



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

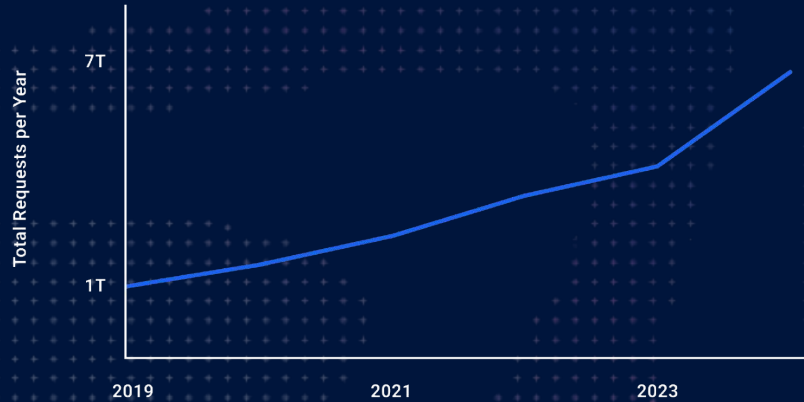


Please fill out the
survey at the end



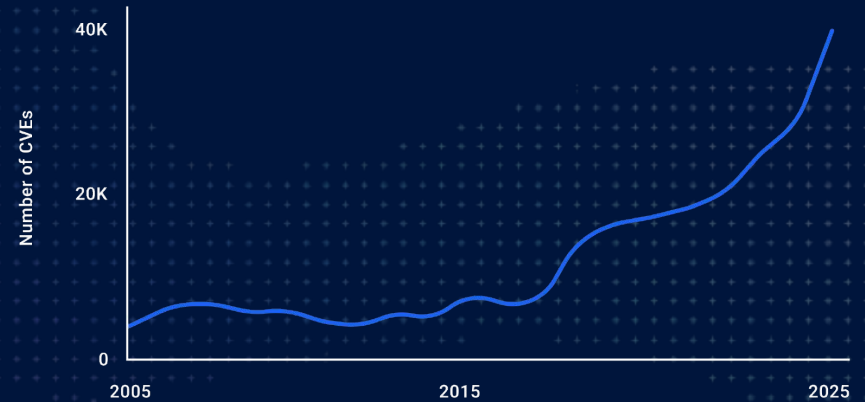
Container adoption and CVEs are both growing exponentially

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

infoq.com

NPM Ecosystem Suffers Two AI-Enabled Credential Stealing Supply Chain Attacks

The Node Package Manager (npm) ecosystem has suffered from two major supply chain attacks in recent months, affecting hundreds of packages...

Ars Technica

AI-generated code could be a disaster for the software supply chain. Here's why.

AI-generated computer code is rife with references to non-existent third-party libraries, creating a golden opportunity for supply-chain attacks.

29 Apr 2025

The Register

AI code suggestions sabotage software supply chain

The rise of LLM-powered code generation tools is reshaping how developers write software - and introducing new risks to the software supply chain in the...

BleepingComputer

AI-hallucinated code dependencies become new supply chain risk

A new class of supply chain attacks named 'slopsquatting' has emerged from the increased use of generative AI tools for coding and the model's tendency to...

IBM

How cyber criminals are compromising AI software supply chains

With the adoption of AI soaring across industries and use cases, preventing AI-driven software supply chain attacks has never been more important.

3 Apr 2025

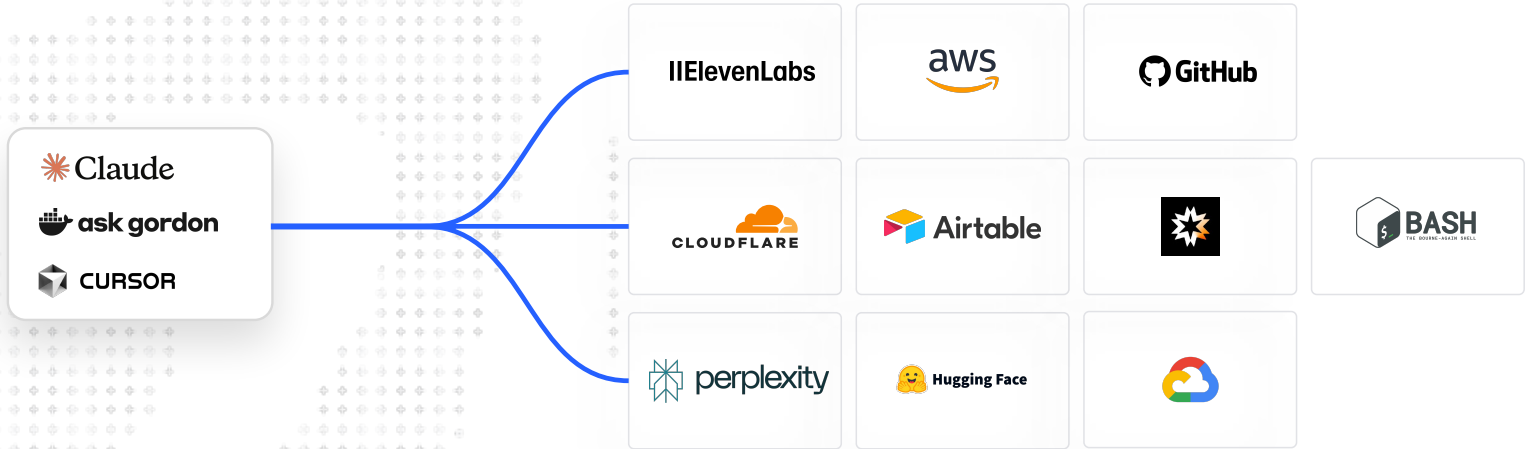
www.trendmicro.com

Exploiting Trust in Open-Source AI: The Hidden Supply Chain Risk No One Is Watching

As open-source AI models become foundational to digital infrastructure, hidden backdoors and tampered supply chains pose a growing...

25 Jul 2025

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

The image displays a collage of screenshots from the Docker Hardened Image Catalog website. The screenshots are arranged in a layered, overlapping fashion, showcasing different categories of images and Helm charts. The categories visible include:

- Hardened Image catalog:** The main landing page showing a search bar, subscription status, and a grid of featured images like DHI Build, Caddy, and Git MCP Server.
- Developer tools:** A section featuring images such as Docker Hub MCP Server, GitHub MCP Server, and MongoDB MCP Server.
- Monitoring & observability:** A section with Helm charts for Prometheus AlertManager, Grafana Alloy, Kube State Metrics Helm chart, and OpenSearch Dashboards.
- Machine learning & AI:** A section with Helm charts for K8serve Agent, K8serve Controller, K8serve LocalModel Controller, and K8serve LocalModel Agent.
- Data science:** A section with images for Airflow and MLflow.
- Infrastructure:** A section with images for K8serve Router, K8serve Storage Initiator, and K8serve Pipelines - API Server.
- AI & ML images:** A section with images for LlamaLLM, MLflow, and PyTorch.

The screenshots also show various filters, search results, and dependency lists for each image or chart, providing a detailed view of the catalog's content.



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

✓ To do



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/fivepillars

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




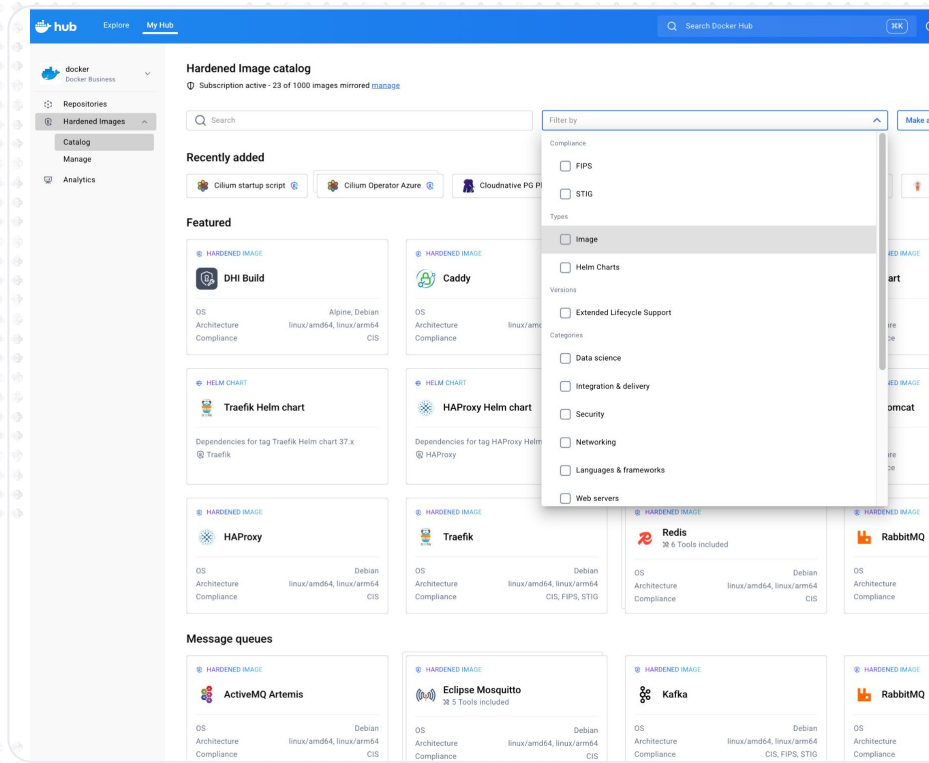
Docker Hardened Images - now FREE to use for every developer

 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



The screenshot displays the Docker Hub interface for the 'Hardened Image catalog'. The top navigation bar includes 'hub', 'Explore', and 'My Hub'. A search bar is present, and a filter dropdown menu is open, showing options for 'Compliance' (FIPS, STIG), 'Types' (Image, Helm Charts), 'Versions' (Extended Lifecycle Support), 'Categories' (Data science, Integration & delivery, Security, Networking, Languages & frameworks, Web servers), and 'Make a'.

The main content area is titled 'Hardened Image catalog' and includes a subscription status: 'Subscription active - 23 of 1000 images mirrored [manage](#)'. Below this, there are sections for 'Recently added' (Cilium startup script, Cilium Operator Azure, Cloudnative PG) and 'Featured' images. The featured images include:

- DHI Build**: OS Alpine, Debian; Architecture linux/amd64, linux/arm64; Compliance CIS.
- Caddy**: OS Linux; Architecture linux/arm64.
- Traefik Helm chart**: Dependencies for tag Traefik Helm chart 37.x; @ Traefik.
- HAPROXY Helm chart**: Dependencies for tag HAProxy Helm chart 37.x; @ HAProxy.
- HAProxy**: OS Debian; Architecture linux/amd64, linux/arm64; Compliance CIS.
- Traefik**: OS Debian; Architecture linux/amd64, linux/arm64; Compliance CIS, FIPS, STIG.
- Redis**: OS Debian; Architecture linux/amd64, linux/arm64; Compliance CIS.
- RabbitMQ**: OS Debian; Architecture linux/amd64, linux/arm64; Compliance CIS.

The 'Message queues' section features:

- ActiveMQ Artemis**: OS Debian; Architecture linux/amd64, linux/arm64; Compliance CIS.
- Eclipse Mosquitto**: OS Debian; Architecture linux/amd64, linux/arm64; Compliance CIS.
- Kafka**: OS Debian; Architecture linux/amd64, linux/arm64; Compliance CIS, FIPS, STIG.
- RabbitMQ**: OS Debian; Architecture linux/amd64, linux/arm64; Compliance CIS.



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

Upstream releases - **at project cadence**

CVE published Upstream patches

time

Upstream patch released You pull patch **Your app is secure**

Days to weeks saved!

Docker releases - **always within SLA**

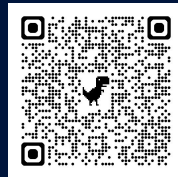
CVE published Upstream patches Docker scans, applies patch, releases DHI You pull patched DHI **Your app is secure**

7-day guaranteed SLA

time

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

 HARDENED IMAGE



Node.js

🔗 4 Tools included

🔗 Extended Lifecycle Support

OS

Alpine, Debian

Architecture

linux/amd64, linux/arm64

Compliance

 HARDENED IMAGE



Python

🔗 3 Tools included

🔗 Extended Lifecycle Support

OS

Alpine, Debian

Architecture

linux/amd64, linux/arm64

Compliance

CIS, FIPS, STIG



Flexible customization: certs, tools, packages...

 **SLSA Level 3**



Docker Hardened Image



Scripts/Certs

STEP 1

Select image version

Python 3.11.x
3.11.13-alpine3.21, 3.11-alpine3.21

STEP 2

Add packages

Add custom packages as an OCI artifact or choose from a predefined list.

Packages

curl x git x wget x Select from a list of pre-defi... 

OCI artifacts

Search for Docker Hub images in the "demonstrationorg..." 

[Learn more about adding custom packages via an OCI artifact](#) 

[Back](#)

[Next: Configure](#)

STEP 3

Configure image settings

Name your custom tag and define platforms, entrypoint, CMD, user, and environment variables.

STEP 4

Review customization

Review the image version, packages, and settings you selected before creating your custom image.



See it in action (demo)

Built to fit seamlessly into your DevSecOps stack



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



"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



"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



"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



DHI Enterprise Security: Verified by Independent Experts

Independent assessment by [SRLabs](#)



Cryptographic Integrity



Rootless by Default



SBOM and VEX Metadata



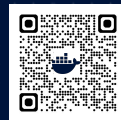
Minimal Attack Surface

“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



Limited edition Docker Lego and swag giveaway!

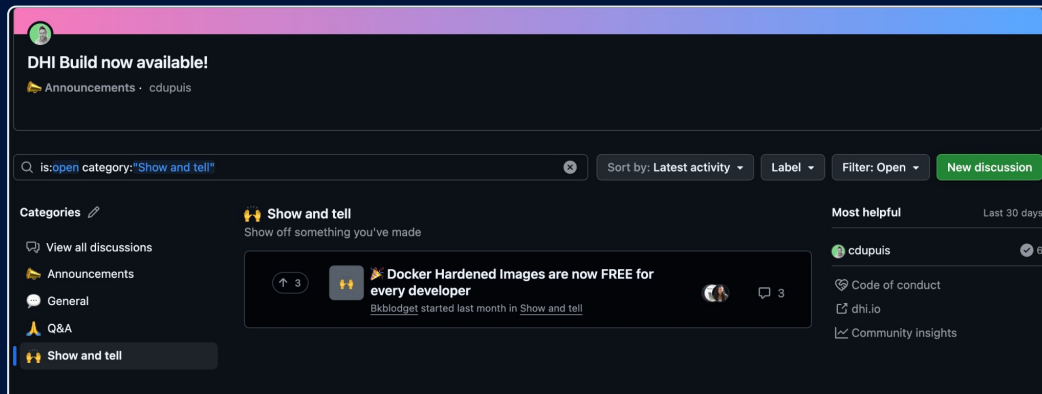


Illustrative images

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

