Chainguard | LogicMonitor

# LogicMonitor Trusts Chainguard to Break the Endless Cycle of Patch Management

## About LogicMonitor

LogicMonitor offers hybrid observability powered by AI. The company's SaaS-based platform, LM Envision, enables observability across on-prem and multi-cloud environments. LogicMonitor provides IT and business teams operational visibility and predictability across their technologies and applications to focus less on troubleshooting and more on delivering extraordinary employee and customer experiences.

### Challenge

As LogicMonitor worked toward achieving FedRAMP Moderate compliance to unlock key government contracts, the company faced significant hurdles around FIPS compliance and container vulnerability management.

With engineers pulling open source software from disparate sources, their container environment had become fragmented, with multiple operating systems and dozens of versions in play. This lack of standardization created blind spots and inflated the attack surface, making it difficult to patch and secure containers consistently. LogicMonitor's security scanning tools also revealed a large backlog of CVEs, compounding the existing security and compliance burden.

As a result, meeting FedRAMP's standards for vulnerability management (with its 30-, 90-, and 180-day SLAs) led to LogicMonitor's engineering and security teams engaging in cumbersome manual processes for triaging, analyzing, and remediating vulnerabilities. The engineering capacity spent preparing for FedRAMP accreditation was pulling away valuable resources from higher-impact product initiatives.

Randall Thomson, VP of Technical Operations recalled, "Whenever a critical vulnerability appeared at the container level, we had to drop everything, rebuild our container images, and switch all of our applications over to the latest build. We were constantly chasing our tails and it just didn't seem like a good use of the team's time."

That sentiment was echoed by Johnathan Hunt, LogicMonitor's CISO, who explained, "Without a secure foundation, you're stuck in an endless cycle of scanning, patching, and monitoring. Having a solution that builds that security in from the start not only reduces our risk, but also reduces the amount of effort required on a daily basis to maintain those systems."

### Solution

Before adopting Chainguard Containers to accelerate compliance and strengthen security, LogicMonitor's engineers experimented with the free, Wolfi-based container images available on Chainguard's website. This hands-on experience gave the team confidence in the technology and a clear view of how it would fit into their environment.

As Randall said, "We researched other solutions, but they still required significant human effort, either by building and maintaining our own Rube Goldberg–like processes or handling extra compliance paperwork. Chainguard was the only option that truly saved us time and resources."

By adopting standardized, FIPS-validated container images from Chainguard, the team was able to replace their fragmented container security strategy with a secure, drop-in foundation that required minimal reconfiguration.

"A lot of companies advertise drop-in replacements, but migrations usually turn into a laborious process," Randall said. "With Chainguard's FIPS-validated images, like Ingress NGINX Controller, it truly was a drop-in. We didn't have to redo our configs, and that was very appealing."

> **"We evaluated a number of products, but Chainguard was the one that provided the greatest ROI and the best opportunity to meet the requirements we needed to achieve FedRAMP from a system level."**
>
> **Johnathan Hunt**
> CISO, LogicMonitor

### Results

**Faster Path to FedRAMP Compliance**

With Chainguard in place, LogicMonitor accelerated its journey to FedRAMP Moderate compliance, which it achieved in July 2025 for its LM Envision platform, and dramatically reduced the day-to-day burden on its security and operations teams.

But LogicMonitor didn't partner with Chainguard just for FedRAMP compliance. Randall explained, "FedRAMP was the primary reason we adopted Chainguard, but we knew there were greater benefits for us beyond just solving for FIPS."

**Less Maintenance, More Time for Innovation**

Standardizing on a single, trusted source for secure-by-design container images simplified security and compliance maintenance and significantly reduced the organization's vulnerability footprint. What once required manual triage, analysis, patching, and documentation became a streamlined process that freed engineers to focus on solving business-critical challenges rather than chasing routine security issues.

The return on investment was clear: Chainguard proved less costly and more valuable than hiring additional specialized staff, and delivered the confidence needed to support both LogicMonitor's commercial and federal customers. As Randall explained, "I don't want people with highly specialized skills solving problems that have already been solved elsewhere. With Chainguard in place, they're solving problems more unique to our environment."

Randall and his team's confidence in Chainguard's ability to alleviate toil led to a multi-year agreement. Here's how he summarized the benefits: "On a month-to-month basis, we're spending far less effort because of the reduced vulnerabilities. Chainguard was a way to reduce headaches and time spent doing the same repetitive tasks."

> **"Chainguard gives us confidence that our systems will stay secure and compliant going forward, while also reducing the maintenance burden compared to other solutions. It delivers both trust in our product and time back to our team."**
>
> **Johnathan Hunt**
> CISO, LogicMonitor