

Arpio trusts Chainguard to accelerate compliance and win enterprise deals

The challenge

Arpio is the only cloud-native, automated disaster recovery platform for AWS and Azure. Built for modern, cloud-native workloads, Arpio delivers one-click disaster recovery for the cloud era. With a lean 12-person engineering team supporting a 30-person company, every resource decision matters, and security has always been baked into how the team operates.

In early 2025, a major enterprise opportunity landed with a catch. The prospect needed Arpio to meet FedRAMP requirements before they could move forward, specifically FIPS 140 compliance, verified cryptographic modules, Software Bill of Materials (SBOMs), and provenance attestation, and they needed to do so within a single quarter.

They knew they needed to address compliance, but weren't sure if they should attempt it alone within the time allowed. As Shaw Terwilliger, Co-founder and CTO, put it, "Give me a year, and I can easily map out NIST 800. But moving so quickly, where the customer said you've got to align with our internal requirements and their customer's customers, the unknown was real. We knew that if we picked a partner who'd mapped this out, we could rely on them to provide the missing pieces that were too risky to build ourselves on that timeline."

The solution

Arpio moved quickly to find a partner that could deliver FIPS 140-compliant images, SBOMs, and provenance attestation without requiring the engineering team to stitch together components or build compliance processes from scratch. Chainguard Containers checked every box.

The licensing model made it easy for Arpio to use the same images across every environment, from local development to production. For a small team managing a complex, multi-environment architecture, that consistency mattered. As Shaw explained, "In our business, we need to deliver security from end-to-end."

Within days of first access, the team had made its first commit using Chainguard Containers and pushed them to production shortly after. Within 30 days, Chainguard was running underneath every Lambda function and Amazon ECS container across the entire platform, including code deployed into customer environments, giving Arpio a unified way to deliver security patches to its own systems and its customers' accounts in a single process. Without this, pushing a fix across customer environments would have meant a manual, account-by-account process every time a vulnerability was found.

Once Arpio won the enterprise deal, the team made a deliberate decision to normalize on FIPS-compliant images across the entire product, not just for the customer that required it. Shaw reflected, "It's nice to normalize on a standard platform. When a customer requires FIPS compliance, we can deliver without customization."

“ Chainguard has been a great partner. They move as quickly as we need them to, with technical support responses the same day. With Chainguard, we’ve been able to move very, very quickly.

Shaw Terwilliger, Co-founder and CTO

The results

A major enterprise deal, won without adding headcount

The most immediate outcome of deploying Chainguard Containers? Arpio won the enterprise customer. What had started as a high-stakes, tight-deadline compliance sprint turned into a repeatable part of how Arpio goes to market. FIPS 140 compliance, once a specific customer requirement, is now standard across the entire platform enabling Arpio to support customers using encryption for sensitive US Government data.

Shaw estimated that maintaining a homegrown FIPS and NIST 800 compliance program would have required growing headcount by roughly 10%, one or two senior engineers whose time would have been pulled entirely away from building the product.

The freedom to grow into containers

Arpio has been steadily moving more of its architecture toward containers, and Chainguard has made that shift easier to manage from a compliance standpoint. As the platform grows beyond Lambda functions and into more sophisticated compute, the OS-level vulnerability management, patching, and configuration work that would normally add compliance burden is largely covered. And because Chainguard handles that layer reliably, the engineering team doesn't have to think about it. Arpio rebuilds its container images from scratch dozens of times a day, and the process just works.

Shaw explained, "We can say that a large portion of our OS configuration, patch, and vulnerability management is covered by Chainguard and that our application lives above it. Its flexibility to grow our business without adding a lot more compliance complexity and work."

Faster sales cycles and customer confidence

The compliance foundation Chainguard provides has had downstream effects on how Arpio's go-to-market team handles security questionnaires, and on how customers respond when Chainguard comes up in conversation. Security questionnaires move faster, and Chainguard's reputation resonates with customers.

What's next

Arpio is just getting started with Chainguard. The team is working toward adopting Chainguard Libraries for Python and npm dependencies, bringing the same security foundation it provides at the OS level to its open source packages.

“ Knowing that the OS, native libraries, and application runtimes are hardened by Chainguard, that's meaningful. That gives us multiple lines of defense to catch vulnerabilities.

Shaw Terwilliger, Co-founder and CTO