nuaware An Exclusive Networks Company | docker

Hardened Docker Desktop

Securing Developer Workstations at Scale

Securing developer workstations at scale

Security risks continue to grow and damages from cyberattacks are estimated to hit $10.5 trillion by 2025. These risks - malware, supply chain attacks, misconfigurations, insider threat etc. - remind us that security is needed at every step of the software development lifecycle. This means from the earliest stages of development on your developers' workstations (e.g., laptops, virtual desktops, etc.) to production and test environments.

Hardened Docker Desktop (HDD) provides a set of enterprise security features that secures developers' workstations without stopping or slowing them down, so developers can focus on what they love most - writing code. HDD:

- Lets IT admins configure and enforce security settings,
- Ensures developers and the containers they deploy can't relax or bypass those settings (purposely or accidentally)
- Hardens container isolation to prevent malicious payloads from breaching the Docker
- Desktop Linux VM and spreading into the underlying host

Hardened Docker Desktop features for protecting every developer workspace

Settings Management

Admins and platform engineering teams can centralize their control of developer workstations by presetting and locking configurations of their choosing across all Docker Desktop instances.

Only IT/system admins will have admin rights into the developer's workstation.

Enhanced Container Isolation

Secure your containers inside the Docker Desktop Linux Virtual Machine (VM). With ECI, all containers are rootless and blocked from accessing the Linux VM and the Docker Engine within it.

This prevents breaches, bypassing admin configurations, and accessing sensitive data or secrets stored from within the VM.

Registry Access Management

Choose which registries developers can access to push or pull artifacts from.

RAM significantly reduces the chance of a container image with malware or a corrupt image being used by your developers.

Image Access Management

Decide which images developers can pull from Docker Hub, including Docker Official Images, Docker Verified Publisher Images, and Docker-Sponsored Open Source Images.

IAM also reduces the chances of compromised and corrupt container images being used by developers.

Secure your supply chain & software integrity...hardening the earliest stages of software development so that threats from malware, the supply chain, misconfigurations, and insiders can't spread beyond the Linux VM into the native host and your company's network.

Save developer time...setting parameters for developer teams, so they can focus on what they do best, writing code.

Sleep better at night...knowing you're protecting your company from financial, reputational, and legal consequences from a supply chain attack.

Getting Started

Hardened Docker Desktop is already available with a Docker Business subscription.
There are a few prerequisites for getting up and running. Learn more in our docs :

- Download Docker Desktop 4.13 or late
- Admins must configure a registry.json as users must be authenticated to use these features

Reach out to Nuaware to learn more about Hardened Docker Desktop for your teams.