Aqua Dynamic Threat Analysis (DTA)

Aqua DTA dynamically analyzes container images in your cloud environment before they are deployed, examining and tracing behavioral anomalies in a secure sandbox 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. 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 found in cloud-based registries 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 Container Image Registries

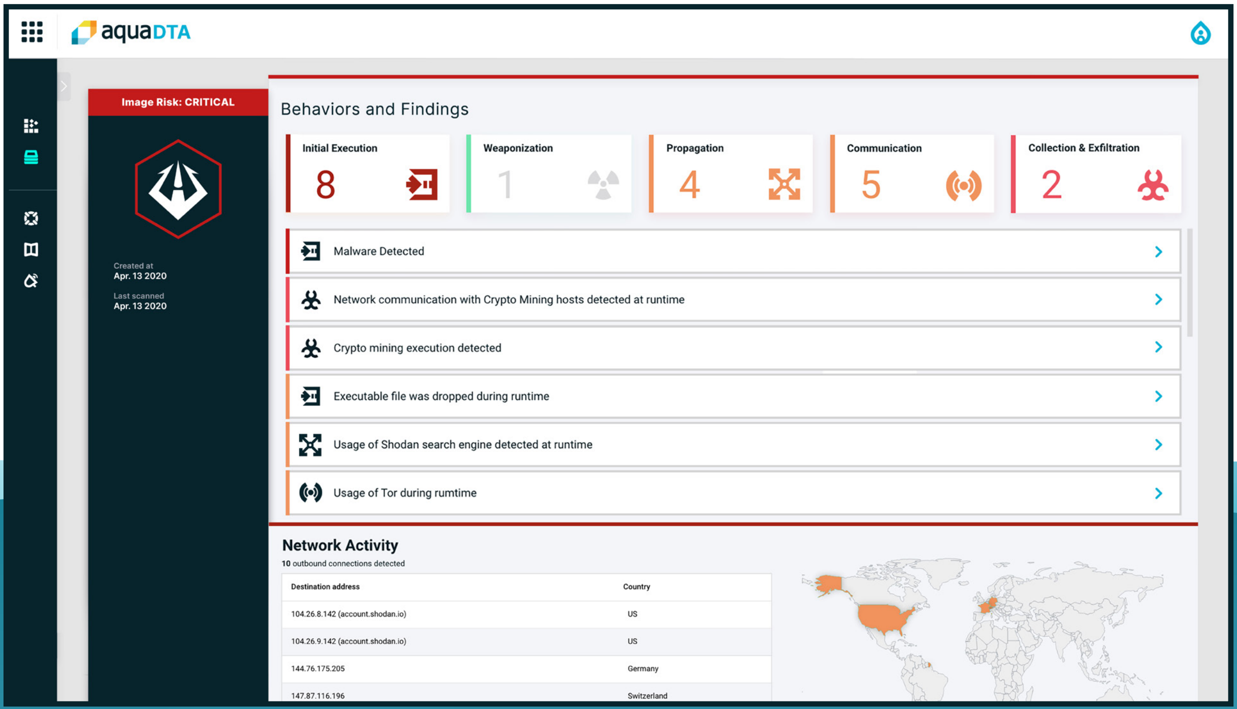
Scan images in cloud registries with dynamic analysis to identify hidden risks, automatically reducing the risk to your cloud-based applications and infrastructure.

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.



Created at
Apr. 13 2020

Last scanned
Apr. 13 2020

Behaviors and Findings

Initial Execution	Weaponization	Propagation	Communication	Collection & Exfiltration
8	1	4	5	2

- Malware Detected
- Network communication with Crypto Mining hosts detected at runtime
- Crypto mining execution detected
- Executable file was dropped during runtime
- Usage of Shodan search engine detected at runtime
- Usage of Tor during rumtime

Network Activity

10 outbound connections detected

Destination address	Country
104.26.8.142 (account.shodan.io)	US
104.26.9.142 (account.shodan.io)	US
144.76.175.205	Germany
147.87.116.196	Switzerland

aqua CSPM

Aqua DTA: An Integral Part of Cloud Security Posture Management

Aqua's dynamic threat analysis is an integrated part of your DevSecOps process, managed within Aqua CSPM. Specific images can be designated for dynamic analysis as well as vulnerability scanning, and the results assessed and reported as part of your overall cloud security risk posture to enable timely remediation.

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

Initial Execution
Runs adversary-controlled code to gain an initial foothold within a network

Weaponization
Keeps access to systems and bypasses security mechanisms

Propagation
Discovers local or remote resources to exploit them or perform lateral movement

Communication
Employs network communication methods to communicate with compromised systems to control them

Collection & Exfiltration
Accumulates resources and reaches the attack objective

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).

Pre-production security gate – scanning images before they are promoted to production.

Reducing risk to cloud infrastructure – preventing attacks and abuse of cloud resources by malware.

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
in aquasecteam AquaSecTeam

Try Aqua DTA at:
cloud.aquasec.com