FEATURE SHEET

Assurance policies: Security gates to deploy only trusted container images

In a dynamic cloud native environment with rapid release cycles and multiple CI/CD pipelines, it's critical to ensure that you deploy only trusted container images in production. The foundation of container security lies in comprehensive image scanning and hardening during the build stage. However, as your images progress through the DevOps pipeline, it becomes essential to ensure that they still adhere to your security and compliance standards when they reach deployment.

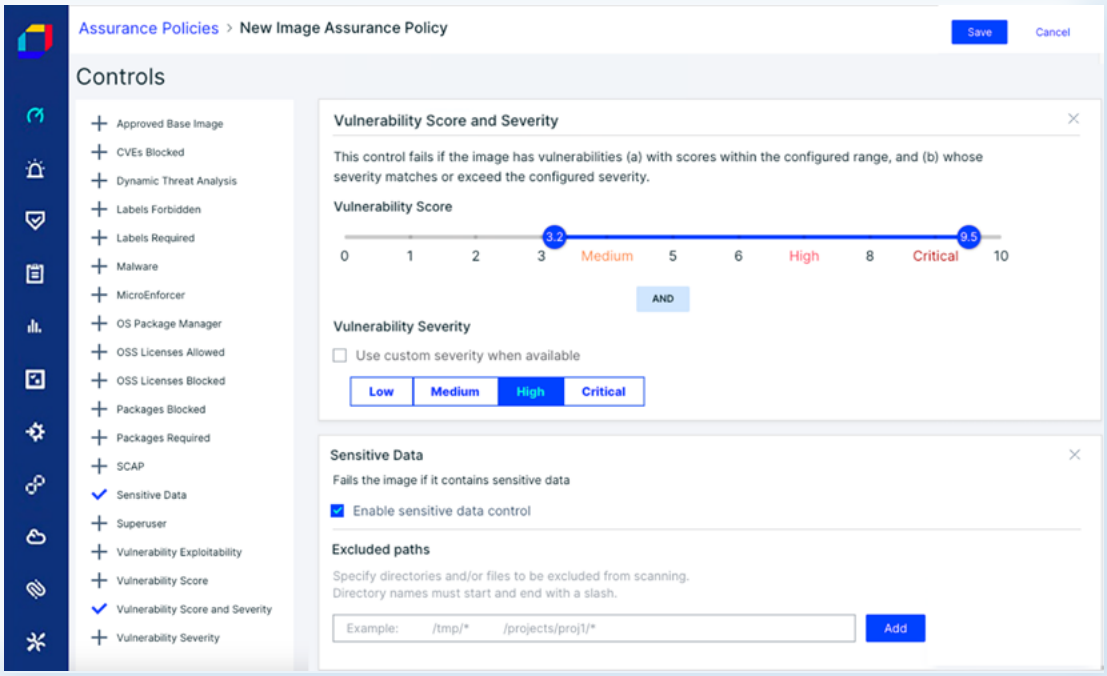
Enter **assurance policies**, which represent the fundamental cloud native concept of admission control. They allow you to set guardrails and define risk thresholds for admitting images into your production environment. Based on highly flexible rules, assurance policies cover a broad spectrum of risk factors, including risk score, excessive privileges, and embedded secrets. The policies act as a key pre-deployment control and are instrumental in establishing and maintaining a secure runtime environment.

As a critical capability of Aqua's robust **container security solution**, assurance policies help DevOps teams significantly reduce the risk of deploying compromised containers, thereby addressing the security challenges of a dynamic cloud native environment and protecting your organization's operations and reputation.

Assurance policies allow DevOps and DevSecOps teams to:

- **Ensure image integrity throughout the software development life cycle**
  Prevent unapproved images from running, which helps reduce operational errors, image sprawl, and rogue deployments.
- **Reduce the attack surface**
  Cut the amount of noise in production, making runtime controls more effective.
- **Tailor policies to fit your unique requirements**
  Customize policies with ease to meet the security needs of various pipelines and environments.
- **Improve collaboration between teams**
  Create a shared sense of trust between DevOps and security teams around the guardrails for allowing artifacts into production.
- **Accelerate development speed**
  Enable DevSecOps for faster and safer software delivery in highly dynamic cloud native environments.
- **Manage risk effectively**
  Set the right level of accepted risk and create multiple assurance policies for various scenarios and use cases.

How it works



An example of an assurance policy and how to set it up.

1. When creating a new assurance policy, define the conditions an image must meet to run. Rules can be based on any combination of CVE severity, risk score, malware severity, the presence of sensitive data, use of super-user permissions, and more.

2. Once a policy is configured, every image in its scope must meet its requirements.

3. If a non-compliant image is detected, Aqua will automatically prevent it from being deployed.

In summary

As part of the comprehensive container security solution, **Aqua's assurance policies** provide the necessary guardrails to ensure that the images you deploy are approved to run and have passed all security checks before deployment. This form the critical middle part between container image scanning and runtime controls, allowing you to reduce the attack surface of running applications while managing risk effectively.