Chainguard

Securing Innovation at Speed: The Army Software Factory Implements New Methods to Deliver Critical Software to the Force

About The Army Software Factory

The Army Software Factory (ASWF), a program under the Army Futures Command, is pioneering a software initiative that empowers soldiers to build modern solutions to U.S. Army challenges. This first-of-its-kind effort is designed to develop, employ, and sustain technical talent across all ranks and roles within the military.

By leveraging soldier-led innovation, ASWF delivers mission-ready software that enhances combat support, streamlines operational planning and execution, and strengthens decision-making for commanders in the field.

In less than 30 days, ASWF dramatically transformed its software delivery pipeline by partnering with Chainguard—eliminating the overhead of two full-time engineers dedicated to image patching, reducing CVE remediation timelines from weeks to hours, and freeing up over 40% of developer time for mission-enabling innovation.

Challenge

Scaling Secure Container Image Management

At the Army Software Factory, open source is central to delivering mission-critical software. As Platform Product Manager Noe Lorona explains, "Our engineering environment uniquely integrates open source software as a strategic capability. We empower engineers to collaboratively build tailored, mission critical, rapid solutions."

However, managing container images at scale posed a major challenge. As Noe shared, relying on many third-party container images requires security and platform teams to manually validate, patch, insert certificates, and harden each container image, often with inconsistent quality and update cycles.

This manual work introduced delays, diverted engineering effort, and limited ASWF's ability to deliver secure, production-ready software at the speed their mission demands. "The status quo led to significant internal efforts to validate, patch, insert certificates, and then harden images before they could be used in our own environment," Noe said.

Solution

Trusted, Secure Containers from Chainguard

Recognizing the operational inefficiency of their existing approach, ASWF sought a solution that would provide verified and frequently updated container images, reduced CVE patching timelines, seamless integrations with their CI/CD infrastructure, and a secure foundation for mission-critical deployments.

Chainguard emerged as the ideal partner to shift ASWF from reactive security to proactive innovation. As Noe shared, "Our platform and security team spent substantial time triaging CVEs and checking configurations and coordinating the deployment of all of this, which slowed down throughput and increased the cognitive load on the engineers. With Chainguard [Containers], we now benefit from consistent, verified, and frequently updated base images that reduce manual overhead and raise our confidence in the integrity of our deployment."

> **"The situation presented an opportunity to leverage Chainguard's pre-packaged secure images, significantly reducing the operational burden and freeing our engineers to focus on more mission-critical innovation and solving user problems effectively."**
>
> **Noe Lorona**
> Platform Product Manager, Army Software Factory

A Trusted Partnership for Risk Mitigation

ASWF moved quickly from identifying a critical software supply chain need to securing their production environments with Chainguard's container images. "From the moment that we identified our supply chain need to deploying the secured Chainguard [Containers] in production environments, the process took approximately 30 days," Noe said.

This rapid turnaround was enabled by strong collaboration and support. "The Chainguard team has been very responsive, professional, and deeply knowledgeable, which have been really conducive to a smooth integration. Chainguard's documentation and support enabled us to move quickly with confidence and maintain and increase security posture."

Results

Increased Innovation, Reduced Developer Toil

For ASWF, adopting Chainguard Containers was more than a tooling decision—it was a strategic enabler. The shift from manually patched, third-party container images to pre-secured, continuously maintained containers fundamentally improved the way ASWF builds, secures, and delivers software.

Security at Speed, Without Additional Headcount

Leveraging Chainguard Containers allowed ASWF to drastically reduce mean time to remediate vulnerabilities and eliminate the need for two full-time engineers dedicated to image patching and hardening. Patching cycles that once took days, or even weeks, are now resolved in hours, enabling faster and safer deployments across environments.

Noe described the transformation as not only a matter of efficiency, but a strategic realignment of developer energy:

> **"We reduced CVE-related patching timelines from days to hours, and even weeks to hours sometimes, significantly shrinking our attack surface and reducing operational risk. Time spent on vulnerability remediation has decreased by an estimated 40%, freeing up critical engineering capacity to focus on mission-enabling tasks."**
>
> **Noe Lorona**
> Platform Product Manager, Army Software Factory

The team now spends more time improving user experience, developing new capabilities, and solving meaningful technical problems.

Secure Foundations That Scale

ASWF's maintenance workflows have been transformed from manual and error-prone to automated and secure by default. With Chainguard Containers integrated directly into their CI/CD pipelines, updates are now consistent, verifiable, and repeatable, without introducing friction to the development process. As Noe said, "Maintenance is now CI/CD driven, repeatable, and secure by default, allowing us to focus more on delivering value to the mission."

This shift also reinforced the team's confidence in leveraging open source technologies. With Chainguard providing detailed SBOMs and hardened base container images that align with zero-trust principles, ASWF can now rely on the open source ecosystem without compromising visibility or integrity.

> **"Chainguard gives us the confidence in user open source by closing critical security gaps in the software supply chain. It allows us to benefit from the open source ecosystem while maintaining a zero-trust approach and mindset. Having verified, secure base [container] images with detailed SBOMs has changed how we evaluate open source security. Transparency is now built in from the beginning, and I think we can all appreciate that."**
>
> **Noe Lorona**
> Platform Product Manager, Army Software Factory

Conclusion

A Secure Foundation for Mission-Ready Software

For ASWF, secure software delivery is not just about compliance; it's about delivering operational capabilities that protect and empower soldiers. With Chainguard, ASWF has found a trusted partner to achieve both security and speed, while advancing a fundamental shift to a true DevSecOps mindset—moving beyond reactive "shift left" approaches to proactively integrating security from the very start of the development lifecycle.

> **"Chainguard helped us maintain a secure baseline without draining developer velocity. Instead of tasking engineers with container image compliance and patching, we redirect their efforts towards platform features, developer experience, and solving user problems. This enables faster delivery of mission-ready capabilities and supports innovation in both connected and disconnected environments."**
>
> **Noe Lorona**
> Platform Product Manager, Army Software Factory