Docker Hardened Images *(now free!)*

The new standard for building securely

Mike Donovan VP Product Management, Docker
Nikhil Kaul VP Product Marketing, Docker

Housekeeping

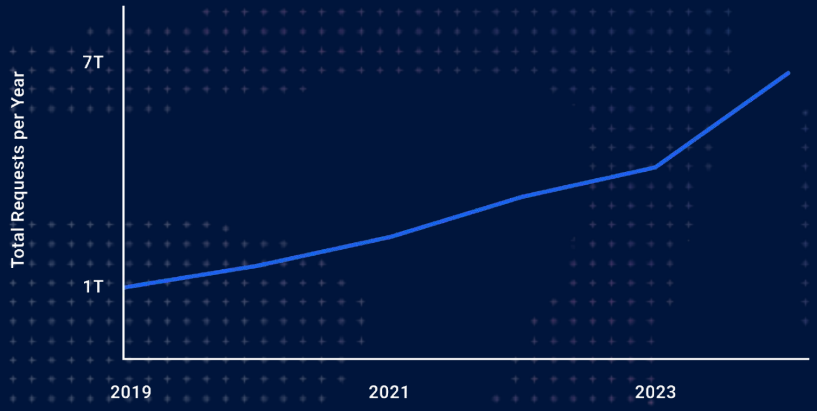
Session is being recorded and will be shared

Please use the Q&A feature to ask questions

Please fill out the survey at the end

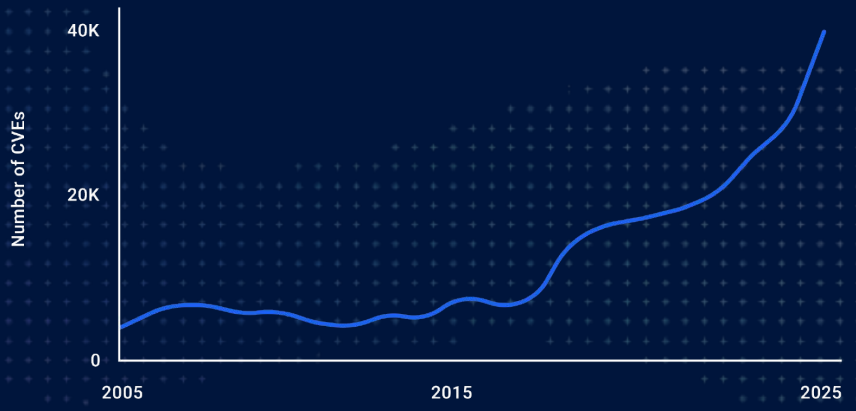
Container adoption and CVEs are both growing exponentially

Open-source downloads across major ecosystems



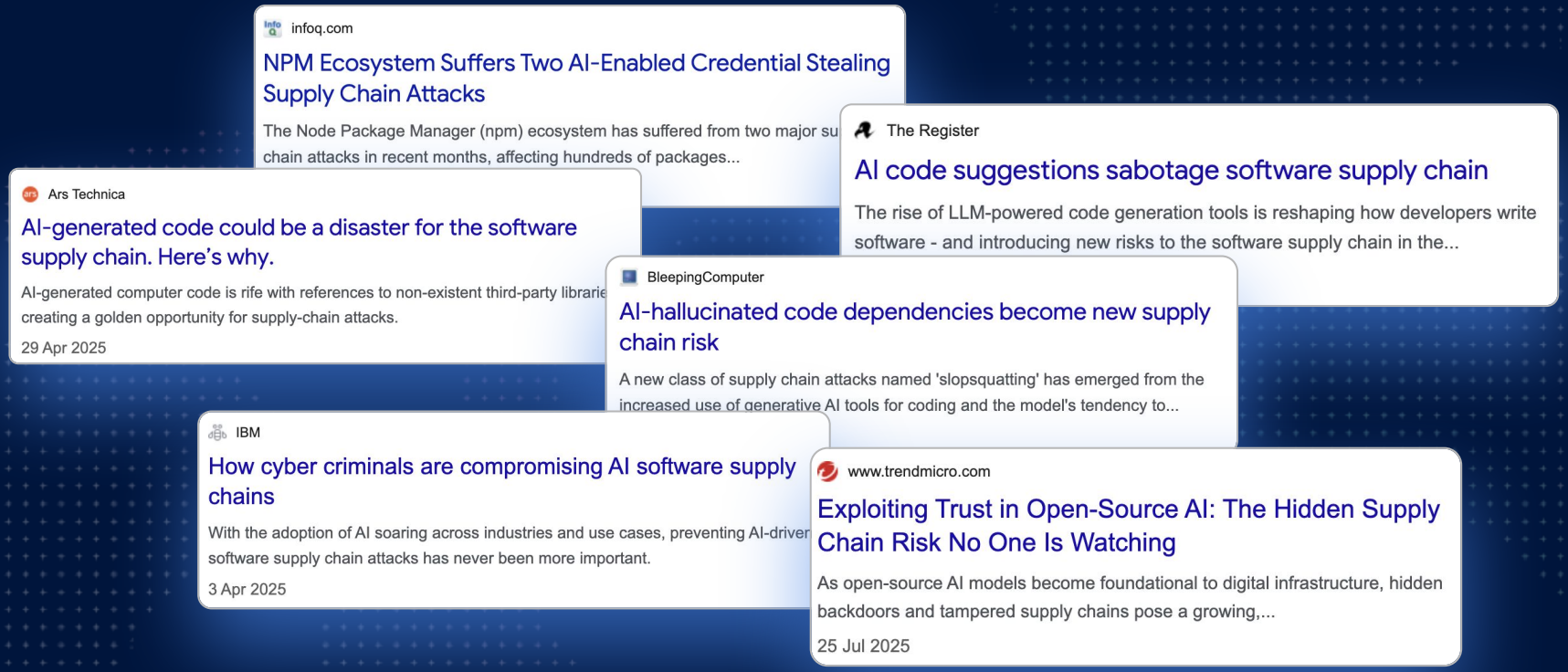
Source: Sonatype
www.sonatype.com/state-of-the-software-supply-chain/introduction

Total Common Vulnerabilities and Exposures (CVEs)

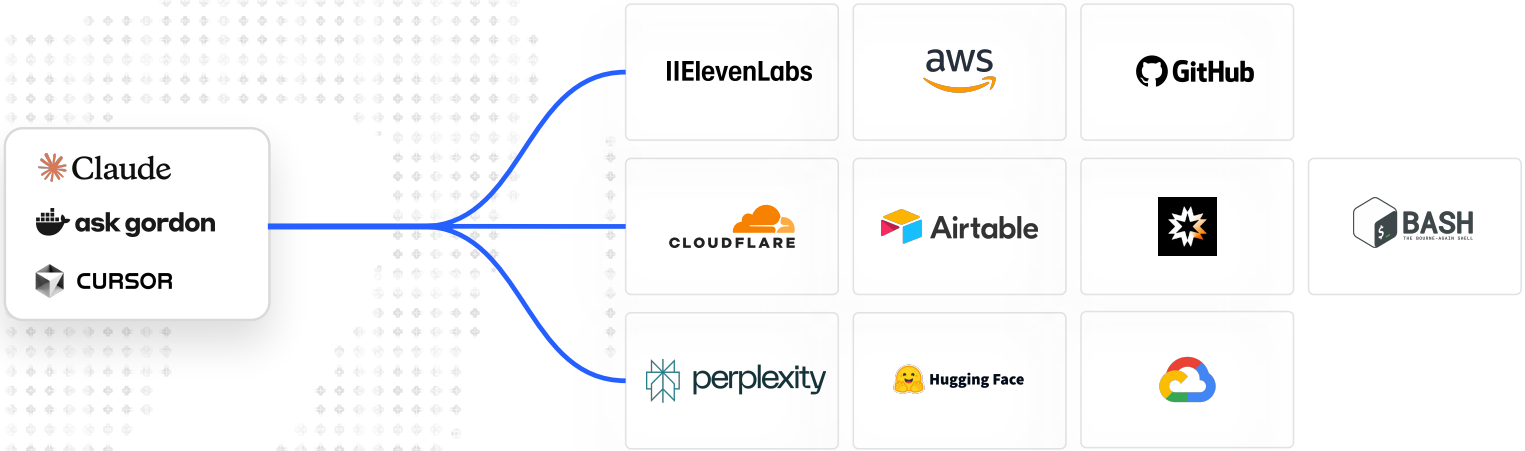


Source: National Vulnerability Database
788960_C

The stakes are higher with autonomous decisions driven by AI



With MCP, non-deterministic tool execution adds further complexity and risk



Same security principles.
Entirely new surface area.

- Isolation - limited blast radius
- Minimalism - reduced attack surface
- Provenance - verifiable trust
- Visible vulnerabilities - SBOMs, VEX

We have lived through this transition once with **containers.**

Stewardship at internet scale:

Docker’s role in securing MCP and containers

Monthly pulls	20B+
Developers	20M+
CE deployments	50M+
Containerized apps that run on Docker images	80%+

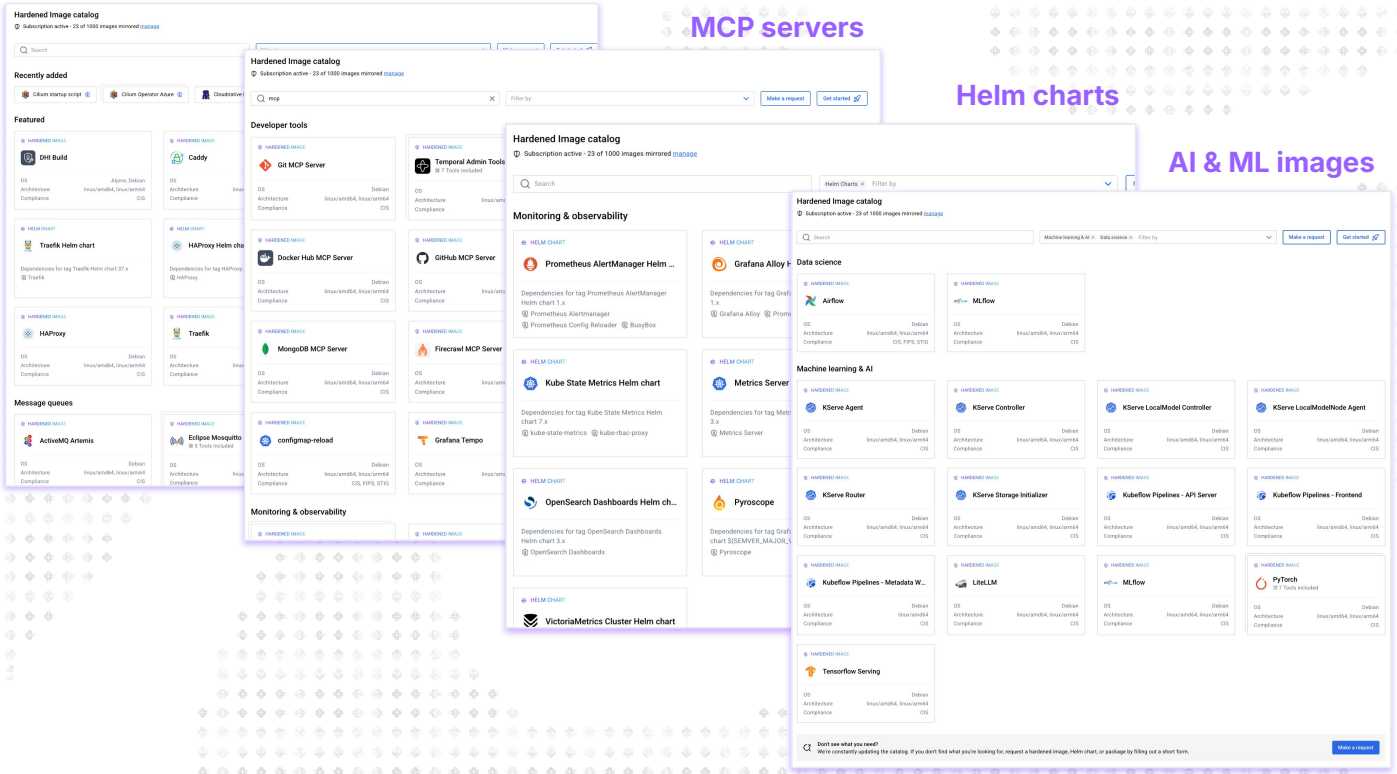
Docker Hardened Images:
The foundation for secure MCP, containers, and more

Hardened base and app images

MCP servers

Helm charts

AI & ML images



Expecting every team to manage CVEs, rebuild images, validate fixes... across every dimension

To do

- Customization pipeline
- Compliance
- Release engineering
- Test and validation
- Security engineering
- Build and provenance
- Platform engineering
- Upstream lifecycles

× times

Image Types

Every base OS image
Every runtime (Python, Node, etc.)
Every application image
Every variant (debian, alpine, dev, prod)
Every architecture (amd64, arm64)

× times

Versions & Lifecycles

Every major version
Every minor and patch version
Every supported upstream lifecycle
Every EOL transition
Every backported fix

× times

Security events

Every new CVE
Every severity change
Every exploit disclosure
Every dependency vulnerability

× times

Compliance & Policy

Every compliance standard (FIPS, STIG)
Every regulated environment
Every customer customization

This is very hard to do at scale

Docker handles all of this complexity on your behalf

Upstream lifecycles

- Release detection
- Advisory ingestion
- Version handling

Platform engineering

- BuildKit orchestration
- Hardened CI
- -Multi-arch builders

Build and provenance

-Source-based builds

- Pinned inputs

-SLSA-aligned provenance capture

Security engineering

- Network isolation
- Malware, vuln scanning
- VEX

Test and validation

- Functional container tests
- Deployment level validation

Release engineering

-Digest-first publishing

- Multi-arch image indexing

Compliance

- FIPS, STIG validation
- SOC2, other regimes

Customization pipeline

-Secure image extension

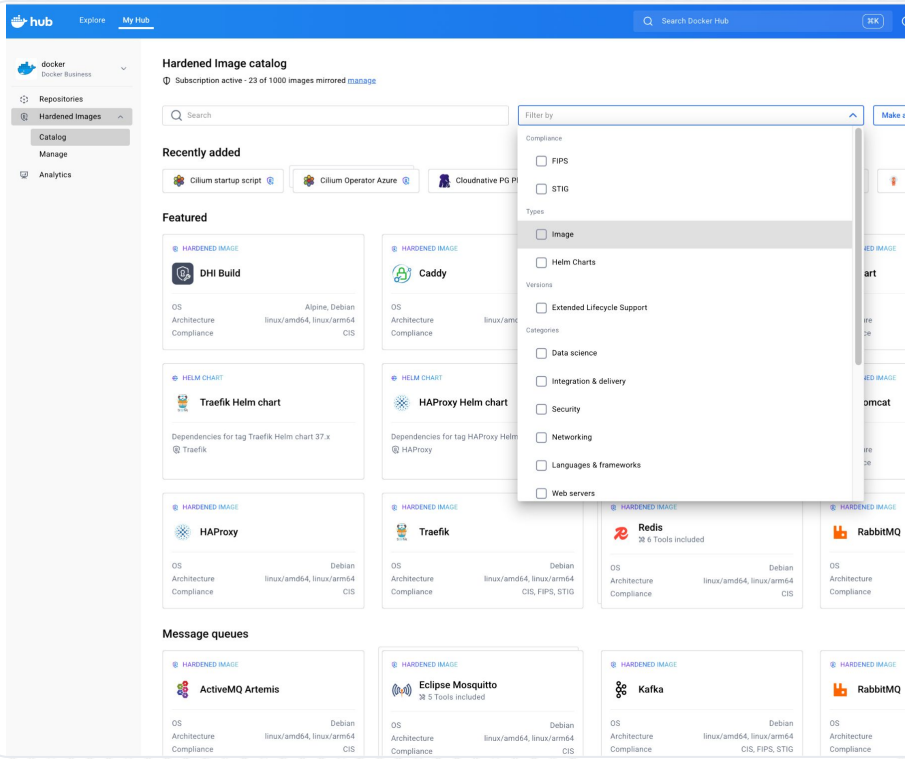
- Inherited guardrails

dockr.ly/fivepilars

***Read blog**: Docker's approach - Five Pillars for Supply Chain Security*

Docker Hardened Images - now FREE to use for every developer

- Fully open source under Apache 2.0
- 1000+ hardened, minimal images with near-zero CVEs
- Verifiable SBOMs and SLSA Build Level 3 provenance
- Multi-distro compatibility



See it in action (demo)

DHI Enterprise and DHI ELS: Guarantees when teams need them most

DHI Enterprise

Everything in DHI, plus operational and security enhancements.

Includes:

- ✓ Critical CVE fixes <7 days
- ✓ FIPS/STIG variants
- ✓ Image lifecycle management with customization
- ✓ Built on Docker's secure build system

DHI ELS

(requires Enterprise)

Security and compliance support for end-of-life software.

Includes:

- ✓ +5 years of hardened updates
- ✓ Updated SBOMs & provenance
- ✓ Maintains compliance post-EOL
- ✓ Protects long-lived workloads

But production teams need guarantees, not just artifacts

01

Patch SLAs

02

Customization

03

Compliance

(SOC2, FIPS & STIG..)

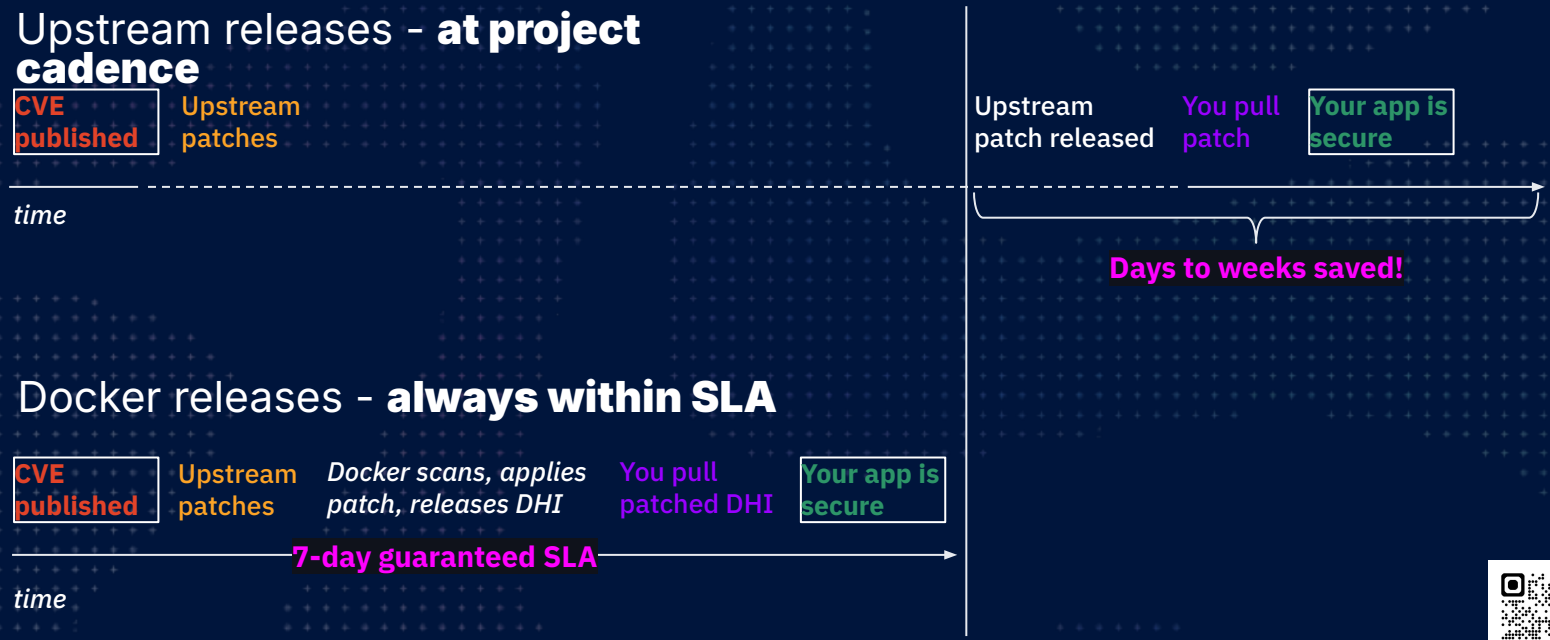
04

Extended Lifecycle Support

More than patches - we take on responsibility

- Docker is responsible for patching under the SLA
- Customizations delivered within SLA
- Customizations preserved in upgrades & patches

DHI SLA guarantees access to fixes - even before a patch is released



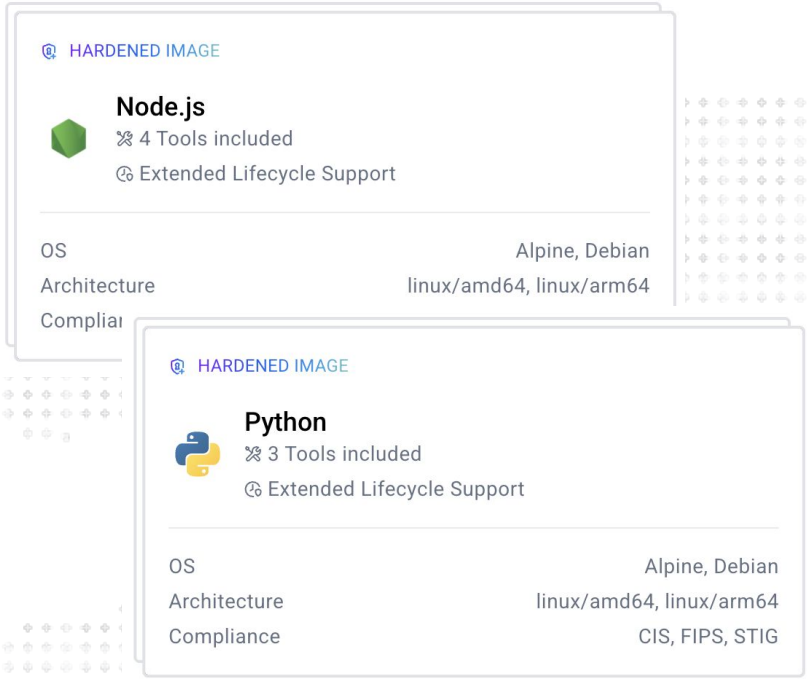
dockr.ly/patchupstream

We also patch upstream when we can! ***Read blog:***

Extended Lifecycle Support (ELS) add-on available with DHI Enterprise

Security That Outlives Upstream:

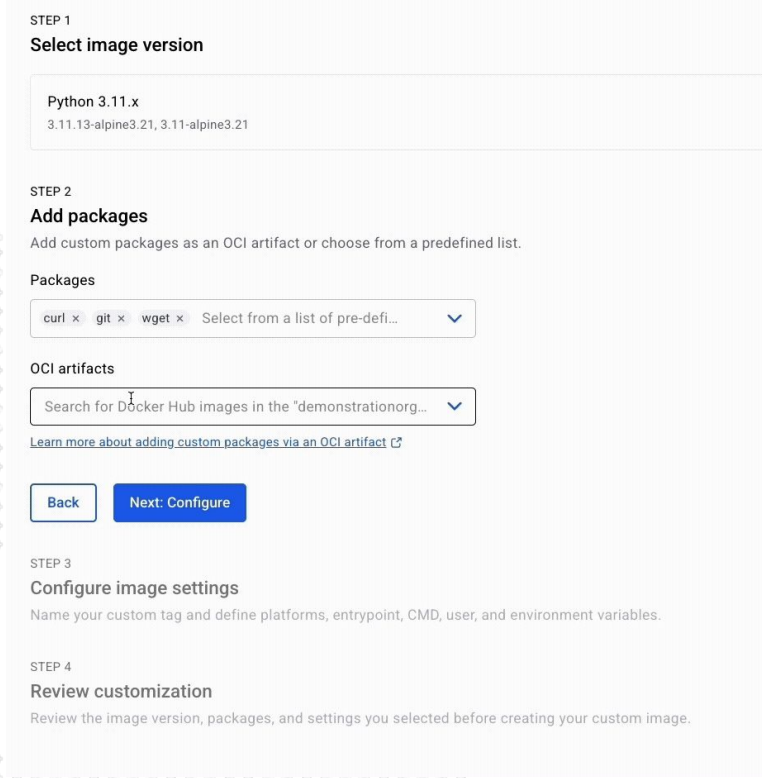
- **+5 years of hardened updates**
- **Updated SBOMs & provenance**
- **Maintains compliance post-EOL**
- **Protects long-lived workloads**



Flexible customization: certs, tools, packages...

SLSA Level 3

Docker Hardened Image + **Scripts/Certs**



See it in action (demo)

Built to fit seamlessly into your DevSecOps stack

Microsoft

NGINX

Google Cloud

WIZ

GitLab

cloudsmith

sonatype

What Our Customers & Partners Are Saying

"Security shouldn't be a premium feature. By making hardened images free, Docker is letting every developer—not just big enterprises—start with a safer foundation. We love seeing tools that reduce noise and toil, and we're ready to run these secure workloads on Google Cloud from day one."

Ryan J Salva, Senior Director of Product, Developer Experiences

Google

"We evaluated multiple options for hardened base images and chose Docker Hardened Images (DHI) for its alignment with our supply chain security posture, developer tooling compatibility, Docker's maturity in this space, and integration with our existing infrastructure. Our focus was on balancing trust, maintainability, and ecosystem compatibility."

Vikram Sethi, Principal Scientist at Adobe

Adobe

"For the first time, I don't have to worry about what's hiding in our base images. That mental overhead is gone, and we can finally focus on the security challenges that are unique to Attentive."

Jacob Rickerd, Principal Security Engineer at Attentive

attentive

"Docker's move to make its hardened images freely available under Apache 2.0 underscores its strong commitment to the open source ecosystem. Many CNCF projects can already be found in the DHI catalog, and giving the broader community access to secure, well-maintained building blocks helps us strengthen the software supply chain together. It's exciting to see Docker continue to invest in open collaboration and secure container infrastructure."

Jonathan Bryce, Executive Director, Cloud Native Computing Foundation

CLOUD NATIVE COMPUTING FOUNDATION

DHI Enterprise Security: Verified by Independent Experts

Independent assessment by SRLabs

- Cryptographic Integrity
- Rootless by Default
- SBOM and VEX Metadata
- Minimal Attack Surface

"Docker Hardened Images deliver on their public security promises for today's threat landscape: all images we sampled are **signed, supply-chain-scanned, and run rootless**; no critical or high-severity break-outs were identified in three weeks of directed testing."

SRLabs

dockr.ly/dhigithub

Limited edition Docker Lego and swag giveaway!

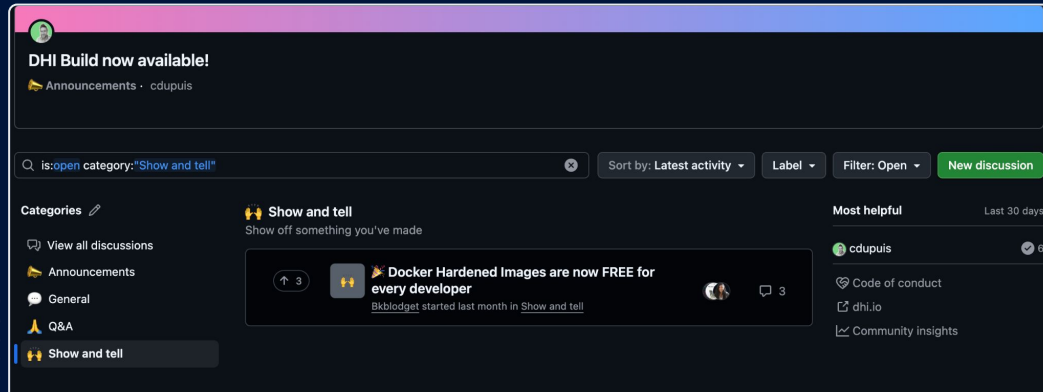
Illustrative images

1. **Update OSS project to use DHI**

2. **Post it to the DHI "Show and Tell" discussion in Github**

github.com/orgs/docker-hardened-images/discussions

Include link to project!



Docker Hardened Images

Use free, and try Enterprise features 30-day trial

Explore the catalog

dockr.ly/freetrial

Get in touch with us

Find the Docker team

YouTube, LinkedIn, X, Bluesky

DHI Discussions on GitHub

dockr.ly/dhigithub

Docker on

Community Slack