# VAULT

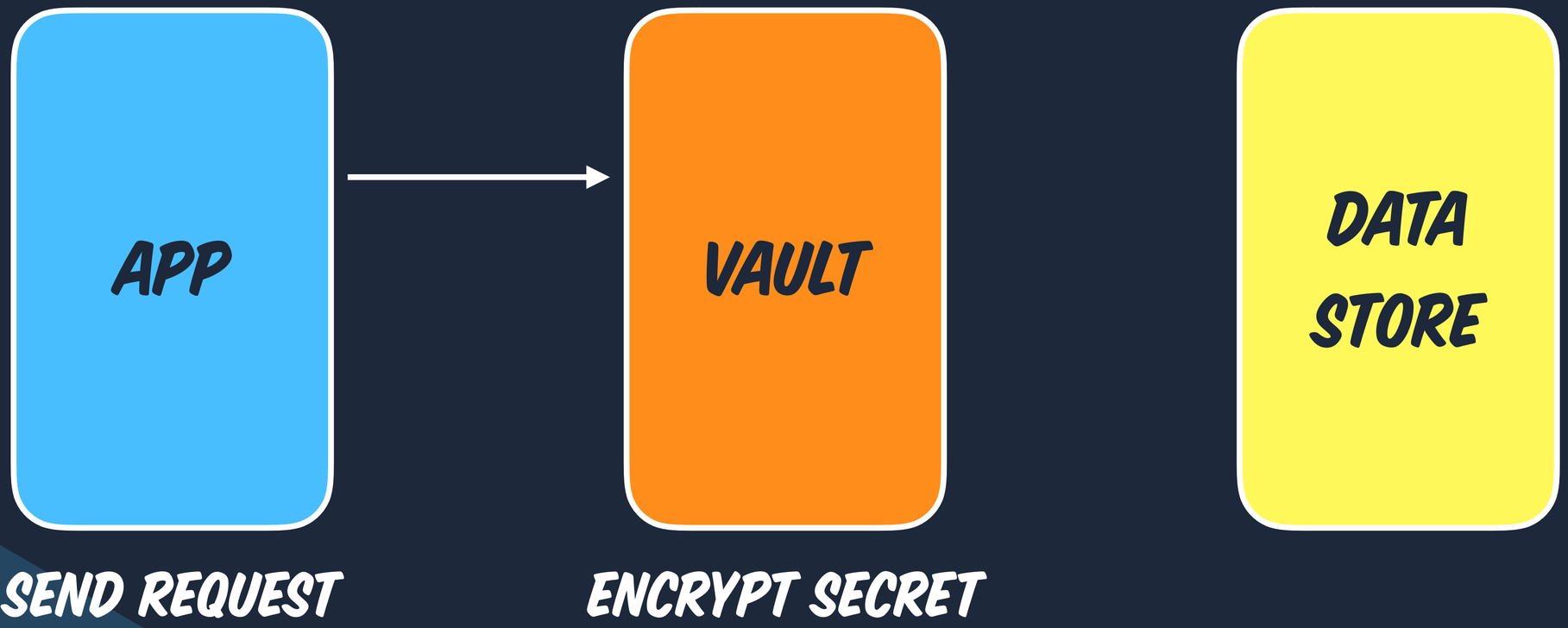
## SECURING YOUR SECRETS

# WHAT IS VAULT?

# BASIC ARCHITECTURE

# BASIC ARCHITECTURE

## WRITE SECRET



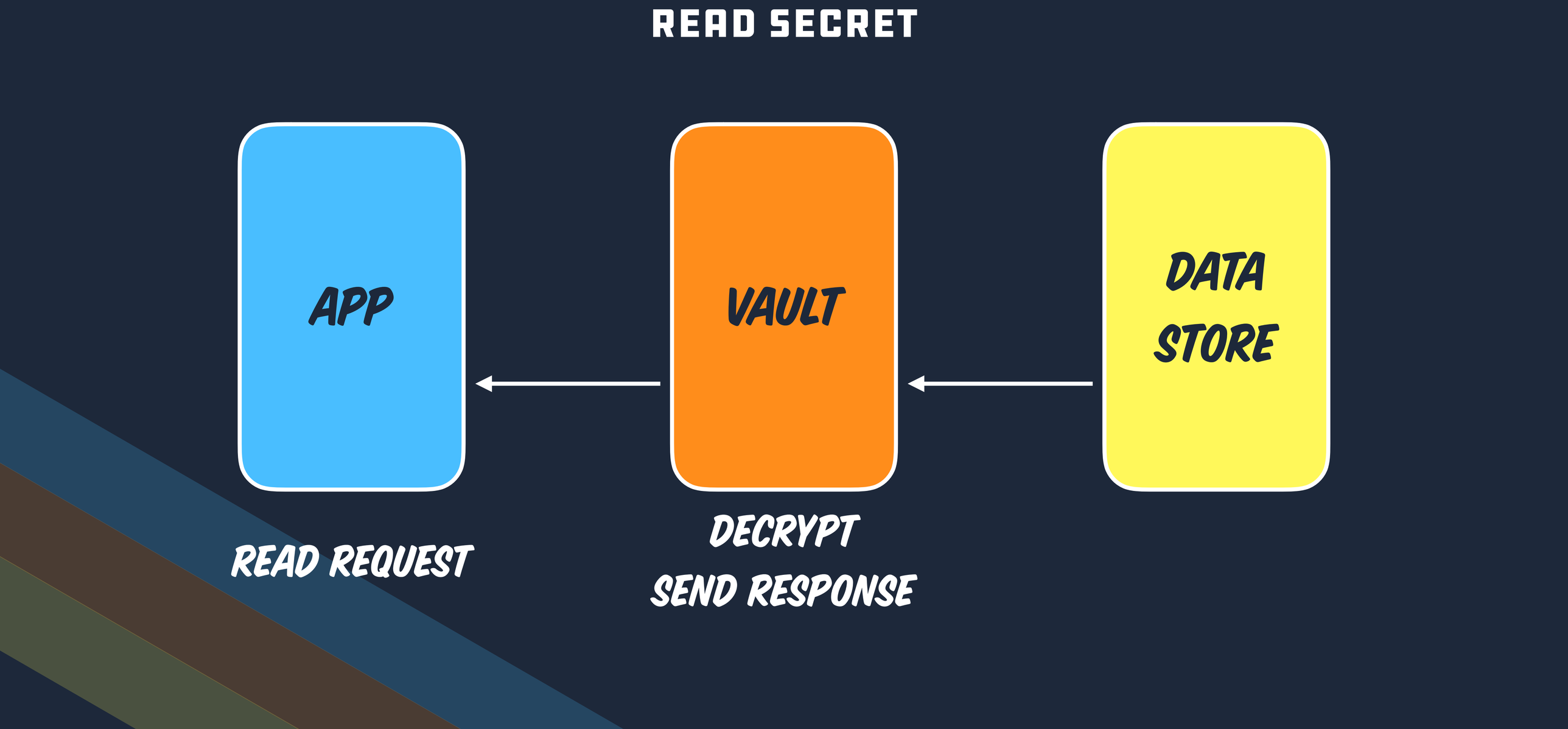
# BASIC ARCHITECTURE

## WRITE SECRET

# BASIC ARCHITECTURE

## READ SECRET

# BASIC ARCHITECTURE



# BACKENDS

## AUTH BACKEND

- TOKENS
- USERNAME / PASSWORD
- APPROLE
- AWS
- LDAP
- GITHUB
- TLS CERTS

## SECRET BACKEND

- GENERIC
- AWS
- MYSQL
- CUBBYHOLE
- RABBITMQ
- SSH
- PKI

# AUTH BACKENDS

AUTH BACKENDS ARE THE COMPONENTS IN VAULT THAT PERFORM AUTHENTICATION AND ARE RESPONSIBLE FOR ASSIGNING IDENTITY AND A SET OF POLICIES TO A USER.

# AUTH BACKENDS

## TOKENS

GENERATED ON BEHALF OF A USER BY A HUMAN OR SOME OTHER PRIVILEGED APPLICATION

THIS DOES NOT PROVIDE ANY FORM OF AUTHENTICATION.
THE TOKEN REPRESENTS AUTHORIZATION WITH AN ASSUMED OTHER FORM OF AUTHENTICATION

# AUTH BACKENDS

## TOKENS

```
curl -X "POST" "https://vault:8200/v1/auth/token/create" \
     -H "X-Vault-Token: 5ceed009-dddd-46ee-2ccc-61235dbdf0f16b" \
     -H "Content-Type: application/json" \
     -d $'{
        "num_uses": "0",
        "display_name": "\\"some cool service\\"",
        "policies": [
          “my-cool-service-dev“
        ],
        "TTL": "1h"
      }'
```

# AUTH BACKENDS

## TOKEN PARAMETERS OF NOTE

| | |
|---|---|
| policies | ACCESS CONTROL. WHAT YOU CAN AND CAN'T DO |
| renewable | IS THIS TOKEN RENEWABLE |
| ttl | HOW LONG THE TOKEN LIVES UNLRESS RENEWED |
| explicit_max_ttl | NOT RENEWABLE PAST THIS TIME |
| display_name | NAME FOR TOKEN |
| num_uses | HOW MANY TIMES IT CAN BE USED BEFORE INVALID |

# AUTH BACKENDS

## APPROLE

# AUTH BACKENDS

## AWS

# SECRET BACKENDS