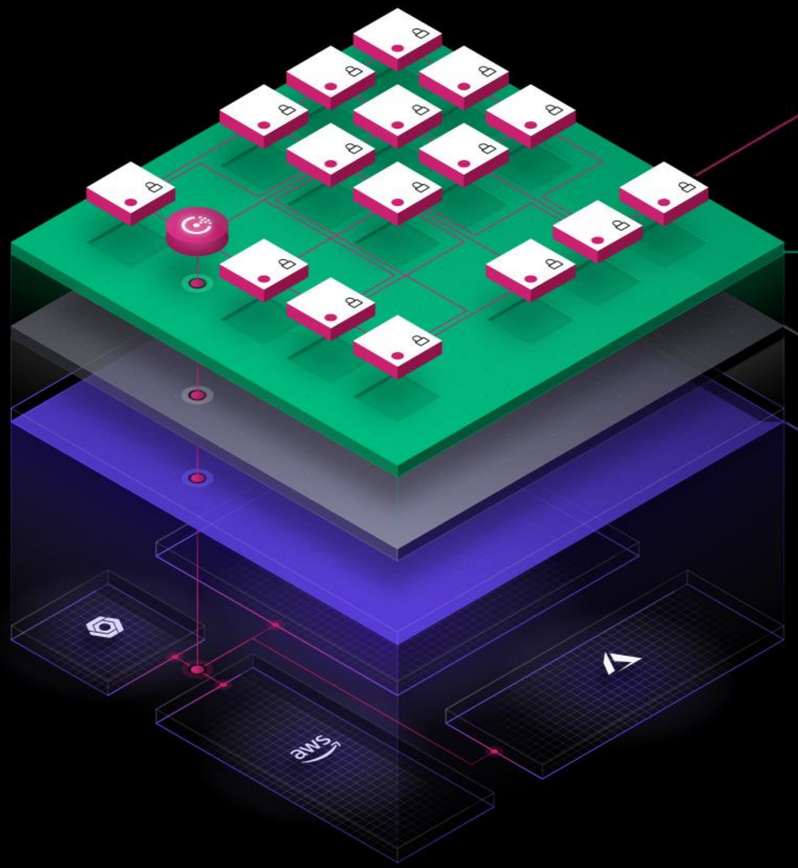
Manage secrets and protect sensitive data

Secure, store, and tightly control access to tokens, passwords, certificates, encryption keys for protecting sensitive data, and other secrets in dynamic infrastructure.

The 4 essential elements of distributed infrastructure



Connect

Infrastructure and applications

Development

Run applications

Security

Secure infrastructure and applications

Operations

Provision infrastructure

The 4 essential elements of distributed infrastructure

Connect

Infrastructure and applications

Development

Run applications

Security

Secure infrastructure and applications

Operations

Provision infrastructure

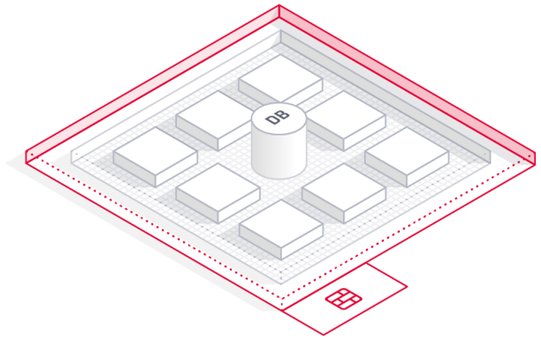
The shift **from static to dynamic networking**

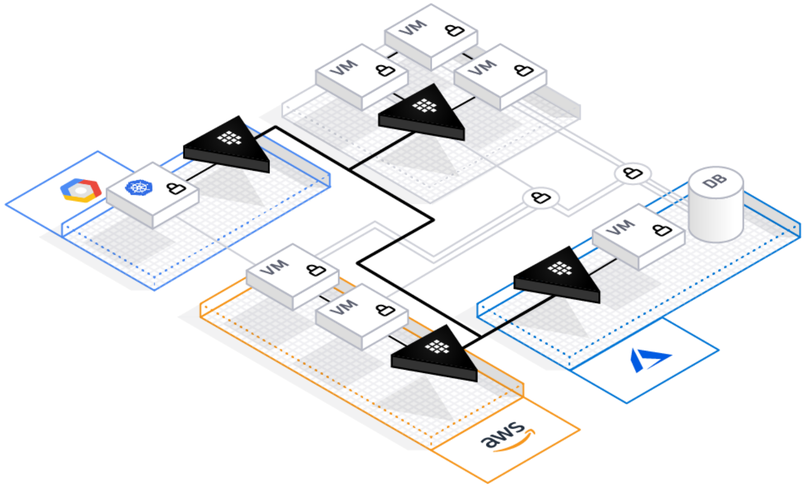
Static Infrastructure

Host-based identity

Dynamic Infrastructure

Service-based identity





The shift **from static to dynamic infrastructure**

Static Infrastructure

Host-based identity

Relies on high-trust networks with clear network perimeters.

Traditional Approach

- High trust networks
- A clear network perimeter
- Security enforced by **IP Address**

Dynamic Infrastructure

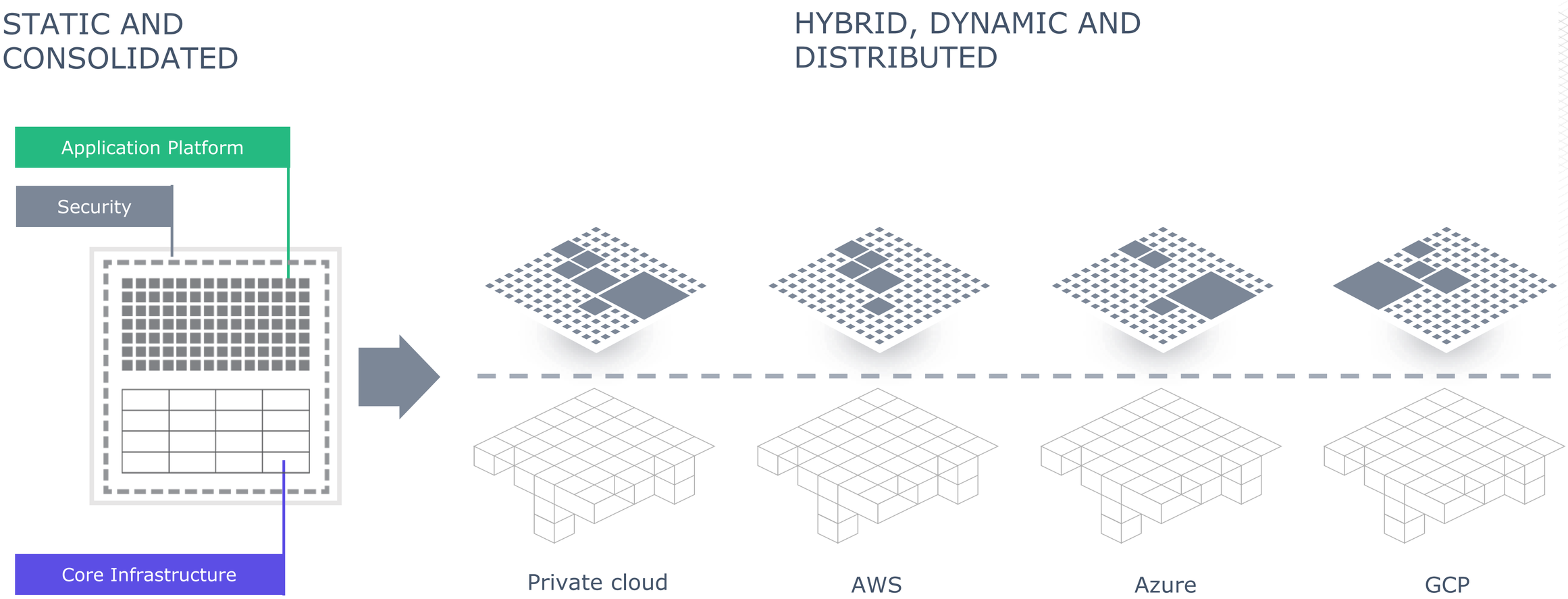
Service-based identity

Low-trust networks across multiple clouds without a clear network perimeter.

Vault Approach

- Low-trust networks in public clouds
- Unknown network perimeter across clouds
- Security enforced by **application identity**

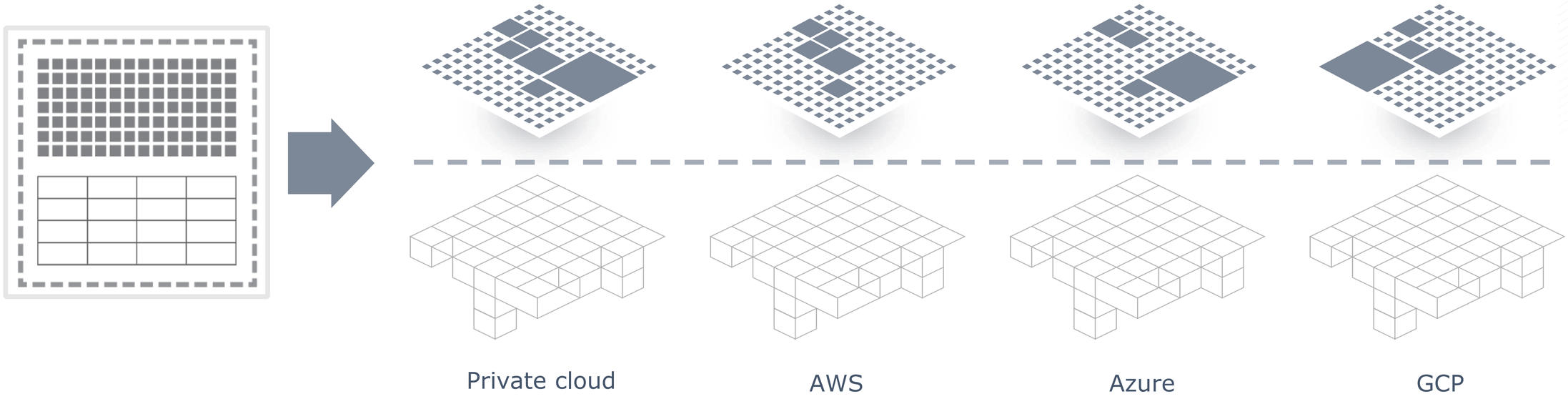
Security in a dynamic world



Security in a dynamic world

Perimeter-based security was sufficient for private datacenters

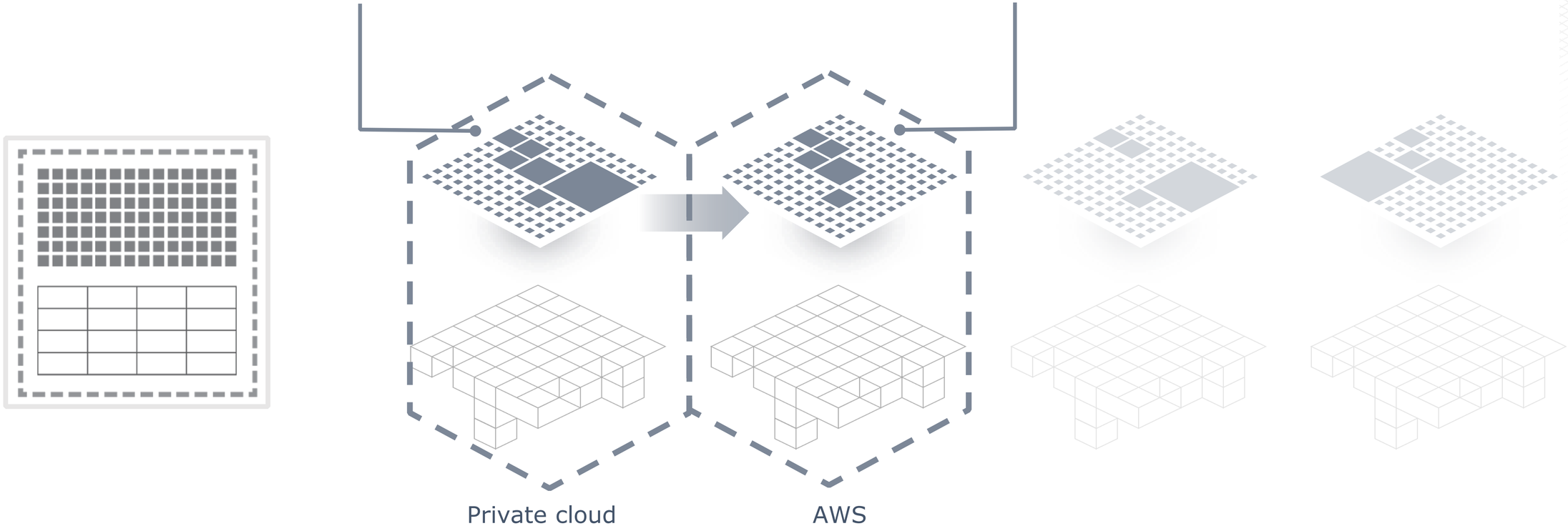
How does security extend across multiple data centers/clouds?



Secure infrastructure

Perimeter-based security pushes authorization to the network. Network security can be applied….

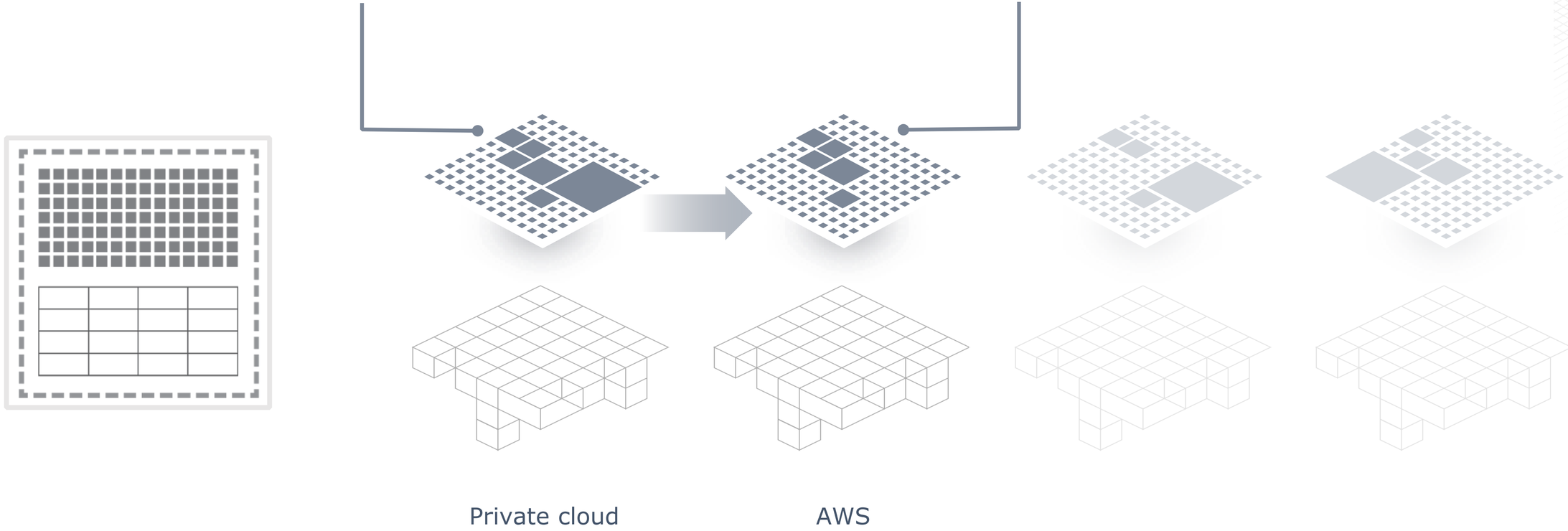
…But Without a fixed perimeter (four walls and single pipe), is my network trusted?



Secure infrastructure

Services, clouds, distributed applications all require secrets.

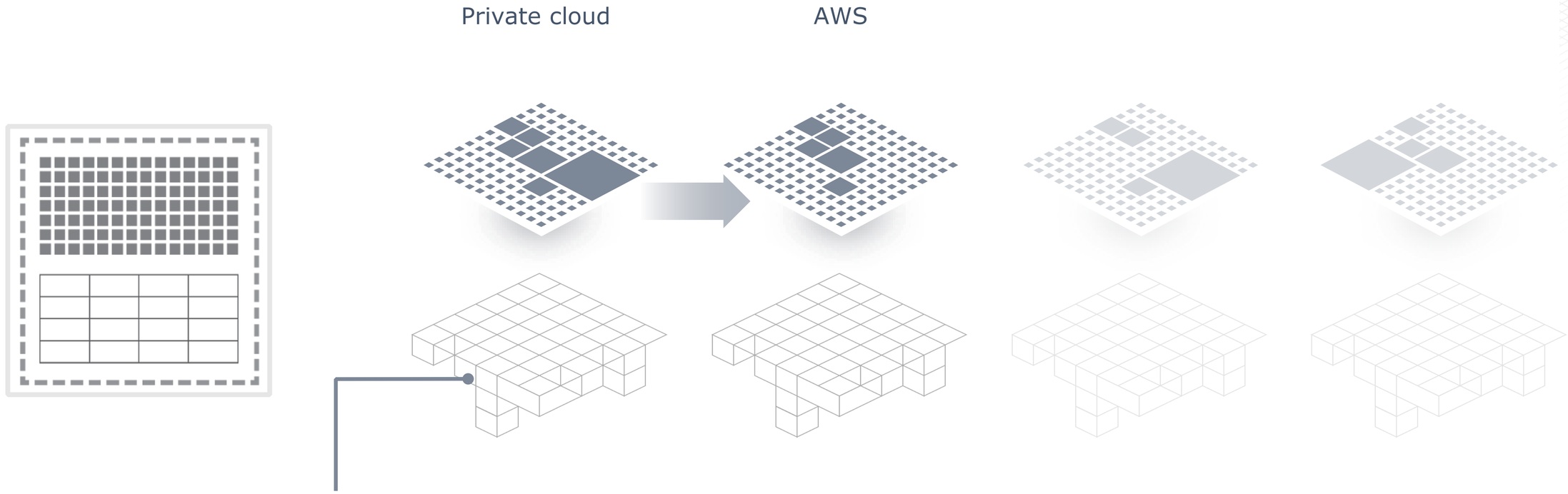
Where are secrets (credentials, tokens, keys) stored? Are they secure?



Private cloud

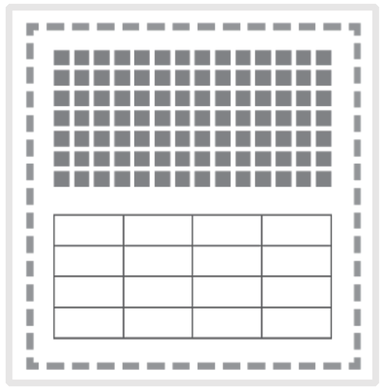
AWS

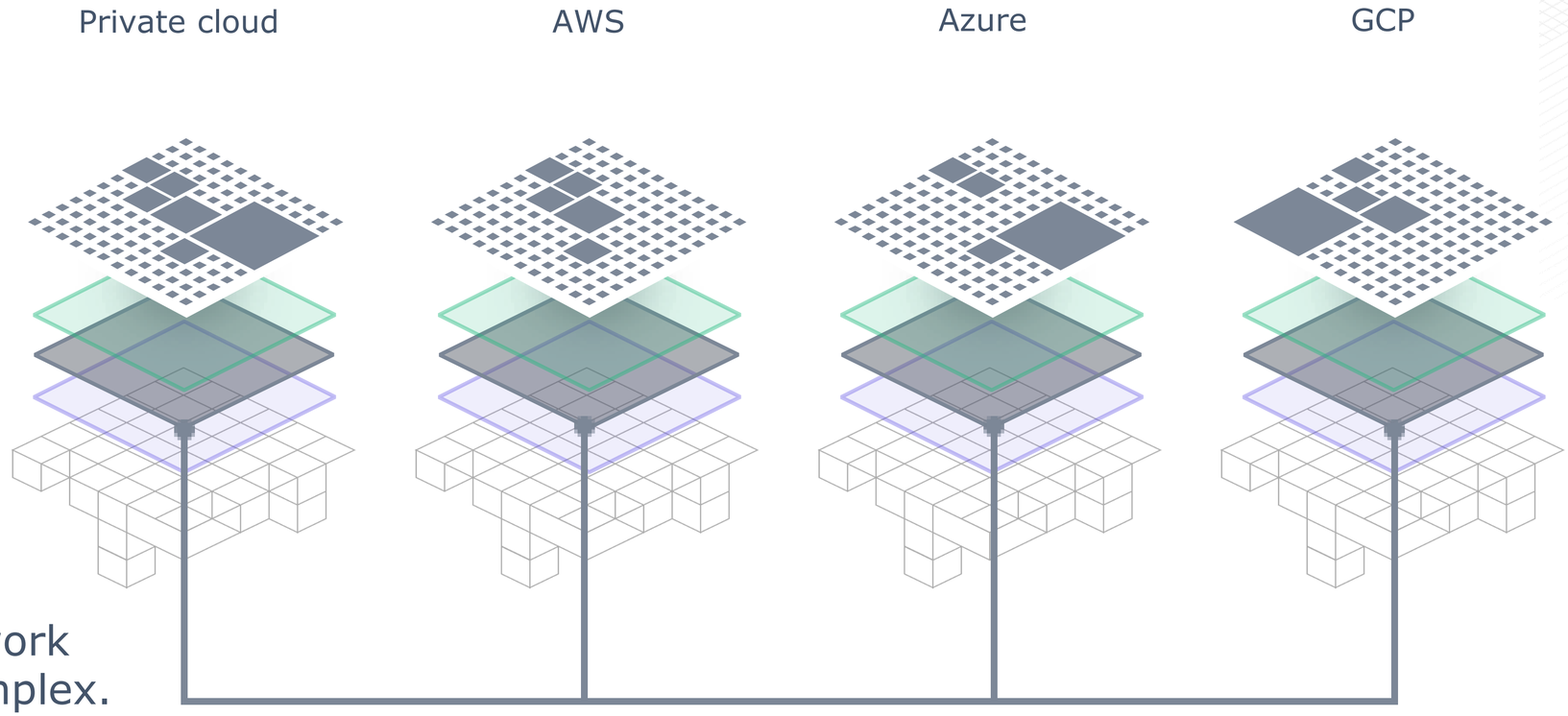
Secure infrastructure



If security is breached, how is data protected?

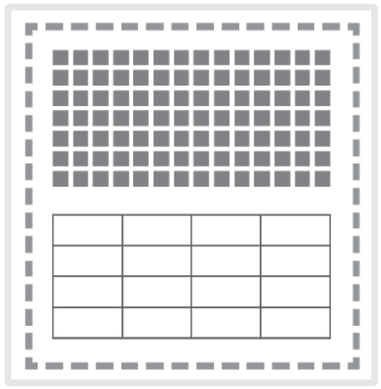
Secure infrastructure

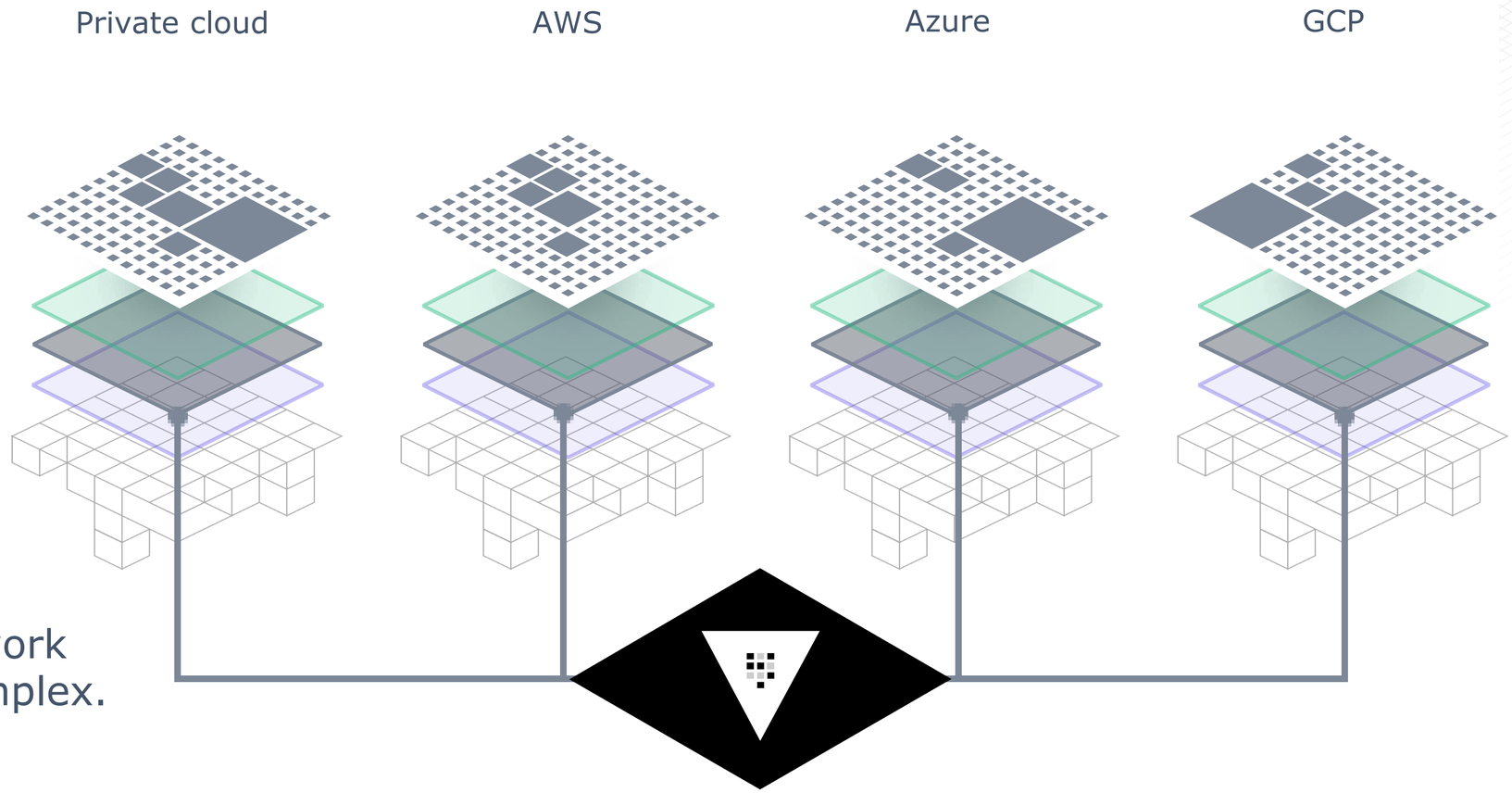




With each new cloud, network topologies become more complex.

Secure infrastructure





With each new cloud, network topologies become more complex.

Business Challenges

Increased risk of breach.

Secrets sprawled across different systems, files, and repositories.

Reduced productivity.

Inefficiencies with managing different systems to manage secrets, HSMs, and cryptographic operations across an organization and different teams

Increased risk of data exposure.

Multi-cloud creates a larger surface area to secure and encrypting data across hybrid environments with HSMs is painful and hard to use.

Business Value

Reduce risk of a breach.

Eliminate static, hard-coded credentials by centralizing secrets in Vault and tightly controlling access based on trusted identities.

Increase productivity and efficiency

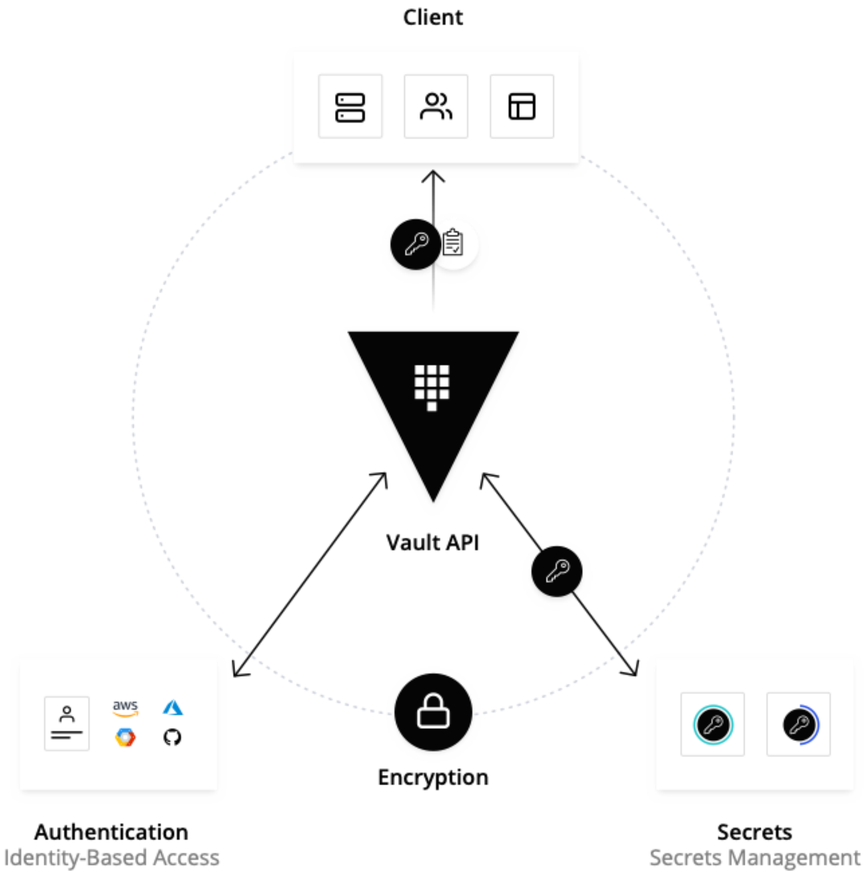
With one platform for secrets management and data encryption through a CLI, API, and GUI.

Reduce risk of data exposure

Encrypt sensitive data in transit and at rest using centrally managed and secured encryption keys in Vault, all through a single workflow and API.

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 Use Cases

Leverage any trusted source of identity to enforce access to systems, secrets, and applications.

Secrets Management

Centrally store, access, and distribute dynamic secrets.

Encrypting Application Data

Keep application data secure with centralized key management and simple APIs for data encryption.

Identity-based Access

Authenticate and access different clouds, systems, and endpoints using trusted identities.

1 2 3

Vault Principles

API Driven

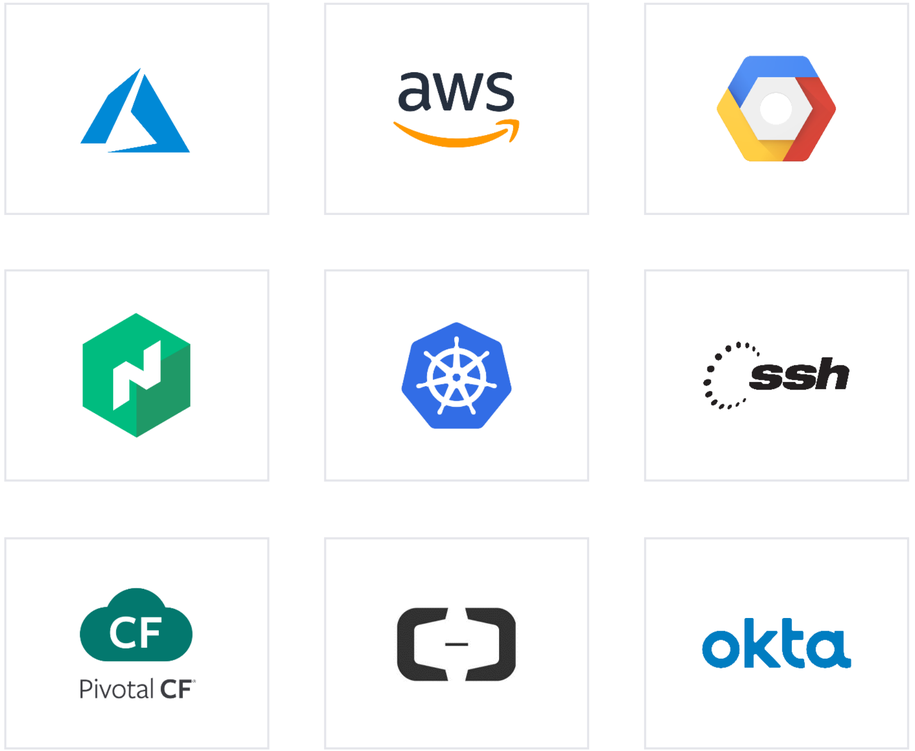
Use policy to codify, protect, and automate access to secrets.

```
$ curl \
    --header "X-Vault-Token: ..." \
    --request POST \
    --data @payload.json \
    https://127.0.0.1:8200/v1/secret/config
```


Vault Principles

Secure with any Identity

Leverage any trusted identity provider, such as cloud IAM platforms, Kubernetes, Active Directory, to authenticate into Vault.



Vault Principles

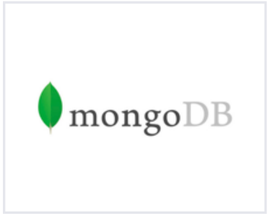
Extend and Integrate

Request secrets for any system through one consistent, audited, and secured workflow.







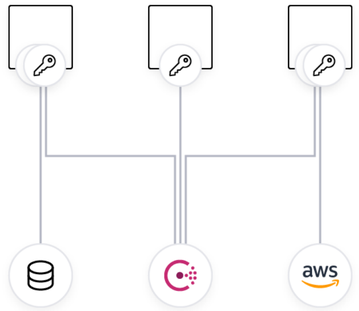


VAULT ADOPTION

Use Case
Secrets Management

Use Case: Secrets Management

Centrally store, access and distribute dynamic secrets across applications, systems, and infrastructure.



The Challenge

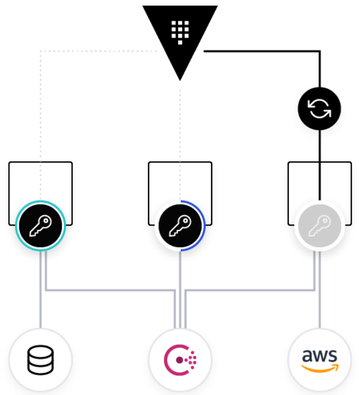
Secrets for applications and systems need to be centralized and static IP-based solutions don't scale in dynamic environments with frequently changing applications and machines.

BEFORE

- **Reduced productivity** from secret sprawl and configuration complexity
- **Increased cost** with redundant management and difficulty in adopting new systems
- **Increased risk** with more complexity, thereby increasing the threat surface and risking non-compliance with major regulatory laws and requirements

Use Case: Secrets Management

Centrally store, access and distribute dynamic secrets across applications, systems, and infrastructure.



The Solution

Vault centrally manages and enforces access to secrets and systems based on trusted sources of application and user identity.

AFTER

- **Increase productivity** & reduce time to deploy security workflows with centralized management
- **Control costs** with automated compliance and policy management, controls to support teams to self-manage their own environments
- **Reduce risk** with dynamic secrets, control groups, and other tools to allow Vault to conduct security operations while protecting sensitive information in flight and at rest.

Features

1 **Secret Storage**

Encrypt and store data in the storage backend of your choice.

2 **Dynamic Secrets**

Dynamic secrets are ephemeral, programmatically generated when they are accessed and do not exist until they are read, reducing risk of someone stealing them or another client using the same secrets. Dynamic secrets can be revoked immediately after use, minimizing the life of the secret.

3 **Namespaces**

ENTERPRISE

Provide secure multi-tenancy with isolated, self-managed environments.

4 **Secure Plugins**

Extend Vault with pluggable secret engines such as Consul, MySql, AWS, MongoDB, and more.

5 **Detailed Audit Logs**

Provide detailed history of client interaction — authentication, token creation, secret access & revocation. Logs can be used to detect security breaches, attempted access to systems, and guide policy enforcement

6 **Lease & Revoke Secrets**

Minimize the impact of secrets exposure by limiting how long credentials can live by creating time-based tokens for automatic or manual revocation and management.

Feature: **Secret Storage**

CHALLENGE SOLUTION RESULTS

Protecting Secrets and Access is Challenging

Deploying a cryptographic infrastructure to protect secrets in flight and at rest is challenging to deploy and maintain, increasing cost and reducing productivity.

Misconfigurations of this infrastructure can lead to exploitable security vulnerabilities, increasing risk.

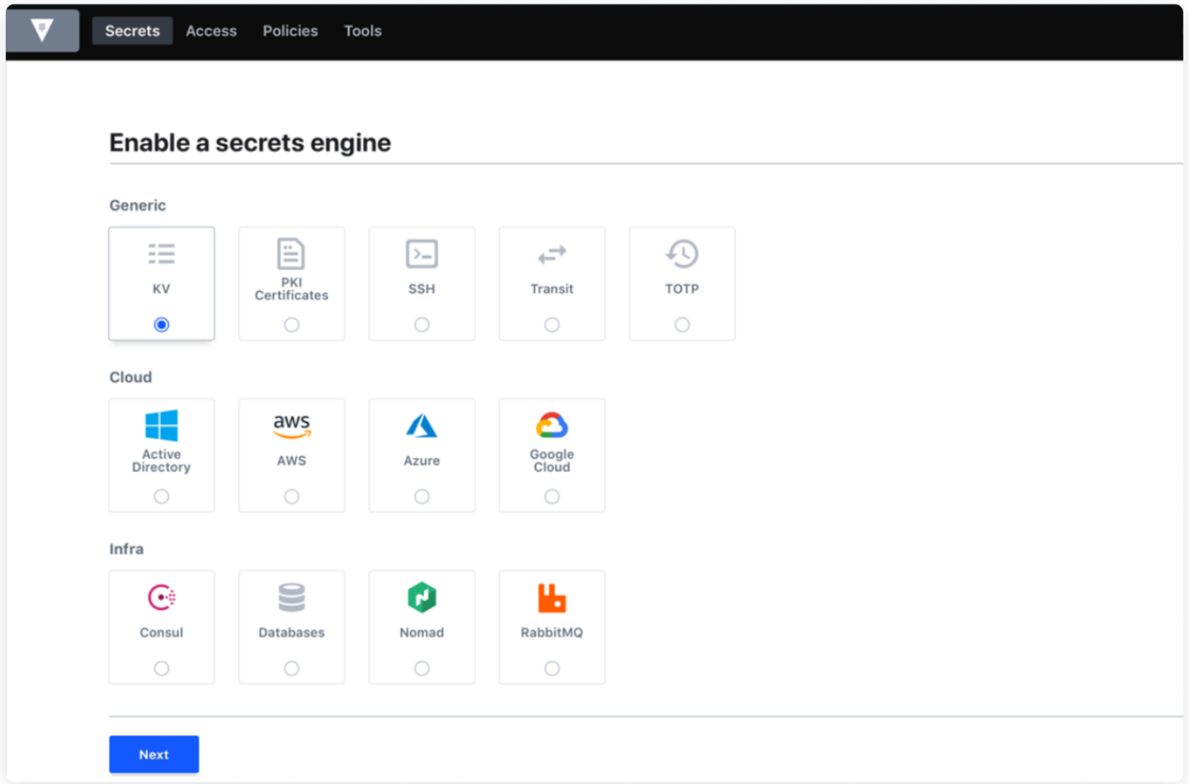
Feature: **Secret Storage**

CHALLENGE **SOLUTION** RESULTS

Vault Secrets Engines

Safely store credentials, keys, and other types of secrets without deploying and managing a complex key management infrastructure

- Store secrets with the K/V Secret Engine to quickly store and retrieve sensitive information
- Orchestrate workflows with stored secrets for creating dynamic credentials (AWS), certifying transactions (SSH), or privileged access management (Active Directory)
- Manage access with ACL policies and audit all transactions via the Audit Log.
- All data is automatically in flight (TLS) and at rest (AES 256 GCM)



Feature: **Secret Storage**

Increase Agility

Quickly deploy security workflows for new applications and cloud environments without having to manage complex key management infrastructure.

Reduce Risks

By not having to deploy and configure cryptographic protections, reduce the risk of accidentally introducing vulnerabilities.

Reduce Cost

Reduced complexity of deploying and managing secrets reduces management overhead.

Empower users to manage and mount their own secret engines reduces the cost of scaling.

Feature: **Dynamic Secrets**

CHALLENGE SOLUTION RESULTS

Secret Sprawl

Secrets in plaintext may accidentally be left in an application or with an individual long after the intended period of access.

Feature: **Dynamic Secrets**

CHALLENGE | **SOLUTION** | RESULTS

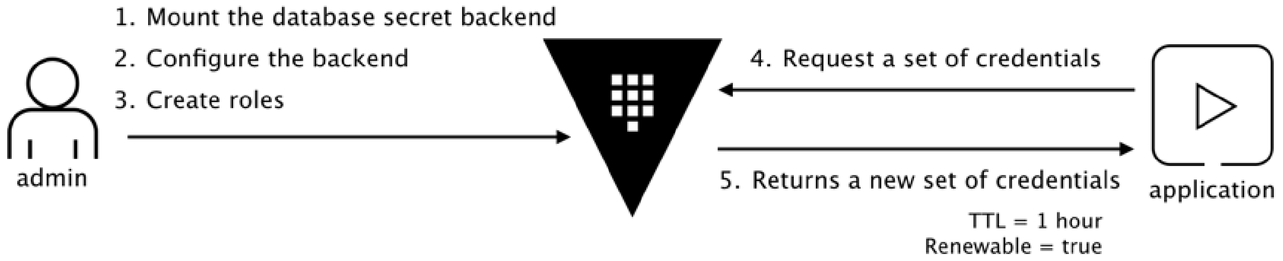
Dynamic Secrets

Vault grants tokens for access, not credentials, to ensure least privilege with security and ensure break glass functionality

- Set expiry to ensure that access is automatically revoked on time
- Revoke outstanding access at will
- Break glass functionality to halt all access in critical situations

ENTERPRISE

- Further control access to secrets with Sentinel policies



Feature: **Dynamic Secrets**

CHALLENGE SOLUTION **RESULTS**

Increase Agility

Dynamic secrets allow users and applications to quickly and safely stored secrets within Vault

Reduce Risk

Break glass procedures and revocation procedures allow for Vault admins to take ex post facto action in the case of security events

Reduce Cost

With established ACL policies, automate management of dynamic secrets and minimize the costs of implementing Least Privilege

Feature: **Namespaces**

CHALLENGE SOLUTION RESULTS

Secure Multi-Tenancy

Allowing a team to manage their own isolated installation of Vault may run at odds in enabling centralized management, complicate ability to scale

Feature: **Namespaces**

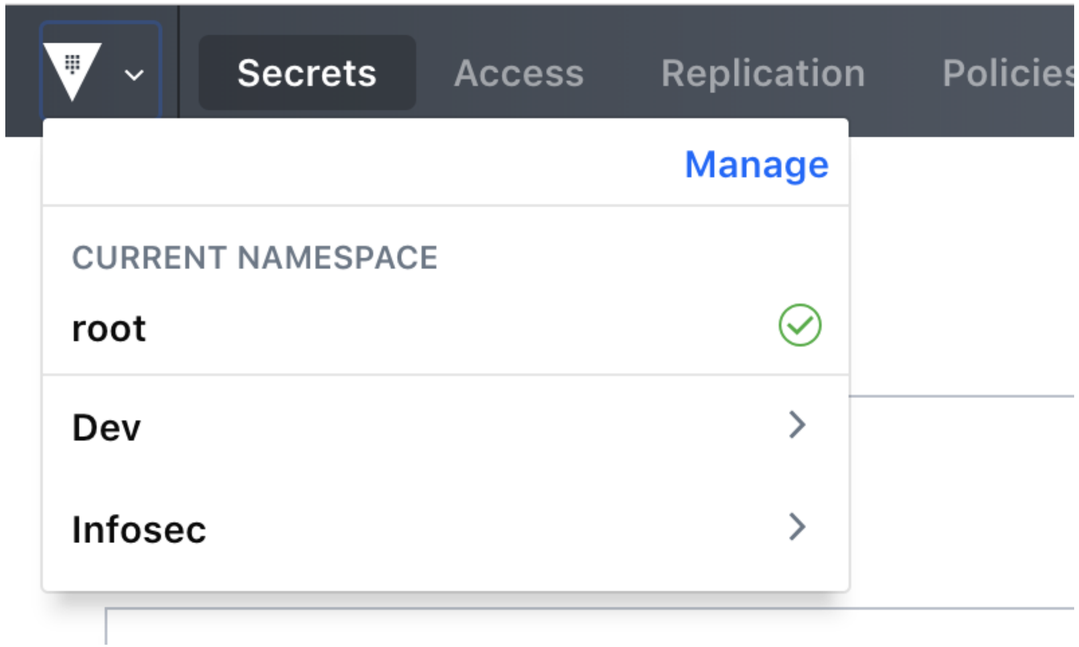
CHALLENGE **SOLUTION** RESULTS

Namespaces for Management, Secure Multi Tenancy

Create isolated “Vaults within a Vault” that allow for parent admins to manage configurations but permit teams to manage their own policies, secrets, and identities.

ENTERPRISE

- Allow teams to self-manage segmented Vault environments with their own auth methods, secret engines, and policy and identity infrastructures
- Isolate tenant environments for security, compliance
- Enforce organizational compliance across isolated teams



Feature: **Namespaces**

Increase Agility

Teams can self-manage their own isolated Vault environments within guard rails set by Vault admins

Reduce Risk

Tenants within Namespaces exist in isolated environments to ensure secure multi-tenancy and remove their ability to compromise their parent Vault environment

Reduce Cost

By empowering teams to self-manage their own policies and environments, Vault admins dramatically minimize the management cost of scaling their Vault environment across an organization

Feature: **Secure Plugins**

CHALLENGE SOLUTION RESULTS

Securing secrets for a constantly growing, changing infrastructure is incredibly challenging

As your infrastructure grows and changes, protecting sensitive information for new applications and environments can be a complex and expensive exercise

Feature: **Secure Plugins**

CHALLENGE | **SOLUTION** | RESULTS

Secure plugins allow for flexibly adding and customizing application integrations

Whether you are adding a new application or customizing an existing implementation, secure plugins allow for flexibility in adding and managing Vault's integration with third party systems

- Leverage the community to integrate an ecosystem of auth methods, secret engines, and storage backends
- Customize existing to support individualized integrations

```
$ vault write sys/plugins/catalog/myplugin-database-plugin \
    sha256=<expected SHA256 Hex value of the plugin binary> \
    command="myplugin"
Success! Data written to: sys/plugins/catalog/myplugin-database-plugin
```

Feature: **Secure Plugins**

CHALLENGE

SOLUTION


RESULTS

Increase Agility

With thousands of plugins under active development in the community, Vault users and admins can quickly adopt integrations for applications, identity management systems, and environments that are not natively supported by Vault

Reduce Risk

Secure plugins contains guard rails to protect against a plugin adversely impacting your system through misconfiguration

Reduce Cost

By leveraging the power of Vault's active community, integrations for applications, third party authentication systems, and other systems integrations can be achieved with minimal or no development effort

Feature: **Audit Logs**

CHALLENGE SOLUTION RESULTS

Security activity across clouds can be difficult to track

Multi-cloud and hybrid cloud security secrets management
can be difficult to track on one platform

Feature: **Audit Logs**

CHALLENGE **SOLUTION** RESULTS

Monitor events for security and compliance across infrastructures

With Vault's audit log, monitoring secret access across multiple clouds and environments is easy and automated

- Push audit logs to syslog, file, or socket for easy consumption by SIEM or log management software
- One schema for all cloud environments and applications


```
  "time": "2018-02-01T14:40:03.226772711Z",
  "type": "response",
  "auth": {
      "client_token": "hmac-
ıa256:09b0c08f04bc69bf10a0b8c1d2fa3d84ad4efc470d4f3125950cb5979e606843",
      "accessor": "hmac-
ıa256:34d5c7474ecac552772fbe091aee99dfc60b6461d42504a117b09928552cfad8",
      "display_name": "root",
      "policies": [
          "root"
      ],
      "metadata": null,
      "entity_id": ""
  },
  "request": {
      "id": "1af553d4-f2a8-4fac-66ec-b333b392011a",
      "operation": "create",
      "client_token": "hmac-
ıa256:09b0c08f04bc69bf10a0b8c1d2fa3d84ad4efc470d4f3125950cb5979e606843",
      "client_token_accessor": "hmac-
ıa256:34d5c7474ecac552772fbe091aee99dfc60b6461d42504a117b09928552cfad8",
      "path": "secret/audittest",
      "data": {
          "value": "hmac-
ıa256:f0dbb2e3574400553d45f259391f17a2c09e7845deb310faf3151ea2527e6c51"
      },
      "policy_override": false,
      "remote_address": "172.28.128.6",
      "wrap_ttl": 0,
      "headers": {}
  },
  "response": {},
  "error": ""
```

Feature: **Audit Logs**

CHALLENGE

SOLUTION


RESULTS

Increase Agility

Track secret access and security events across applications and clouds automatically

Reduce Risk

With support for most SIEM suites, Vault's audit logs can be used as part of a comprehensive solution to monitor an infrastructure for intrusion

Reduce Cost

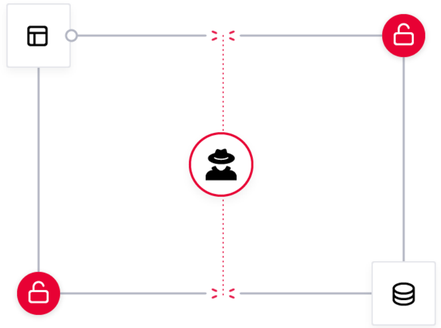
Vault's audit logs work with your existing SIEM/log management suite and are quick and easy to set up - minimizing costs to deploy and maintain

VAULT ADOPTION

Use Case
Data Encryption

Use Case: **Data Protection**

Protect sensitive data with centralized key management and simple APIs for data encryption.



The Challenge

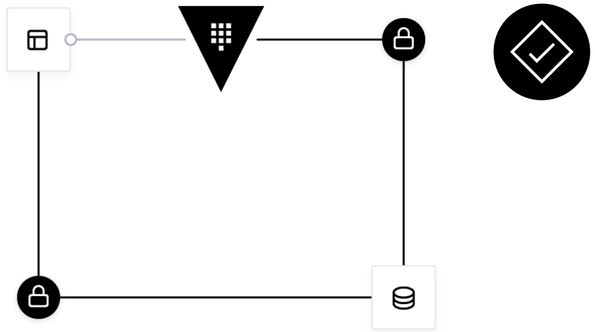
All application data should be encrypted, but deploying cryptography and key management infrastructure is expensive, hard to develop against, and not cloud or multi-datacenter friendly.

BEFORE

- **Increased costs** around HSMs and support
- **Reduced productivity** with multiple workflows/APIs to learn cryptographic standards across an organization and different projects and restricted access to HSMs
- **Increased risk** with multiple attack surfaces to intercept and steal sensitive data

Use Case: **Data Protection**

Protect sensitive data with centralized key management and simple APIs for data encryption.



The Solution

Vault provides encryption as a service with centralized key management to simplify encrypting data in transit and at rest across clouds and datacenters.

AFTER

- **Reduce costs** around expensive HSMs and licensing
- **Increase productivity** and revenue with a consistent workflow and cryptographic standards across an organization
- **Reduce risk of data exposure** by encrypting sensitive data in transit and at rest using centrally managed and secured encryption keys in Vault, all through a single workflow and API

Features

1 API-driven Encryption

Encrypt and decrypt application data with an HTTP (TLS) API call. Key management, encryption algorithm, and more are offloaded and centrally managed by Vault.

2 Encryption Key Rolling

Update and roll new keys throughout distributed infrastructure while retaining the ability to decrypt encrypted data.

3 FIPS 140-2 & Cryptographic Compliance

ENTERPRISE

Use FIPS 140-2-certified HSMs to ensure that Critical Security Parameters are protected in a compliant fashion.

4 Replication Filters

ENTERPRISE

Selectively Whitelist/Blacklist and activate or deactivate mounts for Secret Mounts for replication filtering to protect against the distribution of secrets and key material to certain geographies or regions.

Feature: **API-Driven Encryption**

CHALLENGE SOLUTION RESULTS

Cryptography is hard to deploy and manage

To encrypt/decrypt data, users must traditionally deploy and manage a complex key management infrastructure

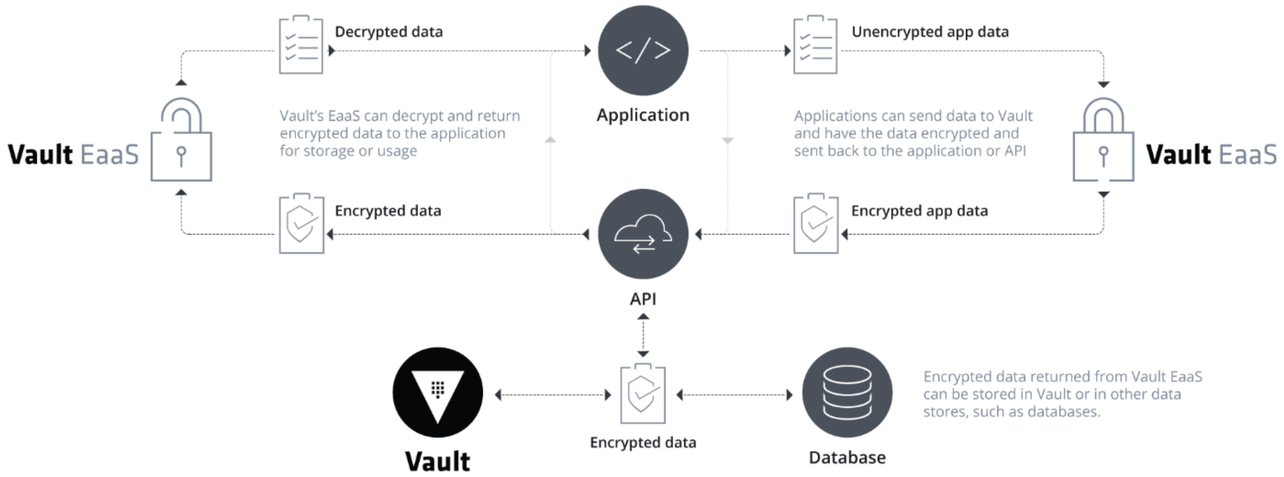
Feature: **API-Driven Encryption**

CHALLENGE | **SOLUTION** | RESULTS

Use the Transit secret engine to handle encryption, decryption, and cryptographic signing

With the Transit secret engine, Vault can enable users and applications to perform cryptographic workloads without a key management infrastructure

- Automate encryption, decryption, and cryptographic hashing and signing without deploying new infrastructure
- Quickly create and manage keys (including rotation) without deploying complex key management servers
- Support AES 256, RSA (2048 and 4096), ECDSA-p256, ed25519, chacha20-poly1305, and more



Feature: **API-Driven Encryption**

RESULTS

Increase Agility

Create keys and automate cryptographic operations without deploying a key management infrastructure

Reduce Risk

Minimize the risk of misconfiguring a cryptographic infrastructure by relying on Vault's internal crypto engines

Reduce Cost

With Vault, you can quickly deploy new and isolated cryptography without the burden of adding new cryptographic servers or management overhead for managing "key sprawl"

Feature: **Certificate Authority (TLS/SSH, PKI)**

CHALLENGE SOLUTION RESULTS

Deploying and managing certificate authority infrastructure is difficult

Safely designing, launching, and administering a certificate management infrastructure is difficult

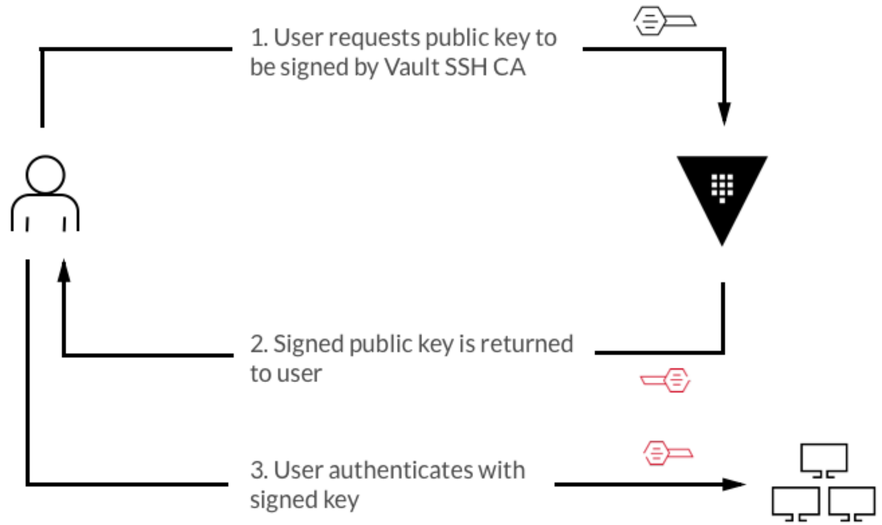
Feature: **Certificate Authority (TLS/SSH, PKI)**

CHALLENGE **SOLUTION** RESULTS

SSH/TLS and PKI CA Secret Engines

With the SSH/TLS and PKI secret engines, you can quickly deploy a certificate authority infrastructure for identifying workloads and automate management:

- Create and authenticate x.509 certificates
- Manage the creation and authentication of SSH/TLS certificates
- Allow Vault to serve as a root or intermediate certificate authority



Feature: **Certificate Authority (TLS/SSH, PKI)**

Increase Agility

Allow the deployment of additional CAs that align with existing certificate authority infrastructure

Reduce Risk

With ACL policies and allowed/denied parameters, restrict how users access and create certificates and certificate authorities

Reduce Cost

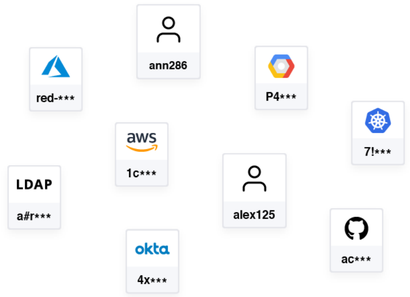
Vault's PKI and TLS/SSH secret engines support being intermediate authorities, allowing Vault to integrate with existing PKI and permit it to economically scale

VAULT ADOPTION

Use Case
Identity-Based Access

Use Case: **Identity-based Access**

Authenticate and access different clouds, systems, and endpoints using trusted identities.



The Challenge

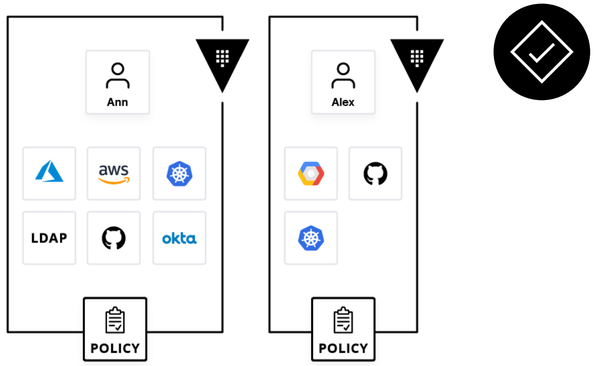
With the proliferation of different clouds, services, and systems all with their own identity providers, organizations need a way to manage identity sprawl.

BEFORE

- **Increased costs** from managing multiple identity management systems
- **Reduced productivity** from added work to unify a single identity across multiple system aliases
- **Increased risk** from complexity at the heart of one's security infrastructure

Use Case: **Identity-based Access**

Authenticate and access different clouds, systems, and endpoints using trusted identities.



The Solution

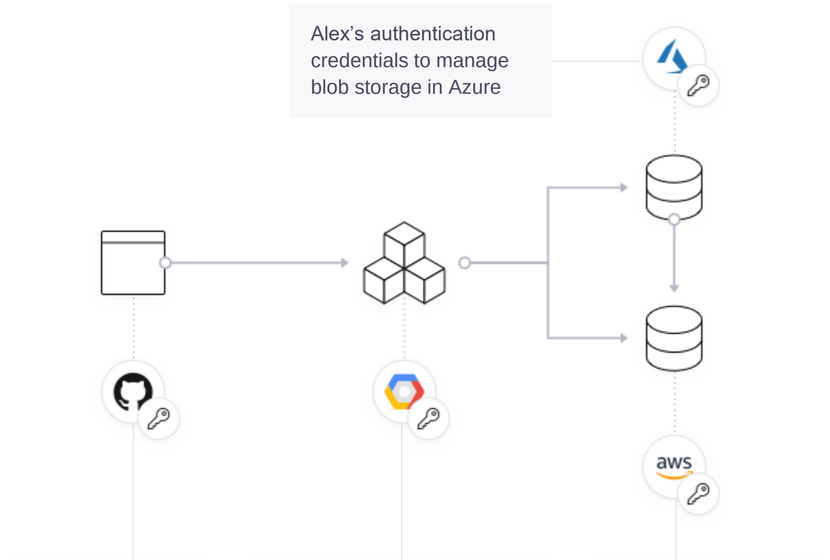
Vault merges identities across providers and uses a unified ACL system to broker access to systems and secrets.

AFTER

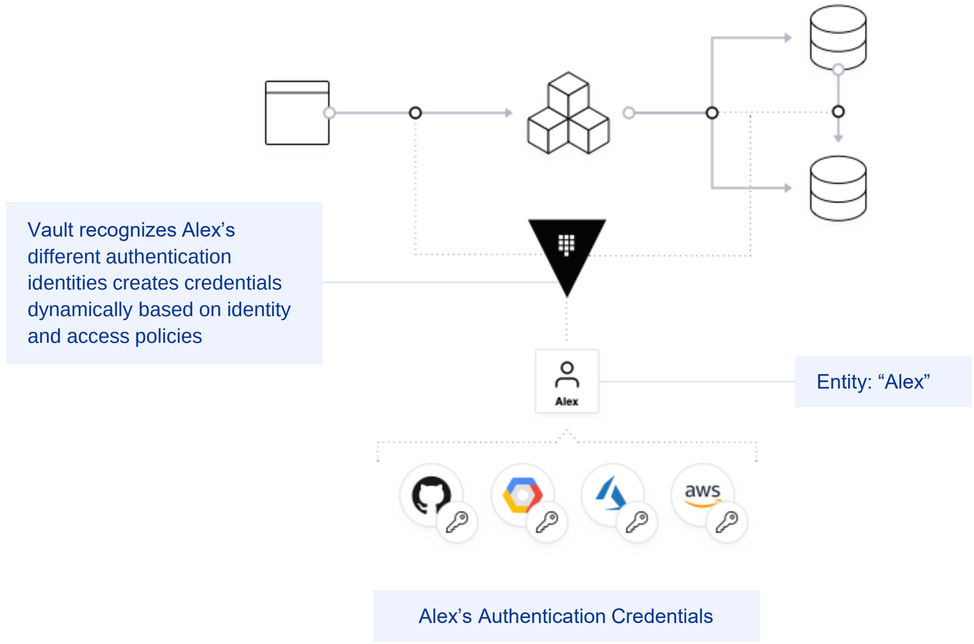
- **Reduce costs** by minimizing the cost of writing multiple redundant ACL policies
- **Increase productivity** by reducing the amount of time necessary to onboard new applications or users
- **Reduce risk** with a single, simplified workflow for managing access across users, applications, and infrastructures

How identity-based access works

Without Vault



With Vault



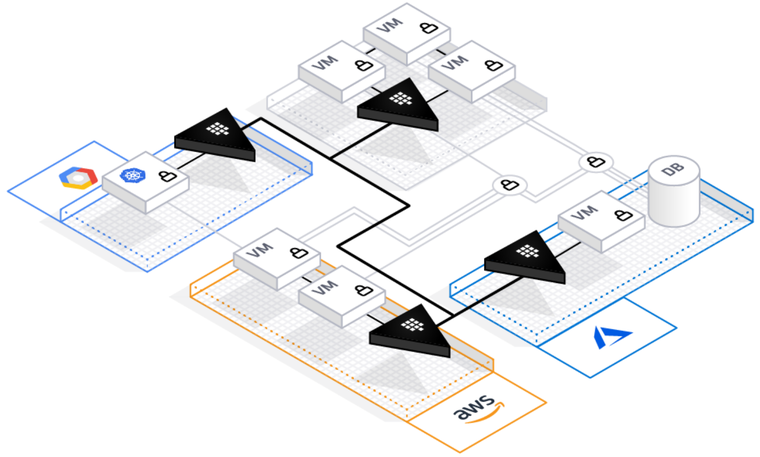
Identity-based security with Vault

Leverage any trusted source of identity to enforce system and application access.

Secrets Management enables centrally managing secrets.

Encrypting Data keeps application data secure

Identity-based Access allows easy integration across systems and clouds



Features

1 **Identity Plugins**

Log into Vault with your existing identity providers.

2 **Entities**

Entities are aggregated external identities that represent users and applications within Vault as a single, common identity. Entities make it easier to identify who someone is across a multitude of providers and assign and control access with policies.

3 **Identity Groups**

Group trusted identities into logical groups for group-based access control.

4 **Control Groups**

Require multiple Identity Entities or members of Identity Groups to authorize any operations or requested action by users or applications.

5 **ACL Templates and Policy Control**

Create and manage policies that authorize access control throughout your infrastructure and organization.

6 **Multi-factor Authentication**

Enforce MFA workflows when accessing a secret or a secret path using different authentication types such as TOTP, Duo,Okta, and PingID.

Feature: **Unified Identity**

CHALLENGE SOLUTION RESULTS

Uniting credentials to one logical identity across multiple cloud platforms is very difficult

Different cloud providers, applications, and environments support different methods and constructs for identity - adding complexity to recognizing one user or identity across multiple forms of credentials

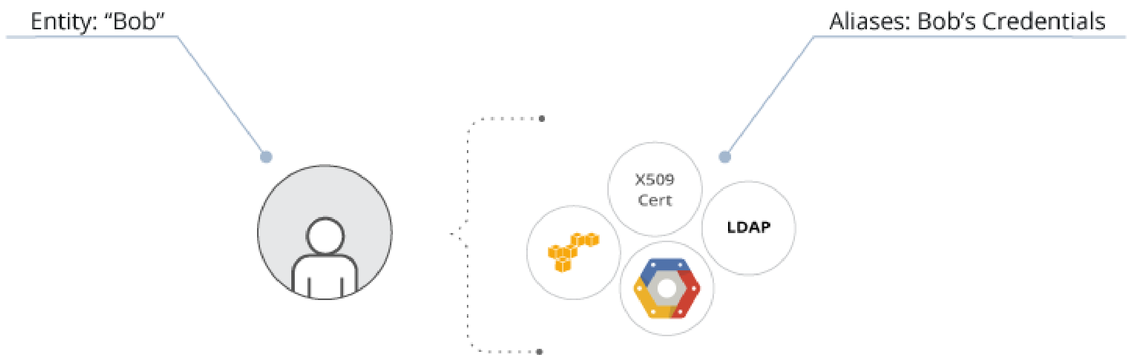
Feature: **Unified Identity**

CHALLENGE | **SOLUTION** | RESULTS

Unified Identity: one identity across multiple environments

With Vault's unified identity system, Vault can match one identity across cloud environments, applications, etc.

- One logical identity can be recognized with multiple aliases from separate cloud, on-prem, app environments
- Use Identity Groups to simplify RBAC logic



Feature: **Unified Identity**

Increase Agility

Instead of modifying an organization's entire identity management infrastructure, adding new credentials and managing RBAC is as easy as affiliating a new alias or adding an entity to an identity

Reduce Risk

Simplifying the logical association of identity with credentials across infrastructures reduces risk and makes it easier to enforce least privilege

Reduce Cost

Unified Identity allows Vault to simplify the management of identity, access, and adopting and managing new identity systems

Feature: **ACL Policies and Sentinel**

CHALLENGE SOLUTION RESULTS

Enforcing Role-Based Access Control (RBAC) across environments is difficult

Enforcing security/corporate policy in RBAC across multiple cloud environments is difficult and extremely challenging as organizations scale

Feature: **ACL Policies and Sentinel**

CHALLENGE | **SOLUTION** | RESULTS

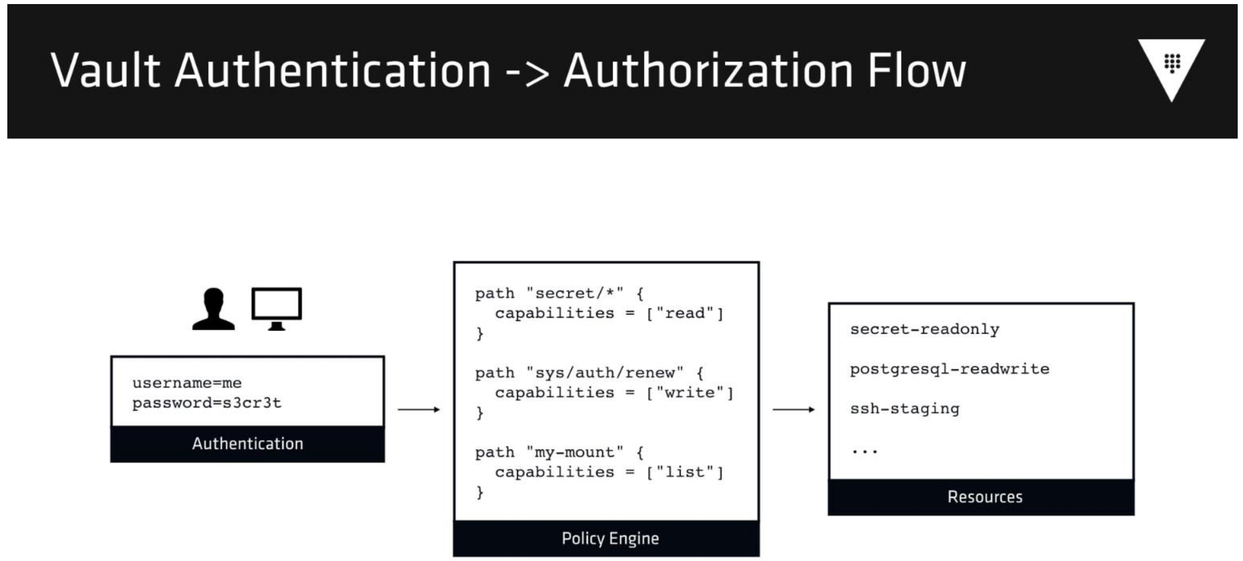
ACL Policies and Sentinel

Vault allows you to flexibly and easily apply policies to entities and groups across its unified identity infrastructure, allowing:

- With ACL policies control RBAC easily and logically for multiple credentials and applications in one line of code

ENTERPRISE

- With Sentinel, apply additional policies on how users connect via specific authentication methods or on accessing specific secrets
- Apply additional controls requiring Multi-Factor Authentication (MFA)



HashiCorp

Feature: **ACL Policies and Sentinel**

RESULTS

Increase Agility

With support for HCL and namespaces, users can apply policies quickly and even grant privileged access to other users to manage their own applications' RBAC

Reduce Risk

Vault admins can restrict which parameters and access users can author in ACL policies, segment the application and creation of policies in namespaces, and apply environment wide controls without changing the architecture of Vault's identity systems

Reduce Cost

Vault admins can empower users to manage their own policy infrastructure with namespaces, allowing Vault to scale while minimizing additional management costs

Feature: **Control Groups**

CHALLENGE SOLUTION RESULTS

Multiple authorization for actions is difficult to implement across environments

Implementing controls to require multiple authorizers across events spanning different applications and cloud infrastructures is incredibly complicated and difficult to implement

Feature: **Control Groups**

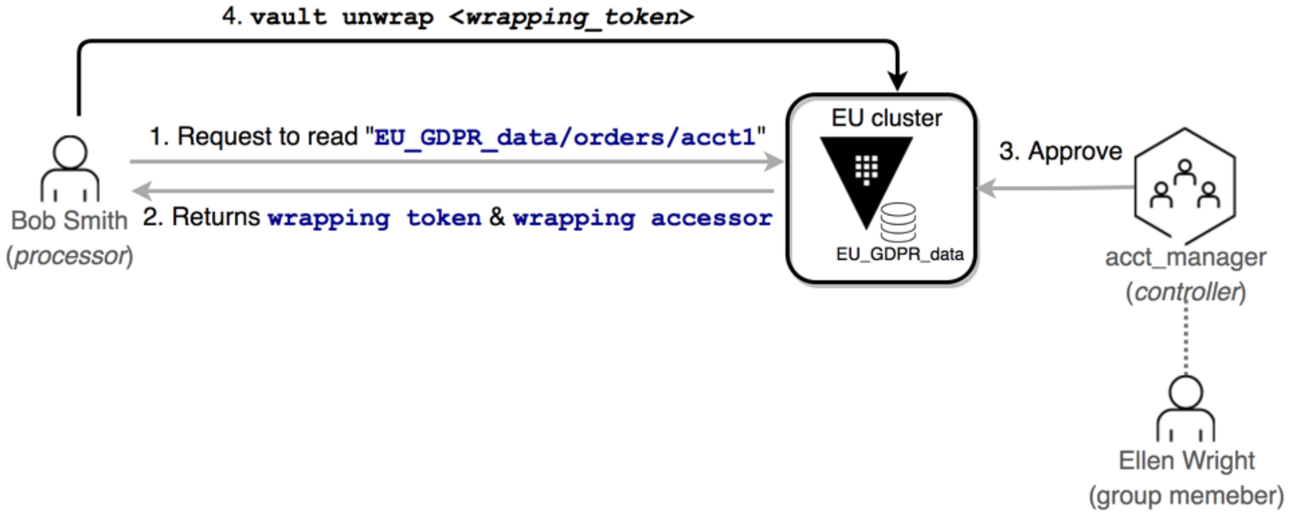
CHALLENGE | **SOLUTION** | RESULTS

Control Groups

With Control Groups, Vault admins can require external authorization for specific actions or security workflows within Vault

ENTERPRISE

- Trigger external authorization on nearly any action in Vault
- Granularly control which identity groups can authorize a transaction
- Comply with regulatory requirements for external controllers (e.g.: GDPR)



Feature: **Control Groups**

Increase Agility

With Control Groups, establishing compliance controls on a constantly expanding and scaling implementation of Vault is easily automated

Reduce Risks

Control Groups allow for Vault users and applications to be empowered as validators of actions within Vault in accordance with regulations such as GDPR

Reduce Costs

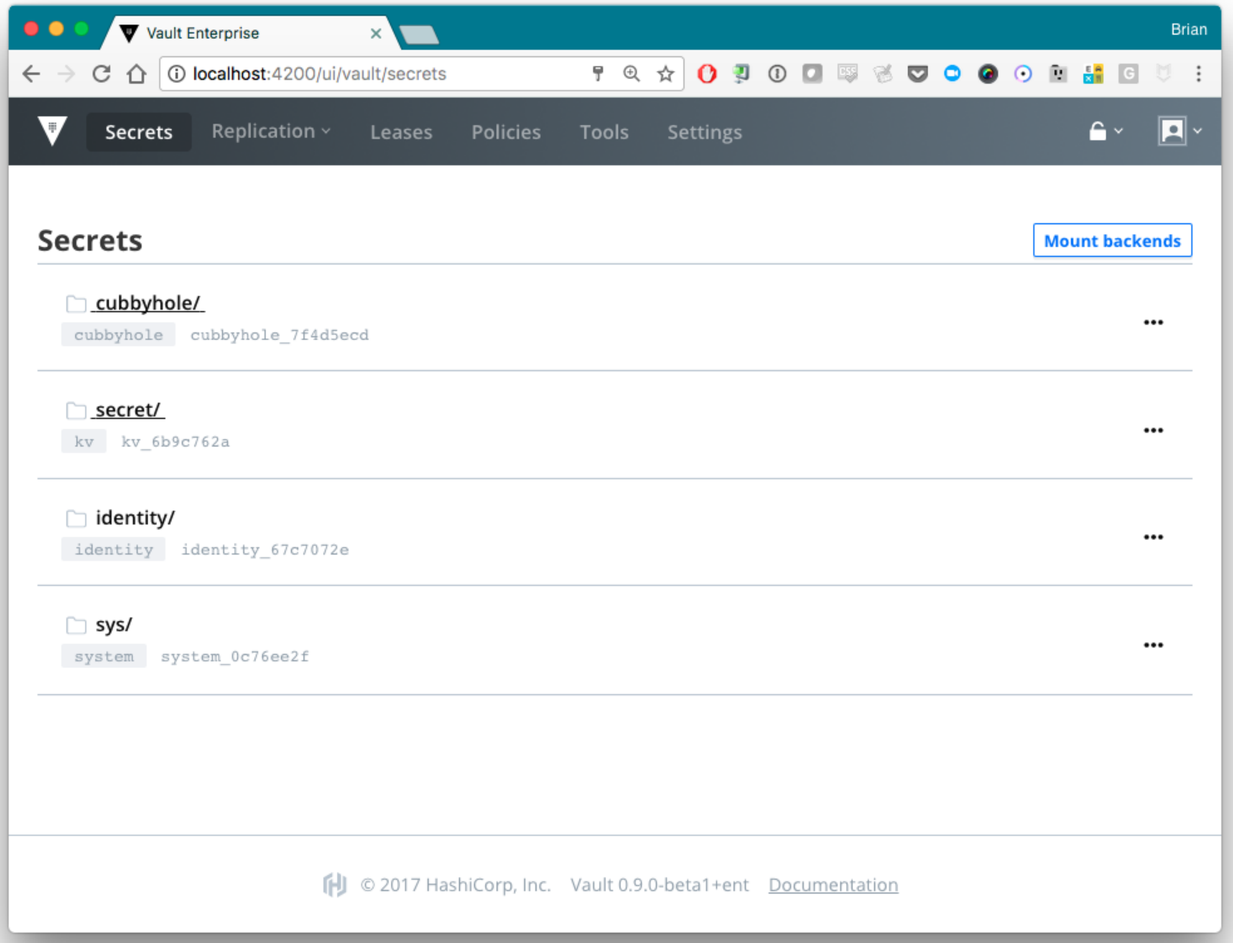
Control Groups allow other non-admin users of Vault to validate the authenticity of a user or application's identity, lowering the management cost and risk of scaling

Vault
Operations

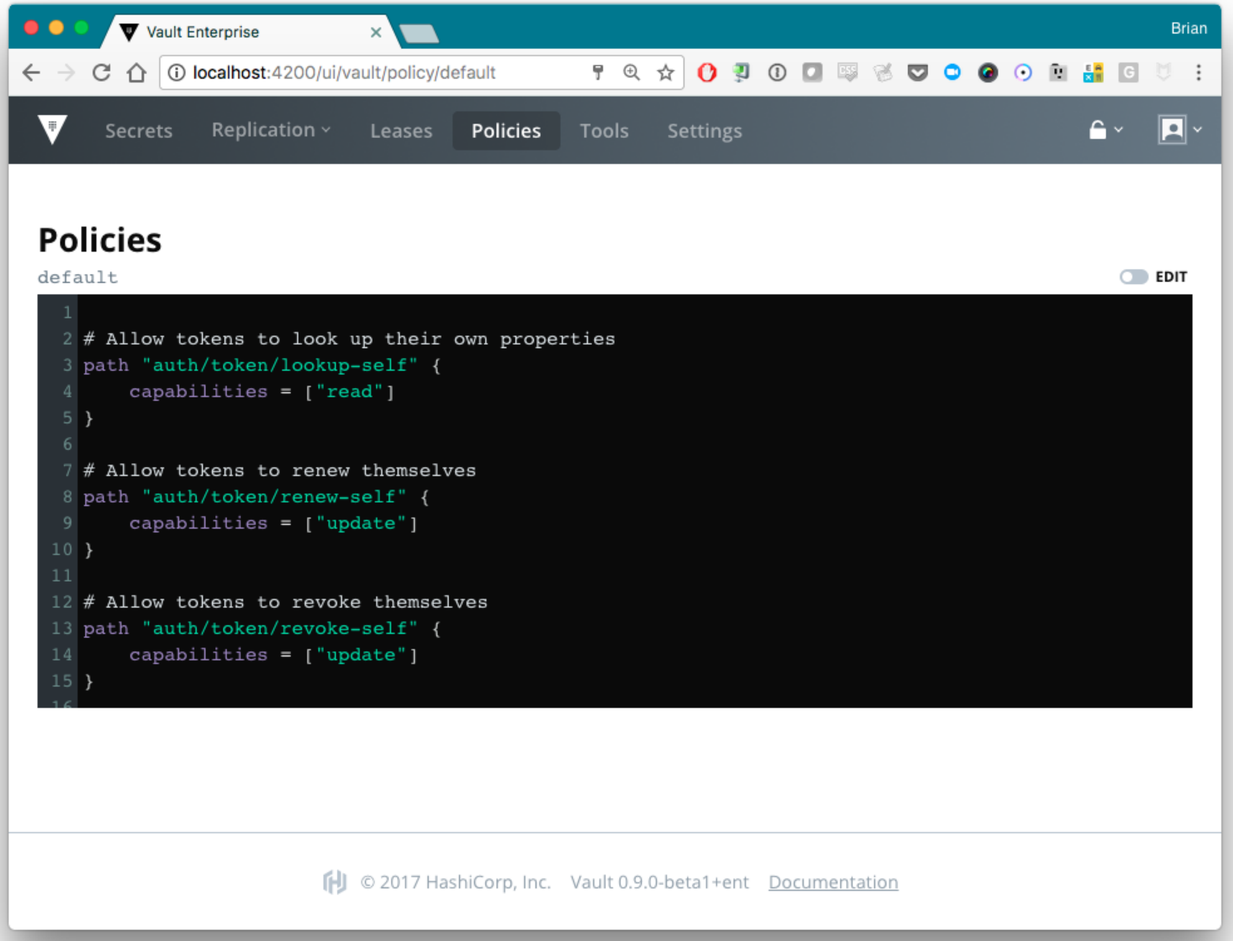
UI Management

- Perform all CLI/API actions from one visual interface
- Easily accessible browser interface for secret administration
- Manage Vault clusters across datacenters

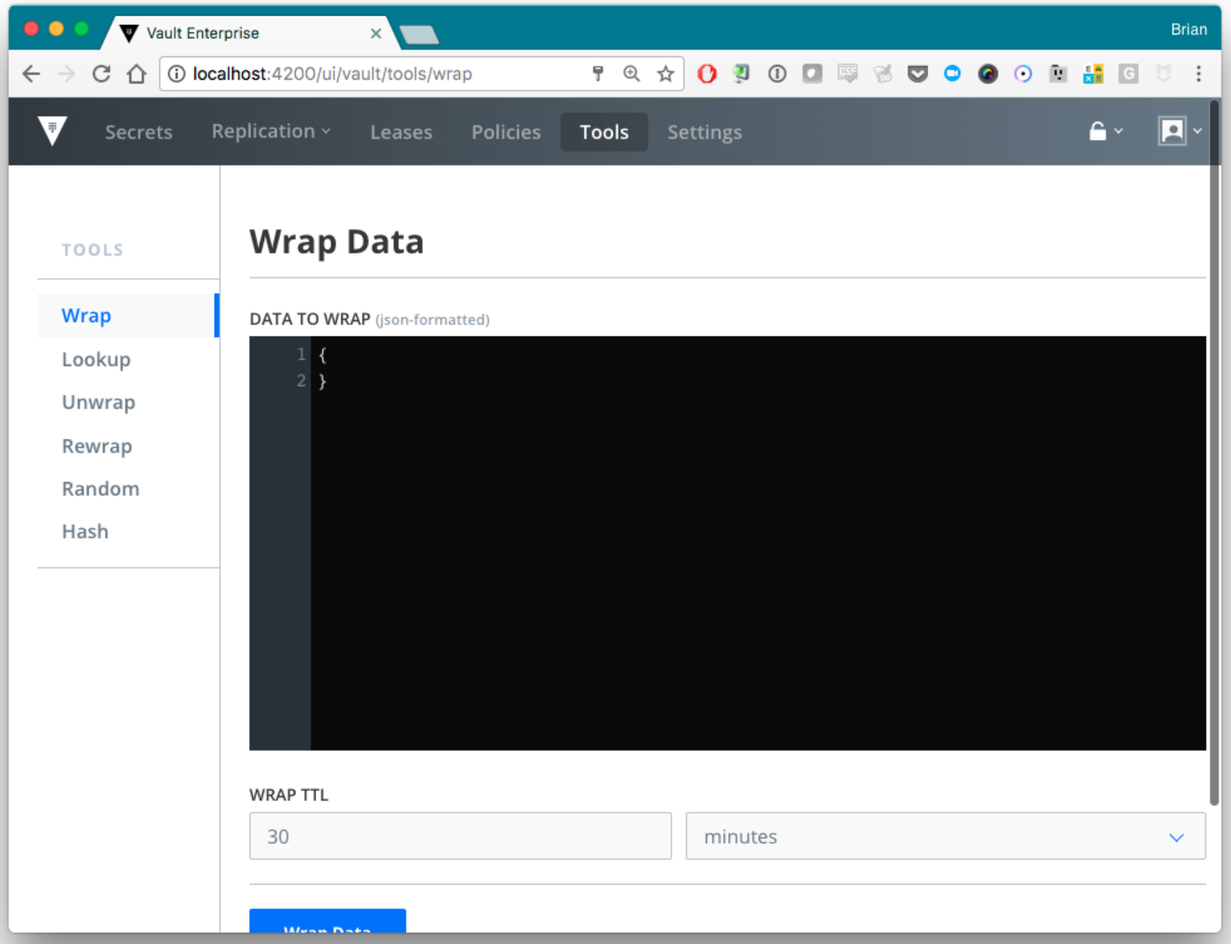
Web User Interface



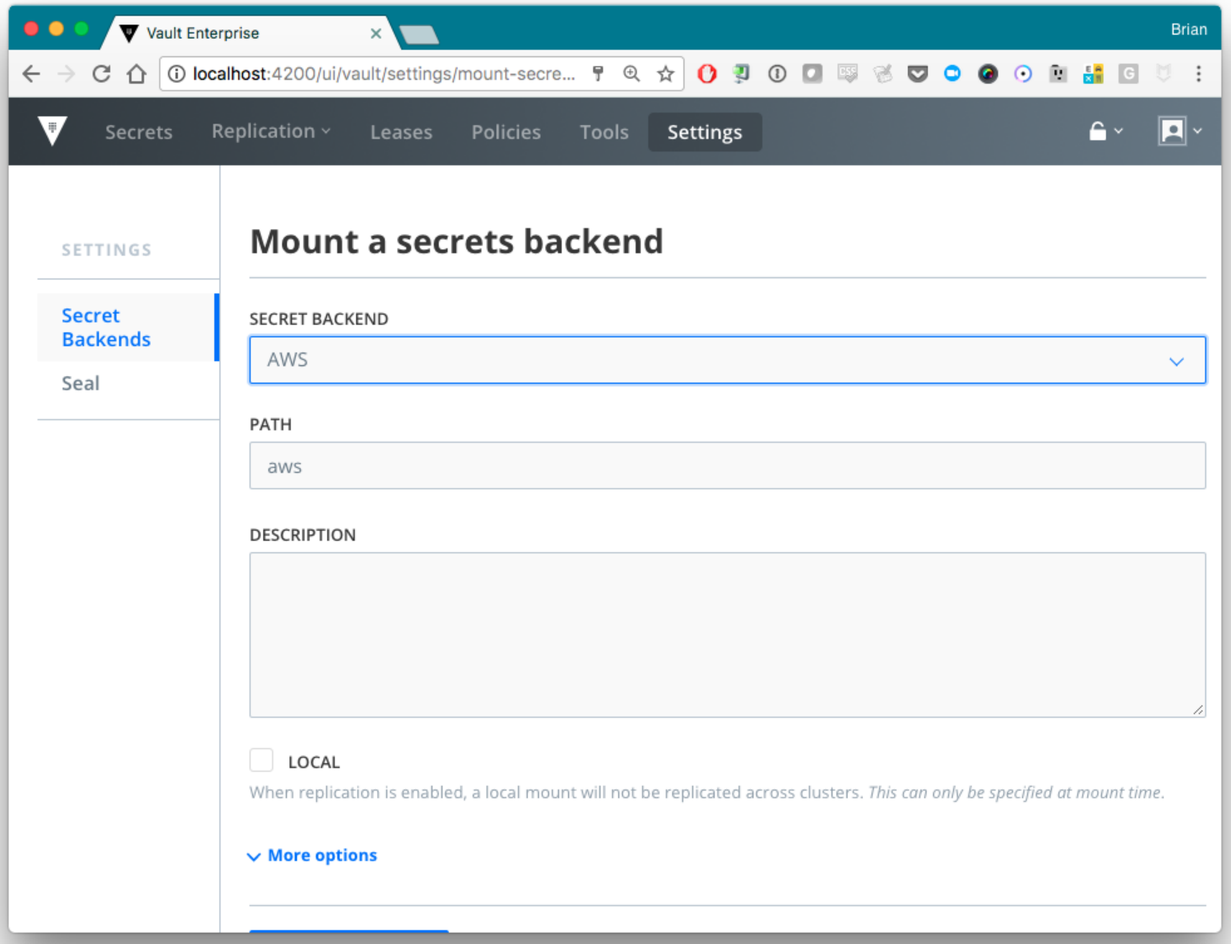
Web User Interface



Web User Interface



Web User Interface

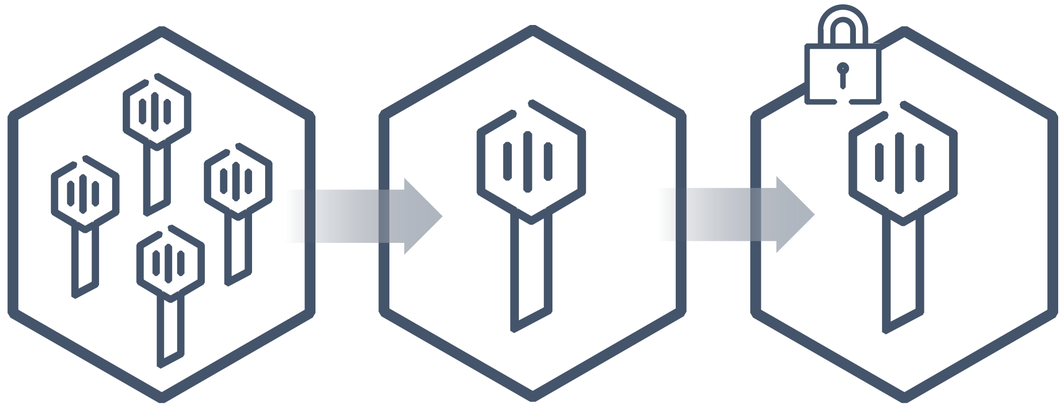


Vault Unseal

Methods of protecting root encryption key

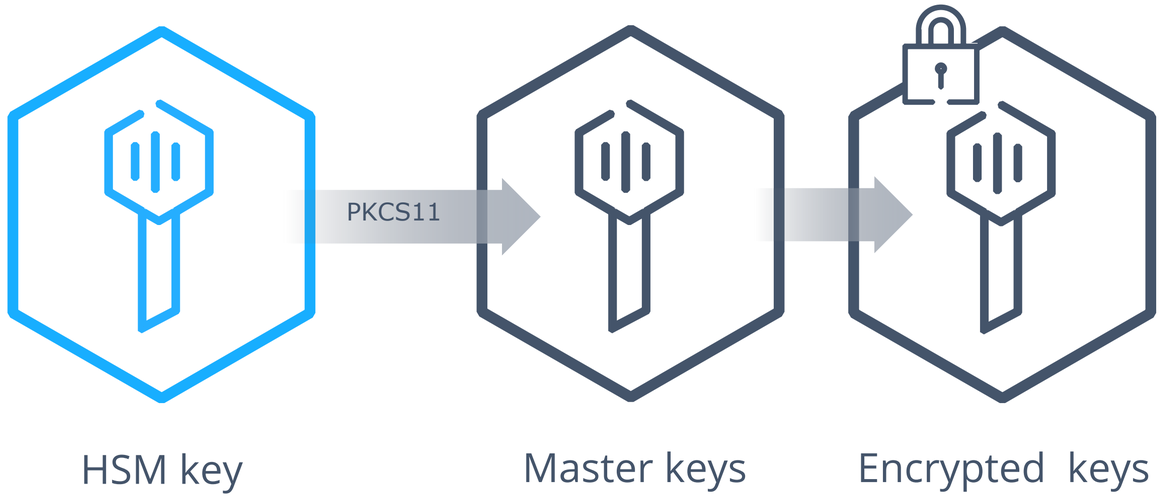
Shamir’s Secret Vault Unsealing

- Protect Encryption Key with Master Key
- Split Master Key into N shares
- K shares to re-compute Master
- Quorum of key holders required to unseal
- Default K:5, T:3



Automated Vault Unsealing

- Protect Encryption Key with Master Key
- HSM encryption key protects master key
- Communication with HSM via PKCS11 API to decrypt Master Key

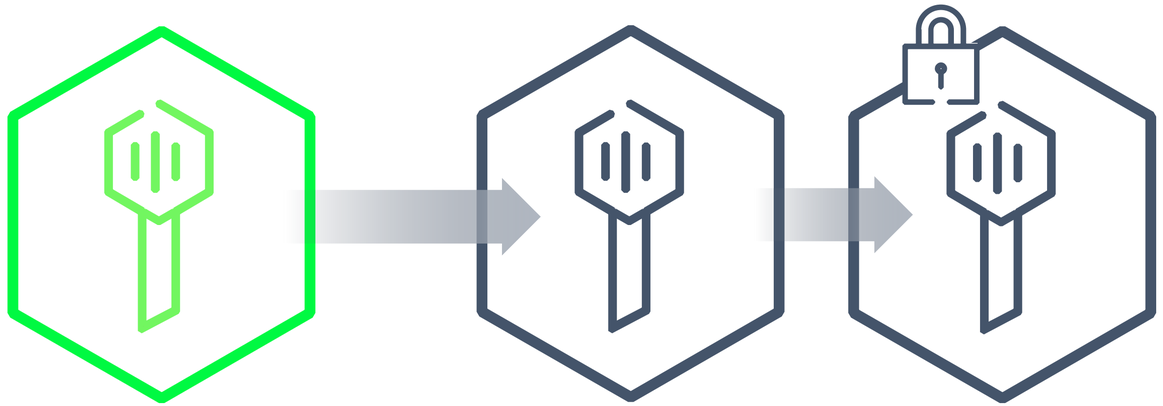


SafeNet THALES

AWS CloudHSM utimaco®

Cloud Key Service Automated Vault Unsealing

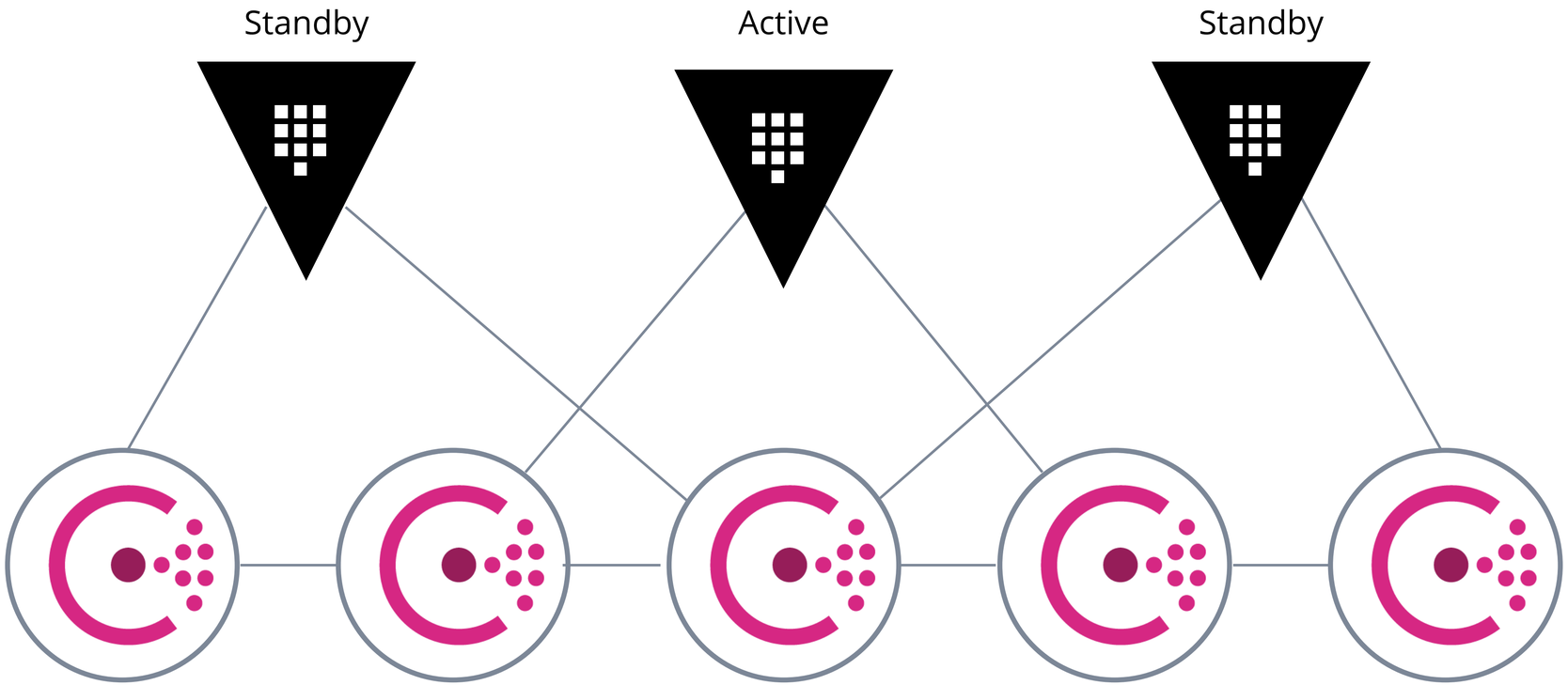
- Protect Encryption Key with Master Key
- Cloud based encryption key protects master key
- Supported cloud services:
  - Google Cloud Key Management Services
  - AWS Key Management Services
  - AliCloud
  - Azure Key Vault



Vault Single Cluster Architecture

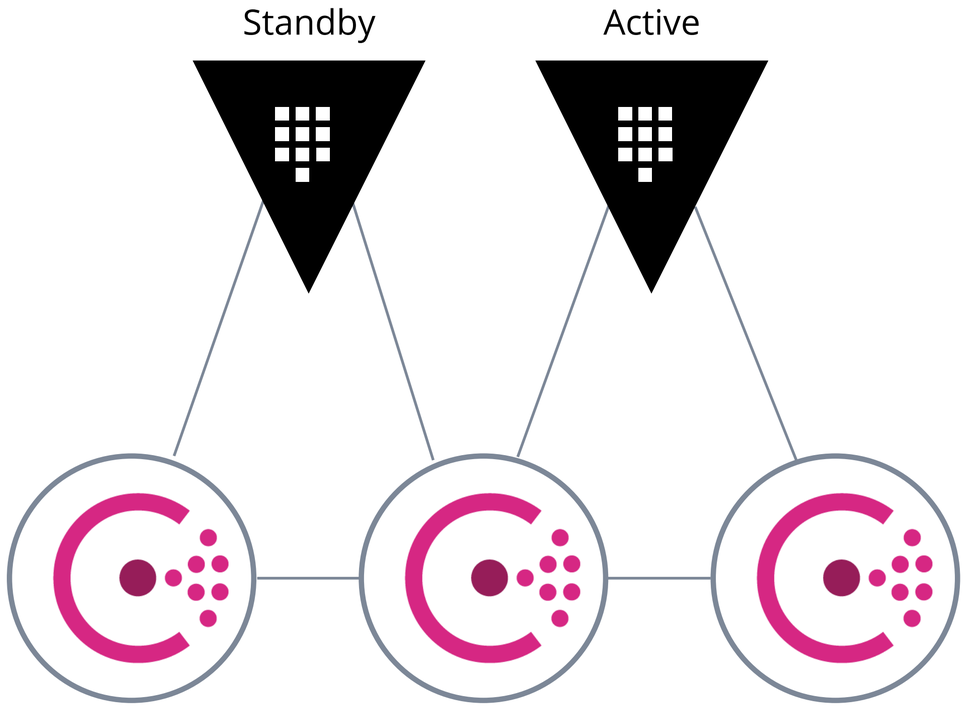
Vault Cluster Architecture

Production



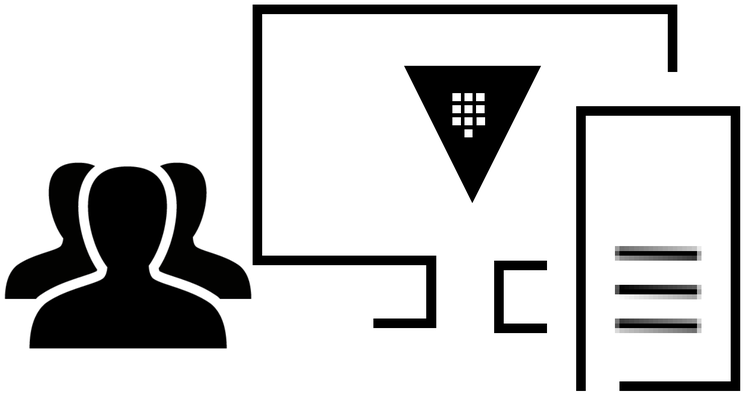
Vault Cluster Architecture

Staging

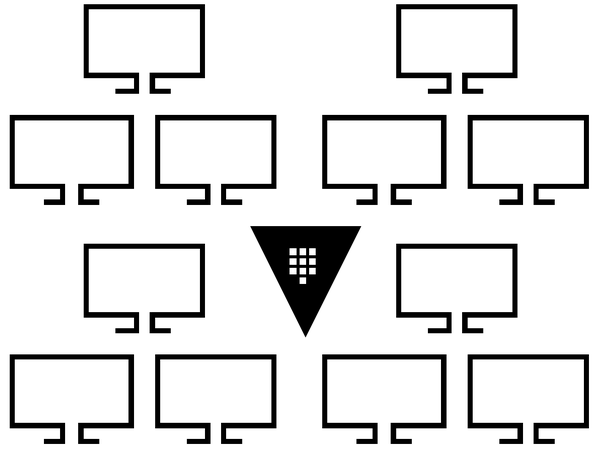


Vault Cluster Architecture

Local Development: Developers can use Vault binary locally to develop applications in environment identical to production.



`VAULT_ADDR=127.0.0.1`

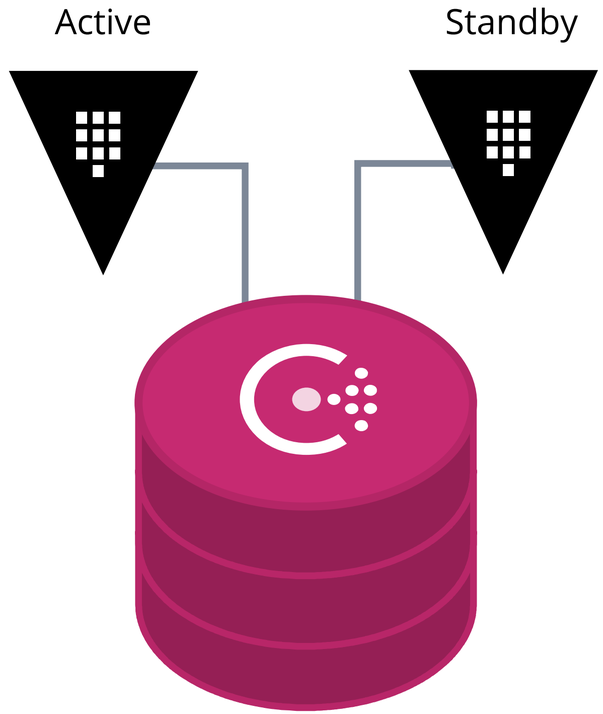


`VAULT_ADDR=vault.prod.example.org`

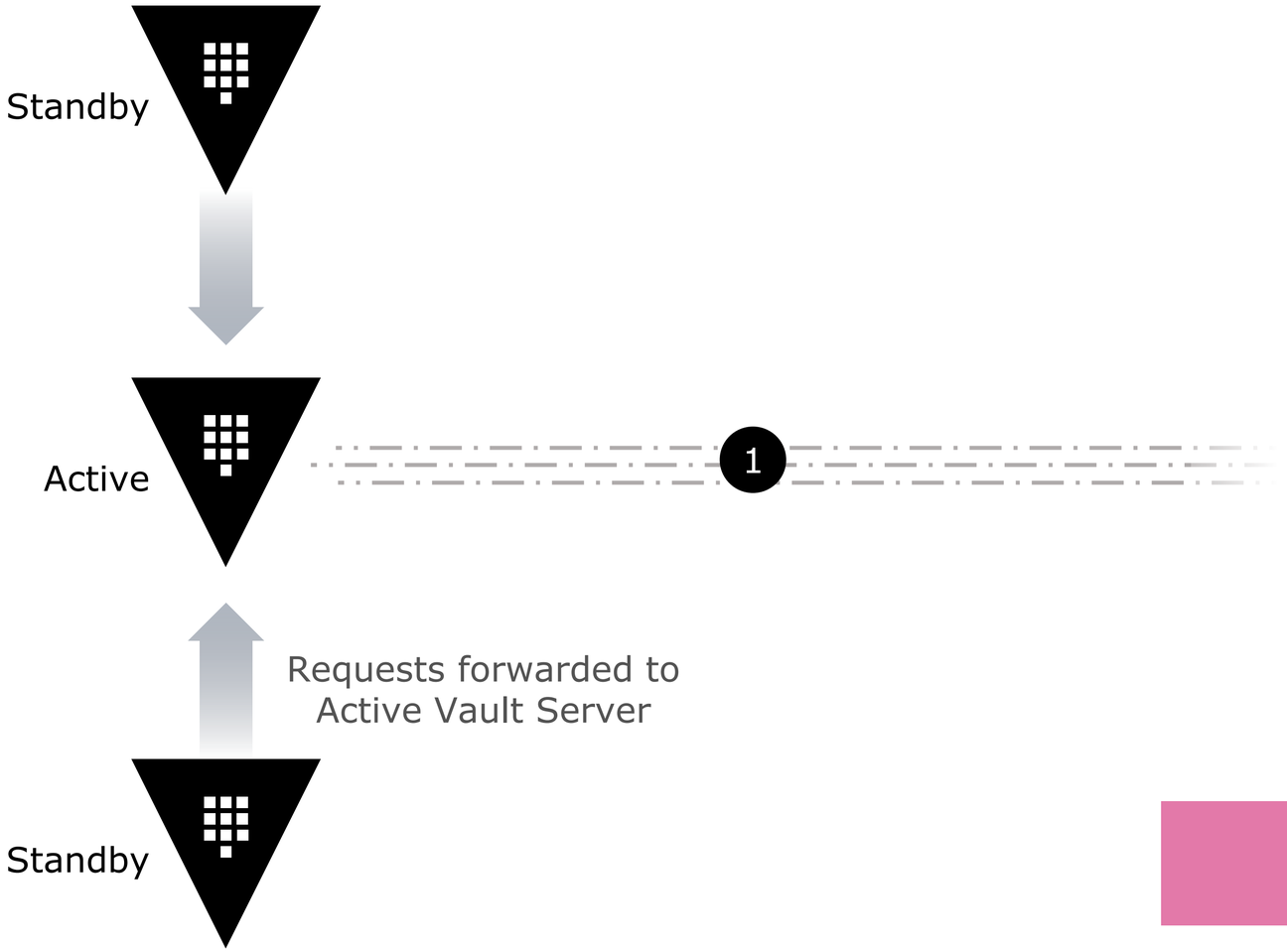
High Availability with Consul Storage backend

Why Consul?

- Officially supported product by HashiCorp
- Highly scalable distributed key-value store, very performant
- Easily configured in Vault
- Vault high availability is achieved through Consul's leader election capabilities
- Automatic registration of Vault services, tags, and health checks in Consul



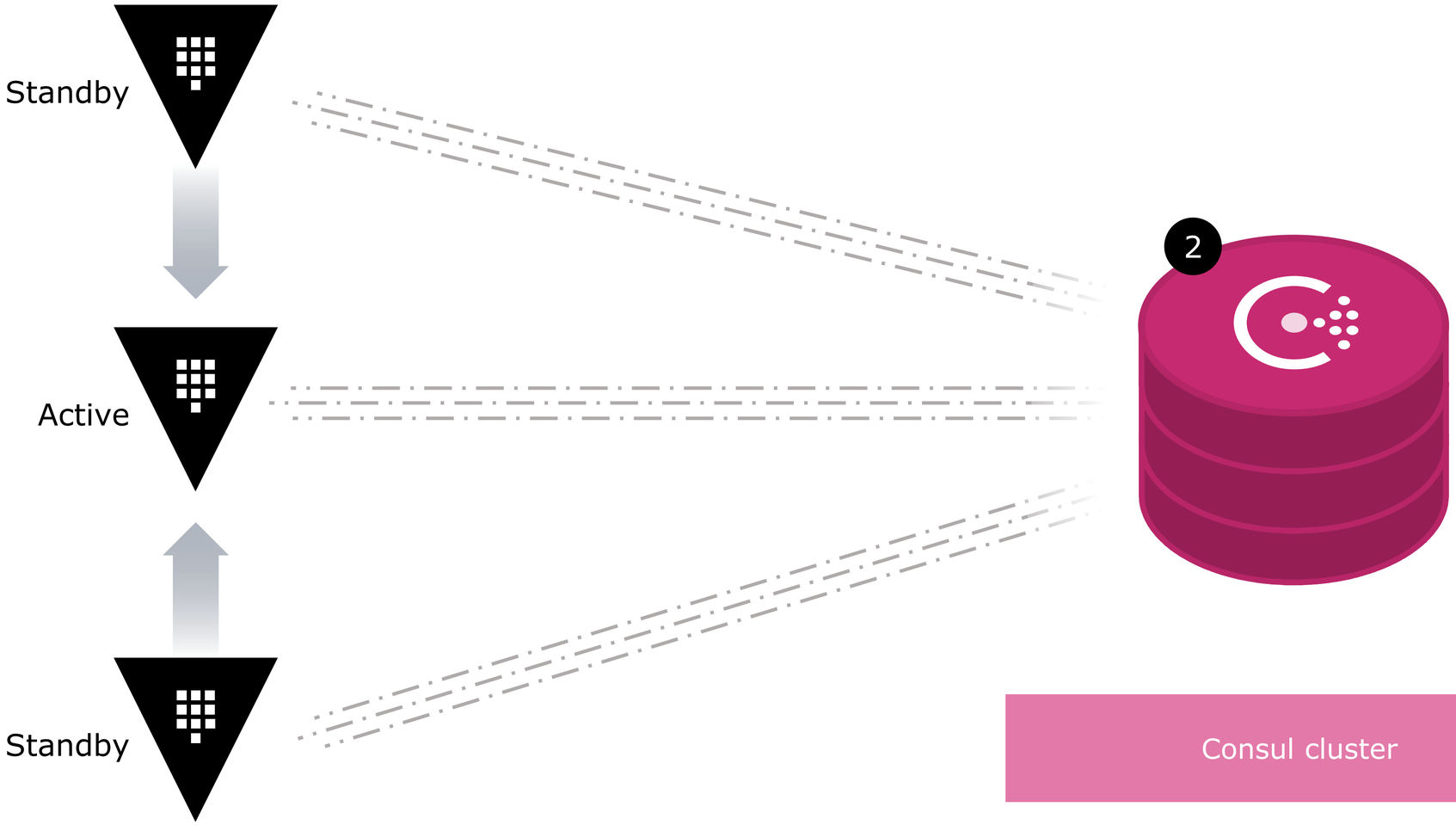
High Availability with Consul Storage backend



1. Active Vault node retains lock on AES-256 encrypted storage.
2. Consul performs regular health checks on Vault nodes.
3. Detection of failure on Active node triggers leader election
4. Standby node is elected as Active Vault agent

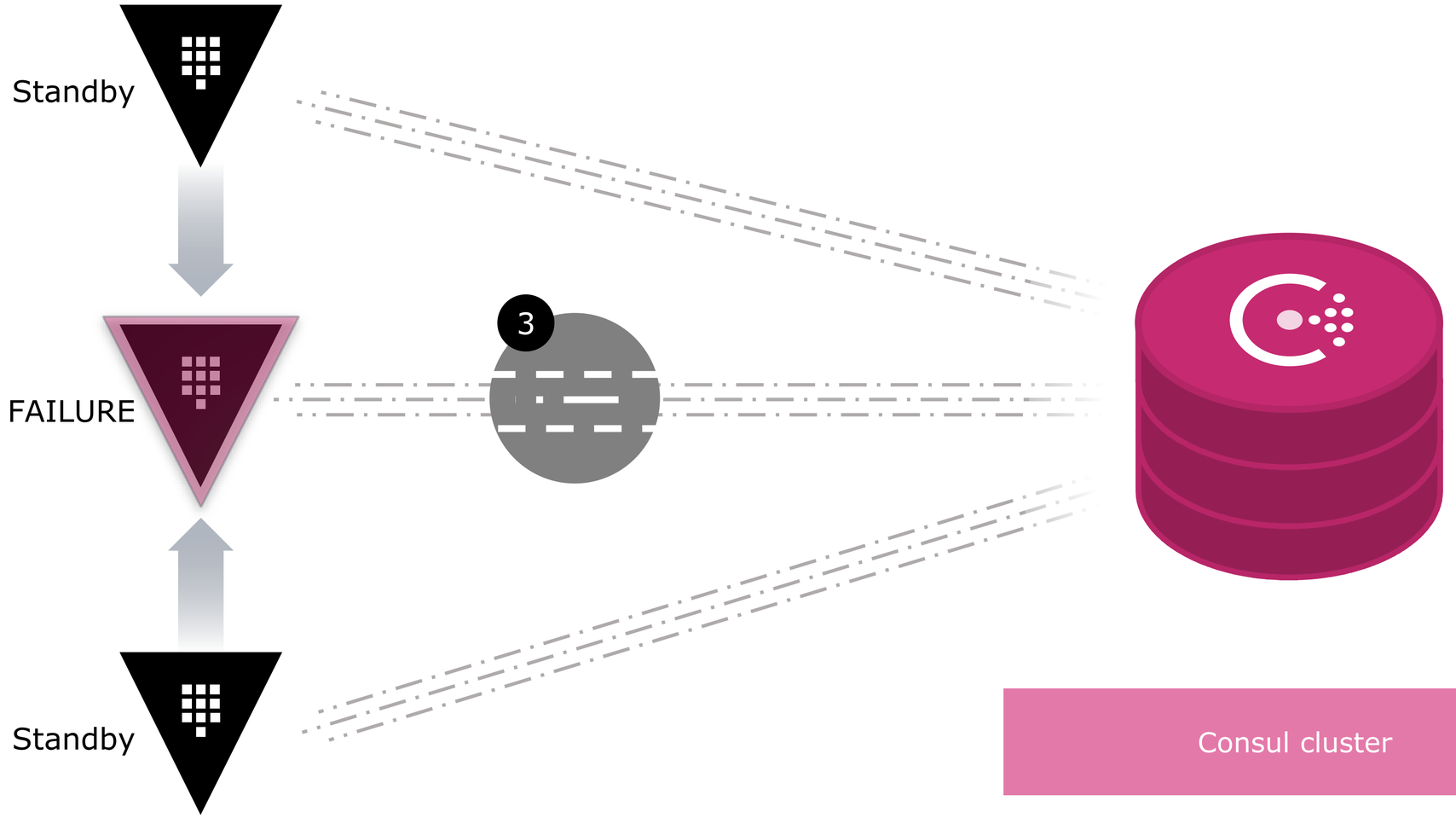
Consul cluster

High Availability with Consul Storage backend



1. Active Vault node retains lock on AES-256 encrypted storage.
2. Consul performs regular health checks on Vault nodes.
3. Detection of failure on Active node triggers leader election
4. Standby node is elected as Active Vault agent

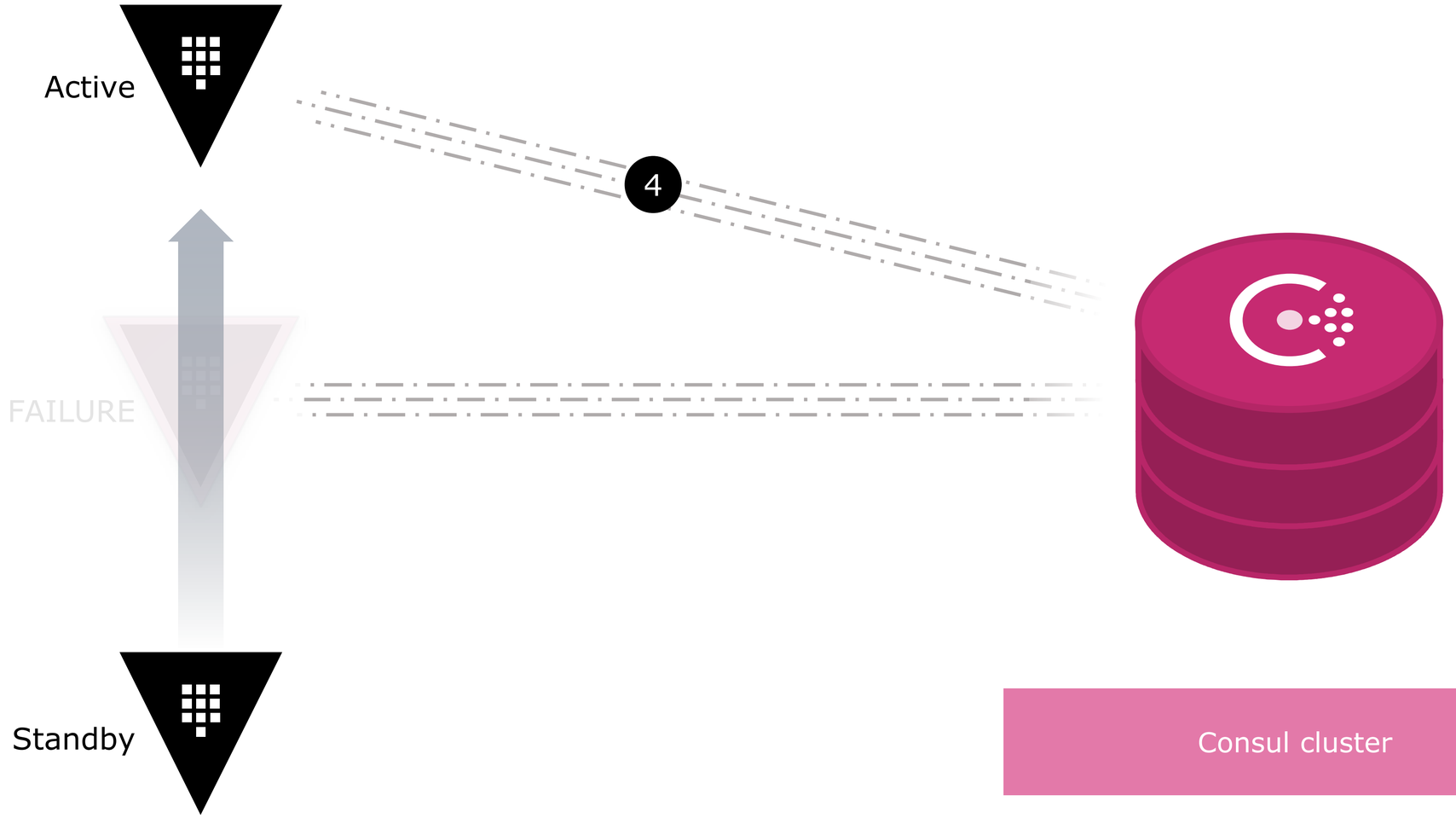
High Availability with Consul Storage backend



1. Active Vault node retains lock on AES-256 encrypted storage.
2. Consul performs regular health checks on Vault nodes.
3. Detection of failure on Active node triggers leader election
4. Standby node is elected as Active Vault agent

Consul cluster

High Availability with Consul Storage backend



1. Active Vault node retains lock on AES-256 encrypted storage.
2. Consul performs regular health checks on Vault nodes.
3. Detection of failure on Active node triggers leader election
4. Standby node is elected as Active Vault agent

Consul cluster

Performance Replication

Synchronized secrets management
across multiple locations

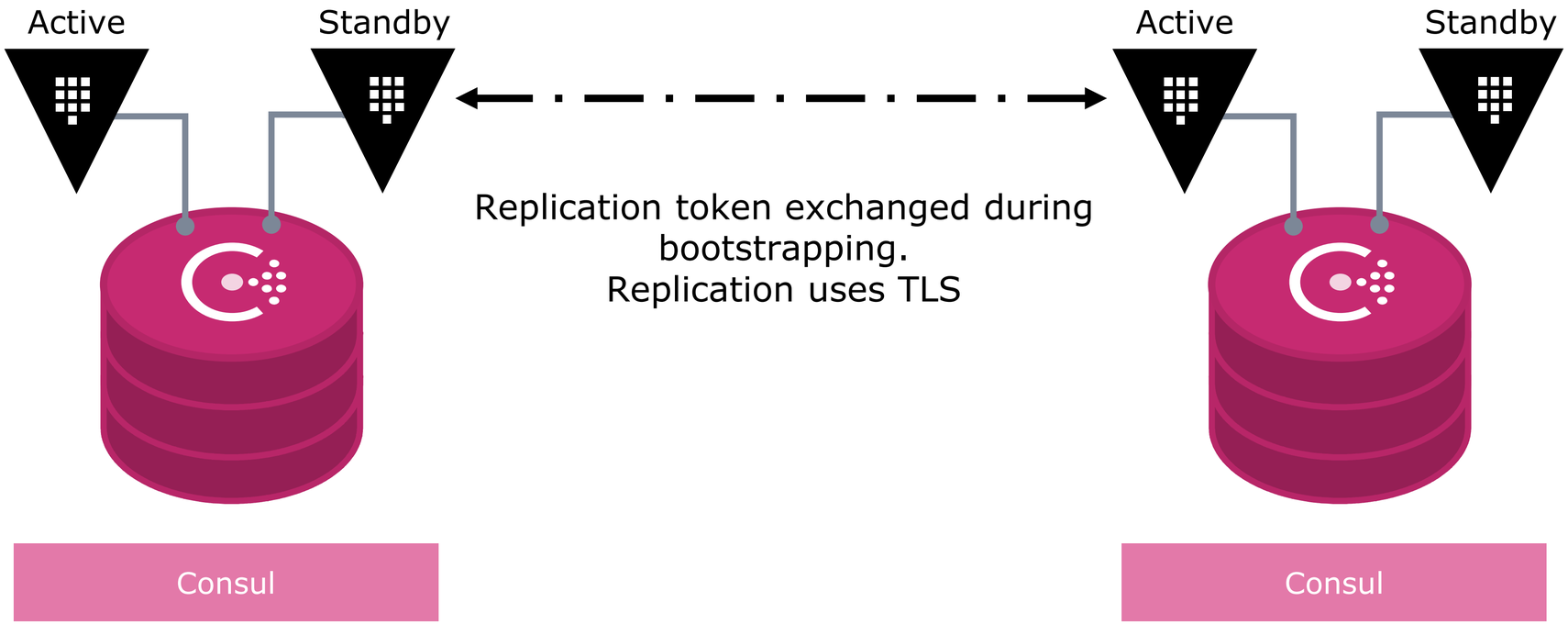
Multi-Datacenter replication for horizontal scalability

Performance
Replication features

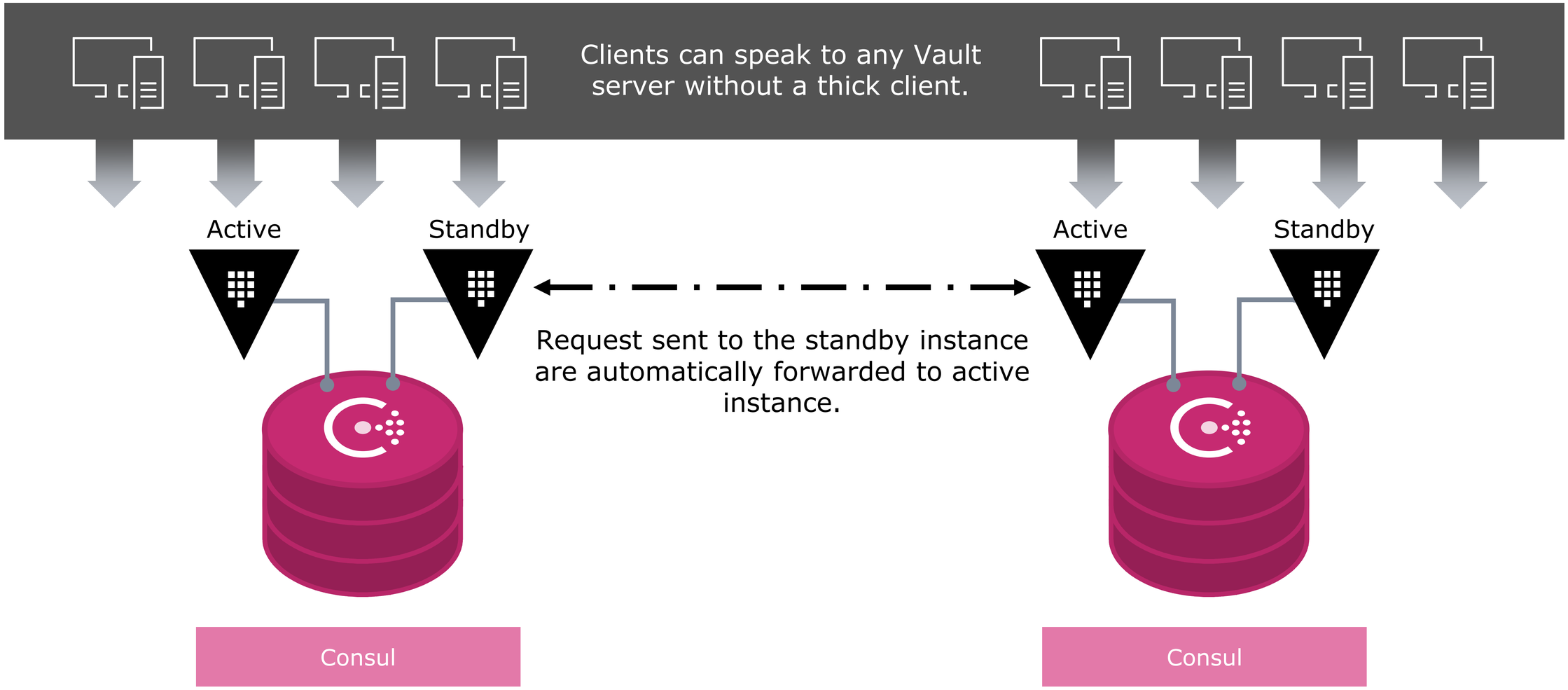
- Vault secret access from any location, with centralized management
- One to many replication
- Leverages Merkle-trees and write-ahead logs for efficient replication
- Vault replication is asynchronous and replicates changes to all of the secondary clusters. Replication occurs for the following:

  - Secrets
  - Policies
  - Secret backends config
  - Auth backends config
  - Audit backends config
  - Access tokens are NOT replicated

Basic Architecture: 2 Clusters

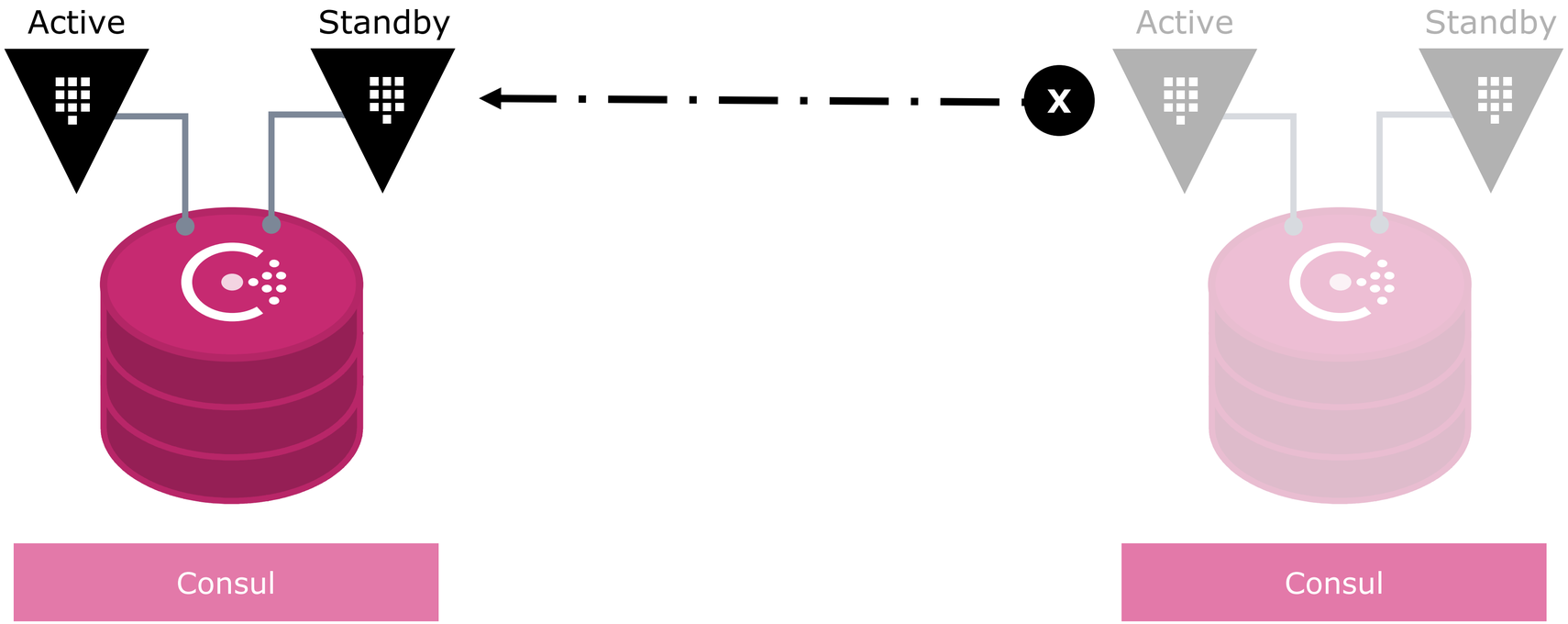


Example



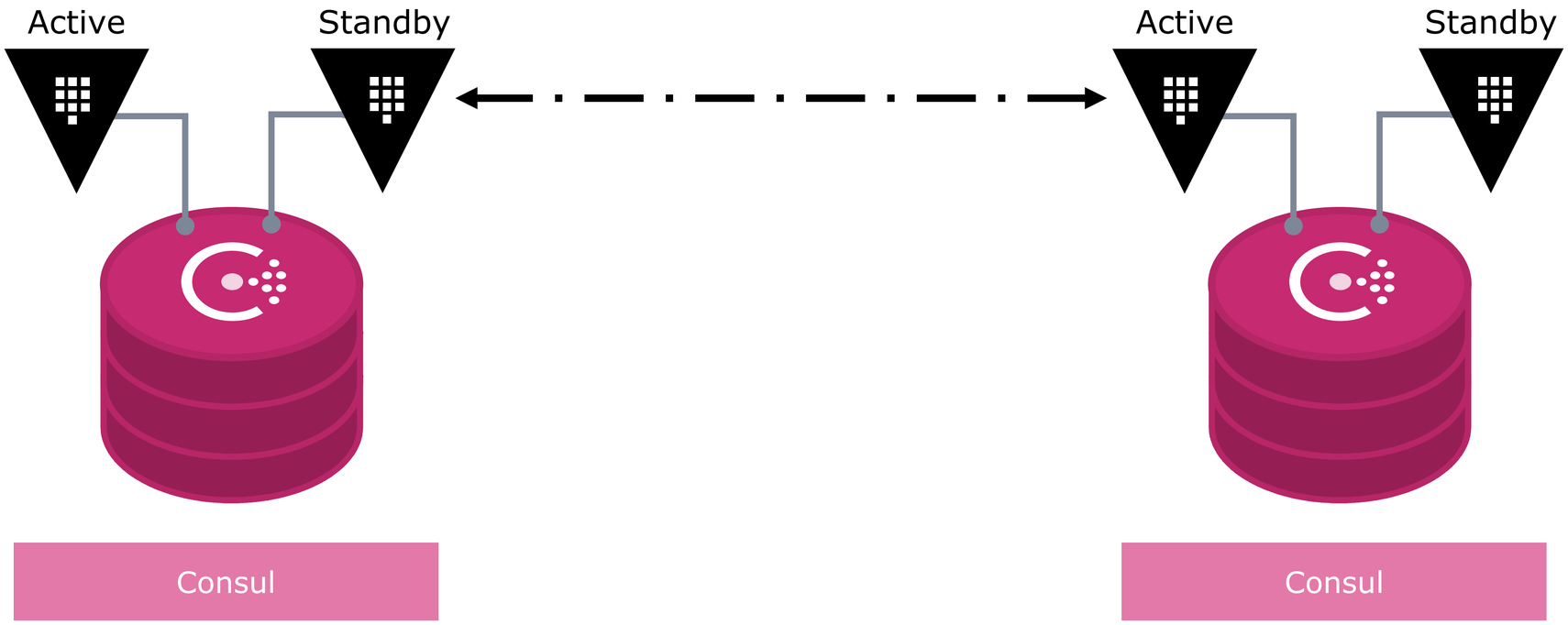
Example

If a secondary is down or unable to communicate with the primary, writes are not blocked on the primary and reads are still serviced on the secondary.



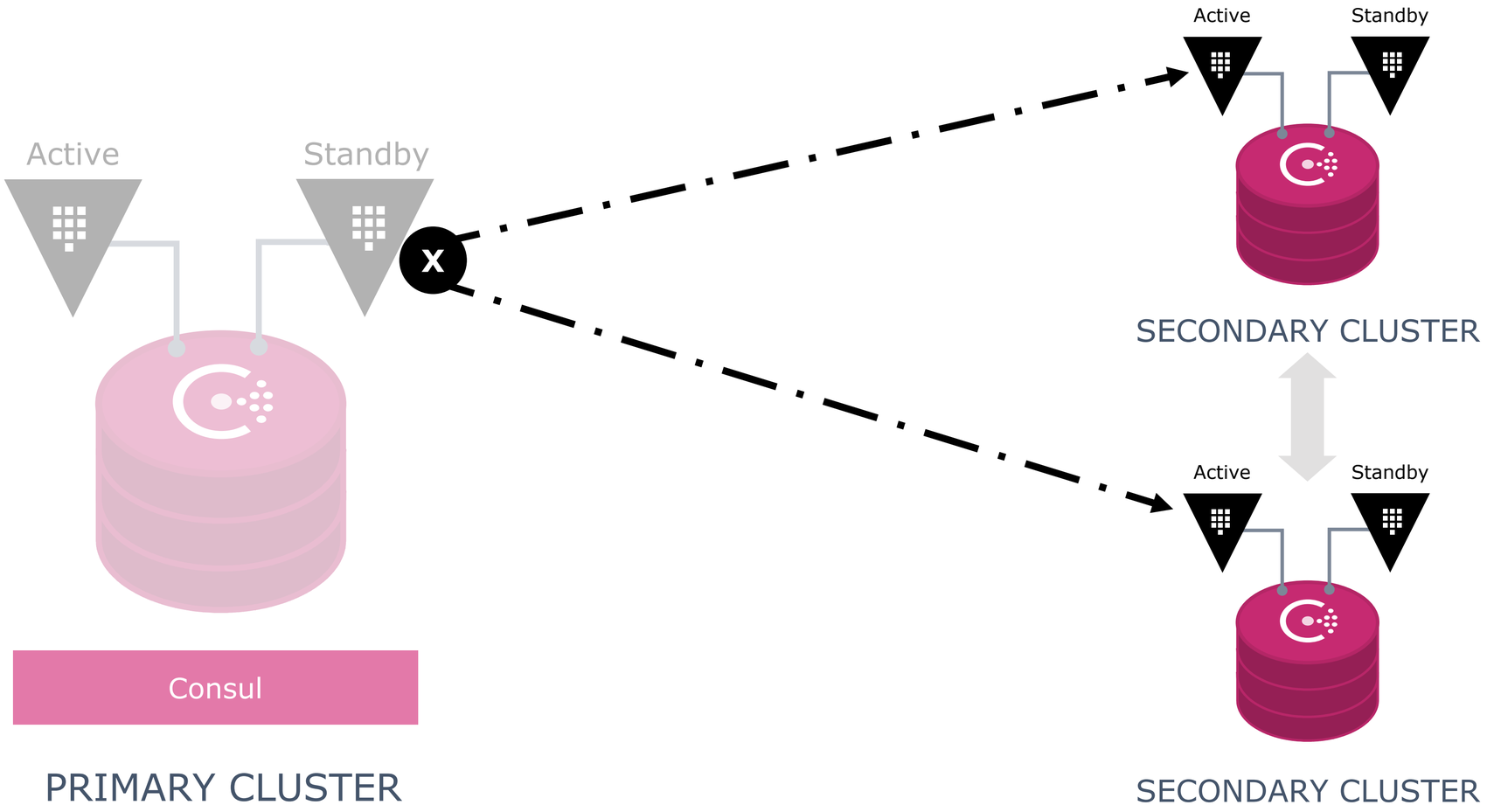
Example

When the secondary is initialized or recovers from degraded connectivity it will automatically reconcile with the primary.

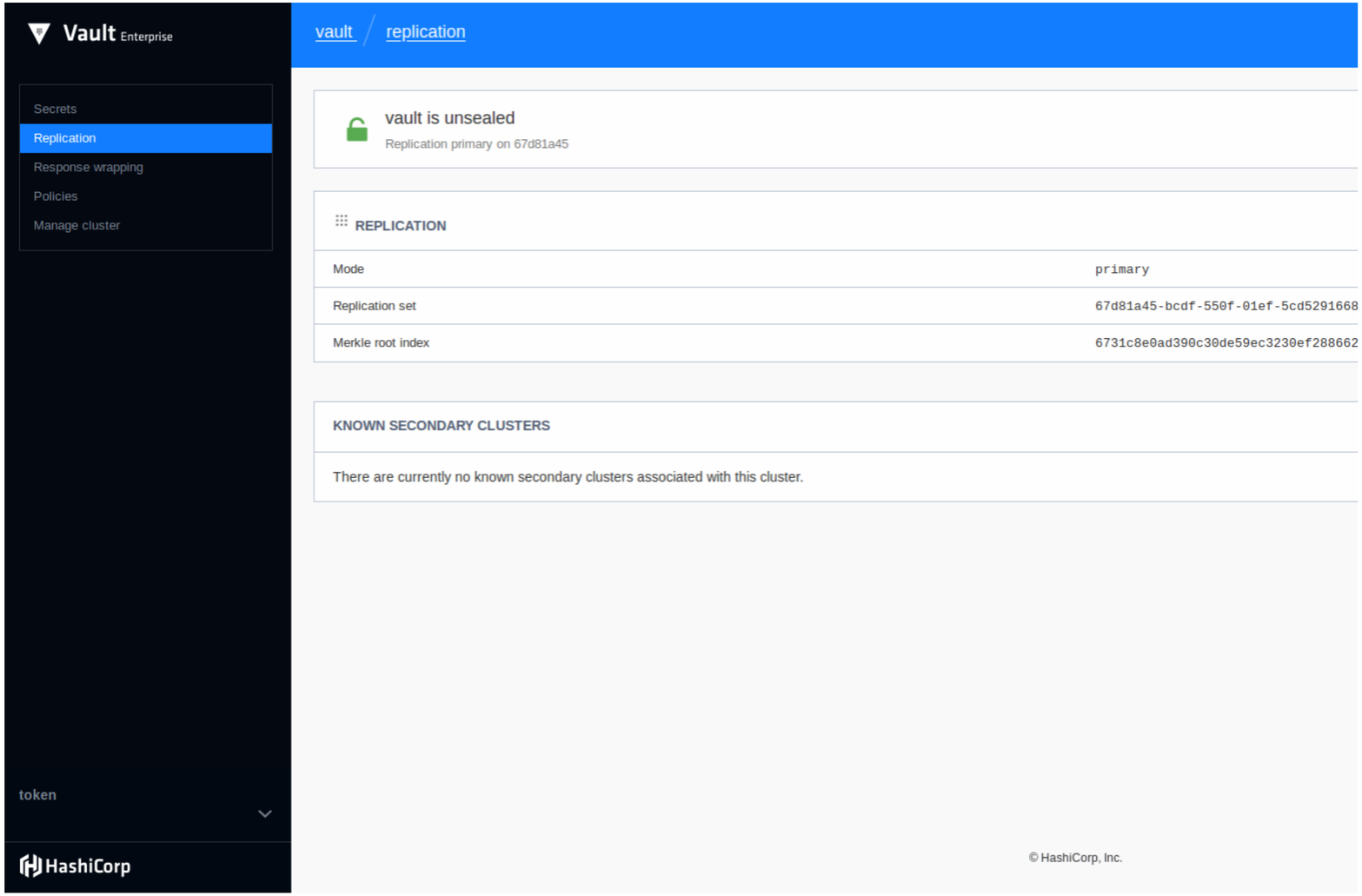


Example

Operator can manually promote a new primary



Multi-Datacenter replication for horizontal scalability

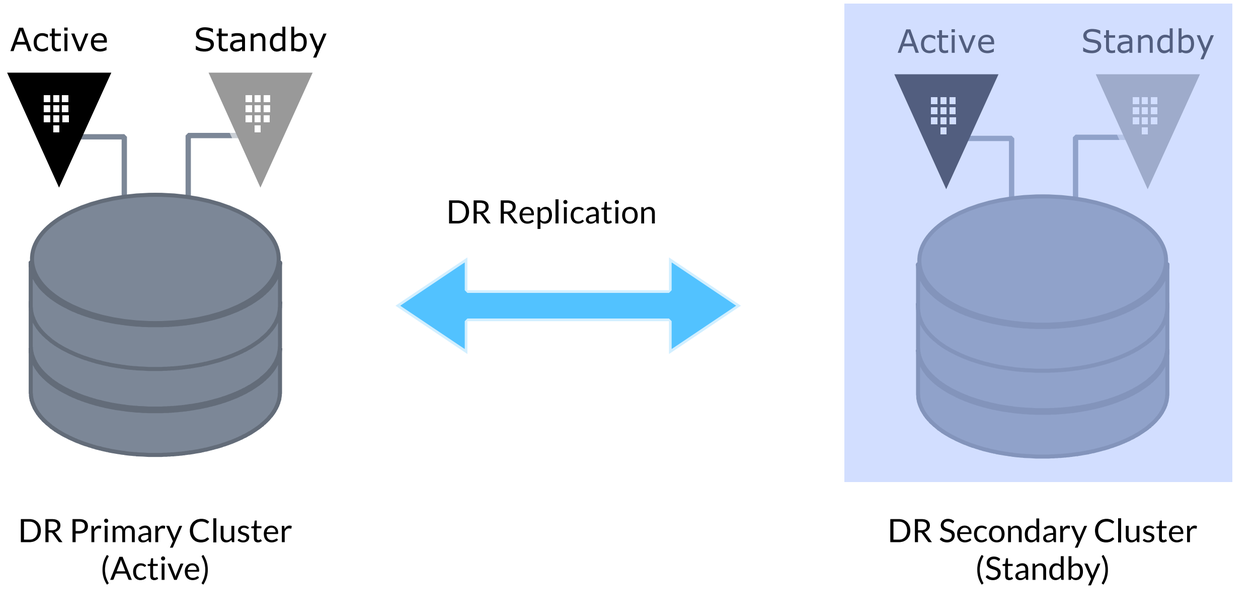


Disaster Recovery Replication

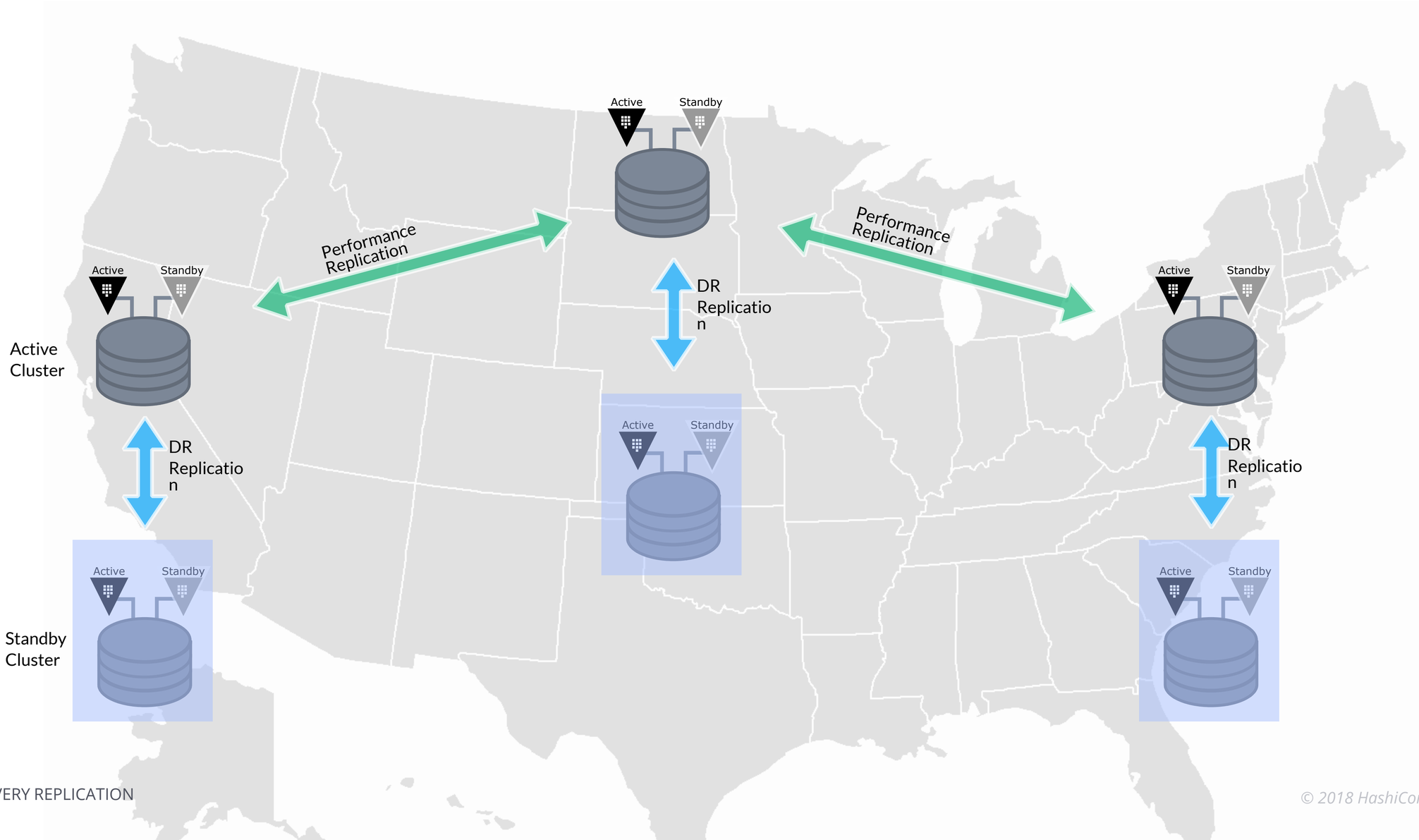
Failover to standby Vault clusters to meet Business Continuity requirements

Disaster Replication Topology

All secrets, access tokens replicated



Multi-site replication topology



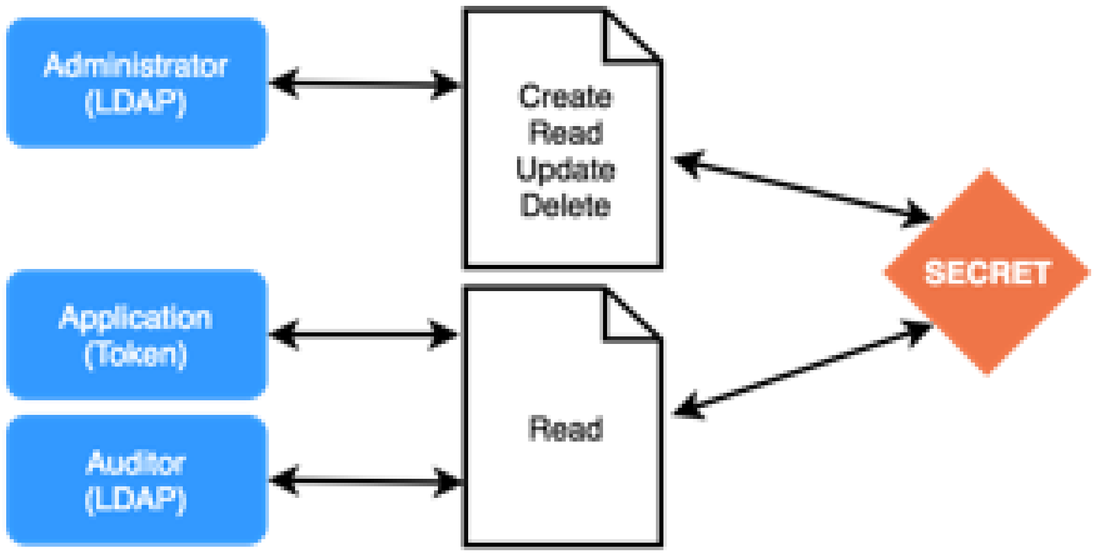
Governance

Establish policies, enforce best practices, monitor implementation.

Access Control Policies

Create and manage policies that authorize access control throughout your infrastructure and organization.

Administrators can assign varying capabilities to users and machines from multiple authentication sources.



Access Control Policy

```
path "secret/*" {
  capabilities = ["create"]
}

path "secret/foo" {
  capabilities = ["read"]
}

path "auth/token/lookup-self" {
  capabilities = ["read"]
}
```

Authentication

Flexibility in authenticating users and machines

- Token
- AppRole
- AWS
- Google Cloud
- LDAP
- GitHub
- UserPass
- Nomad
- Kubernetes
- Pivotal Cloud Foundry
- Okta
- Multi-Factor
- RADIUS
- TLS Certificates
- Custom!

HashiCorp
Nomad

Detailed Audit Logs

Vault stores a detailed audit log of all authenticated client interaction:

- Authentication
- Token creation
- Secret access
- Secret revocation

Audit logs can be sent to multiple backends to ensure redundant copies.

Sensitive information in logs is protected by HMAC.

Sentinel: Policy as Code

Sentinel policy as code engine allows organizations to enforce high level security policies. These are codified and testable, bringing devops style capabilities to security.

Some examples:

- Require multi-factor authentication for sensitive operations
- Ensure some processes are only allowed from internal networks
- Provide delegation capabilities for privileged individuals
- **Custom!** Sentinel language allows for extensible methods to meet unique needs of an organization

Sentinel Code Example

Require Ping MFA on LDAP logins, only allowed from 10.20.0.0/16

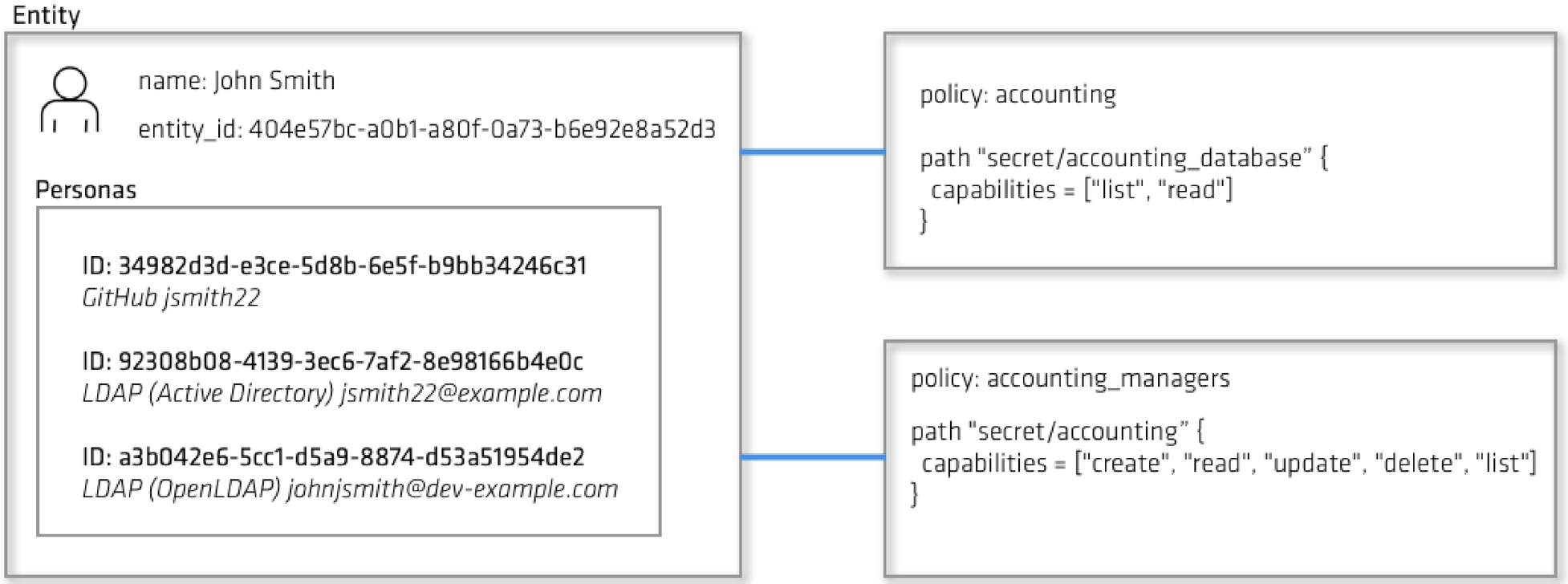
```
import "sockaddr"

# We expect logins to come only from our private IP range
cidrcheck = rule {
    sockaddr.is_contained(request.connection.remote_addr,
"10.20.0.0/16")
}

# Require Ping MFA validation to succeed
ping_valid = rule {
    mfa.methods.ping.valid
}

main = rule when strings.has_prefix(request.path, "auth/ldap/login") {
    ping_valid and cidrcheck
}
```

Unified Identity

Vault identity to unify disparate user entries and roles across a variety of auth backends to improve policy enforcement and auditability

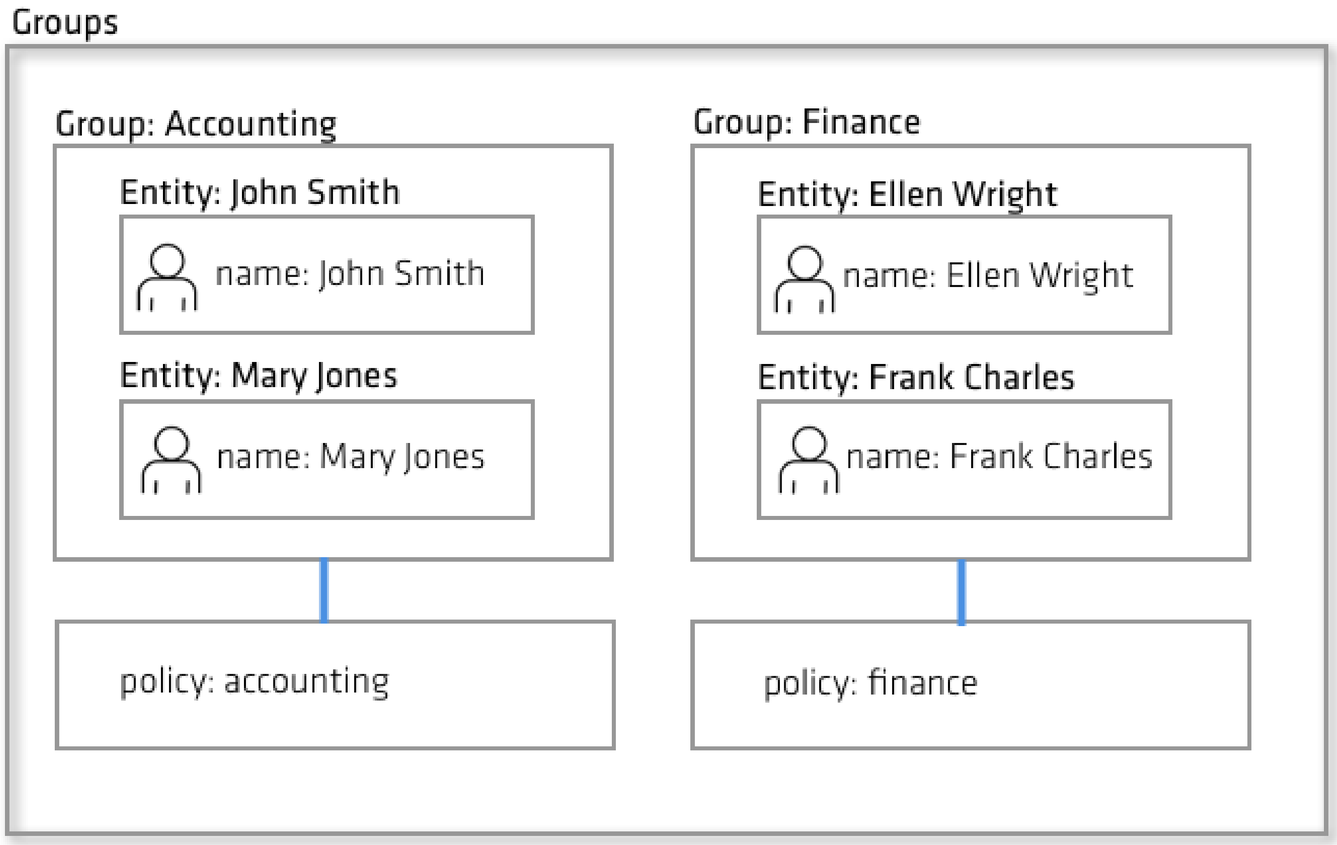
Vault Identity

Map multiple user authentication schemes to a single entity to provide for more efficient authorization management.



Vault Identity Groups

Map multiple user entities to groups for authorization management at scale.



Multi-factor Authentication

Enforce MFA workflows when accessing a secret
or a secret path

Mount Filters

Selectively Whitelist/Blacklist and activate or deactivate mounts for Secret Mounts for Performance Replication

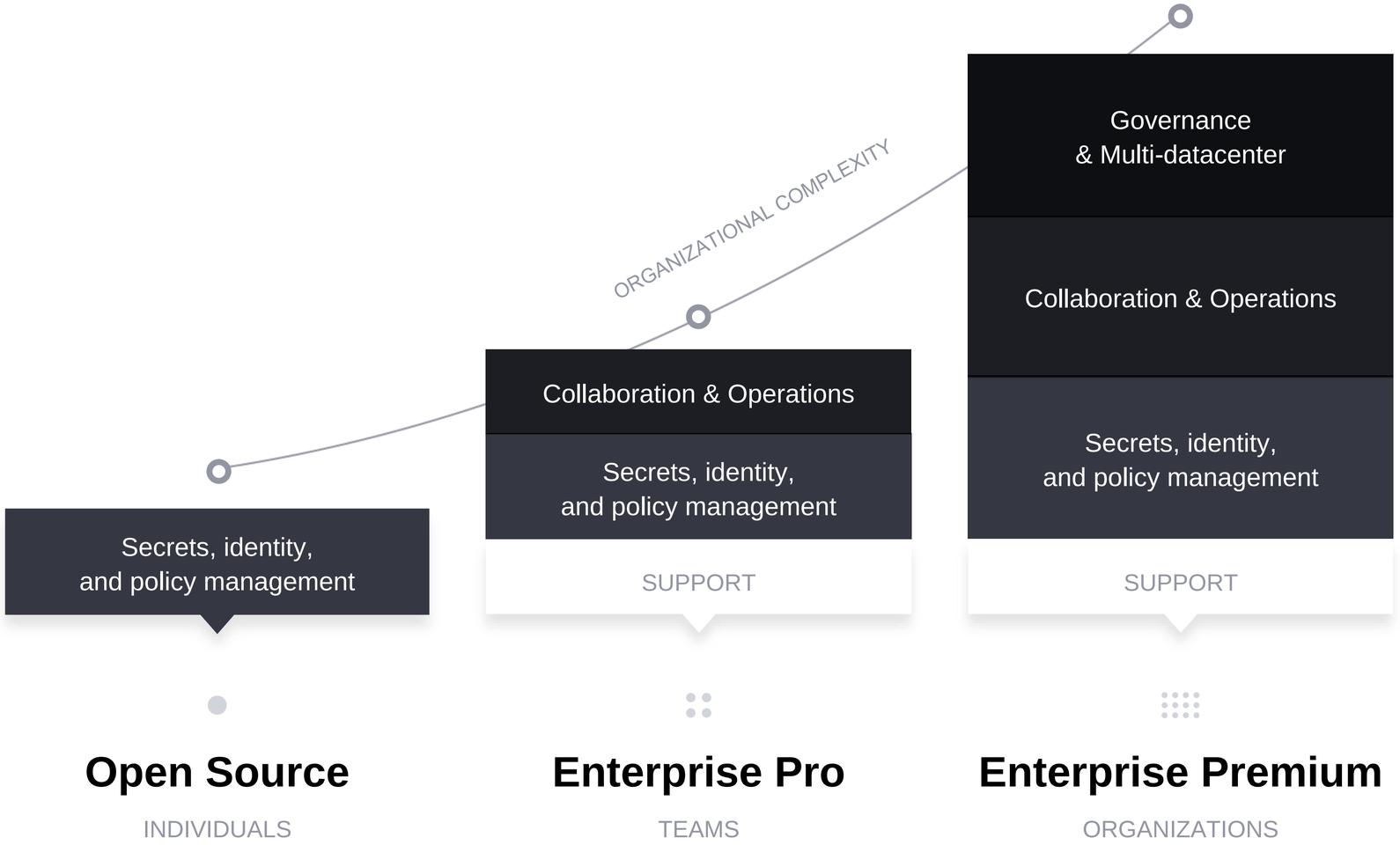
Secure Plugins

Improve the extensibility of Vault with pluggable secret and authentication backends

Open Source
and Enterprise

Vault Packages

Enterprise products build on open source to address organizational complexity.



Key Needs for Functional Areas

Security

CHALLENGE

Ensure data and access is governed by corporate security policies and enforcement can be audited to ensure data is not compromised.

KEY NEEDS

- Detailed Audit Logs
- Credential Revocation and Break-glass procedures and functionality
- Granular Access Management
- Governance Through Policies
- Minimize Exposure with Requests

Development

CHALLENGE

Develop and deploy applications to the cloud quickly and efficiently while centrally maintaining security protocol and data encryption.

KEY NEEDS

- Centrally manage secrets
- Efficiently manage secret lifecycle
- Deploy secrets across multiple environments securely without sacrificing user experience
- Centralize encryption of applications

Operations

CHALLENGE

Efficiently manage hybrid environments, access to systems, and mitigate risk, exposure, and downtime during unforeseen events.

KEY NEEDS

- Secure access of Master Keys
- Rotate Secrets programmatically
- Control Secrets through automated policy enforcement
- Easy to use interfaces and API
- DR and Business Continuity

Secrets Management Requirements

Usability

- Automation friendly, API driven
- Secrets must have a Time to Live (TTL)
- Secrets must be dynamic (created programmatically, on-demand)
- User Interface and single workflow for ease of use
- Pluggable and extensible back ends for custom integrations
- Open Source at the core for community advancement

Scalability

- Secrets must be able to be active in multiple locations
- Solution must have immediate Disaster Recovery (DR) capability
- Ability to replicate across distributed environments

Enforce & Govern

- Secrets must be auditable
- Secrets and access must be governed by repeatable automated
- Secrets must be centralized and encrypted
- Secrets must be stored within FIPS 140-2 Compliant HSM

Compare Packages

Open Source Secrets Management, Data Protection		Enterprise Pro Collaboration and operations features for teams		Enterprise Premium Governance and policy features for organizations	
Secure storage	✓	All **Open Source** Features	✓	All **Enterprise Pro** Features	✓
Vault Agent	✓	Namespaces	✓	Sentinel policy as code management	✓
Credential leasing & revocation	✓	Disaster Recovery (DR)	✓	Control Groups	✓
Detailed Audit Logs	✓			HSM Auto-unseal	✓
Secure Plugins	✓			Multi-Factor Authentication	✓
ACL Governance & Templating	✓			Sentinel Integration	✓
Encryption as a service	✓			FIPS 140-2 & Cryptographic Compliance	✓
AWS, GCP, Azure auto-unseal	✓			Read Replicas	✓
Entities and Entity Groups	✓			Replication	✓
UI with Cluster Management	✓			Replication Filters	✓

Vault
Adoption

Enterprises that trust Vault.

TECHNOLOGY

Adobe
CISCO
slack
ATLASSIAN
SAP Ariba
SAP
SPACEFLIGHT
pagerduty
APPTIO
BuildDirect
AUTODESK
Joyent
distil networks
Ultimate SOFTWARE People first

FINANCIAL

BARCLAYS
CapitalOne
credit karma
Desjardins
BRIDGEWATER
CITADEL
aire
DOW JONES
SOCIETE GENERALE

MEDIA & COMMUNICATIONS

verizon
hulu
TELUS
THOMSON REUTERS
Hootsuite
The New York Times

SOFTWARE & TECH

UNDER ARMOUR
petco

INSURANCE SERVICES

OpenCredo
Arctiq
INTELLIGENT ARCHITECTURE
McKinsey&Company
BCG
THE BOSTON CONSULTING GROUP
CONTINO

FEDERAL & PUBLIC SECTOR

U.S. DEPARTMENT OF HOMELAND SECURITY
NCBI
CN

AUTOMOTIVE

cruise
RENAULT NISSAN

About Vault

2014 Product Launch

10.4K+ Github Stars

2T+ Transactions

1M+ Monthly Downloads

250+ Enterprise Customers Worldwide

Summary

Efficiency of operators to manage secrets

Optimize secrets access and storage

Control secret access and downtime

Minimize exposure

Thank you

hello@hashicorp.com

www.hashicorp.com