

CASE STUDY

# Qanapi Accelerates FedRAMP High Readiness with RapidFort



## Industry

Technology Data Security



## Challenge

Achieve FedRAMP High compliance on an aggressive timeline, reduce vulnerability noise, and secure container images without slowing development



## Solution

RapidFort Platform and Curated Near Zero CVE Images

## The Challenge

Qanapi, a data-security API platform, was on an accelerated path to achieve FedRAMP High compliance for its regulated customers. The organization needed to meet rigorous CIS/STIG alignment requirements while maintaining operational speed and engineering focus. Qanapi faced three primary challenges:



### Complex Vulnerability Backlog

The existing container stack carried a large, noisy vulnerability load, and detect-only tools surfaced issues but did not meaningfully reduce the attack surface.



### Aggressive Compliance Timeline

The organization needed to reach FedRAMP High readiness quickly to meet customer and regulatory commitments.



### Operational Efficiency

Building and maintaining a compliant “gold build” internally would have taken months and diverted scarce engineering resources.

## The Solution

To efficiently meet its compliance and security goals, Qanapi turned to the RapidFort Platform and Curated Near Zero CVE Images, enabling accelerated FedRAMP High readiness, stronger container security, and uninterrupted delivery.

To further strengthen security and streamline operations, Defense Unicorns leveraged several key capabilities of the RapidFort Platform:



**Curated Near Zero CVE Images**

RapidFort provided pre-hardened, benchmarked images with built-in CIS/STIG alignment, enabling Qanapi to start from a clean, compliant foundation rather than hardening vulnerable base layers.



**Runtime Aware Hardening with RBOM**

RapidFort’s runtime-aware engine continuously filtered out non-reachable CVEs and stripped unused components from running containers, dramatically reducing noise and remediation workload.



**Supply-Chain Assurance**

The platform provided signed, provenance-tracked, and SLSA-aligned builds with non-root and distroless options, ensuring integrity and trust across the software supply chain.



**Seamless Integration**

With straightforward CI/CD integration, Qanapi embedded security directly into its pipelines, achieving continuous hardening and compliance alignment with minimal friction.

*“RapidFort became the foundation for our container posture: clean baselines, less noise, and defensible evidence for assessors freeing our team to focus on product and mission.”*

**Trent Telford**  
CEO & Founder, Qanapi

**Results**

By integrating RapidFort into its workflow, Qanapi achieved measurable improvements:



**Reduced Attack Surface**

of a near-zero CVE UDS platform without building in-house hardening pipelines



**Accelerated FedRAMP High Readiness**

by months compared to manual gold-image processes



**Lower Compliance Overhead**

as RapidFort automatically filtered out non-actionable CVEs, streamlining triage and reporting



**Maintained Developer Velocity**

by embedding security directly into the CI/CD pipeline, enabling rapid, compliant delivery

## Conclusion

Qanapi's collaboration with RapidFort enabled the company to achieve FedRAMP High readiness faster and with greater operational efficiency. By leveraging Curated Near Zero CVE images, runtime-aware hardening, and supply-chain assurance, Qanapi strengthened its container security posture and sustained developer agility, demonstrating that compliance readiness and innovation can advance together.

### **Eliminate Attack Vectors At The Source**

Continuously Eliminate Up to 99.9% of CVEs Without Code Changes

[Request Access ↗](#)