ASSESSING EKS SECURITY WITH KUBE-BENCH_

Sandro Cirulli

ABOUT ME_

I work as AWS Consultant at The Scale Factory

I am an AWS Certified SysOps Administrator

I co-organize DevOps Oxford Meetup

TOPICS **COVERED_**

1. AWS Shared Responsibility Model
2. CIS Amazon EKS Benchmark
3. kube-bench
4. Demo
5. Conclusions

AWS
WHAT'S NEW_

Announcing the CIS Benchmark for Amazon EKS

Posted On: Jul 22, 2020

The new CIS Benchmark for Amazon EKS helps you accurately assess the secure configuration of nodes running as part of your Amazon EKS clusters.

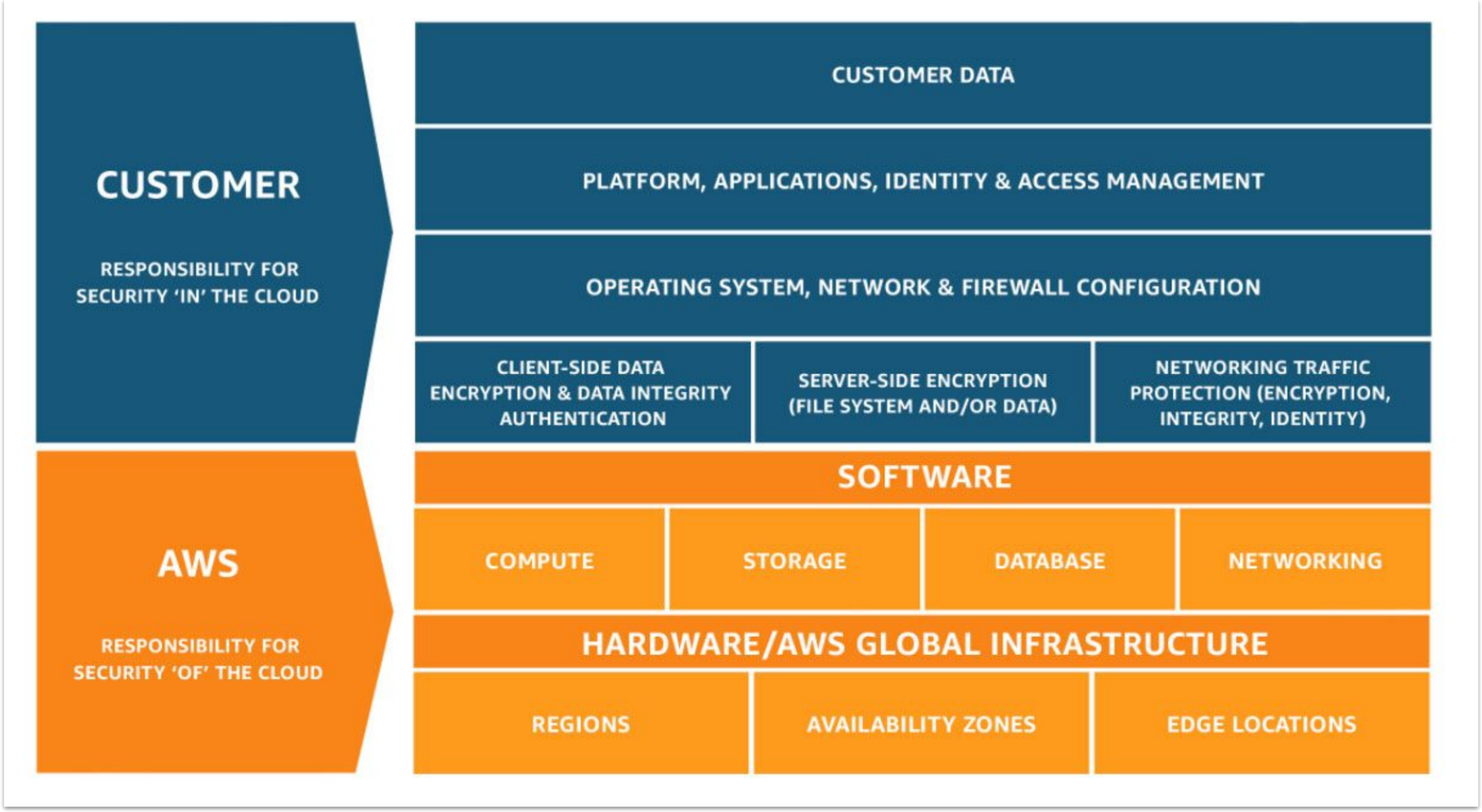
Security is a critical consideration for configuring and maintaining Kubernetes clusters and applications. The Center for Internete Security (CIS) Kubernetes Benchmark provides good practice guidance on security configurations for self-managed Kubernetes clusters, but did not accurately help evaluate the security configuration status for the AWS-managed Kubernetes clusters run by Amazon EKS. Not all of the recommendations from the CIS Kubernetes Benchmark were applicable to EKS clusters as customers are not responsible for configuring or managing the control plane.

Now, the CIS Amazon EKS Benchmark provides accurate guidance for node security configurations for EKS. The benchmark is applicable to EC2 nodes (both managed and self-managed) where you are responsible for security configurations of Kubernetes components. The benchmark provides a standard, community-approved way to ensure that you have configured your Kubernetes cluster and nodes securely when using Amazon EKS.

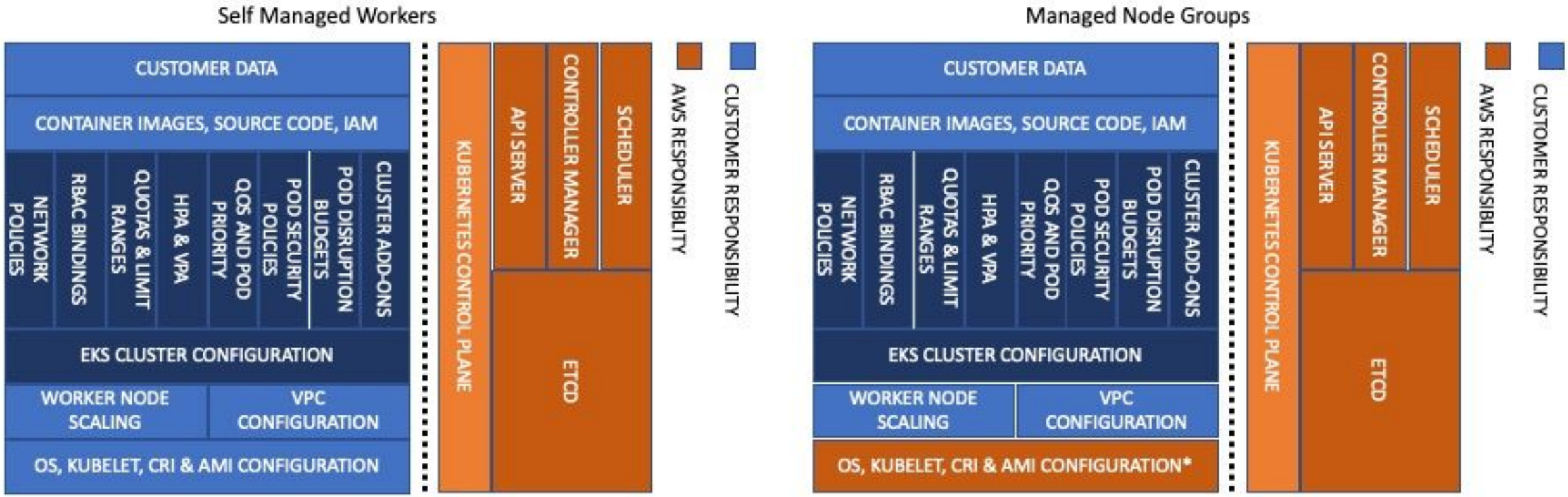
AWS SHARED RESPONSABILITY MODEL_

AWS is responsible for security **of** the cloud

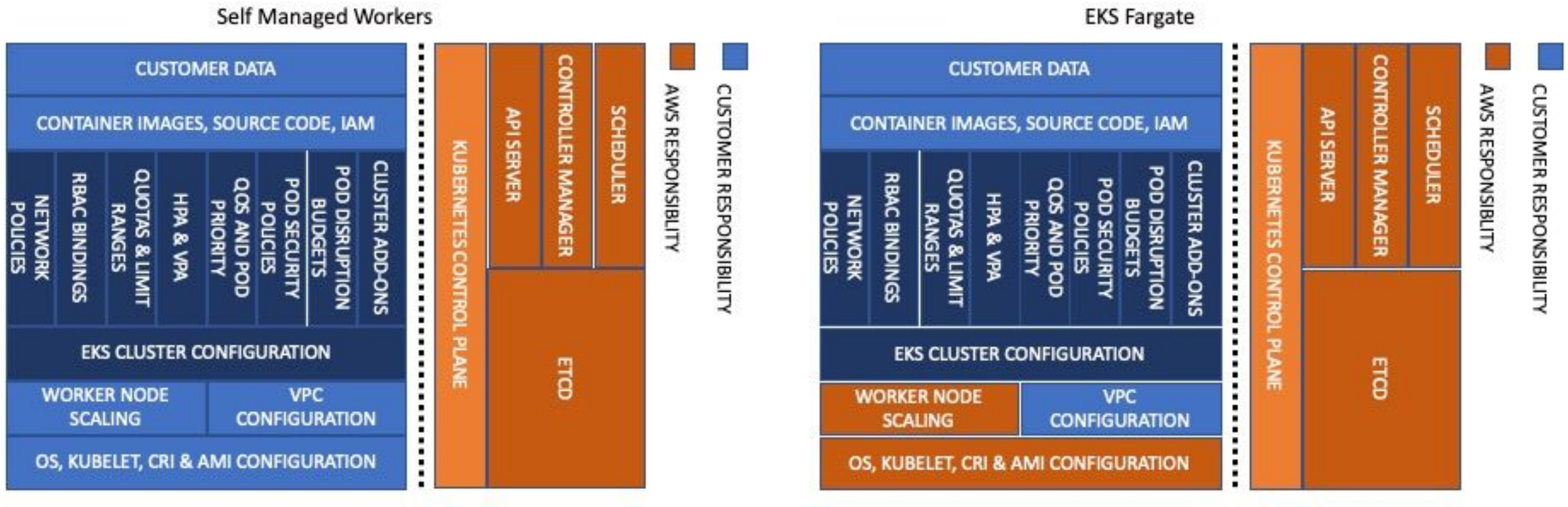
Customers are responsible for security **in** the cloud



EKS
SELF MANAGED VS MANAGED



EKS
SELF MANAGED VS EKS FARGATE



CIS AMAZON EKS BENCHMARK_

In Scope

- Aligned with CIS Kubernetes Benchmark
- Covers EKS supported versions (1.15, 1.16, 1.17)
- Applicable to EC2 nodes (both managed and self managed)

Not In Scope

- Not applicable to Amazon EKS on AWS Fargate
- Not applicable to nodes' operating system level security

CIS AMAZON EKS BENCHMARK_

Sections

1. Control Plane Components
2. Control Plane Configuration
3. Worker Nodes
4. Policies
5. Managed Services

CIS AMAZON EKS BENCHMARK_

Sections

1. Control Plane Components
2. Control Plane Configuration
3. **Worker Nodes**
4. **Policies**
5. **Managed Services**

CIS AMAZON EKS BENCHMARK_

KUBE-BENCH_

kube-bench

- Open source Go application
- Checks whether Kubernetes is deployed according to security best practices
- Implements the CIS Amazon EKS Benchmarks
- Recommended by AWS and developed by AWS Advanced Technology Partner

KUBE-BENCH_

kube-bench

- Install it as rpm/deb package within the worker node
- Run it as a pod in the EKS cluster
- Assessment report maps to CIS EKS Benchmark
- Can run a subset of checks and omit false positives

KUBE-BENCH DEMO_

CONCLUSIONS_

& TAKEAWAYS

- Understand how the AWS Shared Responsibility Model applies to your EKS cluster
- Download and read the CIS Amazon EKS Benchmark
- Run kube-bench to assess your EKS cluster security

FURTHER READING_

kube-bench

https://github.com/aquasecurity/kube-bench

Introducing The CIS Amazon EKS Benchmark

https://aws.amazon.com/blogs/containers/introducing-cis-amazon-eks-benchmark

CIS Benchmarks

https://www.cisecurity.org/cis-benchmarks

Amazon EKS Best Practices Guide for Security

https://aws.github.io/aws-eks-best-practices

Security in Amazon EKS

https://docs.aws.amazon.com/eks/latest/userguide/security.html

THANK YOU
ANY QUESTION?_

sandro@scalefactory.com

scalefactory.com/contact-us