Chainguard | sublime

Sublime Security trusts Chainguard to reduce CVEs and reclaim capacity

About Sublime Security

Sublime's agentic platform stops more email attacks with less work. Its AI agents work like a digital SOC team, automating threat triage in seconds and deploying new defenses in hours. The platform provides full transparency and automatically adapts to stop the unique attacks targeting your organization while eliminating the vendor bottlenecks and one-size-fits-all limits of legacy tools.

The challenge

CVE triage is unglamorous work. Before Chainguard, it was also consuming a disproportionate share of Sublime Security's security team. Every new vulnerability report triggered the same questions: Is this reachable in our environment? Is it actually exploitable? The answers required real investigation, and the volume kept growing.

As a security company, Sublime also holds itself to a higher bar internally—the standard they set for their own production environment reflects the same standard they promise their customers. And enterprise customers were pushing hard on vulnerability management, asking to see SBOMs and evidence of active remediation—checking a SOC 2 box was not enough.

Andrew Becherer, Advisor at Sublime, explained, "Before Chainguard, we had significant issues with the number of CVEs we had in our production environments. Keeping up with them was very difficult. Not every issue is created equal, so we would frequently have to engage in all sorts of analysis."

Jonathon Klobucar, Security Engineer at Sublime, ran into the logical end of this problem: to stay on top of vulnerabilities properly, the team would have had to become its own "image bakery," scanning open source images, tracking down upstream fixes, and sometimes rebuilding packages from source when no fix existed. That's a full-time operation, and Sublime didn't have the headcount for it given the size of their team.

The solution

The team looked at building in-house and at other vendors, but neither was the right solution for Sublime.

"What we were looking for was something that was going to minimize our attack surface, that was going to reduce the number of issues as low as possible, and that was going to be really easy for our engineering organization to implement," Andrew explained. "And that's what we found in Chainguard container images."

Getting Chainguard Containers into production took a matter of weeks. Today, the integration runs through OpenID Connect (OIDC) and GitHub Actions. Sublime engineers pick base images from the catalog without routing through security for approval.

> "At the end of the day, when I compared what Chainguard was going to cost me versus the time I was spending, I was going to spend significantly less time on dealing with this problem by utilizing Chainguard than hiring extra headcount.
>
> Jonathon Klobucar, Security Engineer, Sublime Security

The results

Near-zero CVEs, hours back

Sublime manages weekly triage through rotating "runners" who take new incoming work, assess scope, and score vulnerabilities using internal tooling. Before Chainguard, container image vulnerabilities consumed a significant portion of every triage rotation, crowding out everything else.

As Andrew explained, "the most measurable outcome has been a near 100% reduction in base image CVEs for teams that have adopted Chainguard internally."

Security work that matters

The time freed up has gone toward application-layer security work that had been backlogged. With distroless images carrying a smaller software surface, false positives have decreased.

"Since implementing Chainguard," Jonathon explained, "we've seen both a reduction in false positive reports due to our containers now having a much smaller software surface due to the distroless nature."

Less noise, less paperwork

Vulnerability management often pits security and engineering teams against each other, with security surfacing CVEs that engineering must fix on top of everything else. When the issue count drops, the relationship changes.

Andrew explained, "When those issues don't exist in production, we don't have to talk about them. Not having to raise those issues with our partners in engineering reduces friction, and it really bolsters the messages that we do take to them because we're a lot less noisy."

For Andrew, the individual wins add up to something bigger: a security team that punches above its weight because it's no longer buried in work that shouldn't require its attention.

> "As a CISO, I'm always looking for force multipliers. Things that give me leverage, that provide outsize value for the investment I have to put into it—and Chainguard is exactly that.
>
> Andrew Becherer, Advisor, Sublime Security