

HOW O9 SOLUTIONS ADOPTED A VERIFIED CONTAINER FOUNDATION

COMPANY

o9 solutions

INDUSTRY

Enterprise Software

IT ENVIRONMENT

Cloud-native applications deployed on Kubernetes infrastructure

BACKGROUND

o9 Solutions delivers enterprise planning and decision intelligence solutions to global organizations, operating a large-scale cloud-native infrastructure that supports multiple applications and services.

As container usage scaled across environments, maintaining secure, verified, & standardized container images became increasingly important to strengthen its software supply chain security and improve operational consistency.

THE CHALLENGE

As its container environment scaled, o9 Solutions relied on Bitnami and other externally sourced container images. This made it increasingly difficult to maintain consistent security and control across its image environment.

The team faced four key challenges:

- Limited control over externally sourced images**
Image's were pulled from multiple external repositories and registries, making it difficult to establish a consistent, approved source for container images.
- Growing image sprawl and limited visibility**
Legacy and dormant images remained across environments, with no centralized visibility into image inventory and dependencies.
- Increasing vulnerability exposure**
Routine security scans identified vulnerabilities across container images, creating an ongoing need to identify and address insecure packages.
- No centralized, verified image source**
The team needed a consistent way to source and manage verified images aligned with internal security requirements.

ADOPTING A VERIFIED CONTAINER FOUNDATION

o9 Solutions worked with CleanStart to transition from existing Bitnami images to verified, enterprise-ready container images tailored to its application requirements. CleanStart supported the migration and deployment of multiple customized application images while helping o9 establish a more controlled approach to image sourcing, security, and lifecycle management.

CleanStart supported o9 Solutions with:

- Migration from Bitnami images to verified CleanStart images
- Customized image builds for workload-specific requirements
- Production-ready images built with zero known CVEs
- Removal of unnecessary packages & shell access to reduce attack surface
- Centralized management and tracking of internal image inventory
- Helm chart development for standardized deployment



Migrating away from public container images was an important step for us. CleanStart enabled a smooth transition by providing secure, verified images, customization support, and greater control over image quality, helping us improve both security posture and operational efficiency.

Narasimha Kamath
GLOBAL CISO,
O9 SOLUTIONS.

The transition gave o9 Solutions up to 88% reduction in vulnerability noise while establishing a more secure and standardized foundation across its application infrastructure

STRENGTHENING SOFTWARE SUPPLY CHAIN SECURITY

CleanStart helped o9 Solutions strengthen software supply chain visibility and security governance across its container environment. Key capabilities included:

- Integrated SBOM generation for greater transparency into image contents
- Dependency visibility across container images
- Secure alternatives for vulnerable packages
- Compatibility with existing security tools, including Snyk and CrowdStrike
- Improved vulnerability analysis to distinguish issues originating in source code from those introduced through container dependencies

This gave engineering and security teams deeper visibility into their container ecosystem while helping reduce software supply chain risk.

Outcomes Achieved

✓ Secure, verified images

Multiple production-ready images deployed, including customized workload-specific builds.

✓ Reduced vulnerability exposure

Secure package optimization helped reduce vulnerabilities across the container environment.

✓ Lower attack surface

Unnecessary packages and shell access removed from images.

✓ Centralized visibility and control

Improved image inventory, lifecycle management, and SBOM-based dependency visibility

✓ Standardized deployments

Helm chart development established a more consistent deployment process.

✓ Up to 3x faster path to secure deployment

Reduced the time required to build, verify, and deploy production-ready images.

ABOUT US

CleanStart helps organizations secure modern software supply chains with verified software artifacts. The company enables enterprises to discover software assets, establish software provenance, generate comprehensive SBOMs and AI BOMs, remediate unsafe software components with verified alternatives, and govern software integrity throughout the software lifecycle.



Connect to build a more secure, transparent, and verifiable software supply chain.