Chainguard | Hapag-Lloyd

Hapag-Lloyd trusts Chainguard to secure its global shipping platform at scale

With over 17,000 employees and a presence in over 140 countries, Hapag-Lloyd relies on its mission-critical platform, Freight Information System (FIS), to support global shipping operations and operate reliably at a global scale.

Developed in-house in the early 1990s, FIS was the first system in the maritime transportation industry to unify all business processes. As Hapag-Lloyd modernized FIS from a monolithic mainframe into a cloud-based service architecture, the security and resilience of the platform became even more critical.

The challenge

As the FIS platform evolved, the FIS Cloud Platform team—responsible for the internal developer platform serving Hapag-Lloyd's application developer teams and underpinning the FIS transformation—faced increasing pressure to secure its open source software supply chain.

The team already operated with disciplined engineering practices, treating everything as code and automating delivery through CI/CD pipelines. However, managing vulnerabilities in open source container images became increasingly difficult at scale. The platform leveraged many open source images with high-CVE counts, far more than the team had the capacity to patch and maintain internally.

Pascal Nijhof, Senior Manager, Cloud Platform & DevOps, explained, "CVE remediation is a never-ending burden. Tracking many images with diverse findings, understanding attack vectors, and figuring out how to actually fix them is a full-time job."

This challenge was amplified by the introduction of centralized security reporting. CVE metrics became visible at the management level, and eliminating critical and high-severity vulnerabilities became an explicit expectation. The team quickly realized existing approaches wouldn't be sufficient.

As Johannes Witte, Team Lead IT, FIS Cloud Platform, explained, "Even if we had the right skillset on our team, with 15 engineers, we wouldn't be able to do the actual platform work that's required from us on the FIS Cloud Platform team."

The solution

After assessing their options, the Hapag-Lloyd team saw how Chainguard Containers could drive immediate impact.

Adoption was fast. After a four-image proof of value, the team swapped 25 open source images for Chainguard Containers and shipped them to production in one two-week sprint.

Hapag-Lloyd complemented their Chainguard rollout by combining Chainguard with an "Update Champion" protocol — two dedicated people per sprint for updates and dependencies — further strengthening its approach to secure platform operations.

> "Working with Chainguard has been flawless — they're the kind of partner you can actually rely on. They understand what we need to do to secure our system without slowing us down, and they consistently deliver fast, reliable solutions. It's been a great partnership where we know we can count on the product and what's been promised.
>
> Johannes Witte, Team Lead IT, FIS Cloud Platform, Hapag-Lloyd

The results

Security improvements without workflow disruption
Adopting Chainguard Containers improved Hapag-Lloyd's security posture without disrupting how the FIS Cloud Platform team worked. The team remained focused on enabling internal developers and advancing the modernization of the FIS, while Chainguard handled the continuous work of keeping base images secure and up to date.

Chainguard also introduced a level of standardization that simplified operations across the platform. The use of minimal images without shells further reinforced Hapag-Lloyd's existing security best practices, including support for read-only root file systems, and smoother audits and penetration tests.

Decreasing CVEs and the cognitive load on engineers
With Chainguard and updated internal practices in place, the FIS Platform team saw an immediate, measurable improvement in its security posture, and management saw it too.

"We're using around 60 Chainguard container images, but when we look at our scan results, hundreds of CVEs across severity levels vanished to zero," shared Johannes.

Just as impactful was the reduction in operational and cognitive overhead for engineers. Instead of tracking, prioritizing, and manually remediating vulnerabilities, the team's focus shifted to a far simpler question: how they wanted to leverage their expanded resources.

> "We no longer need to ask how we fix a vulnerability — just whether we're on the latest Chainguard version. That shift has completely changed our operational overhead and frees up a lot of capacity for both our engineering and security teams to move faster.
>
> Pascal Nijhof, Senior Manager, Cloud Platform & DevOps, Hapag-Lloyd

Efficiency gains without additional headcount
During peak periods, the team rolled out hundreds of security updates per week without additional headcount or disruption. By eliminating the need to staff or operate a dedicated internal remediation function, the platform team preserved its ability to ship, scale, and support hundreds of application developers building standalone business modules.

Raising the security baseline across the organization
The improved security posture also changed internal perceptions across Hapag-Lloyd. Management began to view the FIS Cloud Platform team as a model for effective security and remediation, while application teams gained greater confidence in the security of the platform they relied on.

"With the solutions we've found, both Chainguard and our Update Champions process are regarded by management as best practices regarding security and remediation," Johannes said, noting that this progress came with far less effort than alternative approaches.

Over time, the initiative's success extended beyond its original scope. The FIS Platform team launched a mirror service to make all their Chainguard container images available to all IT groups within Hapag-Lloyd, including the teams outside of FIS. What began as a targeted solution evolved into a company-wide service, reinforcing security as a shared foundation rather than a localized concern.

Together, these results enabled Hapag-Lloyd to strengthen its open source security posture without sacrificing speed, focus, or engineering capacity.