

Identity Bootstrapping in Multi-tenant Multi-cluster Kubernetes

Manish Mehta

Chief Security Architect, Volterra

Derek Suzuki

Director of DevOps, The Voleon Group

Volterra

Liberate your Infrastructure, Applications, and Data



SaaS provider enabling customers to **build**, **deploy**, **secure**, and **operate** distributed applications and data across multiple cloud providers and edge locations.

- Why?

- Applications Distributed across Geo-locations, Cloud providers and Edge locations
 - tl; dr; - Not if, but when
 - High Availability, DR, Latency/Performance, Compliance, Multi-cloud, Distributed Cloud, Cost, Dev/Prod, Edge etc.

- Challenges

- Networking/Routing
- Service Discovery
- Visibility/Monitoring
- CI/CD
- Isolation (tenancy)
- Security/Trust

Why Kubernetes?

- Community support
- Rich core functions
- Soft-tenancy available
- Pluggable and Extensible
- ...

- Definition (from Dictionary*)

identity (aI den tih ti)

The unique and entire set of characteristics that make up what a person or thing is known or considered to be.

- Definition (from Crypto Geeks)

identity (aI den tih ti)

The unique and entire set of **unforgeable and cryptographically verifiable** characteristics **cryptographically certified via an undelegated and secure protocol** by a **trusted authority** that make up what a person or thing is known or considered to be.

Why we need Cryptographic Identity?

- Identity Owner
 - Secure Communication
 - Prove eligibility
 - Vindication
- Peers
 - Secure Communication
 - Audit/Accounting
 - Non-repudiation

What makes a solid identity?

1. Granular
2. Securely Minted/Delivered
3. Rich, Usable, Extensible

1. Granular

Kubernetes Documentation:

“*Pods* are the smallest deployable units of computing that can be created and managed in Kubernetes.”

NOT Namespace

NOT Service Account

IT IS Pod



Identity Boundary = Trust Boundary

2. Secure Minting and Delivery

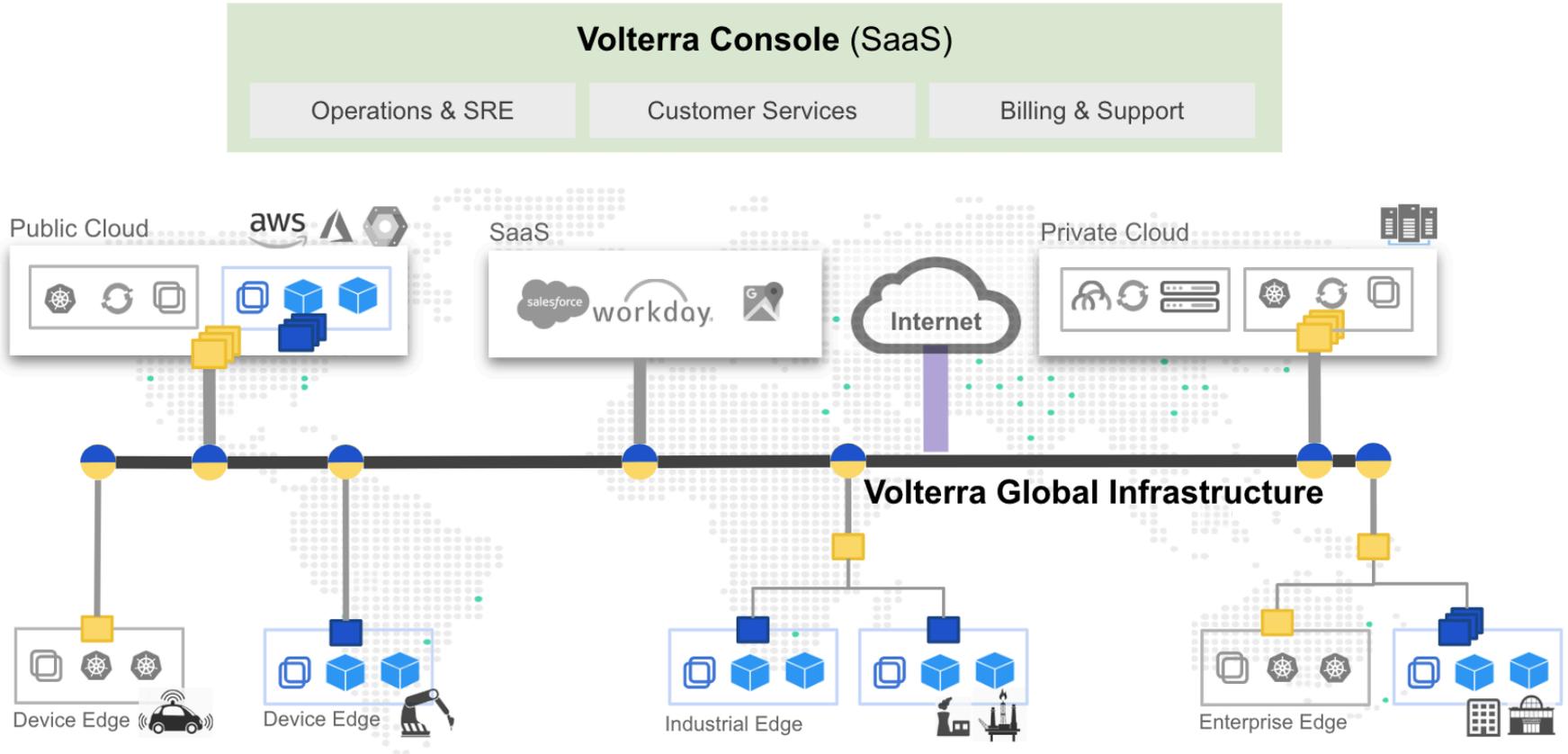
- What is the “blast radius” of a compromised authority?
- Can the compromise go unnoticed?
- Who generated or has access to the identity secrets?
 - Private key generated outside of the pod
 - Private key accessible by anyone other than the pod
- Does the delivery method limit where it can be used?

A solid identity solution should keep identity-related cryptographic material within the trust boundary (pod).

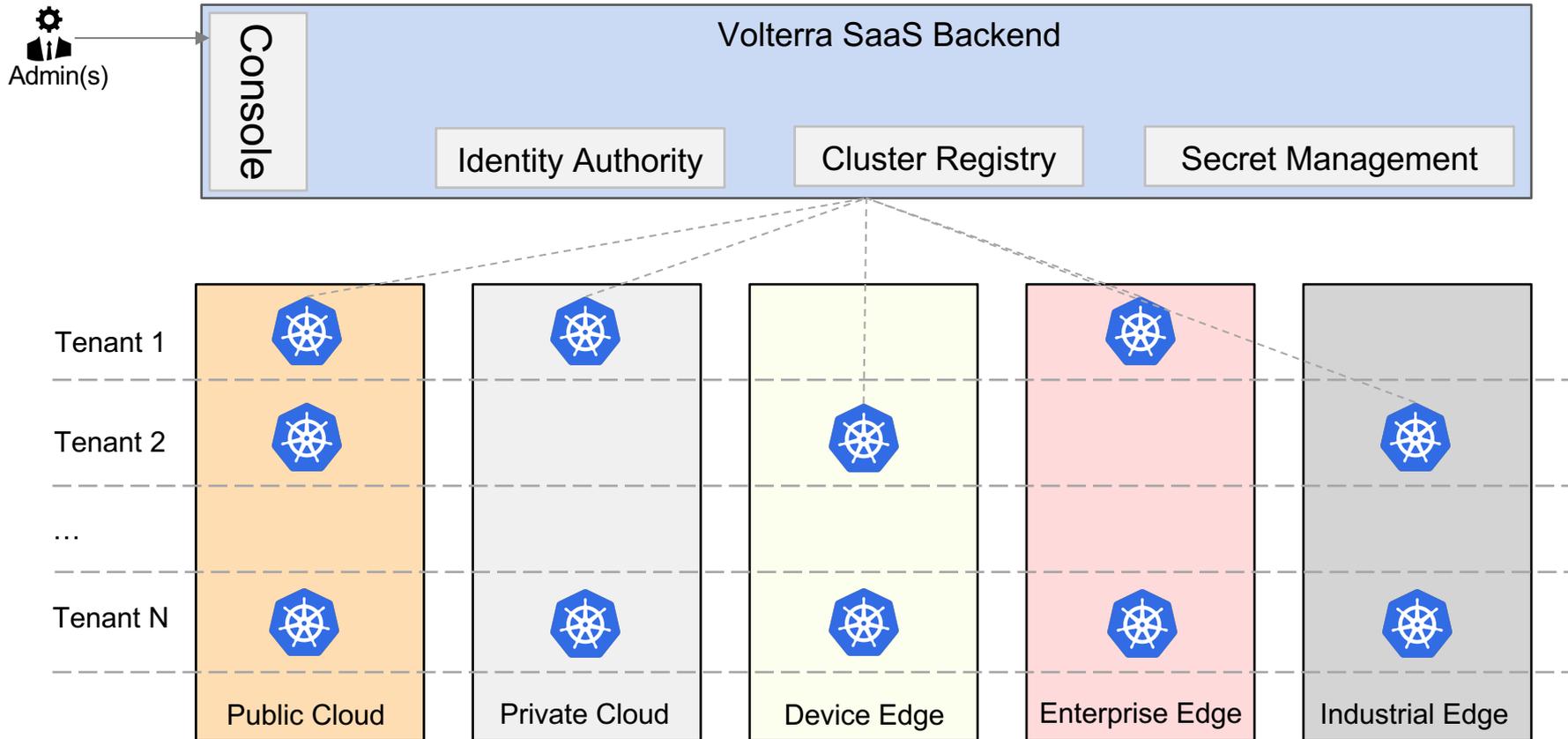
3. Rich, Usable, and Extensible

- What all does the identity credentials contain?
- How usable is it without changing current practices?
- How easy it is to extend identity proof?

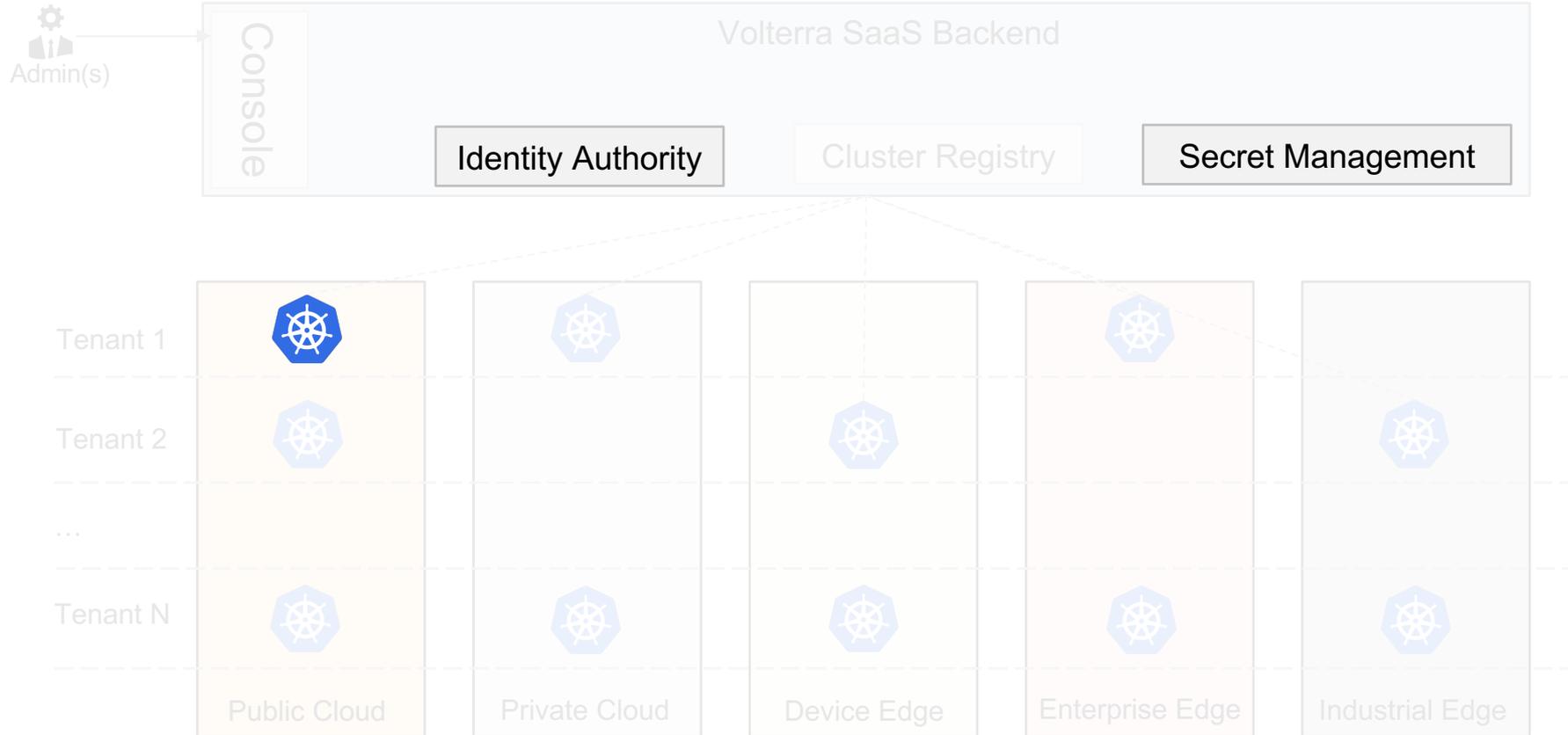
Identity Bootstrapping in Multi-Cluster – Volterra's take



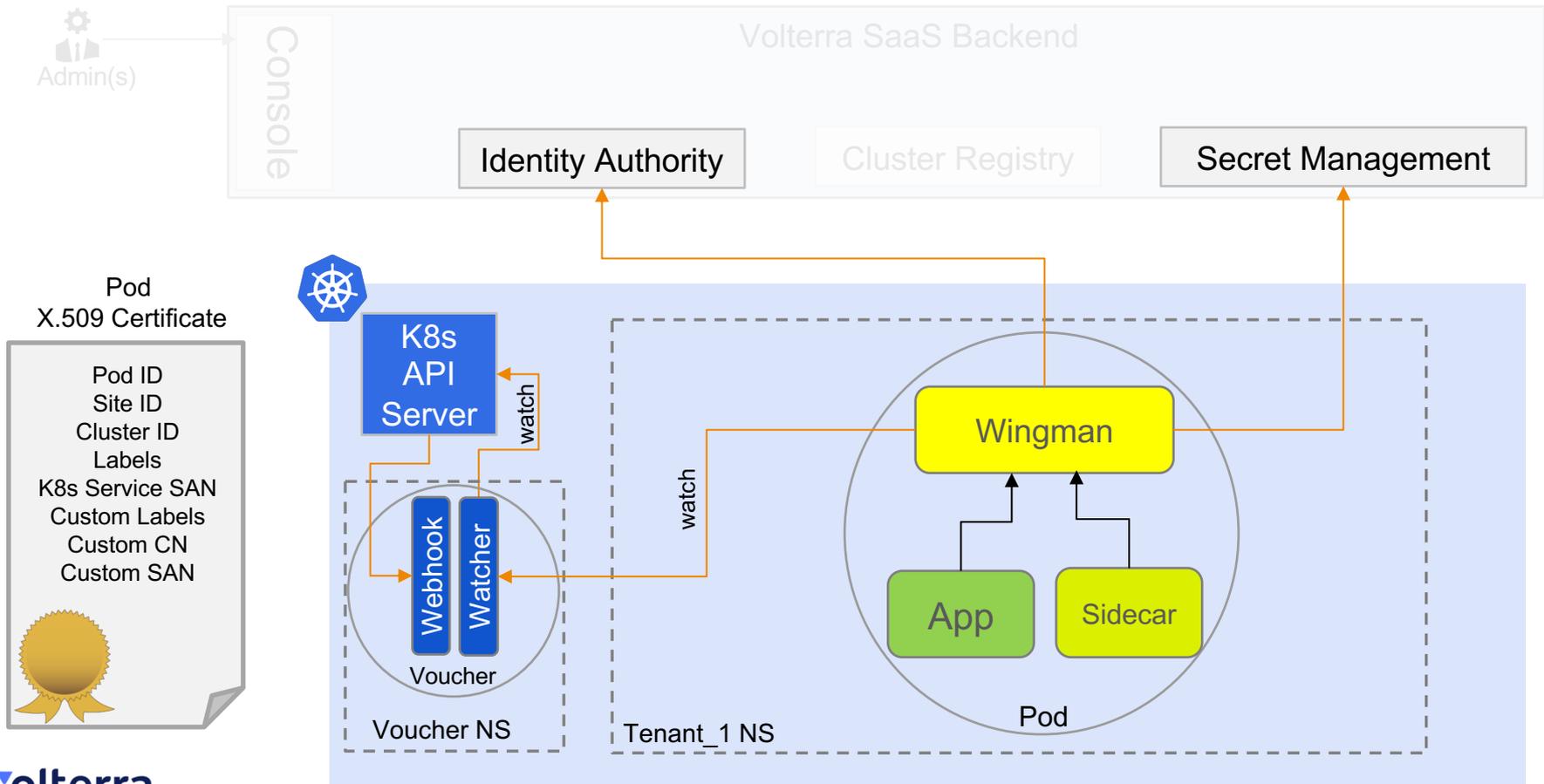
Identity Bootstrapping in Multi-Cluster - Volterra's take



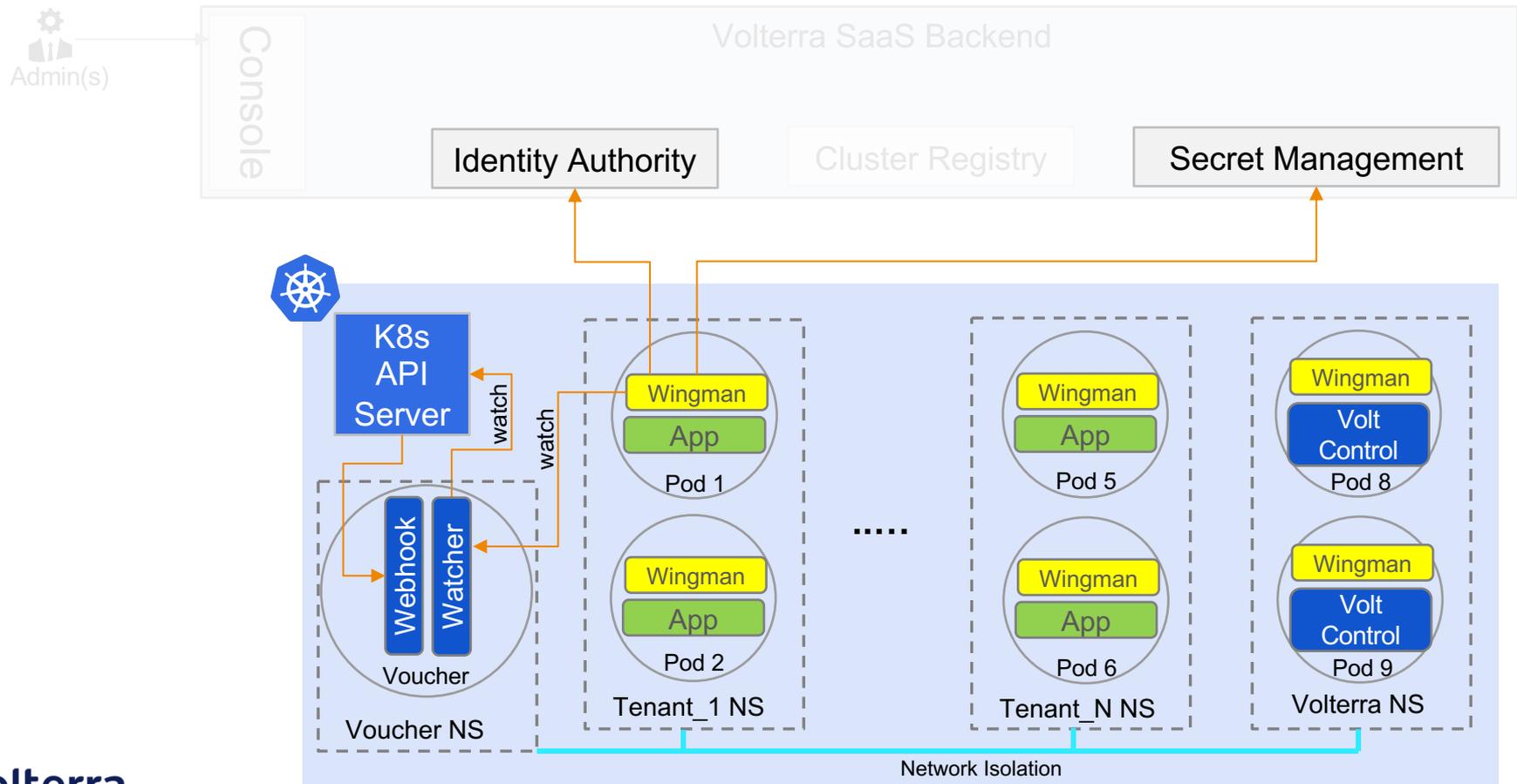
Identity Bootstrapping in Multi-Cluster – Volterra's take



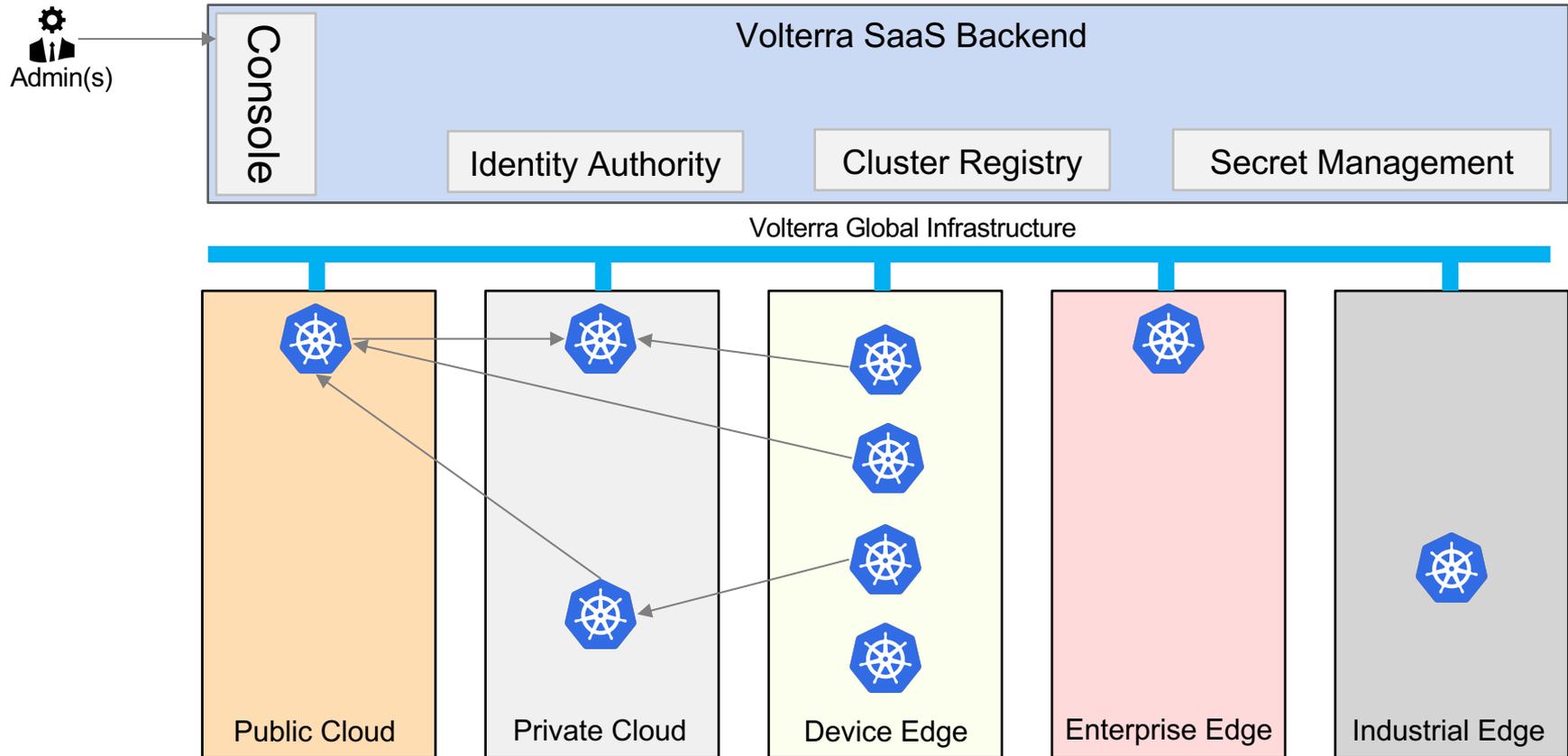
Identity Bootstrapping in Multi-Cluster - Volterra's take



Identity Bootstrapping in Multi-Cluster - Volterra's take

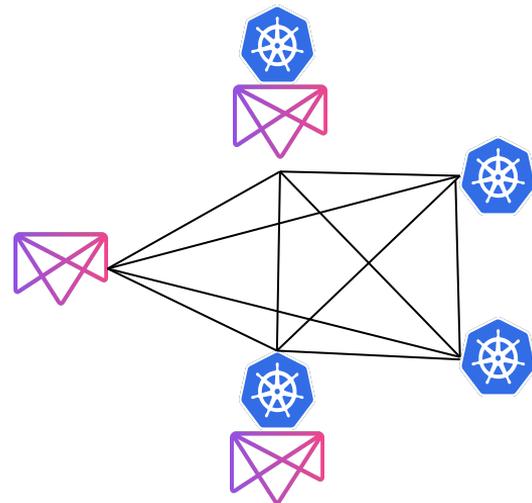


Identity Bootstrapping in Multi-Cluster - Volterra's take



Customer Perspective: Managing Access and Secrets across Multiple Clusters

- Multiple standalone clusters
 - Mesosphere DC/OS, Kubernetes, and Kubernetes on DC/OS
 - Multiple locations, multiple islands
- Cluster-level secrets management
 - Standard Kubernetes secrets
 - DC/OS Enterprise with embedded Vault
- Global secrets management through Vault
 - Single source of truth for secrets



- Possible solutions and their drawbacks
 - Homegrown integration
 - Development/maintenance costs
 - Limited by capabilities of cluster-level tools
 - Third-party container security software (Aqua, Twistlock)
 - Immature
 - Complexity/performance
 - Proprietary vendor software accessing secrets

- Feature requirements
 - Big picture: centralized management of secrets across multiple environments in multiple sites
 - Small picture: fine-grained control over secrets access and other access policies
 - Volterra provides centralized, cross-cluster management to cover the big picture and global identity management to cover the small picture

- Solid Identity
 1. Granular
 - Pod, Not Namespace, Not Service Account
 2. Securely Minted/Delivered
 - Private key always inside the pod, Limit blast radius
 3. Rich, Usable, Extensible
 - Readily usable format, not tied to specific usage

Take Away

- Identity bootstrapping is the foundation of modern security
- Multi-cluster deployments turn *cumbersome* into *unmanageable*
- Understand the risks of prescriptive solutions
- Secrets are called Secrets for a reason. Do not let others ever hand them to you.

Thank you!

We are hiring !

