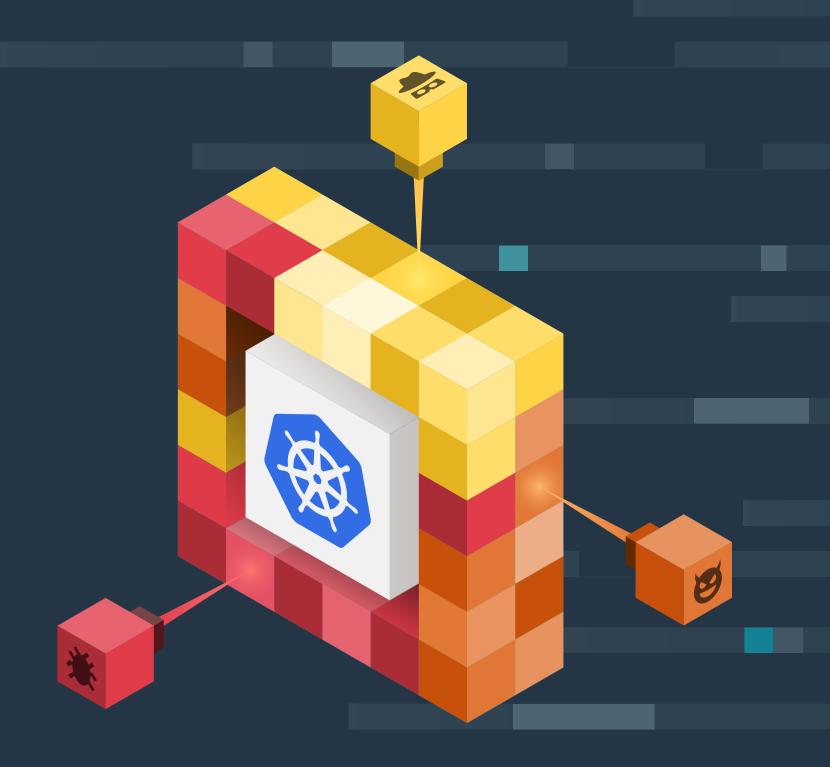
# Kubernetes threat landscape.

A number of enterprises are scaling Kubernetes in production, yet are not aware of the increasing number of vulnerabilities and attack vectors that require them to reconsider their security approach.





**MARCH 2018** 



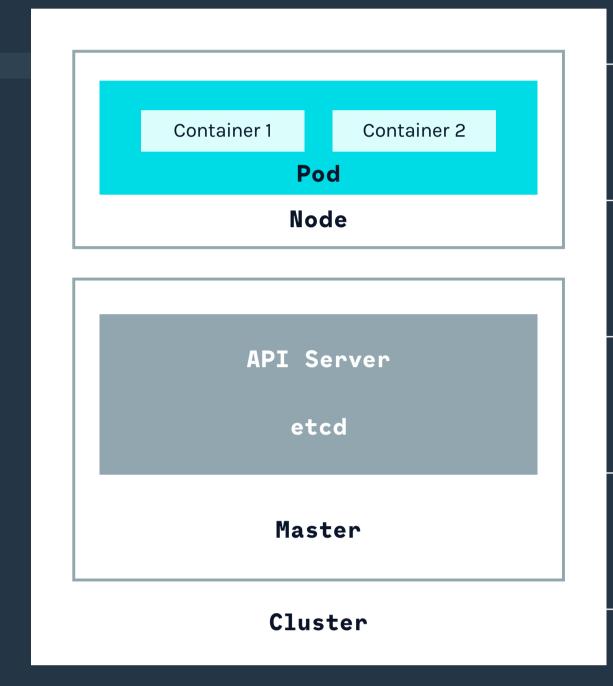
Etcd credentials leak

MAR 2019



Kubernetes dashboard vulnerability

### Kubernetes attack surface.



Container compromise and attacker can escape to access node

Attacker can control pods running on node and perform various malicious tasks (ex. cryptomining)

Attacker can compromise API server for unrestricted access

Attacker can create, modify or delete entire cluster

Attacker has control of your cluster



### Legacy security tools don't work for Kubernetes.

No visibility into vulnerabilities inside containers

Can't keep up with scalable, distributed services

Lack of contextual awareness across **Kubernetes environments** 

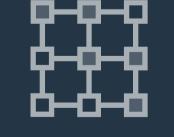
Not tightly coupled with DevOps

Kubernetes requires you to rethink your security approach.



#### Higher container density

Average container density has increased by 10x (much more than VMs)



Ephemeral services

95% of containers live less than a week and securing these ephemeral services requires visibility into the container and its environment



#### Orchestrator policy management

**Kubernetes policy** management has new constructs (ex. Pod Security Policies) that require careful implementation



DevSec0ps agility

Deployment speed makes all security obligations a challenging task



Forensics

Incident response is difficult after Kubernetes has already killed the pod or container

## THE COMPLETE GUIDE TO Securing Kubernetes

Read Now



Sysdig

sysdig.com