

ISOVALENT

Keeping It Simple:

Cilium Networking for Multi-cloud Kubernetes And Beyond



Liz Rice | @lizrice

Chief Open Source Officer, Isovalent
CNCF and OpenUK Board

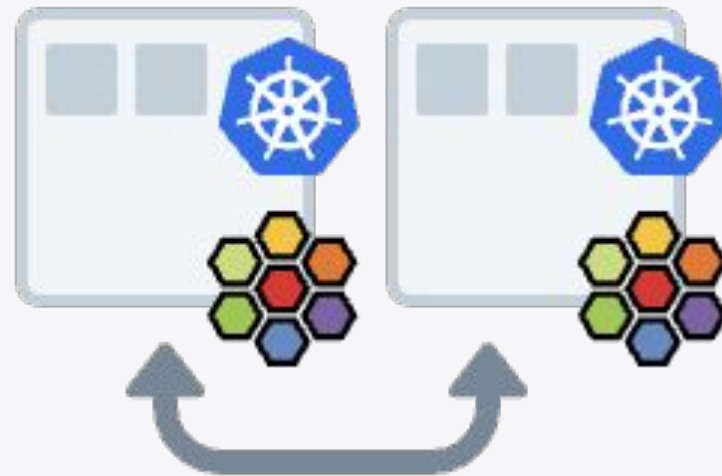
Cilium Mesh

One Mesh to Connect Them All

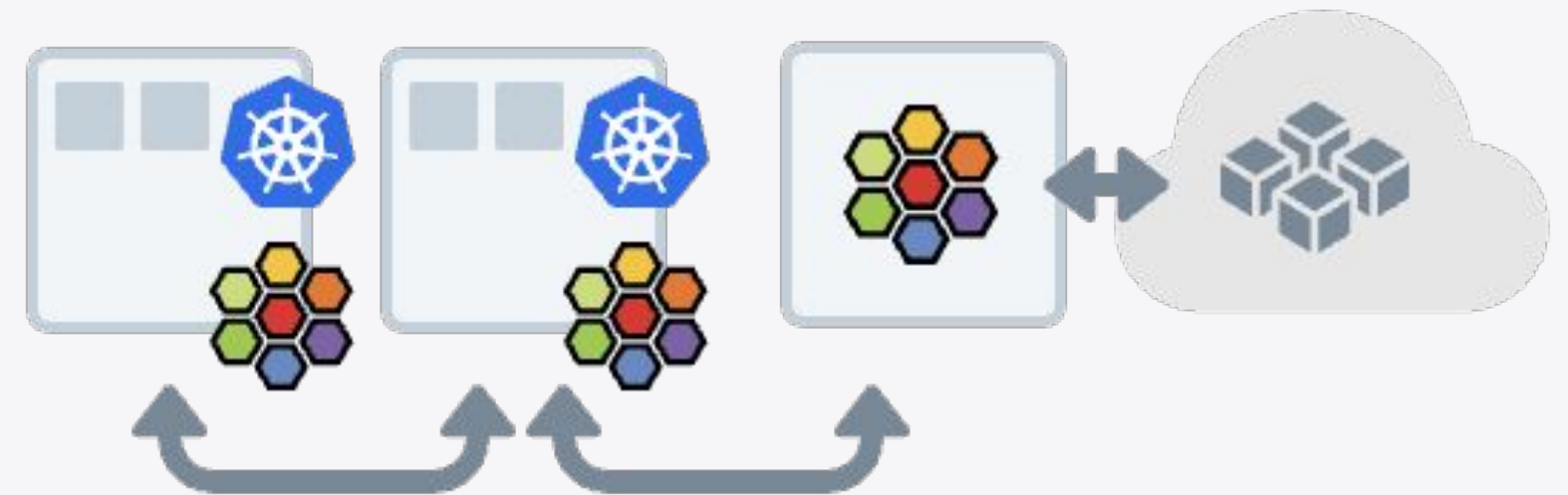
Kubernetes
Networking



Multi-Cluster
Networking



Multi- & Hybrid-
Cloud Networking



Cilium Mesh

**Connect workloads
in multiple clusters
and non-Kubernetes environments
in public clouds and on-prem
securely: network policies
and authenticated + encrypted**

STAR
THE FORCE AWAKENS
WARS

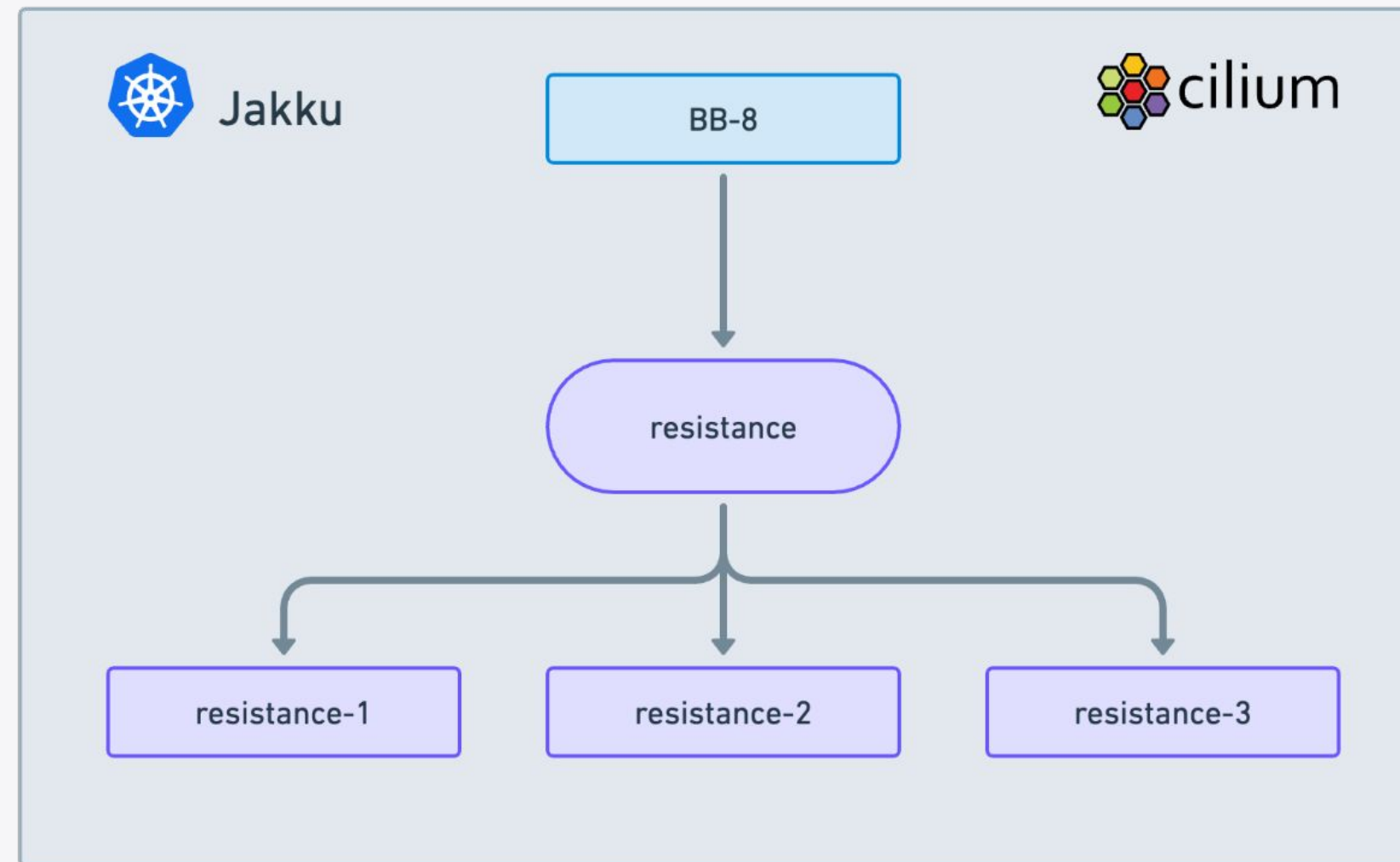


Image credit: [HJ Media Studios on flickr](#)

Services and Endpoints are Kubernetes concepts

ISOVALENT

Services load balance to pods





Service names resolve to an IP address

```
> k get svc
NAME                TYPE          CLUSTER-IP      EXTERNAL-IP      PORT(S)          AGE
kubernetes           ClusterIP      192.168.0.1      <none>            443/TCP           4h20m
resistance            ClusterIP      192.168.0.246    <none>            80/TCP            4h19m
```

```
> k exec -it r2-d2 -- nslookup resistance
...
Name:   resistance-base.default.svc.cluster.local
Address: 192.168.0.246
```



Pods provide endpoints for services

› k get endpoints

NAME	ENDPOINTS	AGE
kubernetes	172.19.0.3:6443	4h18m
resistance	10.0.0.173:8080, 10.0.0.244:8080, 10.0.0.31:8080	4h17m

› k get pods -o wide

NAME	READY	STATUS	RESTARTS	AGE	IP
bb-8	1/1	Running	0	5m48s	10.0.0.119
resistance-5f77df8c9c-56svw	1/1	Running	0	78m	10.0.0.173
resistance-5f77df8c9c-8vvvc	1/1	Running	0	78m	10.0.0.31
resistance-5f77df8c9c-ppxjp	1/1	Running	0	78m	10.0.0.244

Cilium knows about services and endpoints

```
> ks exec -it $CPOD -- cilium service list
```

ID	Frontend	Service Type	Backend
...			
7	192.168.0.246:80	ClusterIP	1 => 10.0.0.31:8080 (active) 2 => 10.0.0.244:8080 (active) 3 => 10.0.0.173:8080 (active)

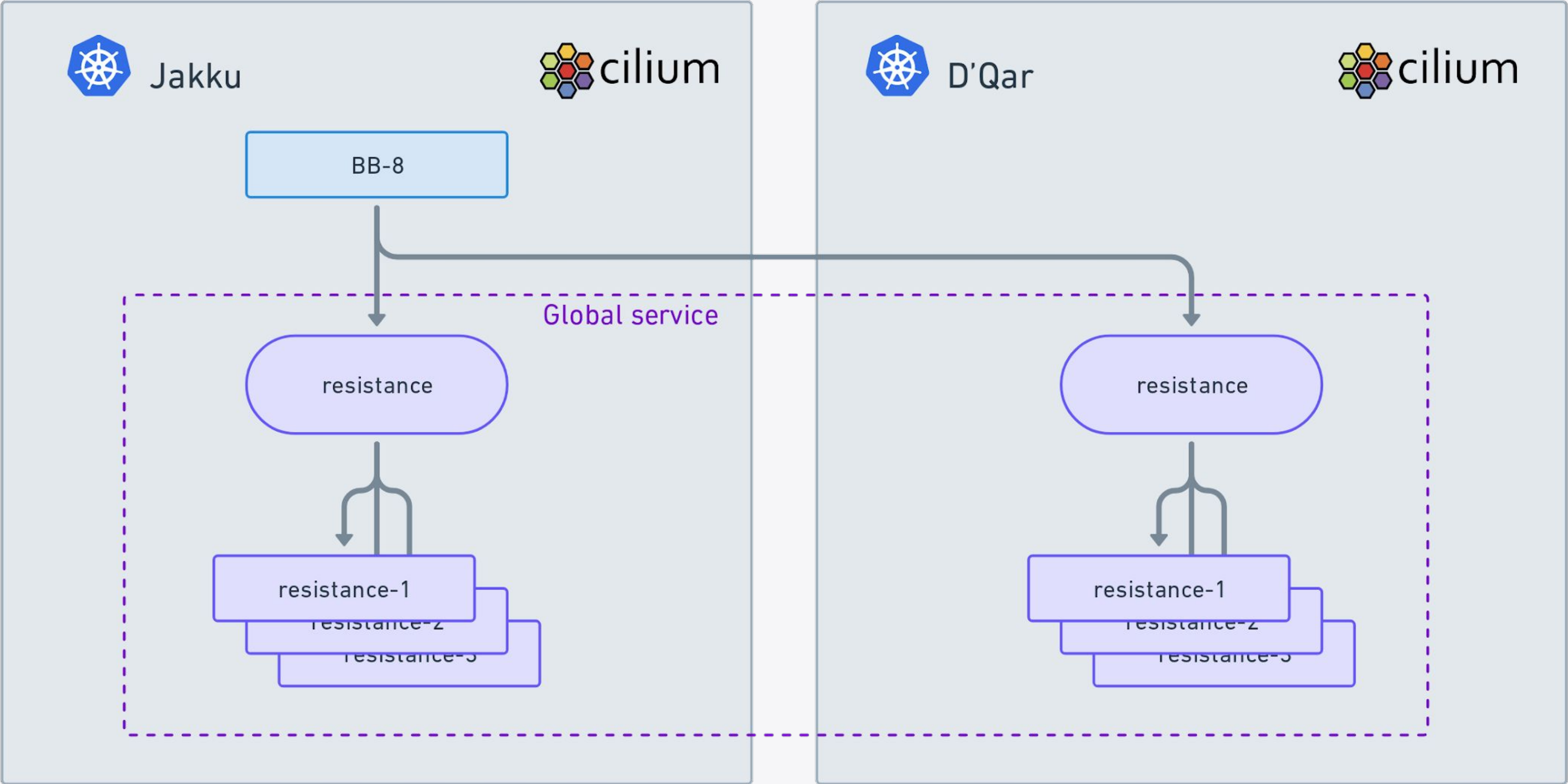
```
> ks exec -it $CPOD -- cilium endpoint list
```

ENDPOINT	...	IDENTITY	LABELS (source:key[=value])	IPv6	IPv4	STATUS
...						
59	...	135505	k8s:app=resistance-base k8s:io.cilium.k8s.policy.cluster=d-qar k8s:io.cilium.k8s.policy.serviceaccount=default k8s:io.kubernetes.pod.namespace=default k8s:org=resistance k8s:io.cilium.k8s.namespace.labels.kubernetes.io/metadata.name=default		10.0.0.173	ready
...						

ISOVALENT

Cilium ClusterMesh for multi-cluster services

ISOVALENT



ClusterMesh - endpoints around the mesh


```
> ks exec -it $CPOD -- cilium service list
```


ID	Frontend	Service Type	Backend
...			
8	192.168.0.30:80	ClusterIP	1 => 10.0.0.31:8080 (active) 2 => 10.0.0.244:8080 (active) 3 => 10.0.0.173:8080 (active) 4 => 10.0.0.136@2:8080 (active) 5 => 10.0.0.4@2:8080 (active) 6 => 10.0.0.120@2:8080 (active)


...


**Not all workloads run on
Kubernetes...**
Cilium external endpoints


ISOVALENT

 Jakku

 cilium

 D'Qar

 cilium



Ahch-to



Add Cilium endpoints for external workloads

```
> k describe svc ahch-to
Name:                ahch-to
Annotations:         io.cilium/global-service: true
                   io.cilium/portal: true
Selector:           jedi=luke
Type:               ClusterIP
IP:                192.168.0.202
IPs:               192.168.0.202
Port:              <unset> 80/TCP
TargetPort:        80/TCP
Endpoints:         <none>
```

```
> ks exec -it $CPOD -- cilium endpoint add --name=ahch-to --labels=jedi=luke --ip=172.19.100.2
```

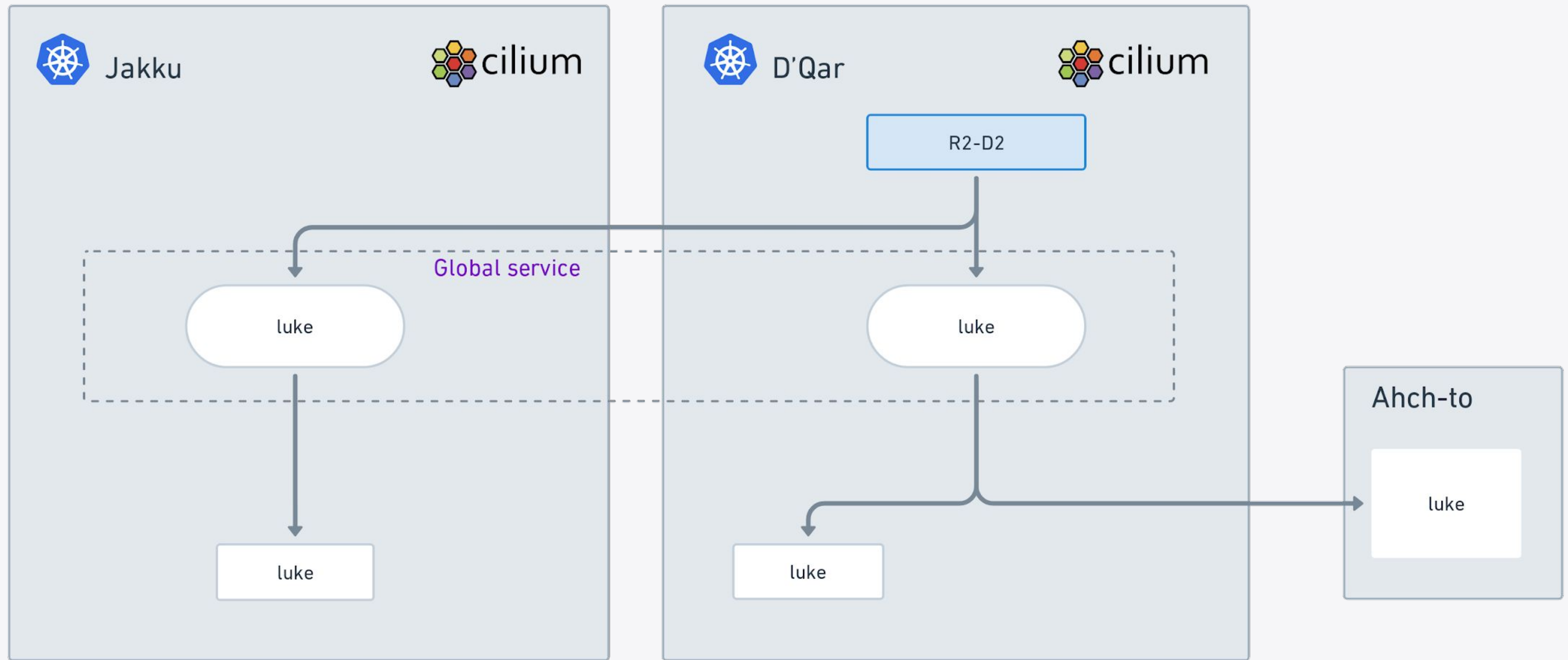
```
> ks exec -it $CPOD -- cilium service list
```

ID	Frontend	Service Type	Backend
...			
9	192.168.0.202:80	ClusterIP	1 => 172.19.100.2:80 (active)

ISOVALENT

Migrate legacy workloads to **Kubernetes**

Migrate legacy workloads to Kubernetes



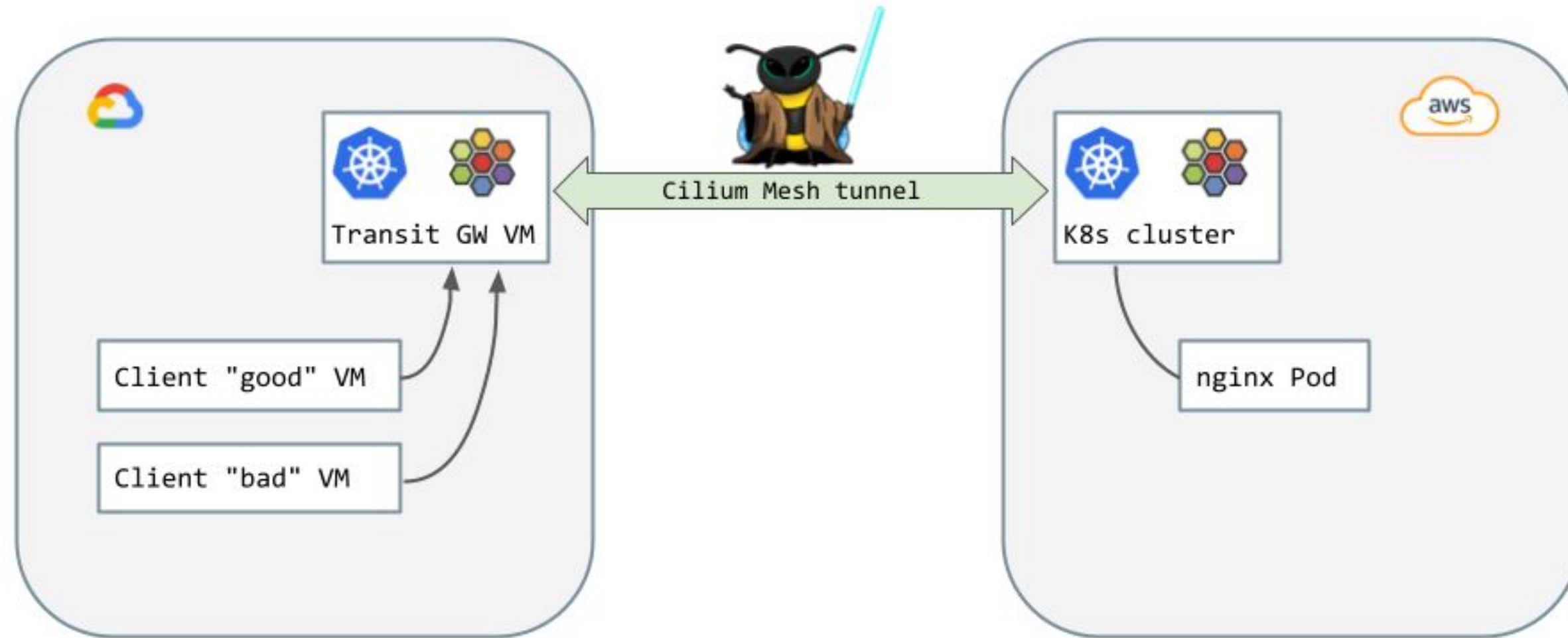
ISOVALENT

Protected with **CiliumNetworkPolicies**

CiliumNetworkPolicies protect traffic to/from endpoints

```
apiVersion: cilium.io/v2
kind: CiliumClusterwideNetworkPolicy
metadata:
  name: resistance
spec:
  endpointSelector:
    matchLabels:
      org: resistance
  ingress:
    - fromEndpoints:
        - matchLabels:
            org: resistance
```

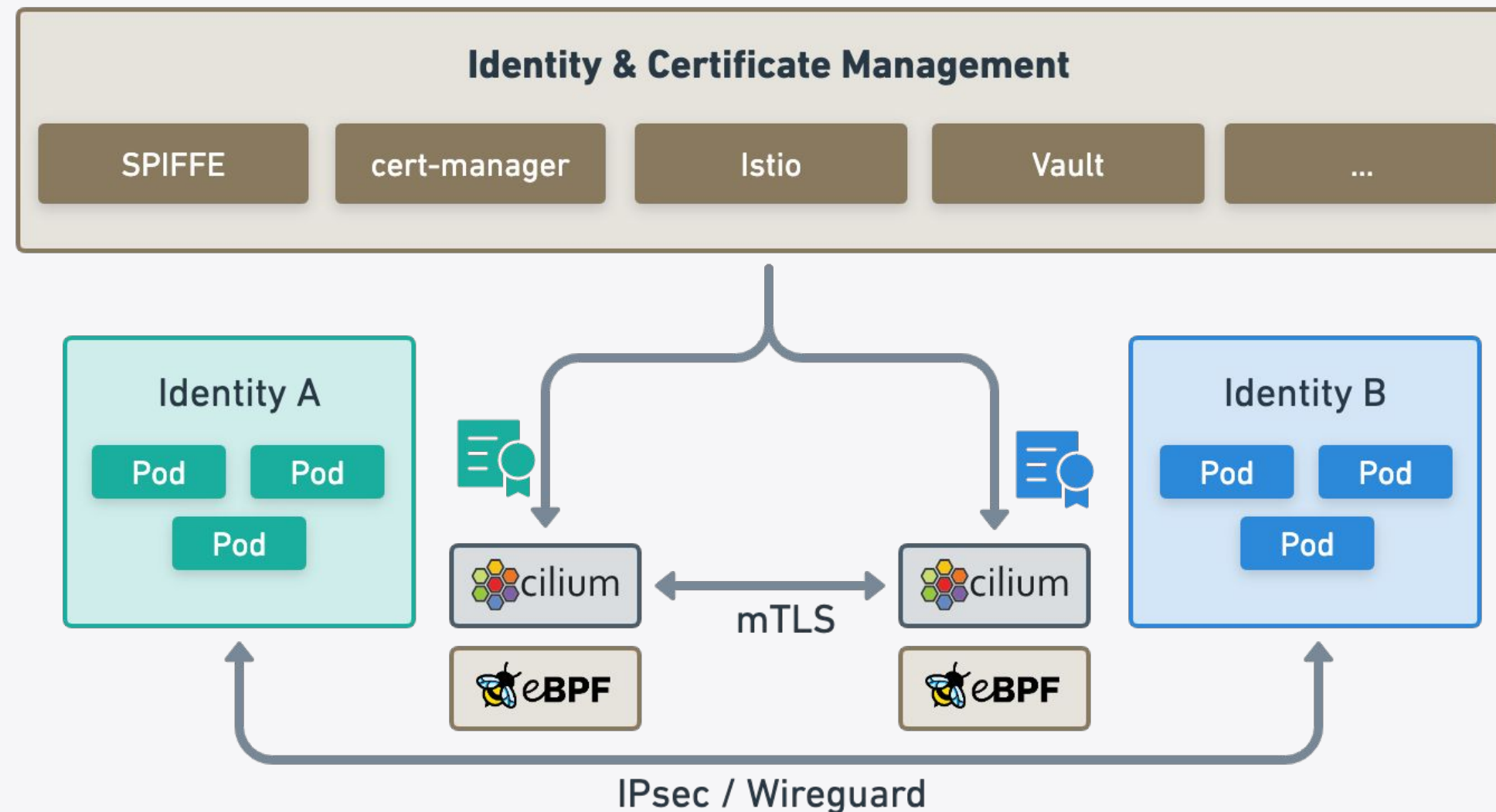
ISOVALENT



ISOVALENT

Authenticated and encrypted
using SPIFFE identities

Cilium next-gen mutual authentication & encryption



Datapath support in 1.13:

<https://github.com/cilium/cilium/pull/21822>

CiliumNetworkPolicy specifies authentication policy

```
apiVersion: "cilium.io/v2"
kind: CiliumNetworkPolicy
metadata:
  name: "auth-ingress"
spec:
  endpointSelector:
    matchLabels:
      app: backend
  ingress:
  - fromEndpoints:
    - matchLabels:
        app: frontend
    auth:
      required: strict
```

Auth PR:

<https://github.com/cilium/cilium/pull/24263>

Encryption tracked under:

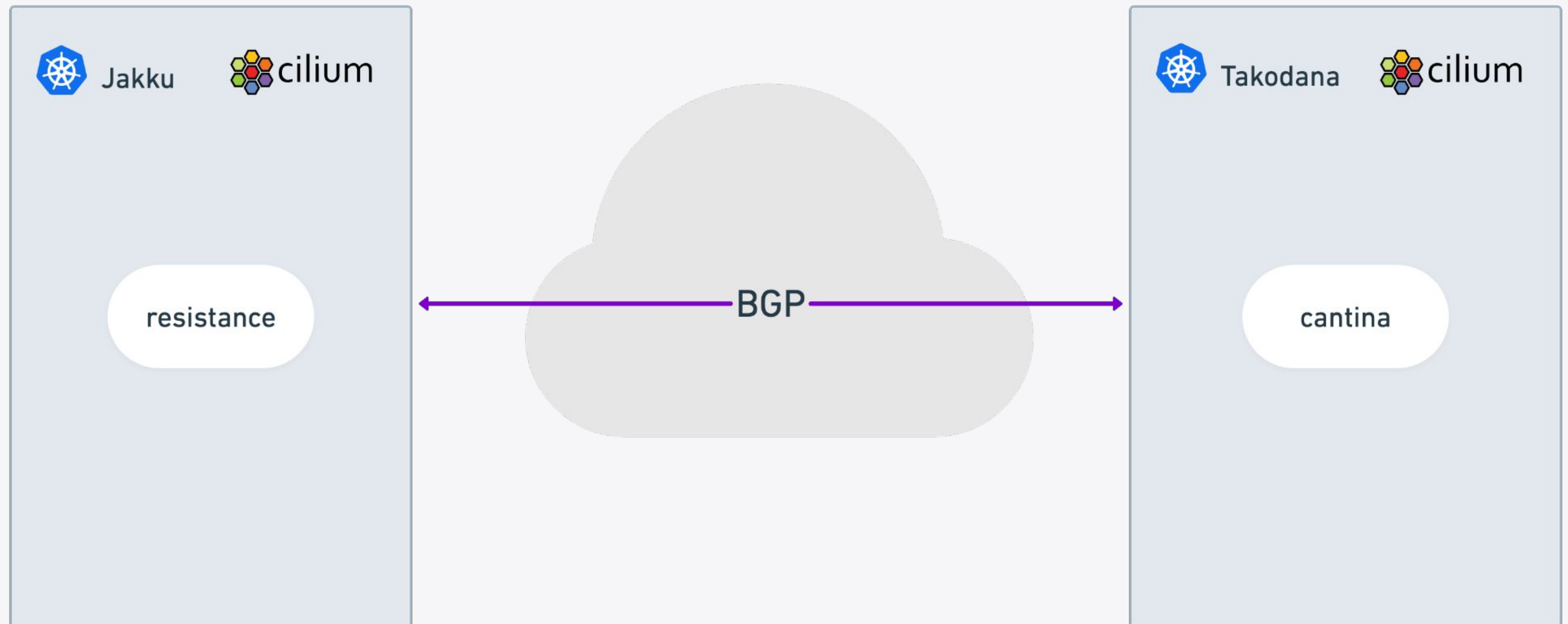
<https://github.com/cilium/cilium/issues/22215>

Require authentication for connections to backends

ISOVALENT

Cilium can advertise **services** **over BGP**

Advertise services over BGP networks



Cilium Mesh

Connect workloads ✓
in multiple clusters ✓
and non-Kubernetes environments ✓
in public clouds and on-prem ✓
securely: network policies ✓
and authenticated + encrypted ✓

ISOVALENT

Thank you



[cilium/cilium](https://github.com/cilium/cilium)



[@ciliumproject](https://twitter.com/ciliumproject)

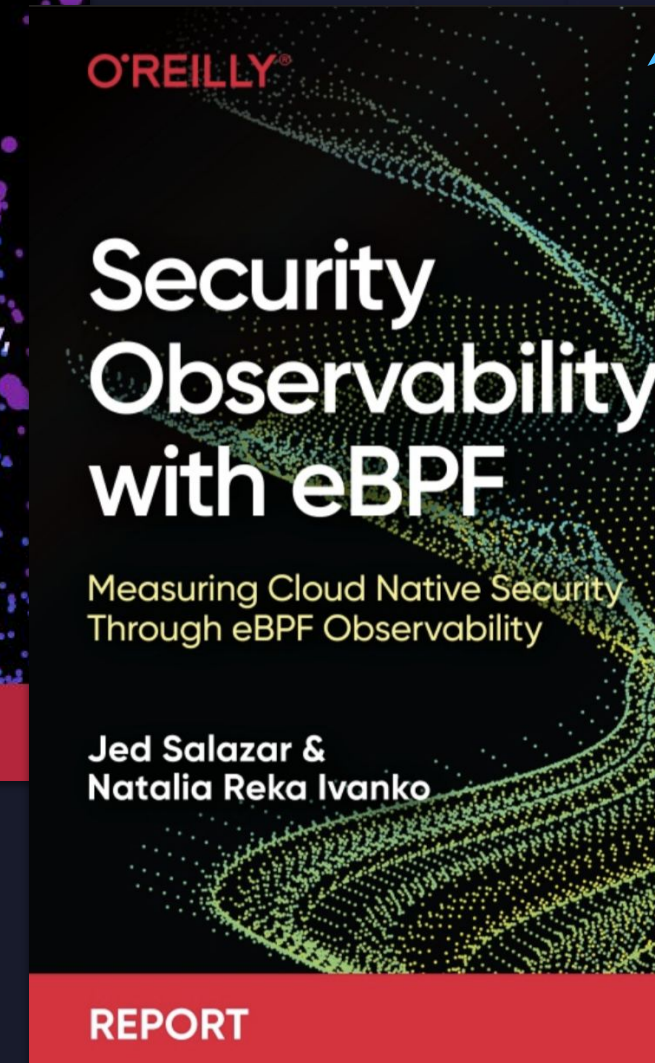
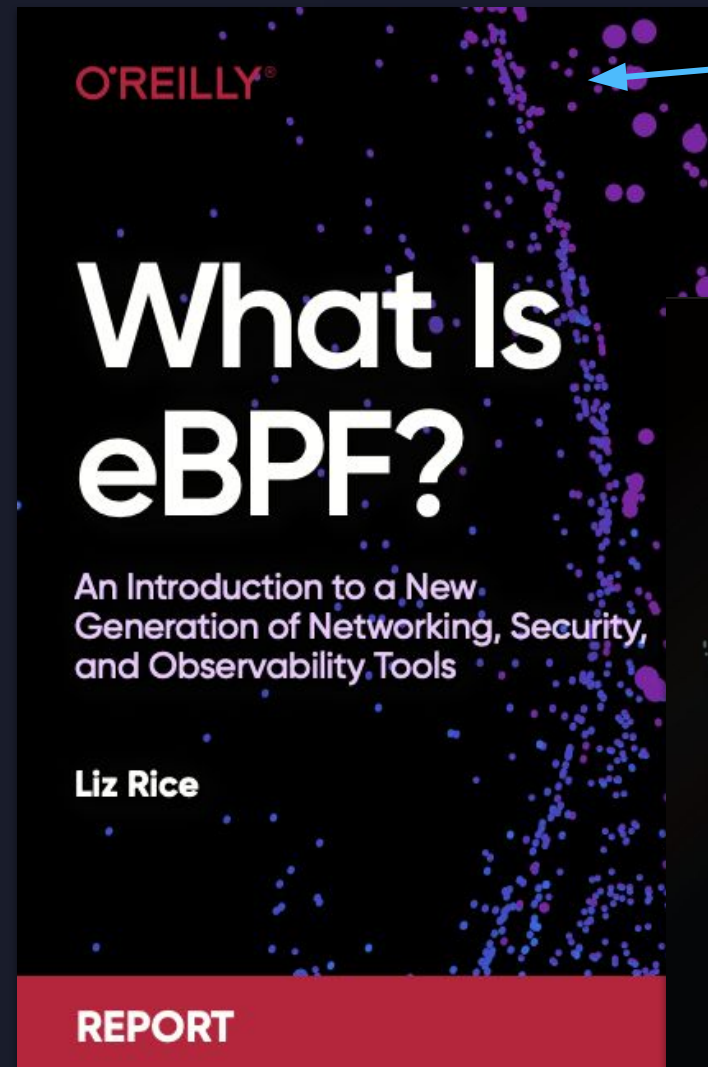


cilium.io



isovalent.com/labs

[@lizrice](https://twitter.com/lizrice)



Download from
isovalent.com