Critical
TechWorks

We are changing
the way the world moves

CoP DevOps 2#
Secret management using Hashicorp Vault

Focus

- What is secret management
- Why do we need it
- What is Vault and how can it help you with secret management
- Vault features and possible use cases

Goal

- Raise awareness regarding security best practices
- Think about your approach to secret management in your project and how can you improve it incrementally
- Go and play with Vault

Why Hashicorp Vault

- Unmatched feature set
- Open Source
    * mostly !! Some closed source features aimed for specific situations
        - Multi-Datacenter replication, Two Factor Authentication, etc.
- Not vendor or framework specific

Secret management 101 1/2

- Not every critical business information is a secret
- Should be a part of your security concept
- Focus on internal threats like:
    - Rogue employees
    - Unauthorized access to secrets
    - Long living secrets

Secret management 101 *2/2*

- Auditing: Who requested credentials ? To which systems ? At what time ?
- High level of automation in changing / revoking / rolling secrets
- High entropy passwords

Secret management – Present 1/2

- Best practices are widely known
- Is usually seen as ”very” important
- Implementation is hard
- Solutions are rare

Secret management – Present 2/2

- High automation still and exception

  (as opposed to external threat mitigation measures like Firewalls, O.S. updates and container updates)

- Often neglected in favor of business-critical features

- Apps and frameworks not ready for modern secret management

Who am I and why talk about this

- Carlos Cunha

  Past :

  - Windows Sysadmin and Ops guy for more than 20 years

  Present :

  - Devops Engineer in the CTW ITOps Team

Team goal

Advertise best practices and tooling for development teams at CTW

Typical project

1/2

- We pass secrets via environment variables
- We read values from Kubernetes secrets (or any other ”secure” way)
- We have role-based access “all figured out”
- Changing and updating passwords is a manual process “for now”

Typical project

2/2

- Yeah: audit is something we are still looking into
- No, we can not confidently say who has the password for DB xyz
- We have role-based access “all figured out”
- Changing and updating passwords is a manual process “for now”
- No, we do not change all passwords if an employee leaves the company **
- Revoking credentials is not something we currently supported

Question

Who , currently has production credentials on his laptop / git repo / confluence ?

- Access Tokens
- API Keys
- DB credentials
- SSH Keys without passphrases

Vault

Auth-n + Auth-z (Authentication + Authorization)

Vault - Summary

1/2

- Secures, stores and tightly controls
  - Tokens
  - Passwords
  - API Keys
  - Other secrets

Vault - Summary

- Handles
  - Leasing
  - Key revocation
  - Key rolling
  - Auditing
- Provides an API for all operations

Vault

Engines – Authorization - Databases	
Cassandra	ElasticSearch
InfluxDB	HanaDB
MongoDB	MSSQL
MySQL / MariaDB	PostgreSQL
Oracle	Custom

Vault

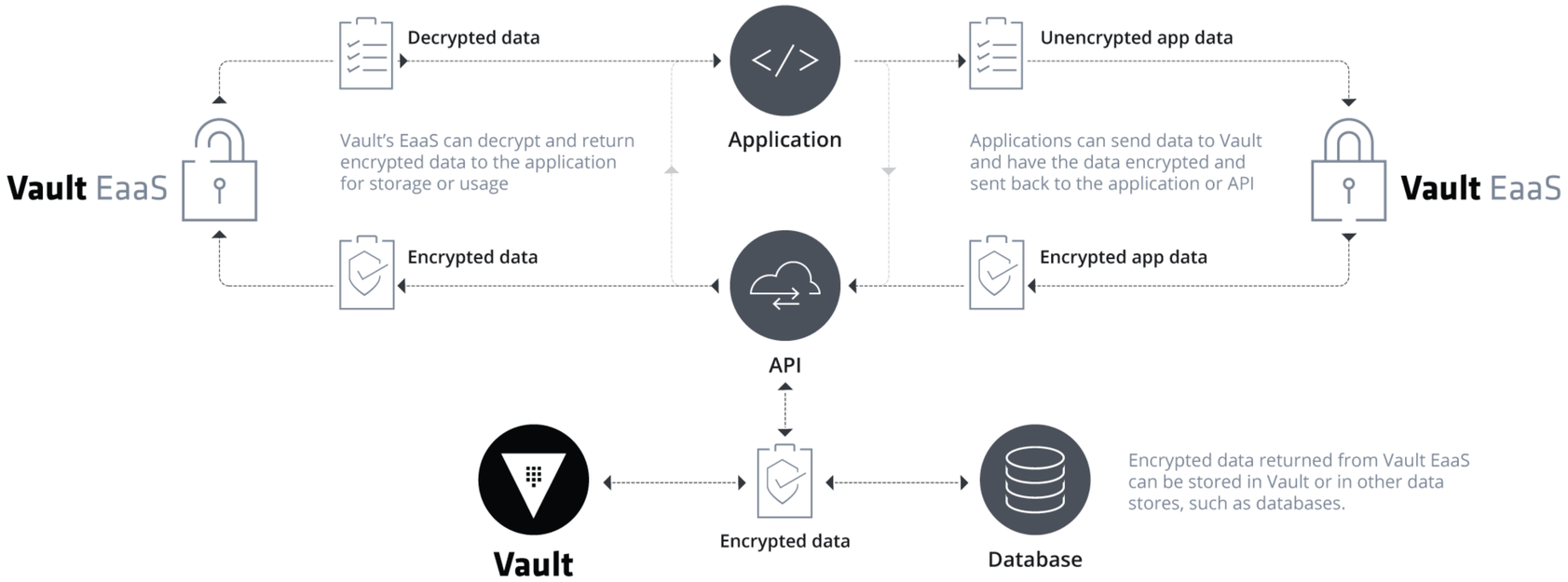
Auth Backends	
Token	GitHub
AliCloud	MFA
Cloud Foundry	Okta
AWS	Tokens
Oracle Cloud Infrastructure	RADIUS
Google Cloud	TLS Certificates
Azure	Username & Password
LDAP	AppRole
JWT/OIDC	
Kubernetes	

Vault

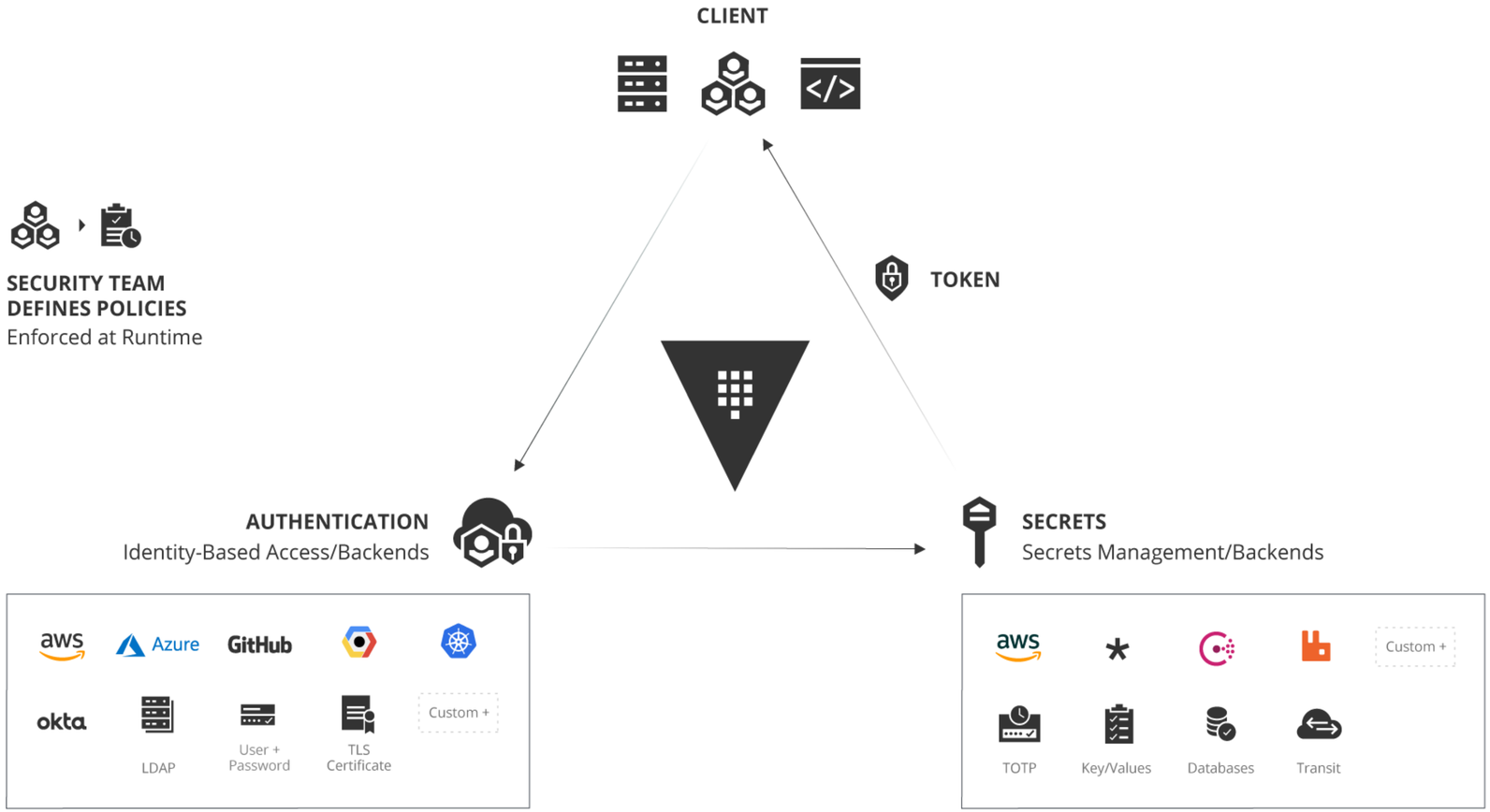
Engines - Authorization	
Active Directory	Nomad
AliCloud	PKI (certificates)
AWS	RabbitMQ
Azure	SSH
Consul	TOTP
CubbyHole	Transit
Google Cloud	**Databases**
Google Cloud KMS	
Identity	
Static Secrets (Key – Value)	

Encryption as a Service

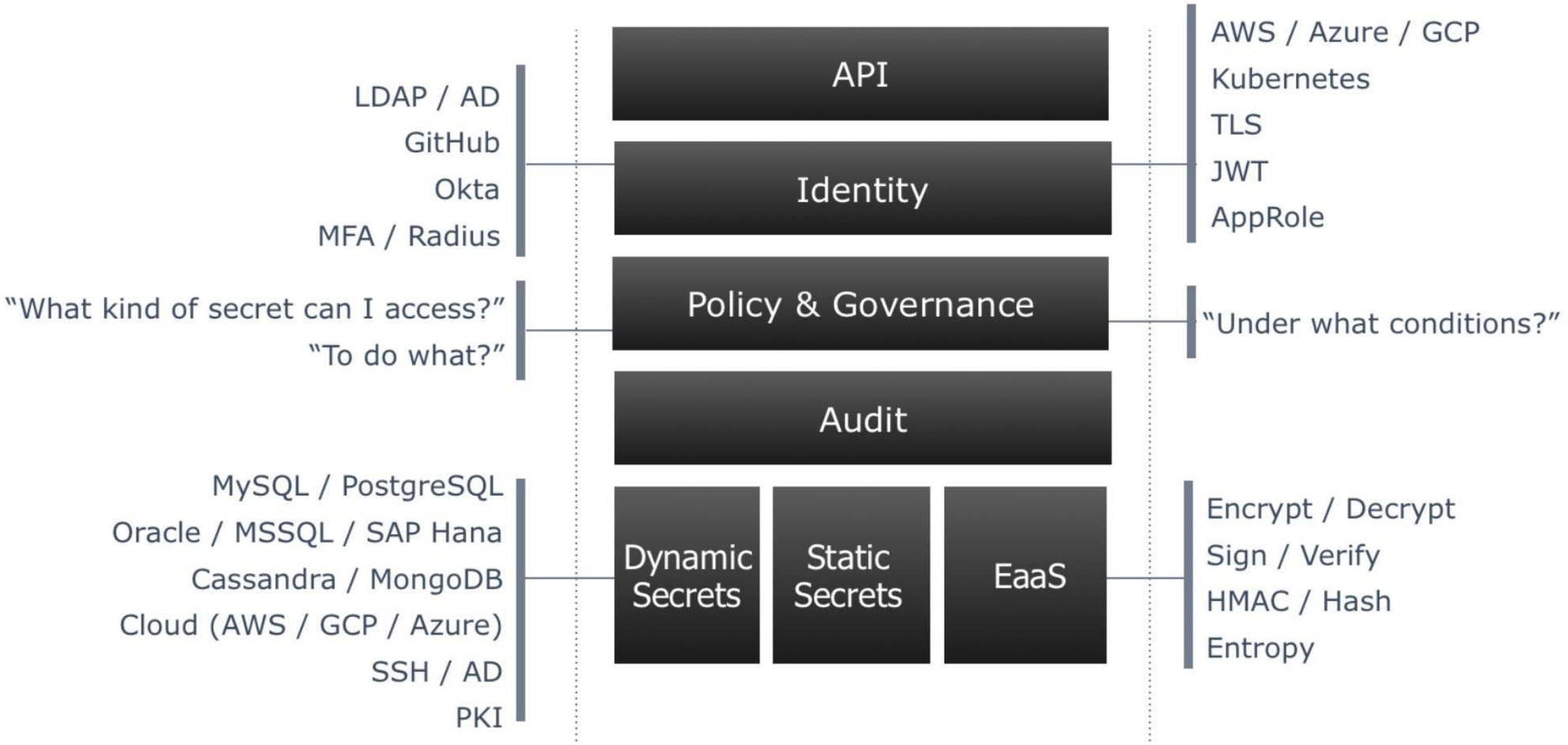
HashiCorp Vault



Vault



Vault

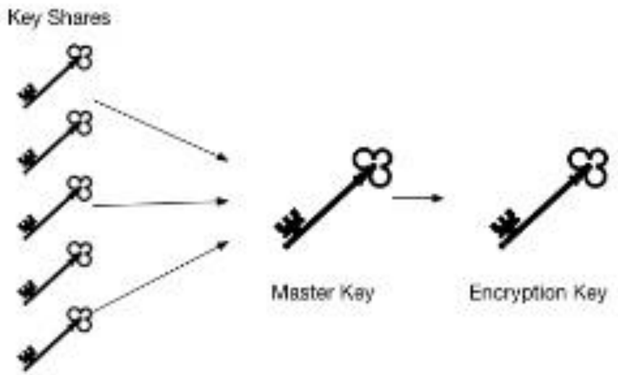


Vault init and operation

HashiCorp Vault

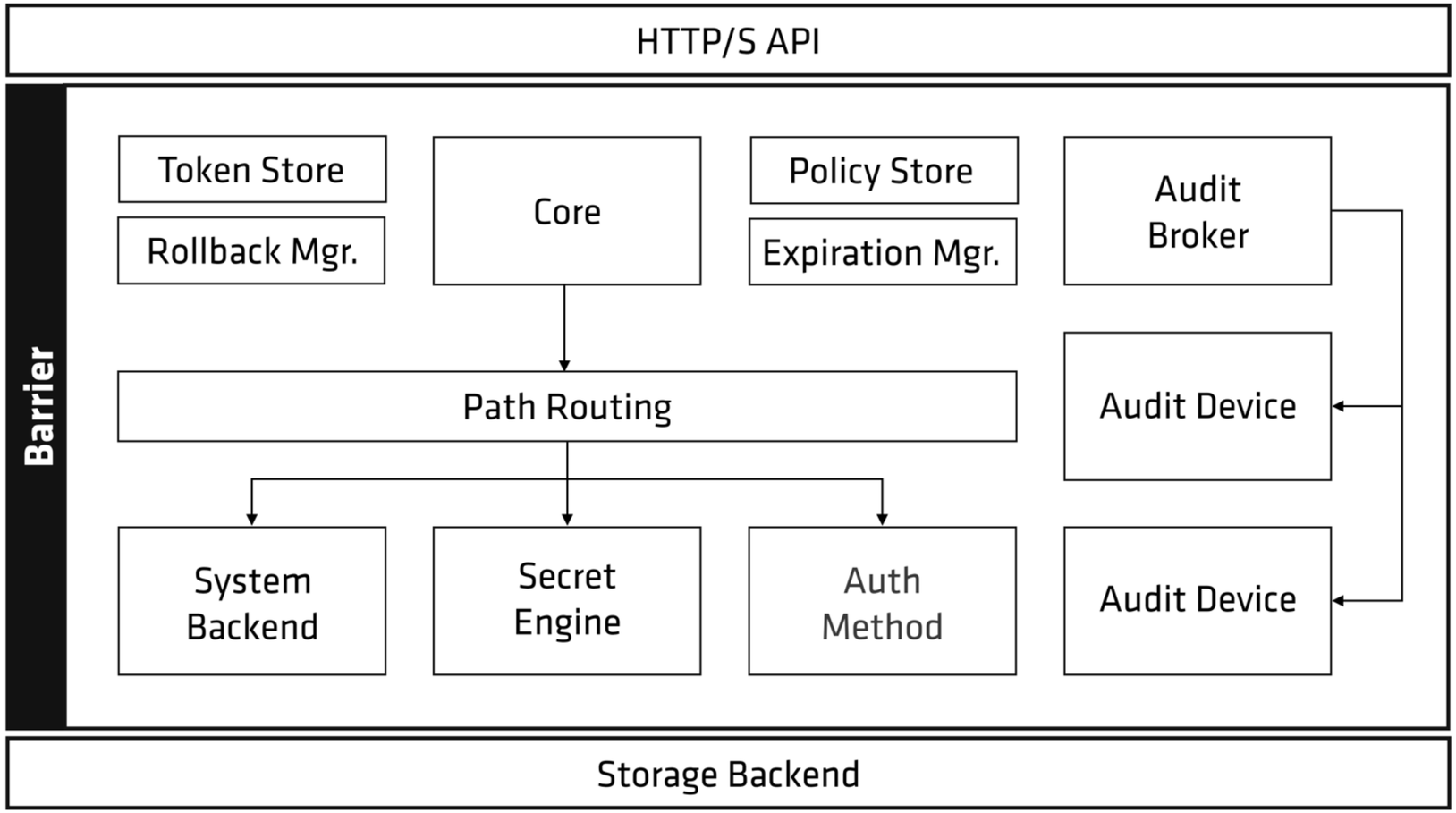
SHAMIR SECRET SHARING

- Protect Encrypt Key with Master Key
- Split Master Key into N shares
- T shares to recompute Master
- Quorum of key holders required to unseal
  - Default N:5, T:3



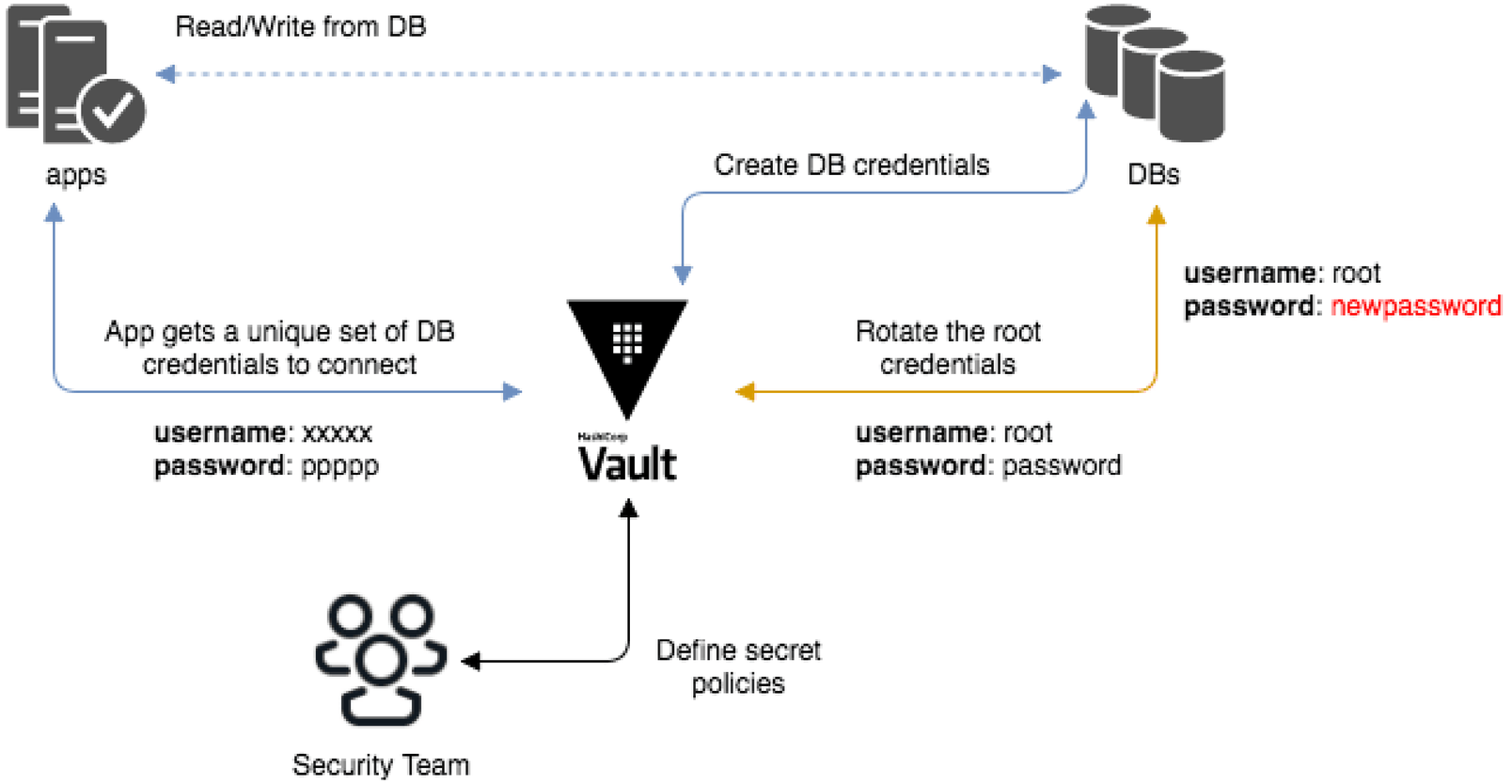
HashiCorp

Vault architecture



Demo 1 – Vault Basics

Credential generation and rotation



Demo 2 – Database Engine

Demo 1 – SSH CA Engine

Critical TechWorks

WWW.CRITICALTECHWORKS.COM