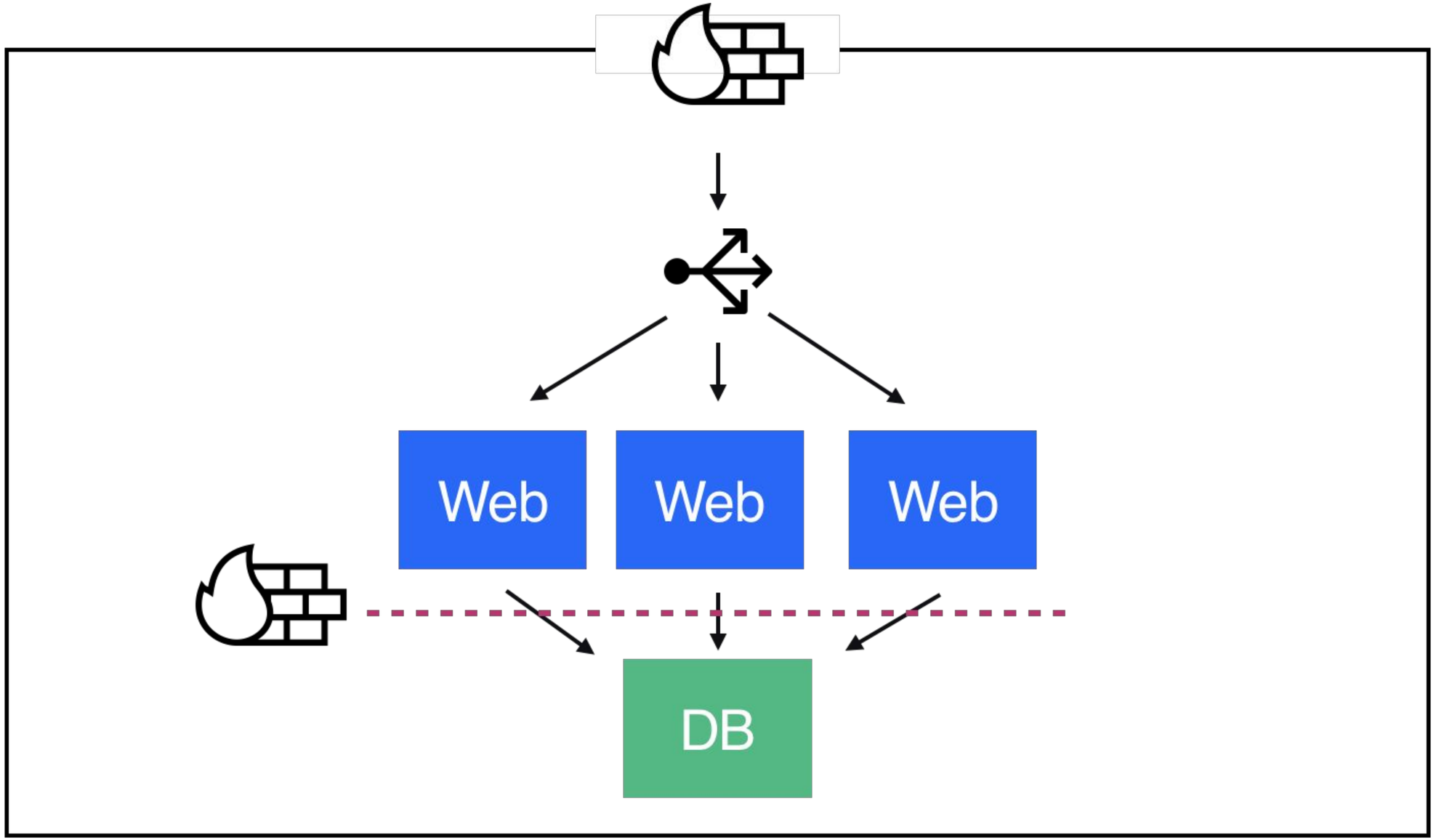
Securing Kubernetes Applications with Consul and Vault

What is Service Mesh?

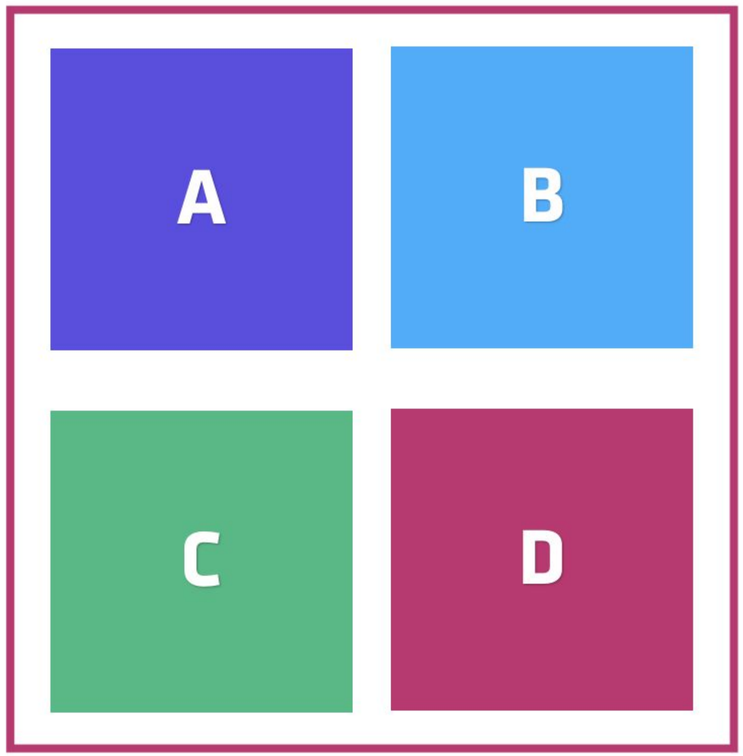
Why should I use Service Mesh?

History of Services

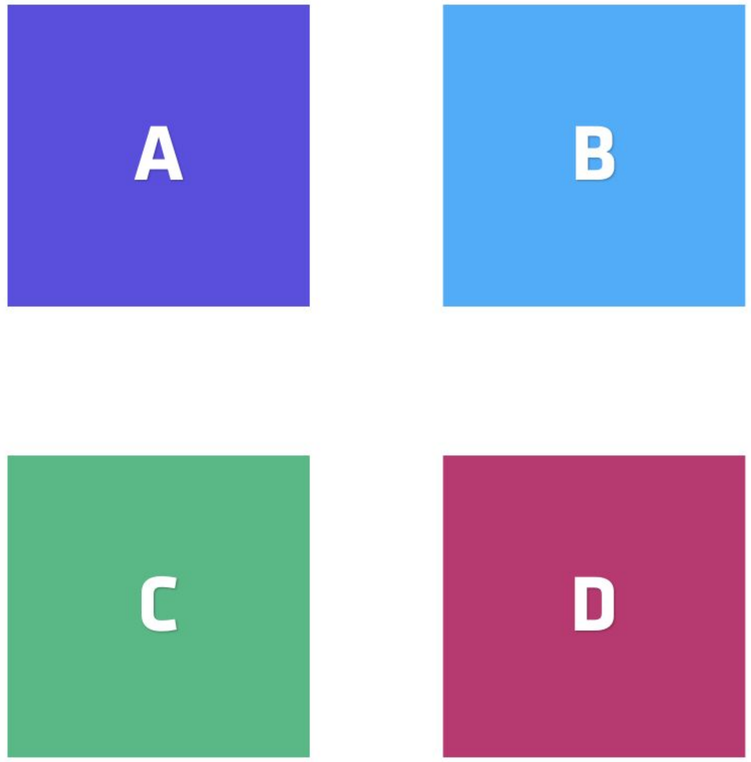
Traditional Datacenter



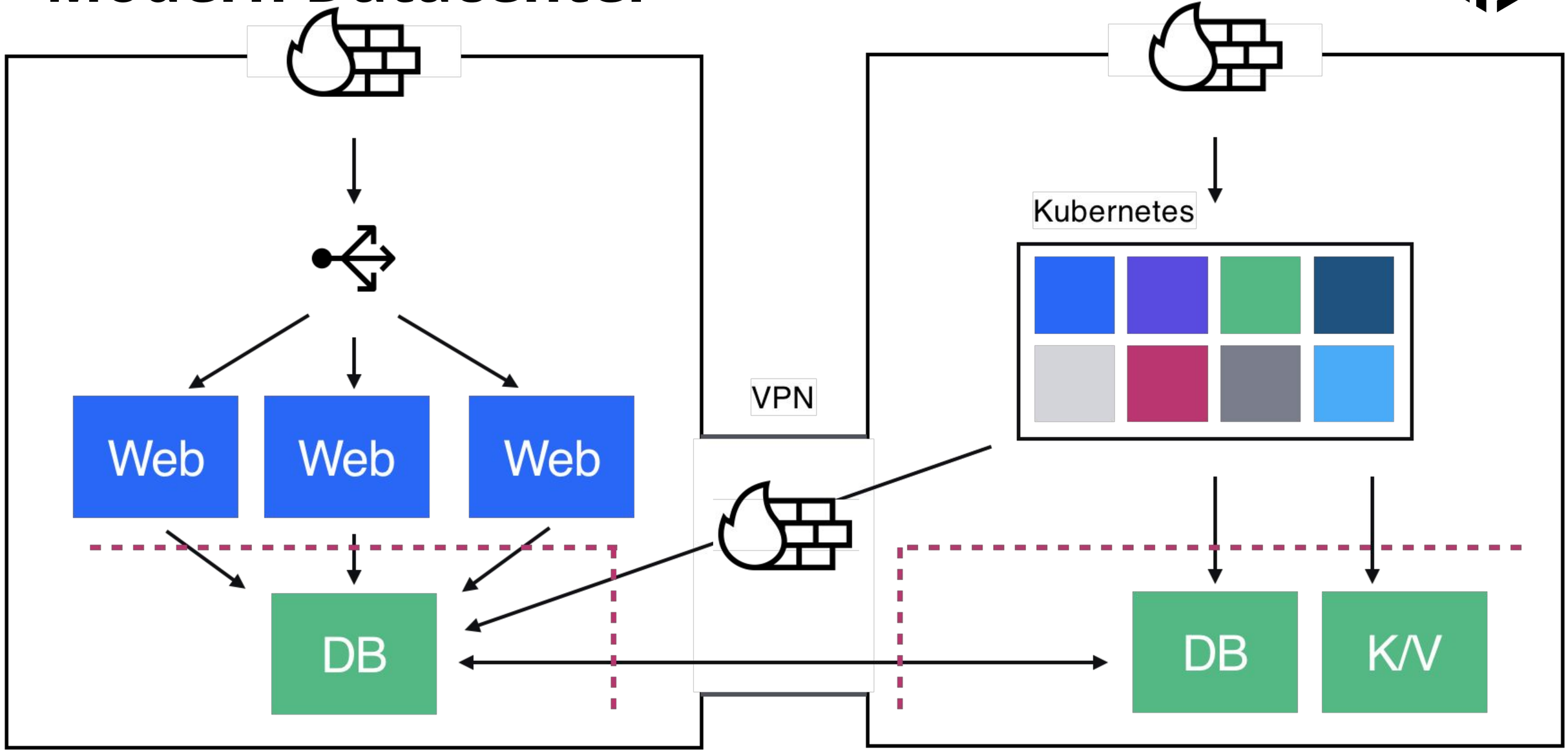
Monoliths



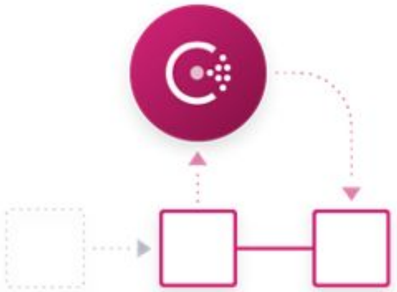
Microservices



Modern Datacenter

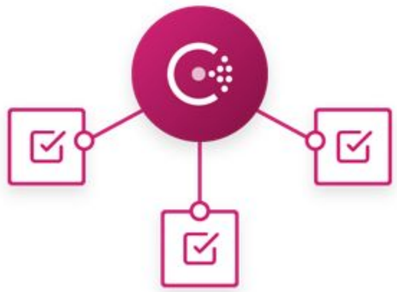


Dynamic Infrastructure Challenges



Service Discovery

Service Segmentation

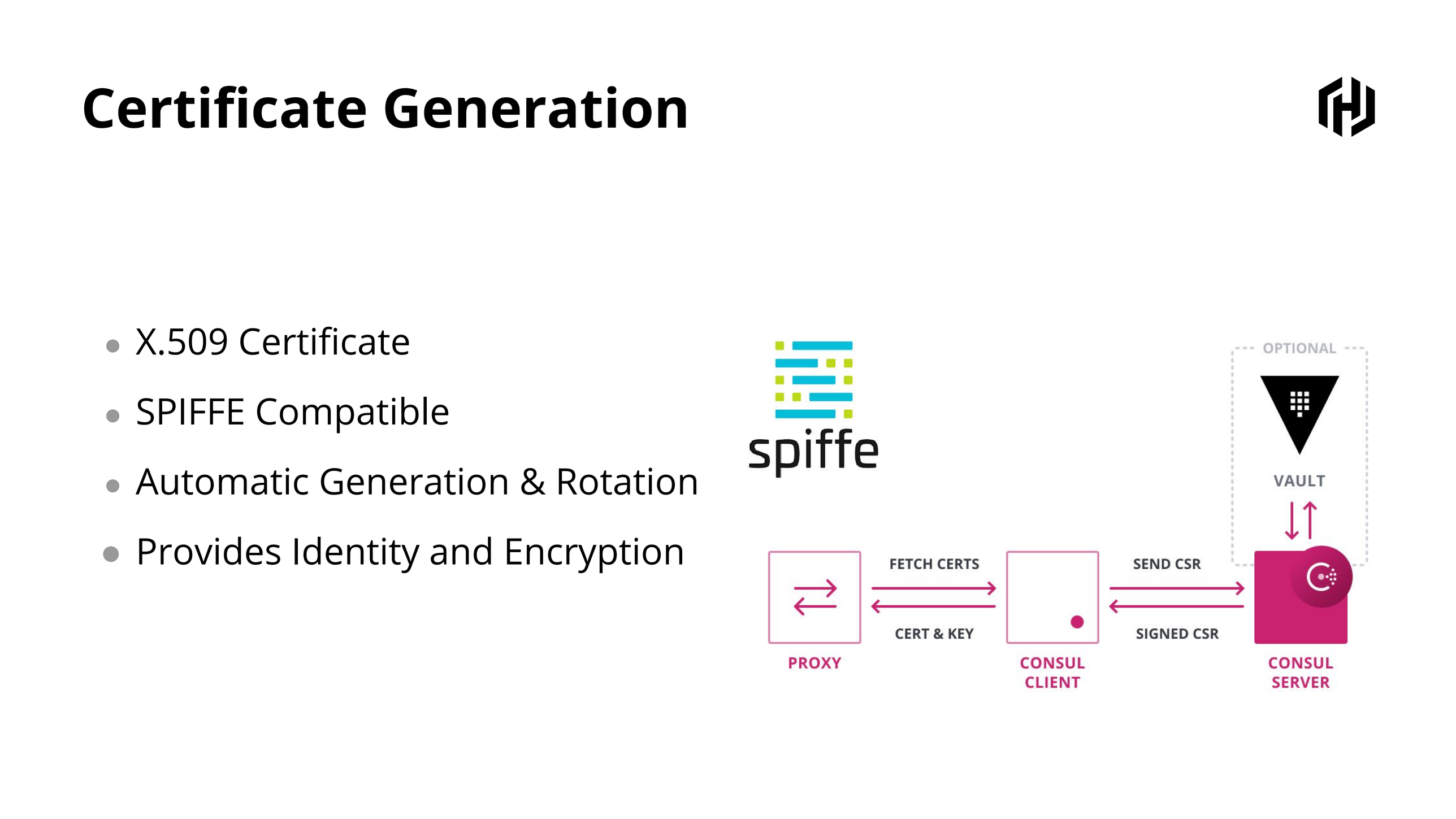


Service Configuration

Consul Service Mesh

Certificate Authority

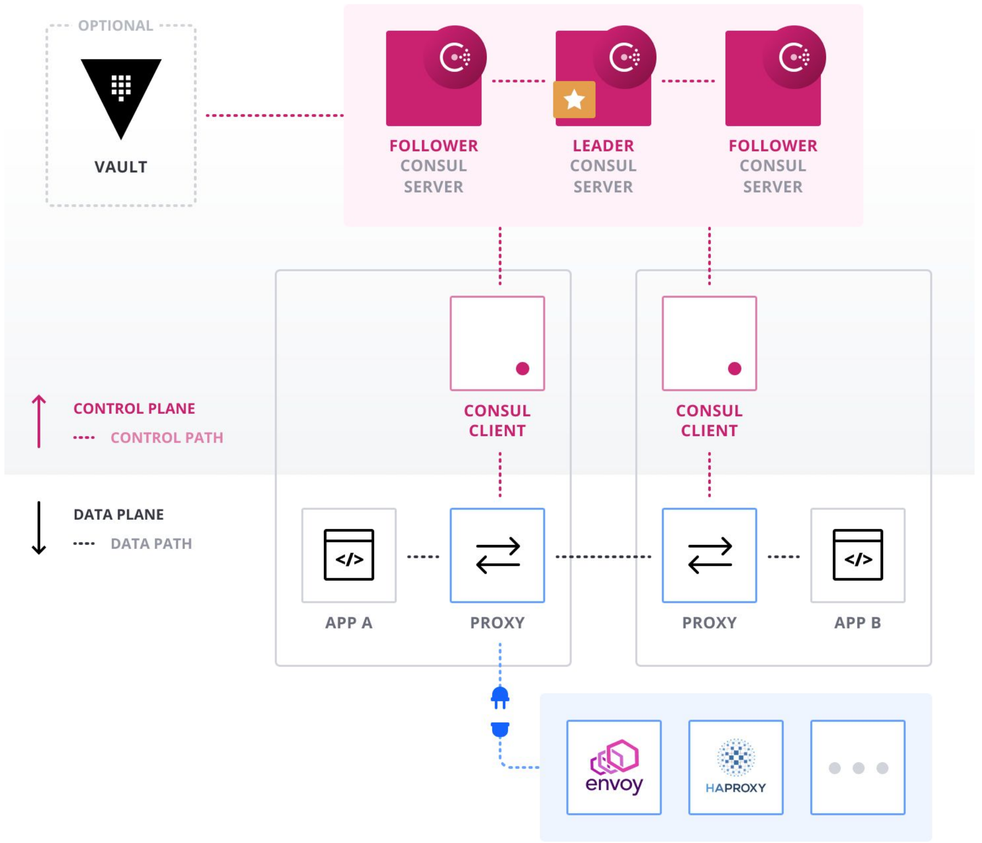
Certificate Generation



- X.509 Certificate
- SPIFFE Compatible
- Automatic Generation & Rotation
- Provides Identity and Encryption

Control Plane vs. Data Plane

- Consul as Control Plane
- Pluggable Proxies as Data Plane
- Instructions to proxies are cached on the Consul agent
- New instructions are pulled only on changes



Service Access Graph

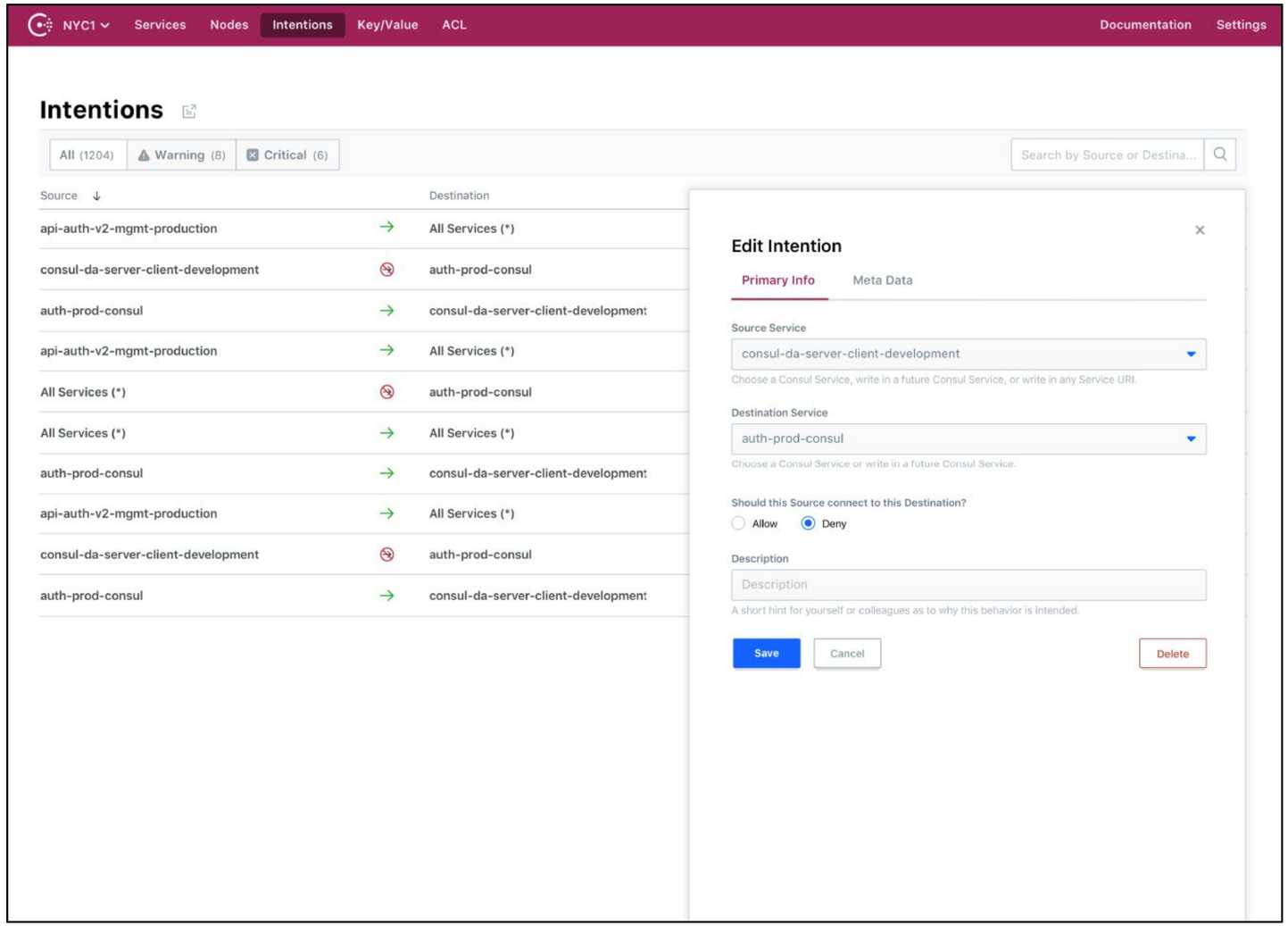
Service Graph

Codify Intentions

Same intentions are applied no matter where the service exists

Web UI

Manage intentions via web interface



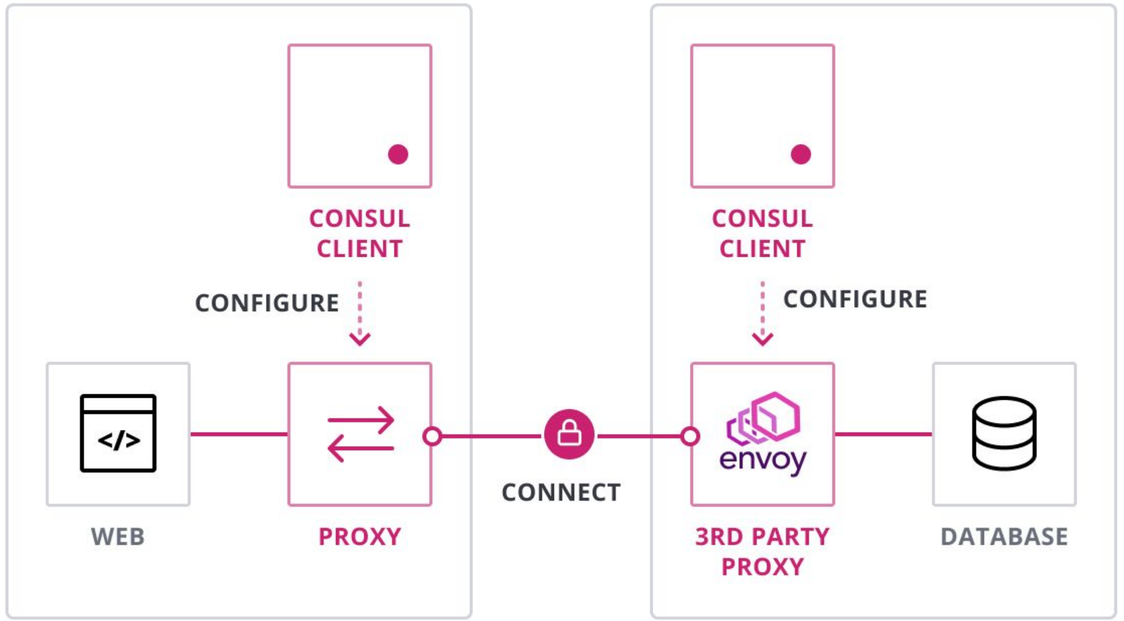
Application Integration

Sidecar Proxies

Sidecar proxy to secure traffic for any application

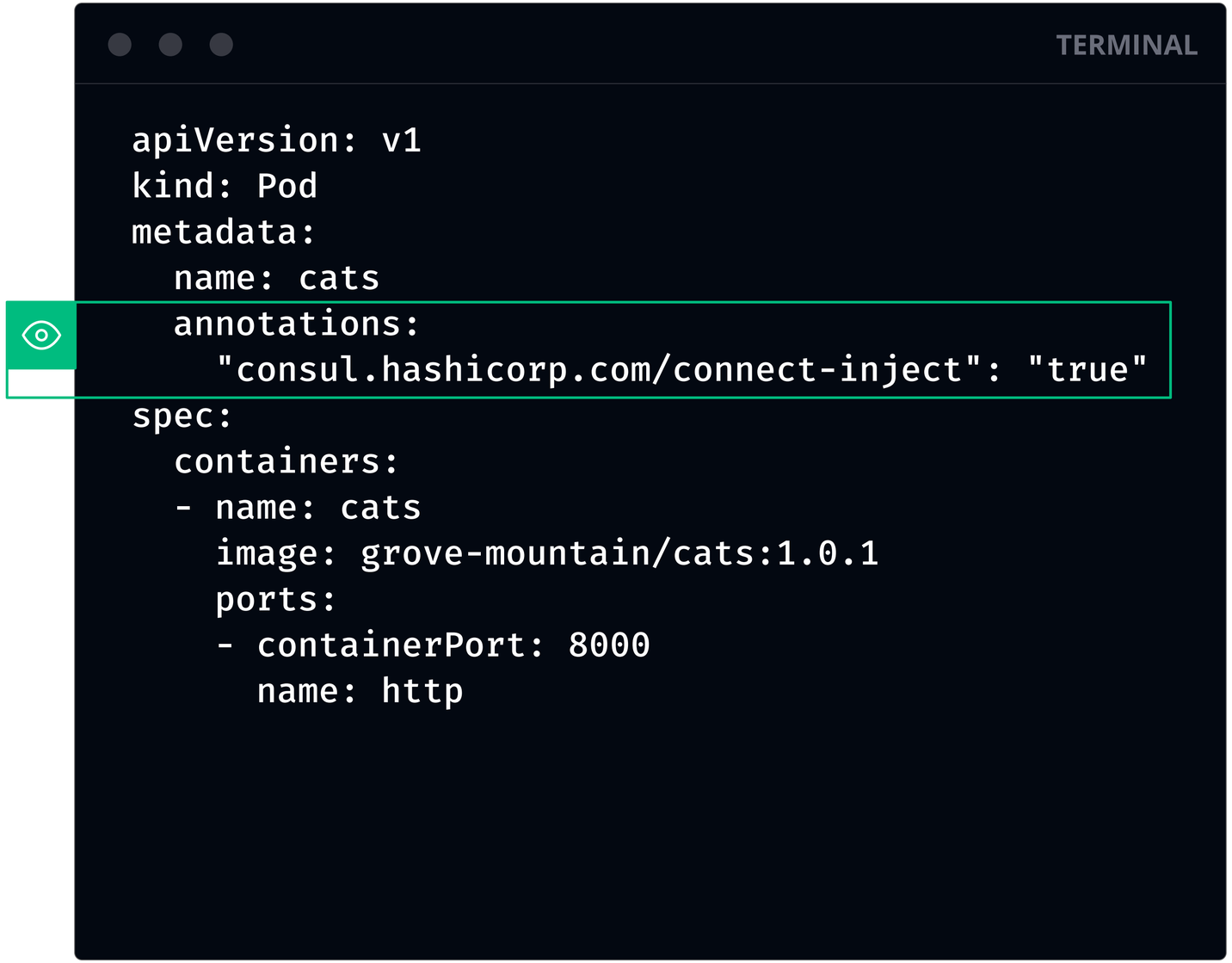
Consul provides sidecar proxies running alongside applications to transparently wraps traffic in TLS and enforces the intentions.

- No code modification required
- Minimal performance overhead
- Pluggable data plane: Built-in Layer 4 proxy, native Envoy integration or other third-party proxy integration
- Operational flexibility, decoupling security concern from the application itself

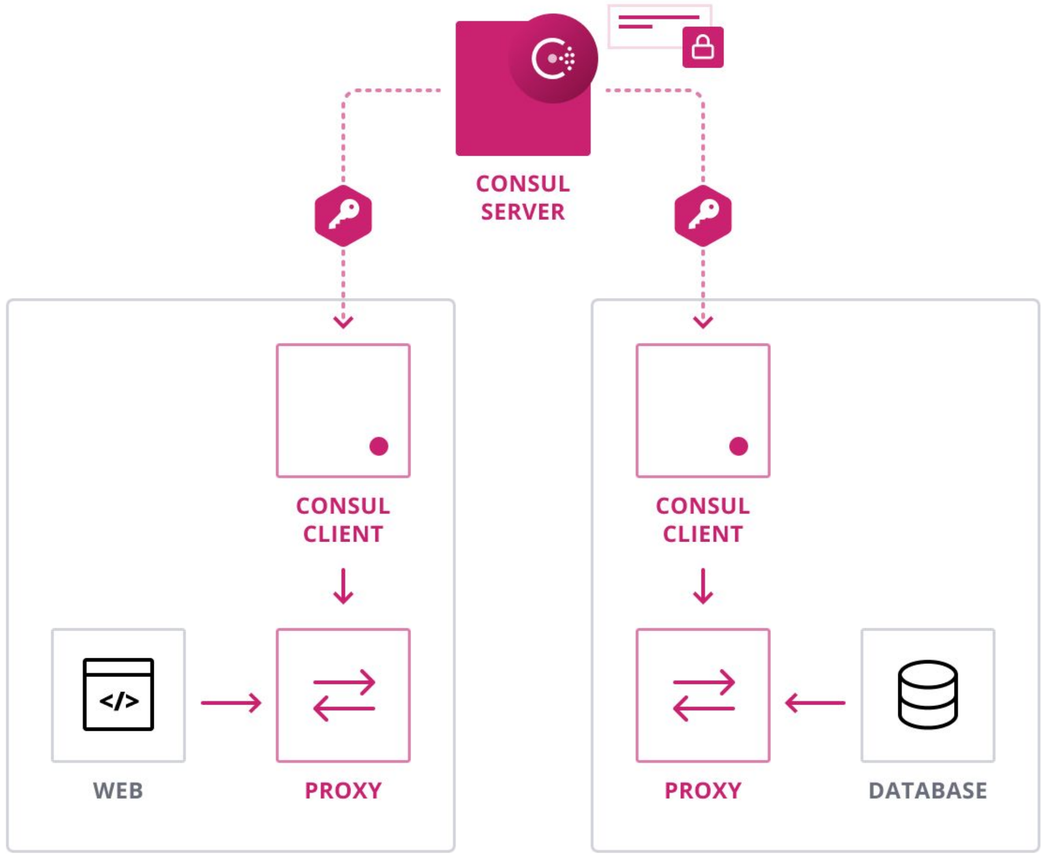


Proxy Registration

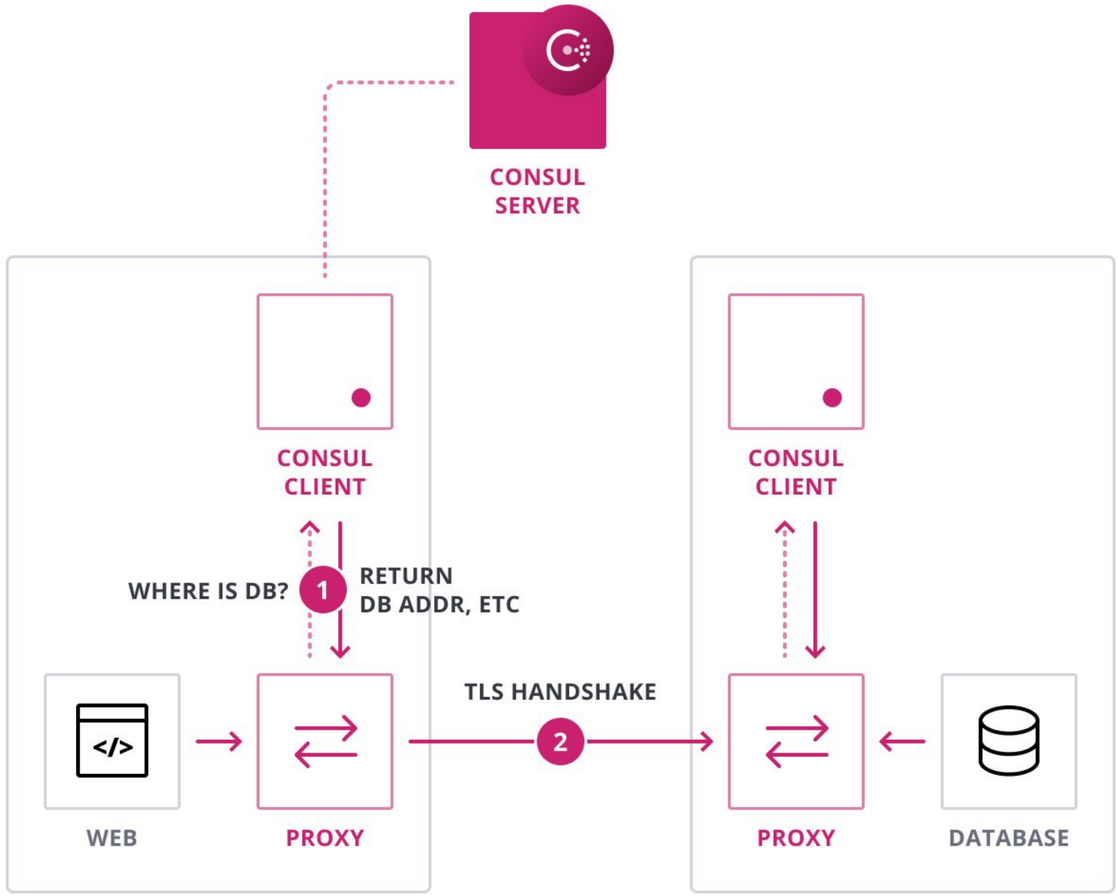
Kubernetes



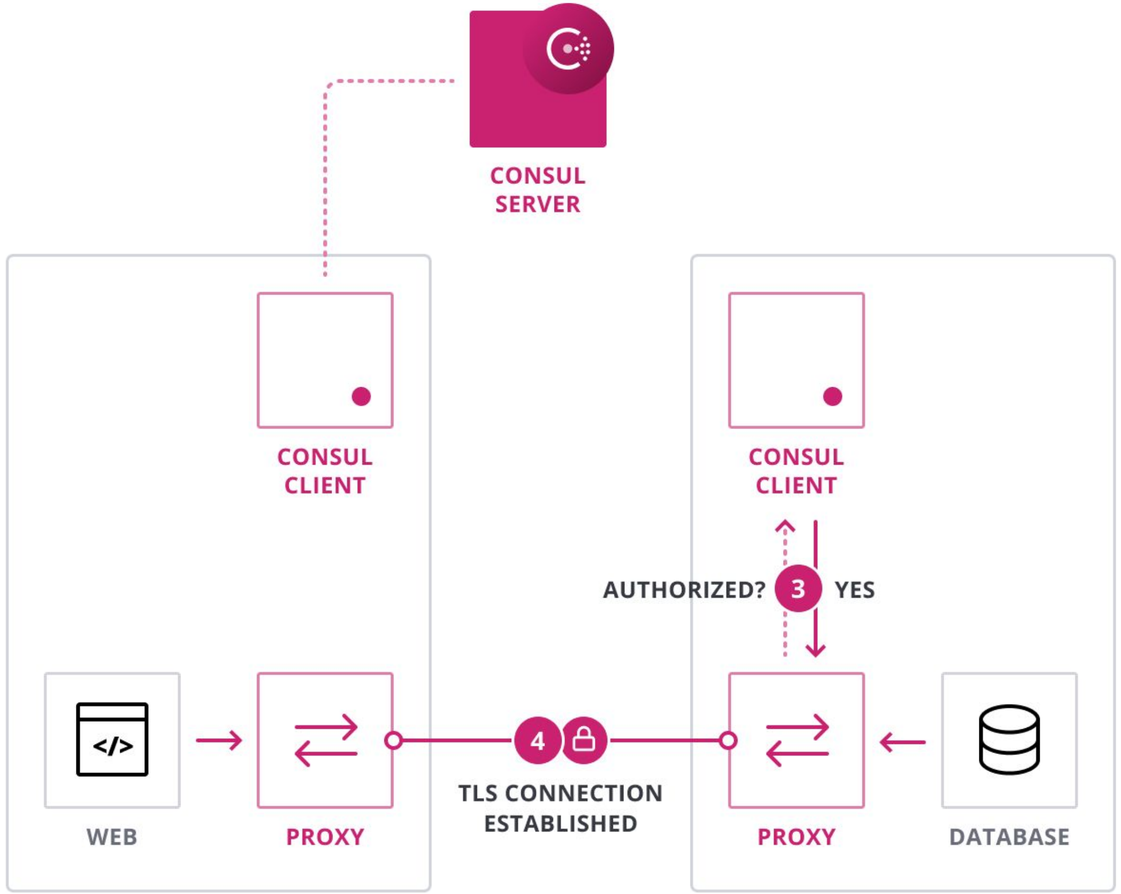
Sidecar Proxies



Sidecar Proxies



Sidecar Proxies



Extra Benefits

Mesh Gateways

Mesh Gateways

Multi-Cloud and -Cluster challenge

Single Kubernetes cluster

Most Service Meshes are build for a single cluster

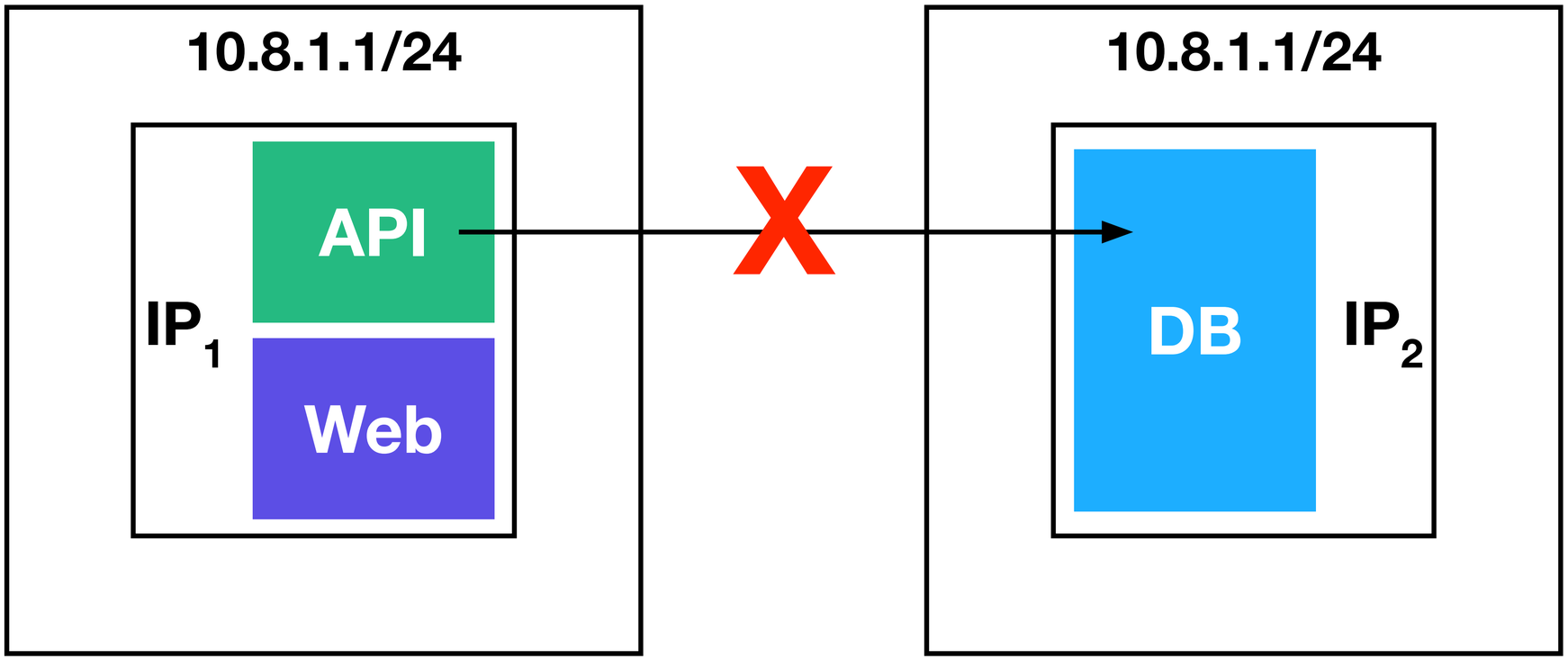
Multi-cluster Service Mesh

Connection multiple Service Meshes across different Kubernetes clusters not solved yet

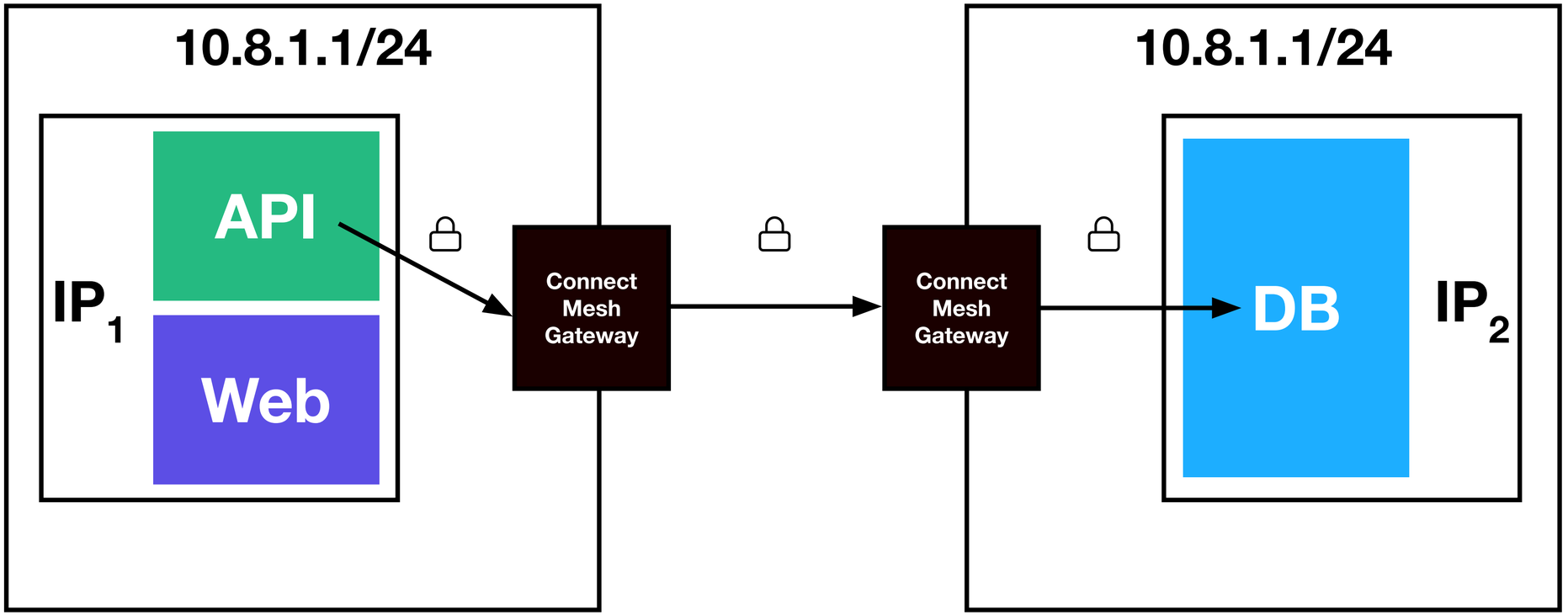
Service Mesh across clouds

Connection Services Meshes across different environments (Clouds, On-Prem, etc.) requires a lot of work

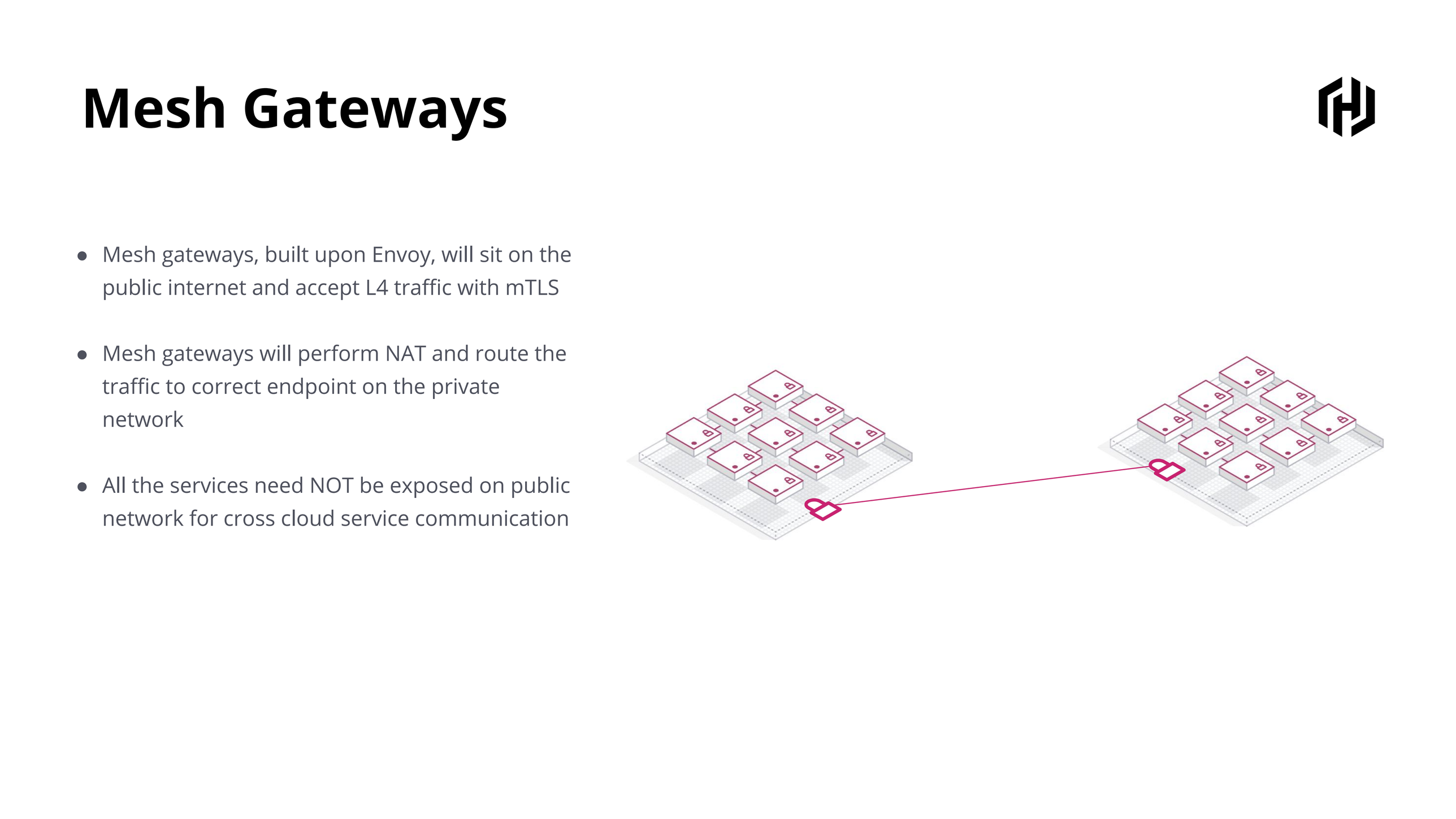
Mesh Gateways



Mesh Gateways



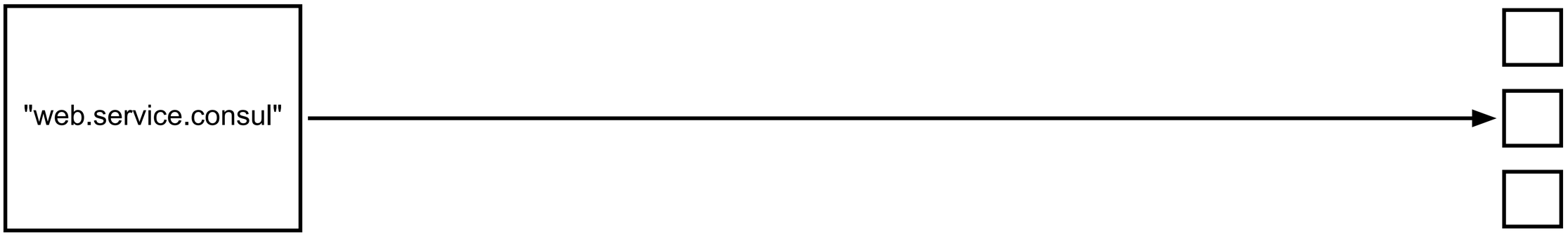
Mesh Gateways



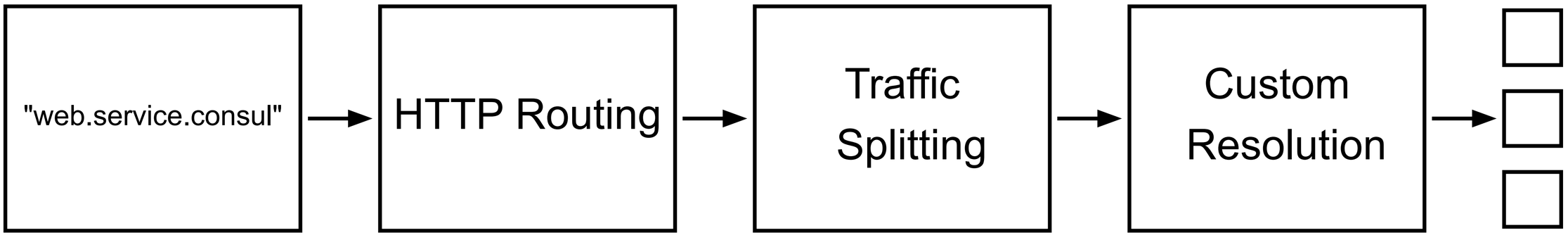
- Mesh gateways, built upon Envoy, will sit on the public internet and accept L4 traffic with mTLS
- Mesh gateways will perform NAT and route the traffic to correct endpoint on the private network
- All the services need NOT be exposed on public network for cross cloud service communication

L7 Traffic Management

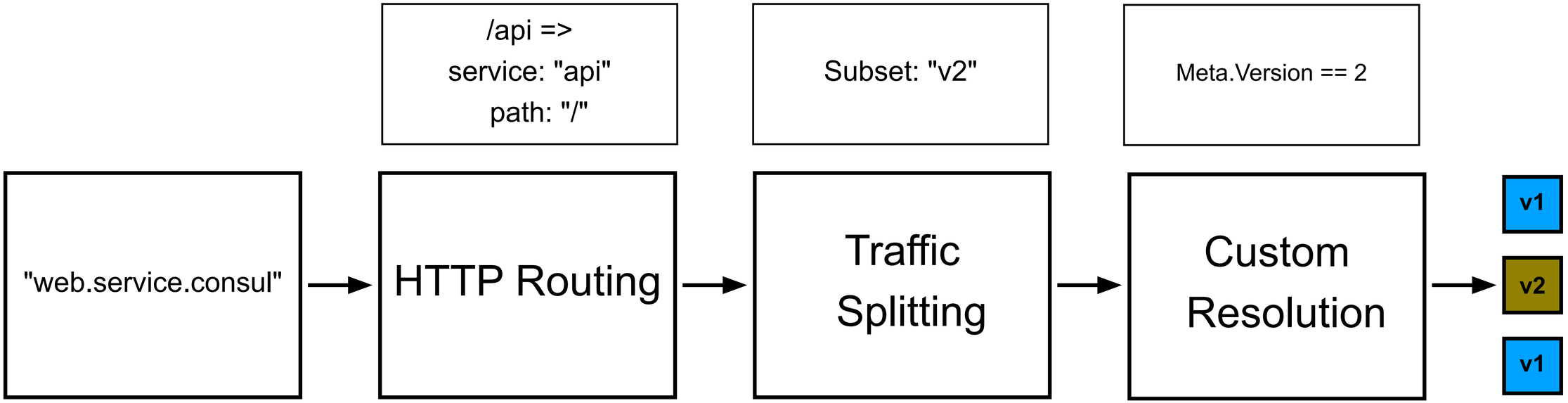
L4 Traffic



L7 Traffic Management



L7 Traffic Management



Secrets

Vault

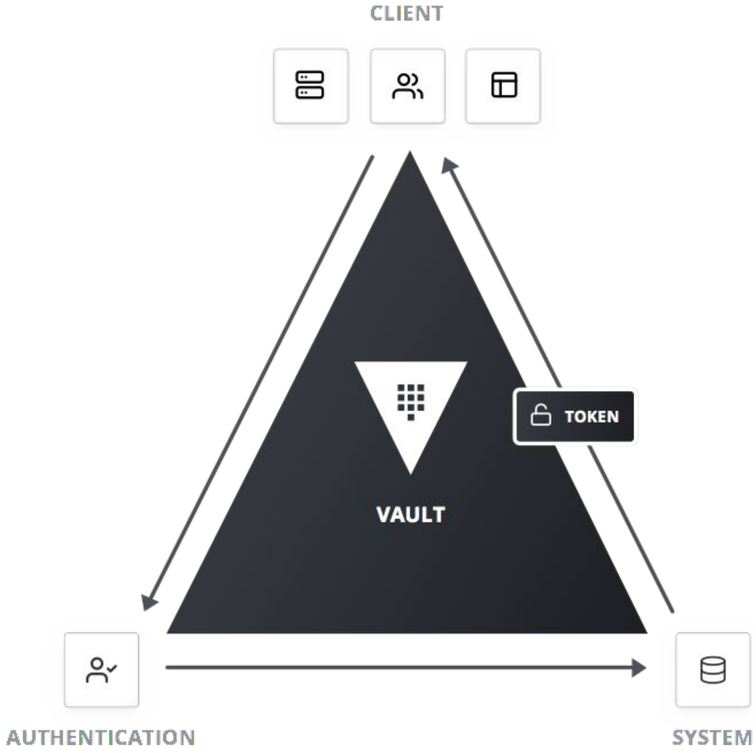
Provides the foundation for cloud security that leverages trusted sources of identity to keep secrets and application data secure in the cloud operating model

- **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

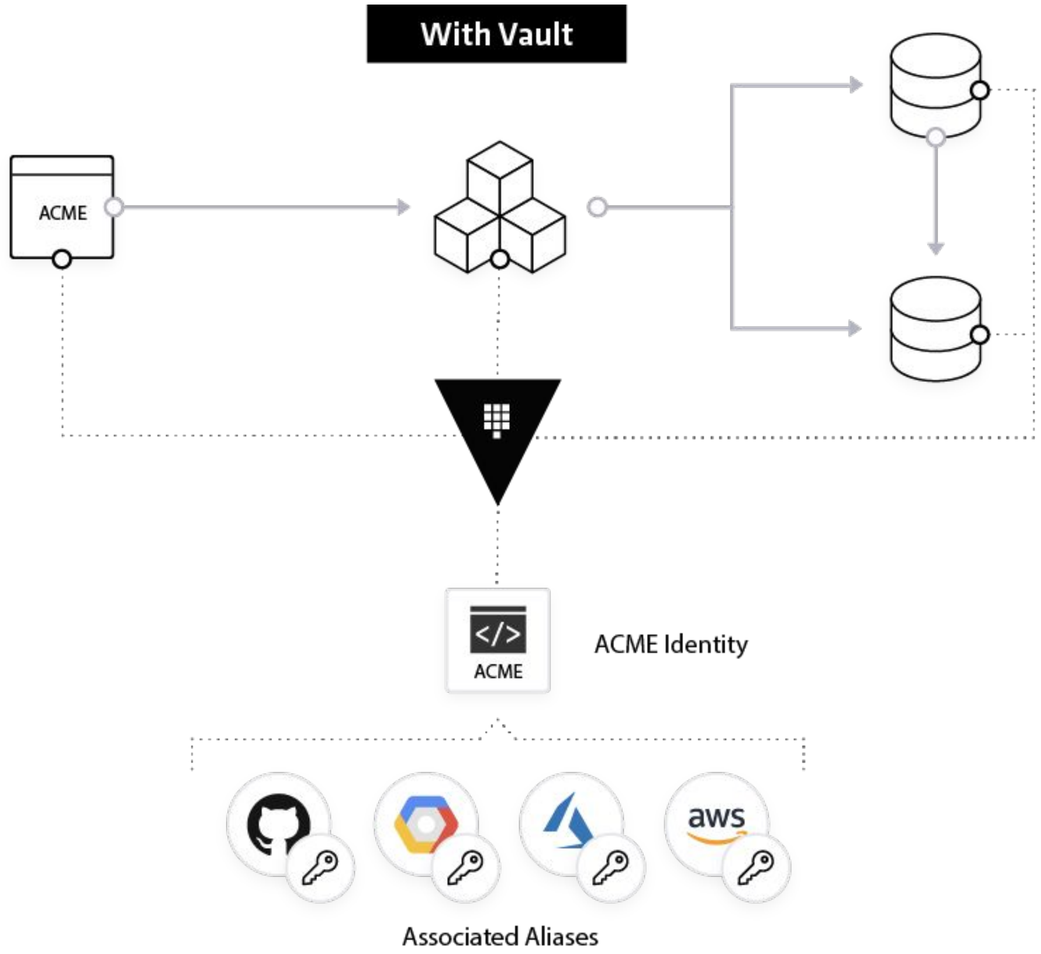
1M+
Monthly D/Ls

300+
Enterprise Customers



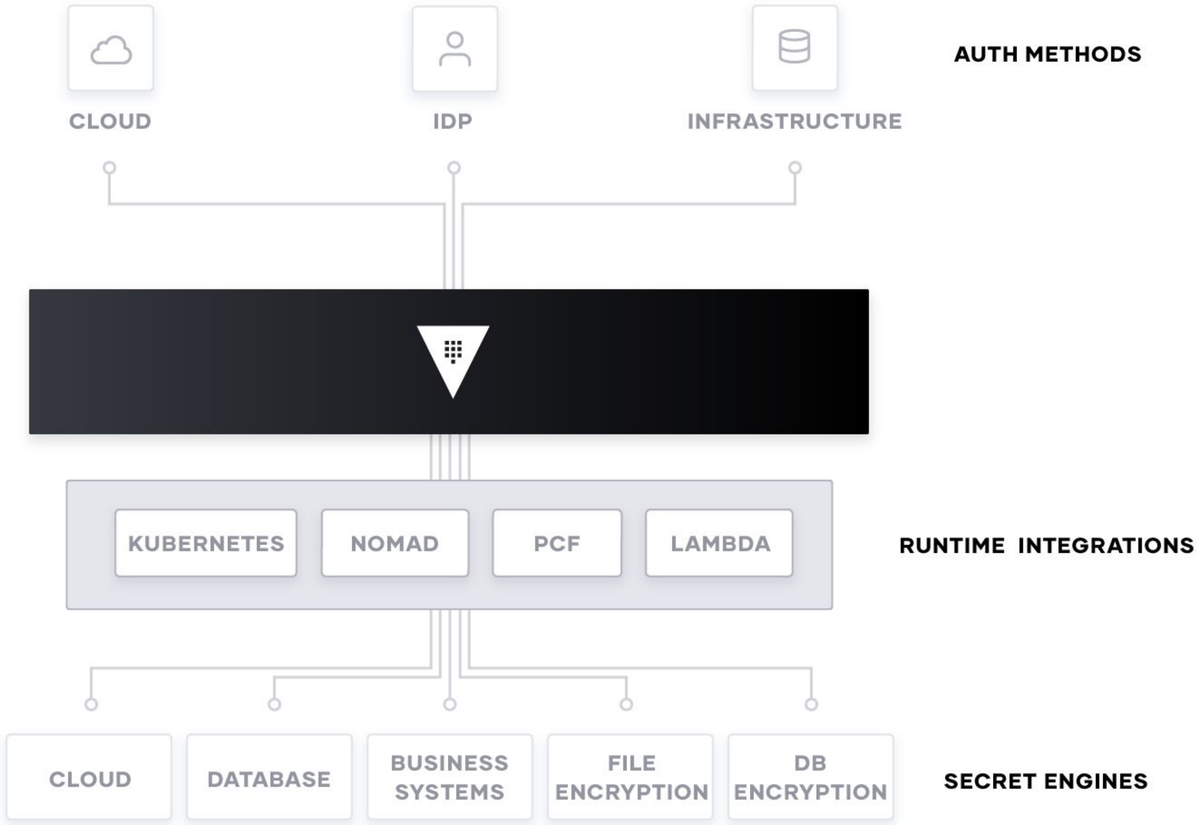
Guiding Principle: **Identity Brokering**

- Authenticate and access different clouds, systems, and endpoints using trusted identities
- Leverage multiple identities across different platforms with single policy enforcement
- Integrate trusted identities in the same application workflow to reduce operational overhead

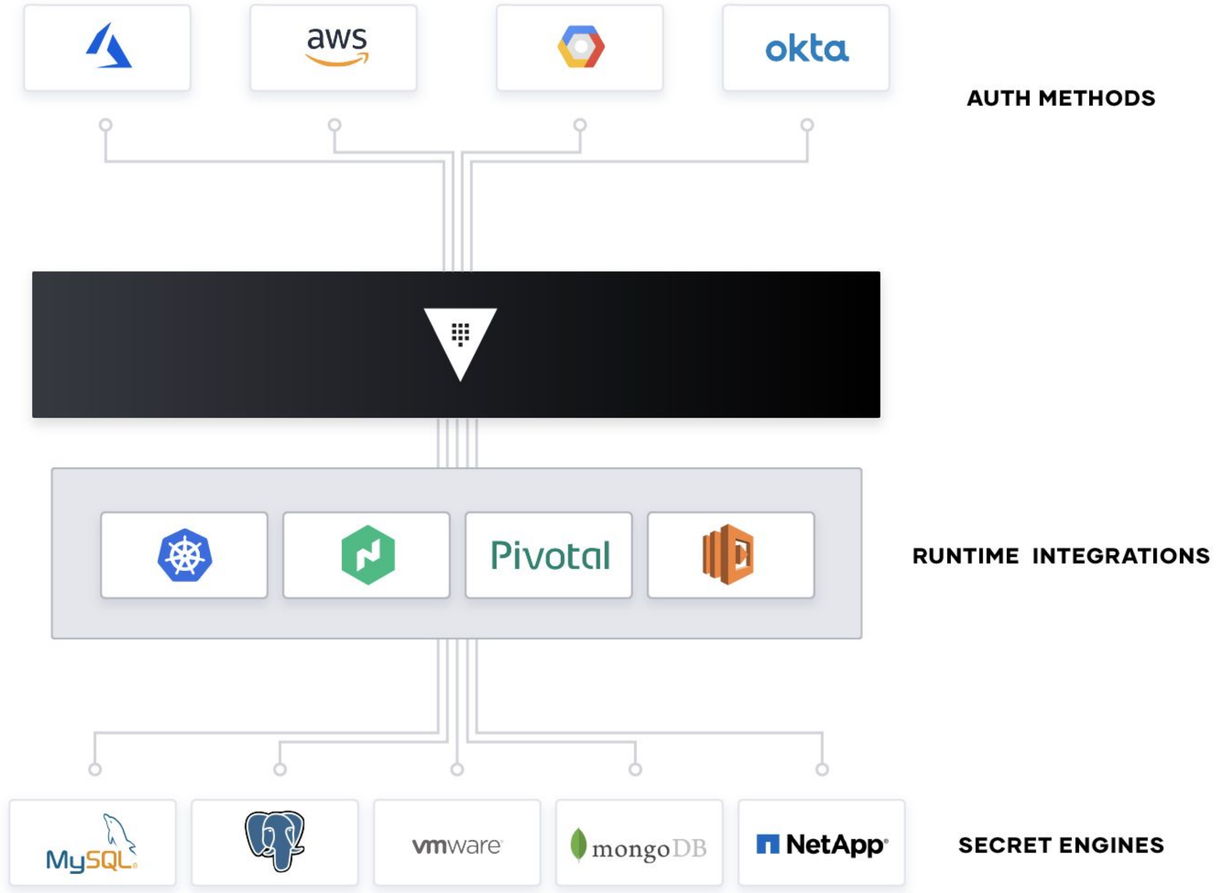


Single Control Plane for cloud security

- Automate, control, and secure infrastructure and applications through one API
- Unified support across heterogeneous environments
- Integrate with providers and technologies you're already using

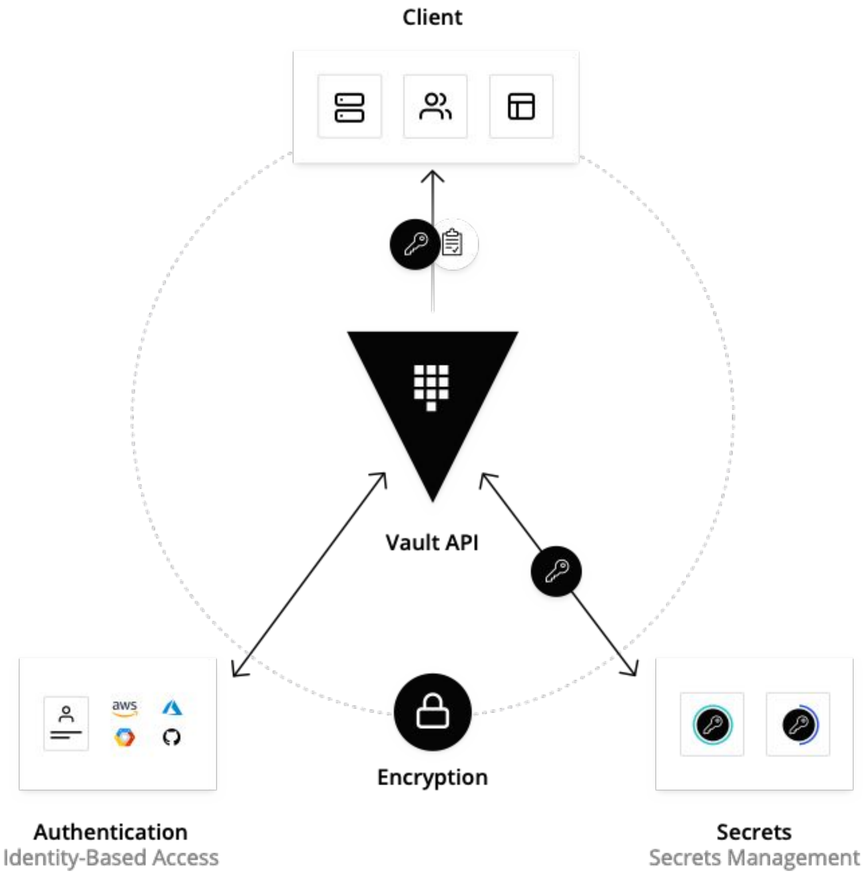


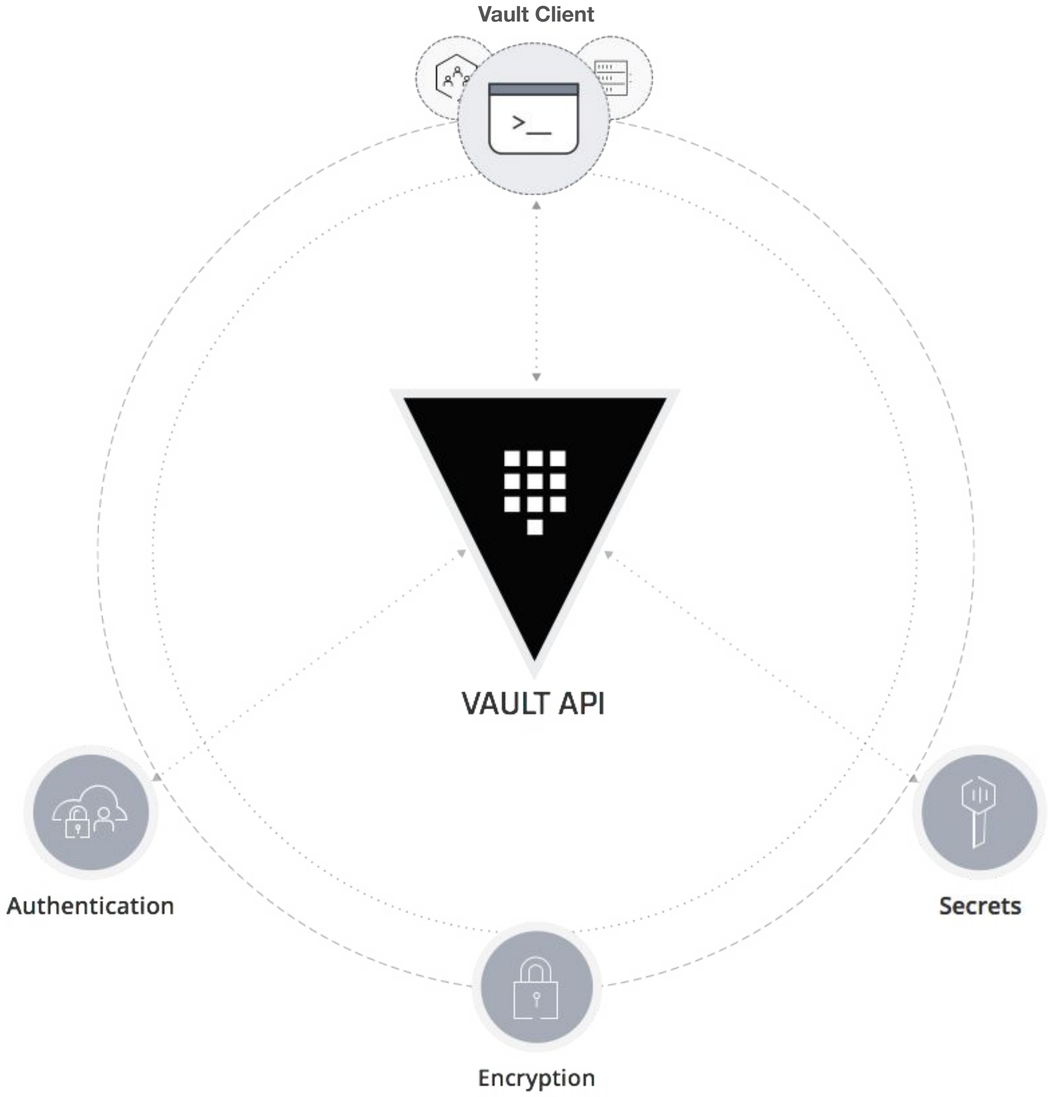
Broad Ecosystem Integration



How Vault Works

Vault tightly controls access to secrets and encryption keys by authenticating against trusted sources of identity such as Active Directory, LDAP, and cloud identity platforms. Vault enables fine grained authorization of which users and applications are permitted access to secrets and keys.

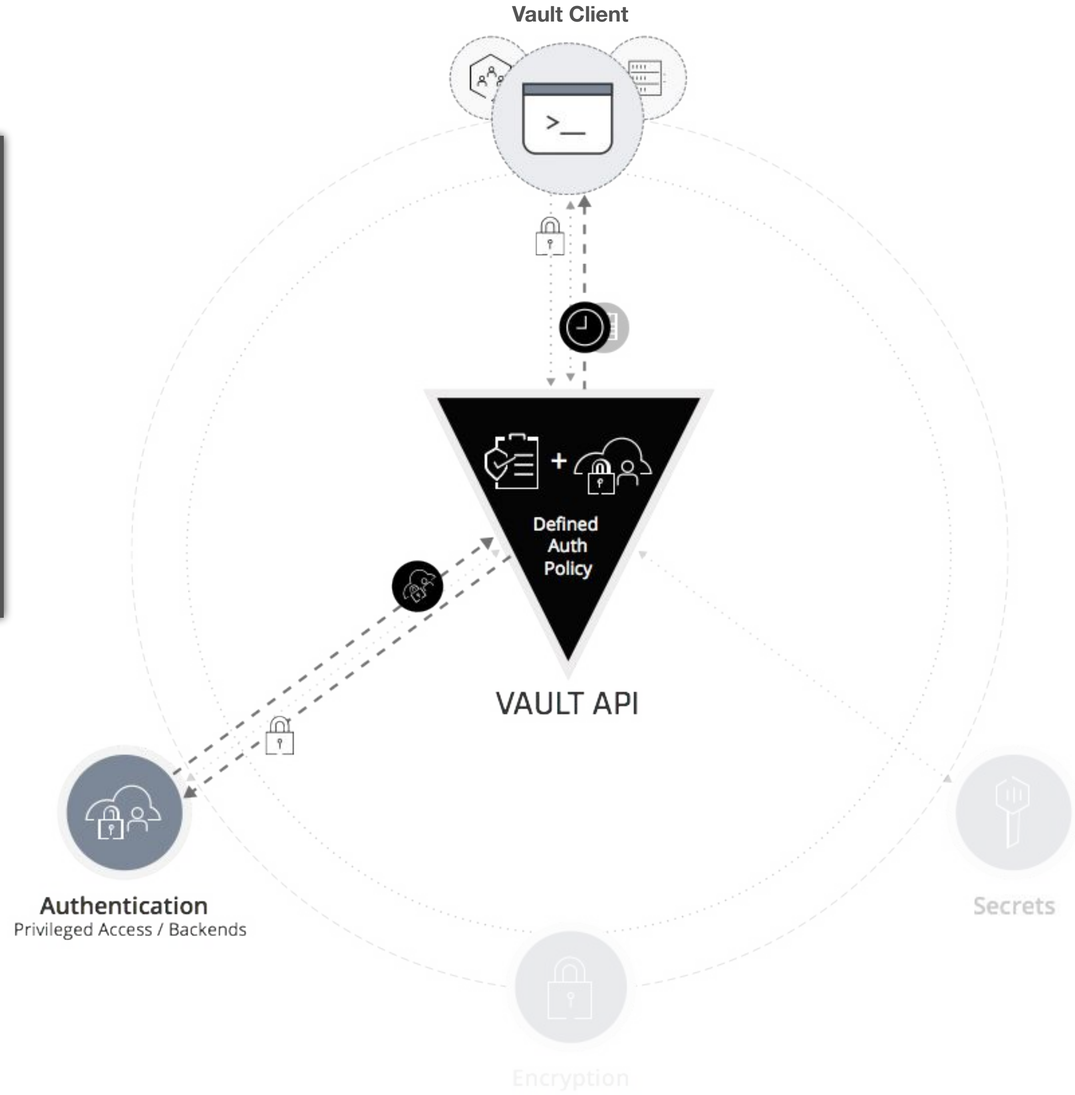



Vault Client
VAULT API
Authentication
Secrets
Encryption

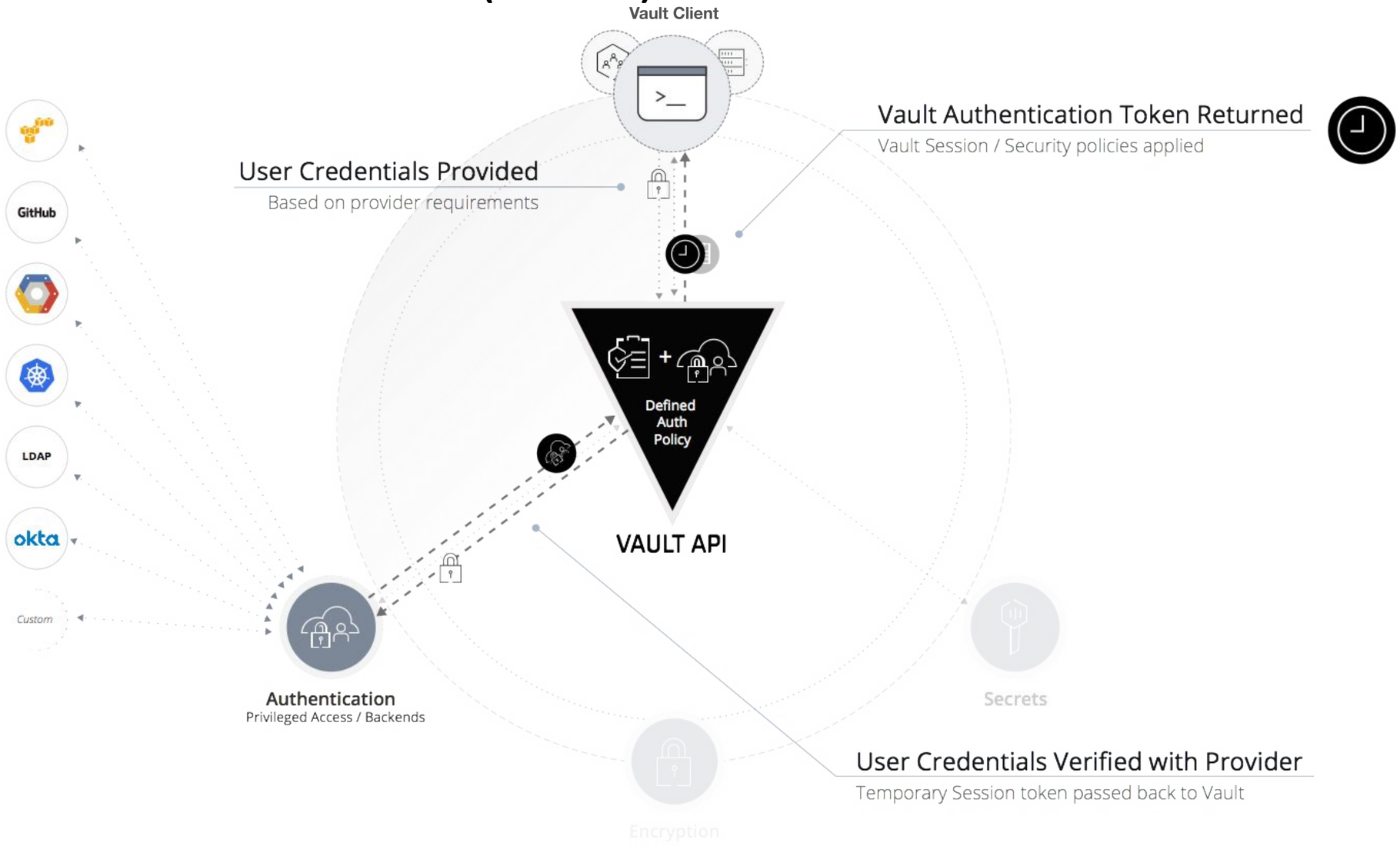
Authentication Workflow

Vault + Authenticating

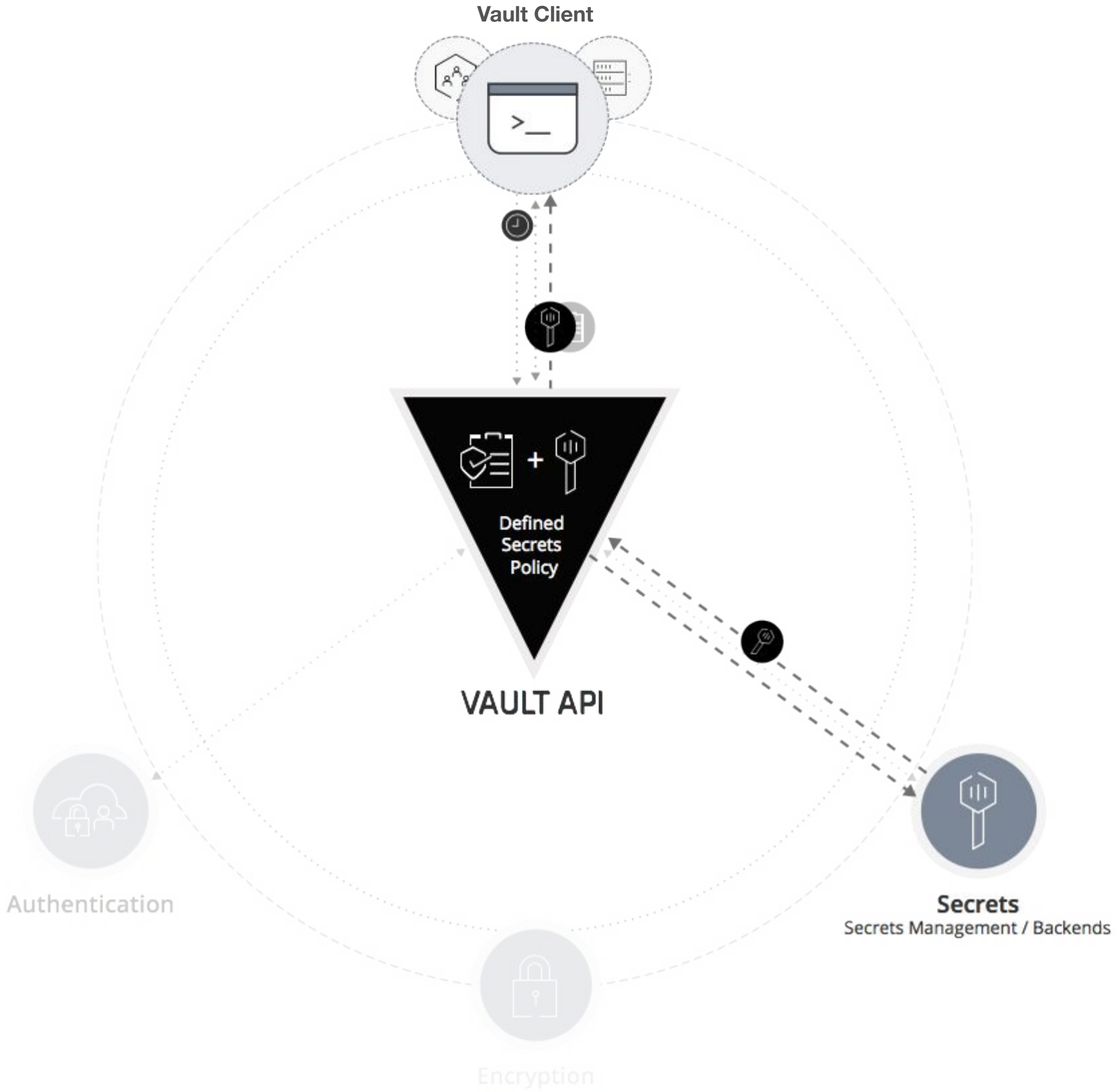
Before a client/user can interact with Vault, it must *authenticate* against an authentication backend. Once authenticated, a token is returned to the user/client with any defined and/or appropriate policies.



Authentication Workflow (detail)



Secrets Workflow

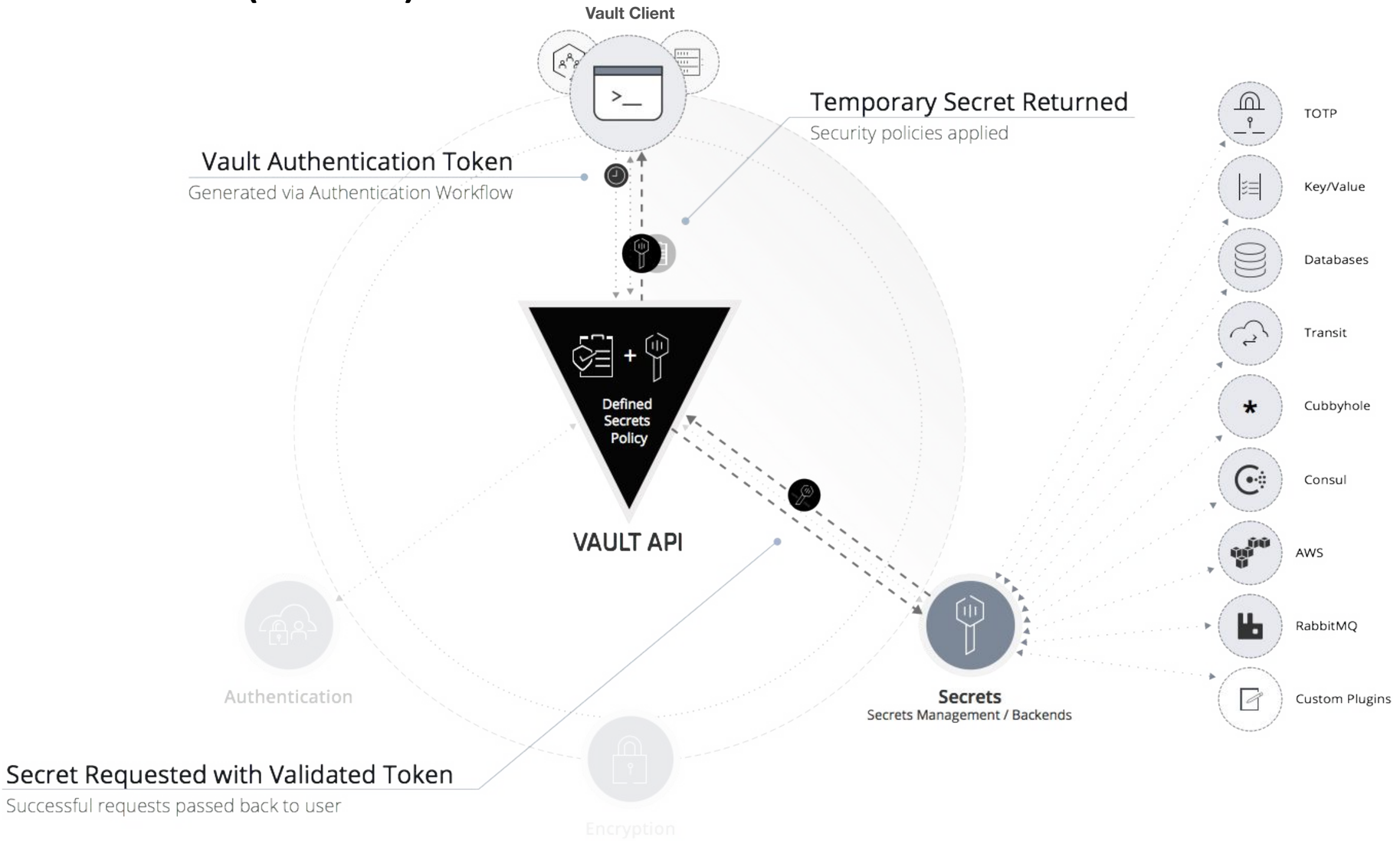


Vault + Secrets

Authentication Token Required

Secrets can be stored and generated. Some secrets can generated dynamically, while others are verbatim. Secrets are returned to the user/client with any defined and/or appropriate policies.

Secrets Workflow (detail)



Demos

Resources

Learn Vault

Vault - Helm Chart

Demo: Vault Helm Chart (youtube)

Learn Consul

Consul - Helm Chart

Demo: Consul Helm Chart (youtube)

Thank you

hello@hashicorp.com

www.hashicorp.com