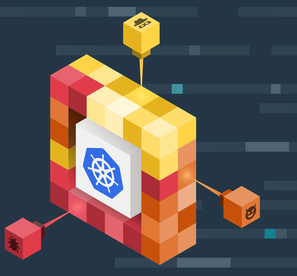
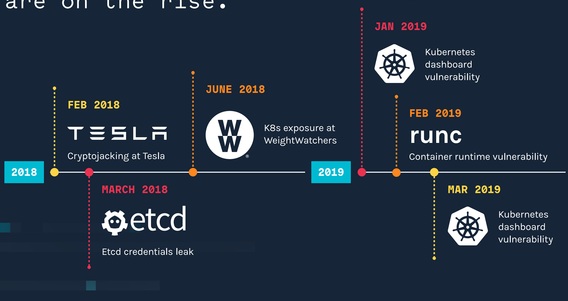
Kubernetes threat landscape.

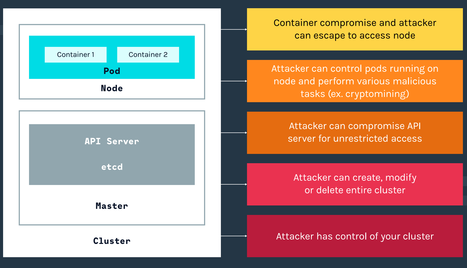
A number of enterprises are scaling Kubernetes in production, yet are not aware of the increasing number of vulnerabilities and attack vectors that require them to reconsider their security approach.



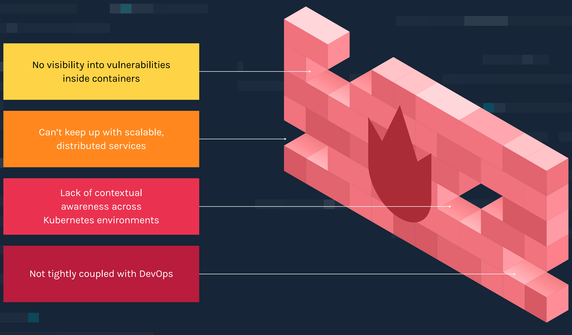
Kubernetes threats are on the rise.



Kubernetes attack surface.



Legacy security tools don't work for Kubernetes.



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

DevSecOps agility

Deployment speed makes all security obligations a challenging task

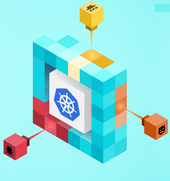
Forensics

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

THE COMPLETE GUIDE TO

Securing Kubernetes

Read Now



Sysdig