



Accelerating Compliance FedRAMP & CMMC

RapidFort offers a powerful, comprehensive End-to-End Vulnerability Management Platform specifically designed to help organizations address security gaps proactively and streamline compliance with rigorous regulatory frameworks like FedRAMP and CMMC. By automating real-time vulnerability reduction and ensuring continuous protection, RapidFort simplifies the path to regulatory compliance while strengthening overall cybersecurity resilience.

Accelerate Compliance in three steps



Curated, Near-Zero CVE Base Images

Deploy with confidence using pre-hardened FIPS 140-3 Validate container images for popular LTS distributions such as Alpine, Debian, Red Hat, and Ubuntu. These images are meticulously curated to minimize vulnerabilities before deployment, reducing the attack surface from the start.



Instrumentation and Profiling at DevTime

Secure your applications during development with proactive DevTime protection. RapidFort's platform identifies and mitigates potential vulnerabilities before they reach production, integrating seamlessly into your existing development workflows. With built-in STIG/CIS benchmarking, you can ensure adherence to industry-standard security baselines. The platform also offers a continuous audit trail and reporting, providing real-time visibility into security events and compliance status, ensuring that every change is tracked and documented for your software supply chain.

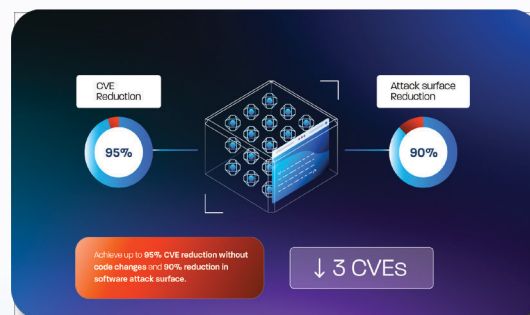


Hardening and Defending at RunTime

Benefit from continuous protection throughout runtime. RapidFort hardens your applications to reduce attack surfaces and container size prior to deployment. It also provides continuous monitoring and updates for new CVEs, ensuring ongoing security throughout your application's lifecycle.

Remediation
95% of CVEs

Reduce Attack Surfaces
By up to 90%





Accelerating Compliance for FedRAMP and CMMC

RapidFort’s proactive security approach addresses vulnerabilities early in the software development lifecycle and extends protection into runtime, ensuring that security measures evolve with your operational environment. This dynamic approach simplifies the often complex and time-consuming certification process by:

- Reducing Security Gaps: Proactively eliminate vulnerabilities before deployment.
- Streamlining Regulatory Audits: Automated reporting and compliance checks
- Ensuring Continuous Protection: Real-time monitoring and updates for new CVEs

Why Choose RapidFort for Compliance Acceleration?

Organizations across both public and private sectors trust RapidFort to navigate complex security and compliance landscapes. Our platform offers a holistic, scalable solution designed to:

- Simplify Compliance: Tailored tools and automated processes ease the path to meeting federal security standards.
- Enhance Operational Security: Continuous runtime defense strengthens your organization’s cybersecurity posture.
- Accelerate Time-to-Certification: Streamline the certification process with built-in reporting and proactive vulnerability reduction.
- Reduce Costs and Effort: Minimize the resources required for compliance by automating labor-intensive processes.

Achieve regulatory compliance faster and strengthen your cybersecurity defenses with RapidFort’s advanced vulnerability management platform. Empower your organization to meet the highest security standards—efficiently and effectively.

Integrate RapidFort directly into your existing workflows

