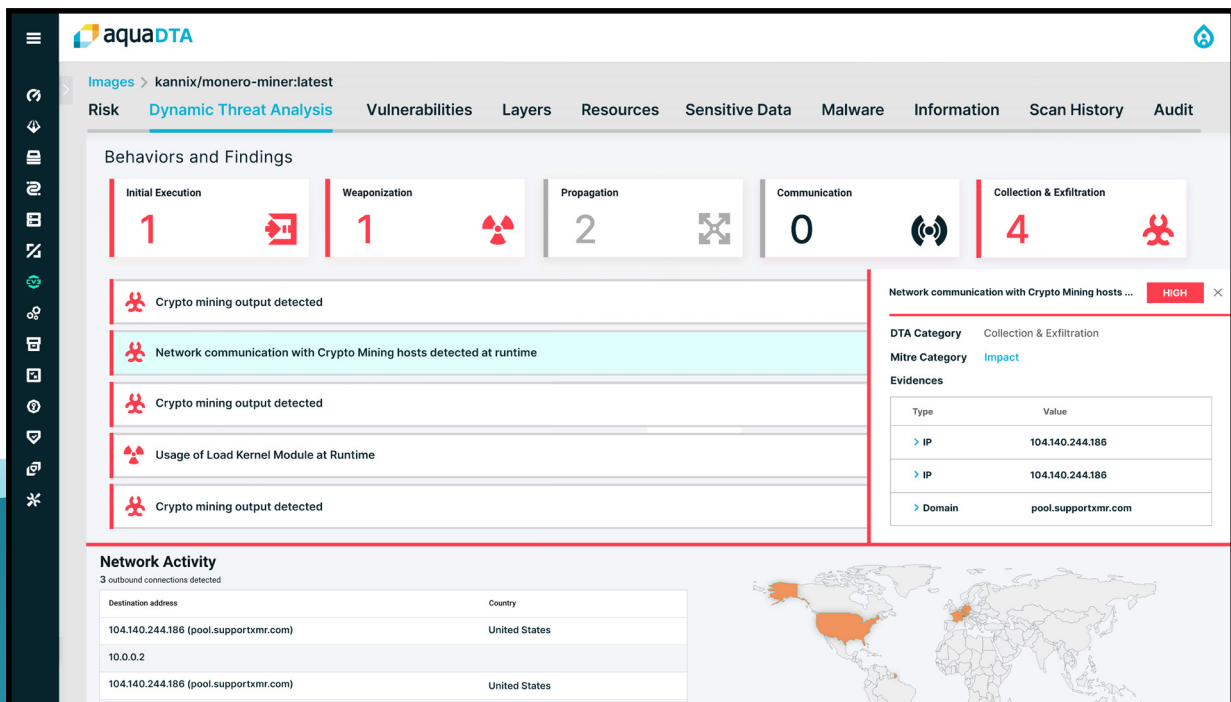
Select 3rd party, sensitive, or pre-production images for dynamic analysis to identify hidden risks, automatically adding advanced threat detection to your CI pipeline and registries.

Safely Detect Sophisticated Malware Before Deployment

Run images in a secure sandboxed environment that traces indicators of compromise (IoCs) such as container escapes, reverse shell backdoors, malware drops, code injection backdoors and network anomalies.

Protect Your Containerized Applications Against Attacks

Mitigate the risks of data theft, credential theft, using containers for DDoS, and cryptocurrency resource abuse targeted by Advanced Persistent Threats and polymorphic malware.



The screenshot shows the aquaDTA interface for the image 'kannix/monero-miner:latest'. The 'Behaviors and Findings' section displays a summary of detected activities:

- Initial Execution: 1
- Weaponization: 1
- Propagation: 2
- Communication: 0
- Collection & Exfiltration: 4

The findings list includes:

- Crypto mining output detected
- Network communication with Crypto Mining hosts detected at runtime
- Crypto mining output detected
- Usage of Load Kernel Module at Runtime
- Crypto mining output detected

The 'Network Activity' section shows 3 outbound connections detected:

Destination address	Country
104.140.244.186 (pool.supportxmr.com)	United States
10.0.0.2	
104.140.244.186 (pool.supportxmr.com)	United States

A world map highlights the United States as the source of the detected network activity.

Aqua DTA, an Integral Part of Your Cloud Native Security

Aqua's dynamic threat analysis integrates with your DevSecOps process, managed within the Aqua Cloud Native Security Platform. Specific images can be designated for automatic analysis based on scope, e.g., where they came from or the applications in which they are used, and the results are fed into Aqua's assurance policies to determine whether those images will be allowed to deploy into runtime environments.

Detecting Indicators of Compromise with Aqua DTA

Aqua DTA detects many types of malicious behavior, classifies them by severity and categorizes them according to the MITRE ATT&CK framework to provide a clear picture of the attack kill chain. Indicators include behaviors such as:

- Dropping and executing files
- Removal of existing executables
- Usage of hidden files
- Connecting to IP addresses not via DNS
- Connecting to known C&C servers
- Network service scanning
- Resource hijacking
- Reverse shell attempts
- Privilege escalation attempts



How Aqua DTA identifies stages of the attack kill chain

By using Aqua DTA, security teams can reduce the potential risk in container images before they are deployed

Vetting public images and their open source packages – as a security gate into the software development life cycle (SDLC).

Approval of ISVs' third-party Images – scanning third-party images from independent software vendors before introducing them into the organization.

Pre-production security gate – scanning images before they are promoted to production from CI/CD pipelines or registries.

Analysis and forensics – analyzing image runtime behavior to understand anomalies or perform forensics after a suspected incident

Aqua Security

✉ contact@aquasec.com 🌐 www.aquasec.com

📍 US HQ: 800 District Avenue, Suite 510, Burlington, MA 01803

👤 [aquasecteam](#) 🐦 [AquaSecTeam](#)

To learn more:
aquasec.com/DTA