

FEATURE SHEET

Real-Time Malware Protection for Cloud Native Environments

Key Benefits

- ✓ **Ensure up-to-date runtime** defense against a broad range of malware threats.
- ✓ **Automatically block or delete** malware on download or execution.
- ✓ **Prevent costly breaches** and runtime incidents.
- ✓ **Detect malware in running** containers and hosts in real time.
- ✓ **Identify and remediate** sophisticated in-memory malware (fileless attacks).
- ✓ **Achieve compliance** with malware protection requirements.

Malware is a significant threat in modern cloud environments due to their interconnected and dynamic nature, which allows it to spread rapidly and disrupt business-critical services. Organizations are targeted daily with a wide range of ever-evolving attacks that leverage advanced and stealthy techniques such as rootkits and fileless malware to fly under the radar. This makes early detection and response increasingly challenging for security teams.

Thus, it's critical for organizations to adopt robust malware protection capabilities as part of their broader runtime protection strategy.

Advanced Malware by the Numbers

 **75**

applications targeted by Kinsing over five years

 **1,400%**

increase in fileless malware attacks in 2023

 **54%**

of attacks leave backdoors

 **1,200+**

servers compromised by Redis-based malware HeadCrab

 **51%**

of attacks include aggressive worm techniques

Source: Aqua Nautilus

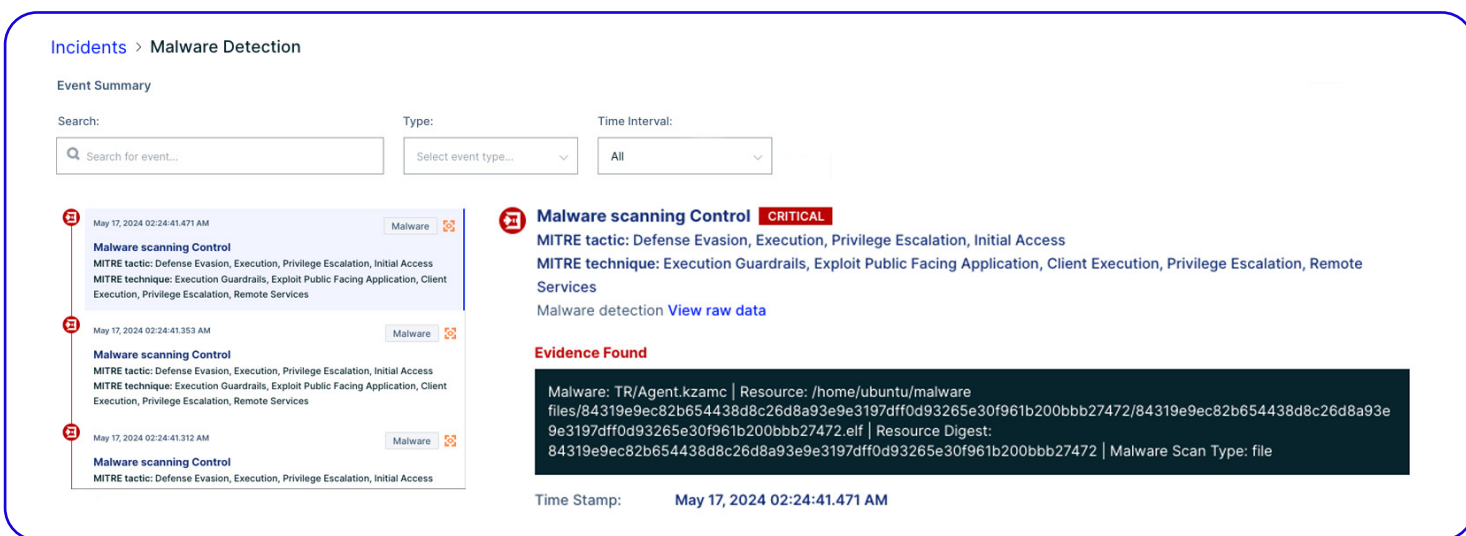
As one of the key controls of Aqua's Runtime Protection solution, **Advanced Malware Protection (AMP)** safeguards your applications in production from diverse malware threats such as ransomware, botnets, viruses, backdoors, cryptominers, and Trojans. Unlike common industry approaches, AMP uses a combination of detection methods – by file hashes and malware patterns – to identify Indicators of Compromise (IOCs), catching what other solutions miss, such as sophisticated fileless attacks.

Security operations center (SOC) and incident response (IR) teams can configure AMP to automatically block or delete malware on download or execution if it's detected on a running workload, instantly stopping the threat in their environments. The AMP malware library is continually updated with the latest malware signatures, ensuring comprehensive and up-to-date runtime defense against emerging threats.

Advanced Malware Protection: How It Works

Advanced Malware Protection provides on-access real-time malware protection for containers and VM hosts in Linux and Windows environments. Files are protected from malware when they're downloaded or executed within a VM or a container. To enable this feature in your environment, refer to the [Aqua documentation](#).

In case malware is detected on a running workload, you'll see an incident screen with all the details and evidence:



Incidents > Malware Detection

Event Summary

Search: Type: Time Interval:

May 17, 2024 02:24:41.471 AM Malware

Malware scanning Control CRITICAL

MITRE tactic: Defense Evasion, Execution, Privilege Escalation, Initial Access
MITRE technique: Execution Guardrails, Exploit Public Facing Application, Client Execution, Privilege Escalation, Remote Services

Malware detection [View raw data](#)

Evidence Found

```
Malware: TR/Agent.kzamc | Resource: /home/ubuntu/malware
files/84319e9ec82b654438d8c26d8a93e9e3197dff0d93265e30f961b200bbb27472/84319e9ec82b654438d8c26d8a93e
9e3197dff0d93265e30f961b200bbb27472.elf | Resource Digest:
84319e9ec82b654438d8c26d8a93e9e3197dff0d93265e30f961b200bbb27472 | Malware Scan Type: file
```

Time Stamp: May 17, 2024 02:24:41.471 AM

Summary

Malware is continually evolving, as cybercriminals constantly develop new evasive techniques to bypass security controls. Once malware infiltrates an organization, it can rapidly propagate across various systems and services, causing widespread disruption.

Aqua's Advanced Malware Protection employs robust detection techniques to protect organizations from these evolving threats. As part of runtime policy controls, it allows SOC and IR teams to identify malware in real time and quickly block and remove it, preventing larger security incidents and ensuring robust defense against even sophisticated malicious threats.



Aqua Security sees and stops attacks across the entire cloud native application lifecycle in a single, integrated Cloud Native Application Protection Platform (CNAPP). From software supply chain security for developers to cloud security and runtime protection for security teams, Aqua helps customers reduce risk while building the future of their businesses. 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 demo >](#)