

Cloudera trusts Chainguard to help secure the foundation of enterprise data

About Cloudera

Cloudera is the only data and AI platform company that brings AI to data anywhere: in clouds, data centers, and at the edge. Cloudera delivers 100% of data in all forms—whether it is in Cloudera or anywhere in the entire data estate. The world’s largest organizations rely on Cloudera to fuel insights that boost bottom lines, safeguard against threats, and save lives.

The challenge

Cloudera’s mission is bold: AI anywhere, cloud anywhere, data anywhere. As the company powers some of the world’s most data-intensive enterprises, the stakes are high, particularly in highly regulated sectors.

Security and compliance sit at the heart of that responsibility. As customer expectations evolved and compliance requirements tightened, Cloudera realized that we needed to evolve to manage our container security posture as challenges grew in scale and complexity.

The distinction between public-sector and commercial compliance environments was disappearing, making scalable vulnerability remediation essential. Instead of relying on a sustainable, automation-first approach, Cloudera’s engineering teams were investing significant time in patching base images, rebuilding, and revalidating—even for vulnerabilities with no runtime impact—creating an opportunity to optimize and modernize their process. Katie Boswell, Vice President, Product Security explained, “Every hour an engineer spends in remediating a CVE is an hour taken away from building better features and higher quality for our customers.”

With exabytes of customer data under management and the rapid rise of AI increasing both opportunity and risk, Cloudera knew they needed a scalable, secure foundation that could maintain its FedRAMP requirements and security posture across both federal and commercial environments, reduce its attack surface area, and ensure it remained a trusted, resilient backbone in its customers’ data supply chain.

“ At Cloudera, data is critical for our customers, especially in highly regulated environments like government, healthcare, and financial services.

Katie Boswell, Vice President, Product Security, Cloudera

The solution

Cloudera evaluated several paths forward, from major OS container vendors to building an in-house solution. Competing options focused on patching, leaving the long tail of medium and low CVEs and the maintenance burden squarely on Cloudera’s teams. Chainguard offered something different: verified container images that removed vulnerabilities across all severities, allowing engineers to stay focused on innovation.

Cloudera adopted [Chainguard Containers](#) to rebuild its container foundation from the ground up. With secure-by-default, continuously verified base images, Cloudera saw immediate reductions in vulnerabilities and gained end-to-end provenance for every image in its supply chain. The company completed integration into production pipelines in just 90 days, setting a new standard for security automation and deployment speed.

Despite some initial hesitation around bringing on a vendor for such critical infrastructure, Chainguard quickly proved its value by aligning with Cloudera’s deep security and compliance culture. The new approach freed engineering teams to focus on delivering high-quality, secure data products for customers.

“ Chainguard is now a standard across our container ecosystem, powering both our FedRAMP and commercial control planes.

Katie Boswell, Vice President, Product Security, Cloudera

The results

Working together, Cloudera reduced its container CVE footprint by more than 90%, strengthening its security posture and ability to scale securely while also establishing a more resilient, future-ready foundation to support evolving AI workloads, compliance requirements, and emerging supply chain risks.

Cloudera also saw significant gains in speed and compliance readiness. By shifting to secure-by-default containers, the company maintained its FedRAMP compliance while accelerating delivery cycles. As Jamison Bennett, Security Engineer, shared, “Chainguard has allowed Cloudera to reliably ship our product faster with fewer CVEs.”

From a leadership perspective, the results were equally transformative. Working with Chainguard, Cloudera can reallocate engineering resources toward innovation and customer outcomes while strengthening trust and data integrity across its enterprise open source platform. As Katie Boswell, Vice President, Product Security, Cloudera, explained, “Chainguard has become a key weapon in our arsenal of tools we use against the security threats that are out there. It’s helped us stay ahead of emerging threats, including those amplified by AI, and frees our teams to focus on delivering enterprise innovation instead of chasing vulnerability noise.”

“ Chainguard gives us peace of mind and knowing that the OS and the system vulnerabilities that are out there that would be under attack are being taken care of for us.

Jamison Bennett, Security Engineer, Cloudera