RAPIDFORT

WHITEPAPER

Optimize and Secure Your Cloud

Reducing your attack surface for stronger security and a simplified path to FedRAMP compliance.

CLOUD SECURITY | FEDRAMP | SBOM MANAGEMENT



© 2026 RapidFort, Inc. | www.rapidfort.com

01 Executive Summary

The Cost of Unused Software

Modern cloud applications often carry excess weight in the form of unused software components. These components linger because of "what if" scenarios or a lack of visibility into how software is actually used in production. This is especially true for open source software, which makes up a significant share of modern applications. Attackers exploit these very components to gain access to systems, often without being detected.

Traditional vulnerability scanning and patching are important, but they are time-consuming and disruptive on their own. Manually identifying and removing unused components takes valuable time away from developers who could otherwise focus on building and shipping software.

85%
of enterprise software is open source

Up to 90%
reduction in software attack surface

Up to 99.9%
of vulnerabilities eliminated within hours

02 The Challenge

The Software Attack Surface: A Security Blind Spot

Think of the software attack surface as the sum of all potential entry points for unauthorized access within an application. Unlike the network attack surface, which forms the digital perimeter, the software attack surface resides inside the code itself.

- **More code = more risk.** Reducing it matters because more code means more potential vulnerabilities, both known and unknown.
- **Network security has well-established practices,** but software attack surface reduction remains a challenge for many organizations, particularly those pursuing FedRAMP compliance
- **FedRAMP mandates strict security controls,** and an oversized software attack surface works directly against those requirements.

03 How It Works

How RapidFort Reduces Risk Across the Lifecycle

RapidFort spans the full software lifecycle, from intake through build to runtime, to eliminate vulnerabilities at the source and continuously reduce the attack surface.

RapidFort Curated Images

- Tens of thousands of near-zero CVE images across Ubuntu, Debian, Red Hat, and Alpine
- Hardened to NIST 800-70 and FIPS 140-3 validated
- Pre-hardened images reduce attack surface from day one
- Aligned with FedRAMP vulnerability management requirements

RapidFort Analyzer and Optimizer

- Analyzer generates a full SBOM and identifies real CVE exposure
- Optimizer removes unused components to reduce the attack surface
- Eliminates vulnerabilities that would otherwise persist in the build

RapidFort Profiler and Continuous Compliance

- Profiler generates RBOM®, showing what actually runs in production
- Continuous Compliance compiles security benchmarks into audit-ready evidence
- Supports FedRAMP, NIST, and other compliance frameworks

Together, this approach can **eliminate up to 99.9% of vulnerabilities within hours** and reduce the attack surface by **up to 90%**, without code changes, significantly reducing the compliance burden associated with FedRAMP.

04 Key Benefits

Key Benefits for FedRAMP Compliance and Beyond

Reduced vulnerability risk

Pre-hardened containers and ongoing attack surface reduction address FedRAMP's vulnerability management requirements directly.

Improved developer productivity

Developers can build on pre-hardened images, freeing them to focus on core application logic rather than chasing vulnerabilities.

Smaller, faster deployments

A reduced workload size supports faster deployments and helps streamline FedRAMP compliance package updates.

Continuous security

Ongoing workload optimization supports a continuously improving security posture, a core part of maintaining FedRAMP compliance.

RapidFort supports FedRAMP compliance by reducing the attack surface, prioritizing vulnerabilities based on real exploitability, streamlining patch management, and providing pre-hardened containers with near-zero vulnerabilities from the start.

05 Additional Capabilities

Optimizing and Securing Your Cloud with RapidFort

Beyond its core capabilities, RapidFort offers additional functionality that streamlines FedRAMP compliance and strengthens overall cloud security.

SBOM management

RapidFort Analyzer generates a software bill of materials for each deployment. SBOMs are a core FedRAMP requirement, providing a detailed inventory of the software components used within an application.

Context-aware vulnerability management

RapidFort prioritizes vulnerabilities using an exploit-aware prediction score (EPSS) based on what actually runs in production, using RBOM® to separate real, exploitable risk from theoretical CVE noise. This focus on in-use components supports FedRAMP requirements while avoiding wasted effort on vulnerabilities in code that is never executed. In addition, RapidFort Continuous Compliance also provides a CISA BOD 26-04 aligned dashboard that prioritizes vulnerabilities accordingly.

Continuous workload optimization

RapidFort Optimizer continuously identifies, removes, and hardens unused components, freeing up developer time and helping maintain consistent security across every deployment.

DevOps integration

RapidFort integrates with existing DevOps tools and workflows, minimizing disruption and allowing teams to adopt stronger security practices within the environments they already use.

Reporting and audit trails

RapidFort Continuous Compliance compiles detailed reports and audit trails documenting an organization's security posture, supporting compliance audits and demonstrating an ongoing commitment to security best practices.

06 The RapidFort Advantage

Security and Compliance, Simplified

In an increasingly complex cloud environment, achieving FedRAMP compliance can be a significant undertaking. Traditional vulnerability management and manual attack surface reduction are time-consuming and resource-intensive. RapidFort offers an approach that streamlines this process and delivers meaningful benefits.

Faster path to FedRAMP compliance

RapidFort accelerates the compliance journey by continuously reducing the attack surface from the outset.

Improved security posture

Curated, pre-hardened containers and ongoing attack surface reduction lower vulnerability risk without requiring code changes.

Stronger developer productivity

RapidFort frees developers from manual vulnerability management tasks so they can focus on core application development.

Lower infrastructure costs

Smaller, leaner deployments support reduced infrastructure costs and improved operational efficiency.

KEY TAKEAWAYS

- Reduces attack surface by **up to 90%**, without code changes
- Eliminates **up to 99.9%** of vulnerabilities within hours
- Generates FedRAMP-ready SBOMs and **audit evidence automatically**
- Integrates with existing **DevOps pipelines** — no workflow disruption

RAPIDFORT

ABOUT RAPIDFORT

RapidFort is the leader in Software Supply Chain Security, enabling organizations to eliminate risk across their software stack at scale. Its platform combines hardened near-zero CVE container images, runtime profiling, and attack surface management to remove up to 99.9% of vulnerabilities within hours and reduce the attack surface by up to 90%, without code changes. RapidFort appears in the inaugural Gartner® Magic Quadrant™ for Software Supply Chain Security and is a Gartner® Cool Vendor™ and Nutanix Global Cloud Native Partner of the Year.

© 2026 RapidFort, Inc.

Eliminate attack vectors at the source

Schedule a Call ↗

www.rapidfort.com | sales@rapidfort.com