RAPIDFORT

DATASHEET

# RapidFort Runtime

## Continuous Threat Elimination for Live Production Environments

Know exactly what is running live in production. Detect what changes. Identify and address new risks before they become incidents. RapidFort Runtime extends software supply chain security beyond build, deployment, and static monitoring into live production environments.

## The Runtime Security Gap

Nearly all existing software supply chain security tools stop at deployment. But production environments do not remain static. New CVEs are disclosed hourly, packages are updated, processes change, dependencies are downloaded, and unauthorized modifications can occur after software has passed its original security checks.

- Software may become vulnerable immediately after deployment.
- Static SBOMs quickly become outdated.
- Security and DevOps teams must manually determine whether new CVEs affect production.
- Unauthorized package, binary, or behavioral changes can go undetected.
- Audit teams lack definitive evidence of what is actually executing.

## Key Capabilities

- ✓ Continuous CVE Monitoring
- ✓ Dynamic Runtime Bill of Materials
- ✓ Runtime Tamper Detection
- ✓ Actionable Mitigation Recommendations
- ✓ Evidence-Based Runtime Profiling

## How RapidFort Runtime Works

**Establishes a runtime baseline**
RapidFort identifies approved packages, libraries, binaries, processes, and behaviors within the production environment.

**Observes actual execution**
Lightweight agents use BPF and ptrace technology to capture evidence of what software is truly running.

**Generates a dynamic RBOM®**
The platform continuously creates an accurate inventory of executing software and runtime dependencies.

**Monitors CVEs and environmental changes**
RapidFort correlates newly disclosed vulnerabilities with deployed software and detects unexpected changes.

## Business Benefits

### Reduce Vulnerability Noise

Prioritize vulnerabilities using evidence of actual runtime execution rather than relying solely on static package inventories, SBOM snapshots, or theoretical exposure.

### Eliminate Manual CVE Correlation

Continuously correlate new vulnerability disclosures with live production software instead of requiring teams to manually review every new CVE.

### Detect Unauthorized Changes

Identify modifications to packages, libraries, processes, and behaviors that could indicate tampering, drift, or compromise.

### Improve Audit Readiness

Generate dynamic RBOM®s and verifiable runtime evidence to support compliance, security reviews, and software integrity requirements.

## Why RapidFort

- End-to-end protection from software intake through live production
- Dynamic, audit-ready RBOM® generation
- Reduced false positives and vulnerability noise
- Continuous monitoring of newly disclosed CVEs
- Runtime tamper and integrity monitoring
- No code changes or proprietary platform migration required

> *"Maintaining an accurate, real-time inventory of what is actually executing in production has been a consistent audit and compliance hurdle. RapidFort Runtime's ability to generate a precise, dynamic RBOM® provides us with undeniable evidence of our software's state. We can now verify integrity and confirm our compliance in real time, which is a total game-changer for our security operations."*

SD **Sangram Dash**
CISO and Vice President of IT, Sisense

RAPIDFORT

## See RapidFort Runtime in Action

Up to 99.9% reduction in CVE exposure with RapidFort hardened software. Request a Demo at RapidFort.com.

Request a Demo ↗

www.rapidfort.com | sales@rapidfort.com

440 N Wolfe Rd, Sunnyvale CA 94085

RapidFort, RAPIDFORT, and RBOM® are registered trademarks of RapidFort, Inc.