FEATURE SHEET

Stop Runtime Attacks with Drift Prevention

Enforcing the immutability of containers for robust workload protection

Protecting applications against runtime attacks in a dynamic and constantly changing cloud environment is no simple task. Given the steep increase in zero-day attacks, you need to ensure that your production workloads are running as intended and stay identical to their originating states at any given moment. Here emerges one of the key cloud native concepts – the concept of immutability.

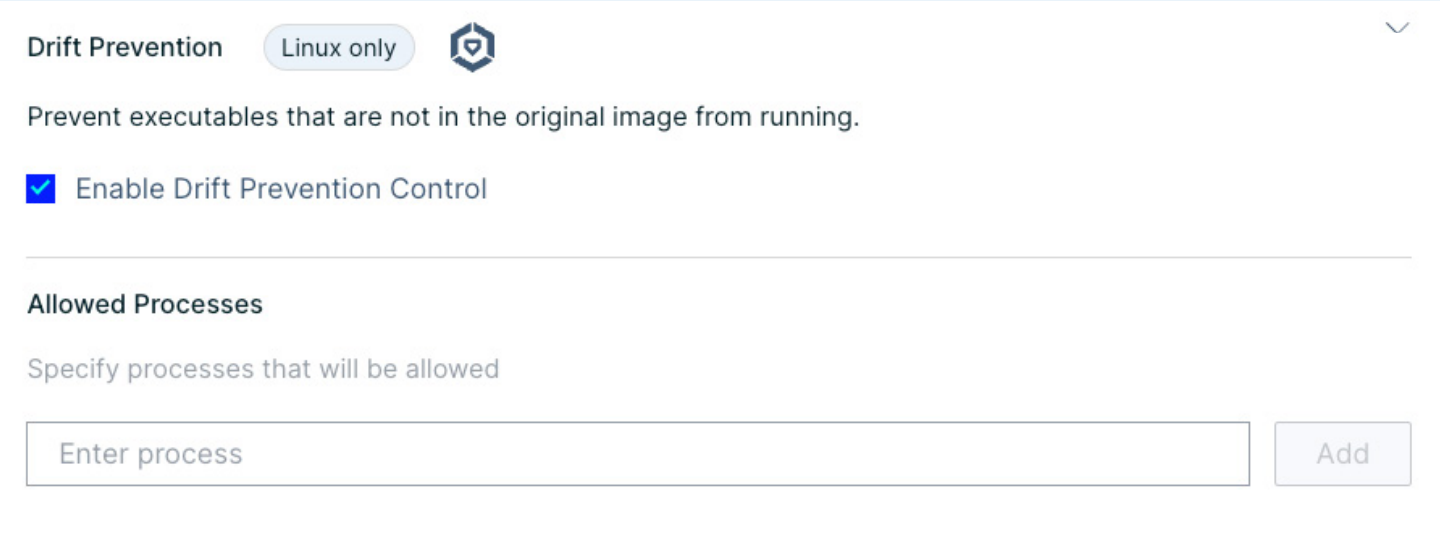
In the cloud reality, containers are designed to be immutable – they are not supposed to be updated or modified at runtime. By not allowing any changes to live containers, it becomes easy to determine suspicious behavior. If your container runs a process that wasn't part of its original image, it means something anomalous is happening and your container might have been compromised.

Enter Drift prevention. Drift prevention makes it easy to detect and stop any drifts from the intended state. It deterministically prohibits any changes to the image after it is instantiated into a container and blocks everything that wasn't part of the original image – without killing a container itself.

Drift prevention is built to help security teams:

- **Protect workloads against zero-day attacks**
  Detect and block known and unknown malware, zero-day exploits, and internal threats that can't be caught early on in the application life cycle.
- **Ensure workload integrity**
  Enforce the immutability by preventing code injection and unauthorized changes to running workloads.
- **Stop runtime attacks at any point**
  Automatically block any lateral movement or escalation within or between your cloud workloads.
- **Identify & block anomalous behavior in running containers**
  Prevent any executables and commands from running if they weren't in the original image.
- **Maintain business continuity**
  Only run code that should run and block everything else without interrupting business continuity.
- **Save time**
  Enable a single system-wide runtime control that works out of the box and doesn't require any configuration setup.

How It Works



1. **With Aqua, you can enforce the immutability of container workloads by ticking a single box in your runtime policies without impacting the container.**

2. **Aqua tracks a workload from its inception to runtime and compares its current payload to its original state to identify any differences.**

3. **If detected, Aqua automatically blocks any lateral movement or escalation within or between your cloud workloads**

With Aqua's Drift prevention, you can seamlessly enforce the container immutability to block any unauthorized processes in running workloads and protect them from a wide range of runtime threats. This helps you reduce the attack surface and provides a solid foundation for robust protection of your cloud native workloads.

Aqua Security sees and stops attacks across the entire cloud native application lifecycle in a single, integrated platform. 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.
The Aqua Platform is the industry's most comprehensive Cloud Native Application Protection Platform (CNAPP).
Founded in 2015, Aqua is headquartered in Boston, MA and Ramat Gan, IL with Fortune 1000 customers in over 40 countries.
For more information, visit https://www.aquasec.com

Copyright ©2023 Aqua Security Software Ltd., All Rights Reserved

Schedule demo ›