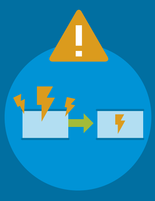
# Docker Security: What You Need to Know

From streamlining software delivery to automating the set up and configuration of development environments, Docker enables users to make their apps more agile and cloud-ready. While Docker can be a great solution for developers, operators, and enterprises, users should ensure that their containers are secured before diving in.

## UNIQUE CONTAINER SECURITY CHALLENGES

Security threats on containers fall into several categories. While some of these threats are par for the course in any type of computing environment, threats to Docker containers are often amplified.

**Risk of privilege escalation via containers**



**Attack originating from one container that compromises data or resources used by a different container**

**Risk of insecure or unvalidated app images**

## PROTECTING DOCKER CONTAINERS

New features from Docker, as well as the introduction of crucial security tools elsewhere in the container ecosystem, have made it much easier to keep Docker containers secure. Here are a few tools and strategies you can use to mitigate potential issues.

1


**Always start Docker containers with the -u flag so they run as an ordinary user instead of root**

This is a basic first step toward improving security

2


**Remove SUID flags from container images**

This makes privilege escalation attacks more difficult

3

**Configure Docker control groups to set limits on how many resources each container can use**

This will go a long way toward preventing container-based DoS attacks

4

**Use namespaces in Docker to isolate containers from one another**

Namespaces help assure that a user or process running inside one container can't affect those in other containers

5

**Don't use images from repositories that you don't trust**

This may sound like a no-brainer, but it can be tempting to pull an image from a random registry

6

**Consider using Clair to validate containers from your registries**

Use Clair to scan images locally or run it directly from supported public registry services

7

**Get visibility into what's happening in your containers**

You can't stop what you can't see, so having a robust tool to analyze your container data is key

sumologic™

## Docker Logging with Sumo Logic

Visibility is key to understanding if your containers are secure, and Sumo Logic can help. Our advanced machine-learning and analytics capabilities enable you to analyze, troubleshoot, and perform root cause analysis of issues surfacing from distributed container-based applications and Docker containers themselves.

**Sign up for Sumo Logic Free to try it for yourself at**
www.sumologic.com/lp/log-monitoring/full-stack-log-analytics/