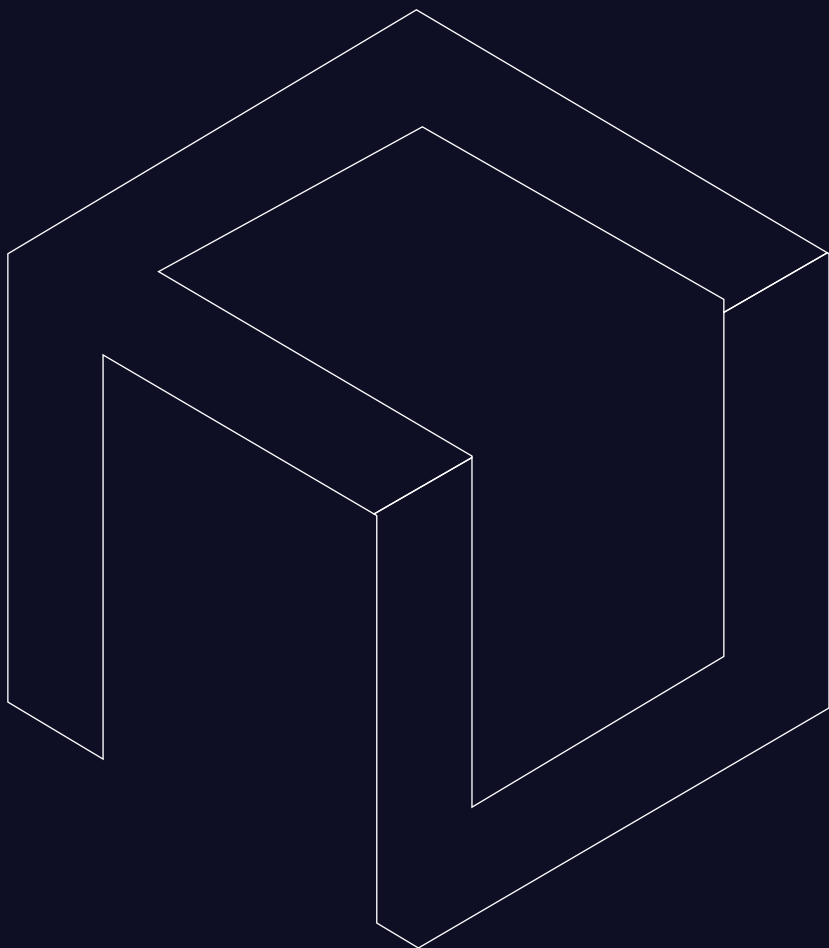
CleanStart™

Enterprise-Grade Hardened Container Images

Simplifying compliance and reducing vulnerability exposure across DevSecOps pipelines.



Executive Summary

Vulnerabilities continue to be a major concern in DevSecOps. The widespread adoption of containers has introduced complexity to this challenge.

Using container images from public registries adds a significant burden of vulnerabilities, which are inherited. If not gated, these vulnerabilities reach production, where remediation costs are significantly higher.

Our meticulously crafted container and virtual machine images are built with security at their core, boasting a near-zero CVE footprint and hardened according to best security practices.

CleanStart's hardened images minimize the attack surface using industry-leading hardening techniques, resulting in **reduced deployment times and enhanced security posture.**

Key Challenges

Inherited Vulnerabilities

Public images may contain unpatched vulnerabilities increasing the attack surface of any container built from them.

Hidden Malware

Malicious actors might upload container images containing malware disguised as legitimate software.

Outdated Images

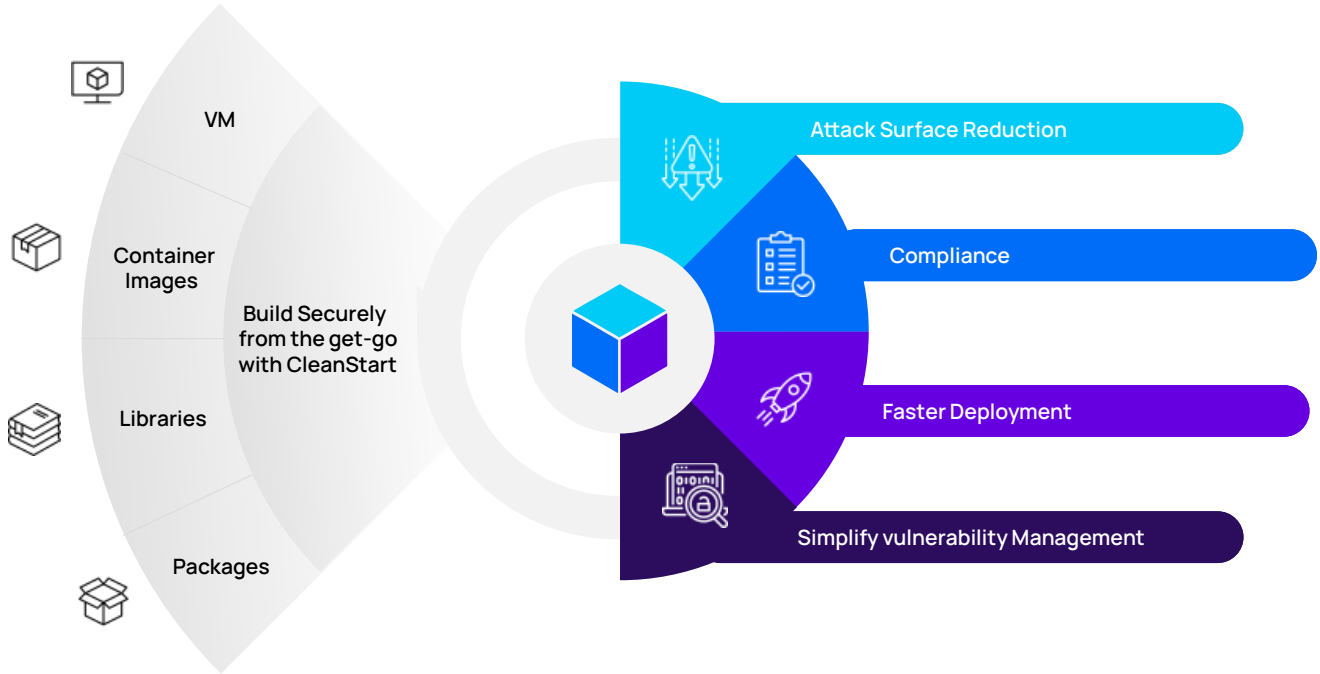
Public images are poorly maintained missing regular updates for vulnerabilities.

Limited Visibility

Public registries often lack detailed build and security information, making risk assessment before deployment difficult.

Supply Chain Attacks

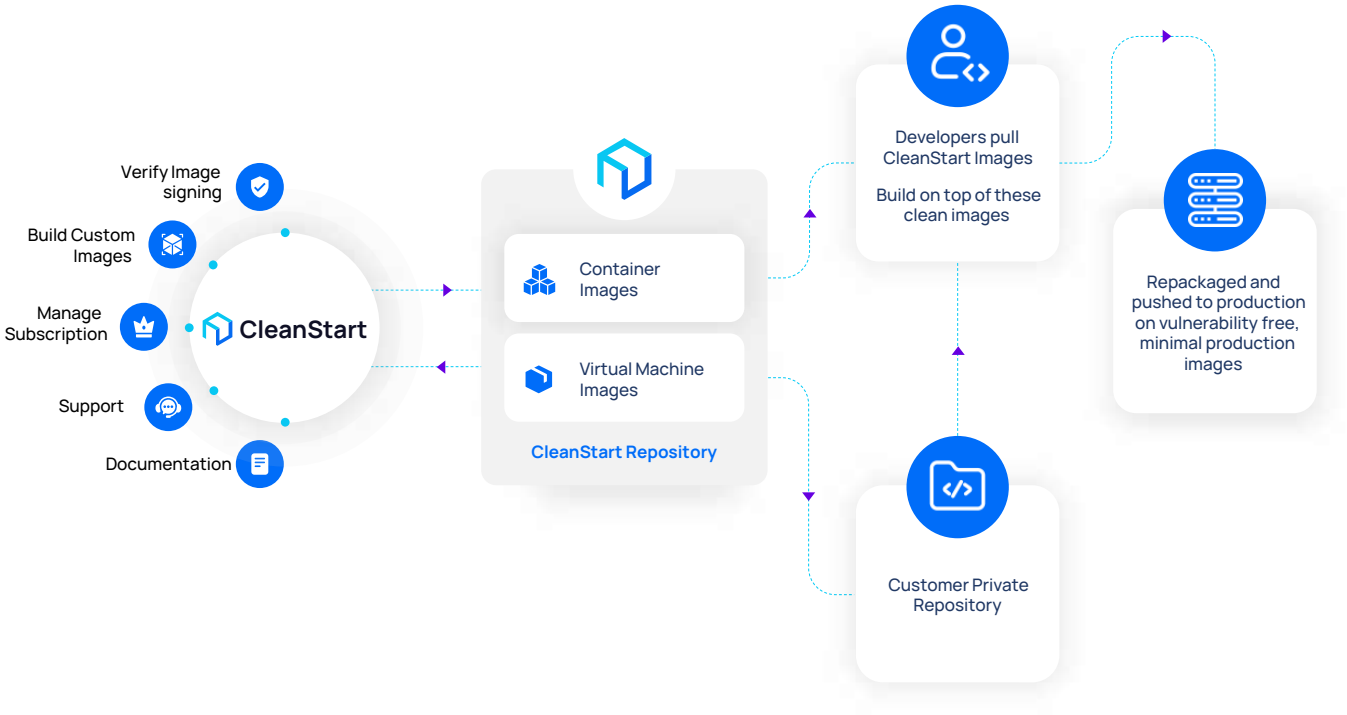
A compromised public registry image can cause supply chain attacks, spreading malicious code to numerous deployments.



Solution & Design

CleanStart images undergo rigorous security processes to achieve near-zero CVEs, ensuring they are secure, hardened, and minimal, reducing the attack surface by excluding unnecessary components.

These images are hardened to avoid misconfigurations, scanned for vulnerabilities and malware, designed to be compliant with standards like FIPS. They are also signed to maintain integrity and provenance.



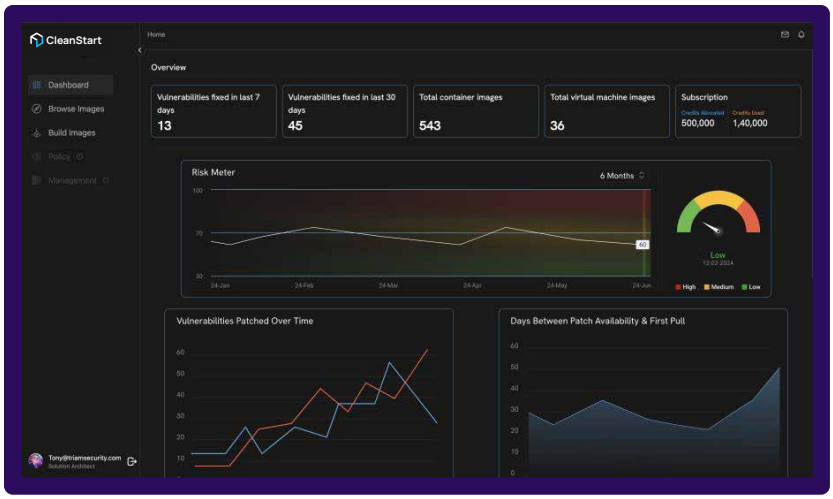
CleanStart solution includes two main components

CleanStart Portal

CleanStart Portal lets customers manage subscriptions, check usage, request custom images, verify signatures, contact support, and access documentation.

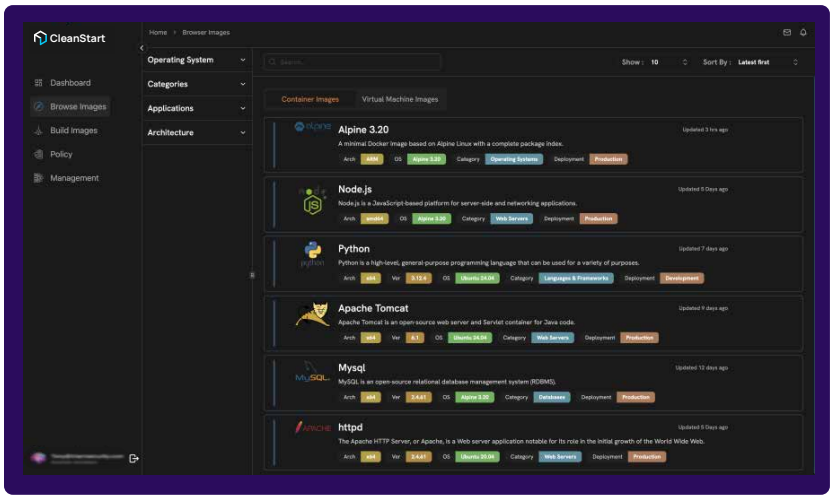
CleanStart Repository

CleanStart Repository offers clean, vulnerability-free container and virtual machine images. Customers may choose accessing directly from CleanStart or replicate images to their own private repositories.



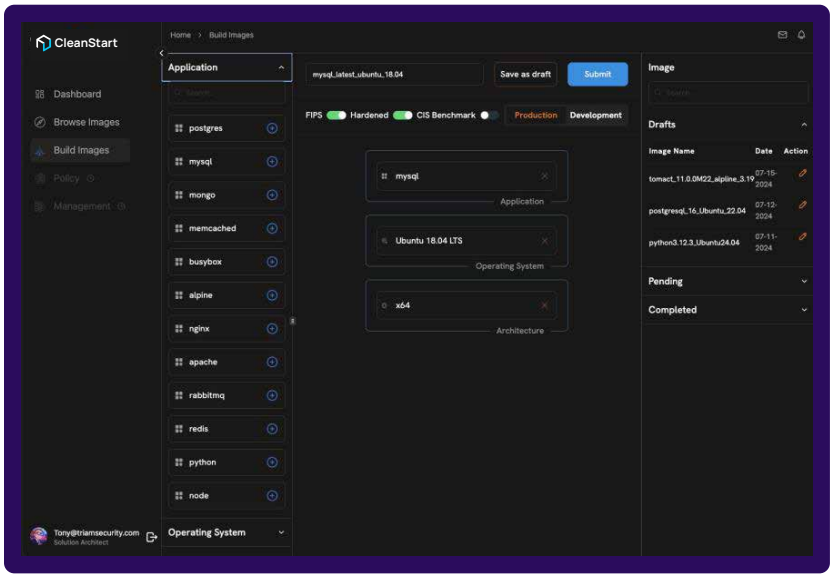
Dashboard

Presents the user with current and trending risk profiles, latest threat landscape information and usage information. It also presents statistics revealing ROI of the product in the organization.



Browse Images

Displays the catalog container and virtual machine images available via the CleanStart solution.



Build Images

Provides an intuitive interface for customers to request images for specific combinations of architecture, Operating system and application versions. They also can choose production vs development images and compliance and hardening options.

Why CleanStart?

Reduce Attack Surface

Minimize entry point for attackers using our slim images

Faster Deployment Cycles

Save time spent on vulnerability scanning and remediation by using our clean pre-scanned images

Improve Compliance

Align with industry standards and build trust with customers and partners

Simplify Vulnerability Management

With near zero vulnerabilities vulnerability management is a breeze

Reduce Bloat, Gain Efficiency in Production

Leaner Application perform better