



RapidFort Quick Facts

Near-Zero CVE Images, Hardened to NIST 800 - 70 Guidelines FIPS 140-3 Validated, STIG/CIS Benchmarked

As organizations increasingly adopt containerized environments, security, compliance, and vulnerability management have become critical priorities. Choosing the right security-focused container solution is essential for mitigating risks, maintaining regulatory compliance, and ensuring software integrity.

RapidFort is a trusted security provider that delivers a comprehensive container hardening and CVE remediation solution. With 95% CVE remediation, RapidFort enhances security across the container build process and production by leveraging:

- · RF Curated Images: Near-zero CVE container images
- · RF Instrumentation and Profiling DevTime Protection Tools
- · RF Hardening and Defending tools RunTime Protection Tools

RapidFort supports Long-Term Support (LTS) Linux distributions, ensuring stability and broad compatibility for enterprises and government agencies.









Speed up Software Releases



Fast-Track Compliance

Security and Compliance

- Built on widely trusted LTS distributions, including: Ubuntu, Red Hat, Debian, Alpine
- Ensures long-term stability and compatibility
- Patches only upstream CVEs

Government and Enterprise Compliance

- **DISA STIG Benchmarking**
- FIPS 140-2 and FIPS 140-3 validated
- Preferred DoD Vendor IronBank

Vulnerability Management and Attack Surface Reduction

- Daily image builds with continuous patching
- Software Attack Surface Management (SASM)
- Patches & eliminate vulnerabilities at build time.

Transparency and Operational Reliability

- Full visibility into image builds, updates, and security patches.
- Ensures enterprises can track, validate, and audit security measures.



Integrate RapidFort directly into your existing workflows































Learn more about our new capabilities at https://hub.rapidfort.com/



