



Rethinking Container Builds for Security and Scale

The tradeoffs of building versus adopting secure containers



Executive Summary

The enterprise container security imperative shapes modern infrastructure decisions. Building custom Golden Docker images offers maximum control and customization but requires significant investment in expertise and ongoing maintenance. Cleanstart Distroless images provide enterprise-grade security with minimal operational overhead, daily nano-patching, and compliance ready automation turning container security from a persistent risk into a strategic advantage.

Organizations can expect 3-year TCO ranging from \$600K–\$1.45M for building Golden images depending upon the distinct images.

The decision fundamentally hinges on whether your organization values control and customization over rapid deployment and guaranteed security outcomes. With data breaches averaging \$4.88M in 2024 and container vulnerabilities representing a primary attack vector, this choice has profound implications for enterprise security posture and operational efficiency.

Golden Docker Images: Standardization with Significant Investment

Golden Docker images are standardized, pre-configured container templates serving as foundational baselines for all containerized applications within an enterprise. These intentionally configured snapshots contain:

- 1 Hardened operating systems
- 2 Common runtime dependencies
- 3 Monitoring agents
- 4 Security tools
- 5 Enterprise-specific configurations



Key Benefits

Organizations create Golden images to achieve:

- ① Standardization across environments
- ② Organization wide security controls
- ③ Regulatory compliance requirements
- ④ Reduced deployment complexity

Implementation Requirements

01 **Technical Infrastructure:**
Docker Engine/BuildKit, Packer, Ansible/Chef/Puppet, vulnerability scanners (JFrog Xray, Snyk, Twistlock)

02 **Staffing:**
Medium enterprises require 5–7 platform engineers, 5 security engineer, 3–5 DevOps engineers; large orgs may need 35–50 specialists

03 **Maintenance Burden:**
Aggressive patching schedules with immediate response for critical CVEs and monthly cycles for regular updates

CleanStart Distroless Images: Security Excellence Through Managed Simplicity

CleanStart Distroless offers minimal, hardened container images achieving near-zero CVEs through daily automated rebuilds. Built on a purpose-built Linux “undistro,” these images contain only the essential software required to run applications.

Key Features

- 1 No shells, package managers, or unnecessary OS components
- 2 Up to 90% reduction in attack surface
- 3 Application compatibility maintained
- 4 Industry-leading SLAs with 7-day remediation for critical CVEs

Security Advantages

- 1 **Vulnerability Management:**
Daily nano-patching, backporting for older versions, 77% fewer CVEs
- 2 **Compliance Ready:**
FIPS 140-3, SLSA Level 4, automated SBOMs (no “NOASSERTION” entries), cryptographic provenance tracking, full RBI/DORA alignment

Operational Efficiency

- 1 Images shrink by 75–98% (1.9–150MB)
- 2 80–95% faster pull/start times (1–10s pull, 0.5–2s startup)
- 3 70–90% less memory (10–50MB baseline)
- 4 3–5x faster CI/CD pipelines
- 5 Run 5–10x more containers per node
- 6 25–40% cost reduction through optimized resource use and fewer security incidents

Customer Success Stories

- 1 BFSI sector reports 30–50% reduction in downtime and deployment failures
- 2 Up to 90% reduction in attack surface
- 3 Application compatibility maintained
- 4 Industry-leading SLAs with 7-day remediation for critical CVEs

Security and Performance Comparison

CleanStart Distroless offers minimal, hardened container images achieving near-zero CVEs through daily automated rebuilds. Built on a purpose-built Linux “undistro,” these images contain only the essential software required to run applications.

Aspect	Golden Images	CleanStart Distroless
Attack Surface	200+ packages; shells, package managers	3–30 packages; no shells or package managers
Active CVEs	21–50 typical	0–3 via daily rebuilds
Image Size	1.2GB+ (Python example)	1.9–150MB (75–98% smaller)
Startup Times	2–5s	0.5–2s (80–95% faster)
Memory Usage	150–300MB baseline	10–50MB baseline (70–90% less)
CI/CD Pipelines	Slower, complex	3–5x faster pipelines
Containers per Node	Moderate density	5–10x more containers per node
Compliance	Manual SBOM; partial RBI/DORA alignment	Automated SBOM; full RBI/DO-RA alignment

Return of investment

Cleanstart ROI Analysis - Enterprise

Current Annual Costs		with CleanStart	
Security & Dev Teams :	Compliance & Audits :	CleanStart Solutions :	Streamlined Deployment :
\$1.3M	\$300k	\$250k	\$60k
Tools & Infrastructure :	Deployment Delays :	Reduced Team Costs :	Infrastructure :
\$450k	\$600k	\$195k	\$100k
Emergency Patching :		Automated Compliance :	
\$300k		\$45k	
Total : \$3.05M		Total : \$650K	

Annual Savings: \$2.4M (78.7%)

85% Time Savings
Faster Security Reviews

70% Cost Reduction
Lower Operating Costs

685% 3-Year ROI
Return on Investment

25-40% Cost Reduction
Optimized Resource use

Additional Benefits



Reduced security breach risk



Enhanced Compliance Posture



Improved developer Productivity



Faster time to market

Transforming Container Image Security

From Public uncertainty to Enterprise Control

Traditional Public Registry	CleanStart Private Registry
✗ Limited Visibility into image contents.	✓ Complete transparency & visibility
✗ No control transparency & standards	✓ Full control over security posture
✗ Vulnerable dependencies included	✓ Near Zero vulnerabilities
✗ Limited Visibility into image contents.	✓ Controlled, predictable updates
✗ No governance or compliance control	✓ Built-in governance & compliance
✗ Security as an afterthought	✓ Security first approach



These results make one point clear: security and efficiency are no longer separate pursuits. CleanStart’s distroless model converts what was once a costly, manual process into a predictable, automated foundation. The measurable ROI from reduced patching effort to improved compliance and faster releases demonstrates that secure-by-design architectures can directly drive business performance.



Conclusion

CleanStart's engineered framework delivers stronger security outcomes faster while dramatically improving operational efficiency and lowering total cost of ownership. By **shrinking images by up to 98%**, accelerating pull and **start times by 80–95%**, and reducing memory usage by up to **90%**, CleanStart enables organizations to run **5–10× more containers per node** and achieve **3–5× faster CI/CD pipelines**.

Combined with **25–40% cost reduction** through optimized resource use and fewer security incidents, it empowers teams to focus on innovation, not security firefighting. These results make one point clear: security and efficiency are no longer opposing goals. CleanStart's distroless model turns what was once a costly, manual process into a predictable, automated foundation for secure operations.

The decision to build or buy ultimately comes down to priorities: full control versus sustained acceleration. For most enterprises, simplicity, predictability, and measurable impact now outweigh the overhead of maintaining custom images. **CleanStart's distroless framework delivers a secure-by-default foundation**, one that transforms container security from a persistent burden into a strategic advantage.

