Chainguard OS On Raspberry Pi

Secure Workloads Anywhere with Chainguard OS

Chainguard

About Me

- Staff DevRel Engineer at Chainguard
- Linux, VMs, containers, and PHP
- Hobbyist 3D designer and maker

What we'll talk about today

- How we got here: Wolfi and Chainguard OS
- Chainguard OS on the Raspberry Pi
- Demos
- What's next
- Q&A

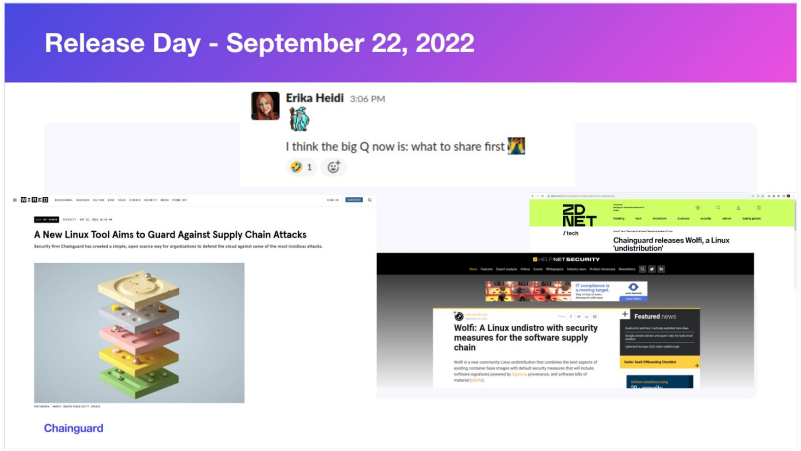
How We Got Here

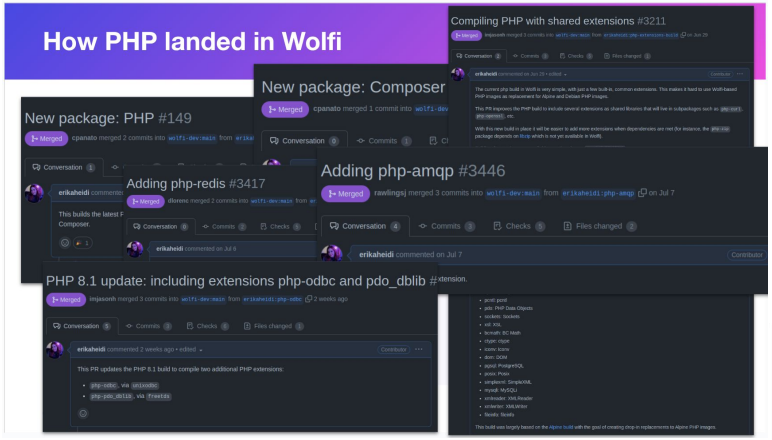
Wolfi and Chainguard OS

How we got here

Released in September 2022, **Wolfi** was the first rolling Linux distro **built for containers**. No kernel, no fluff: a minimal design to limit attack surface and daily builds for fresh packages.

All Hands on Deck: with a much smaller team, we all got involved in building the massive repository of packages that composed Wolfi. I helped with PHP.





How we got here

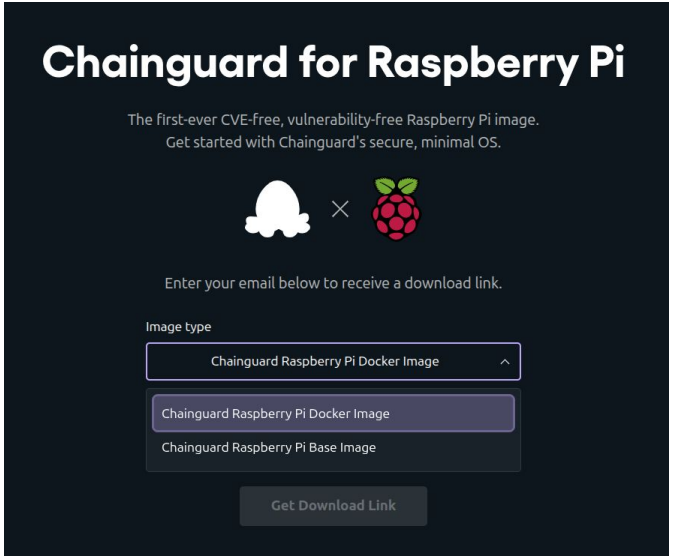
- Three years later, Wolfi OS still powers our free / starter images and doesn't have a kernel, running only on containers
- We built **Chainguard OS** as the **premium** version of Wolfi, including extended version support and enterprise-grade features
  - More packages and versions
  - Production-grade SLAs
  - Now with a Kernel! Increased portability
  - The base for all our paid products
    - a free degustation is available for the Raspberry Pi ;)

Chainguard OS on the Raspberry Pi

We're going bare metal

Chainguard OS for the Raspberry Pi

- Released in October 2025 as a beta freebie for makers and tinkerers, the Chainguard OS image for Raspberry Pi is a low-to-zero CVE base for your Raspberry projects
- Two versions: **Base** and **Docker Host**
- **Docker Host** image is designed for running containerized workloads, and emulates our Chainguard Docker Host VM image - includes both **docker** and **docker-compose** executables.



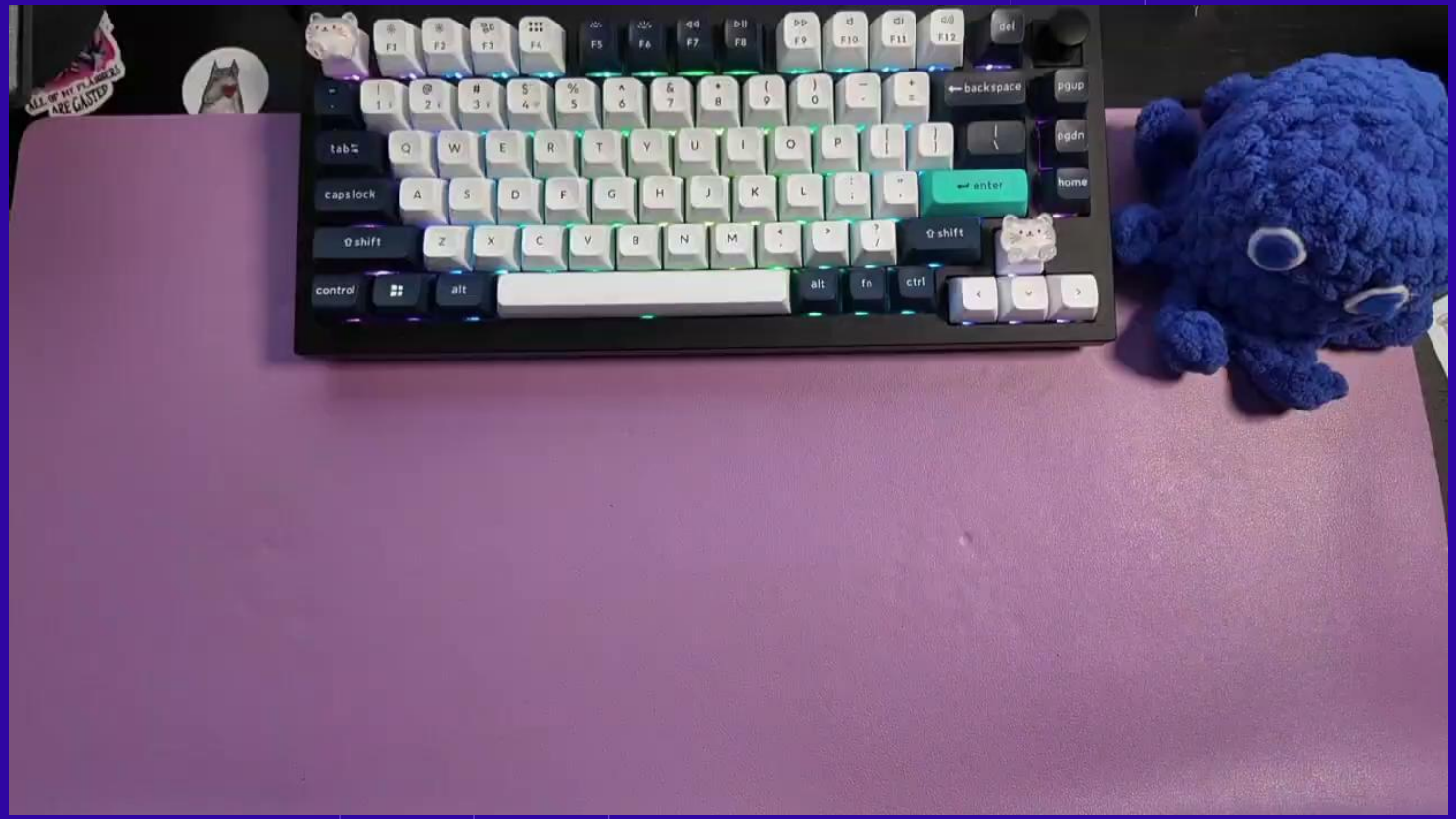
```
erika@stargate:~/Projects/raspi-chainguard

❯ ls
rpi-generic-base-arm64-20251102-032508.raw  rpi-generic-docker-arm64-20251102-032508.raw
❯ grype rpi-generic-base-arm64-20251102-032508.raw
 ✔ Vulnerability DB                [rehydrated]
 ✔ Indexed file system                            rpi-generic-base-arm64-20251102-032508.raw
 ✔ Cataloged contents              95269fb26b1b31a2bd71a1cf92e338f704cd118c5f3d6a429d2832318a
   ├── ✔ Packages                        [0 packages]
   └── ✔ Executables                     [0 executables]
 ✔ Scanned for vulnerabilities     [0 vulnerability matches]
   ├── by severity: 0 critical, 0 high, 0 medium, 0 low, 0 negligible
No vulnerabilities found
❯ grype rpi-generic-docker-arm64-20251102-032508.raw
 ✔ Indexed file system                           rpi-generic-docker-arm64-20251102-032508.raw
 ✔ Cataloged contents              76772b6af251ee78b3084d7b75b1cd74f456bbb0aa78b7a4fd73edbc6c
   ├── ✔ Packages                        [0 packages]
   └── ✔ Executables                     [0 executables]
 ✔ Scanned for vulnerabilities     [0 vulnerability matches]
   ├── by severity: 0 critical, 0 high, 0 medium, 0 low, 0 negligible
No vulnerabilities found

 ~/Projects/raspi-chainguard                                  took 13s  at 19:06:03
❯
```

Why this, and why now?

- The **Raspberry Pi** is one of the most beloved platforms for makers
  - Linux-based, higher level implementations
  - Easy to understand when compared to Arduino
- **Why not?** Since Chainguard OS now has a kernel of its own 👀

FEATURE	CHAINGUARD CONTAINER	CHAINGUARD VM
Includes Kernel?	**No** – uses host's kernel	**Yes** – ships and boots with its own hardened kernel

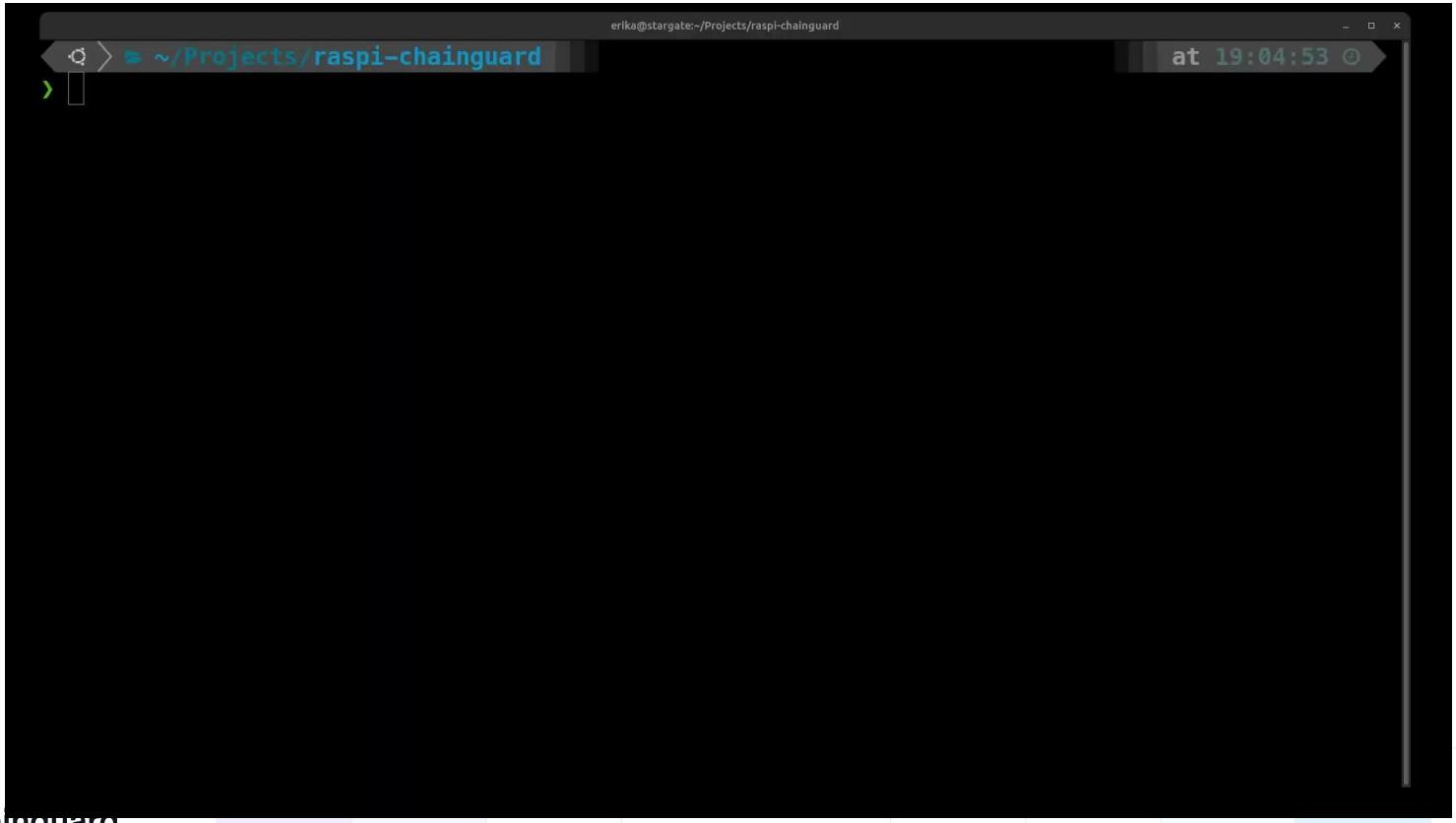
Video: Getting Started



Quickstart

- **Obtain the Image**
  - Visit **images.chainguard.dev/rpi** and fill the form to obtain a download link for the most up-to-date build of Chainguard OS for the Raspberry Pi
- **Build your boot disk**
  - Unpack the file
    - `gunzip rpi-generic-docker-arm64-*.raw.gz`
  - Plug a microSD to your computer and create the startup disk
    - `sudo dd if=rpi-generic-docker-arm64-*.raw of=/dev/sda bs=1M`
- **Boot the system**
  - Connect display, keyboard, and ethernet
  - Boot and log in with User `linky`, password `linky`
- **Find local network IP address**
  - run `ip addr` to find IP address (end0 interface)

Scanning the Image with Grype

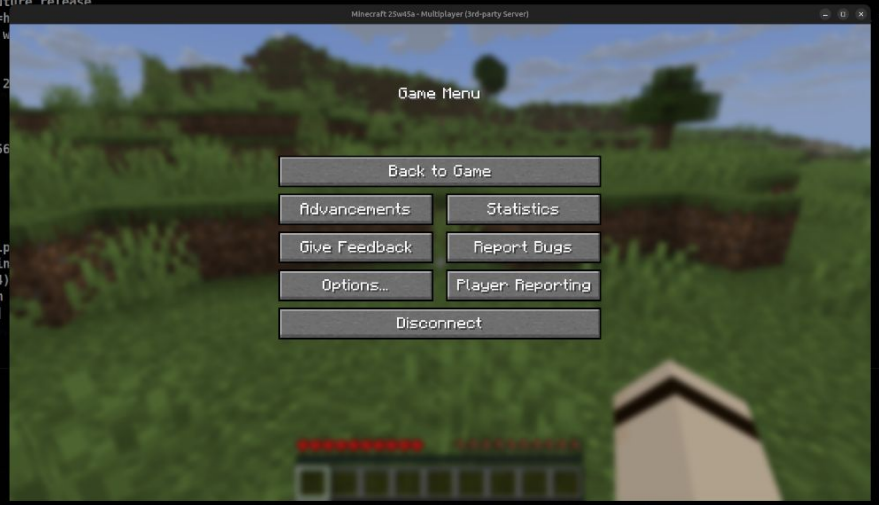


Demo: Guardcraft Pi

Running a Chainguarded Minecraft server on the Raspberry Pi 5

Demo: Chainguarded Minecraft server on RPi

```
Nov 7 17:33
ssh linky@192.168.178.36
java-server-1  | WARNING: java.lang.System::load has been called by com.sun.jna.Native in an unnamed module (file:/usr/share/minecraft/libraries/net/java/dev/jna/jna/5.17.0/jna-5.17.0.jar)
java-server-1  | WARNING: Use --enable-native-access=ALL-UNNAMED to avoid a warning for callers in this module
java-server-1  | WARNING: Restricted methods will be blocked in a future release unless native access is enabled
java-server-1  |
java-server-1  | WARNING: A terminally deprecated method in sun.misc.Unsafe has been called
java-server-1  | WARNING: sun.misc.Unsafe::objectFieldOffset has been called by org.joml.MemUtil$MemUtilUnsafe (file:/usr/share/minecraft/libraries/org/joml/joml/1.10.8/joml-1.10.8.jar)
java-server-1  | WARNING: Please consider reporting this to the maintainers of class org.joml.MemUtil$MemUtilUnsafe
java-server-1  | WARNING: sun.misc.Unsafe::objectFieldOffset will be removed in a future release
java-server-1  | [16:52:55] [ServerMain/INFO]: Environment: Environment[sessionHost=h
java-server-1  | [16:52:57] [ServerMain/INFO]: No existing world data, creating new w
java-server-1  | [16:52:58] [ServerMain/INFO]: Loaded 1470 recipes
java-server-1  | [16:52:58] [ServerMain/INFO]: Loaded 1584 advancements
java-server-1  | [16:52:58] [Server thread/INFO]: Starting minecraft server version 2
java-server-1  | [16:52:58] [Server thread/INFO]: Loading properties
java-server-1  | [16:52:58] [Server thread/INFO]: Default game type: SURVIVAL
java-server-1  | [16:52:58] [Server thread/INFO]: Generating keypair
java-server-1  | [16:52:59] [Server thread/INFO]: Starting Minecraft server on *:2556
java-server-1  | [16:52:59] [Server thread/INFO]: Preparing level "GuardCraft"
java-server-1  | [16:52:59] [Server thread/INFO]: Selecting global world spawn...
java-server-1  | [16:53:05] [Server thread/INFO]: Loading 0 persistent chunks...
java-server-1  | [16:53:05] [Server thread/INFO]: Preparing spawn area: 100%
java-server-1  | [16:53:05] [Server thread/INFO]: Time elapsed: 5678 ms
java-server-1  | [16:53:05] [Server thread/INFO]: Done (6.047s)! For help, type "help
java-server-1  | [16:54:05] [Server thread/INFO]: Server empty for 60 seconds, pausin
java-server-1  | [16:54:10] [Server thread/INFO]: boredcatmom (/192.168.178.40:52094)
java-server-1  | [16:54:28] [User Authenticator #1/INFO]: UUID of player boredcatmom
java-server-1  | [16:54:36] [Server thread/INFO]: boredcatmom[/192.168.178.40:45330]
java-server-1  | [16:54:36] [Server thread/INFO]: boredcatmom joined the game
localhost:~/guardcraft-server$

CPU variant     : 0x4
CPU part        : 0xd0b
CPU revision    : 1

Revision        : d04171
Serial          : 1203b6724ca216af
Model           : Raspberry Pi 5 Model B Rev 1.1
localhost:~$ cat /etc/os-release
ID=chainguard
NAME="Chainguard"
PRETTY_NAME="Chainguard"
VERSION_ID="20230214"
HOME_URL="https://chainguard.dev/"
localhost:~$
```



name=PROD]

Dockerfile

```
FROM cgr.dev/chainguard/jre:latest-dev

ARG VERSION="latest"
USER root
RUN apk update && apk add curl libudev jq
RUN adduser --system minecraft
WORKDIR /usr/share/minecraft

COPY build-config.sh server-install.sh /usr/share/minecraft/
RUN chmod +x /usr/share/minecraft/build-config.sh /usr/share/minecraft/server-install.sh
RUN /usr/share/minecraft/server-install.sh ${VERSION}
RUN chown -R minecraft /usr/share/minecraft
USER minecraft

ENTRYPOINT ["/usr/share/minecraft/build-config.sh", "java", "-jar" , "/usr/share/minecraft/server.jar", "nogui"]
```

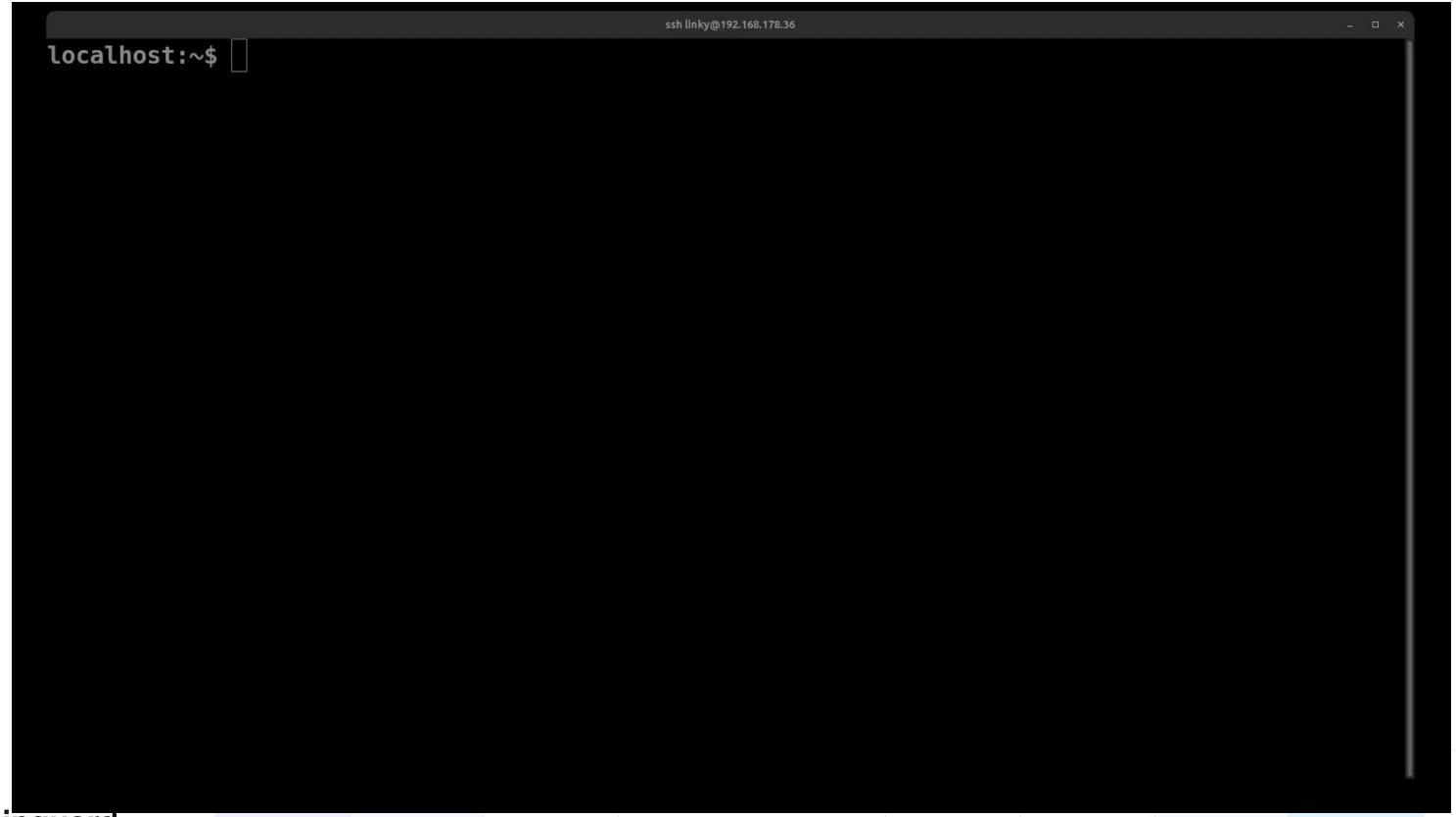
docker-compose.yaml

```yaml
services:
  java-server:
    image: guardcraft-server
    build:
      context: .
    restart: unless-stopped
    ports:
      - 25565:25565
    environment:
      # Server properties Set Up
      # MC_* variables will be replaced in the server.properties file
      # Hyphens must be replaced with underscores
      MC_gamemode: "survival"
      MC_difficulty: "easy"
      MC_motd: "Welcome to GuardCraft!"
      MC_level_name: "GuardCraft"
      MC_level_seed: "-1718501946501227358"
```

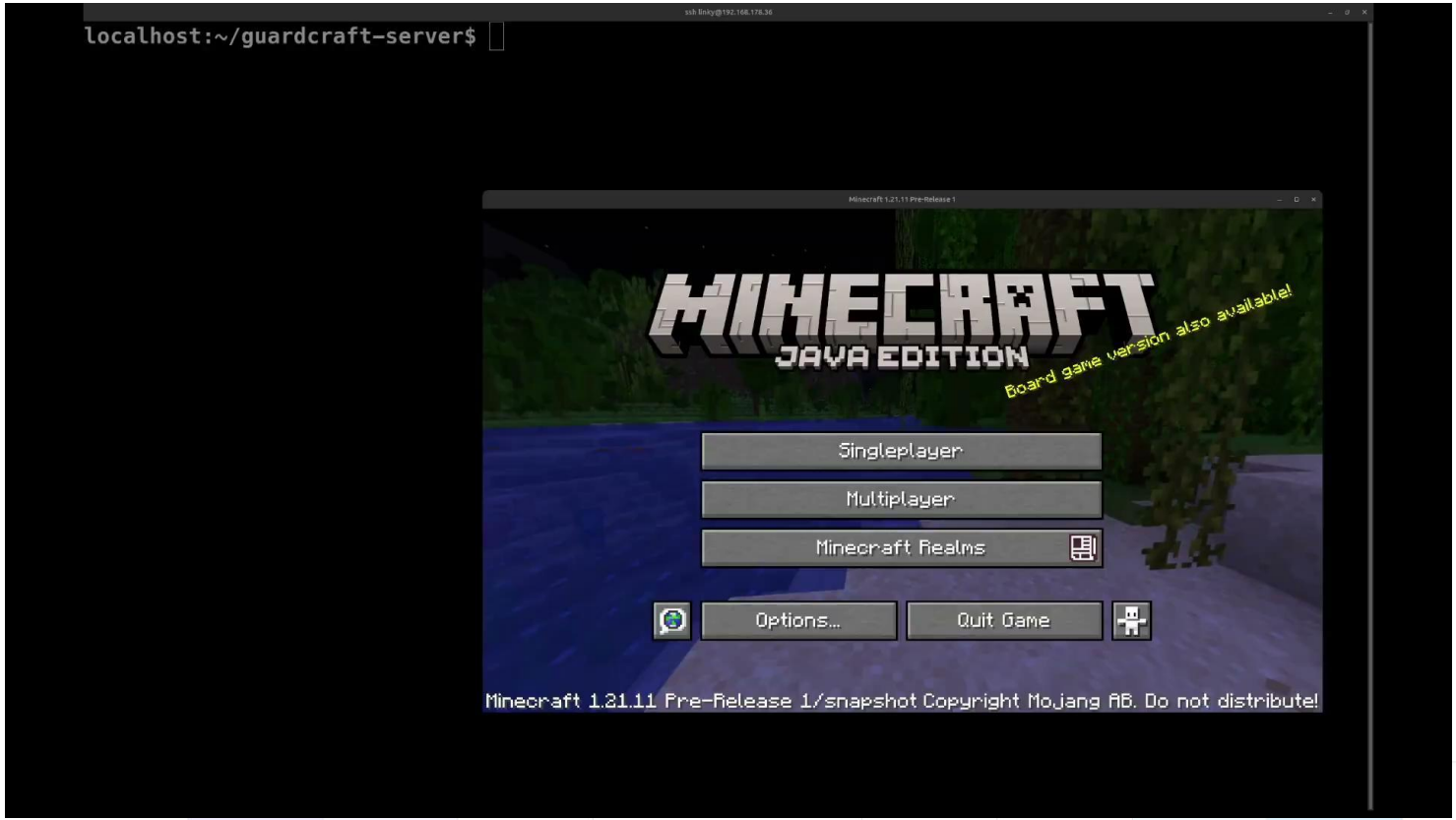
Quickstart

- **Clone the Repo**
  - `git clone https://github.com/chainguard-demo/guardcraft-server.git`
  - `cd guardcraft-server`
- **Configure Options**
  - Edit the `docker-compose.yaml` file if you want to change any of the default options, including the server seed
- **Build the Image**
  - `docker build . -t guardcraft-server`
- **Run the Server**
  - `docker-compose up`

Grype Scan: Guardcraft Image



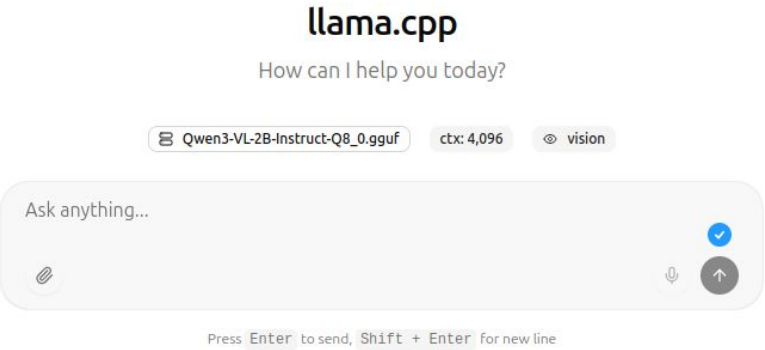
Live Demo


localhost:~/guardcraft-server$
MINECRAFT
JAVA EDITION
Board game version also available!
Singleplayer
Multiplayer
Minecraft Realms
Options...
Quit Game
Minecraft 1.21.11 Pre-Release 1/snapshot Copyright Mojang AB. Do not distribute!

Demo:
Open Source LLM server

Running a Chainguarded Llama.cpp server with open source LLMs on the Raspberry Pi 5

Demo: Chainguarded Llama.cpp server on RPi



Please describe this image for someone with low vision

This is a close-up photograph of a black French bulldog lying on a grey, ribbed fabric couch. The dog has a short, smooth coat and is looking directly at the camera with wide, dark eyes. It has a distinct facial structure with a wrinkled forehead and small, erect ears. A small patch of white fur is visible on its chest. The dog is holding a pink plush toy in its front paws; the toy is somewhat worn and appears to be a doll or a bear. The background is softly blurred, keeping the focus on the dog and the toy.

Statistics: 4.98 tokens/s 118 tokens 23.71s

Dockerfile

```
FROM cgr.dev/chainguard/gcc-glibc:latest-dev

RUN apk add cmake --no-cache
WORKDIR /opt/llama
RUN git clone https://github.com/ggerganov/llama.cpp.git && cd llama.cpp

WORKDIR /opt/llama/llama.cpp
RUN cmake -B build -DLLAMA_CURL=OFF && cmake --build build --config Release

ENTRYPOINT ["/opt/llama/llama.cpp/build/bin/llama-server"]
```

Docker Run Command for Reference

```
docker run --rm --device /dev/dri/card1 --device /dev/dri/renderD128 \
 -v ${PWD}/models:/models -p 8000:8000 wolfi-llama:latest --no-mmap --no-warmup \
 -m /models/Qwen3-VL-2B-Instruct-Q8_0.gguf --mmproj /models/mmproj-F32.gguf \
 --port 8000 --host 0.0.0.0 -n 512 \
 --temp 0.7 \
 --top-p 0.8 \
 --top-k 20 \
 --presence-penalty 1.5
```

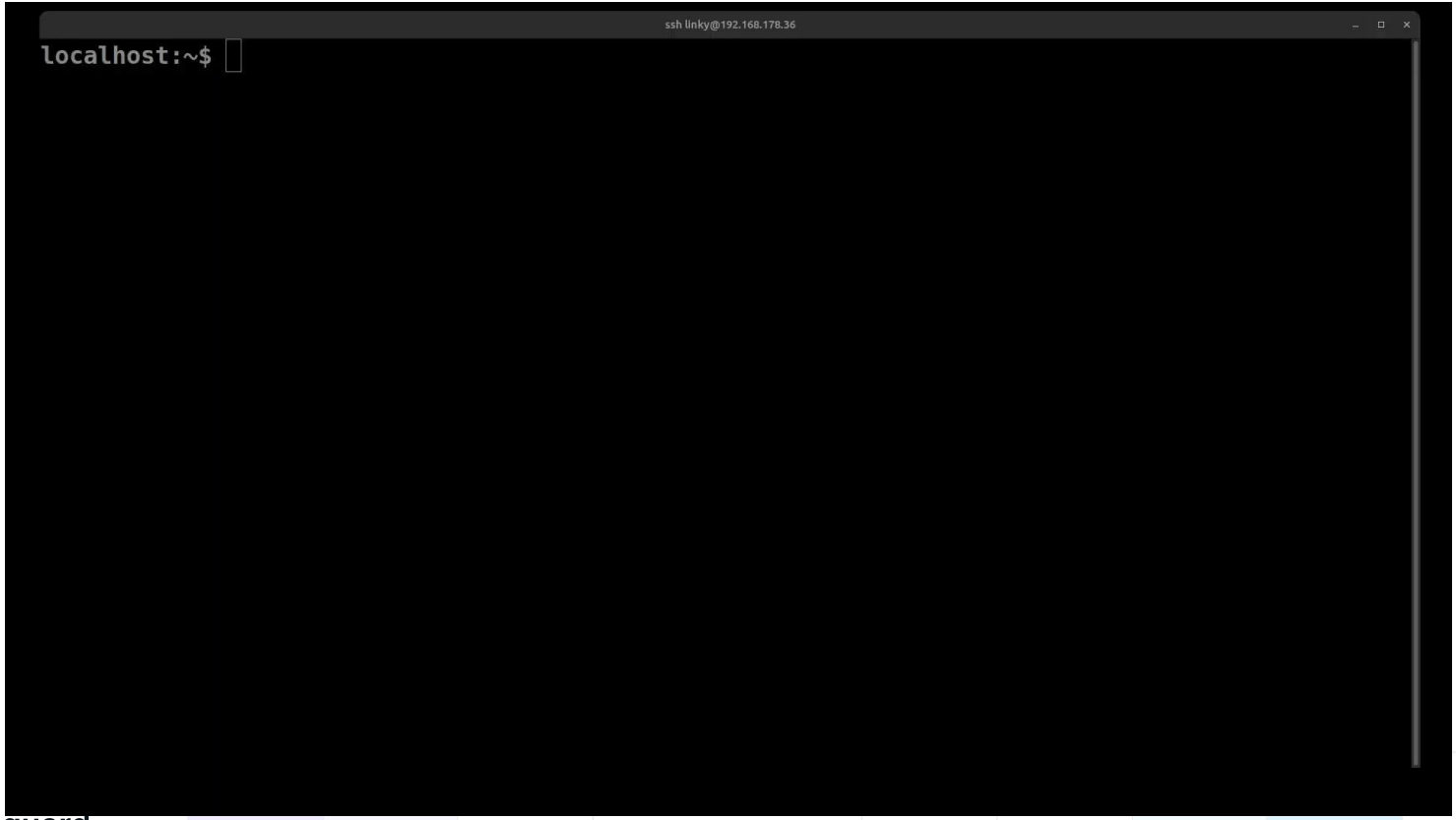
docker-compose.yaml

```
services:
  llama:
    image: wolfi-llama
    build:
      context: .
    restart: unless-stopped
    ports:
      - 8000:8000
    command: --no-mmap --no-warmup -m /models/Qwen3-VL-2B-Instruct-Q8_0.gguf --mmproj
/models/mmproj-F32.gguf --port 8000 --host 0.0.0.0 -n 512 --temp 0.7 --top-p 0.8 --top-k 20
--presence-penalty 1.5
    volumes:
      - ./models:/models:ro

volumes:
  models:
```

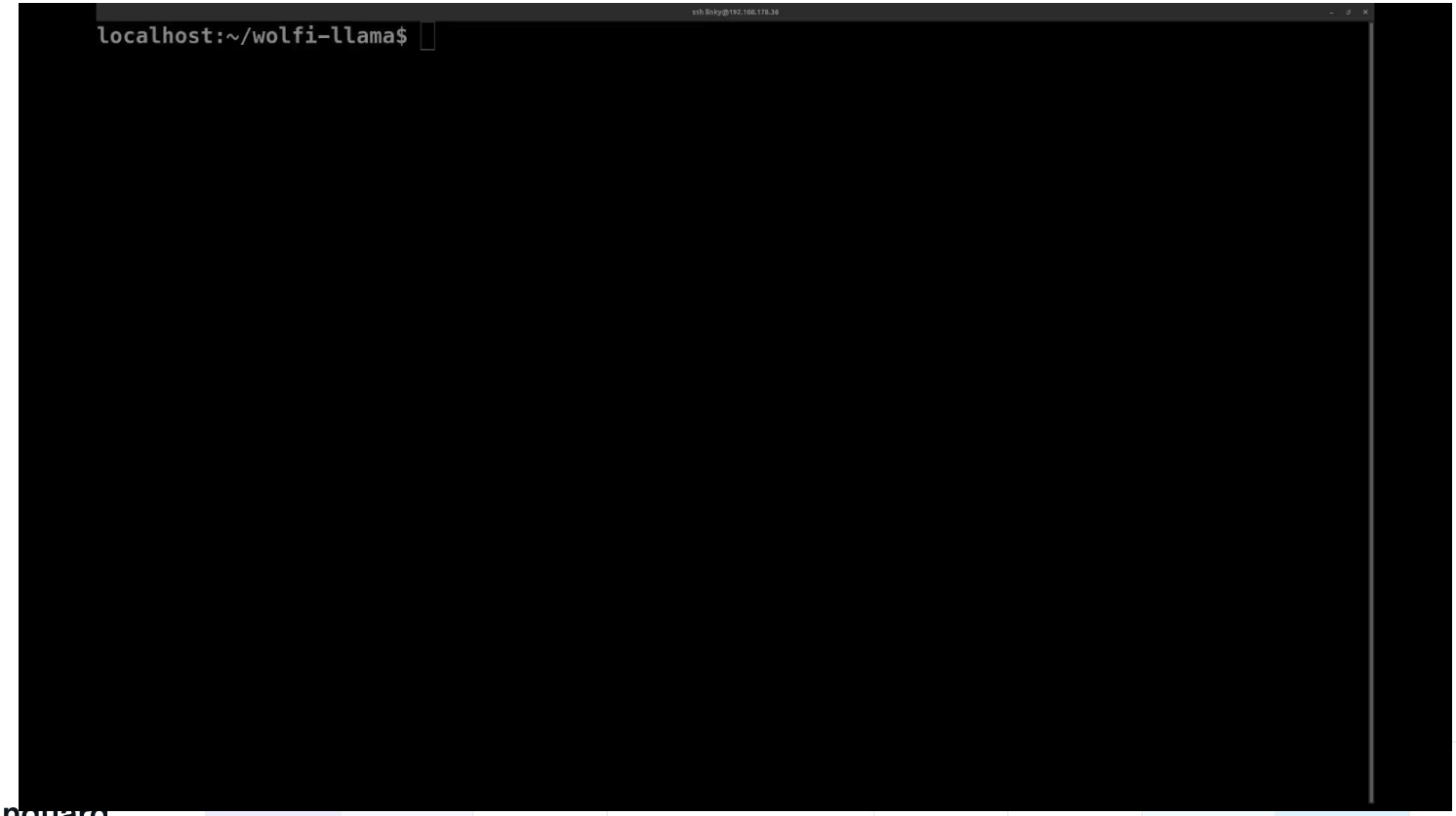
Quickstart

- **Clone the Repo**
  - `git clone https://github.com/erikaheidi/wolfi-llama.git`
- **Build the Image**
  - `docker build . -t wolfi-llama`
- **Download the Qwen3-VL open source model from Huggingface**
  - `curl -L -O` https://huggingface.co/unsloth/Qwen3-VL-2B-Instruct-GGUF/resolve/main/Qwen3-VL-2B-Instruct-Q8_0.gguf?download=true
  - `curl -L -O` https://huggingface.co/unsloth/Qwen3-VL-2B-Instruct-GGUF/resolve/main/mmproj-F32.gguf?download=true
- **Run the Server**
  - `docker-compose up`

Grype Scan: wolfi-llama Image



Live Demo



What's Next

Now: Chainguard VMs Compliance Features

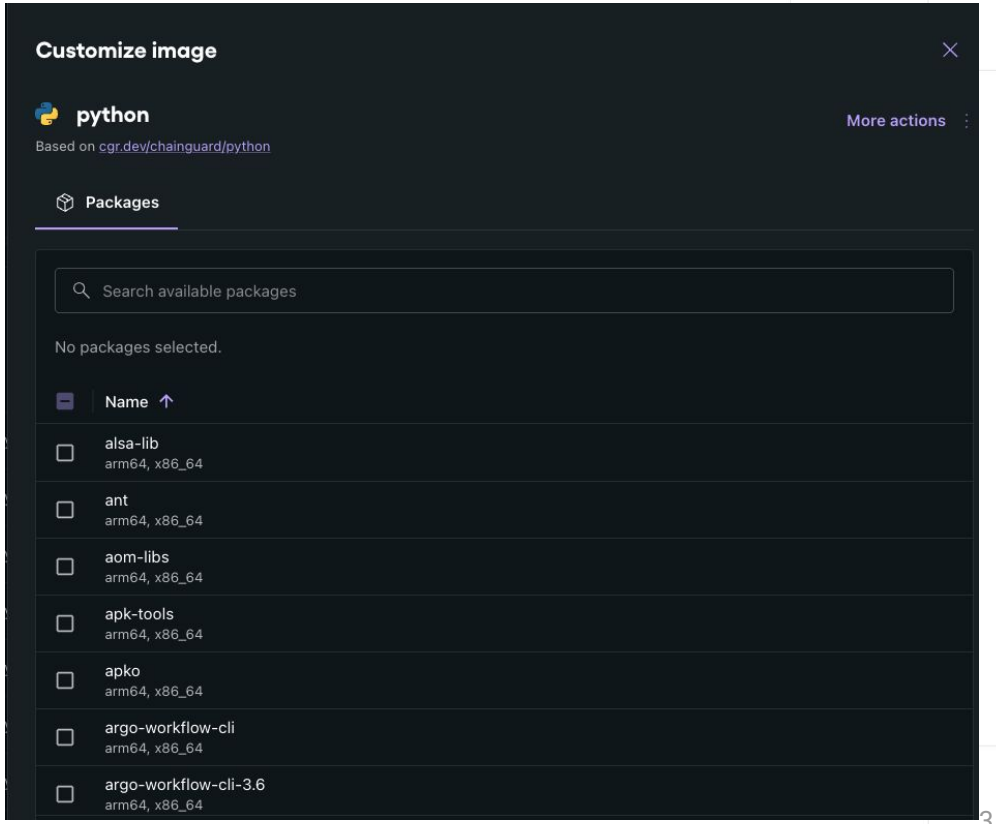
- Announced today, the new compliance features for Chainguard VMs empower engineering teams to ship faster compliant workloads to production
- Drop-in VM replacements for AWS, Azure, and GCP that deliver instant FIPS 140-3 compliance without workflow disruption
- Pre-configured to meet CIS Level 1 and DISA STIG requirements

Next: Custom Assembly for VMs

Make golden image pipelines a thing of the past

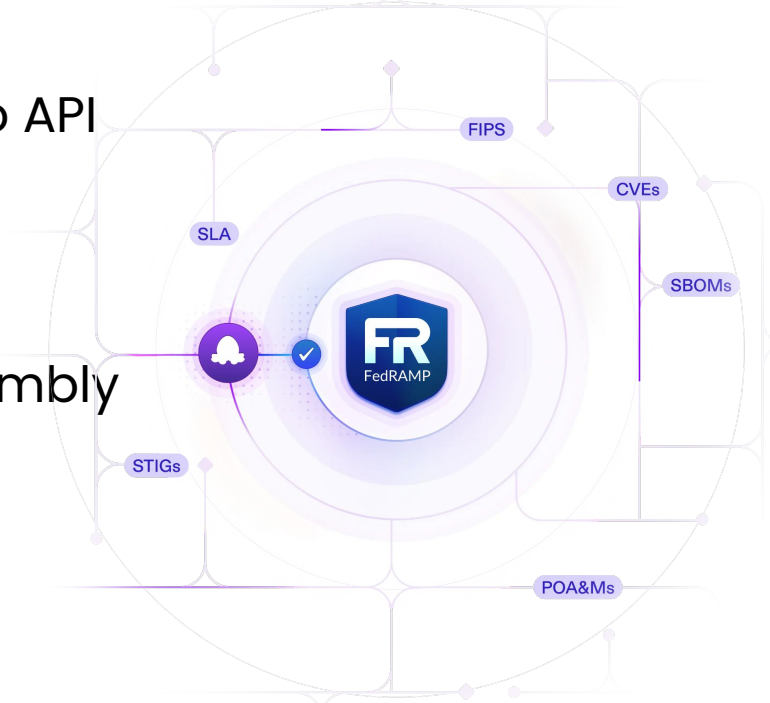
Specify VM image requirements: packages, target deployment platform, processor architecture, security hardening, FIPS etc..

Chainguard Custom Assembly builds the image and refreshes it every day



The future of Chainguard VMs

1. Full kernel level FIPS with crypto API
2. Hyper-V support
3. Grow the VMs catalog
4. Chainguard VMs Custom Assembly
5. Immutable Chainguard VMs
6. In place updates



Coming soon!

The future of Chainguard VMs

- Join our Next Learning Labs o **December 16** to learn more about **Chainguard VMs**!
  - Register here

Resources

Resources

- **Chainguard's FIPS-validated, hardened VM images: compliance Without the complexity**
- **A Gift for the Open Source Community: Chainguard's CVE-Free Raspberry Pi Images (Beta)**
- **Tutorial: Setting Up a Minecraft Server with the JRE Chainguard Container**
- **Tutorial: Running Open Source LLMs on a Raspberry Pi 5 with Llama.cpp**
- Guardcraft Demo Repository
- Wolfi-llama Demo Repository

Thank you!

chainguard.dev