



Sidecar injection

A Kubernetes Pod is a group of one or more containers with shared storage and network resources. Sidecar container is a term that is used to describe an additional container that resides alongside the main container. For example, service-mesh proxies are operating as sidecars in the applications' pods. Attackers can run their code and hide their activity by injecting a sidecar container to a legitimate pod in the cluster instead of running their own separated pod in the cluster.



Info

ID: MS-TA9011

Tactic: [Execution](#)

MITRE technique: [T1610](#)

Mitigations

ID	Mitigation	Description
MS-M9003	Adhere to least-privilege principle	Prevent unnecessary users and service accounts from creating new pods and controllers.
MS-M9013	Restrict over permissive containers	Restrict over permissive containers in the cluster using admission controller.
MS-M9005.003	Gate images deployed to Kubernetes cluster	Restrict deployment of new containers from trusted supply chain