HOW IIFL STRENGTHENED TRUST WITH A VERIFIED CONTAINER FOUNDATION

CASE STUDY

CUSTOMER SNAPSHOT

COMPANY

India Infoline Finance Limited (IIFL)

INDUSTRY

Financial Services

ARCHITECTURE

Cloud-native, Kubernetesbased platform

CUSTOMER PERSPECTIVE

"CleanStart helped us standardize our container foundations without slowing development. Tasks that previously required significant manual effort are now eliminated, deployments are faster, and our security team has greater confidence in the images we use."

Shanker Ramrakhiani,
CISO & HEAD OF BCP,
IIFL FINANCE

BACKGROUND

India Infoline Finance Limited (IIFL) delivers digital-first financial services in a highly regulated environment. As its containerized, microservices-based platform grew, maintaining trust in the container foundation became critical for security, compliance, and operational stability.

THE CHALLENGE

IIFL relied on containerized environments to deliver new services. Over time, different teams began using different container images and OS configurations, creating inconsistency across the environment.

This resulted in recurring issues:

- Vulnerabilities detected during late-stage scans
- Manual effort to clean and harden runtime images
- Inconsistent patch levels across services
- Increased effort during audit and security reviews

Existing scanning tools could detect problems but couldn't verify how containers were assembled or whether all workloads followed a consistent baseline, making it difficult to maintain an auditable security posture in a regulated setting.

STANDARDIZING THE CONTAINER FOUNDATION WITH CLEANSTART

IIFL traced these issues to the container foundation layer and standardized on CleanStart images across all workloads. Built from source using deterministic, hermetic pipelines,

CleanStart enabled IIFL to :

- Use hardened, minimal images by default
- Remove reliance on unverified public images
- Maintain consistent OS configuration across teams
- Verify all included dependencies
- Generate SBOMs and provenance data for audit workflows

By starting every workload from a verified container foundation, security controls were applied before application code entered the CI/CD pipeline, reducing variability and improving confidence across environments.

MEASURABLE IMPACT

Reduced OS-level vulnerabilities detected during scans

Eliminated manual image hardening and cleanup effort

Faster deployment cycles and shorter time to market

Consistent container posture across all services

Improved audit readiness through standardized build evidence and SBOMs

ABOUT US

CleanStart is a software supply chain posture management platform that provides visibility into security blind spots across the software delivery pipeline. By using secure, verified container images built from source, along with built-in transparency and policy-driven controls, CleanStart helps organizations reduce risk, strengthen software supply chain integrity, and simplify compliance.

Connect with us to build a secure and verifiable software supply chain.

marketing@cleanstart.com

www.cleanstart.com