What is host namespace sharing?

Host namespace sharing is running a container with flags like `--pid=host`, `--net=host`, or `--ipc=host` (or the Kubernetes equivalents `hostPID`, `hostNetwork`, `hostIPC`), which place the container in the host's namespace instead of its own. That removes a layer of isolation: with `hostPID` the container sees and can signal host processes (and read their memory), with `hostNetwork` it shares the host's network and local services. Each shared namespace is a direct path toward host compromise.

HOW IT WORKS

01 What each shared namespace exposes

Each flag opens a different door:

- `--pid=host`: the container sees all host processes. With the right capability it can read their memory (secrets, tokens) via `/proc/<pid>/` or inject into them, and `nsenter` can drop into the host.
- `--net=host`: the container shares the host network, reaching services bound to `localhost` (databases, the kubelet, cloud metadata) that were never meant to be exposed.
- `--ipc=host`: shared memory access to host and other containers.

Documented techniques shown for defenders.

> EACH SHARE REMOVES A WALL
>
> *Namespaces are what isolation is *made of*. Every* `host*` *namespace you share removes one of those walls, and combined with a capability it often leads straight to a host escape.*

HOW TO DEFEND

- Do not set `hostPID`, `hostNetwork`, or `hostIPC` on application workloads.
- Block them with Pod Security Standards (restricted) and admission control in Kubernetes.
- Audit compose files and manifests for `--pid=host` / `network_mode: host` and the pod-spec equivalents.
- Bind host services to specific interfaces, not `0.0.0.0`, so `hostNetwork` exposure is limited.
- Combine with dropping capabilities so a shared namespace is less useful to an attacker.

SOURCES

[1] Docker docs: Container runtime options

[2] Kubernetes docs: Pod Security Standards

[3] NIST SP 800-190 Application Container Security Guide

Find the container escape paths before an attacker does.

securelayer7.net/learn/containers/what-is-host-namespace-sharing

Open online