docker

CASE STUDY

IDOM builds security into its cloud-native foundation

By adopting Docker Hardened Images, IDOM reduced high-severity vulnerabilities by 80% while maintaining zero critical CVEs.

IDOM

Company: IDOM

Industry: Automotive purchasing and sales

Engineering team: 50–200

Infrastructure: AWS (ECR, ECS, EKS)

Key technologies: Docker Hardened Images, Docker, AWS; Java, Python, JavaScript/TypeScript, Ruby

Challenge: Eliminating base-image vulnerabilities and standardizing on trusted images after a cyberattack

Mission

IDOM is one of Japan's largest vehicle buyers and retailers. It operates approximately 460 locations nationwide under the Gulliver brand, purchasing and selling used vehicles across Japan.

Guided by the principle that "people selling their vehicles are also valued customers," IDOM standardized used vehicle appraisal prices nationwide, replacing the regional inconsistencies that had previously existed and creating new value in the used vehicle market.

After completing its migration to AWS, the company began rebuilding its infrastructure around cloud-native technologies. The objective is to create systems that can scale flexibly as the business grows while keeping operational costs under control.

With every system migration, moving to a more scalable and secure environment has become a central priority. Security is the most important consideration in this effort.

Following a previous cyberattack, IDOM conducted a comprehensive review of its security practices and established a goal of creating an environment in which vulnerabilities were reduced as close to zero as possible.

Achieving this goal required a platform that used trusted container images as the standard and embedded security from the very beginning of the development process.

To make this possible, IDOM reconsidered the design of its container infrastructure.

> Based on our previous experience with a cyberattack, we needed to establish an internal policy requiring the use of secure images only. With a goal of **achieving zero vulnerabilities,** standardizing on trusted base images became our highest priority."
>
> **Kazunari Shiono,** Software Engineering Manager

> For most of our applications, migrating to Docker Hardened Images meant changing the FROM statement in our multi-stage builds, rebuilding, and updating health checks that previously relied on sh — since Hardened Images ship without a shell. Beyond that, the transition was straightforward and **required very few other code or pipeline changes.**"
>
> **Masumi Fukumoto,** Team Lead, Software Engineering

Challenge

Continuously managing vulnerabilities in a cloud-native environment had become a significant operational challenge for IDOM.

As the development organization grew, it became increasingly difficult to maintain consistent security standards across every build while teams were using a wide range of container images from public registries.

The situation also presented opportunities to improve development efficiency.

By standardizing base images across the organization, IDOM could simplify development workflows while ensuring that every team applied the same security standards.

With long-term security improvements and greater operational efficiency in mind, IDOM decided to transition to a more secure and standardized container foundation.

Solution

By adopting Docker Hardened Images, IDOM established a uniform standard for trusted infrastructure. Their approach was straightforward: substitute standard images with the Docker Hardened Images catalog.

IDOM also introduced a policy restricting approved base images to Docker Hardened Images, ensuring that every development team used the same secure foundation.

As a result, Docker now provides ongoing container image maintenance and security patches, eliminating the need for IDOM engineers to evaluate the security of each base image themselves.

Developers can now focus on application development in an environment that is secure from the start.

Here's how IDOM implemented Docker Hardened Images

- Updated Dockerfiles to support multi-stage builds for migration to Docker Hardened Images
- Replaced shell-based health checks with health checks that do not rely on sh, because Docker Hardened Images do not include a shell
- Replaced standard Docker Hub base images with Docker Hardened Images
- Established an internal policy restricting approved base images to Docker Hardened Images
- Documented the containerized development environment and setup procedures so that new team members could begin contributing quickly

This standardized development environment has also proven effective when team membership changes. New engineers can follow the prepared documentation, configure their local environments, and begin development within a short period of time, helping the team maintain overall productivity.

Impact

80% reduction in high-severity vulnerabilities

Over two months, high-severity CVEs in IDOM's Python image fell by 80%. The trusted base did the work that manual remediation did not.

Zero critical CVEs

The images carried no critical, high-attack-risk CVEs before, and none after. IDOM kept that clean record while cutting the high-severity count.

Container image size reduced by approximately 50%

Docker Hardened Images were approximately half the size of the container images IDOM had previously used.

As a result, the company was able to:

- **Reduce** Amazon ECR storage usage
- **Shorten** deployment times to Amazon ECS and Amazon EKS

The reduction in image size contributed not only to lower costs, but also to faster development and operations.

Developers can focus on product development

Previously, whenever engineers wanted to use a new container image, they had to spend time assessing its security and selecting an appropriate base image.

Those decision criteria are now standardized through an organization-wide policy.

By using Docker Hardened Images as a shared foundation, engineers no longer need to spend time reviewing vulnerabilities or selecting base images. They can dedicate more time to the application development work that matters most.

A standardized security foundation

Trusted images are now the standard base images at IDOM. All new systems begin development from a common, secure foundation rather than allowing each team to select base images independently.

This enables IDOM to maintain consistent security standards across the organization.

Next steps

Docker Hardened Images now run on part of IDOM's container environment. The company plans to extend them to every system that uses containers. With a trusted base in place, IDOM is looking at automated, continuous vulnerability scanning through AWS Inspector and at tightening supply chain security further. The cloud-native transformation that began with the AWS migration now has a security layer to build the rest on.

> By adopting secure container images as a company-wide standard, we plan to expand their use to every system that uses containers. We also intend to automate continuous vulnerability scanning and **build an even stronger security posture.**"
>
> **Masumi Fukumoto,** Team Lead, Software Engineering