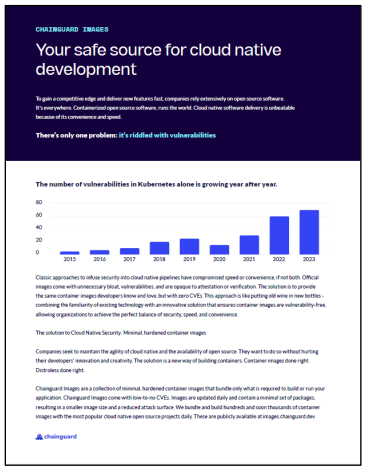
chainguard

carahsoft


CHAINGUARD IMAGES

Your safe source for cloud native development

To gain a competitive edge and deliver new features fast, companies rely extensively on open source software. It's everywhere. Containerized open source software, runs the world. Cloud native software delivery is unbeatable because of its convenience and speed.

There's only one problem: it's riddled with vulnerabilities

The number of vulnerabilities in Kubernetes alone is growing year after year.

Classic approaches to infuse security into cloud native pipelines have compromised speed or convenience, if not both. Official images come with unnecessary bloat, vulnerabilities, and are opaque to attestation or verification. The solution is to provide the same container images developers know and love, but with zero CVEs. This approach is like putting old wine in new bottles - combining the familiarity of existing technology with an innovative solution that ensures container images are vulnerability-free, allowing organizations to achieve the perfect balance of security, speed, and convenience.

The solution to Cloud Native Security: Minimal, hardened container images

Companies seek to maintain the agility of cloud native and the availability of open source. They want to do so without hurting their developers' innovation and creativity. The solution is a new way of building containers. Container images done right. Distroless done right.

Chainguard Images are a collection of minimal, hardened container images that bundle only what is required to build or run your application. Chainguard Images come with low-to-no CVEs. Images are updated daily and contain a minimal set of packages, resulting in a smaller image size and a reduced attack surface. We bundle and build hundreds and soon thousands of container images with the most popular cloud native open source projects daily. These are publicly available at images.chainguard.dev.

chainguard

Your Safe Source for Cloud Native Development

Chainguard Images

Thank you for downloading this Chainguard datasheet. Carahsoft is the public sector aggregator for Chainguard solutions available via NASA SEWP V, ITES-SW2, and other contract vehicles.

To learn how to take the next step toward acquiring Chainguard's solutions, please check out the following resources and information:

For additional resources:
carah.io/ChainguardResources

For upcoming events:
carah.io/ChainguardEvents

For additional Chainguard solutions:
carah.io/ChainguardSolutions

For additional DevSecOps solutions:
carah.io/DevSecOpsSolutions

To set up a meeting:
Chainguard@carahsoft.com
703-871-8570

To purchase, check out the contract vehicles available for procurement:
carah.io/ChainguardContracts

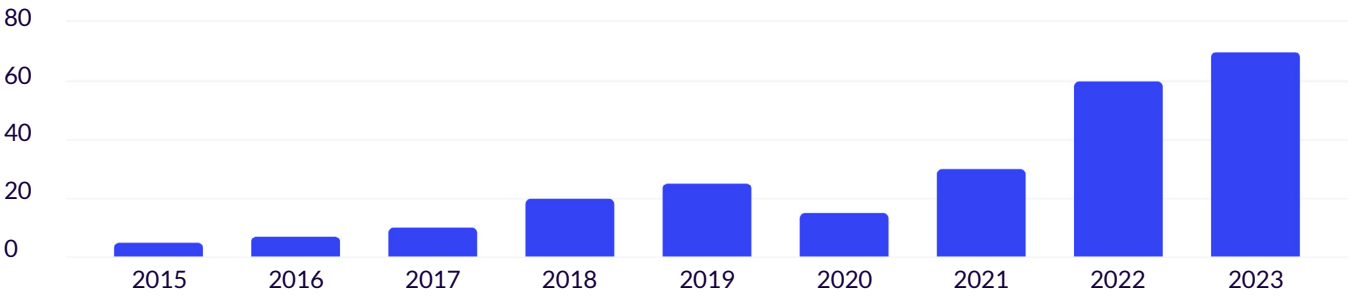
CHAINGUARD IMAGES

Your safe source for cloud native development

To gain a competitive edge and deliver new features fast, companies rely extensively on open source software. It's everywhere. Containerized open source software, runs the world. Cloud native software delivery is unbeatable because of its convenience and speed.

There's only one problem: it's riddled with vulnerabilities

The number of vulnerabilities in Kubernetes alone is growing year after year.



Classic approaches to infuse security into cloud native pipelines have compromised speed or convenience, if not both. Official images come with unnecessary bloat, vulnerabilities, and are opaque to attestation or verification. The solution is to provide the same container images developers know and love, but with zero CVEs. This approach is like putting old wine in new bottles - combining the familiarity of existing technology with an innovative solution that ensures container images are vulnerability-free, allowing organizations to achieve the perfect balance of security, speed, and convenience.

The solution to Cloud Native Security: Minimal, hardened container images

Companies seek to maintain the agility of cloud native and the availability of open source. They want to do so without hurting their developers' innovation and creativity. The solution is a new way of building containers. Container images done right. Distroless done right.

Chainguard Images are a collection of minimal, hardened container images that bundle only what is required to build or run your application. Chainguard Images come with low-to-no CVEs. Images are updated daily and contain a minimal set of packages, resulting in a smaller image size and a reduced attack surface. We bundle and build hundreds and soon thousands of container images with the most popular cloud native open source projects daily. These are publicly available at images.chainguard.dev.

chainguard

Production Images

Enterprise-ready – Patch and zero-CVEs SLAs included. CVEs are fixed and addressed in timelines that no one can beat.

Production-ready – These are battle-tested, fortified, nimble images ready for any production environment that track a specific version of the project they bundle.

Version specific – Pin your build process to a specific image version. Choose from an array of supported images listed in the public directory at images.chainguard.dev.

FIPS – designed to protect sensitive information and ensure compliance with gov't regulations, making them ideal for organizations handling classified or sensitive data.

Built from source daily – We built our own undistro – Wolfi – to be able to package the major cloud native projects and build them daily from SOURCE.

One command and it's done – Browse to the image you want and run a Docker pull to fetch the image from our registry in cgr.dev or from Docker Hub.

Fully OCI compatible – work seamlessly with any system that supports the OCI standard, including Docker.