CleanStart™

CleanSight

Complete Container Visibility. Achieved.

Built Clean. Run Secure.

Product Sheet

Continuous and Comprehensive Container Visibility

Containerized infrastructure scales rapidly across Kubernetes clusters and registries. Images accumulate over time, often without centralized inventory or lifecycle governance.

Most security programs rely on point-in-time scanning of active workloads. They do not establish complete container inventory across stored, dormant, and deployed assets.

CleanSight delivers continuous and comprehensive container visibility across your infrastructure. It enumerates every container image, analyzes its internal components, and quantifies exposure with deployment-aware intelligence.

The Container Visibility Gap

Enterprises operate hundreds to thousands of container images across distributed environments. Over time:

Dormant images persist in registries without review	Orphaned artifacts remain ungoverned	Vulnerabilities remain embedded in unused images	Exposure reporting lacks deployment context

Industry research indicates that a significant percentage of containers run only once or intermittently, while the majority of container images contain known vulnerabilities. As development velocity increases, registry sprawl expands faster than inventory controls.

Without comprehensive enumeration, exposure metrics are inherently incomplete.

Infrastructure-Wide Enumeration

CleanSight continuously enumerates container images across Kubernetes clusters and registries, including:

- Running workloads
- Dormant & unused images
- Shadow deployments
- Orphaned artifacts

It resolves image references to immutable digests and correlates registry metadata with cluster deployment state, ensuring stored and referenced artifacts are included in analysis.

This establishes a defensible, infrastructure-wide container asset record.

Component-Level Exposure Intelligence

- Generates SBOMs in industry standard formats
- Extracts full component and transitive dependency trees
- Correlates vulnerabilities at the package level
- Applies severity and exploitability context
- Aligns exposure to major compliance frameworks

Exposure is presented with infrastructure and workload awareness, not as isolated vulnerability counts.

Beyond Vulnerability Scanning

01 Focus on point-in-time image analysis

02 Emphasize CVE counts over deployment context

03 Provide limited insight into dormant or stored artifacts

04 Generate findings without infrastructure correlation

CleanSight establishes continuous inventory and correlates exposure with workload state and deployment context. It connects container assets, dependencies, and vulnerabilities into a unified visibility layer

Enabling Measurable Risk Reduction

When vulnerable images are identified, CleanSight recommends compatible hardened CleanStart alternatives and quantifies projected exposure reduction.

This enables informed replacement decisions grounded in measurable security impact.

Remediation is guided through visibility.

Operational Impact

Organizations using CleanSight achieve:

01 Discovery of previously untracked container assets

02 Enterprise-wide exposure visibility

03 High coverage of vulnerable images with secure alternatives

04 Improved compliance and audit readiness

Container Visibility as a Foundational Security Control

Modern container security cannot rely solely on point-in-time scanning. Without continuous and comprehensive enumeration, exposure metrics remain fragmented and risk reduction efforts remain incomplete.

CleanSight establishes infrastructure-wide container visibility and correlates exposure with operational context, enabling measurable and defensible container risk governance.

Visibility becomes controlled, measurable, and strategic.