SUSE HashiCorp Adfinis

24. June

Secrets Management at Scale with Vault & Rancher

Bastian Hofman
Senior Field Engineer
SUSE
bastian.hofmann@suse.com

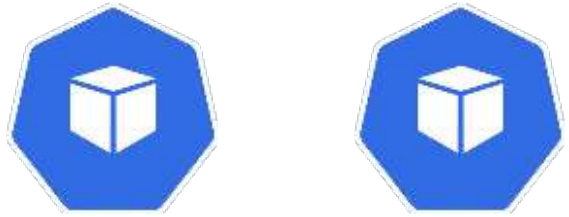
Kapil Arora
Senior Solution Engineer
HashiCorp
kapil@hashicorp.com

Robert de Bock
Senior DevOps Engineer
Adfinis
robert.debock@adfinis.com

Containers are great!

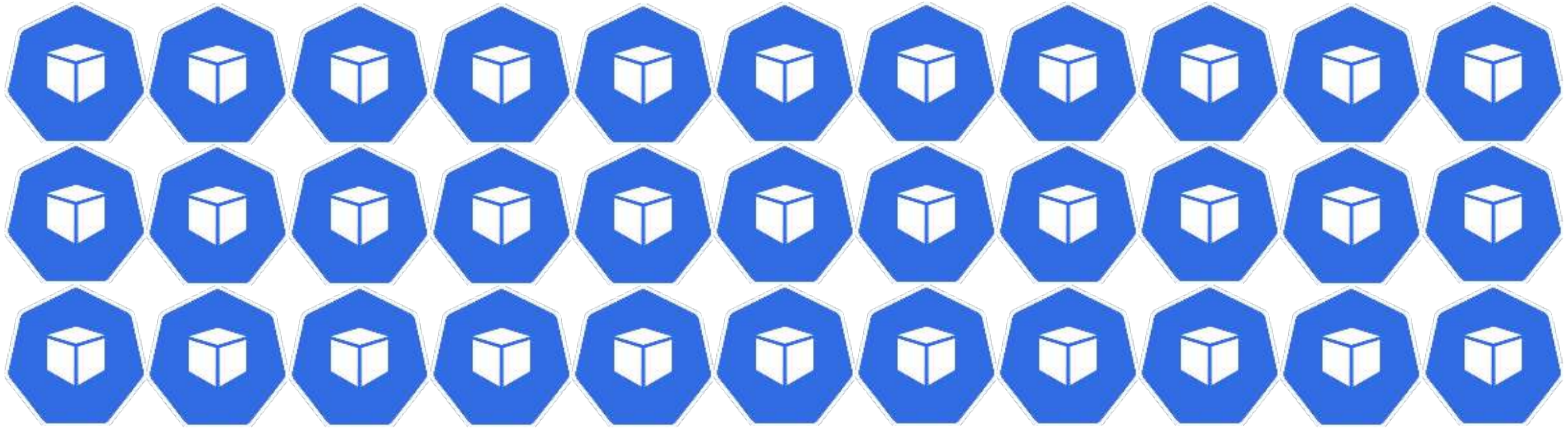
One self-contained, portable package for your application

Containers are great.....but



Managing a couple – no problem

Containers are great.....but



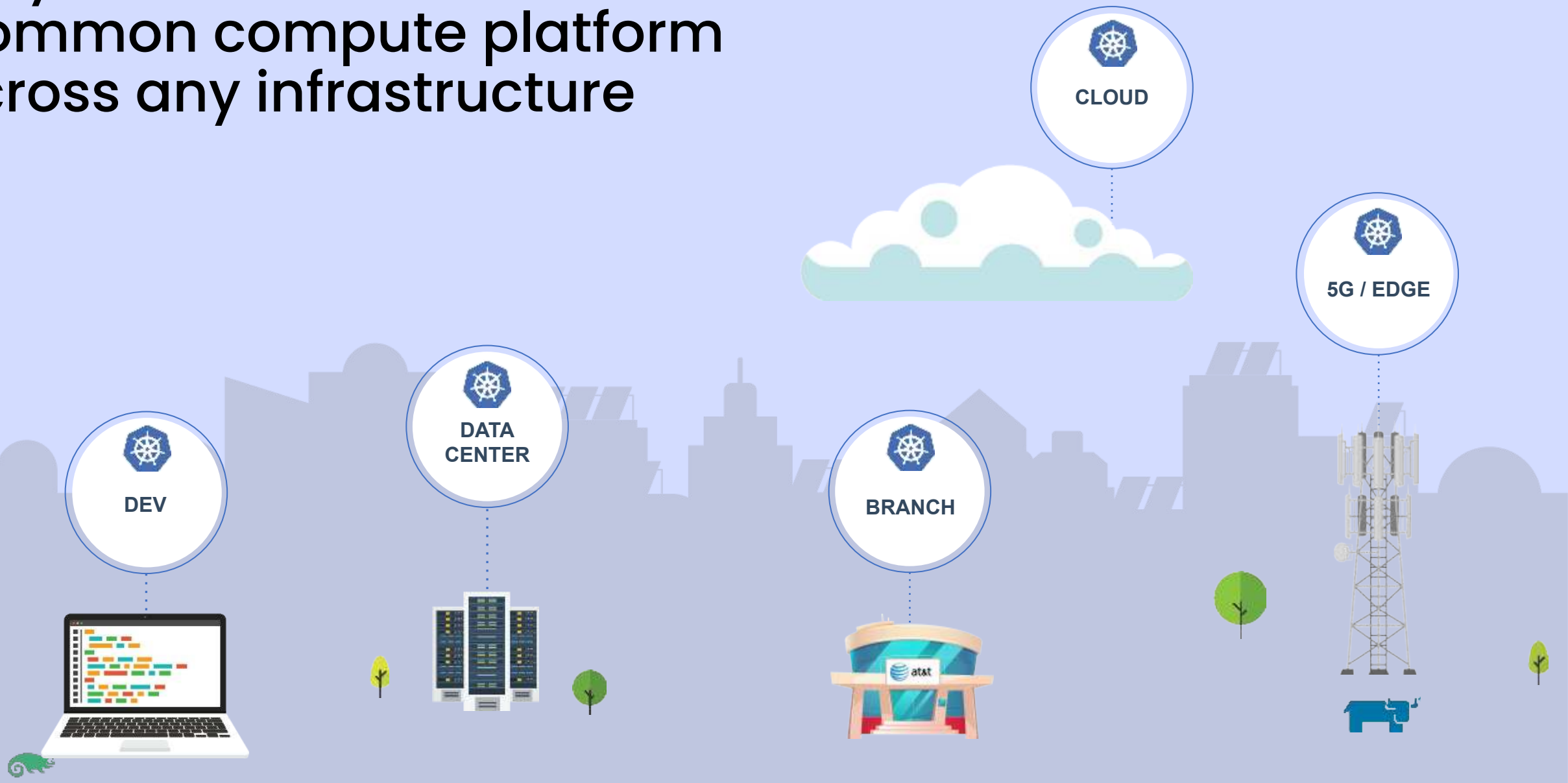
How about managing many?

How do we address:

Networking, Security, Scheduling, Automation, etc?

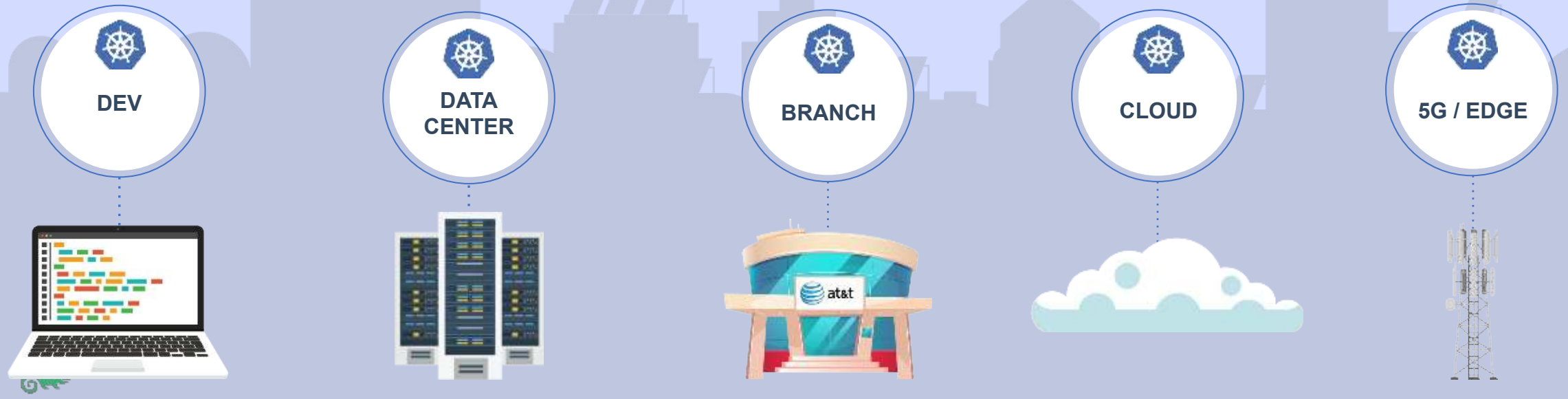
kubernetes

Why Kubernetes ?
Common compute platform across any infrastructure

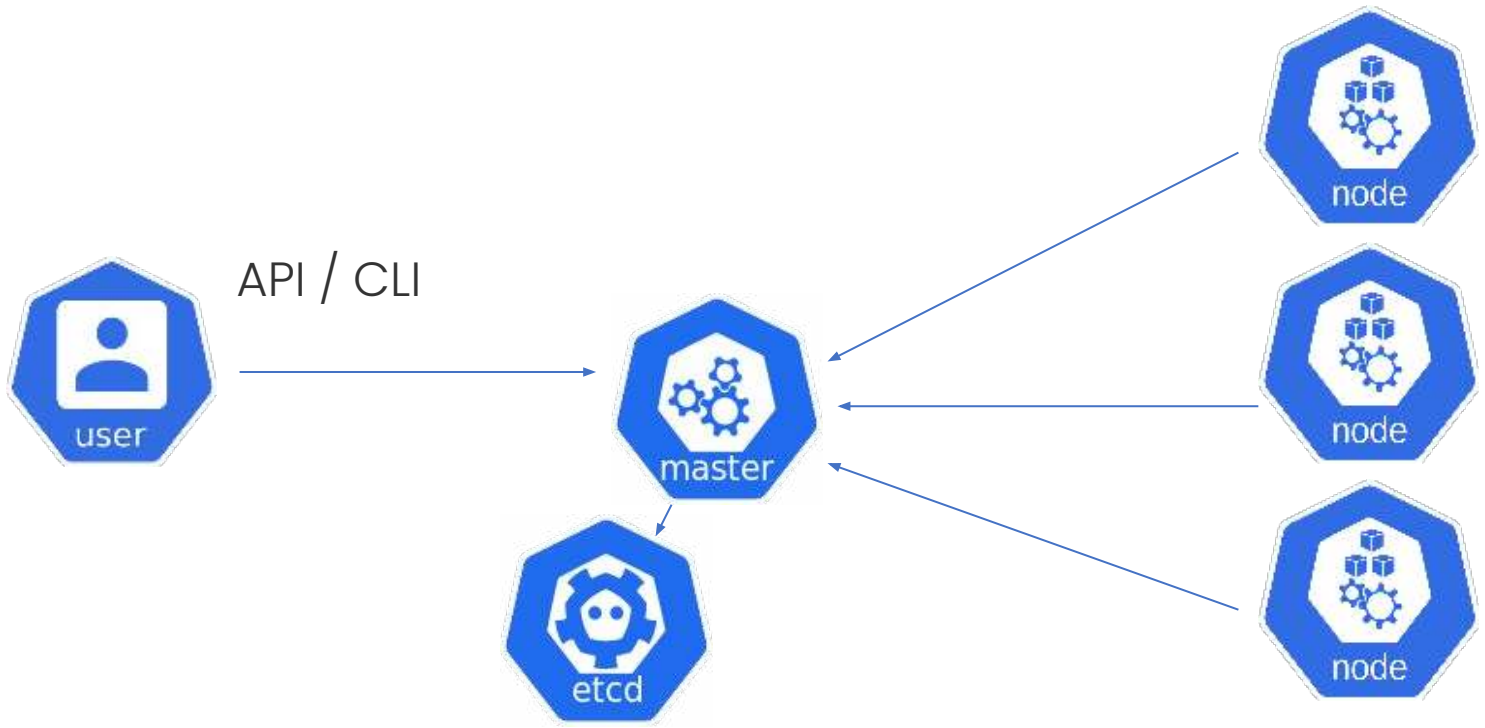


Common compute platform across any infrastructure & a consistent set of infrastructure capabilities

- Common API & Packaging
- Health Checks/HA
- Load Balancing
- Overlay Networking
- Network Security Policies
- Backup and Recovery
- Autoscaling
- Service Discovery
- Networking
- RBAC & Access Control

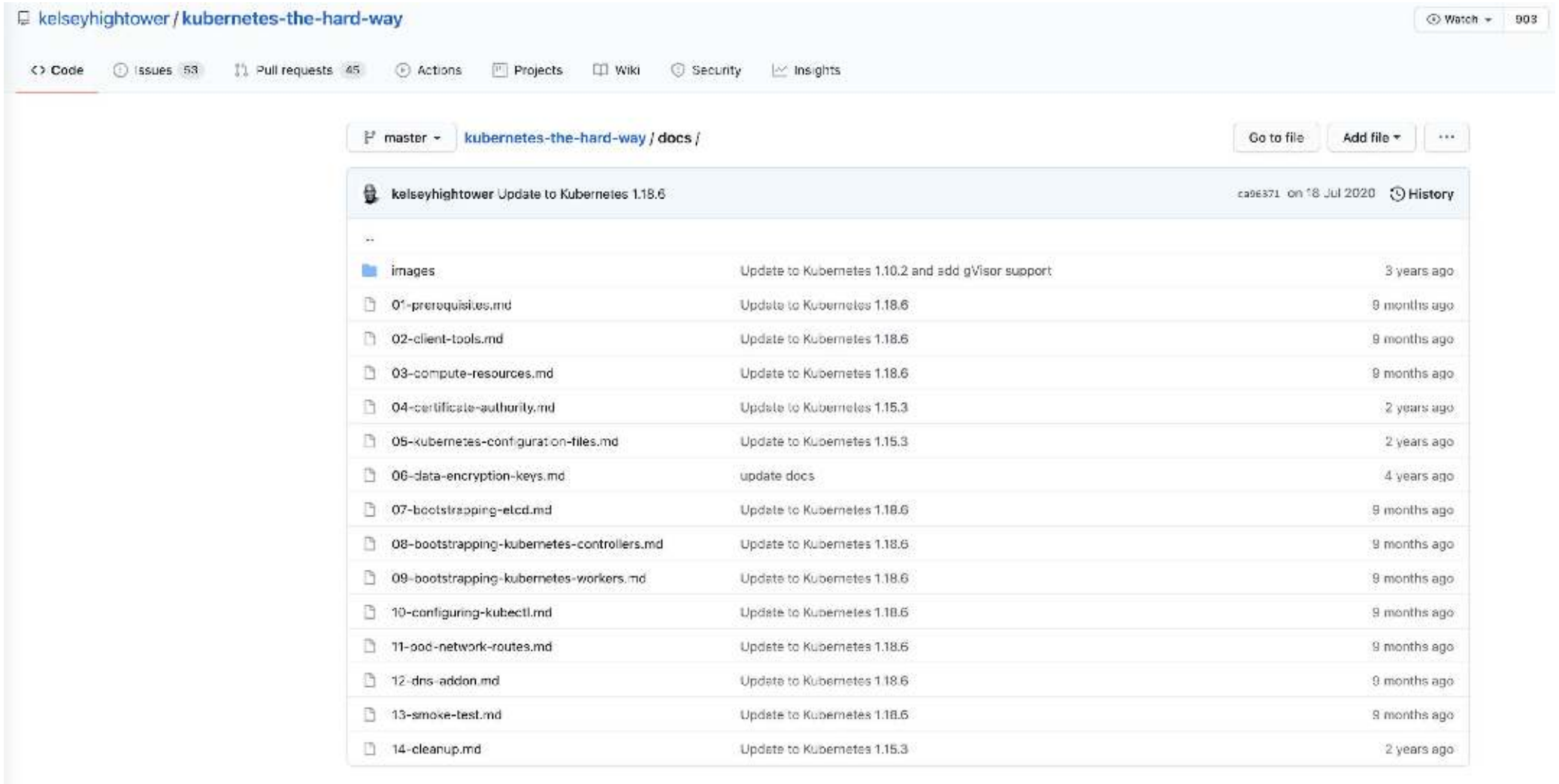


Kubernetes architecture



- Controlplane: Manages the cluster and exposes an API for control
- Etcd: a key value store used as Kubernetes' backing store for all cluster data.
- Worker: Runs workloads and all of the supporting components.

Setting up Kubernetes is hard



You don’t compile Linux from scratch, you use a distribution

Rancher Kubernetes Engine

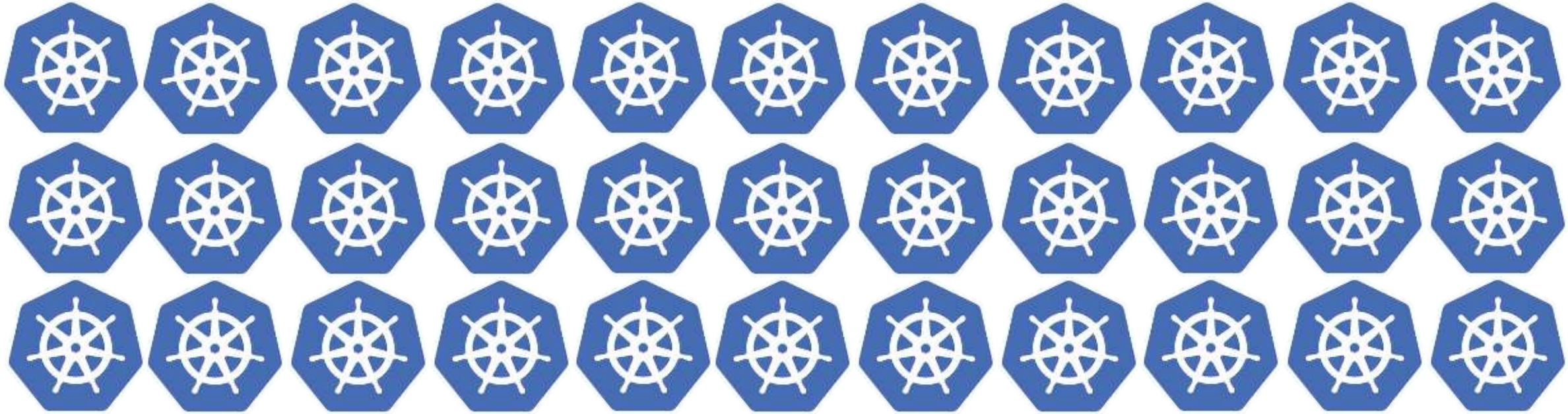
- 100% Upstream Kubernetes
- CNCF certified
- Easy installation
- Zero-downtime upgrades
- Backup & Disaster Recovery
- Air gapped installation support

RKE

Kubernets clusters are great.....but

Managing a couple – no problem

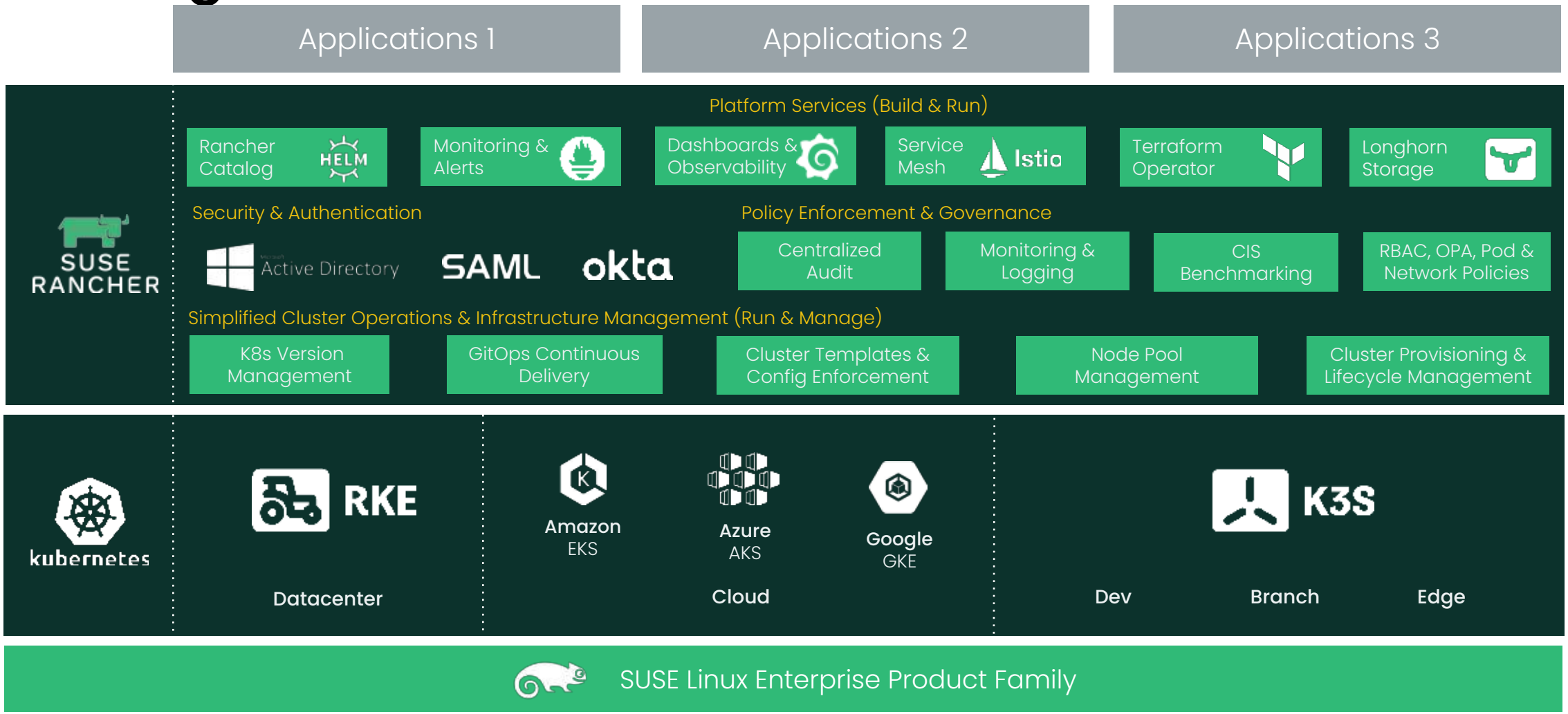
Kubernetes clusters are great……but



How about managing many?

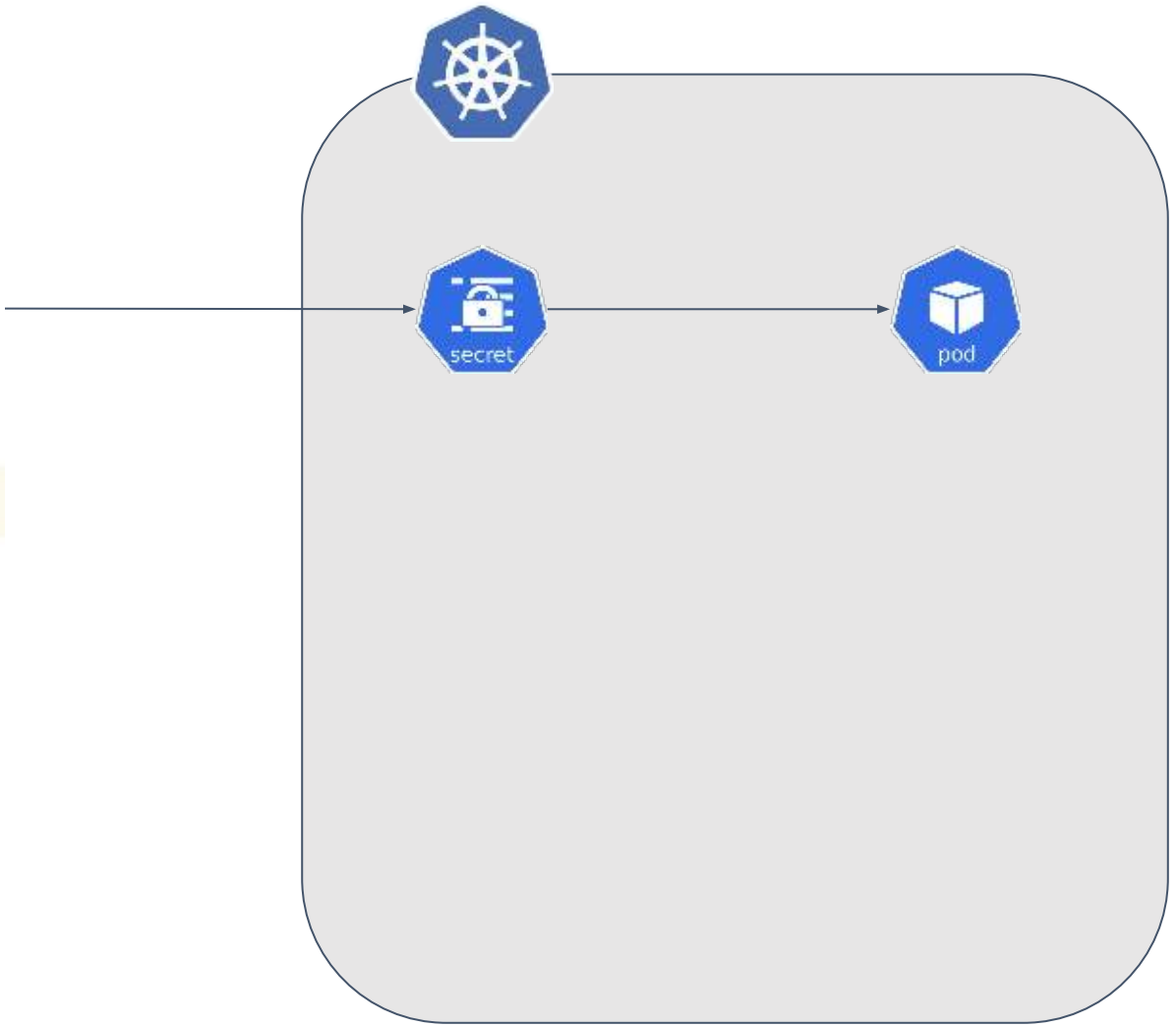
- Different environments
- Different teams
- Different hardware
- Different locations
- Edge devices

SUSE Rancher – the industry's only platform to manage all Kubernetes distributions



Secret Management in Kubernetes

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: database-config
stringData:
  root-password: not-very-secret
```




HashiCorp
Vault

Secret Management Challenges

- Secrets sprawl
- Secrets rotation
- X.509 certificates, SSH and Cloud access
- Encryption
- Multi-platform and multi-cloud
- Central control and management
- Auditing
- Compliance & Hardware Security Module (HSM) integration
- Costs, scalability & productivity

HashiCorp Vault

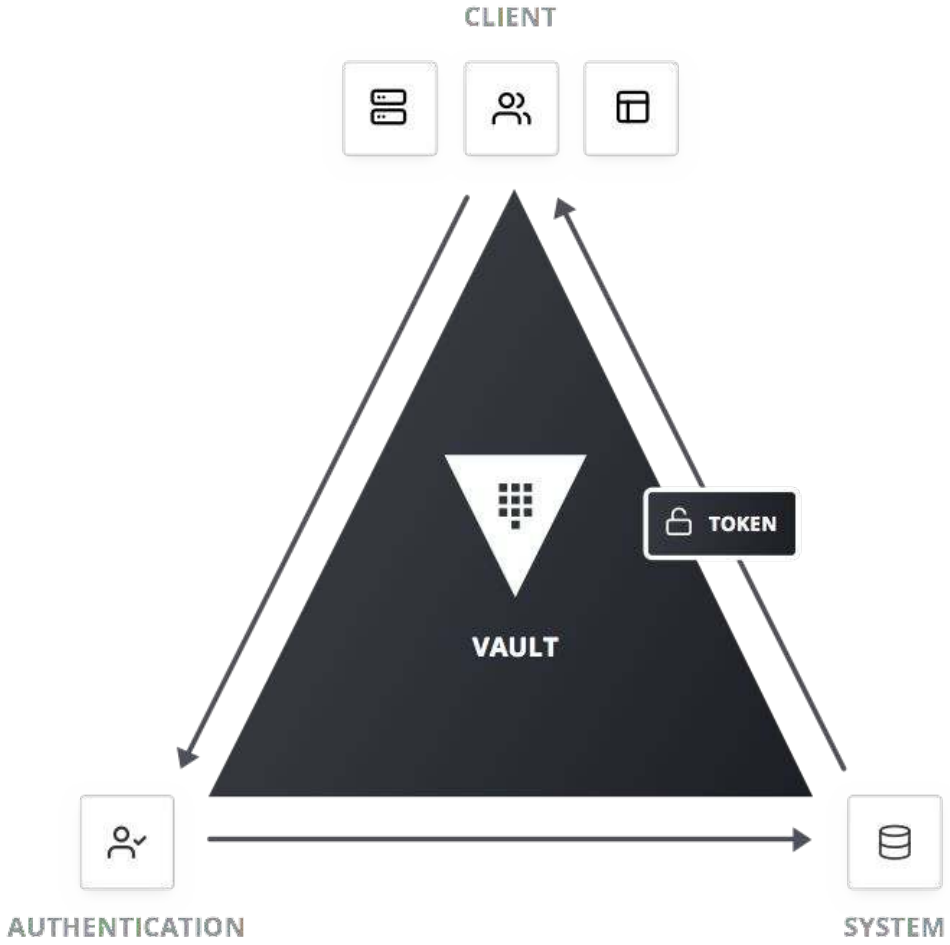
Provides the foundation for cloud security that leverages trusted sources of identity to keep secrets and application data secure

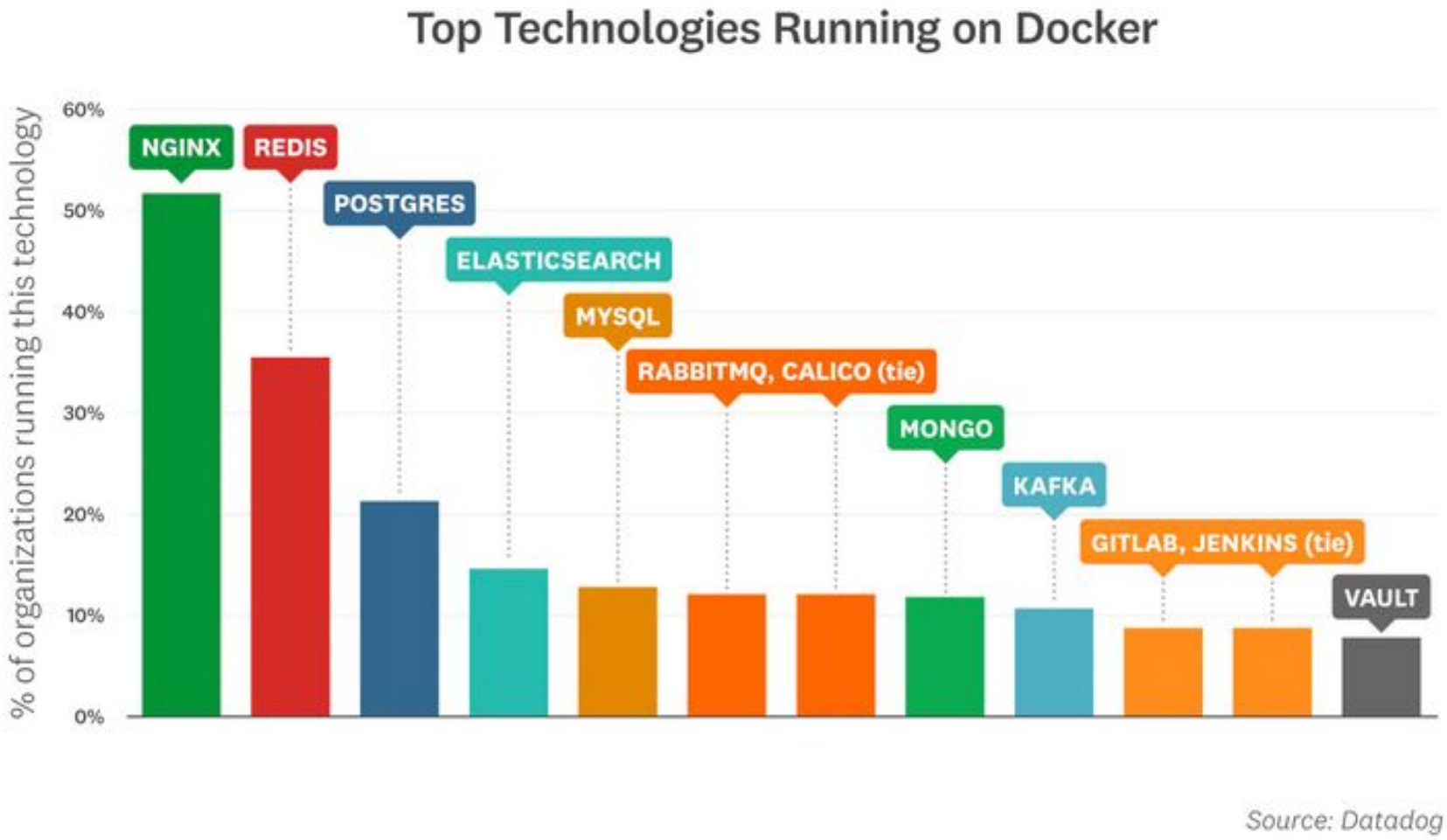
- **Secrets management** to centrally store and protect secrets across clouds and applications
- **Data encryption** to keep application data secure across environments and workloads
- **Advanced Data Protection** to secure workloads and data across traditional systems, clouds, and infrastructure.

2T+
Transactions Weekly

1M+
Monthly D/Ls

475+
Enterprise Customers





Source: https://www.datadoghq.com/container-report/

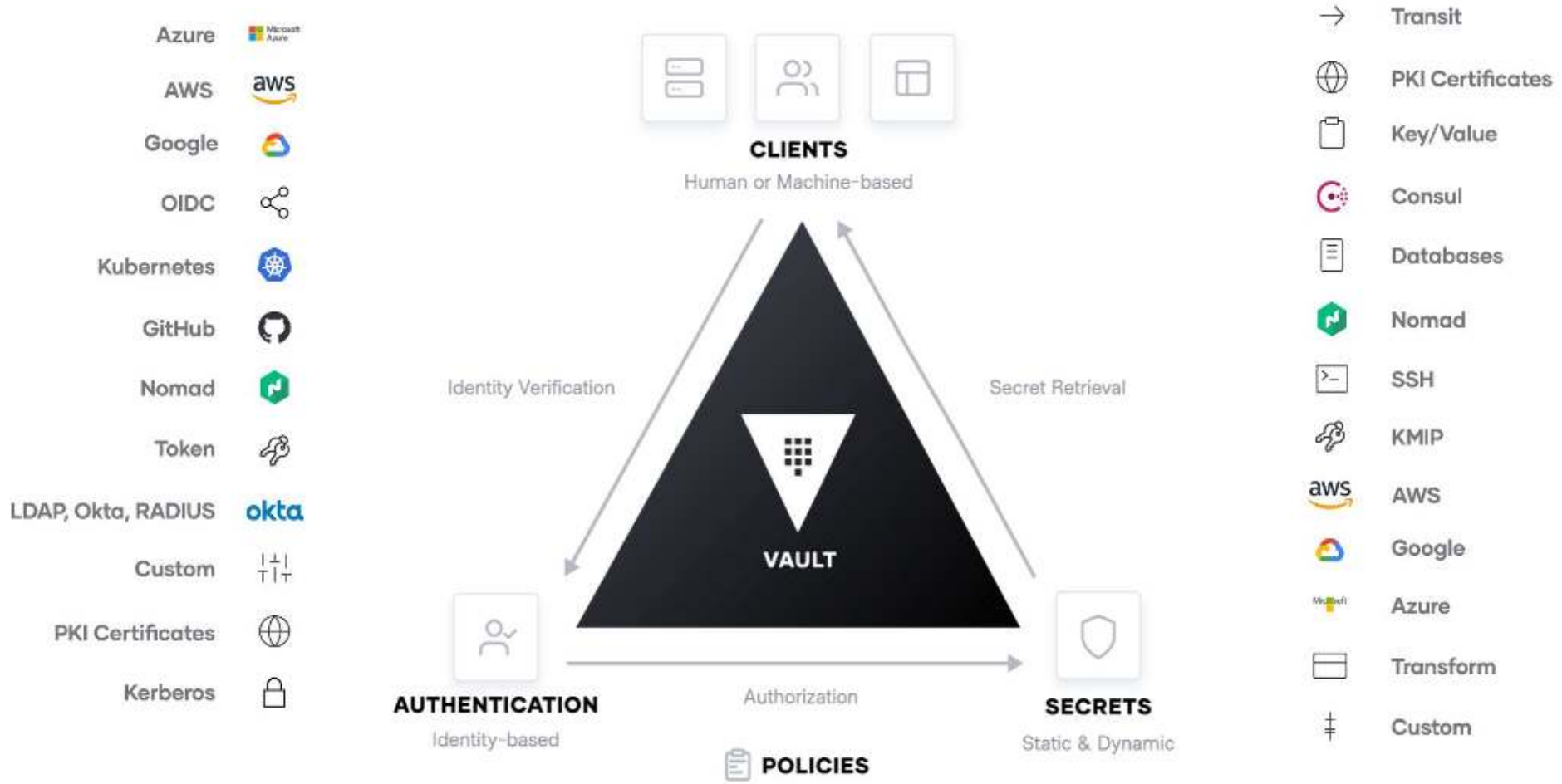
Secrets Management

As of 3 August 2020

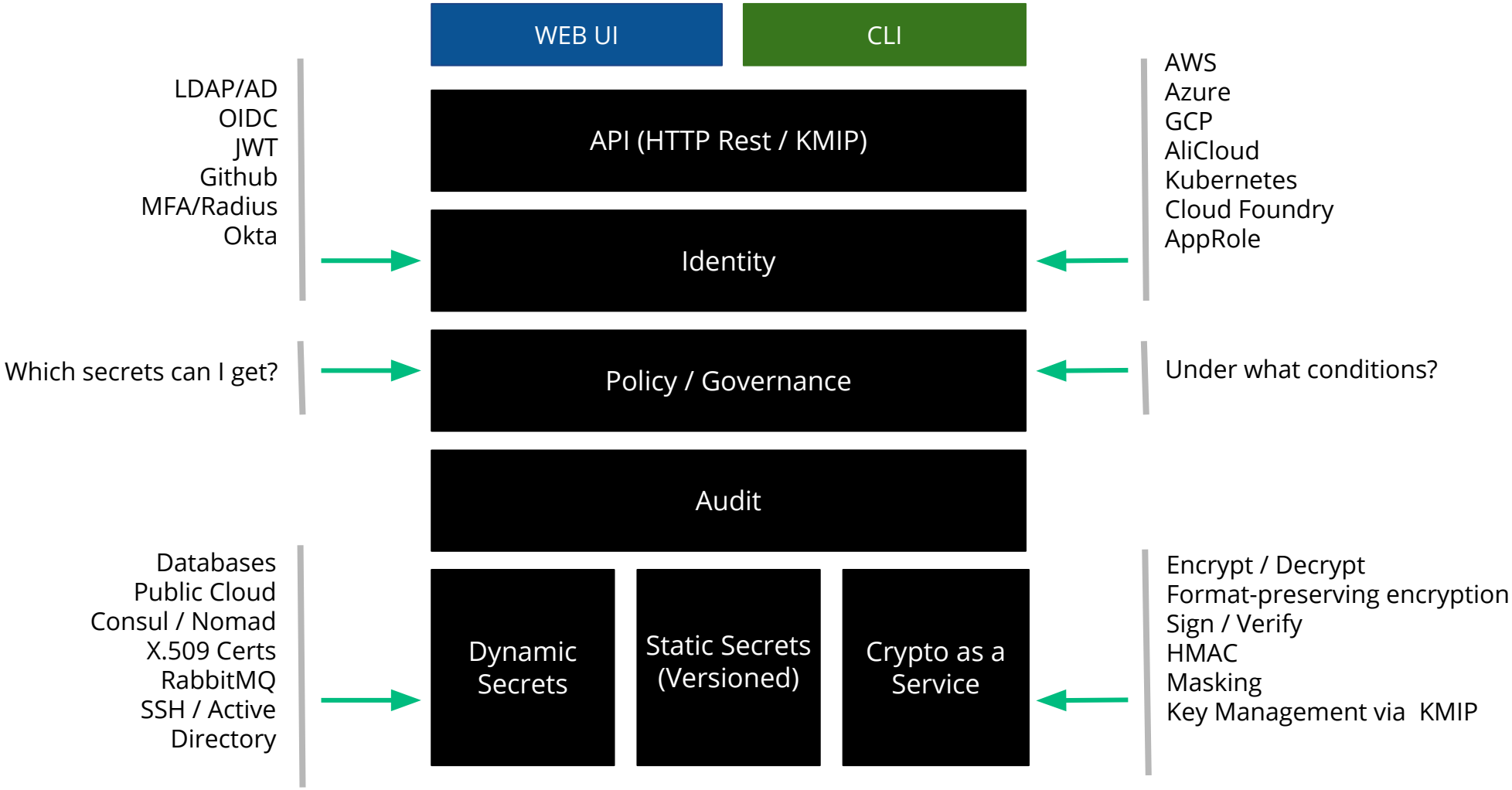
This is a specialized use case for privileged access, consisting of the need to programmatically manage, store and retrieve credentials and secrets for software and machines.

Source: https://www.gartner.com/en/documents/3988410/critical-capabilities-for-privileged-access-management

Vault Workflow Overview



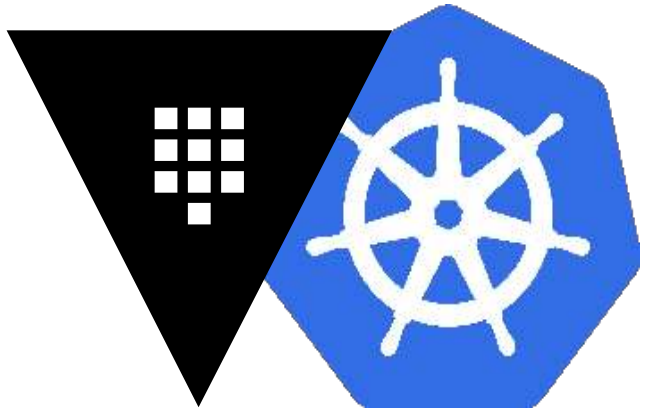
Vault Principles



Combining Vault and Rancher

Vault & Rancher - Why?

- Automation: both products have a strong API.
- The combination prevents vendor lock-in.
- With Rancher and K8s a secrets engine becomes important.



Deploy Vault on Ranchers K8s clusters

$ helm repo add hashicorp https://helm.releases.hashicorp.com
"hashicorp" has been added to your repositories

$ helm install vault hashicorp/vault

Stolen from **https://www.vaultproject.io/docs/platform/k8s/helm**

Demo deploying Vault

If demo-gods are angry: https://youtu.be/k9lpsnXQv-I

Use Ranchers K8s authentication for Vault

Vault typically uses an authentication provider, like *Active Directory* or *GitHub*.

K8s is also an authentication provider.

This makes Vault quite easy to integrate.

Let’s review https://www.vaultproject.io/docs/auth/kubernetes

Use Secrets in Rancher Kubernetes Containers

Multiple Methods

Vault Agent

```
spec:
  template:
    metadata:
      annotations:
        vault.hashicorp.com/agent-inject: "true"
        vault.hashicorp.com/role: "internal-app"
        vault.hashicorp.com/agent-inject-secret-database-config.txt:
"internal/data/database/config"
```

https://learn.hashicorp.com/tutorials/vault/kubernetes-sidecar

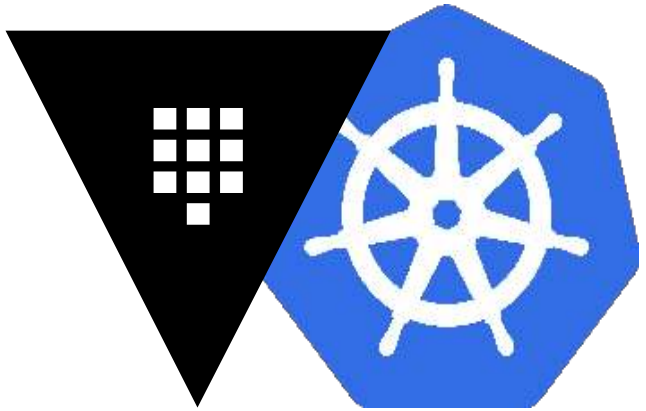
Vault CSI (Container Storage Interface)

A Vault secret shows as a file in a mount.

https://www.vaultproject.io/docs/platform/k8s/csi

Vault & Kubernetes Summary

- Vault can be installed on Kubernetes using a **Helm Chart**
- Vault supports Kubernetes authentication. Applications can use a **K8S Service Account** to authenticate and fetch secrets
- Vault can leverage Kubernetes mutating admission webhook to intercept pods that define specific **annotations** and **inject** a **Vault Agent** container to manage these secrets
- Mount Vault secrets as volume using secrets store **CSI** driver



Conclusion

- Vault is a logical component in Ranchers K8s clusters.
- It’s easy to install Vault in K8s.
- There are sufficient methods to consume secrets.

Resources

- SUSE Rancher
  - https://www.suse.com/de-de/products/suse-rancher/
  - https://rancher.com/docs/rancher/v2.5/en/
- HashiCorp Vault
  - https://www.vaultproject.io/docs/platform/k8s
  - https://learn.hashicorp.com/collections/vault/kubernetes

Q&A

Thank You

hello@hashicorp.com
www.hashicorp.com
www.adfinis.com
www.suse.com