FEATURE SHEET

Protecting Workloads Against the Exploitation of Vulnerabilities with Aqua vShield™

Key Benefits

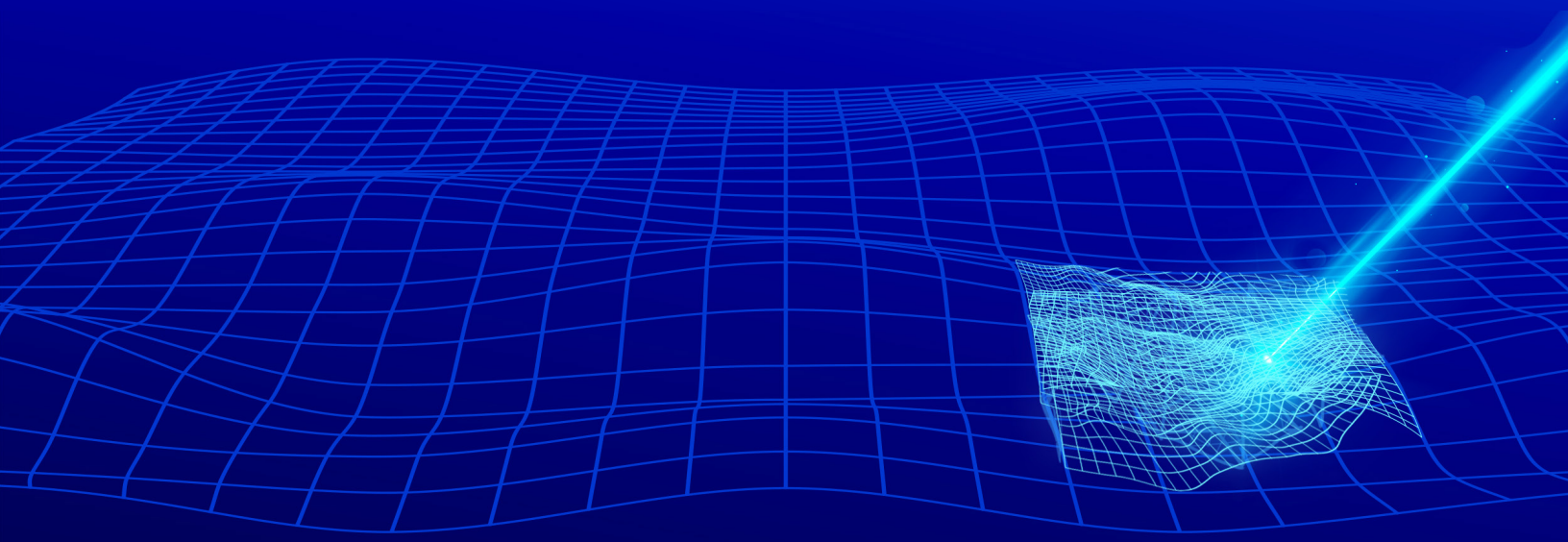
- ✔ Reduce the risk of known vulnerabilities in running applications.
- ✔ Automatically detect and block exploitation attempts.
- ✔ Save developers time by eliminating the need for manual mitigation.
- ✔ Protect workloads when you can't patch a vulnerability or afford downtime.
- ✔ Optimize the patching process and prioritize vulnerable images with ease.
- ✔ Enhance compliance posture with the use of compensating controls.

With the heavy reliance on open source software and the growing volume of CVEs, mitigating known vulnerabilities at scale has become a never-ending task. As manual patching is often time-consuming and not always feasible, organizations are left running vulnerable applications while attempting to prioritize and manage their risk. That's where virtual patching comes in – acting as a compensating control in runtime, it allows organizations to reduce their exposure to known threats and improve compliance.

What is Aqua vShield?

Aqua Vulnerability Shield (Aqua vShield) is a patent-pending capability that provides a compensating control for known vulnerabilities detected in running containers. It generates a runtime policy that detects and blocks access to vulnerable components in containers without the need to go back to the source and modify the image itself. Acting as a shield against exploitation of vulnerabilities, it allows security teams to reduce risk, block exploits in real time, and prioritize patching more efficiently while meeting auditor requirements for compensating controls.

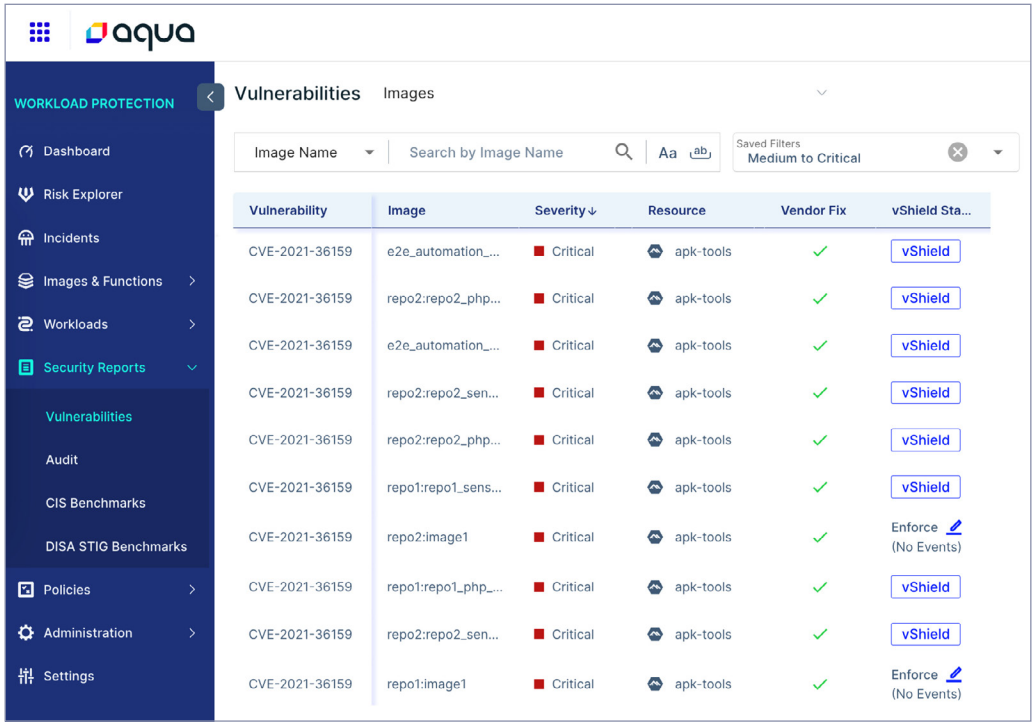
Aqua vShield, or "virtual patching" mechanism, automatically detects and can prevent attempts to exploit the vulnerability to which it is applied. It's non-intrusive, in that it does not change the image code, nor require any developer intervention. Automated virtual shielding allows for consistent, repeatable enforcement of mitigating factors and compensating controls in your runtime environment.



vShield: How Does It Work

1. Aqua vShield can be activated for vulnerabilities found in your scan results and will automatically enable the relevant runtime controls.

2. Depending on the underlying component that the vulnerability impacts and potential attack vector, an Aqua vShield can detect or block access to various resources during runtime:
e.g., a vulnerable network protocol, access to certain files, the use of a vulnerable package, or other capabilities required for an exploit.



Aqua vShields are automatically generated for newly discovered vulnerabilities and are reviewed and managed by the Aqua Nautilus research team, who find new ways to mitigate exploits, continuously refining the accuracy of vShields. When an unpatched vulnerability needs to be mitigated quickly, the team can prioritize a specific vShield to cover it.

Summary

Aqua vShield enables security teams to reduce the risk from known vulnerabilities in running containers by detecting and preventing exploit attempts without the need to rebuild the image and with zero downtime.
As part of Aqua's advanced code-to-cloud vulnerability management, vShield simplifies vulnerability mitigation, improves compliance, and helps security teams protect runtime environments while providing the flexibility to address the underlying issues when it best fits engineering teams.

Schedule a demo ›