CleanStart™

The Real Cost of Public Container Images

Quantifying the security and financial impact of public container use

Executive Summary

The adoption of containers and open-source base images has skyrocketed globally, with over 75% of organizations running containerized applications and more than 30 billion image pulls monthly from public registries. However, this rapid growth exposes enterprises to mounting risks, as public Docker images and open-source dependencies often contain hundreds of known vulnerabilities, outdated components, and hidden malware.

This white paper evaluates the strategic and economic advantages of Cleanstart, a near zero-CVE hardened container image platform designed to reduce the attack surface, simplify vulnerability management, and align with compliance standards like FIPS and SLSA. It presents a comparative analysis between Cleanstart and Docker Hub images, showing the risks of using unverified sources and the costs incurred in fixing vulnerabilities manually.

Highlights include:

- Global container adoption trends and their implications for security
- Quantified vulnerability benchmarks and attack vectors
- Cost of vulnerability remediation and developer resource drain
- Financial savings from automation and hardened image use
- Strategic comparison with DIY golden image initiatives

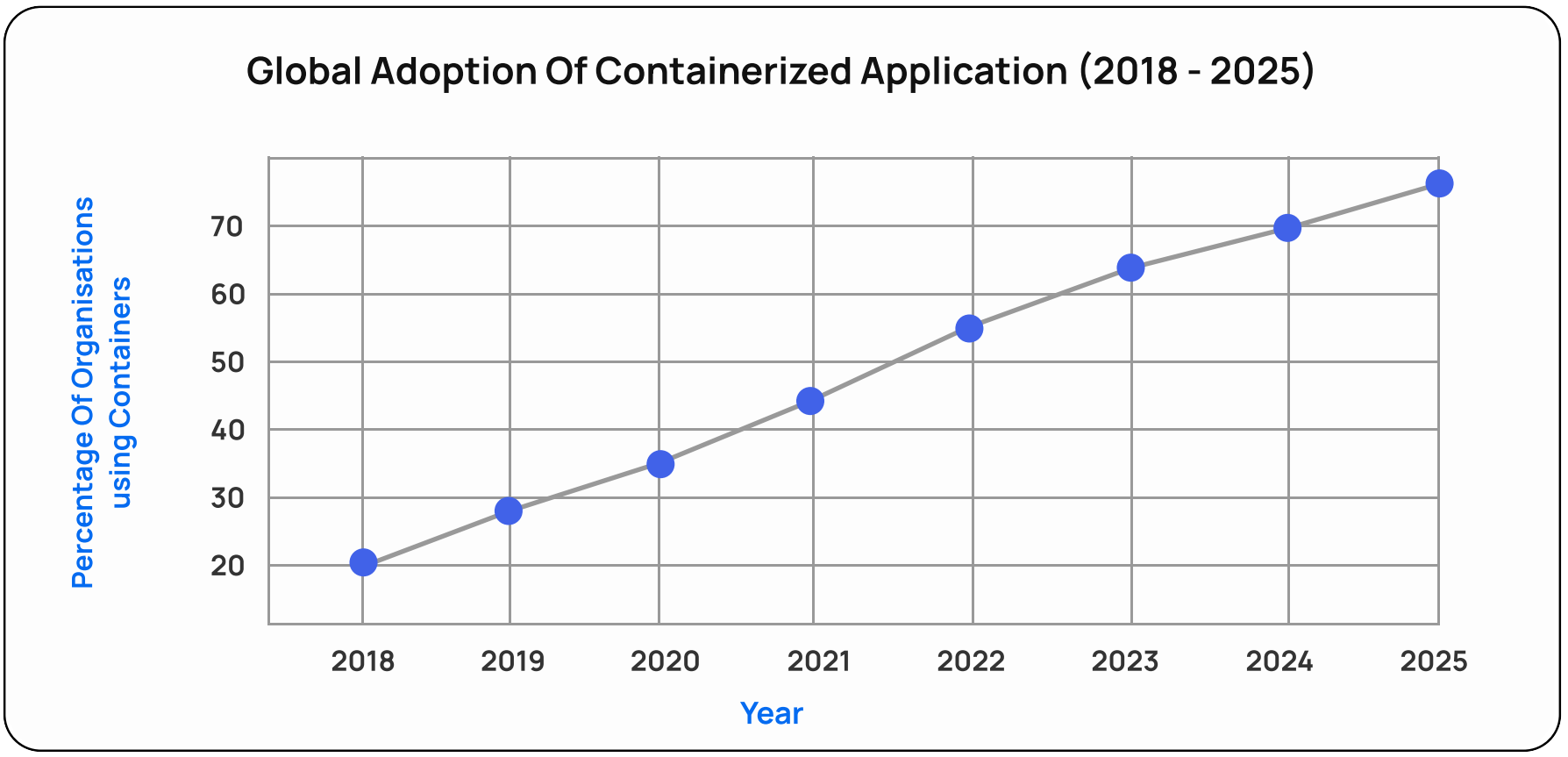
The data shows that Cleanstart can eliminate over 80% of vulnerability triage effort, reduce breach exposure, and offer up to 85% cost savings. For security leaders, Cleanstart is not just a preventive measure—it's an operational advantage for securing modern DevSecOps pipelines.

1.The Problem with Public Images

1.1 Global Container Adoption Trends

The use of containers and open-source container images has surged globally, driven by microservices architectures, Kubernetes adoption, and DevOps scalability demands:

- As of 2025, over 75% of global organizations run containerized applications in production, with over 30 billion container image pulls monthly from public registries.
- Docker Hub, GitHub Container Registry, and similar platforms collectively serve tens of millions of public container images, many of which are unverified or unmaintained.
- The rise in developer reliance on community-maintained images has outpaced the availability of secure, actively maintained alternatives.



Implication

Without hardened base images like CleanStart, the exponential growth of container adoption exposes enterprises to cascading security risks. Each container built from a vulnerable base image can amplify CVE propagation across production clusters. At global scale, even a single overlooked vulnerability in a popular image can trigger multi-tenant breaches, supply-chain attacks, and regulatory non-compliance. The burden of scanning, triaging, and patching grows non-linearly with scale, making it increasingly unsustainable for security teams to keep pace.

As container adoption accelerates, standardizing on near zero-CVE hardened images becomes critical for resilience. CleanStart provides that proactive foundation, enabling secure, scalable, and compliant container growth.

1.2 Hidden Risks in Libraries and Packages

Container images are just one layer. Dependencies pulled from package managers (npm, Maven, PyPI, pip) also introduce serious vulnerabilities:

- **The 2025 JFrog Software Supply Chain report showed that:**
  - 88% of CVEs rated critical were contextually downgraded, but this introduces complexity in correct risk assessment.
  - More than 4.6 million Docker Hub repos contain phishing or malware content.
  - The same study uncovered 6,790 active tokens/secrets embedded in public artifacts—an enormous exposure vector.
- **GitHub's Advisory Database contains:**
  - 20,607 reviewed advisories and
  - 262,857 unreviewed issues across major ecosystems (npm, Maven, PyPI, Go, RubyGems, etc.).

Takeaway

Each image can inadvertently introduce critical vulnerabilities—both from OS components and layered dependencies. Cleanstart's near zero-CVE pre-hardening mitigates these compounded supply chain risks.

Container images from Docker Hub and other public registries suffer from:

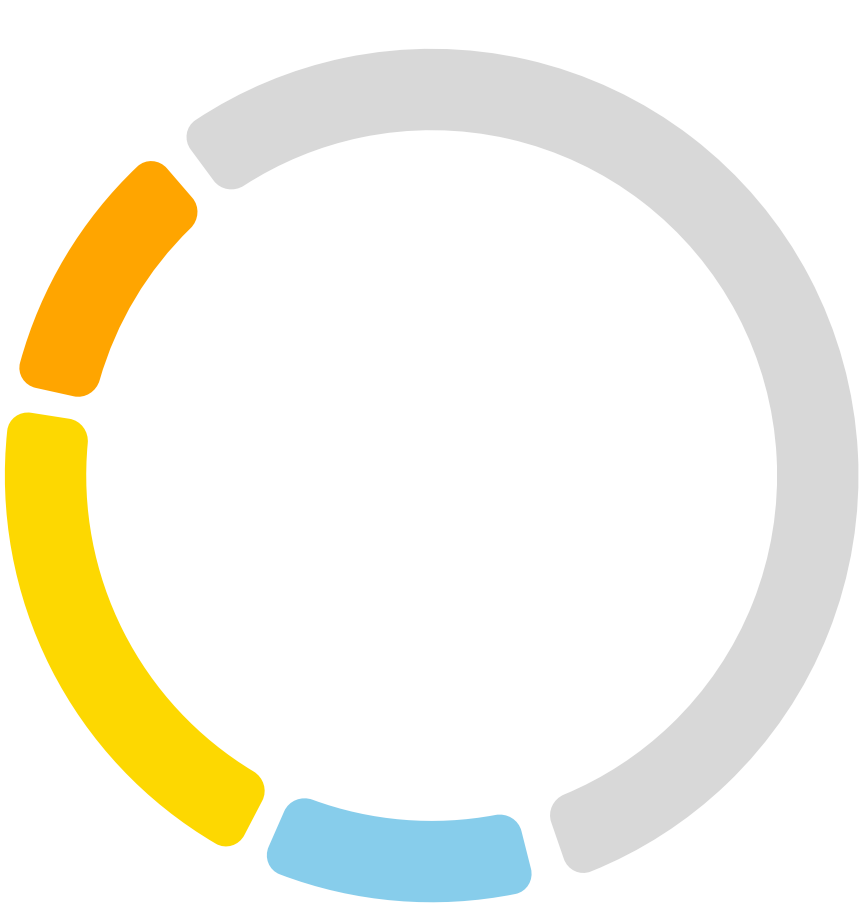
- **High CVE counts**
  Up to 997 vulnerabilities per image (Node.js)
- **Outdated components**
  Poorly maintained base images
- **Hidden malware**
  Potential for compromised uploads
- **Opaque provenance**
  No verifiable SBOMs or signatures
- **Compliance risks**
  Difficulty aligning with FIPS, STIG, and SLSA standards

According to data available as of March 2025:

- Over 51% of Docker Hub images contain critical vulnerabilities
- 87% of production images have critical or high-severity vulnerabilities
- Debian-based official images average ~239 CVEs and updating OS packages only reduces ~6% of them
- Breakdown by severity for public images: - Critical: 0.01% - High: 5.38% - Medium: 21.42% - Low: 8.87%
- 1,300% increase in supply chain attacks over three years

These factors create costly post-deployment risks. Fixing vulnerabilities after deployment leads to downtime, resource drain, and increased breach exposure.

Vulnerability Severity Distribution in Public Container Images (2025)



As container adoption accelerates, standardizing on near zero-CVE hardened images becomes critical for resilience. CleanStart provides that proactive foundation, enabling secure, scalable, and compliant container growth.

2. Cleanstart Advantage

Cleanstart provides

- **Near Zero-CVE images**
  Hardened at build-time, not patched retroactively
- **Compliance-ready images**
  FIPS, STIG, SLSA Level 3 & 4, SBOM (SPDX & Cyclonedx), and signed with Sigstore
- **Developer-ready**
  Accessible via portal or private registry replication
- **85%+ reduction in image size**
  Faster deployments, reduced surface area
- **SLA for CVE remediation**
  - 7 days for Critical CVE
  - 14 days for high/medium/low CVE

Example: Node.js 23.6.0 Image

Metric	Docker Hub	CleanStart
Image Size	1.12 GB	106 MB
Vulnerabilities (Synk)	997	0
Vulnerabilities (Trivy)	2247	0

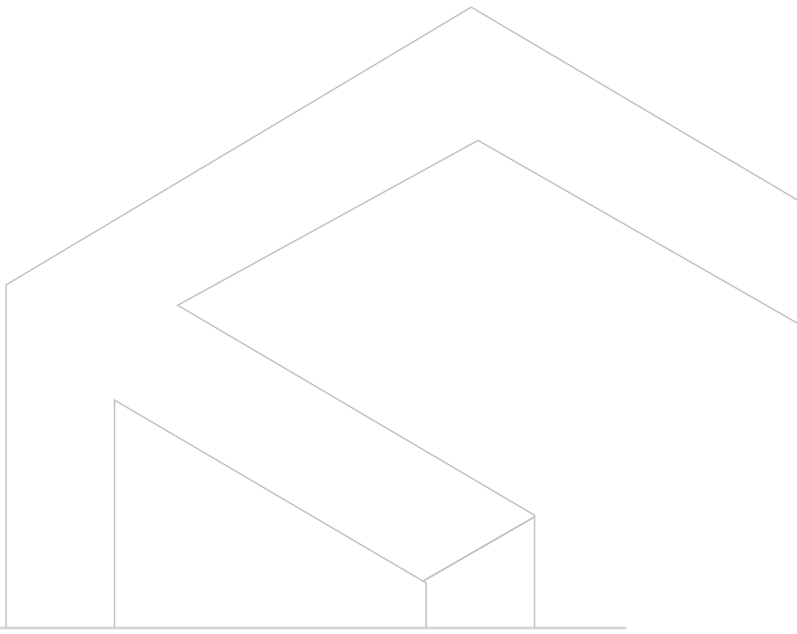
3.Cost-Benefit Analysis

3.1 Real-World Savings from CVE Outsourcing

According to a 2025 industry report on the cost of CVEs:

- **Outsourcing CVE management can yield annual savings of $2.1 million in large enterprises.**
- **Tech-sector companies see savings up to $147K annually, while mid-sized businesses average $327K in cost avoidance.**
- **DIY golden image programs in regulated environments often cost $800K+ per year, factoring in team size, remediation cycles, and compliance tooling.**
- **Firms using hardened image services saved:**
    - $400K+ in image maintenance costs
    - $278K+ in compliance operations
    - $2M+ in engineering effort
- **Business value unlocked across security, compliance, and time-to-market exceeded $30M–$50M in many large organizations, particularly in healthcare and telecom.**

These findings reinforce that Cleanstart offers similar or greater value, especially when scaled across 100+ images in production.



3.1.1 Remediation Costs (per year)

Time and Cost of Addressing Critical and High CVEs

Consider the impact of remediating 1,000 critical or high vulnerabilities manually:

- **Developer time per CVE**
  1 hour
- **Hourly cost of developer**
  $200
- **Total cost for 1,000 CVEs**
  $200,000

With hardened image automation (like Cleanstart):

- 60% automation = 600 CVEs avoided → $120,000 saved
- 80% automation = 800 CVEs avoided → $160,000 saved

Scenario	CVEs Fixed Manually	Hours Saved	Savings
Manual (No Service)	1,000	0	$0
Cleanstart (60% Automation)	400	600	$120,000
Cleanstart (80% Automation)	200	800	$160,000

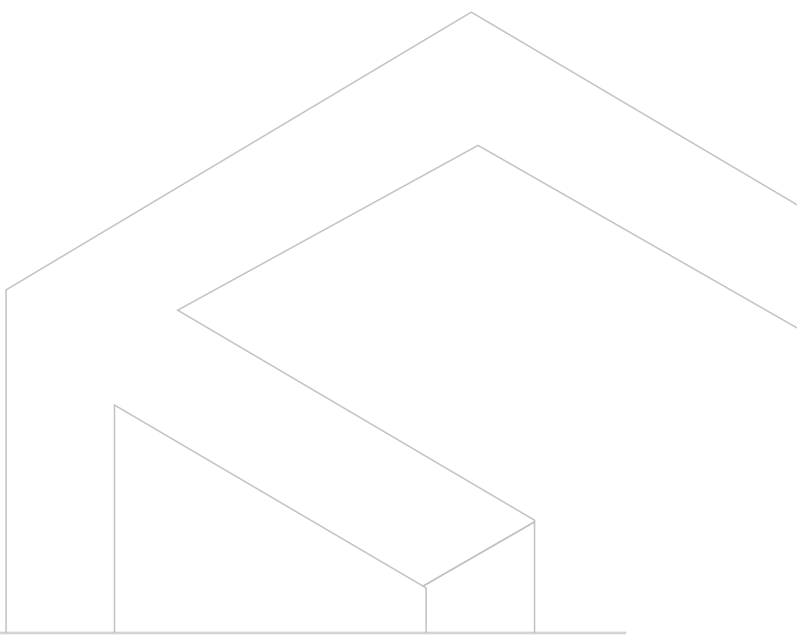
Metric	Docker Hub (100 Images)	Cleanstart (100 Images)
Developers required	4–6	1
Hours/month on CVE management	12,000 hrs	1,000 hrs
Annual DevOps labor cost	~$840,000	~$70,000

3.1.2 Tooling & Infra Overhead

Metric	DIY Golden Image	Cleanstart
Tool licensing & infrastructure	$100K/year	Included
CVE response SLA	24–72 hrs (manual)	7 days (guaranteed)
Training cost per engineer	$5K–$15K/year	Minimal

3.1.3 Breach Risk & Impact

- **Avg. breach cost (2024)**
  $4.88M globally / $9.36M in U.S.
- **Containers as breach vector**
  48% of all software supply chain incidents
- **Potential incidents avoided**
  3–5 per year, savings in millions



4. Why Not Build Internally?

Building your own Golden Images:

- Takes 6–18 months to implement
- Requires a dedicated team of 5–10+ engineers
- Involves constant maintenance, dependency tracking, and patch cycles
- Risks delayed patching and increasing technical debt

4.1 Estimated 3-Year TCO

Option	TCO Estimate (3 Years)
DIY Golden Images	$2.9M
Cleanstart Subscription	$210K–$300K

- Even for mid-size enterprises, Cleanstart is 85% more cost-effective and achieves better security outcomes.

5. Strategic Benefits of Cleanstart

- **Accelerated DevSecOps workflows**
  No delays for image hardening or CVE triage
- **Built-in compliance**
  PCI, NIST, FIPS, STIG
- **Lower operational risk**
  Verified provenance, reproducibility, and supply chain assurance
- **Minimal lock-in risk**
  Cleanstart images integrate with standard CI/CD pipelines
- **Scalability**
  Pre-hardened images scale across teams, regions, and environments

6.Conclusion: Why Security Teams Choose Cleanstart

Security and platform teams today are overwhelmed by patching cycles, vulnerability triage, and compliance workloads. CleanStart removes this burden by providing pre-secured, near zero-CVE images built for scale, enabling teams to focus on application logic rather than base image maintenance.

As public container images continue to expose enterprises to high rates of critical vulnerabilities and mounting operational costs, CleanStart stands out as the secure, scalable, and cost-efficient foundation for modern DevSecOps pipelines. It transforms container security from a recurring operational task into a built-in organizational advantage.

References

- CNCF Annual Survey Report 2024
- Docker, Inc. – Docker Hub Usage Statistics 2024
- Sysdig Cloud-Native Threat Report 2024
- RedHat State of Container Security Report 2024
- Anchore 2024 Software Supply Chain Report
- Software Supply Chain State of the Union 2025
- GitHub Advisory Database
- IBM Cost of a Data Breach Report 2024
- Aqua Nautilus Threat Research 2024