Who’s managing the credentials for your managed database?

Dewan Ahmed

Note: These slides have been modified from their original versions which were dedicated for a live audience.

THANKS TO ALL OUR SPONSORS!

BizStream

ATOMIC OBJECT

THE C2 GROUP

KL&A
KUNZ, LEIGH AND ASSOCIATES

{M} MICHIGAN SOFTWARE LABS

WEST MICHIGAN TECH TALENT

TEKTON®

KFORCE℠

Leading EDJE

Mutually human

Scout APM

Sweetwater®
Music Instruments & Pro Audio

Hi, I’m Dewan

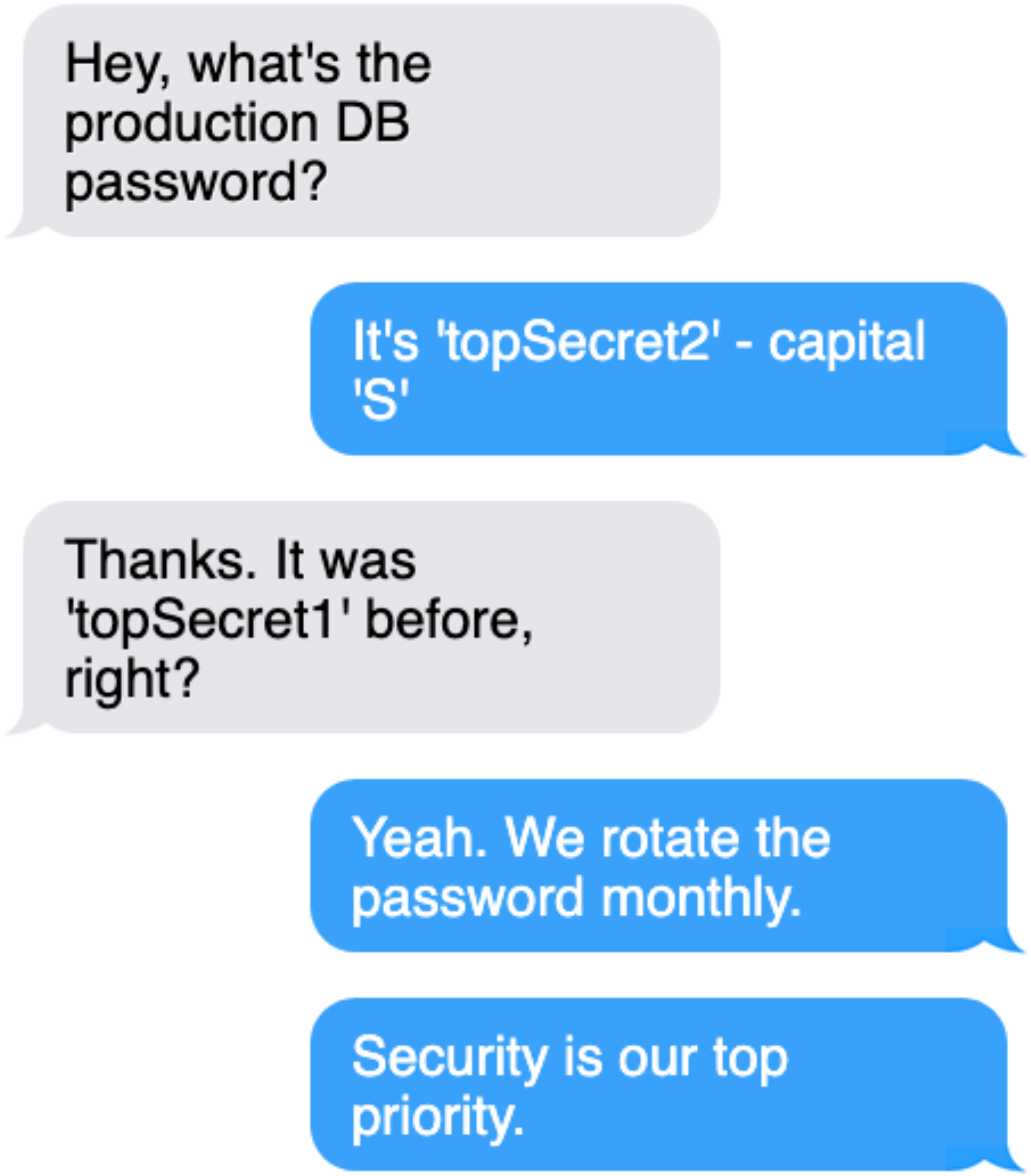
- Senior Developer Advocate, Aiven
- New Brunswick, Canada
- Focus on app/data infrastructure
- Pro bono career coach

@aiven_io

in/diahmed | @DewanAhmed

Agenda

- Managed Database
- Database Security
- Dynamic Credentials
- Choosing the Right Tool
- Demo



Hey, what's the production DB password?

It's 'topSecret2' - capital 'S'

Thanks. It was 'topSecret1' before, right?

Yeah. We rotate the password monthly.

Security is our top priority.

Managed Database

- Managed host
- Regular updates/patches
- Orchestrate; not click-ops
- Backups and disaster recovery

Database Security

- Physical access
- Host access
- SQL injection attack
- Data loss/backup
- Database access

80%

of data breaches are the result of poor or reused passwords.

* 2021 Data Breach Investigations Report: https://www.verizon.com/business/resources/reports/dbir

Database Access

- Authentication
- Authorization
- Auditing

Secret Sprawl

- You don’t know where are all the secrets stored
- You have limited control over how these secrets are used
- What do you do when there’s a breach? Do you have a strategy about rotating these secrets?

Applications are bad at keeping secrets

Do you really want your engineering team to write their own encryption-as-a-service??

The SAME database password since FOREVER

Dynamic Credentials

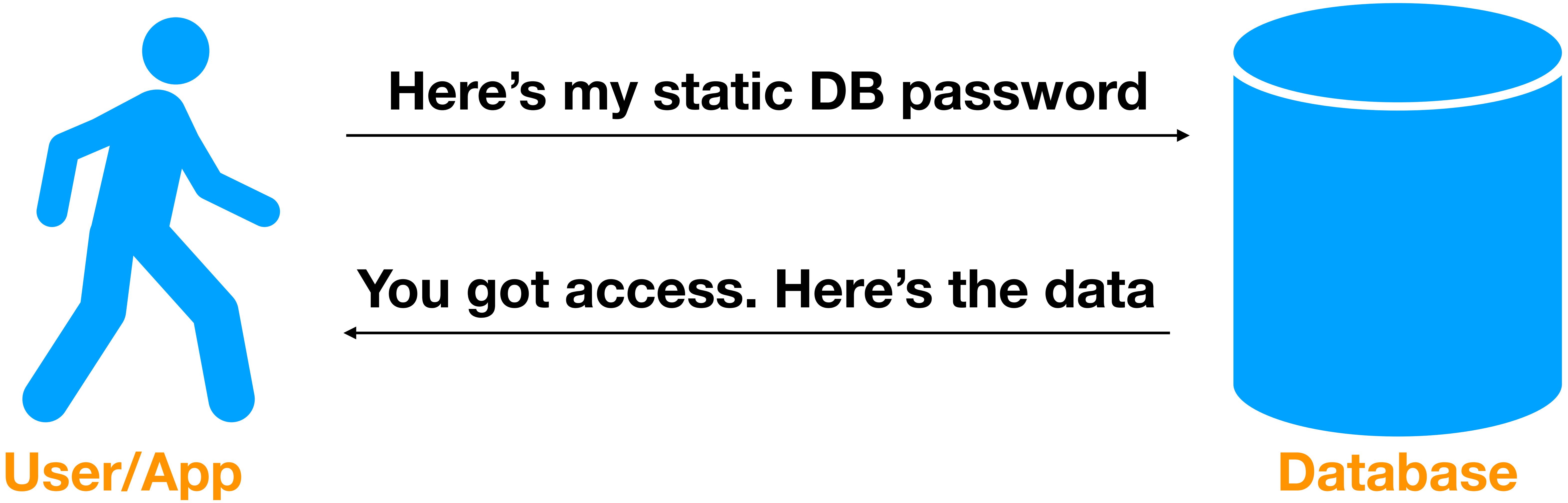
- Generated on demand
- Time-bound access
- Can be audited

Choosing the right tool

- Flexibility
- Integrations/providers
- Encryption
- Automatic expiry of tokens/secrets
- Password revocation

Why HashiCorp Vault?

- Interact using HTTP API, CLI, or UI
- Secret engines for cloud providers, databases, and more
- Encryption-as-a-service
- Store long-lived secrets
- Manage/revoke leases on secrets
- Manage access to secrets using ACLs
- Generate dynamic X.509 certificates (PKI)
- Built-in high availability

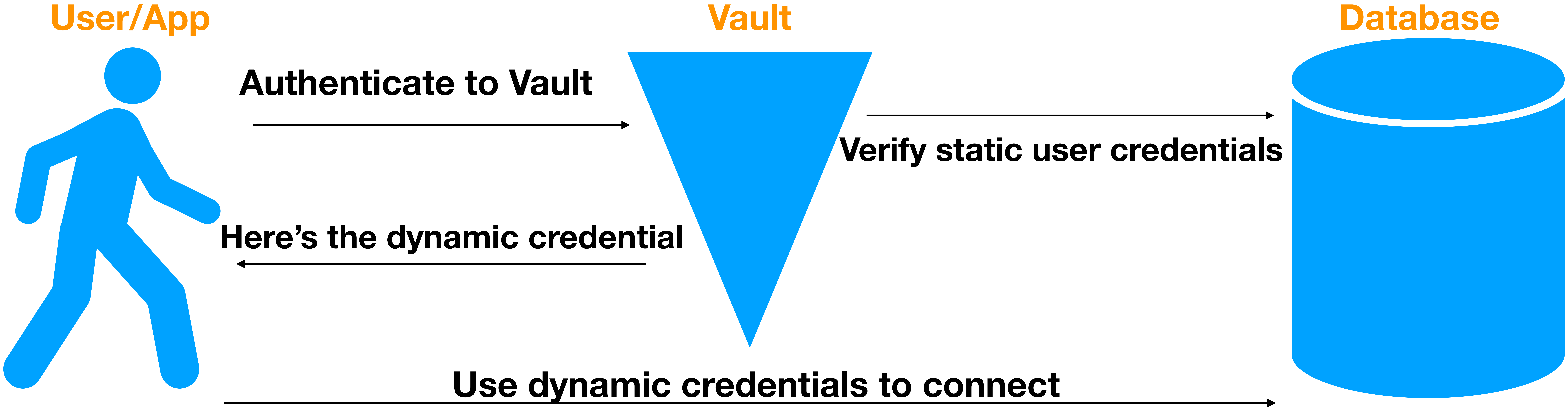


Here's my static DB password

You got access. Here's the data

User/App

Database



User/App

Vault

Database

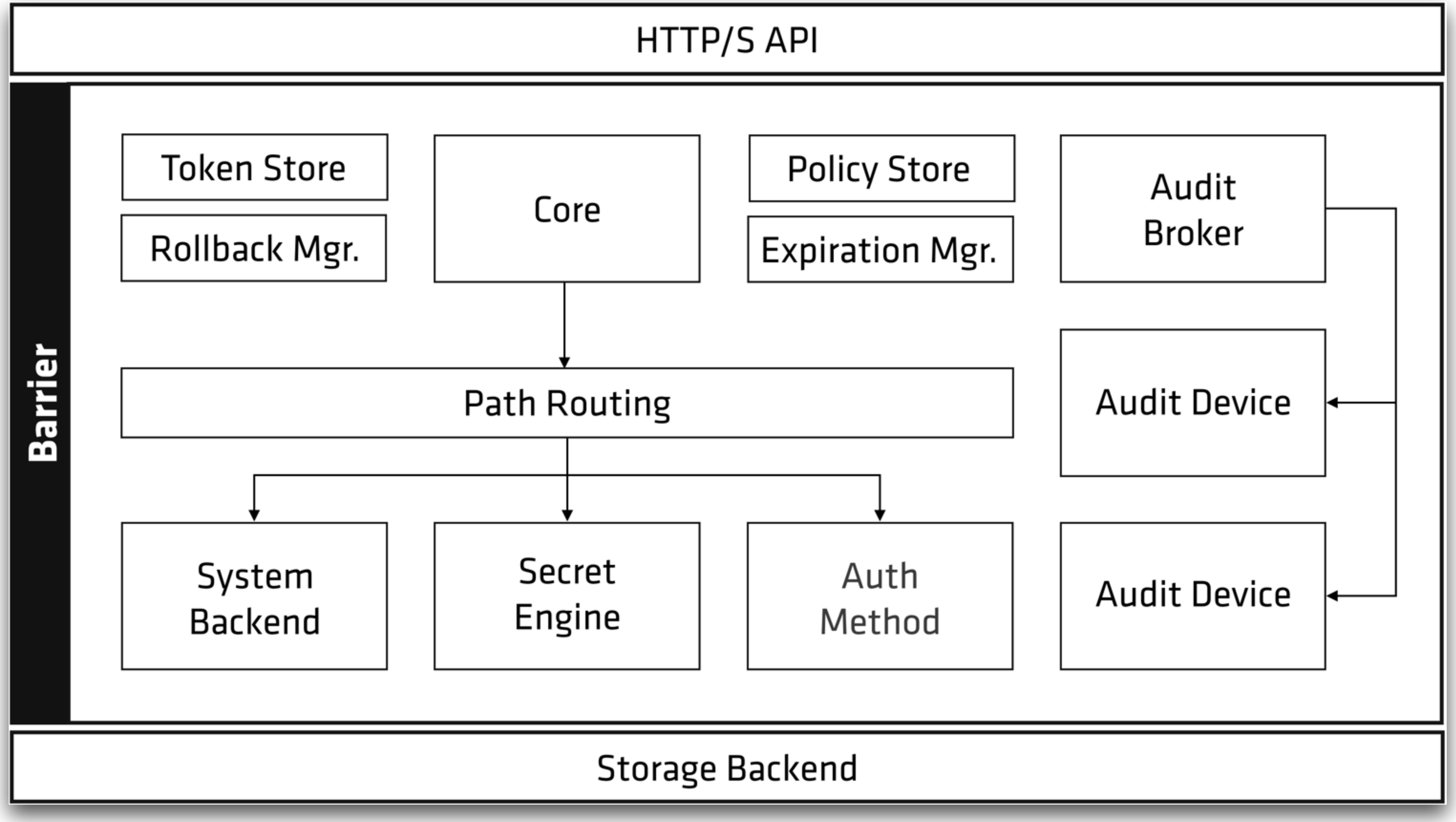
Authenticate to Vault

Verify static user credentials

Here’s the dynamic credential

Use dynamic credentials to connect

Vault - Architecture



Source: https://www.vaultproject.io/docs

Demo Time

There was a demo in this slide.

https://aiven.io/blog/secure-your-db-with-vault to follow the demo

SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.

Do you have a break glass procedure?

Thank you for your time.

Further learning/resources:

- Aiven for PostgreSQL: https://aiven.io/postgresql
- Aiven Developer Docs: https://developer.aiven.io
- Blog (includes demo): https://aiven.io/blog/secure-your-db-with-vault
- HashiCorp Vault Docs: https://vaultproject.io

Questions?

dewan@aiven.io