RAPIDFORT

SOLUTION BRIEF

Trusted Image Bundle for AI

Secure your AI stack with zero and near-zero CVE images and vetted libraries

Harden the open source beneath your AI workloads and applications with near-zero CVE, FIPS-validated, and STIG-hardened images and vetted libraries, **with no code changes**.

NVIDIA CUDA | AMD ROCm | PyTorch | vLLM | Kubernetes | PyPI | NeMo RL

More than 90% of an AI application is designed with open source software. These software images and code contain and inherit significant numbers of security vulnerabilities which must be patched prior to production. Bloated GPU and ML framework images pass inherited CVEs downstream and vulnerability scanner findings are growing 140% each year. Transitive PyPI, npm, and Java dependencies let malicious, typosquatted, and tampered packages slip into AI builds unreviewed. At the same time FedRAMP, ATO, CMMC, and CRA reviews demand FIPS crypto, STIG hardening, and SBOMs that often take months to assemble.

Organizations building AI applications and large language models need a way to start fast and safe. Their time needs to be spent on quickly developing new applications and not fixing or patching underlying software.

RapidFort Image Bundle for AI includes zero and near-zero CVE images for the full AI stack, rebuilt daily on published patch SLAs. The bundle also includes curated libraries for PyPI, npm, and Java, vetted for malware, tampering, and secrets. It includes options for FIPS-validated, STIG-hardened images on standard distros, shipped with SBOM, STIG, and CVE reports.

NEAR-ZERO CVE · VETTED

01 Source and intake
Signed images · vetted libraries

→

02 Build or train
CI · CLI · analyze & optimize · attestation

→

03 Deploy and serve
Kubernetes · GPU clusters · profiling · runtime analyzer

→

04 Audit and operate
ATO · FedRAMP · CRA reviews · STIG · CycloneDX JSON/XML · advisories · POA&Ms

Teams implement the RapidFort Image Bundle for AI with **a one-line FROM change** in existing Dockerfiles, pipelines and registries, while security teams are able to verify signatures and SLSA provenance.

The result is that AI development teams are able to ship models or features on a near-zero CVE foundation, with no code changes. Security and compliance teams get signed provenance and audit evidence for every image.

KEY CAPABILITIES

Full AI stack coverage
Near-zero CVE minimal images for NVIDIA CUDA, AMD ROCm, PyTorch, TensorFlow, Triton, vLLM, and Kubernetes cluster components.

Drop-in replacement images
Pin-for-pin replacements on Ubuntu, Debian, Red Hat, and Alpine, adopted with a one-line FROM change.

Curated Libraries
PyPI, npm, and Maven packages checked for malware, tampering, and secrets.

Verifiable compliance evidence
Cosign signatures, SLSA provenance, and SBOM, CVE reports for each image, and DISA-supported STIG.

Runtime-aware optimization
RapidFort Profiler (RBOM®) maps what your workload runs, and Optimizer removes the components it never uses.

COMMON USE CASES

01 Clear ATO for mission AI
Iron Bank approved, DISA validated, FIPS 140-3 images with per-image evidence cut roughly 3 months from ATO timelines.

02 Shorten security reviews
SaaS and AI-native teams answer FedRAMP and SOC 2 reviews with per-image SBOM, STIG, and CVE evidence.

03 Standardize training and inference foundations
Give every training and inference team the same near-zero CVE CUDA, ROCm, PyTorch, and vLLM base images.

04 Vet dependencies in AI-generated code
Route pip, uv, and Poetry through Curated Libraries so dependencies added by AI-generated code are vetted before install.

05 Stay on pinned versions
Keep the exact CUDA, framework, and runtime versions your models need, with older and minor versions patched.

STANDARDS AND PROGRAMS SUPPORTED

The bundle includes the validations and evidence that regulated AI programs request during audits.

- ✓ FIPS 140-3
- ✓ Distroless
- ✓ STIG
- ✓ Benchmarks
- ✓ NIST 800-70
- ✓ Iron Bank
- ✓ DISA validated
- ✓ SLSA
- ✓ FedRAMP
- ✓ EU CRA

Works alongside your existing scanners, CI/CD tools, registries, and cloud platforms.

OUTCOMES

Smaller attack surface
Up to 90% less attack surface to defend.

Developer velocity
Ship 2 to 3 weeks sooner with about 60% less remediation effort.

Faster authorization
Up to 30% faster compliance, roughly 3 months off ATO.

Supply chain trust
Malicious and tampered packages stopped before your pipeline.

No lock-in
Keep your distros, pipelines, and tooling; return upstream anytime.

SUMMARY

RapidFort Image Bundle for AI replaces the roughly 90% of your AI stack that is open source with **zero and near-zero CVEs, compliance-ready images and vetted libraries**, so your teams ship the safest models and features without code changes.

RAPIDFORT

About RapidFort

RapidFort leads Software Supply Chain Security with the largest distribution of curated, genuinely open-source software. Its platform combines near-zero CVE minimal container images, runtime profiling, attack surface management, and the first independently malware-scanned open-source images on common Linux distributions. RapidFort appears in the inaugural Gartner® Magic Quadrant™ for Software Supply Chain Security and is a Gartner® Cool Vendor™ and Nutanix .NEXT Partner of the Year.

Up to 99.9%
VULNERABILITIES ELIMINATED WITHIN HOURS

Up to 90%
ATTACK SURFACE REDUCED, NO CODE CHANGES