

# DOCKER SECURITY CHEAT SHEET

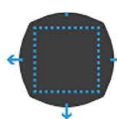
DISCLAIMER: The following tips should help you to secure a container based system. They are not a complete solution and will not in themselves guarantee security. They should only form a small part of your security policy which should mandate a holistic approach with multiple layers of defence.

## TYPES OF SECURITY THREATS AND HOW TO AVOID THEM



### KERNEL EXPLOITS

If a container can cause a kernel panic or similar, it will bring down the whole host.



### DENIAL OF SERVICE (DOS) ATTACKS

All containers share kernel resources. If one container monopolizes access to a resource, it will starve out the other containers.



### CONTAINER BREAKOUTS

If an attacker can breakout of a container, they can gain access to the host and other containers.



### POISONED IMAGES

Images may be injected with trojan or virus infected software. Or they may simply be running outdated, known-vulnerable versions of software.



### COMPROMISED SECRETS

API keys and database passwords must be kept secure to prevent attackers gaining access.

SEGREGATE CONTAINER GROUPS WITH VMs					
DEFANG SETUID/SETGID BINARIES					
BE AWARE OF CPU SHARES					
VERIFY IMAGES					
SET CONTAINER FILE SYSTEM TO READ-ONLY					
SET A USER					
DO NOT USE ENVIRONMENT VARIABLES TO SHARE SECRETS					
DO NOT RUN CONTAINERS WITH THE --privileged FLAG					
TURN OFF INTER-CONTAINER COMMUNICATION					
SET VOLUMES TO READ-ONLY					
SET MEMORY LIMITS					
DO NOT INSTALL UNNECESSARY PACKAGES IN THE CONTAINER					