

A red-themed illustration on the left side of the slide. It features a central vertical pipe with a valve. To the left of the pipe are several cloud icons, a stack of four cylinders, and a server rack with three horizontal lines. To the right of the pipe is a grid with a mix of 'X' and 'O' symbols, and a curved arrow pointing upwards. Arrows also point upwards from the cylinder stack and the server rack towards the central pipe.

# OCP+ Red Hat Integration

**Eoin Crosbie**  
EMEA Technical Partner Development Manager

# Welcome!



- Eoin (Owen) Crosbie



V0000000



# Welcome!



- Eoin (Owen) Crosbie



V0000000

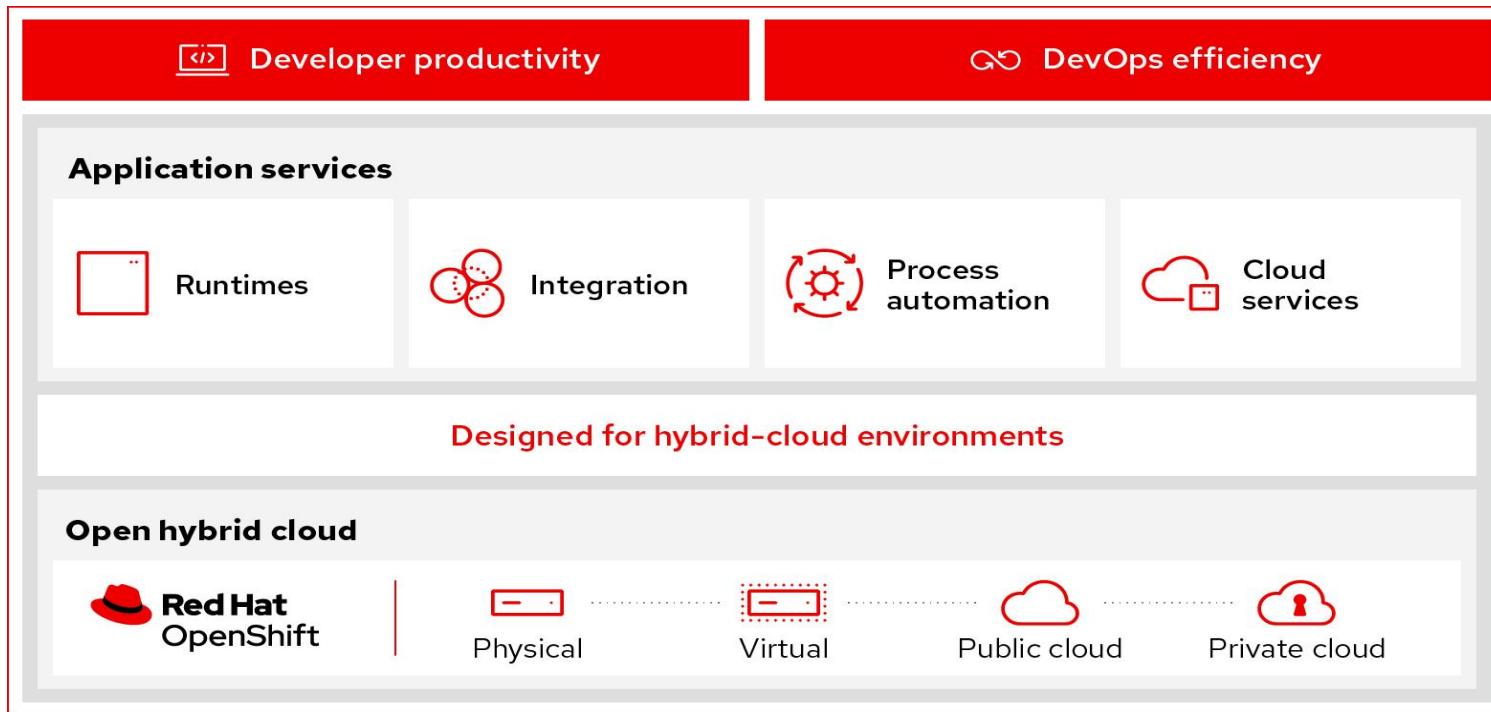
 Red Hat

# Agenda

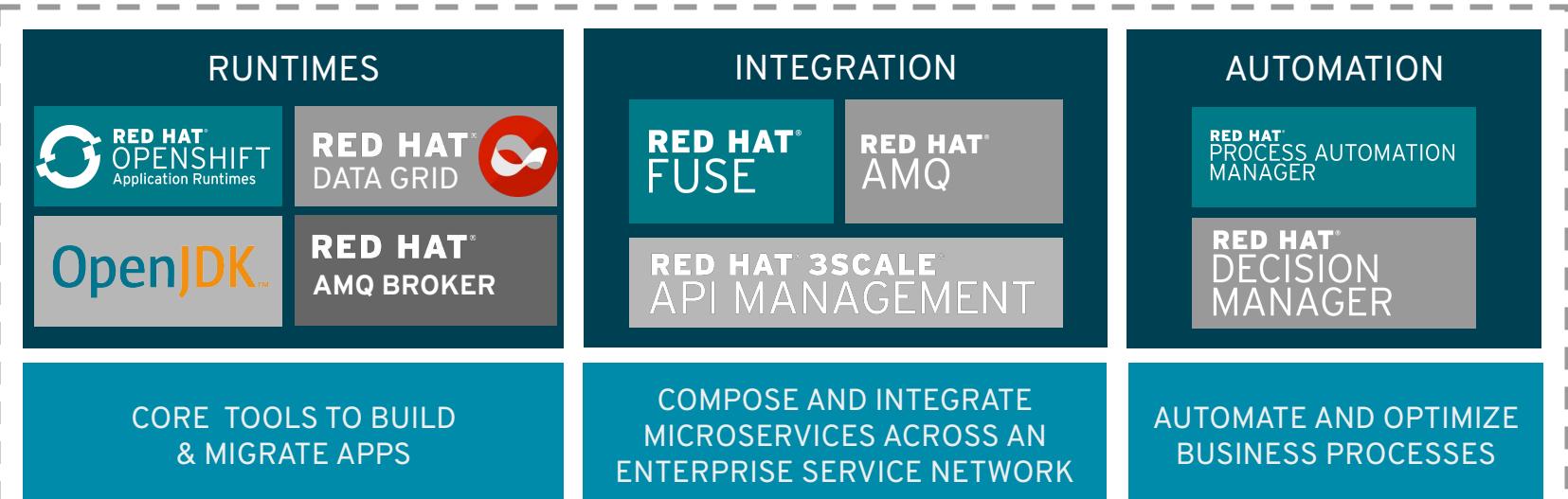
- Red Hat Integration
- Business Value
- Products
- API Security
- Partner Events
- Demo

# Red Hat Application Services Portfolio

Integration and more: Develop, optimize, connect and automate Apps across hybrid cloud

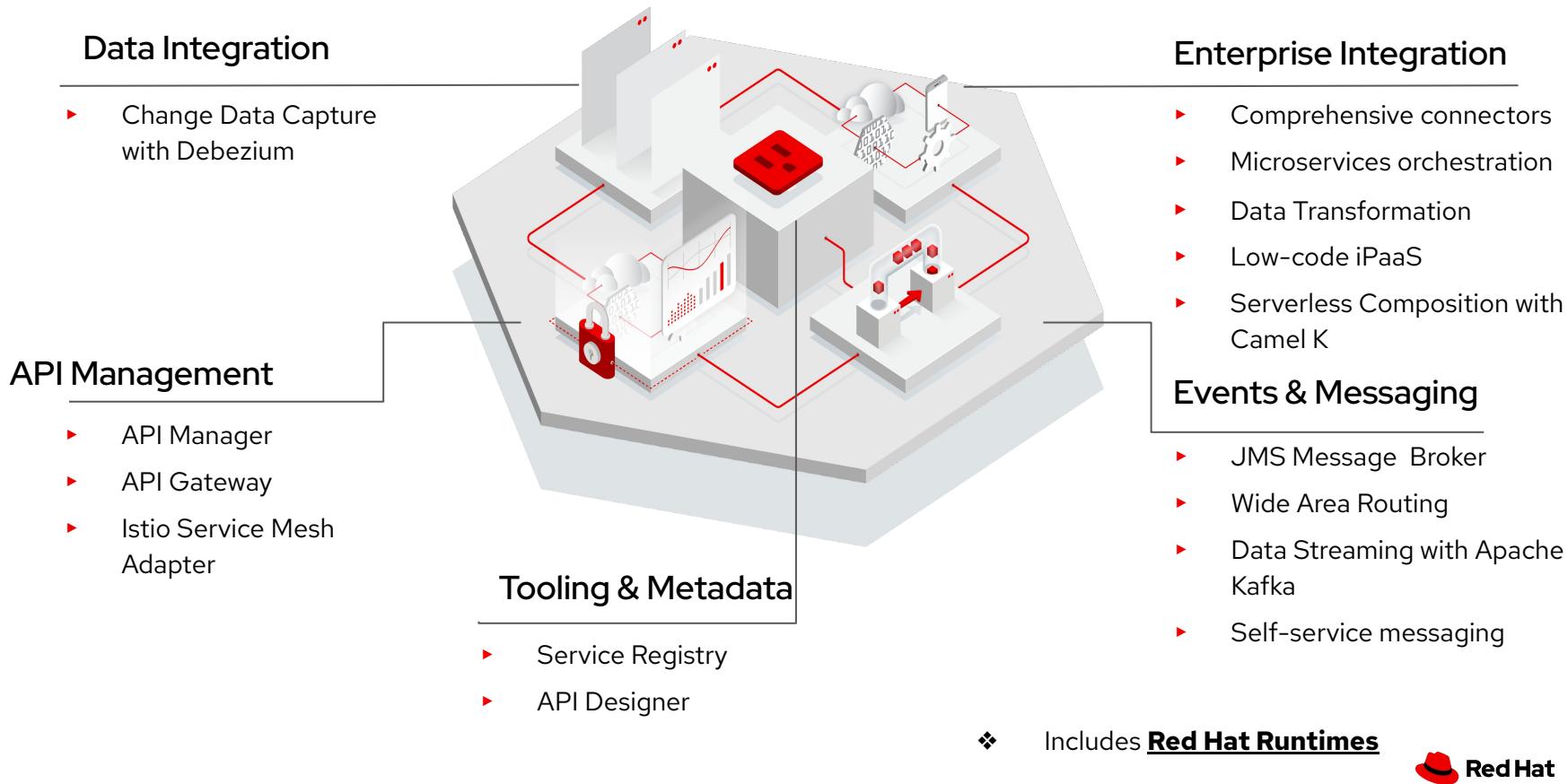


# Application Services Bundles



**Develop, Deploy and Manage Across a Hybrid Cloud**

# Red Hat Integration: Cloud-Native Integration



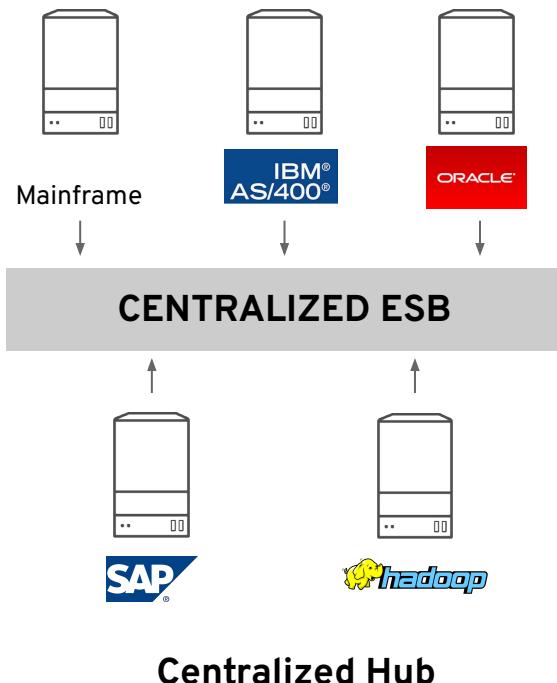
---

# Business Value

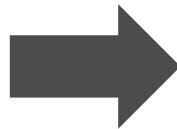
“ People try to copy Netflix, but they can only copy what they see. They copy the results not the process. ”

*Adrian Cockcroft, former Chief Cloud Architect. Netflix*

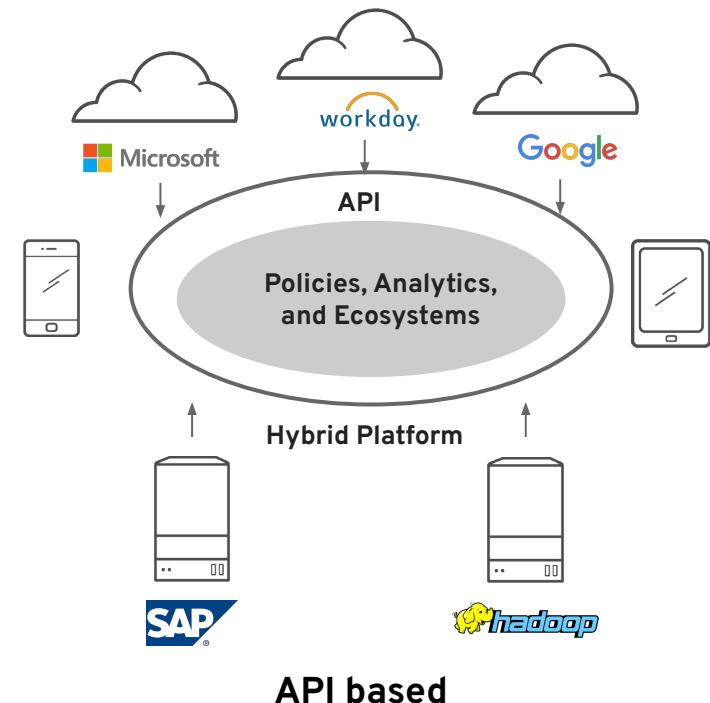
# WHAT'S NEEDED? API-CENTRIC INTEGRATION.



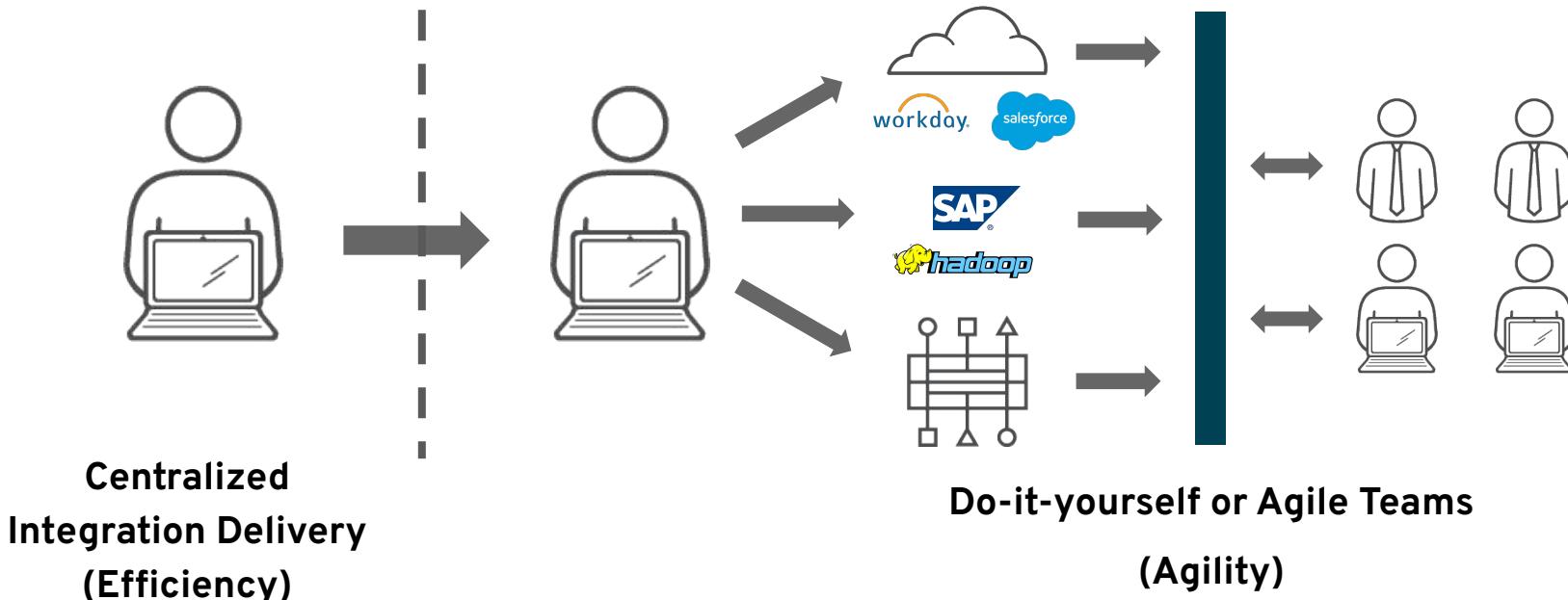
Decentralized



More Agility



# INTEGRATION DELIVERY NEEDS TO CHANGE



RESHAPING THE INTEGRATION DELIVERY MODEL: ENABLE DIY TEAMS

# Realizing business value with Red Hat Integration

 **507%**

return on investment over 3 years

 **6 months**

to payback

 **21%**

more efficient DevOps teams

 **2x**

more applications integrated

 **43%**

reduced unplanned downtime

 **38%**

more applications developed

 **US \$1.8 million**

additional revenue gained

 **10%**

more efficient Center of Excellence teams

 **40%**

more APIs developed

 **17%**

more productive end users

# Why Red Hat Integration for business applications?

IDC research: The business value of Red Hat Integration

“ ”

“The most significant benefit is the integration. We moved from a pure in-house development to focus on application integration to support a hybrid model.”

“ ”

“The benefit really is the efficiency. We have a pretty complex environment and Integration helped us streamline everything a lot better than before. It's made it easier for people to jump in and work on our systems.”

“ ”

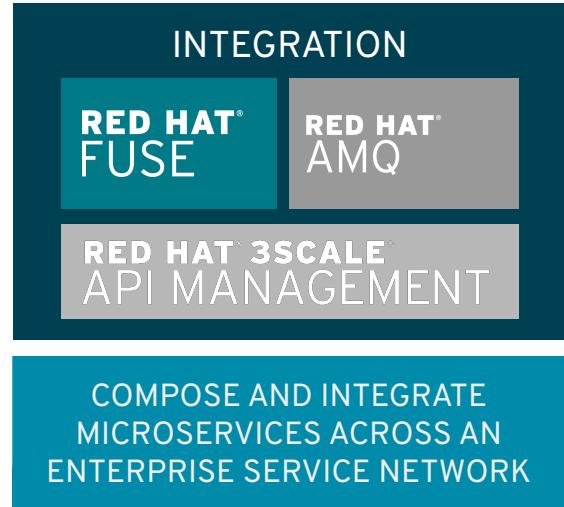
“Integration is making sure that we have accurate subscription counts so that we're not oversubscribing or undersubscribing. This helps manage and keep costs down.”

Source:

IDC White Paper, sponsored by Red Hat, [“The Business Value of Red Hat Integration”](#), doc # US47989320, July 2021.

---

# Products



## DISTRIBUTED INTEGRATION

- LIGHTWEIGHT
- PATTERN BASED
- EVENT ORIENTED
- COMMUNITY SOURCED

## FLEXIBILITY

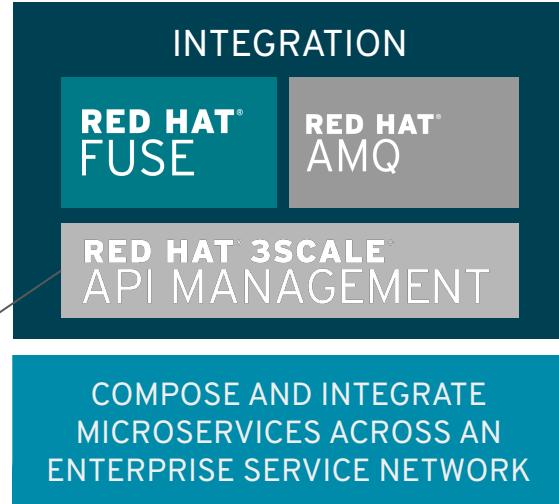
### INTEGRATION

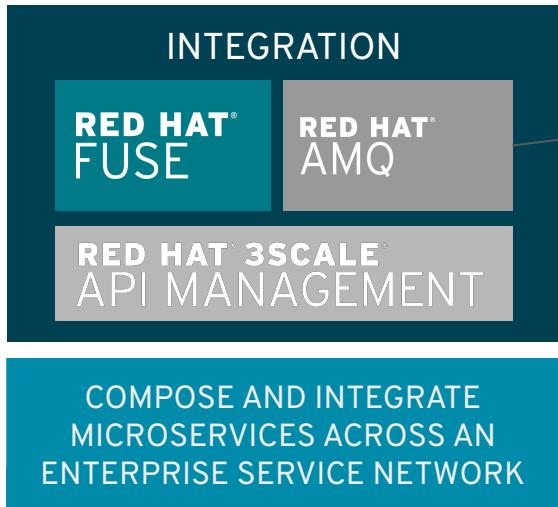
RED HAT®  
FUSE

RED HAT®  
AMQ

RED HAT 3SCALE®  
API MANAGEMENT

COMPOSE AND INTEGRATE  
MICROSERVICES ACROSS AN  
ENTERPRISE SERVICE NETWORK





## MESSAGING

- ENTERPRISE GRADE MESSAGING SOLUTION
  - DATA STREAMING
  - SELF-SERVICE MESSAGING

## COMMUNICATION

## CONTAINERS

---

- TRADITIONAL & CLOUD NATIVE SOLUTIONS
- LEAN ARTIFACTS, INDIVIDUALLY DEPLOYABLE
- CONTAINER BASED SCALING AND HIGH AVAILABILITY

## SCALABILITY



	<b>API</b>	
Interface	<ul style="list-style-type: none"> <li>▶ API Contracts</li> <li>▶ Monetisation</li> <li>▶ Business strategic policy enforcement</li> <li>▶ Partner ecosystem</li> </ul>	  
Application concerns	<b>APPLICATION</b> <ul style="list-style-type: none"> <li>▶ Choice of language/framework</li> <li>▶ Self-service / productivity</li> <li>▶ Low mem, fast startup</li> <li>▶ Integrations framework</li> </ul>	    
Microservices	<b>SERVICE TO SERVICE</b> <ul style="list-style-type: none"> <li>▶ Network resilience</li> <li>▶ Service security</li> <li>▶ Policy enforcement</li> <li>▶ Metrics/Observability</li> <li>▶ Load balancing</li> </ul>	  
Infrastructure concerns	<b>DEPLOYMENT PLATFORM</b> <ul style="list-style-type: none"> <li>▶ Reliability</li> <li>▶ Instance placement</li> <li>▶ Scaling/autoscaling</li> <li>▶ Resource usage</li> <li>▶ Job scheduling</li> <li>▶ Distributed Logging</li> </ul>	  

# Red Hat 3scale API Management

# RED HAT 3SCALE API MANAGEMENT

## System Architecture

The 3scale API Management architecture consists of :

- The **API Manager** which manages the API, Developers and Applications
- The **Traffic Manager** (API Gateways) that enforce the policies from the API Manager and delegate authorization to 3rd party IDPs
- The **Identity Provider** (IDP) identity hub that supports many authentication using various protocols
- The **API Backend** the API. i.e. the API Provider

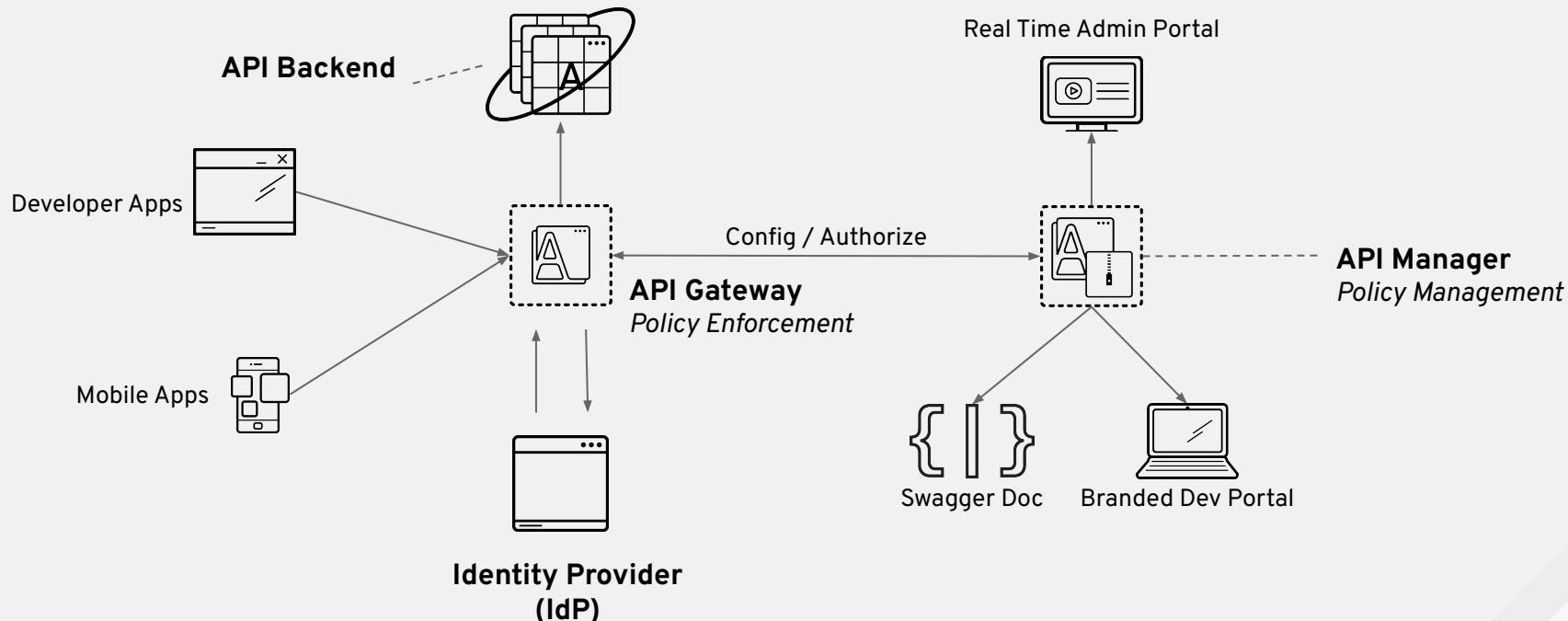
# RED HAT API MANAGEMENT

## Gateway Operations

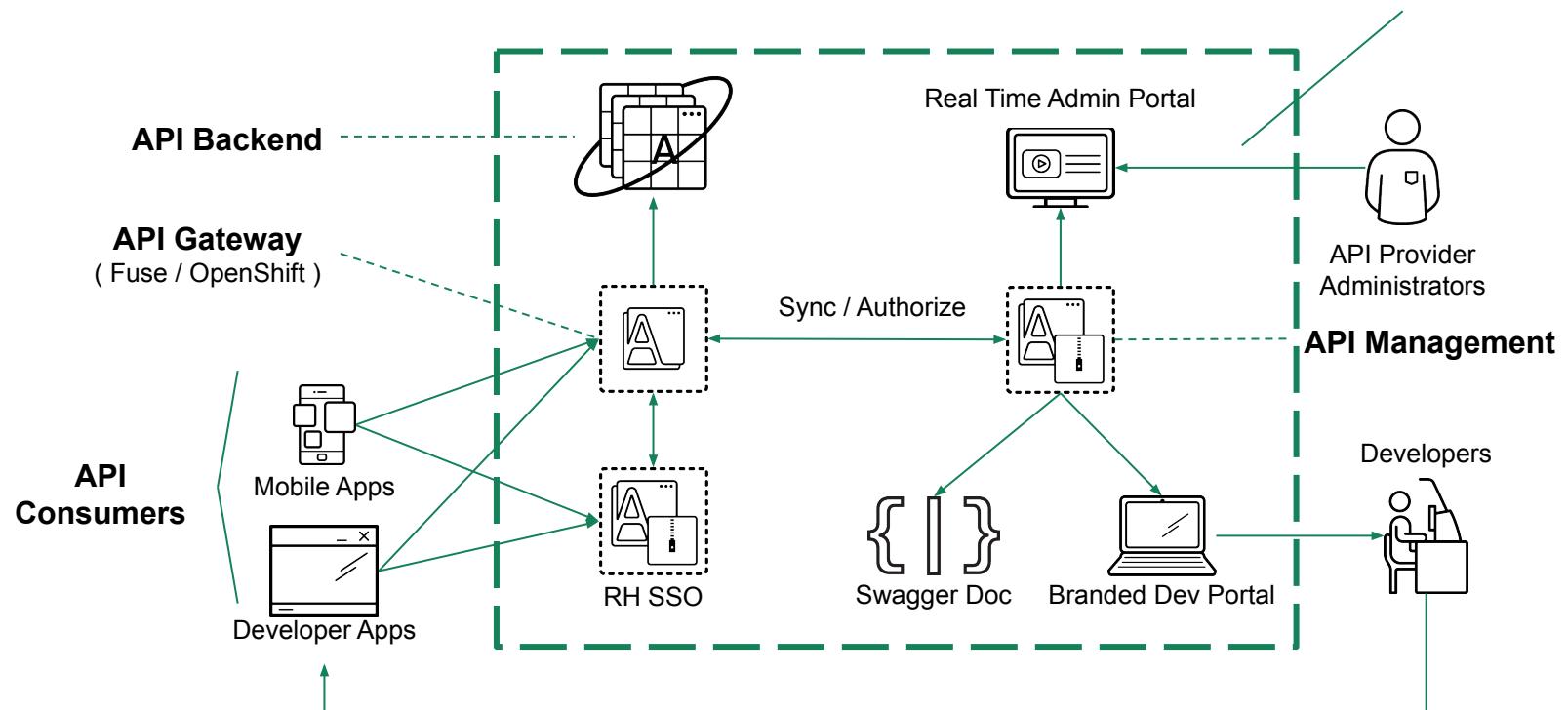
- Checks the timestamp for ‘expired’ token.
- Checks the client\_id is still valid
- Performs a check on the signature of the JWT using RH SSO public key

# RED HAT API MANAGEMENT

## System Architecture



# RED HAT API MANAGEMENT



---

# API Security

# CUSTOMER MOVING TO CONTAINERS?

## Customer Benefits

- Breaking down the monolith means faster turnaround.
- Greater flexibility.
- Fully automated testing driving better QA.
- Free from single technology limits
- Makes customer agile, cloud native, reactive compliant, with bounded security and fully aggregate enabled!

# REMEMBER SECURITY

Everything Has To Be Super Secure

- Independent services that are no longer bound to one monolith i.e. just one security context on one cluster or multiple ones ?
- So in microservices - does each service have to store identity?
- Ownership of identity data is a risk if not done properly.



# CSO IS ON THE SPOTLIGHT (2020)

Recent News On Data Breaches Is Not A Good Start



**77,000,000 PSN RECORDS STOLEN**

Sony



**143,000,000 ACCOUNTS**

Equifax



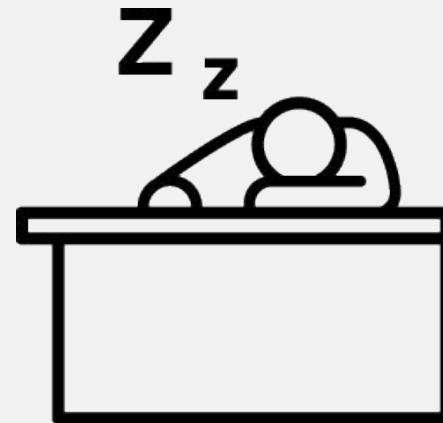
**117,000,000 RECORDS STOLEN**

LinkedIn

# DEVELOPERS HEADACHE

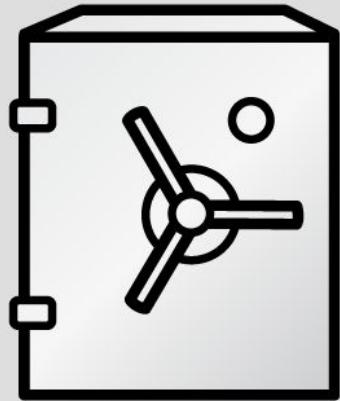
Homemade Security Is Always A Recipe For Disaster

- The bar for appdev security has been raised substantially.
- Most devs don't really 'do' security.
  - E.g. Storing user information - should be as salted hash.
- The hand rolled solutions of the past are not viable going forwards.
- Are you still sure you want to store 'identity' in your App?



# PROBLEM WAS SOLVED WHILE AGO

Banks

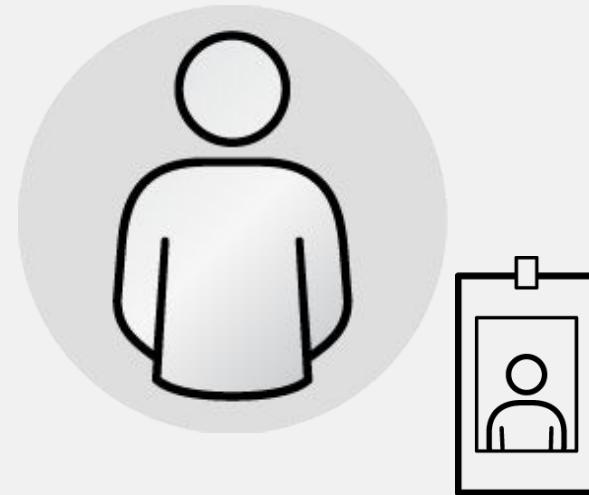


- Most people do not keep their savings under their mattress for the same security reasons.
- They store them in a trusted environment - i.e. the bank.
- Then use a separate means to authorise / authenticate payments.

# API SECURITY WORKS IN THE SAME WAY

Trusted Identity Authority

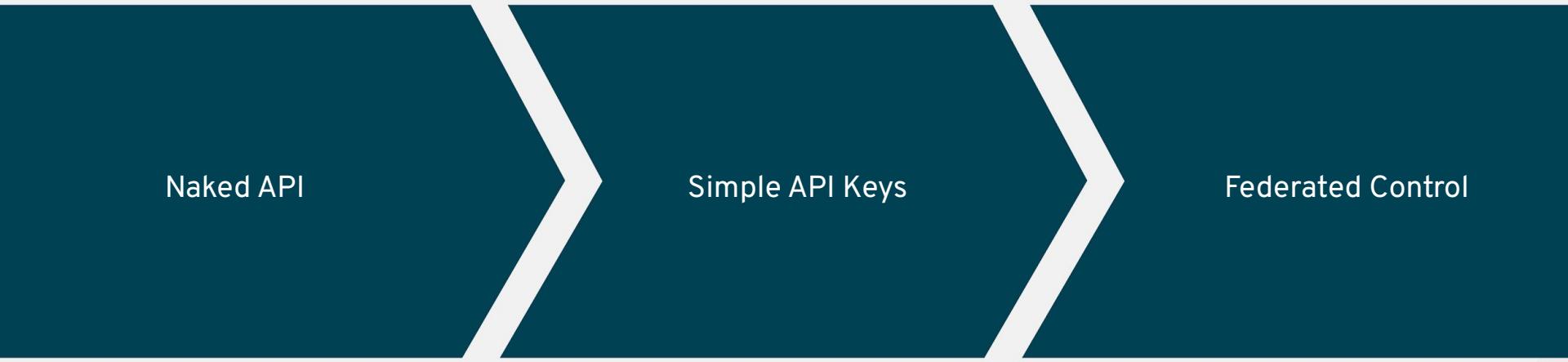
- Identity is abstracted away to a single ‘fortress’.
- Tokens are issued as a means of allowing access to services and resources.
- So now your application services no longer have to store sensitive data!





# API SECURITY

Evolution of API Security



Naked API

Simple API Keys

Federated Control

# API SECURITY

## Top Schemes

Most API Management platforms supports the following security schemes:

- **API Key** single token string
- **APP ID/APP Key (Basic Auth)** two token strings i.e. username, password
- **OpenID Connect (OIDC)** simple identity layer on top of OAuth framework

---

# OAuth

# OAUTH 2.0

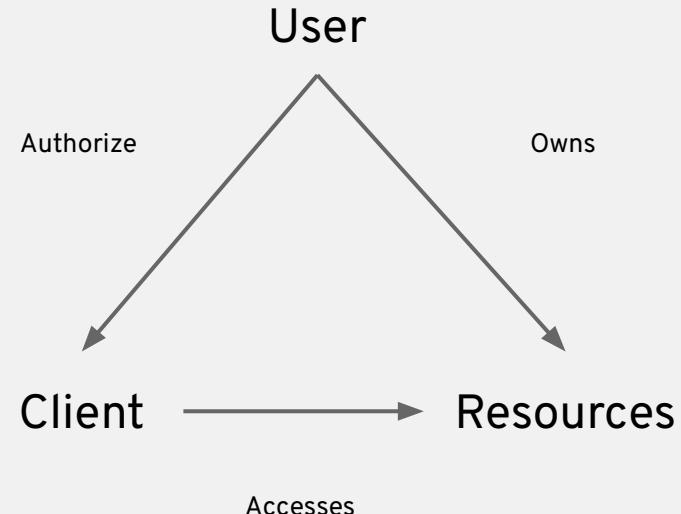
From 20,000 FT



OAuth (Open Authorization) is an open standard for access delegation:

- One service can request access to resources on another service on the behalf of the user.

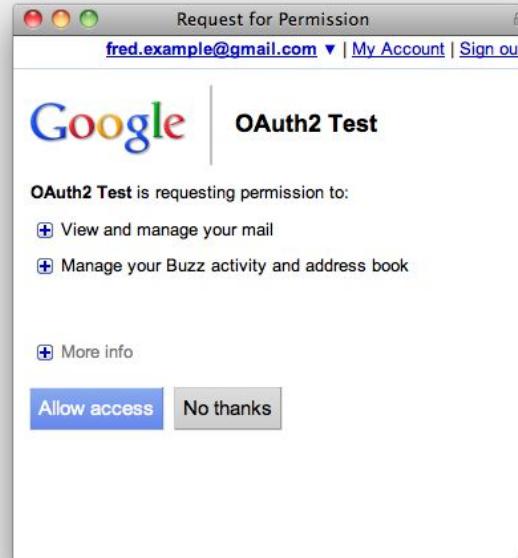
Published October 2012



# OAUTH 2.0

## Delegation

OAuth enables users to grant third-party access to their web resources without sharing their passwords.



# OAUTH 2.0

## Terminology

- **Resource Owner:** generally yourself.
- **Resource Server:** server hosting protected data (for example Google hosting your profile).
- **Client:** application requesting access to a resource server (i.e. a mobile application).
- **Authorization Server:** server issuing token to the client. This token will be used for the client to request the resource server.

# OAUTH 2.0

## Grant / Flow Types

### **Authorization Code Flow**

The most secure and used where a user logs into Identity server and grants access to Application to retrieve their data

### **Client Credentials Flow**

Only Application data is passed in a single request for an Access Token

### **Implicit Flow**

User logs in but secret is not passed

### **Resource Owner Password Flow**

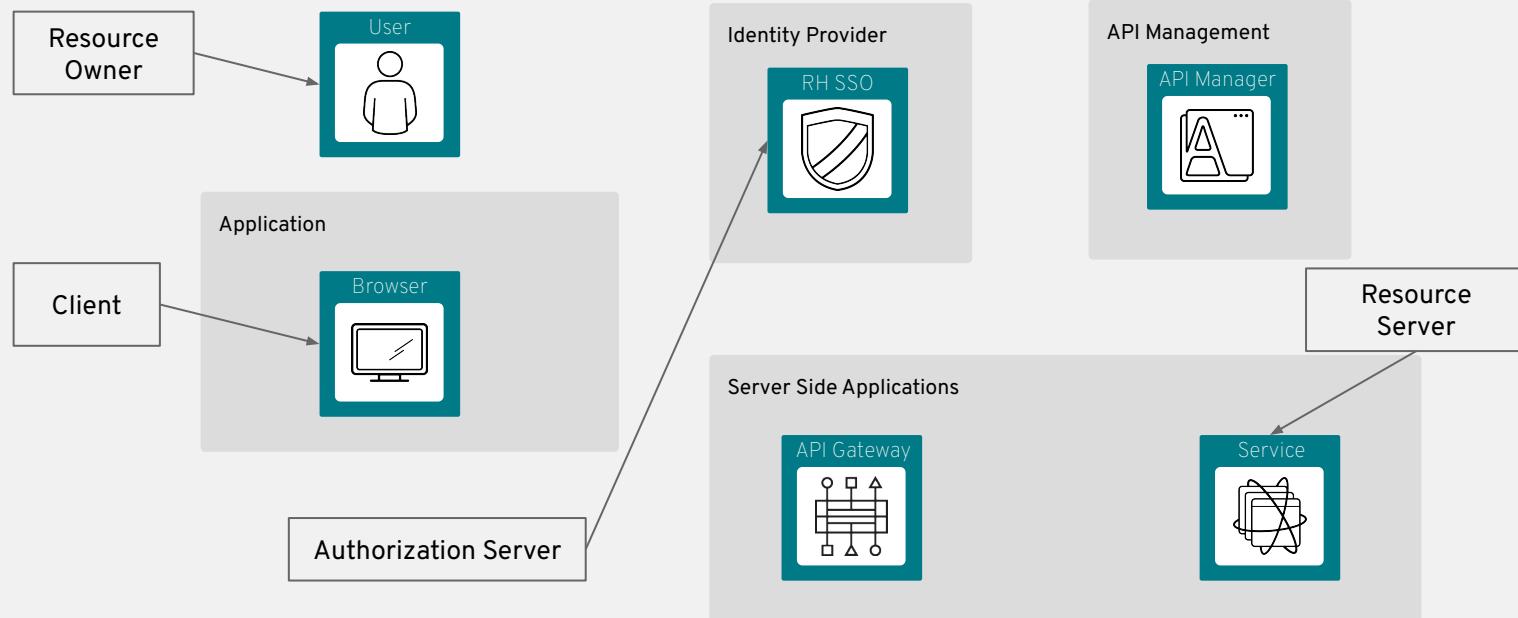
Application, username and password data is passed in a single request for an Access Token

---

# Authorization Code Flow

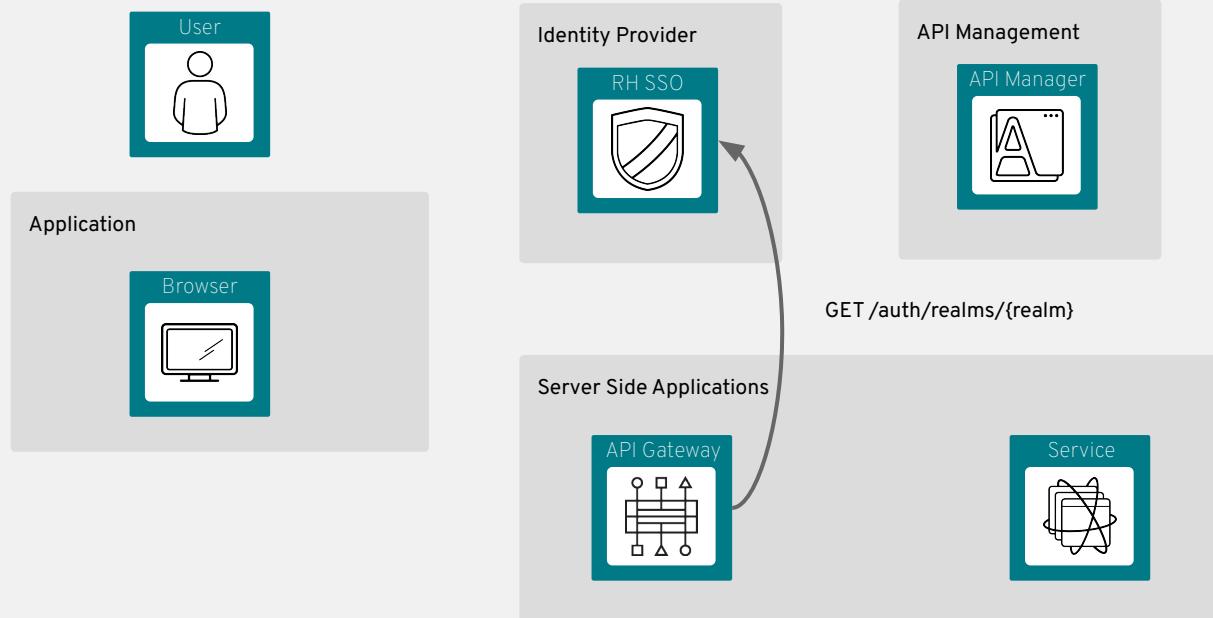
# AUTHORIZATION CODE FLOW

An Orientation



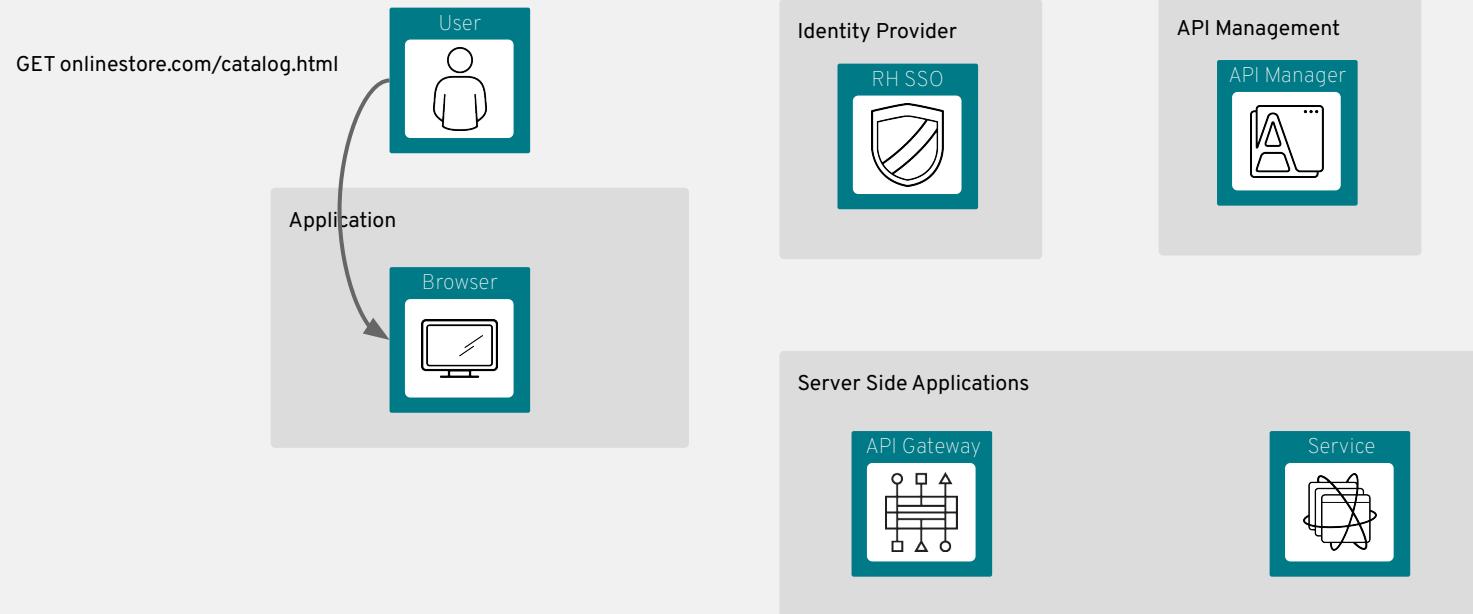
# AUTHORIZATION CODE FLOW

#0 - 3scale API Gateway Gets RH SSO Public Key On Configuration Load



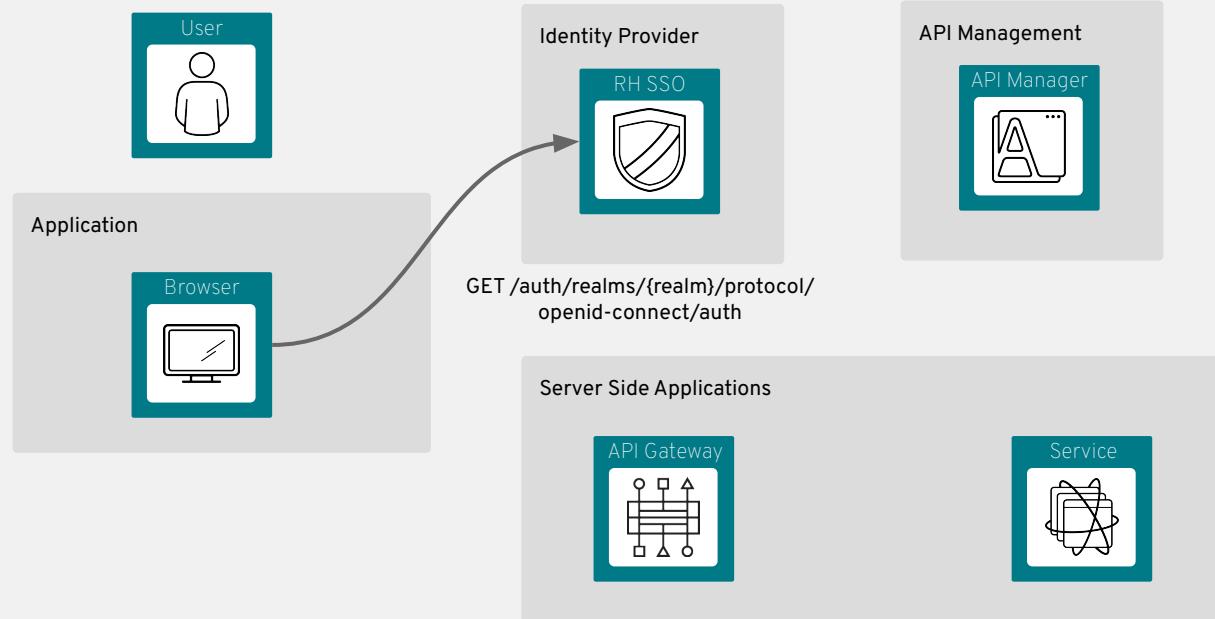
# AUTHORIZATION CODE FLOW

## #1 - User Starts Using The Web App



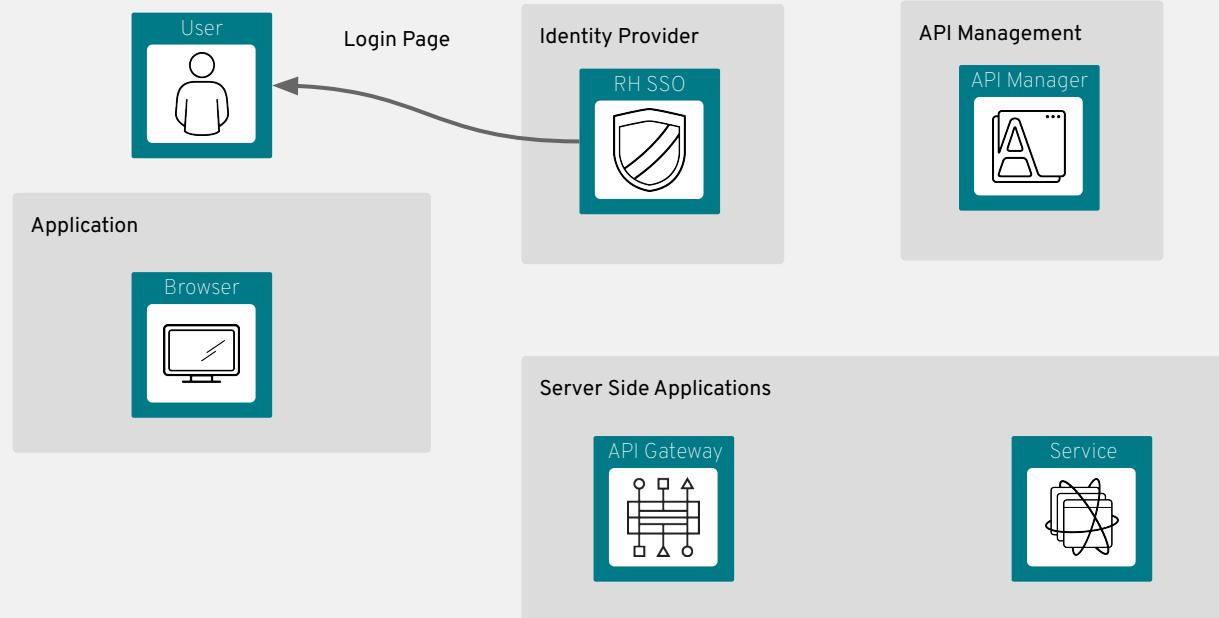
# AUTHORIZATION CODE FLOW

## #2 - The Application Introduces RH SSO



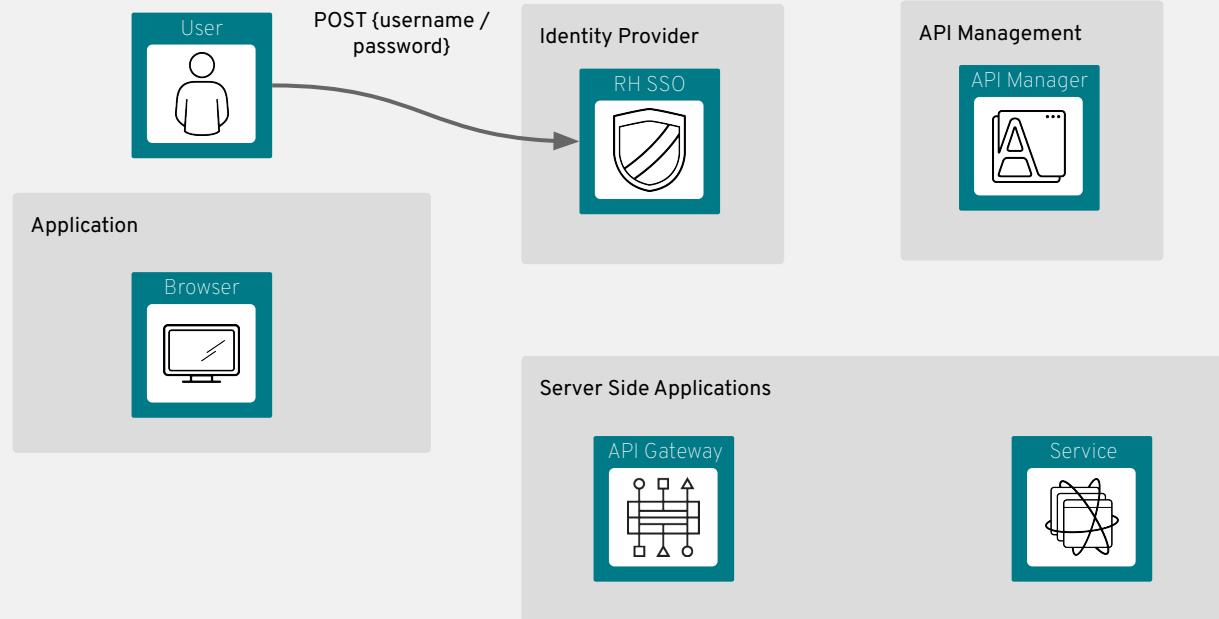
# AUTHORIZATION CODE FLOW

## #3 - RH SSO Forwards To Login Form



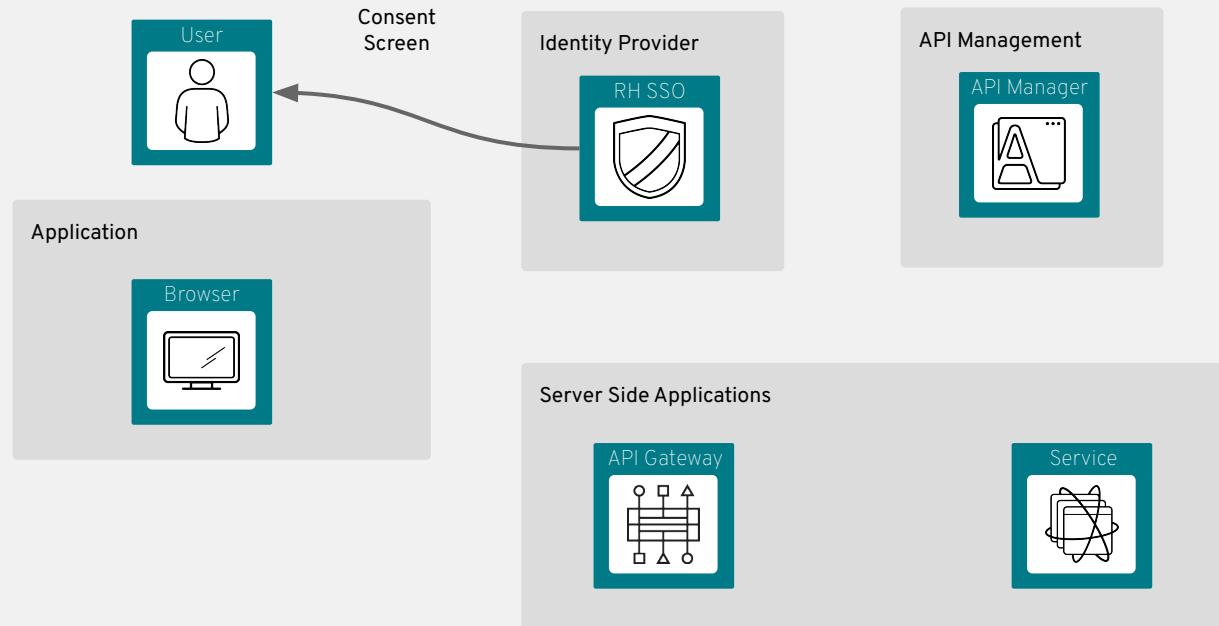
# AUTHORIZATION CODE FLOW

## #4 - The User Logs Into RH SSO



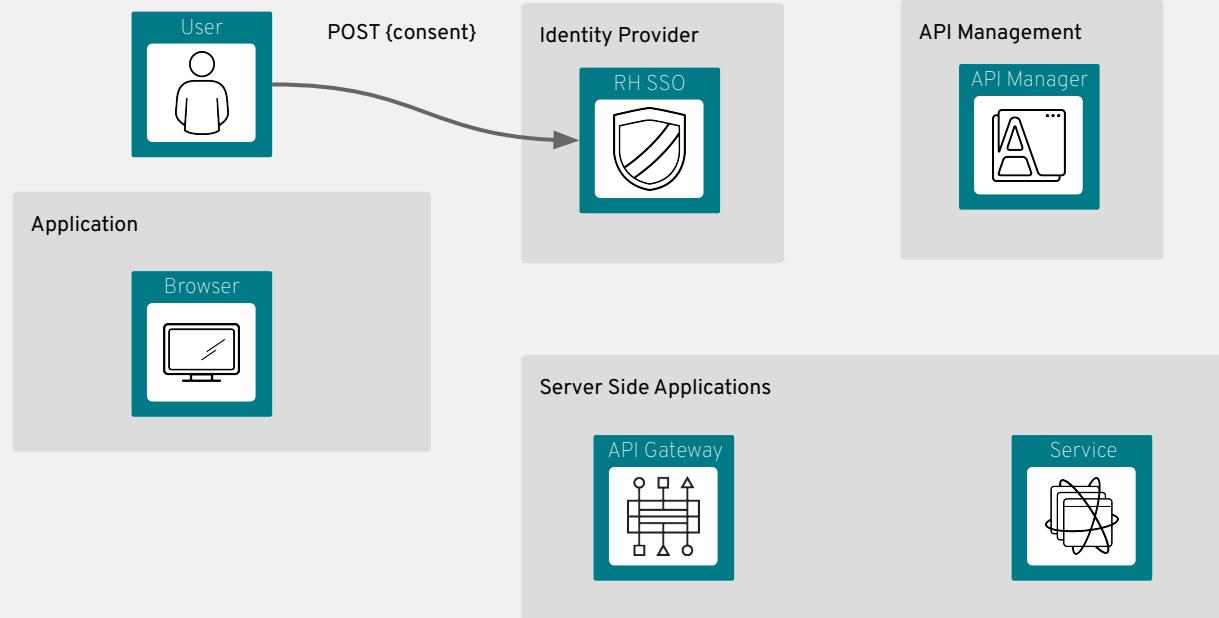
# AUTHORIZATION CODE FLOW

## #5 - RH SSO Forwards To Consent Page



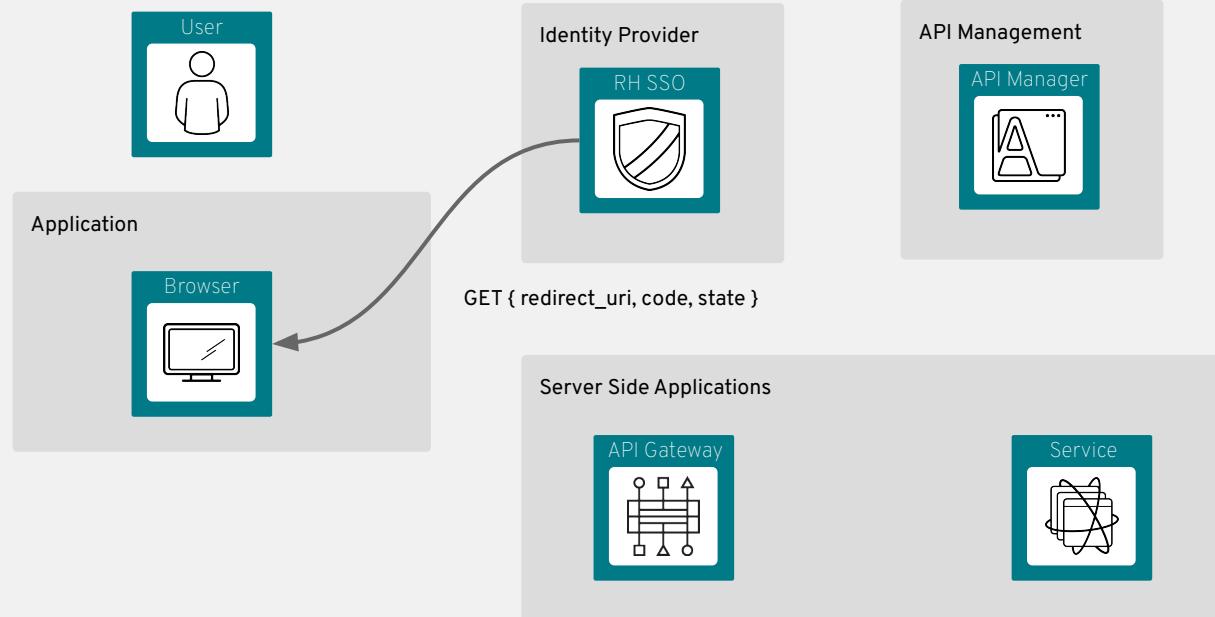
# AUTHORIZATION CODE FLOW

## #6 - The User Consents



# AUTHORIZATION CODE FLOW

#7 - RH SSO Redirects To Application And Sends An Auth Code



# AUTHORIZATION CODE FLOW

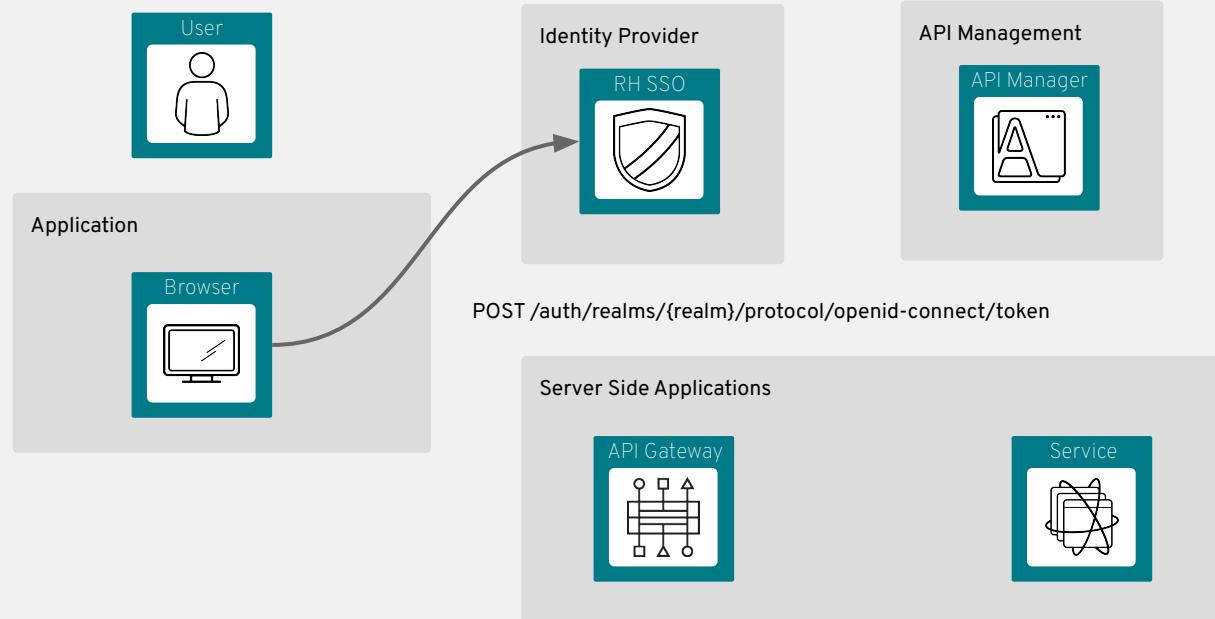
## #7.1 - The Temp Auth Code

- Is used to acquire an access code.
- Think of this as being a cloakroom ticket - this can be used once only to acquire a bearer token.



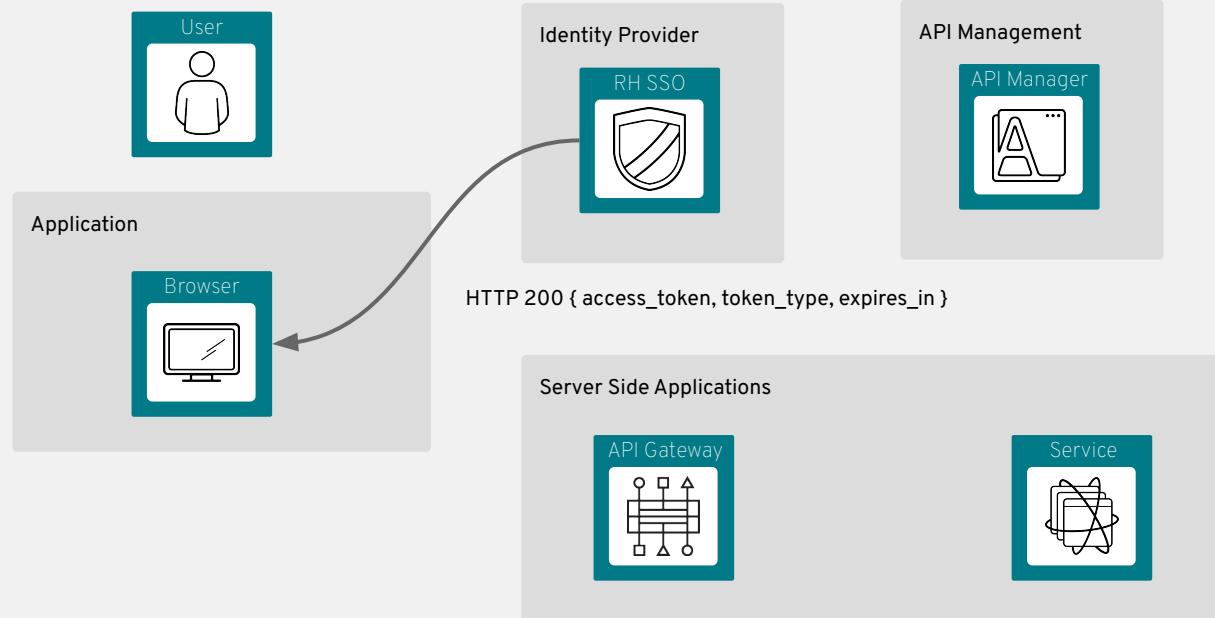
# AUTHORIZATION CODE FLOW

## #8 - The Web App Calls The Token Endpoint



# AUTHORIZATION CODE FLOW

#9 - RH SSO Sends A Valid Bearer Token



# AUTHORIZATION CODE FLOW

## #9.1 - The Bearer Token



"A security token with the property that any party in possession of the token (a "bearer") can use the token in any way that any other party in possession of it can"

# AUTHORIZATION CODE FLOW

## #9.2 - The Bearer Token

```
Authorization: Bearer QXV0aG9yaXphdGlvbjogQmVhcmVyIA0Kew0KICJqdGki0iAiYmNiMTFmNDktZTZhZS0NGNhLWIwNzctMzc5MjU5NGYwZDk4IiwNCiAizXhwIjogMTQ5NTI3MjczOSwNCiAibmJmIjogMCwNCiAiaWF0IjogMTQ5NDMyMjMzOSwNCiAiaXNzIjogImh0dHA6Ly8w0TY2ZWExZi5uZ3Jvay5pby9hdXR0L3J1Ywxcty9mb3VybWFya3MiLA0KICJhdWQioiAingQ2NTI0MDYiLA0KICJzdWIi0iAizDIwZGM0MTUtNzUyZi00YtC5LWEzYTgtNTJ10TV1YTzKzWm2IiwNCiAidHlwIjogIkJ1YXJ1ciIsDQogImF6cCI6IC10ZDY1MjQwNiIsDQogInNlc3Npb25fc3RhdGUi0iAiNTVh0DQzMjktY2Y2ZC00Yj1iLWJhOGYtWjhMDM3NjRjMjFjIiwNCiAiy2xpZW50X3Nlc3Npb24i0iAiYmYxYTA3MzktYTM5Yy00NTE1LT1jMDAtNzh1MTgyNmI4ZDM2IiwNCiAiyWxsb3d1ZC1vcmlnaW5zIjogWw0KICAiaHR0cHM6Ly93d3cuZ2V0cG9zdG1hb15jb20iDQogXSwNCiAicmVhbG1fyWNjZXNzIjogew0KICAicm9sZXMi0iBbDQogICAiYWNjZXNzX215X3Jlc291cmN1Ig0KICBdDQogfSwNCiAicmVzb3VY2VfYWNjZXNzIjogew0KICAiYWNjb3VudCI6IHsNCiAgICJyb2xlcYI6IFsNCiAgICAibWFuYWd1LWFjY291bnQiLA0KICAgICJ2aWV3LXByb2ZpbGUdDQogICBdDQogIH0NCiB9LA0KICJuYW1IjogInRlc3QgdXNlc1IsDQogInByZWZlcnJlZF91c2VybmfTzSI6ICJ0ZXN0dXNlc1IsDQogImdpdmVuX25hbWUi0iAidGVzdCIsDQogImZhbWls eV9uYW1IjogInVzZXIiLA0KICJ1bWFpbCI6ICJ0ZXN0QGjsYWguY29tIg0KfQ0K
Accept: /*
Postman-Token: 86b86d4a-8369-40af-8612-9f0d3589fdfb
Cf-Ray: 35c3a94bb1ac35ae-LHR
X-3Scale-Proxy-Secret-Token: Shared_secret_sent_from_proxy_to_API_backend_169ad455fe40801e
```

What does a bearer token look like?

# AUTHORIZATION CODE FLOW

## #9.3 - The Bearer Token

if you base64 decrypt you get:

notice the role information

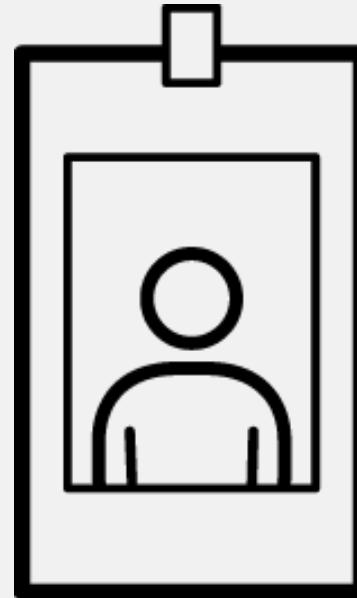
the token is a JWT.

```
Authorization: Bearer
{
  "jti": "bcb11f49-e6ae-44ca-b077-3792594f0d98",
  "exp": 1495272739,
  "nbf": 0,
  "iat": 1494322339,
  "iss": "http://0966ea1f.ngrok.io/auth/realms/fourmarks",
  "aud": "4d652406",
  "sub": "d20dc415-752f-4a79-a3a8-52e95ea6dec6",
  "typ": "Bearer",
  "azp": "4d652406",
  "session_state": "55a84329-cf6d-4b9b-ba8f-aba03764c21c",
  "client_session": "bf1a0739-a39c-4515-9c00-78e1826b8d36",
  "allowed-origins": [
    "https://www.getpostman.com"
  ],
  "realm_access": {
    "roles": [
      "access_my_resource"
    ]
  },
  "resource_access": {
    "account": {
      "roles": [
        "manage-account",
        "view-profile"
      ]
    }
  },
  "name": "test user",
  "preferred_username": "testuser",
  "given_name": "test",
  "family_name": "user",
  "email": "test@blah.com"
}
```

# AUTHORIZATION CODE FLOW

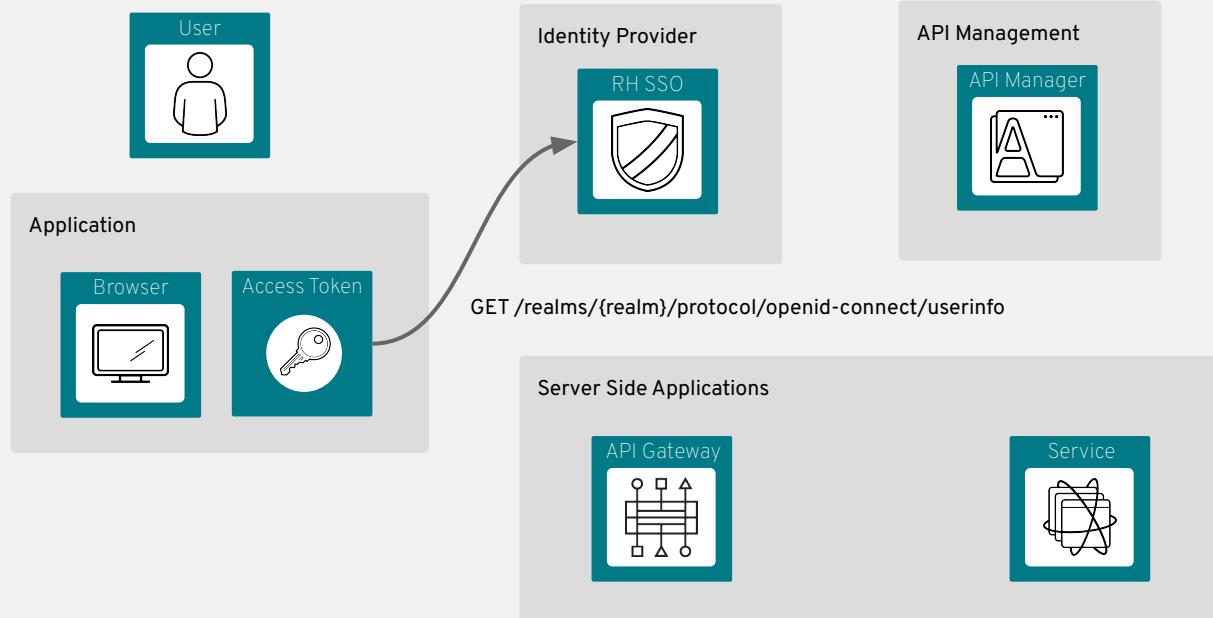
## #9.4 - The Bearer Token

- Digitally signed by the Auth Server.
- A Standardised Identity token.
- Contains the username and roles, but can also add custom claims.



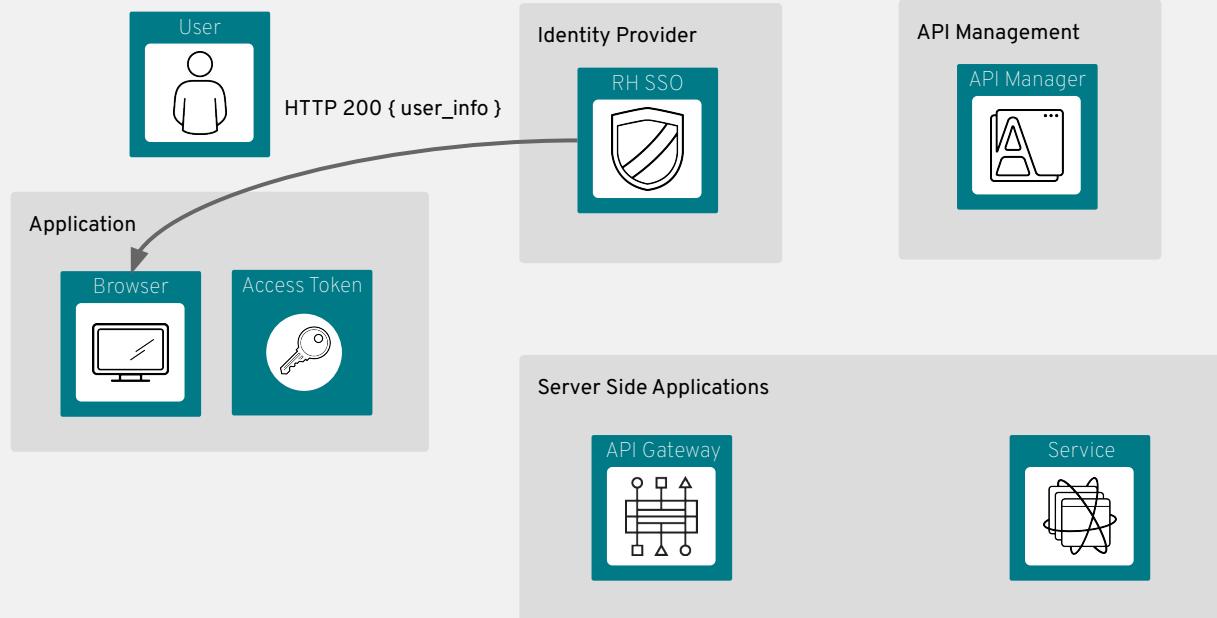
# AUTHORIZATION CODE FLOW

#9.5 - Web App Submits The Access Token To Get User Info (Optional)



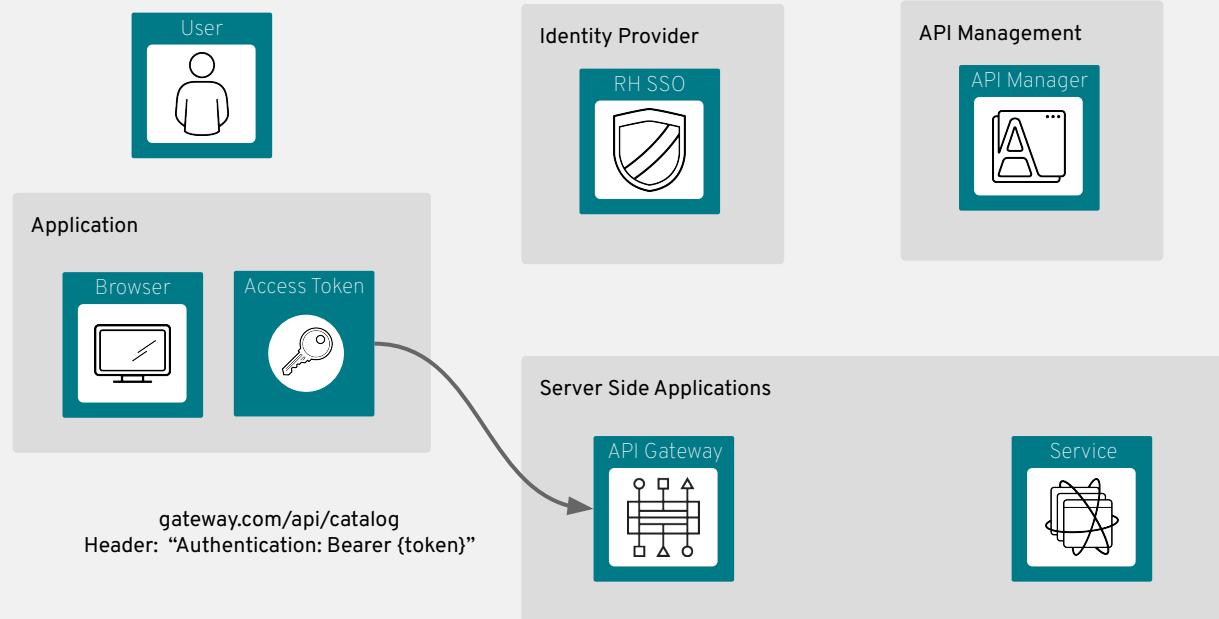
# AUTHORIZATION CODE FLOW

## #9.6 - Web App Receives UserInfo



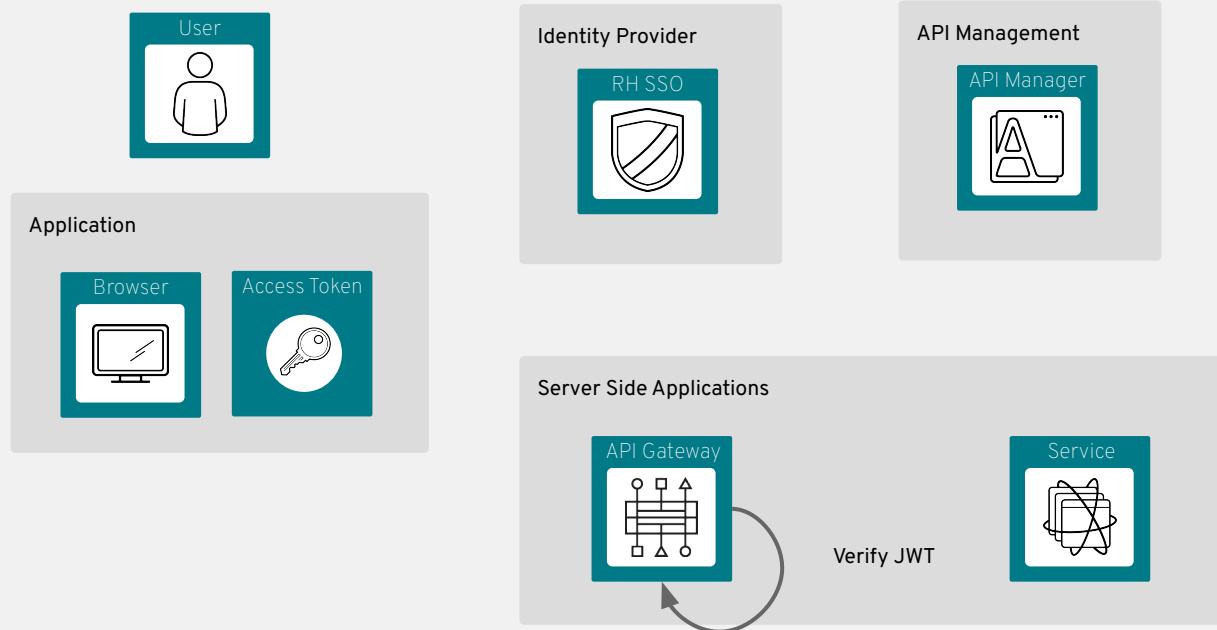
# AUTHORIZATION CODE FLOW

#10 - Web App Submits The Bearer Token



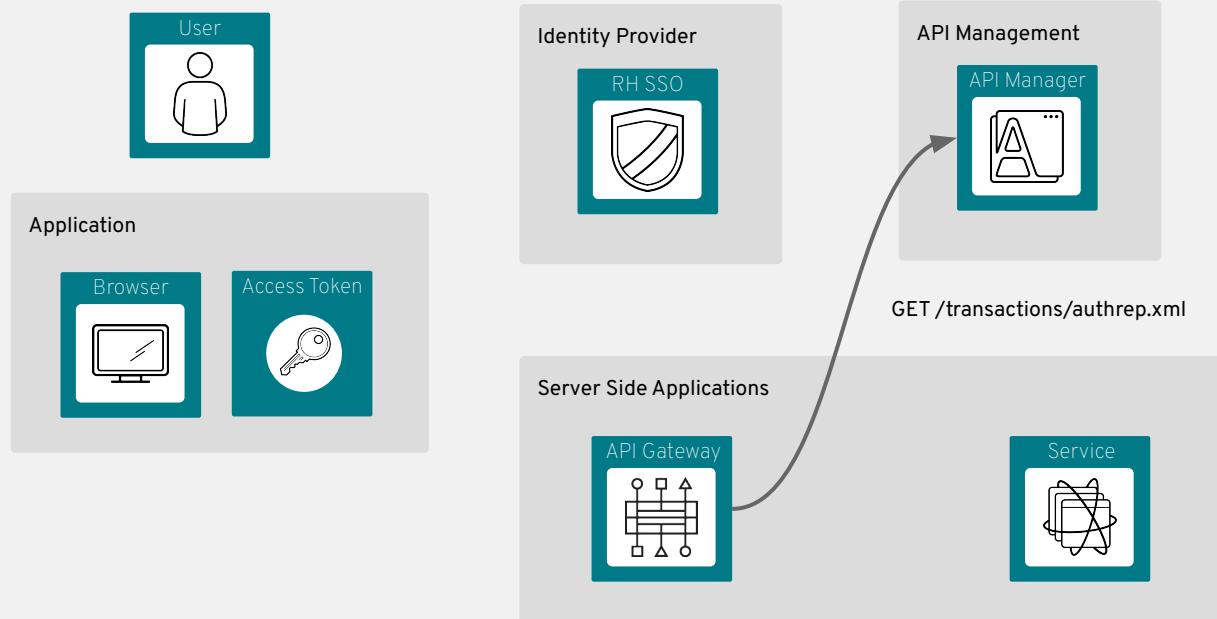
# AUTHORIZATION CODE FLOW

## #10.1 - Gateway Verifies Token



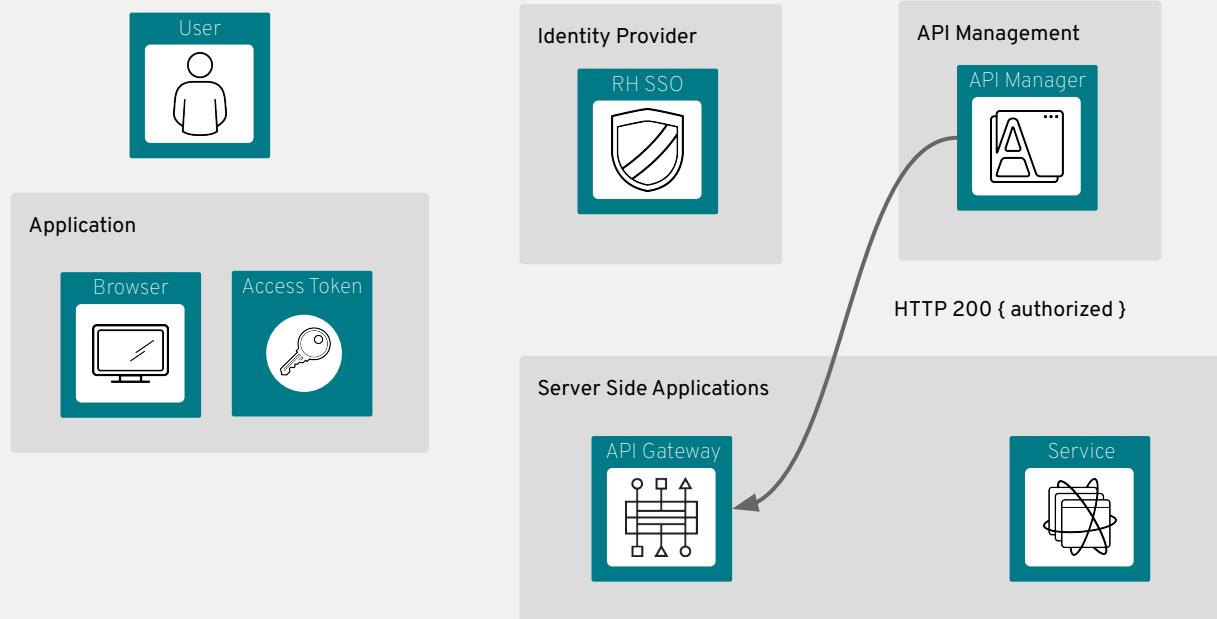
# AUTHORIZATION CODE FLOW

## #10.2 - Gateway Requests Auth To API Manager



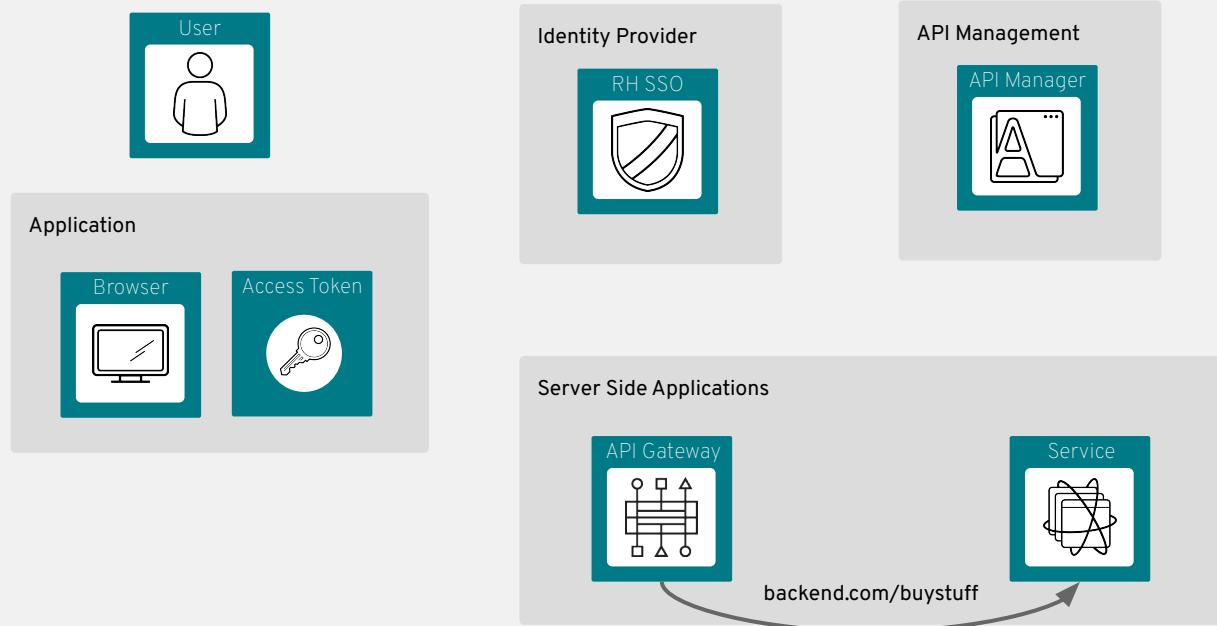
# AUTHORIZATION CODE FLOW

## #10.3 - API Manager Response “Authorized”



# AUTHORIZATION CODE FLOW

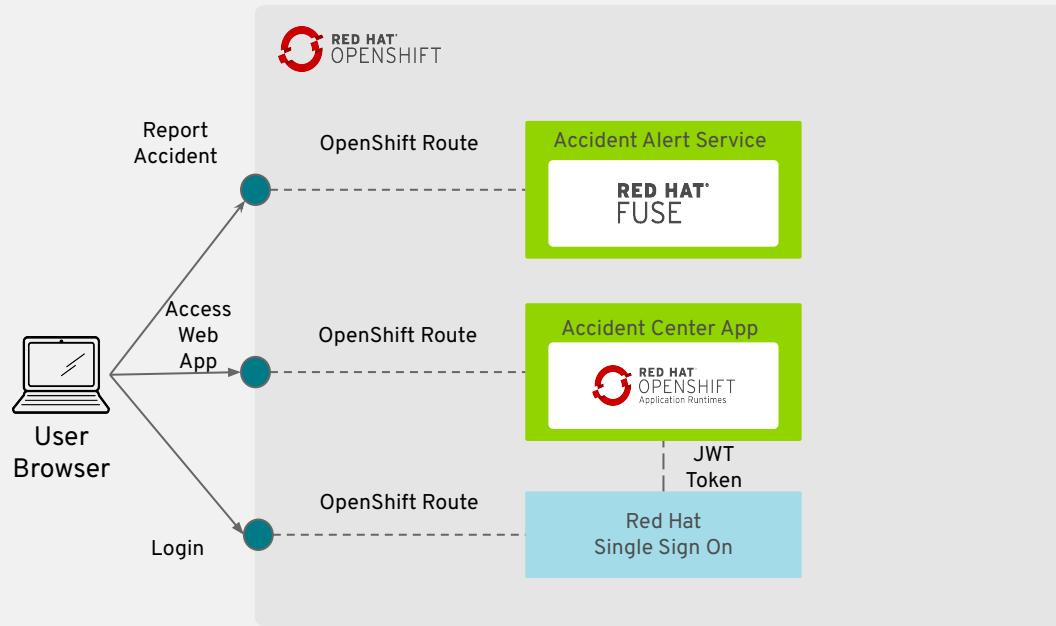
## #10.3 - Gateway Calls Backend API



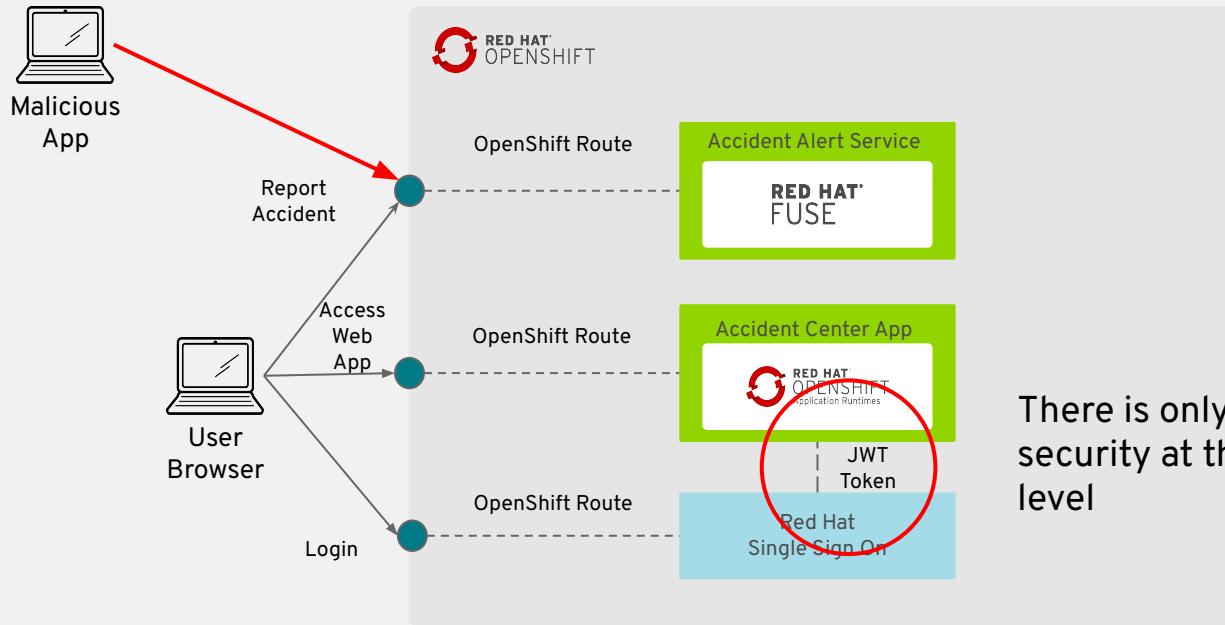
---

# Demo

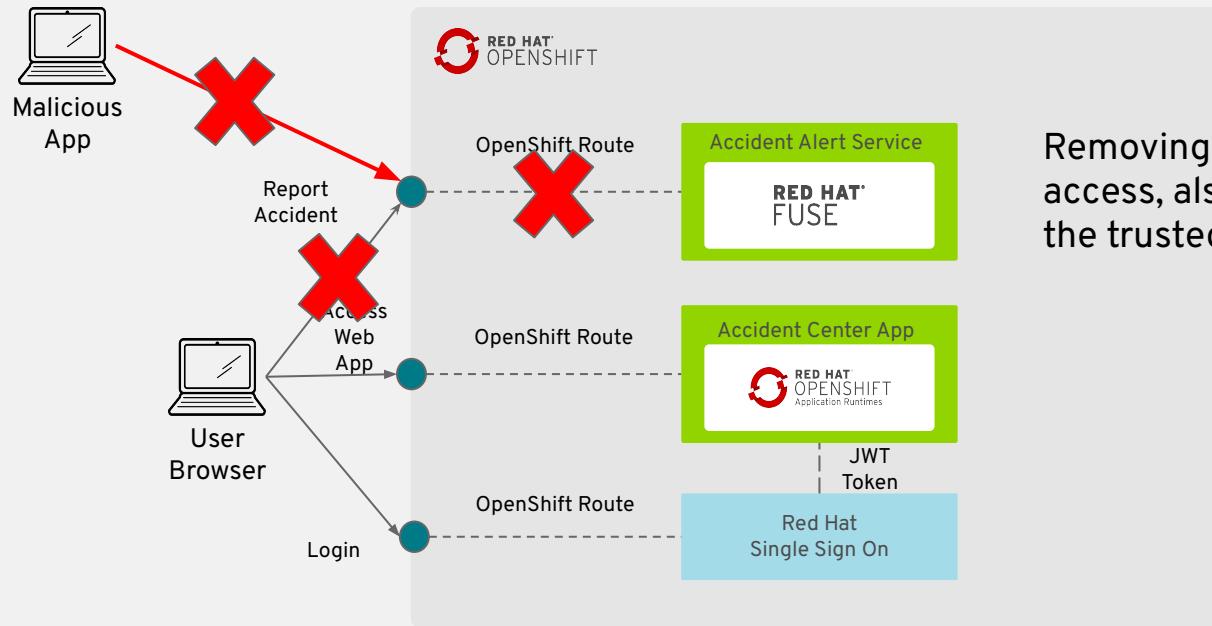
# INITIAL SCENARIO



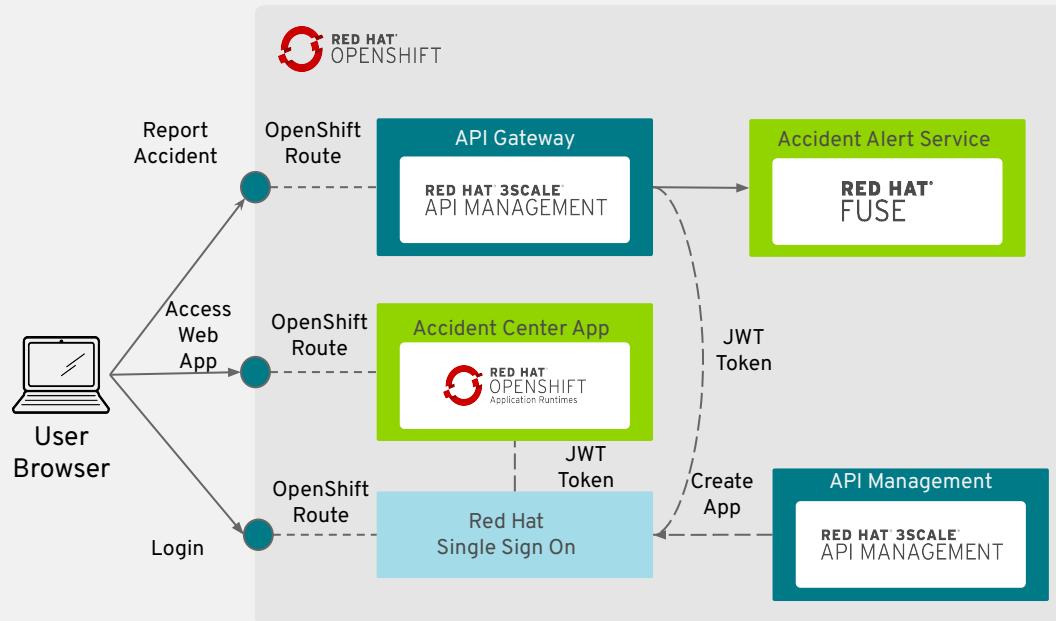
# INSECURE SCENARIO



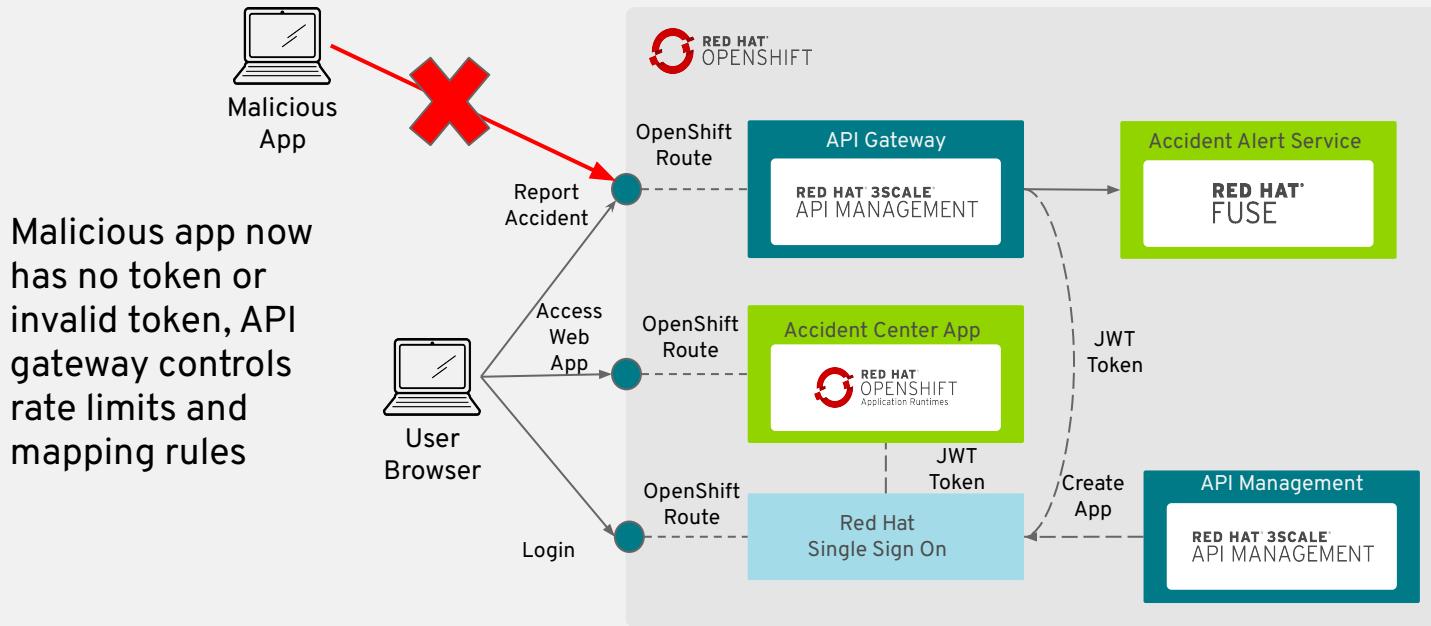
# ISOLATE BACKEND API



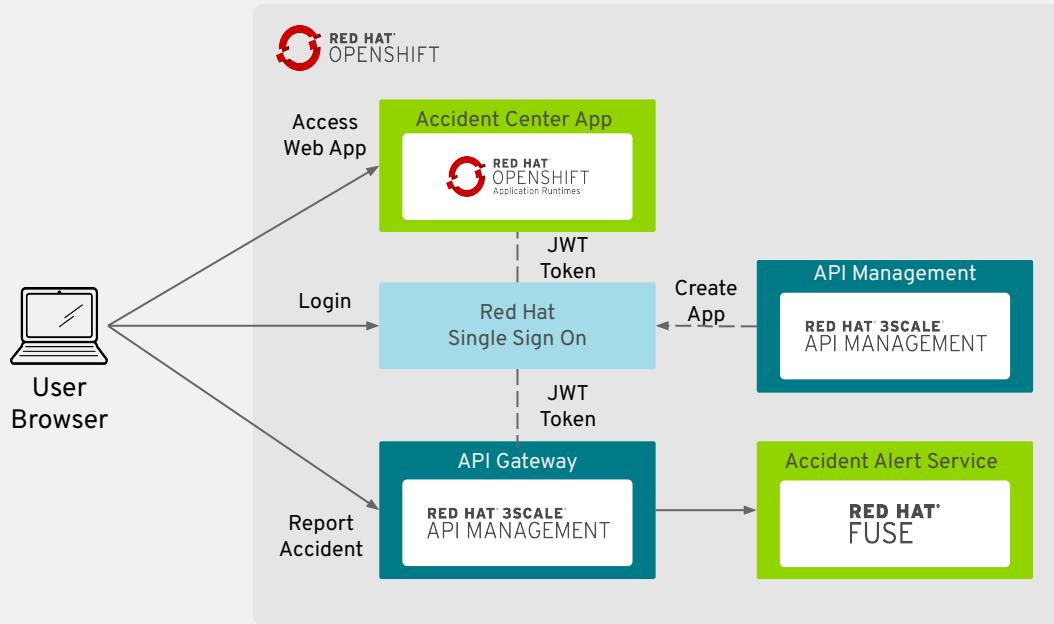
# SECURING THE SERVICE



# SECURING THE SERVICE



# FINAL DEPLOYMENT



---

# Partner Led Workshops (PLWs)

# Agile Integration Roadshows

## API Centric Strategy



### Enabling your API-Centric Strategy

A Day In The Life

## Event Driven Architecture



### Event-Driven Architecture Workshop

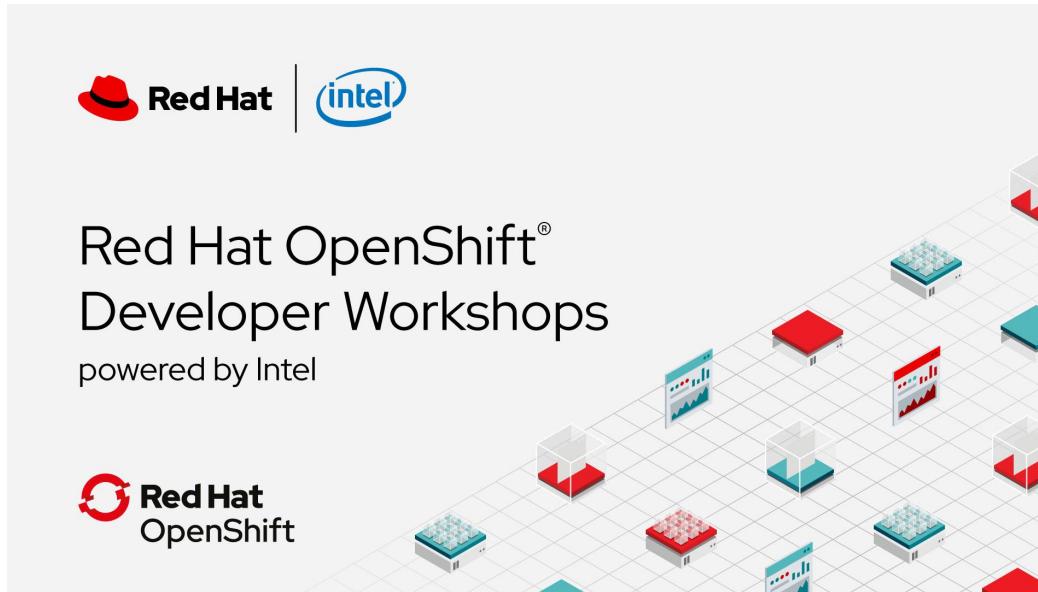
A Day In The Streaming Life

Contact: Iveta Babulenkova, Red Hat EMEA Partner Development Manager -

[iveta.babulenkova@redhat.com](mailto:iveta.babulenkova@redhat.com)

# OSDW

## Openshift Developer Workshops



Program overview: <https://osdw.redhat-partner.com/>

73

Contact: Iveta Babulenkova, Red Hat EMEA Partner Development Manager -

[iveta.babulenkova@redhat.com](mailto:iveta.babulenkova@redhat.com)

---

# Q & A



# Thank you



[linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)



[youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)



[twitter.com/RedHat](https://twitter.com/RedHat)