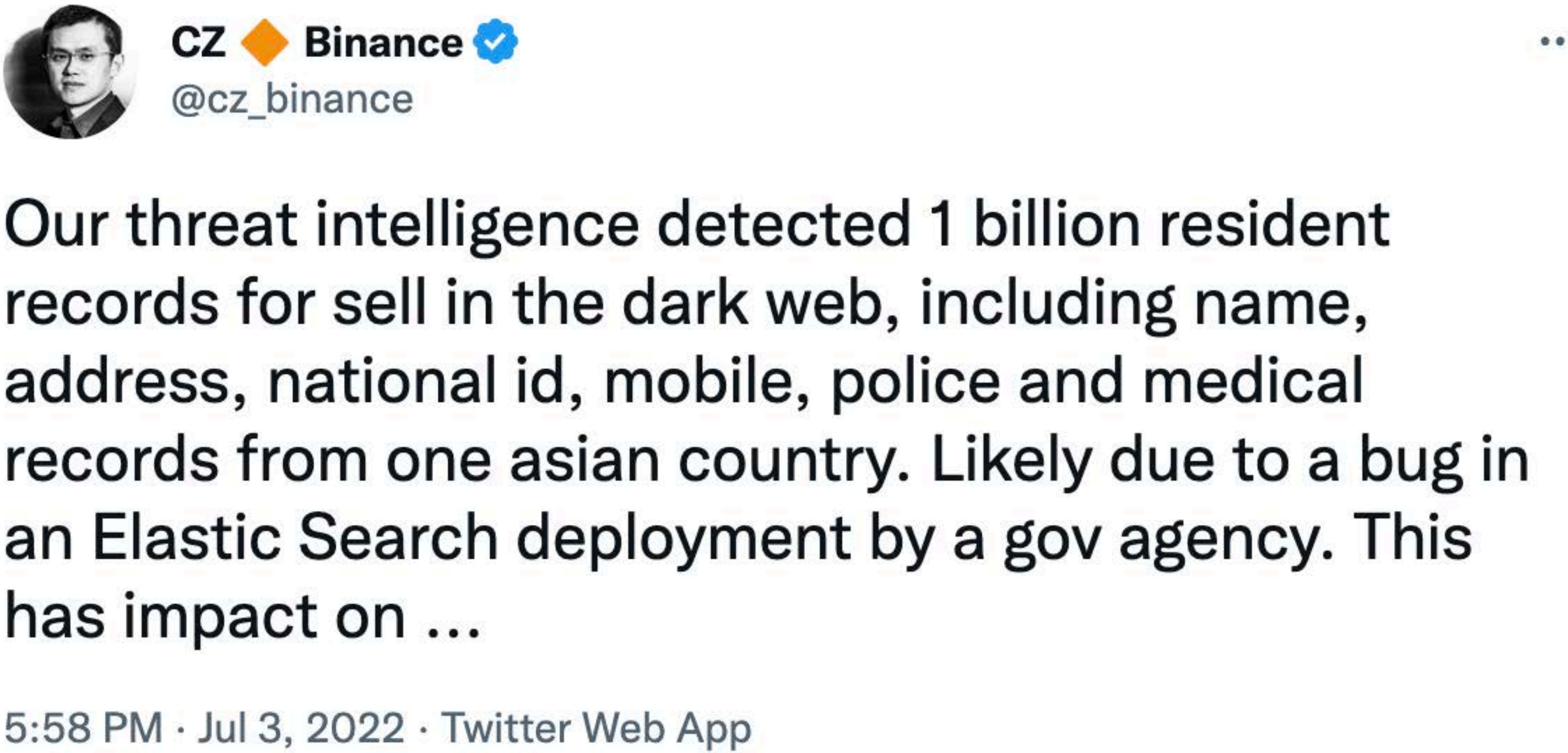
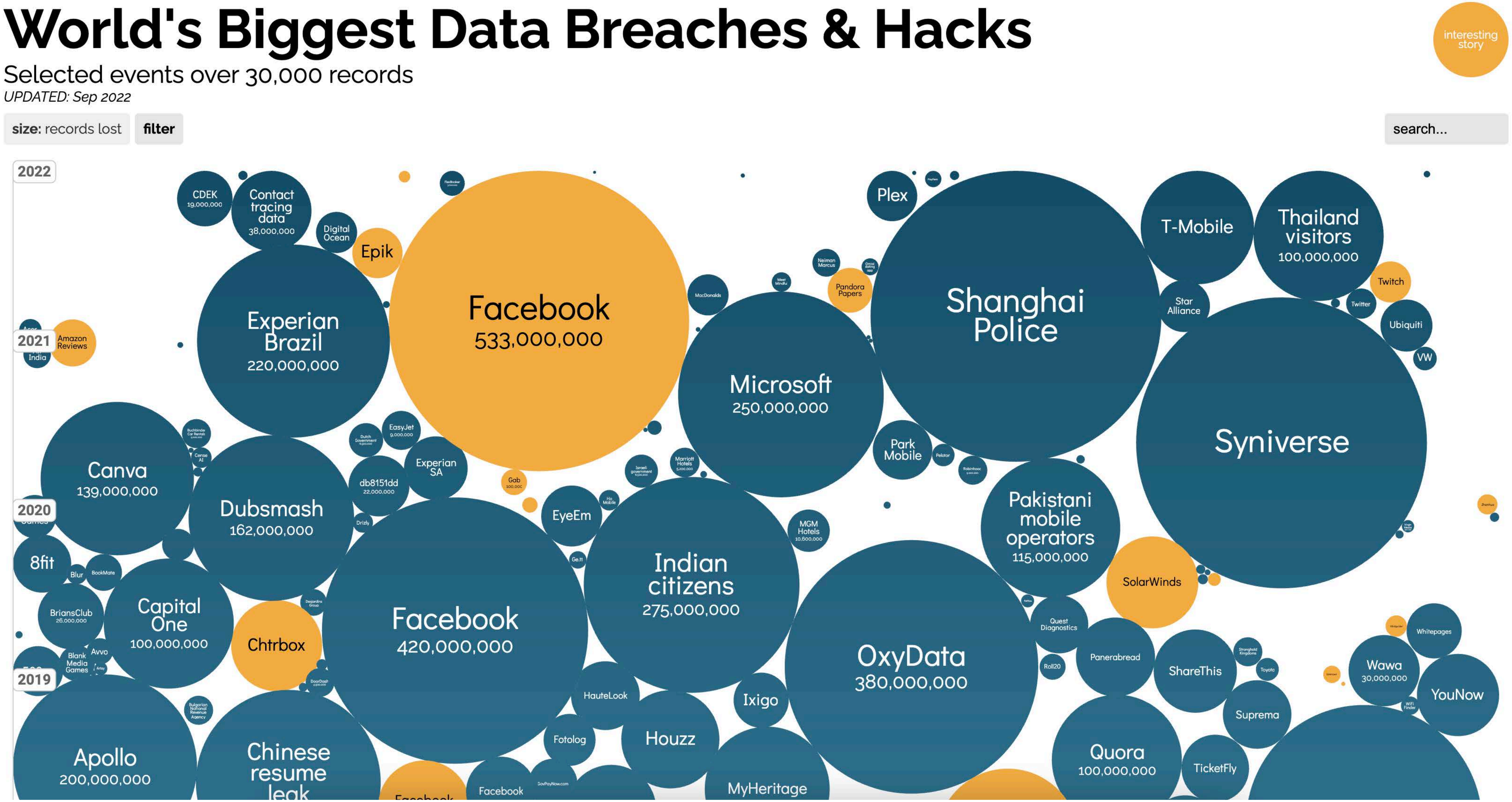


CZ 🔶 Binance
@cz_binance

Our threat intelligence detected 1 billion resident records for sell in the dark web, including name, address, national id, mobile, police and medical records from one asian country. Likely due to a bug in an Elastic Search deployment by a gov agency. This has impact on ...

5:58 PM · Jul 3, 2022 · Twitter Web App



World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Sep 2022

Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Who’s managing the credentials for your data infrastructure?

Dewan Ahmed

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

Data Infrastructure Security

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

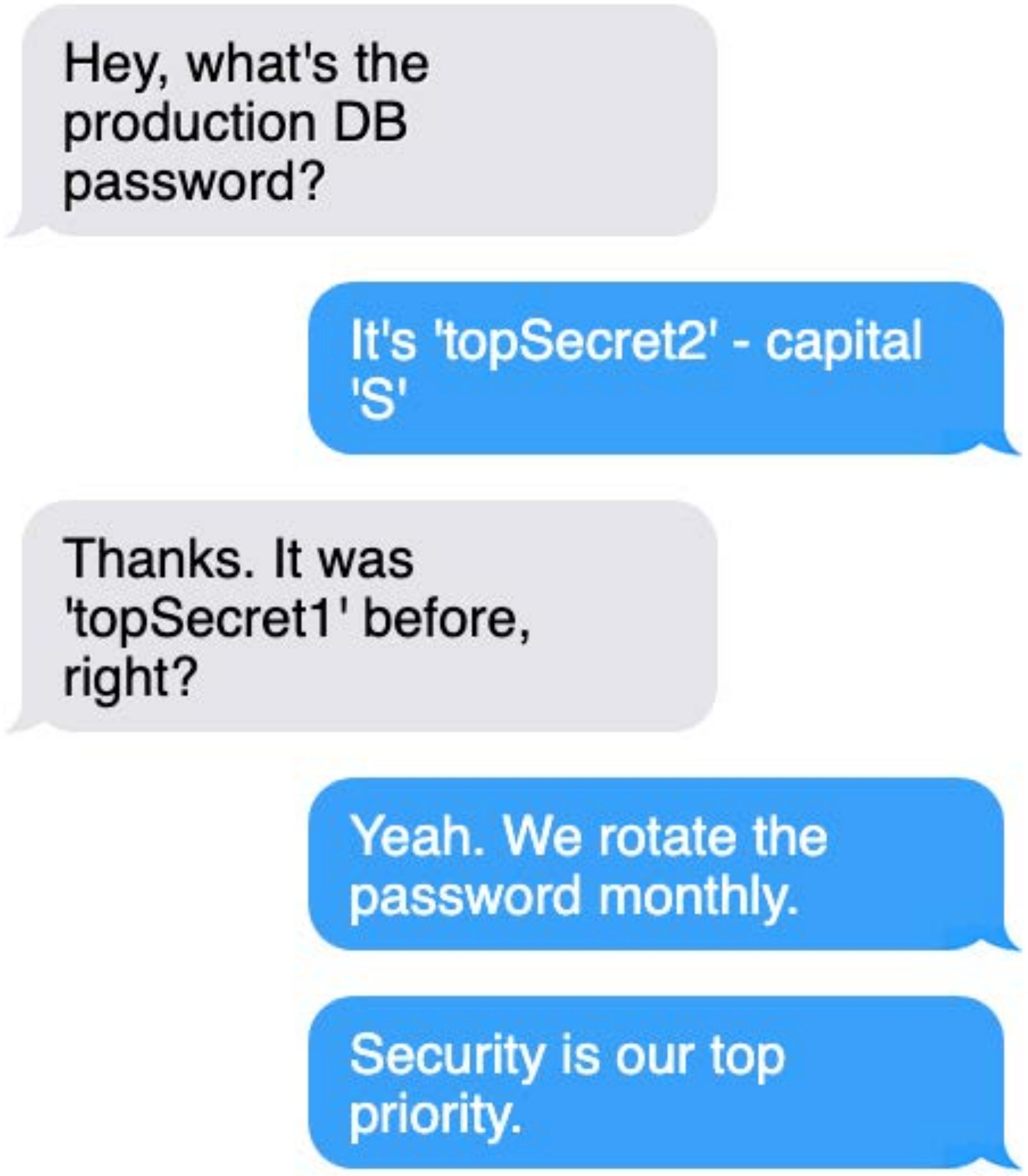
80%

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

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

Agenda

- Problem: Database access
- Solution: 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.

Secret Sprawl

CUSTOM CRYPTOGRAPHY
ENCRYPTION AS A SERVICE
JAKE-CLARK.TUMBLR
imgflip.com

The SAME database password since FOREVER

Applications keeping secrets
MUST HOLD IT IN....

AAA model for Apache Kafka®

Authenticate your Kafka clients to brokers

- SSL - Secure Sockets Layer
- SASL - Simple Authorization Service Layer

AAA model for Apache Kafka®

Using an Access Control List (ACL), your Kafka cluster decides what a user can and can’t do.

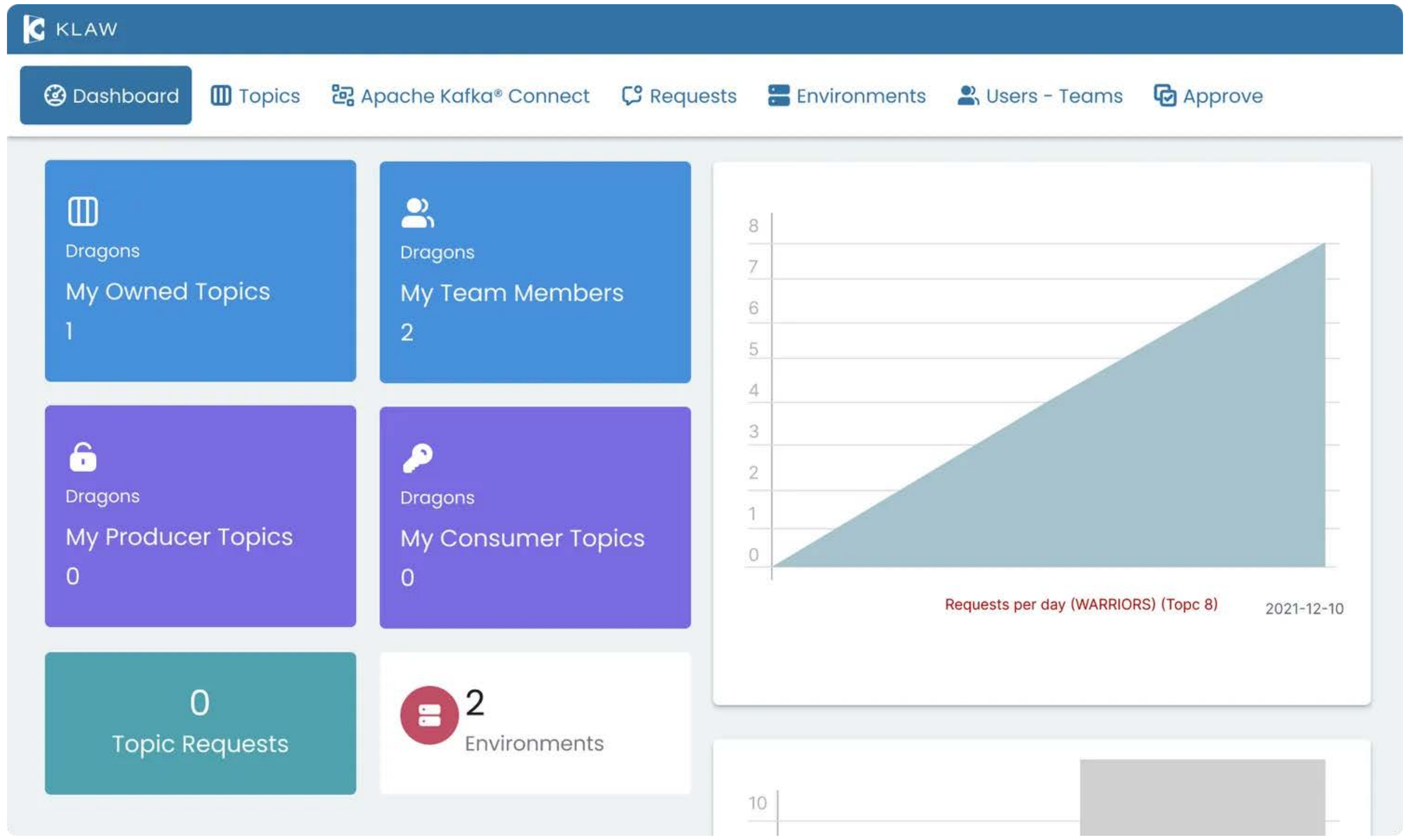
AAA model for Apache Kafka®

Apache Kafka audit logs:

- assess security risks in Kafka clusters
- sink connectors to move your audit log data

Klaw for Apache Kafka® governance

- Open-source web based data governance toolkit
- An audit layer on top of Apache Kafka
- Manage topics, ACLs, and schemas
- Log of all events related to configuration changes



Dragons
My Owned Topics
1

Dragons
My Team Members
2

Dragons
My Producer Topics
0

Dragons
My Consumer Topics
0

0
Topic Requests

2
Environments

https://www.klaw-project.io

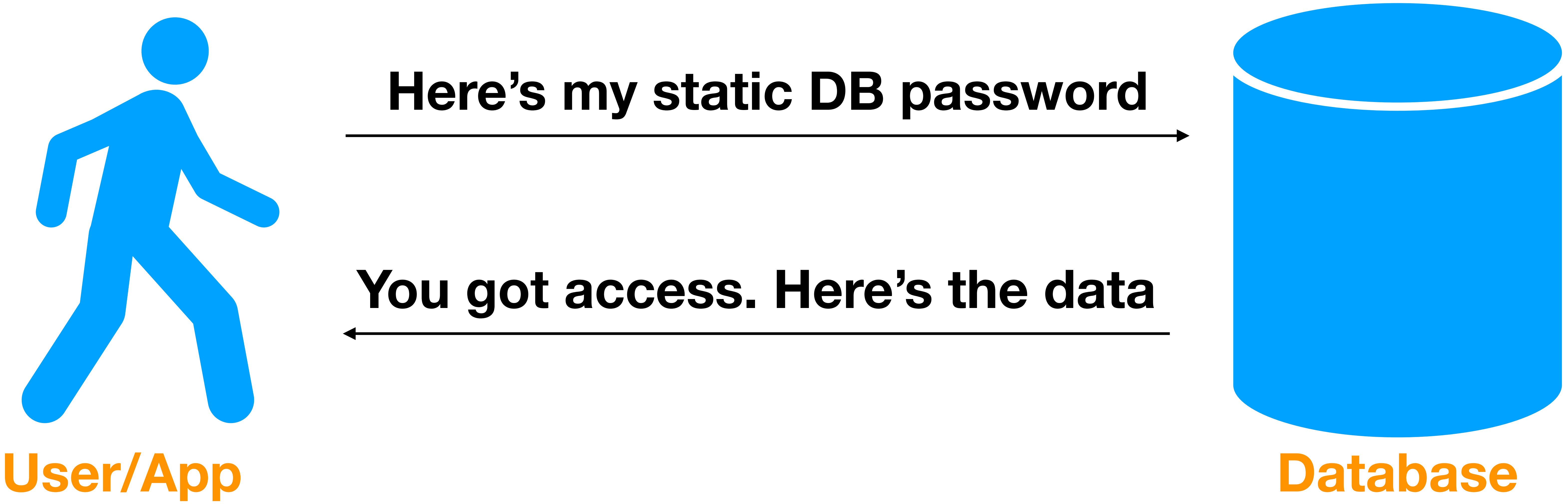
Dynamic Credentials

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

Choosing the right tool

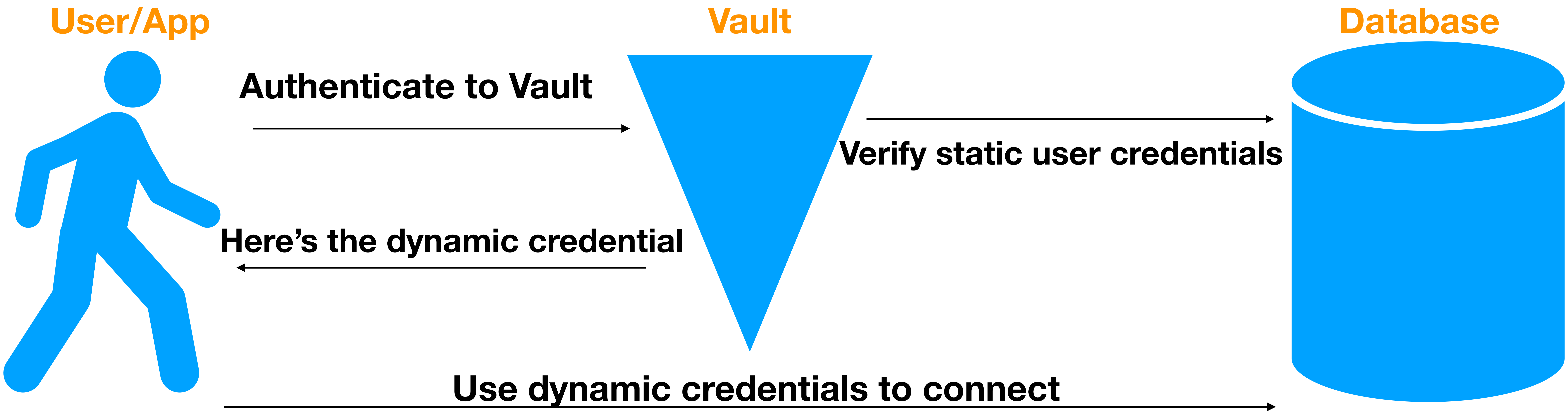
- Flexibility
- Integrations/providers
- Encryption
- Automatic expiry of tokens/secrets
- Password revocation

Why HashiCorp Vault?



Here’s my static DB password

You got access. Here’s the data



User/App

Vault

Database

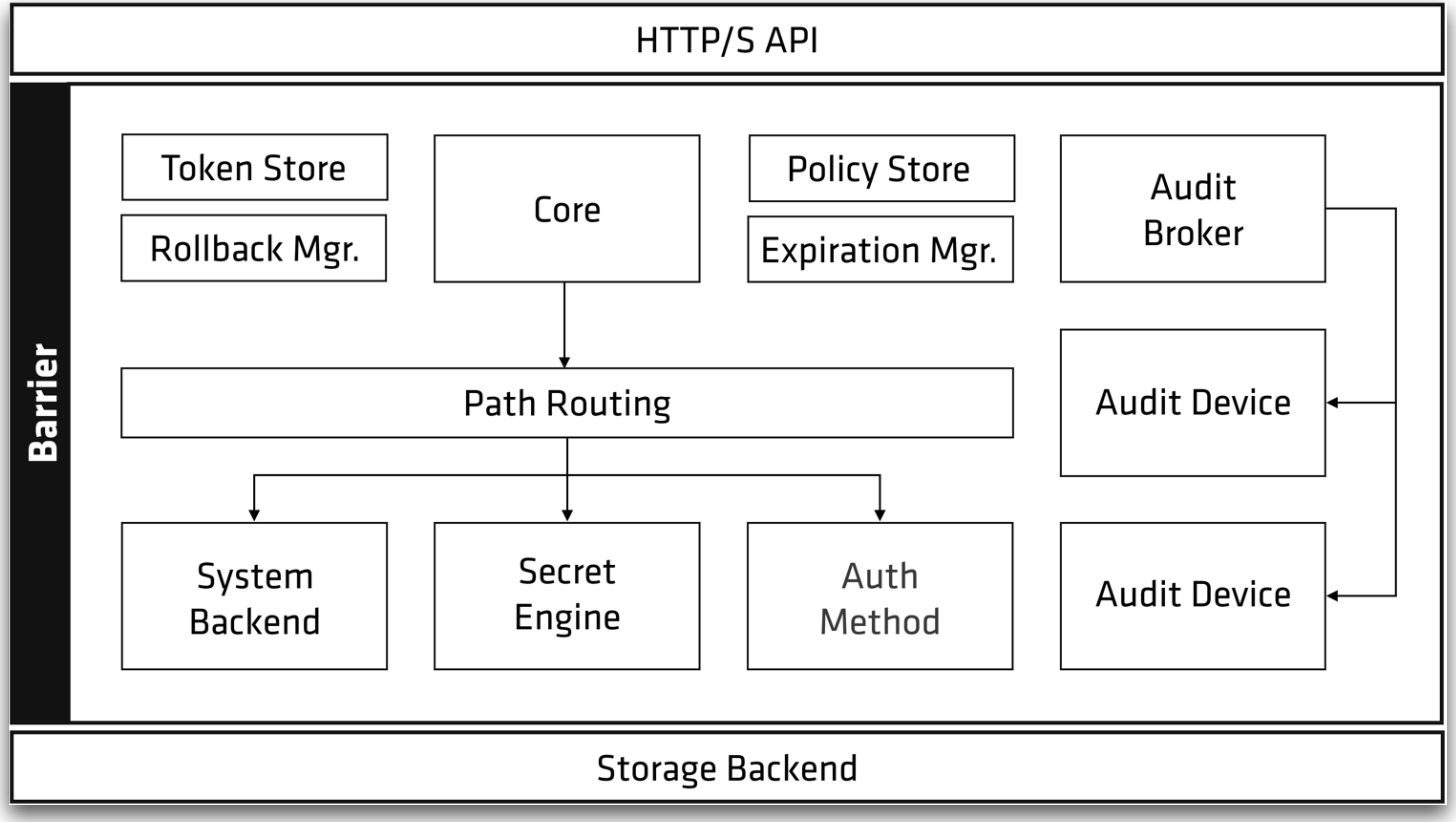
Authenticate to Vault

Verify static user credentials

Here’s the dynamic credential

Use dynamic credentials to connect

Vault - Architecture



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

Demo Time

console.aiven.io/project/dev-advocates/services
Gmail
YouTube
Imported
Aiven Onboarding
Aiven Employee O...
Aiven HR
Aiven DevRel
Useful Slab resour...
Aiven Product
Blogs I want to re...
Apache Flink
Aiven SA
Aiven OSPO
Aiven Travel
aiven
CONSOLE
PROJECT:
dev-advocates
Solutions Architecture
Services
Events
Members
VPC
Service Integrations
Billing
Settings
$31.11
BILLING
Search services by name, plan, cloud and tags...
+ Create a new service

Current services

Service	Nodes	Plan	Cloud	Created
demo-kafka Apache Kafka • Running	●●●	Business-4 1 CPU / 4 GB RAM / 600 GB storage - 3-node high availability set	Google Cloud: europe-west3 Europe, Germany	8 hours

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

Do you have a break glass procedure?

Let’s recap. Scan the QR ⬇️

Blog (includes demo):
https://aiven.io/blog/secure-your-db-with-vault

in/diahmed | @DewanAhmed

Questions?

dewan@aiven.io