aws marketplace

Chainguard Containers

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Chainguard Containers

Chainguard Containers Recap

Chainguard Containers provide security-focused container solutions designed to address modern application challenges. Its use enhances system integrity and ensures robust protection against vulnerabilities.

Chainguard Containers stand out by offering an innovative approach to container security. Expertly crafted to ensure only verified code runs, it emphasizes reducing attack surfaces and enhancing overall workload security. Its utility is crucial for maintaining a secure software pipeline, minimizing risks in application deployments.

What are the standout features of Chainguard Containers?

- Secure by Default: Incorporates security best practices automatically to protect system deployments.
- Minimal Base Images: Ensures a smaller attack surface by using minimalistic container bases.
- Supply Chain Security: Enhanced visibility and control over the software supply chain to mitigate threats.
- Automatic Updates: Regularly updates containers to address new vulnerabilities promptly.
- Compliance Tools: Facilitates meeting regulatory requirements with built-in compliance features.

What benefits should users consider in reviews?

- Increased Security: Enhances overall security posture with reinforced protection measures.
- Faster Deployment: Streamlines deployment processes, boosting operational efficiency.
- Cost Efficiency: Reduces the overhead of manual security checks, saving time and money.
- Regulatory Compliance: Assists in adhering to industry regulations, reducing legal risks.
- Operational Stability: Improves system stability through a more secure infrastructure.

Chainguard Containers find significant application in industries like finance and healthcare, where data security is paramount. By integrating seamlessly into existing IT frameworks, they bolster security without disrupting operational workflows, a critical advantage in sectors with stringent compliance demands.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Chainguard Containers has positively impacted my organization by reducing constant CVE fixing, resolving security versus DevOps conflicts, and minimizing compliance headaches."

ParthasarathyT

Senior Associate Infrastructure at Publicis Sapient

- "The best feature of Chainguard Containers is being distroless, and the main thing I liked about it is that they follow the SBOM process and the continuous rebuilds they were doing, and they were helping me to rapidly remediate the failures which were happening."

Abhishek

DevSecOps at a tech services company with 51-200 employees

- "Specific outcomes and metrics show that before this, every month there would be 15 to 20 vulnerabilities, but after switching to Chainguard Containers, there are now only one or maybe two vulnerabilities."

Udit Parekh

DevOps Engineer at Veefin

"Chainguard Containers has positively impacted my organization even during the proof of concept phase by improving our security posture."

Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

What users had to say about valuable features:

"The best feature of Chainguard Containers is being distroless. That means I am a minimalist. I am a fan of having a minimalistic view in front of me and looking at the right dataset in front of me instead of GUI effects or a lot of animations in front of me. That is where I found Chainguard Containers delivers. There was a lot of less vulnerability, CVE counts in Chainguard Containers comparatively to other tools. The main thing I liked about it is that they follow the SBOM process and the continuous rebuilds they were doing, and they were helping me to rapidly remediate the failures which were happening. This was something I liked about it because the images are much more leaner and it helps me to reduce noise, which is kind of a thing I look for in microservices.

"Sometimes if you are using the latest image, instability comes. However, if you are using a bit older image, I think that is more stable. Chainguard Containers is much more stable comparatively to others.."

Abhishek
DevSecOps at a tech services company with 51-200 employees

Read full review

"Based on my evaluation, the best features Chainguard Containers offers are pre-hardened images. They are now adding pre-hardened libraries as well, but the pre-hardened base operating systems are what we were looking for, and Chainguard offers this and does a pretty good job except for the fact that many of their images are Alpine-based, which are not that friendly with Kubernetes native environments.

I find the quality and security of those pre-hardened images compared to what we were using before to be absolutely solid, as they are minimal images, small in size, and clean.

Chainguard Containers has positively impacted my organization even during the proof of concept phase by improving our security posture. Some of our groups ended up using Chainguard base operating systems for their container images, and that led to improved security posture and fewer vulnerabilities. There was a reduction in vulnerabilities for the teams that were using Chainguard.."

Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

Read full review

"After switching to Chainguard Containers, it was noticed that if you pull any open-source image, such as Java OpenJDK, you have to do the dependency patching yourself, but Chainguard Containers regularly updates the images with patched dependencies, making it very useful and less vulnerable to hackers.

"The best features of Chainguard Containers are the strong focus on software supply chain security, the provision of minimal container images with a very small attack surface, and the practice of regularly updating images with patched dependencies, which is very useful for a secure application.

"The most impactful features are the minimal container images and the patched dependencies, which reduce manual effort to patch the image every time a vulnerability comes, saving engineers' time, and if there are already patched dependencies, then it is very secure and reduces the vulnerability of the image.

"Chainguard Containers are very positive for the SaaS platform. Before switching, dependencies were regularly patched and open-source tools were used to detect vulnerabilities. Vulnerabilities in the base image would be found and fixed. However, after switching to Chainguard Containers, it has significantly impacted the effort and time required. Now, the latest image of whatever language is used for building the application is pulled directly from Chainguard Containers, resulting in a very secure and compliant image.

"Specific outcomes and metrics show that before this, every month there would be 15 to 20 vulnerabilities, but after switching to Chainguard Containers, there are now only one or maybe two vulnerabilities. Time is saved by 60 to 70% because previously it was necessary to first find the vulnerabilities in the base image, then find the patched version and manually patch that version in the base image, which took a lot of effort from engineers. The improvement is very good, and 70% of the time on securing the base image has been reduced.

"Chainguard Containers are the best in minimal container images, and they regularly update their images, making it very easy to integrate with existing container platforms. They have a strong focus on software supply chain security.."

Udit Parekh
DevOps Engineer at Veefin

Read full review

"The benefit of Chainguard Containers is that it makes development simpler. It makes the development team confident there will not be any bugs or vulnerabilities in the image they are using. It is mainly needed for vulnerabilities, SLAs, security audits, and SOC 2, ISO, and PCI compliance. The image includes SBOM, signature, and provenance metadata, which makes audits much easier.

"The best features Chainguard Containers offers include a reduced image size. It removes the shell and the package manager, resulting in a significantly smaller image size compared with a normal image. We can deploy production workloads directly without worrying about security concerns. If we want a strong supply chain for security, we will be using it. Many users are already tired of scanning alerts, so this will be a great thing.

"Removing the shell and package manager has positively impacted my team's workflow and deployment speed by making it quite user-friendly, where the developer can touch it without any hesitation. Chainguard Containers are built and pushed from non-patched binaries, with the packages compiled directly from the source. No dependencies or pre-built distro packages like Debian or Alpine are required, so there are no hidden vulnerabilities. The developer gains full control over what goes inside, and the image size is smaller with fewer vulnerabilities, in fact, zero. It has built-in processes like SBOM, which is Software Bill of Material generated. The image is cryptographically signed, and provenance is tracked, leading to faster patching, minimal footprint, and best supply chain control.

"Chainguard Containers has positively impacted my organization by reducing constant CVE fixing, resolving security versus DevOps conflicts, and minimizing compliance headaches. After implementing secured-by-default containers, there is less effort on fixing vulnerabilities, faster delivery, and better compliance. The impact on security teams includes a lower risk of attack, less panic during audits, and significantly fewer security noises.

"A specific outcome we have noted since implementing Chainguard Containers is that for a client who uses more than 200 containers, they previously received vulnerability warnings for every deployment. Once we implemented Chainguard Containers, the vulnerability ratio drastically decreased, from 100 to 30. Nearly 70% of the vulnerability checks have passed. Chainguard Containers are CVE-

resistant, which is significant as CVEs represent Common Vulnerabilities and Exposures.."

ParthasarathyT
Senior Associate Infrastructure at Publicis Sapient

Read full review

Other Solutions Considered

"We used to use multiple solutions, but we are not switching right now. We have not made the decision yet. So, it will be difficult for me to tell right now. I am evaluating it right now, but for more results and less noise.."

Abhishek
DevSecOps at a tech services company with 51-200 employees

Read full review

"Before using Chainguard Containers, we did use Sonar and Trivy, but wanted to move beyond that due to hosting and scanning each in the pipeline, which has too many bugs and can corrupt our images. To avoid this, we planned to adopt Chainguard Containers.."

ParthasarathyT
Senior Associate Infrastructure at Publicis Sapient

Read full review

"We used to use multiple solutions, but we are not switching right now. We have not made the decision yet. I am evaluating it right now, but for more results and less noise.

"I was evaluating a lot of options. We are evaluating DataDog tools, Snyk, Wiz, and some other two companies as well. There are a lot of competitors for Chainguard Containers we are evaluating. For now, I cannot disclose that information, but Chainguard Containers is kind of a prominent service among the other competitors.."

Abhishek

DevSecOps at a tech services company with 51-200 employees

Read full review

ROI

Real user quotes about their ROI:

"It is an early stage to comment about it. However, based on the numbers I have, I'll say it definitely reduced my overall team's hours and cost spent on them. Definitely it will be a positive trend for me if I integrate it in my tool. However, considering the cost it incurs, I have to check exactly what it bills and basically how much time it saves. Occasionally, for a larger team, if they want to integrate it and they have, they have to put in fewer hours comparatively. So it will be a great tool to invest in.."

Abhishek
DevSecOps at a tech services company with 51-200 employees

Read full review

"I am uncertain about the return on investment with Chainguard Containers. I have heard it costs nearly $13,000 per year. When factoring in the setup of tools like Sonar scanning and Trivy, which costs over $6,000 to $7,000, investing an additional $5,000 for Chainguard Containers provides good support and granular checks on each image, so I do not see it as wasteful; rather, it is a good investment for our startup.."

ParthasarathyT
Senior Associate Infrastructure at Publicis Sapient

Read full review

Use Case

"Chainguard Containers is primarily used for securing containerized applications, reducing vulnerabilities in the software supply chain, and meeting compliance requirements. The SaaS platform is built on Java and React, so Java images are directly pulled from Chainguard Containers, which reduces the vulnerability in that image to attack the application and gives hackers a very small attack surface to the application.."

Udit Parekh
DevOps Engineer at Veefin

Read full review

"Chainguard Containers was a tool brought into my enterprise as a proof of concept that we evaluated, but we have not rolled it out for enterprise usage.

Our main use case for Chainguard Containers during the evaluation period was for hardened images, as we do not have a central source of hardened images for all use cases in the enterprise. Chainguard was a solution that proposed we could use their offering as a source of pre-hardened or pre-vetted images.

During our evaluation, we were trying to use Chainguard Containers for hardened images such as various types including Debian, UBI, Dynatrace, Nginx, and other similar images. We were attempting to see what Chainguard offers and then run a scan on them with their tools to see how hardened they are in terms of vulnerabilities.."

Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

Read full review

"My main use case for Chainguard Containers is for every container deployment as a best practice, and it has been applied at the compliance level. The use case is specifically for compliance checks and best practices.

"A quick, specific example of how I use Chainguard Containers for compliance checks or best practices in my workflow is that it replaces our normal Docker images with secure, low-CVE images in production. Traditional images like Docker Alpine have many vulnerabilities, while Chainguard Containers does not have them. It is minimal, with near to zero CVEs. Teams can use it for API, backend services, and microservices in Kubernetes. The matter here is that it drastically reduces the CVEs, and no manual patching or effort is needed. The practical use case is where it is in Kubernetes, specifically where GKE workloads use Chainguard Containers for Cloud Run and all the popular services.."

ParthasarathyT
Senior Associate Infrastructure at Publicis Sapient

Read full review

"I have been working in my current field for the last five and a half years. I have been evaluating Chainguard Containers for the last three months.

"I was looking for security and compliance, supply chain integrity in our containers. We have heavy workloads which require security maintenance, and we wanted to reduce the burden on it. That is why we need something for debugging, traceability, and auditable builds. That is why we use Chainguard Containers.

"I am currently using this tool and testing the log integrity and having all the security monitoring of the containers to ensure that there is no unusual case happening within containers. We are always using the container processing all the right traffic for us. Apart from it, I am just checking how much processing power it requires to handle the concurrency accordingly. I am also evaluating other tools, but Chainguard Containers is kind of becoming a permanent tool in our evaluation right now.

"For security monitoring, I am using Chainguard Containers right now as an adapter functionality to my respective pod. What is happening is that we are basically pulling the logs of all the containers and auditing those logs with the help of Chainguard Containers and basically understanding exactly how our containers are behaving. A few things I liked about it are how easily Chainguard Containers documentation is to go through, and the integration was a bit seamless compared to other monitoring tools. Comparatively, I have tested a lot of tools such as DataDog, Snyk, and Wiz, and I found Chainguard Containers documentation a bit more comfortable. Apart from it, there are a lot of places where I found Chainguard Containers could have improvised, but throughout my experience right now, it felt a bit seamless compared to others. I am basically using it for logging and metrics or basically understanding of the auditing.."

Abhishek

DevSecOps at a tech services company with 51-200 employees

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"Initially, we had a lot of images which were kind of very heavy and outdated, which I replaced with the help of Chainguard Containers distroless. Apart from it, I am continuously testing on CI builds, not yet finalized yet. The overall PR processing time is lower than others which I have tested right now. That is kind of a plus gain for us as well because we try to automate as much as possible. Having a reduced timeline accordingly helps us to navigate.."

Abhishek

DevSecOps at a tech services company with 51-200 employees

Read full review

Customer Service and Support

“The customer support, for me, was not great. It was okay. The response is saved and versus the solution received, it was not that much. I'll say that they have to improvise a lot on the customer support. The key thing, customer obsession is one of AWS's major things. If you are not following it thoroughly, then you will not be in the market. A faster product support team response would be really great..”

Abhishek
DevSecOps at a tech services company with 51-200 employees

Read full review

Other Advice

"If you are struggling with vulnerabilities and compliance management and looking for a secure base image solution, Chainguard Containers can be used, which has a catalog of thousands of images, so whatever you are building, you can directly pull images from Chainguard Containers, and it will be very helpful for you. I would rate this product 10 out of 10.."

Udit Parekh
DevOps Engineer at Veefin

Read full review

"I am not familiar with Chainguard Containers' AI capabilities.

Regarding the governance and security of those AI features, I was not and am not familiar with the AI features of Chainguard Containers.

I did not have any experience with the accuracy and reliability of output of Chainguard Containers' AI capabilities.

Chainguard Containers is primarily based on Alpine, and most of their images follow this pattern.

I would rate this review an eight overall.."

Verified user
DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

Read full review

“Regarding Chainguard Containers' AI capabilities, my thoughts on its governance and security are that not much is in place, as we have to use other tools to catch vulnerabilities during runtime. Although it has AI, it does not effectively catch all the vulnerabilities.

“The accuracy and reliability of the output from Chainguard Containers are below average, but I still give it an average rating of 6.5 to 7 because of its capabilities and its functionality for a developer-friendly approach.

“My advice for others looking into using Chainguard Containers is that as a firm working for an insurance company, everything we deploy and provision matters. If you want security at a granular level, Chainguard Containers is a great option. I would rate Chainguard Containers an 8 out of 10 because it is a simple tool, but it can still be enhanced in the future. Even though it is great, there are some lags. We are confident that there will not be any issues during build time, but in runtime, there are some hacks that cannot be tracked, changed, or prevented. If Chainguard Containers can address those runtime issues, that would be great. My overall review rating for Chainguard Containers is 10..”

ParthasarathyT
Senior Associate Infrastructure at Publicis Sapient

Read full review

“Chainguard Containers on its own, the tool is great. The only thing I liked about Chainguard Containers is that the secured by default philosophy they have. That is where I really got connected to it because being a DevSecOp, this is something we look for from the scratch, because there are a lot of pods that are running inside our infrastructure. I want that to ensure that no pod is going nuts and ensuring that all the data log that is being processed is being processed as a productive workload, not as some hackers' attempts.

“I am yet to get it to production right now because I am still in the evaluation phase. I am deliberately checking it out. It is a positive candidate for us to leverage

it. However, for now, I have not yet decided because I am continuously evaluating its competitor as well. The good part I love about it is that it has zero CVE alerts, SBOM in it. That is something I loved about it, but there are a few things that I actually did not like about it. There were some problems which occurred, and there were no quick fixes. I have to wait for a longer duration, the SLA is a long wait. Basically, there is no shell support, and I have to get time to debug the things. That is where I felt the freedom of having a dev environment, where basically I should be able to debug on my own, was something lacking.

“However, as a product, as a SaaS platform, if I integrate it to my platform, having a distroless image, is something that is cool. It helps to improve the team efficiency overall. However, as an individual person, I would love if there is some configurability there as well from a DevSecOps standpoint.

“I'll say that if you need a distroless container-based system where basically you do not want to increase your size of image just because you want to secure your infra, then Chainguard Containers is a very good product to evaluate because it has less noise and comparatively to other toolsets. The second thing is, it has SBOM and zero CVE alerts, which is something always every security engineer is looking for. You can scale on Kubernetes, that is the plus point. That is something that makes this a competitive candidate to always have a lookout for.

“I have covered my review from the last three months. I will be in a better state to have more discussion if we integrate it. I would rate this product a seven out of ten..”

Abhishek
DevSecOps at a tech services company with 51-200 employees

Read full review

Top Industries

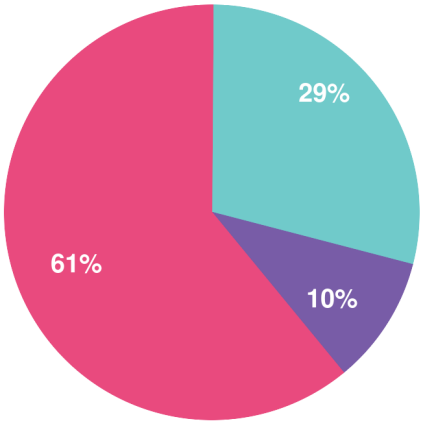
by visitors reading reviews

Manufacturing Company	16%
Financial Services Firm	8%
Computer Software Company	7%
Healthcare Company	7%

Company Size

by reviewers

by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944