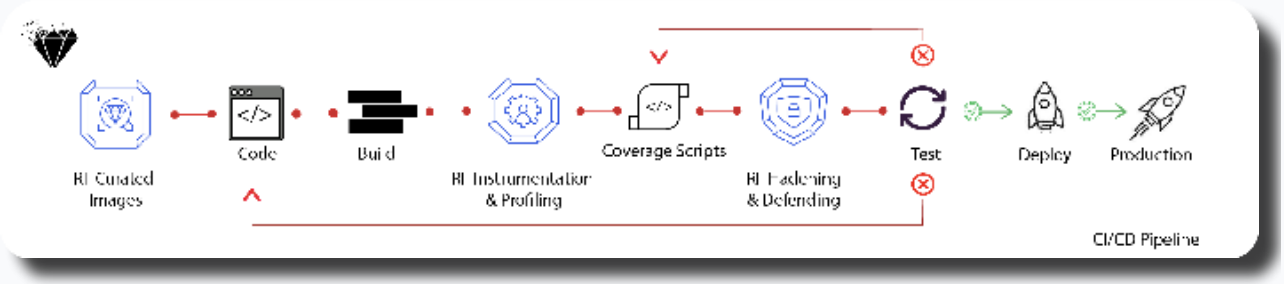
RAPIDFORT

RF Hardening & Defending - RunTime Protection Tools

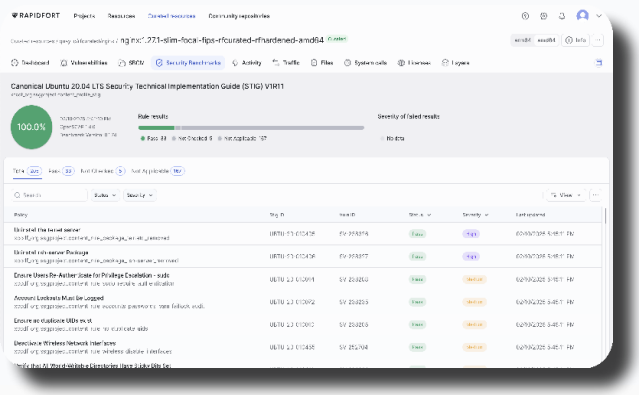
See exactly what's running in the execution path, instantly pinpoint unusual behaviors, and make informed decisions with Runtime Protection.

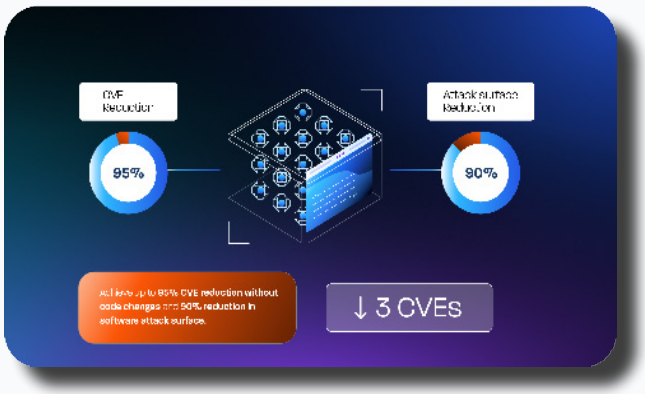
With Runtime Protection, security teams can filter out and pinpoint vulnerabilities that lie within the application's execution path and automatically eliminate the CVEs hanging out in zombie code. The result? A 60-90% reduction in vulnerabilities and software attack surface size.

RF Hardening and Defending tools automatically profiles container behavior, learning and identifying unused or vulnerable components. With a single click, it removes or remediates unnecessary elements, transforming an unsecured container in the CI/CD pipeline into a hardened, secure one. Users have full control over the hardening process, with the ability to remove all critical vulnerabilities or selectively keep/exclude specific files and directories. This automated approach streamlines security while ensuring optimized and efficient container deployments while deep binary scanning enhances security beyond metadata inspection.



Integrated support for CIS and STIG benchmarks enhances security compliance, while the RapidFort advisory system intelligently filters noise, allowing teams to focus on the most relevant threats. These features streamline security workflows, helping organizations build and deploy secure applications with confidence.





RAPIDFORT

Get crystal clarity in runtime

Deploy Runtime Protection in minutes and immediately receive scan results on all of your running containers. See the big picture, zoom in on what's critical, and ignore the CVEs that don't matter.

- See your runtime execution path
- Prioritize with precision using runtime intelligence

Baseline activity with runtime intelligence

Runtime Protection composes a baseline of container activity that will inform your optimization and remediation strategy. It'll also immediately detect unusual software usage and protect your production infrastructure with meaningful, actionable alerts.

- Lower your compute overhead to less than 1%
- Remediate on your terms with baseline data
- Shift the conversation from CVEs to code quality

Secure and harden workloads

Remove 60-95% of your total vulnerabilities in a day. Automatically secure all of your unused components and shrink your software attack surface – without burdening dev teams. RapidFort will immediately detect unusual software usage and protect your production infrastructure with meaningful, actionable alerts.

- Eliminate up to 95% of your patch backlog – instantly
- Harden your containers automatically
- Future-proof your CVEs
- Secure third party software

"RapidFort's Runtime Protection toolset is rethinking a massive and timely problem that cybersecurity teams face: CVE remediation. Instead of chasing enormous patch backlogs, shipping late, etc, companies will be able to focus only on the vulnerabilities that lie within their applications execution path and let RapidFort secure the rest."

Philip Martin, CSO Coinbase

Partners

aws Google Cloud Microsoft carahsoft

Integrate RapidFort directly into your existing workflows

Nessus vulnerability scanner · Jira · harness · circleci · slack · GitLab · sumo logic · Twistlock · PRISMA · aqua · splunk> · CROWDSTRIKE · Jenkins · snyk

Start your trial today

Learn more about our new capabilities at www.rapidfort.com

RAPIDFORT