RAPIDFORT

WHITE PAPER

Software Supply Chain: Your Path to Zero CVEs

Software Supply Chain: Your path to Zero CVEs

The software supply chain faces a growing array of sophisticated threats that put critical government systems and national security at risk. “Adversaries are exploiting the entire development pipeline, including open-source dependencies, Continuous Integration and Continuous Delivery/Deployment environments, and third-party integrations. In fact, based on the latest DBIR report from Verizon, exploitation of CVEs has become the #1 way breaches are occurring at 24%, even higher than credential abuse (23%),” said RapidFort Chief Strategist, George Manuelian.

The Open Source Security Foundation reports that 70 percent of all software today is open source, and that 82 percent of those components are inherently risky due to poor maintenance, outdated code, or Common Vulnerabilities and Exposures (CVEs). Two independent reports confirm a 400% increase in software vulnerability exploits.

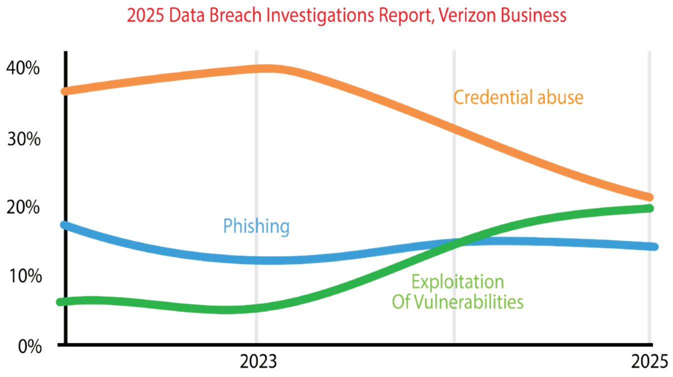
> **“To effectively secure the modern software supply chain, developers need a comprehensive, secure-by-design platform that proactively automates vulnerability remediation across both first-party and third-party containerized applications — throughout the entire software development lifecycle.”**
> - George Manuelian, Chief Strategist at RapidFort

The Current Landscape

Contemporary adversaries have evolved beyond targeting deployed applications to focus on compromising the software development lifecycle itself. Attack vectors now encompass the entire pipeline from source code repositories through build systems to deployment infrastructure. The Open Source Security Foundation’s analysis reveals that these attacks exploit vulnerabilities in open-source dependencies, compromise Continuous Integration and Continuous Delivery environments, and infiltrate third-party integrations that are often overlooked in traditional security assessments.

The emergence of AI-assisted development tools has introduced additional complexity to the threat landscape. Cybercriminals are increasingly targeting the infrastructure used to develop and train machine learning models, creating novel attack vectors that traditional security frameworks were not designed to address. This evolution represents a fundamental shift in adversary tactics, moving from reactive exploitation of known vulnerabilities to proactive compromise of development infrastructure. What used to take bad actors months to find vulnerabilities in production software now takes minutes with the help of AI and automation.

Verizon’s 2025 Data Breach Investigations Report documents this evolution, noting that software vulnerabilities have transitioned from occasional incidents to systematic exploitation patterns that create widespread organizational impact. For defense organizations, these compromises can result in breaches of mission-critical systems, exposure of classified information, disruption of essential services, and degradation of operational readiness capabilities.



A New Approach

What's needed is a fundamental shift in how security is integrated into the software development process, Manuelian said.

Government agencies require a platform that delivers a secure-by-design methodology — "shifting left" by starting with CVE-free open source base images, enabling DevTime protection, and removing all the unused software that bloats applications and harbors hidden vulnerabilities.

To secure software from the start, agencies must use container images that are regularly patched and hardened — free of known vulnerabilities (CVEs), based on well-trusted LTS (Long Term Support) distributions like Ubuntu and UBI. These "Curated Open Source Images" are also hardened by stripping excess, unused code, minimizing the software attack surface. They need DevTime tools that accurately scan, analyze, and minimize false positives while generating actionable insights such as a Runtime Bill of Materials (RBOM).

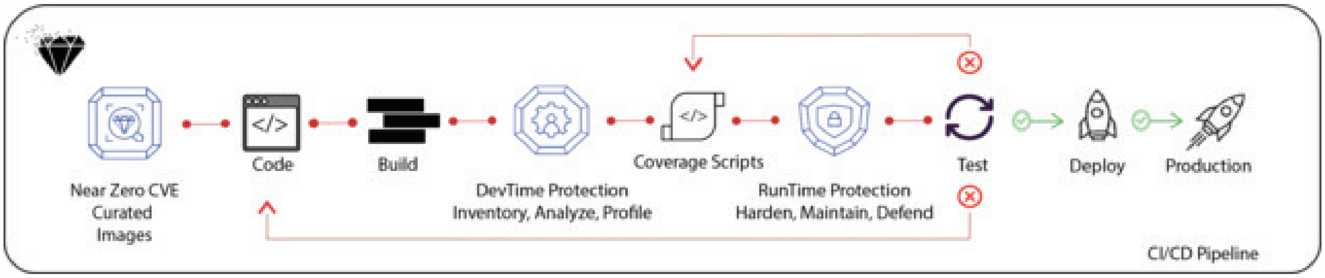
Finally, to maintain security in production, agencies must continuously monitor and harden containers at runtime, reducing software bloat with Software Attack Surface Management (SASM) and enforcing security and compliance policies.

The right platform delivers real-time security feedback and policy enforcement within CI/CD pipelines, without disrupting velocity, along with deep, continuous visibility into which components are actually used at runtime.

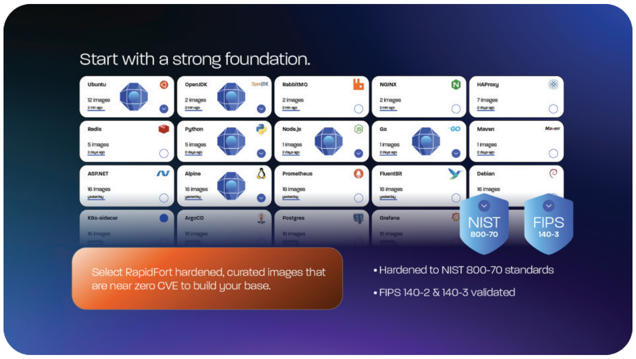
In short, it eliminates vulnerabilities before they're exposed by combining CVE-free, hardened images and developer-focused tooling both in DevTime and runtime. This proactive approach ensures software supply chain security from build to deploy.

How RapidFort Helps

A comprehensive solution requires fundamental changes to how security is integrated into the software development lifecycle. The secure-by-design approach addresses these challenges through three primary technical components that work together to reduce vulnerability exposure throughout the application lifecycle.


Near Zero CVE Curated Images
Code
Build
DevTime Protection Inventory, Analyze, Profile
Coverage Scripts
RunTime Protection Harden, Maintain, Defend
Test
Deploy
Production
CI/CD Pipeline

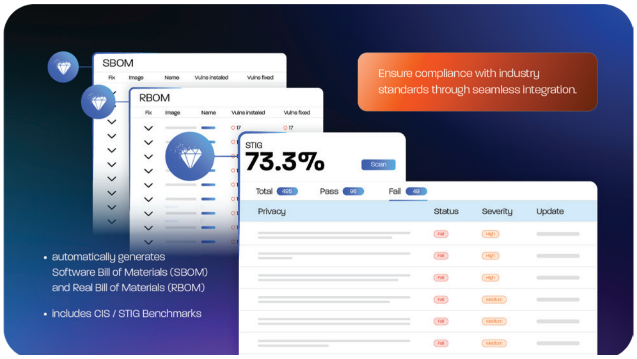
The first component focuses on curated container image management, where base images are continuously maintained with the latest security patches and hardened configurations—aligning with best practices for compliance frameworks such as FedRAMP, CMMC, SOC 2, and NIS2. These images must also conform to FIPS and NIST standards and be benchmarked against STIG and CIS guidelines.


Start with a strong foundation.

Select RapidFort hardened, curated images that are near zero CVE to build your base.

- Hardened to NIST 800-70 standards
- FIPS 140-2 & 140-3 validated

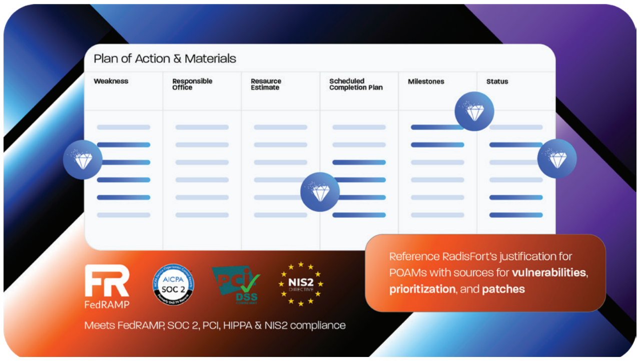
Regular vulnerability assessments are conducted, and updates are applied proactively rather than reactively. Unused packages and unnecessary system components are systematically removed to reduce the attack surface. This approach ensures applications start from a secure foundation, rather than inheriting vulnerabilities from upstream dependencies.



Ensure compliance with industry standards through seamless integration.

- automatically generates Software Bill of Materials (SBOM) and Real Bill of Materials (RBOM)
- includes CIS / STIG Benchmarks

The second component integrates security assessment directly into the development pipeline through enhanced CI/CD tooling. Rather than treating security as a separate workflow, vulnerability scanning and policy enforcement become integral parts of the build and deployment process. This integration provides developers with immediate feedback on security issues while maintaining development velocity. Advanced scanning techniques reduce false positive rates by analyzing actual dependency usage patterns and runtime behavior rather than simply cataloging installed packages.



Reference RadisFort's justification for POAMs with sources for **vulnerabilities**, **prioritization**, and **patches**

Meets FedRAMP, SOC 2, PCI, HIPPA & NIS2 compliance

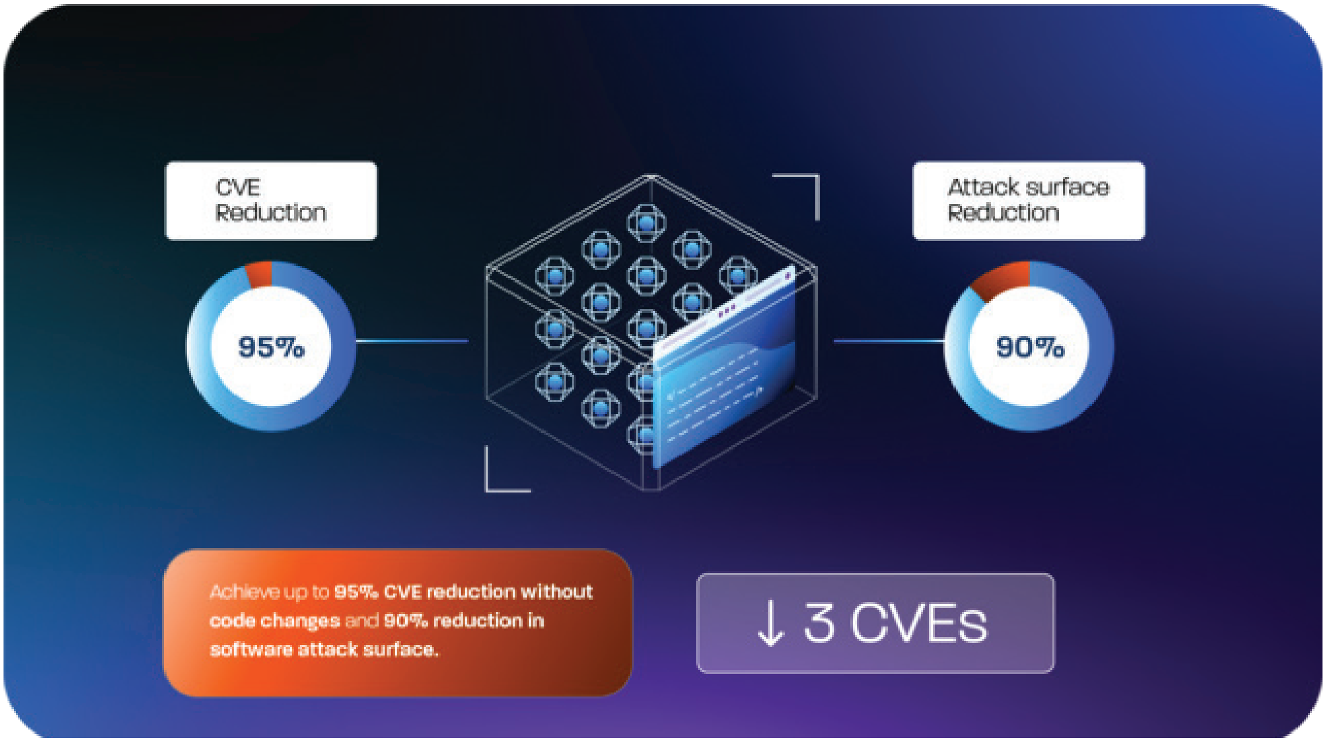
The third component implements runtime attack surface management through continuous monitoring of deployed applications. This approach provides visibility into which components are actually executed in production environments, enabling security teams to prioritize vulnerabilities based on real exploitation risk rather than theoretical exposure. Runtime analysis also enables detection of anomalous behavior patterns that may indicate compromise attempts or successful breaches.

Going forward

Technical implementation of secure-by-design principles requires careful coordination between security, development, and operations teams. The initial phase involves comprehensive assessment of existing development toolchains, container registries, and deployment infrastructure. This assessment identifies current vulnerability exposure levels, evaluates existing security tool effectiveness, and maps dependencies between different components of the software supply chain.

The integration phase focuses on embedding security controls into existing development workflows without disrupting established processes. Container image curation involves establishing automated pipelines for base image updates, implementing security scanning at build time, and creating governance processes for managing third-party dependencies. CI/CD integration requires configuring security policy enforcement points, establishing vulnerability threshold criteria, and implementing automated remediation workflows where possible.

Runtime protection implementation involves deploying monitoring agents across production environments, configuring behavioral analysis rules, and establishing incident response procedures for detected anomalies. The system generates Runtime Bills of Materials that provide precise visibility into actual component usage, enabling security teams to focus remediation efforts on actively exploited vulnerabilities rather than comprehensive patch management across all installed components.


CVE Reduction
95%
Attack surface Reduction
90%
Achieve up to 95% CVE reduction without code changes and 90% reduction in software attack surface.
↓ 3 CVEs

www.rapidfort.com

RAPIDFORT