Chainguard | asana

Asana trusts Chainguard to simplify compliance and expand into federal markets

About Asana

Asana is the System of Action for work, where humans and AI collaborate to help individuals work smarter, teams move faster, and organizations deliver results. Powered by the Work Graph®, Asana provides the context and governance for AI to operate inside real workflows, helping 180,000+ organizations build the Agentic Enterprise.

The challenge

Asana runs a large, containerized AWS environment built on a two-decade-old technology stack that has gradually migrated from legacy infrastructure. The team relies heavily on Amazon Elastic Kubernetes Service (EKS) and a wide range of third-party public base images, using AWS Inspector to scan EKS workloads for vulnerabilities.

Because those third-party base images were maintained at varying levels of quality and frequency, vulnerability scans from AWS Inspector produced extremely noisy results, resulting in a poor signal-to-noise ratio across its AWS environment. As Kyle Ip, Security Software Engineer at Asana, put it, "Inspector scan results were extremely noisy, which made it difficult to determine what actually mattered and what to prioritize. Our security team had to manually review, triage, and remediate each finding, creating significant operational overhead."

The volume of findings turned vulnerability management into a compliance bottleneck. For audits like SOC 2, ISO, and FedRAMP, the team had to manually track and report on vulnerabilities, at one point managing a spreadsheet with over 100,000 rows. The effort pulled engineers away from higher-impact security work and feature development, limiting their ability to focus on building secure-by-default systems.

> "Without Chainguard, we were not able to shift our focus from toilsome work to the more pressing needs of the new feature or frameworks that we wanted to build.
>
> Vishrut Shah, Senior Engineering Manager, Asana

The inflection point came when Asana began pursuing FedRAMP authorization to unlock future business with federal agencies. When the team calculated the work required to meet federal vulnerability management and documentation standards under their existing approach, they determined it would require hiring two full-time engineers dedicated solely to this effort. At that scale, vulnerability management was no longer just a workflow problem; it was a barrier to FedRAMP and federal market access.

The solution

Asana evaluated hiring additional engineers, alternative hardened image providers, and Chainguard Containers. Ultimately, the team chose Chainguard, leveraging AWS Marketplace to streamline procurement and integrate seamlessly with their Amazon EKS environment. Asana was confident in Chainguard's broad base image coverage and the assurance that new container images and variants would continue to be supported as the company's needs evolved.

Once the integration with Asana's automated CI/CD pipelines and build tools was established, along with image synchronization to Amazon Elastic Container Registry (ECR), the rollout of Chainguard container images accelerated significantly. The CI/CD automation handled image validation, vulnerability scanning, and promotion workflows, ensuring consistent and policy-compliant builds across environments.

Within six months, Asana's federal environment advanced from zero to 99% Chainguard base image coverage. This included the adoption of FIPS-compliant images, which helped meet strict federal security and compliance standards. Chainguard's OpenSSL implementation enabled rapid mitigation of security vulnerabilities and ensured faster delivery of patched and validated components. As a result, Asana was able to deliver new FIPS-validated images on schedule, maintaining compliance without compromising deployment velocity.

The results

Vulnerability reduction at scale

The most immediate impact of Asana's Chainguard Containers implementation was a dramatic reduction in vulnerabilities. After standardizing on Chainguard base images, the team's FedRAMP tracking spreadsheet of over 100,000 vulnerabilities dropped to roughly 200. This shift transformed vulnerability management from an overwhelming, manual process into a focused, manageable one. With fewer vulnerable base images running in Amazon EKS, AWS Inspector findings became significantly more actionable. Audit preparation for SOC 2, ISO, and FedRAMP became significantly easier, with far less time spent gathering evidence and triaging noisy scan results.

And with the reduction in engineering toil came a real impact on morale. Instead of constantly reacting to noisy findings, engineers can now focus on building secure-by-default systems and advancing long-term security improvements.

FedRAMP enablement and market expansion

Chainguard played a critical role in making FedRAMP achievable at Asana's scale. As Kyle shared, "FedRAMP accreditation would not have been possible without a solution like Chainguard." Achieving FedRAMP positions Asana to serve U.S. government customers and compete in highly regulated environments, expanding Asana's addressable market and reinforcing its broader commitment to operating with enterprise-grade security at scale.

> "Chainguard is enabling us to achieve FedRAMP accreditation, which opens up Asana to expanding our customer base to include local and federal government.
>
> Vishrut Shah, Senior Engineering Manager, Asana

With Chainguard, Asana transformed vulnerability management from a compliance burden into a scalable security advantage.