Asia's Largest

Cloud & AI

Conference 2023

17 - 18, November 2023
IIT Madras Research Park, Chennai

Beyond Barriers: Addressing Access Control Challenges with OPA & Keto

Vivek Dhayalan
Founder, TechConative

Kannan Ramamoorthy
Co-Founder, TechConative

Does your application have a Login Page?

Are you using social logins in your App?

What’s the protocol used for Social Logins?

Is OAuth an Authentication protocol?

Is OpenID built with additional layer in OAuth 2.0 an authentication protocol?

Authentication

Process of verifying the identity.

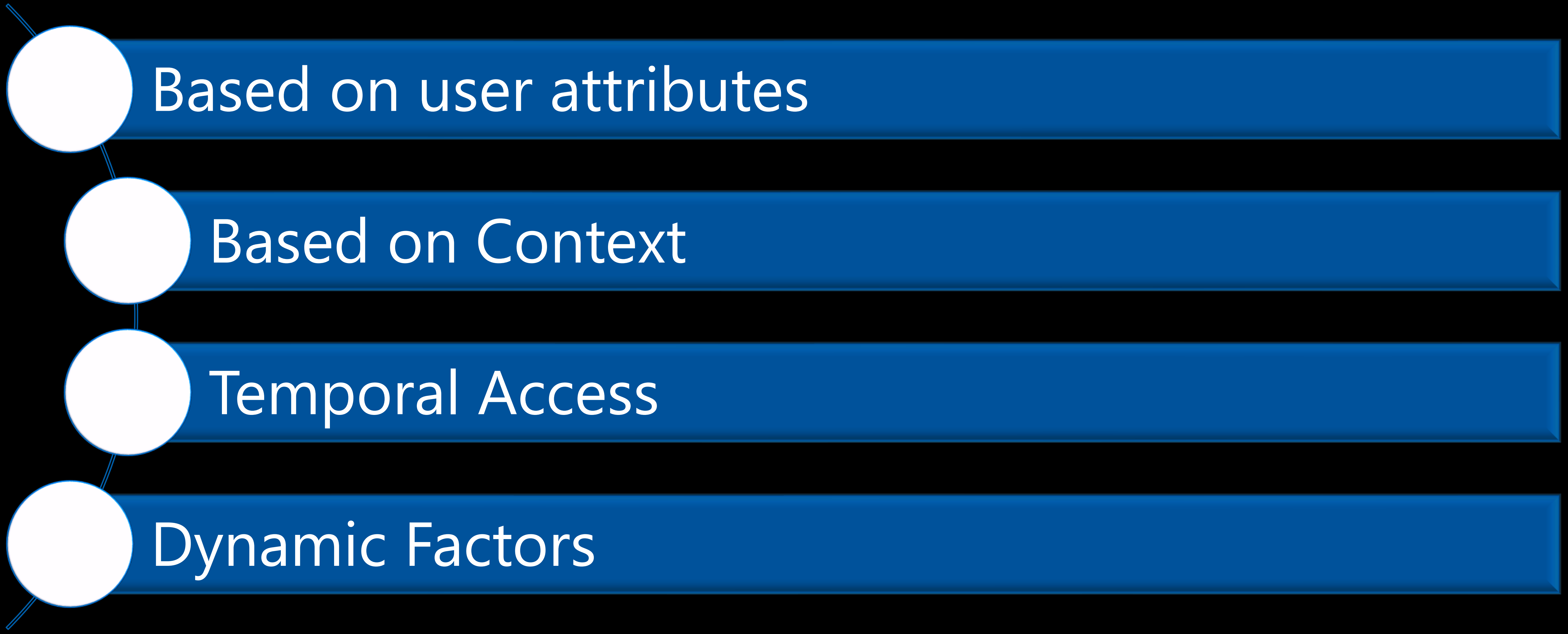
Access Control

Process of controlling access to resources, services, or information in a system.

Authorization

Specific aspect of Access Control focuses on granting or denying access for authenticated resources.

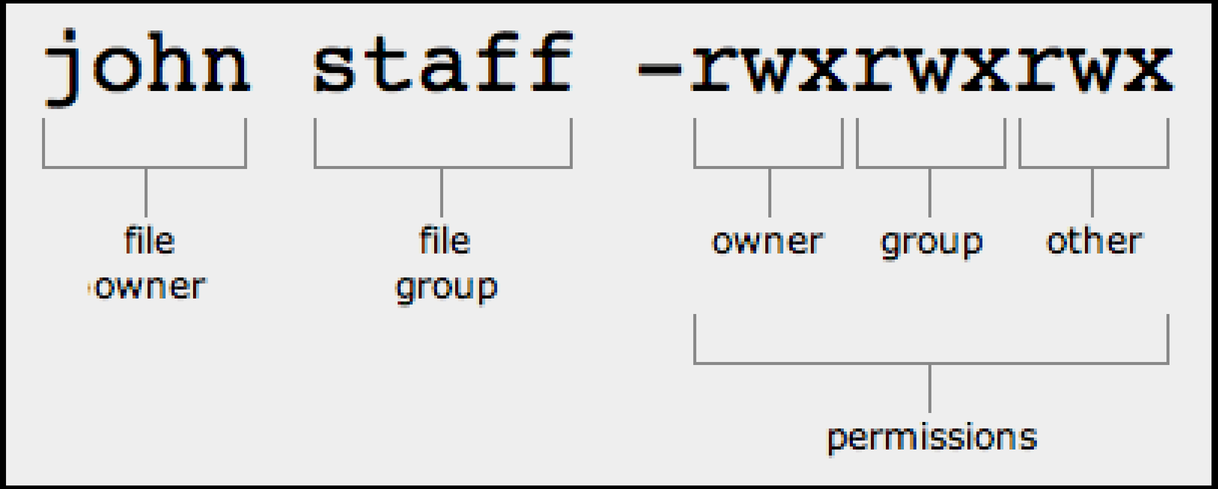
Common Access Control Scenarios



- Based on user attributes
- Based on Context
- Temporal Access
- Dynamic Factors

Discretionary Access Control

- Control lay with resource owner
- File System in Unix / Linux



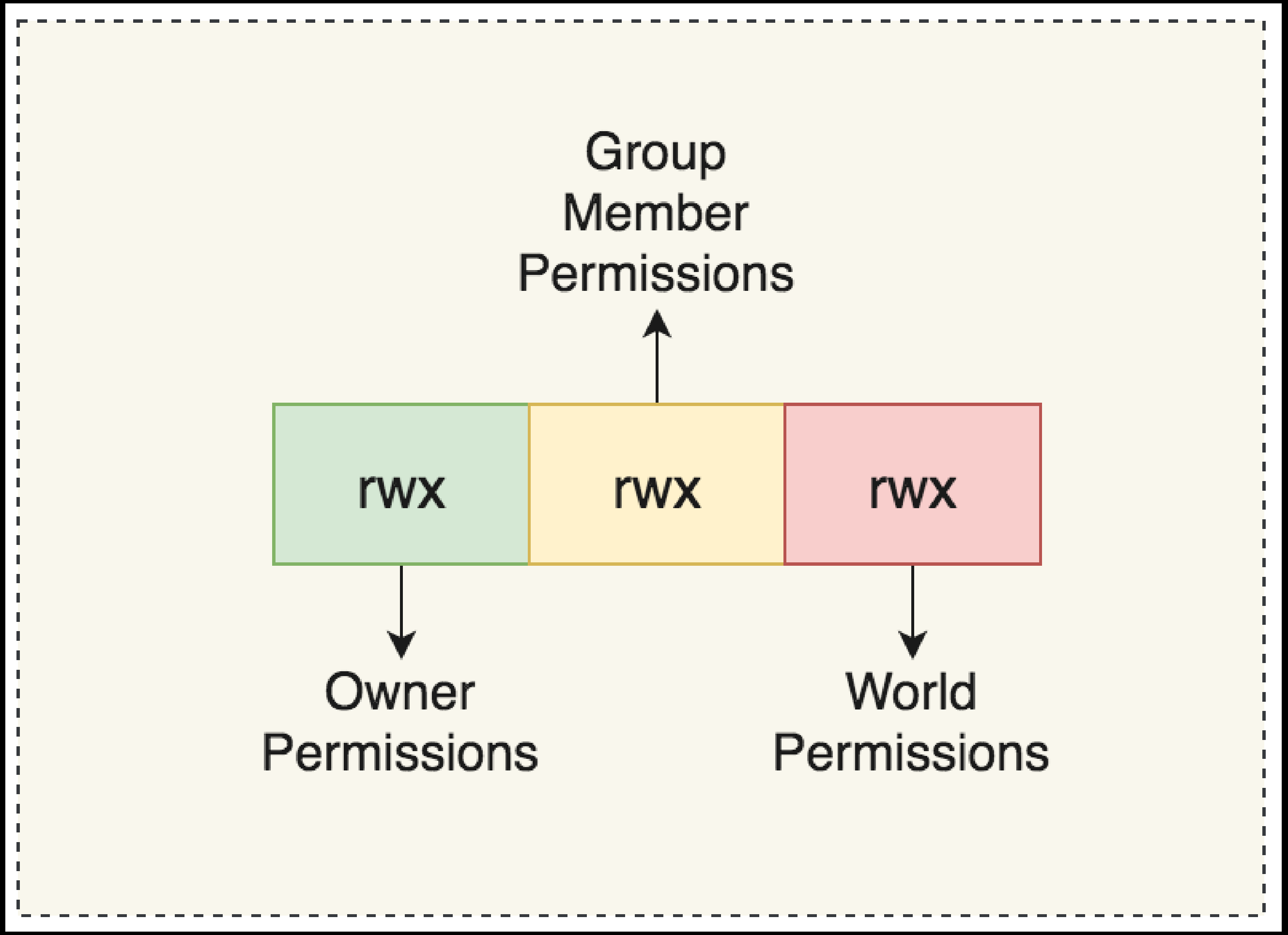
john staff -rwxrwxrwx

file owner

file group

owner group other

permissions



Group Member Permissions

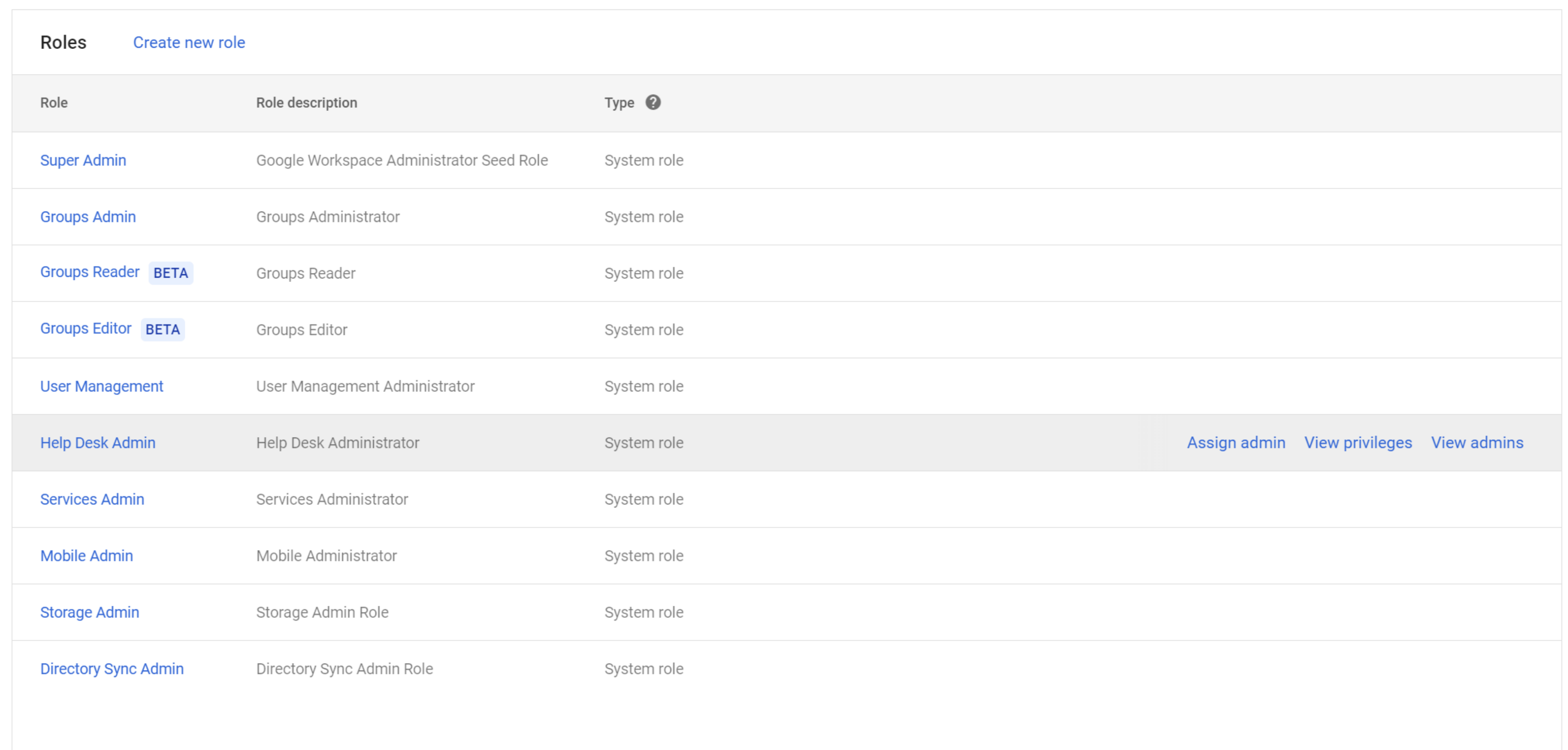
rwx rwx rwx

Owner Permissions

World Permissions

Role-Based Access Control

- Based on role membership.
- Google Workspace / G Suit Roles

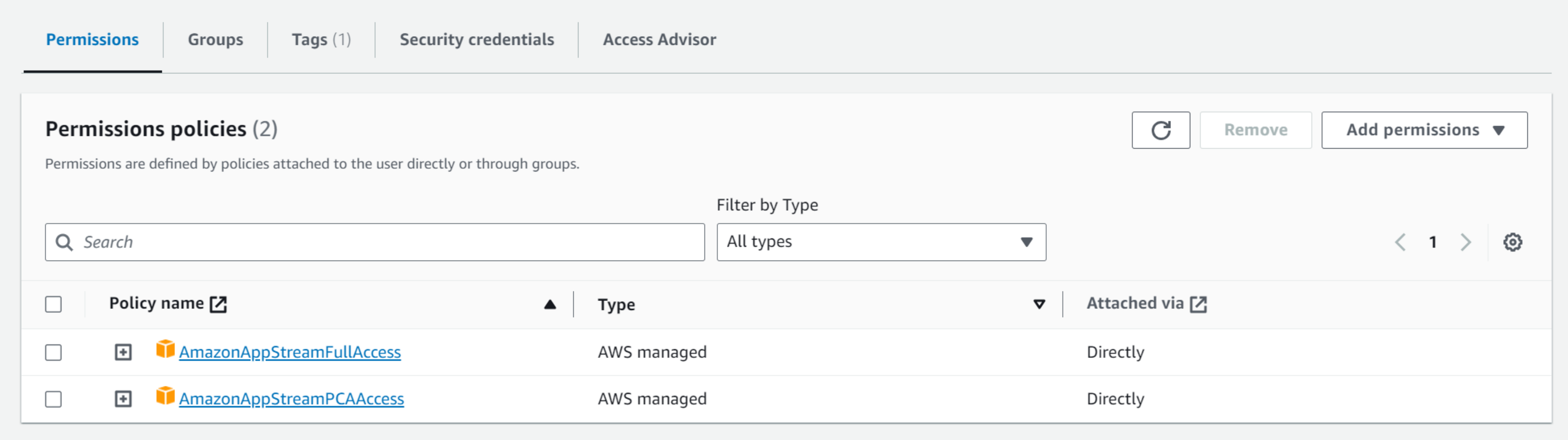


Roles   Create new role

Role	Role description	Type	
Super Admin	Google Workspace Administrator Seed Role	System role	
Groups Admin	Groups Administrator	System role	
Groups Reader BETA	Groups Reader	System role	
Groups Editor BETA	Groups Editor	System role	
User Management	User Management Administrator	System role	
Help Desk Admin	Help Desk Administrator	System role	Assign admin View privileges View admins
Services Admin	Services Administrator	System role	
Mobile Admin	Mobile Administrator	System role	
Storage Admin	Storage Admin Role	System role	
Directory Sync Admin	Directory Sync Admin Role	System role	

Attribute Access Control

- Based on user attributes.
- AWS IAM.



Permissions policies (2)

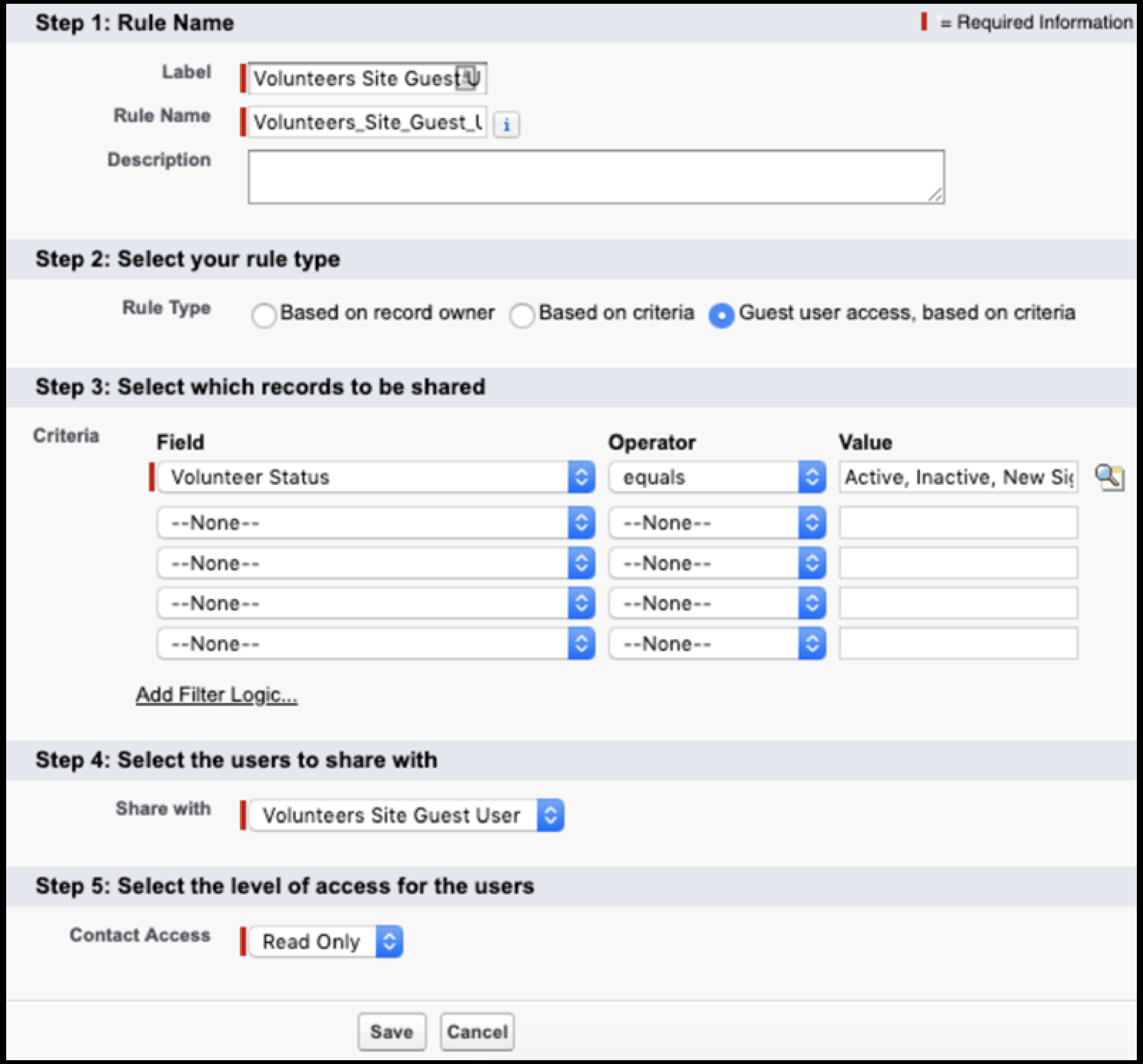
Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

□	Policy name	Type	Attached via
□	AmazonAppStreamFullAccess	AWS managed	Directly
□	AmazonAppStreamPCAAccess	AWS managed	Directly

Rule-Based Access Control

- Policies are defined through rules or conditions
- Salesforce CRM



Step 1: Rule Name

= Required Information

Label	Volunteers Site Guest U
Rule Name	Volunteers_Site_Guest_U
Description	

Step 2: Select your rule type

Rule Type: ○ Based on record owner ○ Based on criteria ● Guest user access, based on criteria

Step 3: Select which records to be shared

Criteria

Field	Operator	Value
Volunteer Status	equals	Active, Inactive, New Si
--None--	--None--	
--None--	--None--	
--None--	--None--	
--None--	--None--	

Add Filter Logic...

Step 4: Select the users to share with

Share with: Volunteers Site Guest User

Step 5: Select the level of access for the users

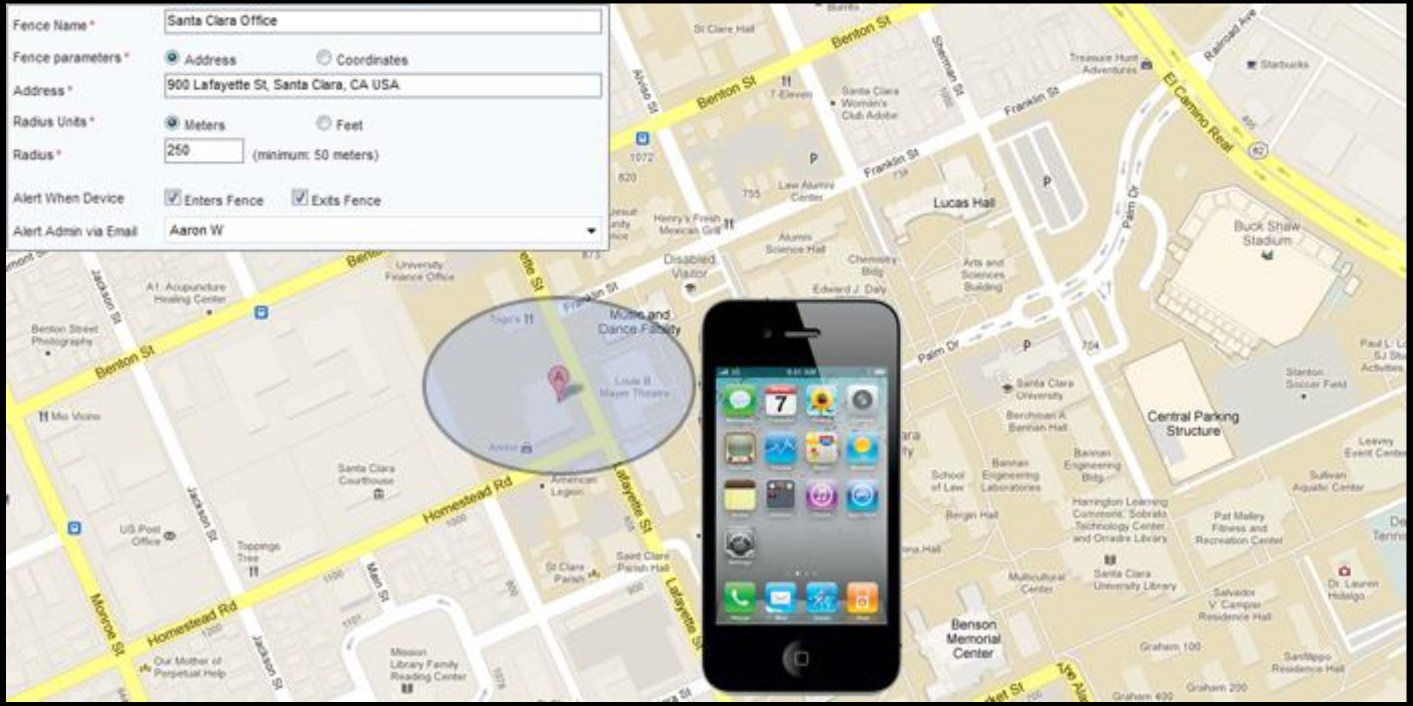
Contact Access: Read Only

Time-Based Access Control

- Access control based on specific time window
- Balance Mouse from Samsung (Ad)

Location-Based Access Control

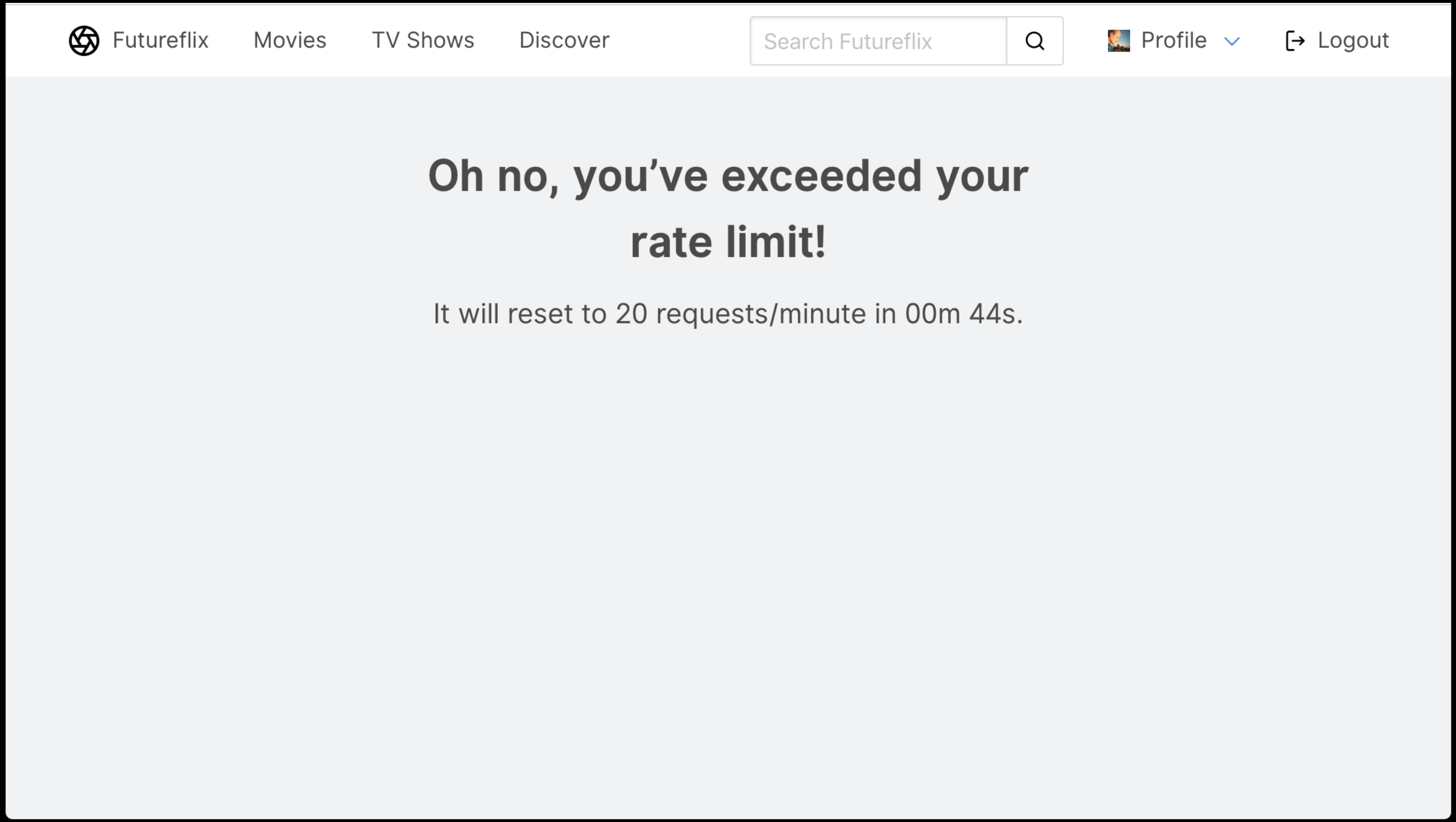
- Restrictions based on location
- Mobile Device Management



Fence Name *	Santa Clara Office	
Fence parameters *	● Address	○ Coordinates
Address *	900 Lafayette St, Santa Clara, CA USA	
Radius Units *	● Meters	○ Feet
Radius *	250	(minimum: 50 meters)
Alert When Device	☑ Enters Fence	☑ Exits Fence
Alert Admin via Email	Aaron W	

Usage-Based Access Control

- Limits on resource usage
- API/Service rate limiting

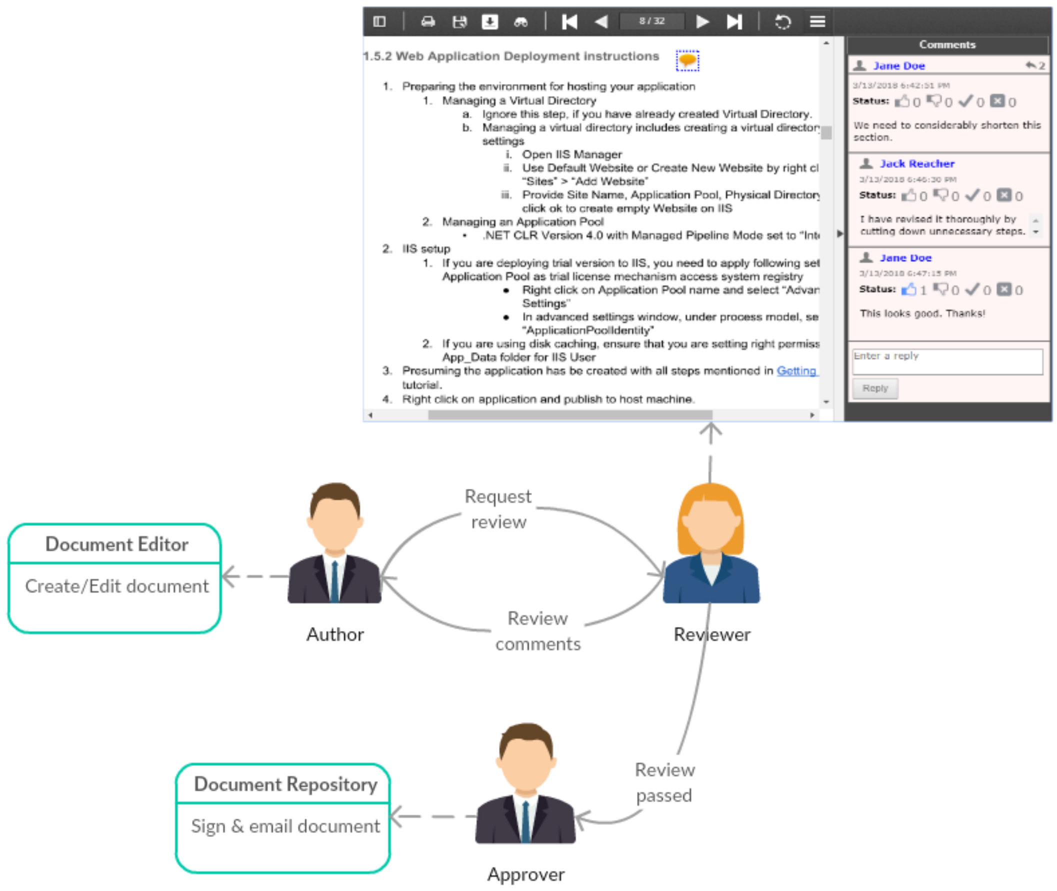


Oh no, you’ve exceeded your rate limit!

It will reset to 20 requests/minute in 00m 44s.

Capability-Based Access Control

- Possession of a specific capability
- Smart contracts
- Workflow System



1.5.2 Web Application Deployment instructions

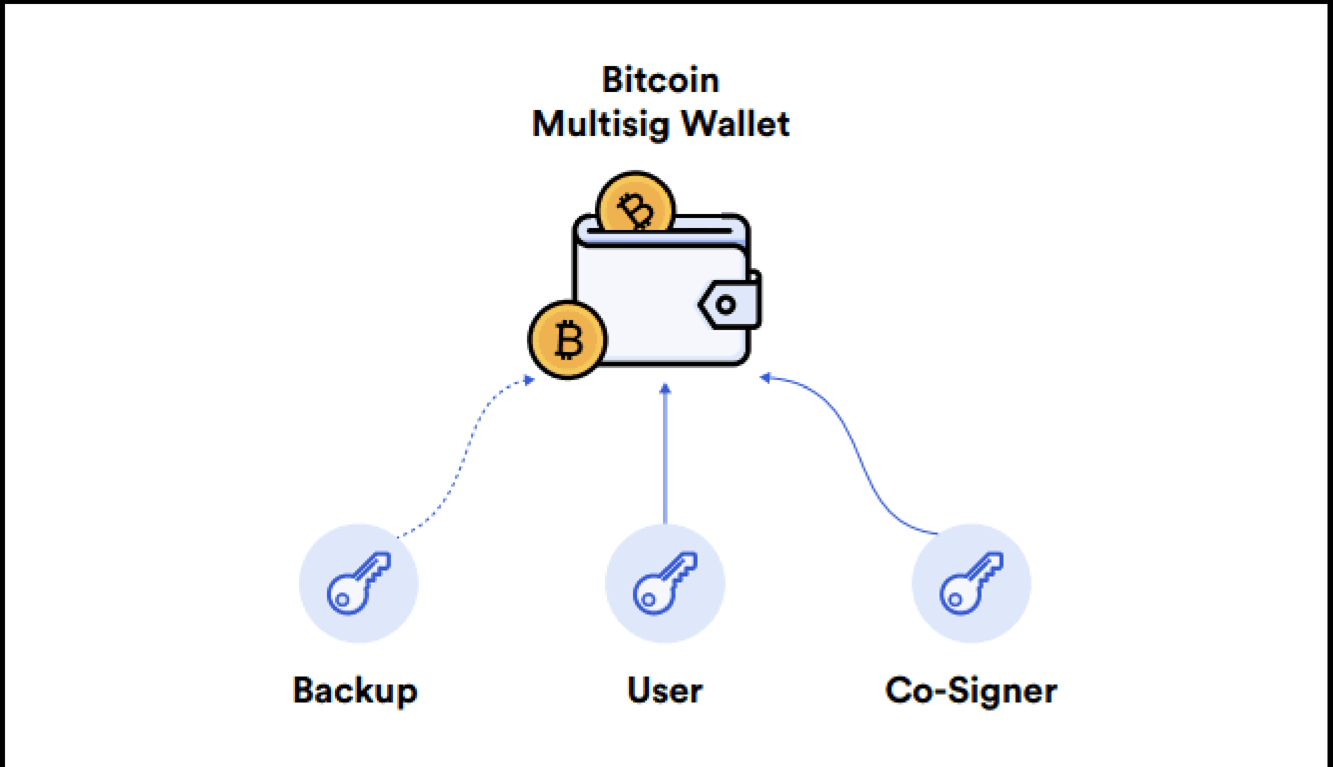
1. Preparing the environment for hosting your application
    1. Managing a Virtual Directory
        a. Ignore this step, if you have already created Virtual Directory.
        b. Managing a virtual directory includes creating a virtual director settings
            i. Open IIS Manager
            ii. Use Default Website or Create New Website by right cl "Sites" > "Add Website"
            iii. Provide Site Name, Application Pool, Physical Director click ok to create empty Website on IIS
    2. Managing an Application Pool
        - .NET CLR Version 4.0 with Managed Pipeline Mode set to "Int
2. IIS setup
    1. If you are deploying trial version to IIS, you need to apply following set Application Pool as trial license mechanism access system registry
        - Right click on Application Pool name and select "Advan Settings"
        - In advanced settings window, under process model, se "ApplicationPoolIdentity"
    2. If you are using disk caching, ensure that you are setting right permiss App_Data folder for IIS User
3. Presuming the application has be created with all steps mentioned in Getting tutorial.
4. Right click on application and publish to host machine.

Comments

Jane Doe ↰2
3/13/2018 6:42:51 PM
Status: 👍 0 👎 0 ✓ 0 ☒ 0
We need to considerably shorten this section.

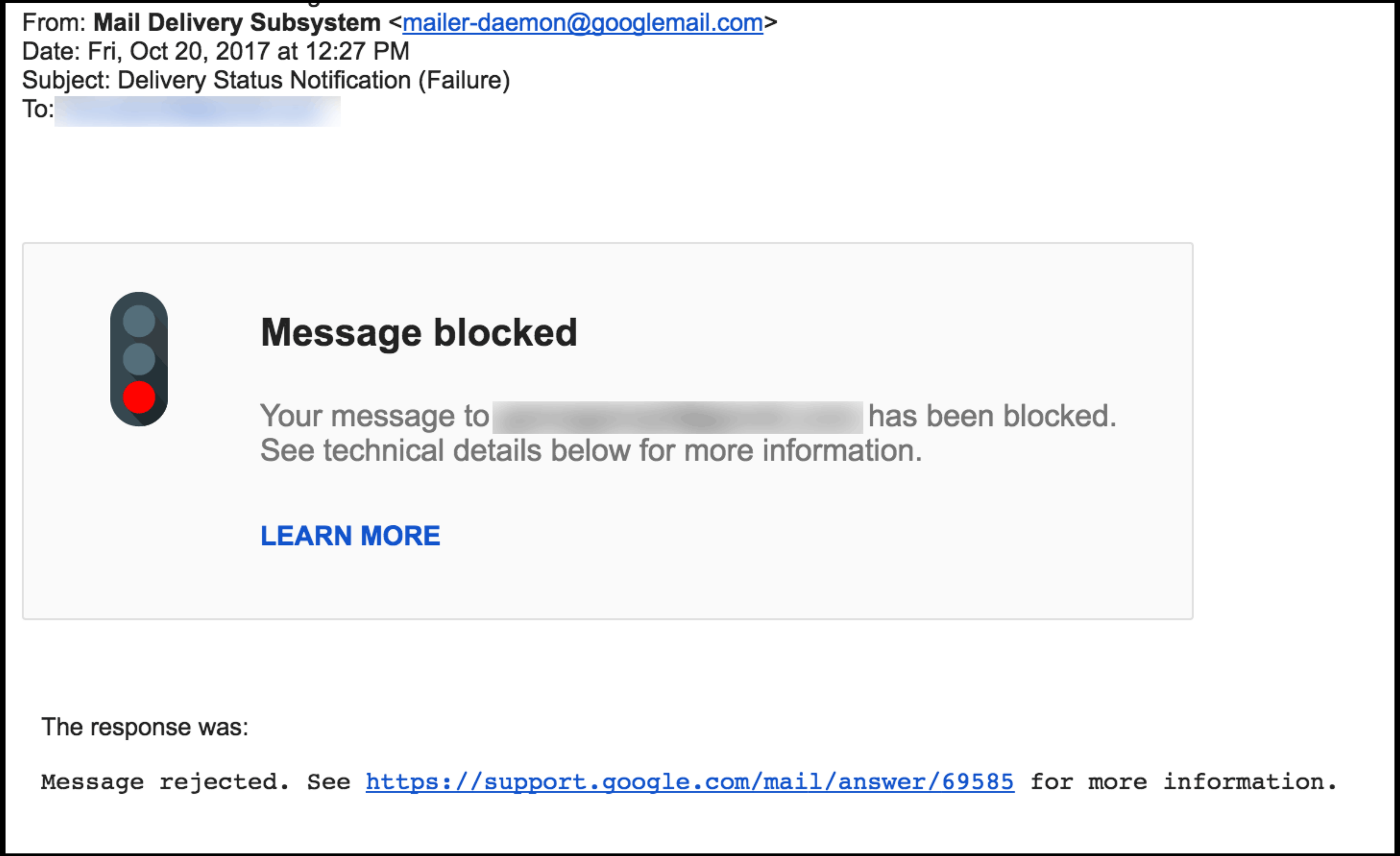
Jack Reacher
3/13/2018 6:46:30 PM
Status: 👍 0 👎 0 ✓ 0 ☒ 0
I have revised it thoroughly by cutting down unnecessary steps.

Jane Doe
3/13/2018 6:47:15 PM
Status: 👍 1 👎 0 ✓ 0 ☒ 0
This looks good. Thanks!



Content-Based Access Control

- Based on the content of the resource
- Email Systems with content-based filtering



From: **Mail Delivery Subsystem** <mailer-daemon@googlemail.com>
Date: Fri, Oct 20, 2017 at 12:27 PM
Subject: Delivery Status Notification (Failure)
To: [redacted]

Message blocked

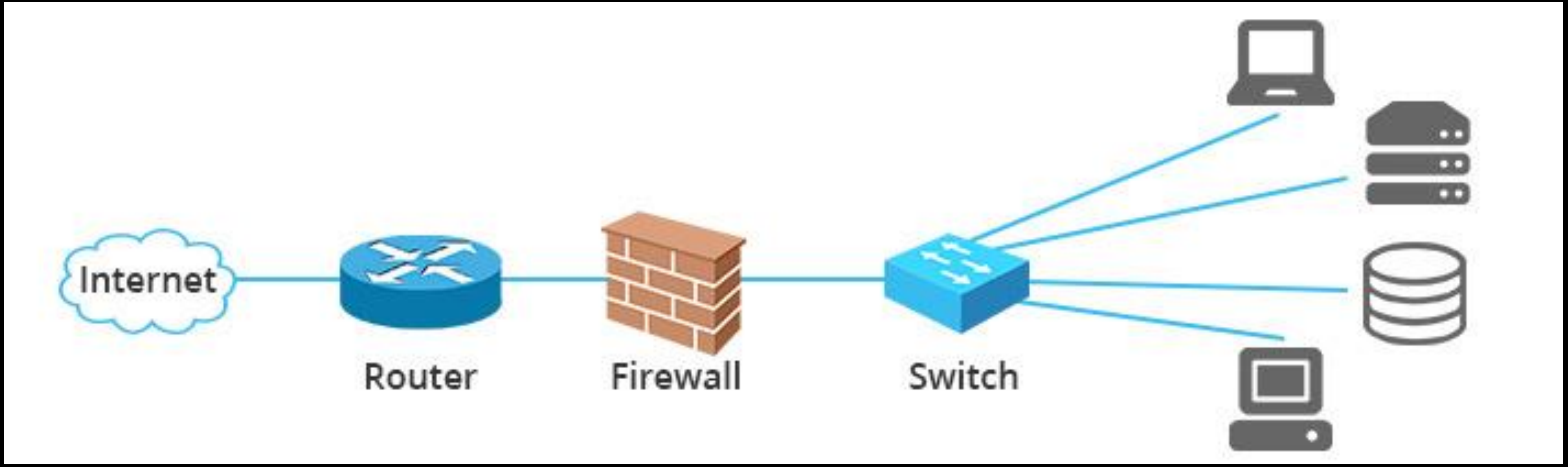
Your message to [redacted] has been blocked.
See technical details below for more information.

The response was:

```
Message rejected. See https://support.google.com/mail/answer/69585 for more information.
```

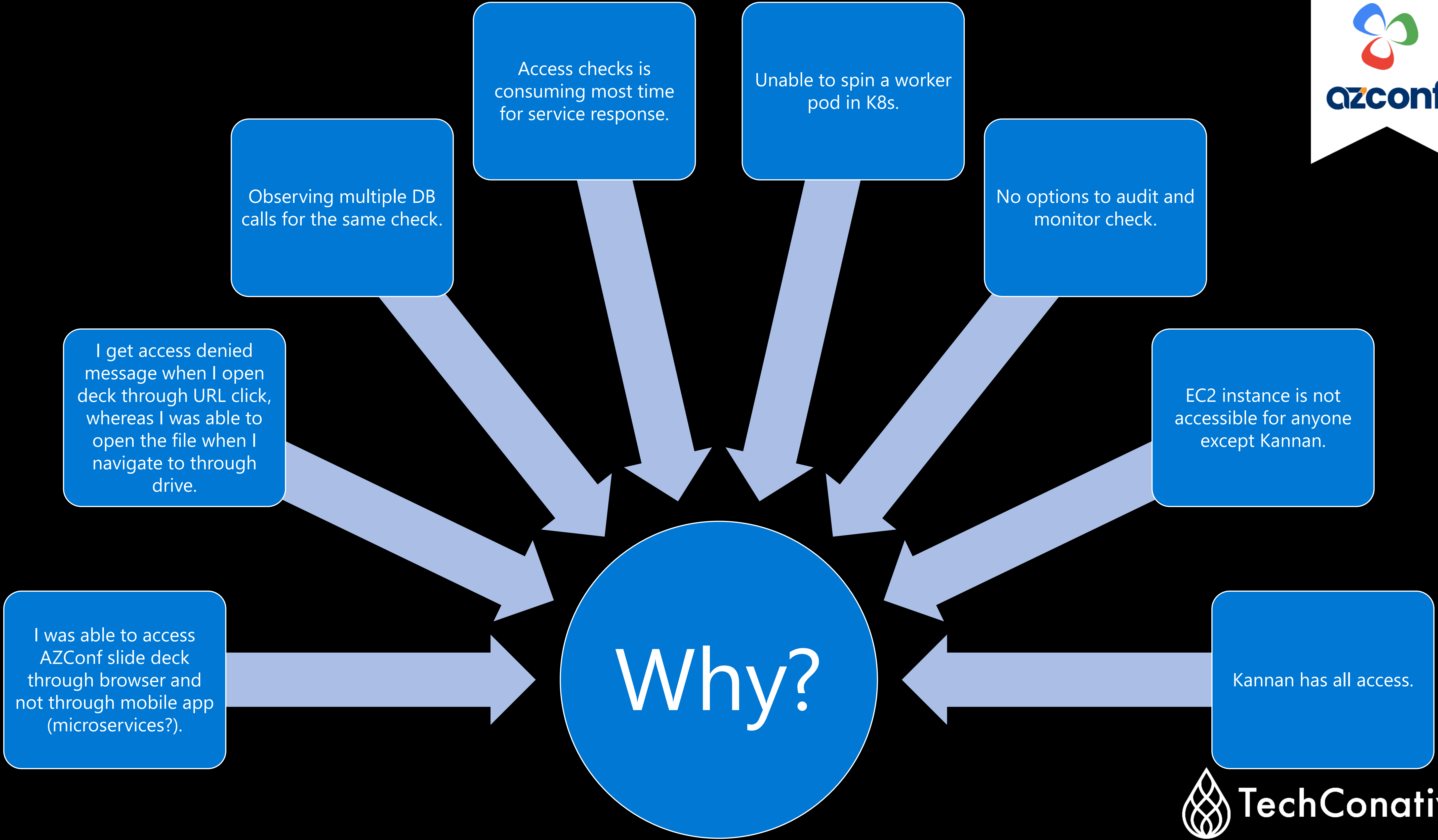
Access Control List

- Data structures that has information about granted access
- Routers & Firewalls



Access Control Techniques

- Discretionary Access Control → owner controls access
- Role-Based Access Control → based on role memberships
- Attribute-Based Access Control → based on user attributes
- Rule-Based Access Control → based on the policies
- Time-Based Access Control → based on specific time
- Location-Based Access Control → based on physical or network location
- Usage-Based Access Control → based on resource usage
- Capability-Based Access Control → based on possession of certain
- Content-Based Access Control → based on attributes of the resource
- Access Control List → based on list



I was able to access AZConf slide deck through browser and not through mobile app (microservices?).

I get access denied message when I open deck through URL click, whereas I was able to open the file when I navigate to through drive.

Observing multiple DB calls for the same check.

Access checks is consuming most time for service response.

Unable to spin a worker pod in K8s.

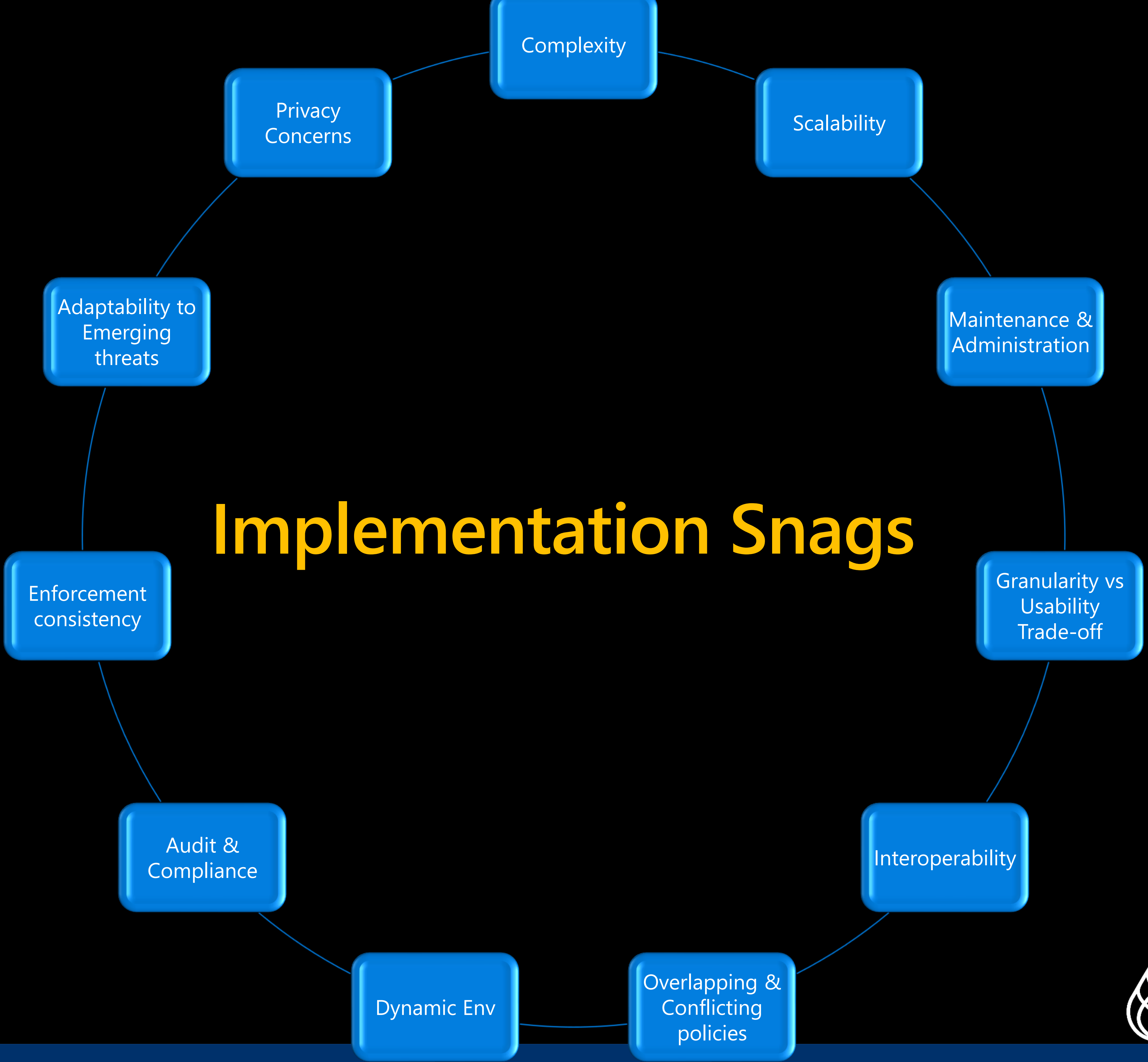
No options to audit and monitor check.

EC2 instance is not accessible for anyone except Kannan.

Kannan has all access.

Why?

Implementation Snags



Complexity

Scalability

Maintenance & Administration

Granularity vs Usability Trade-off

Interoperability

Overlapping & Conflicting policies

Dynamic Env

Audit & Compliance

Enforcement consistency

Adaptability to Emerging threats

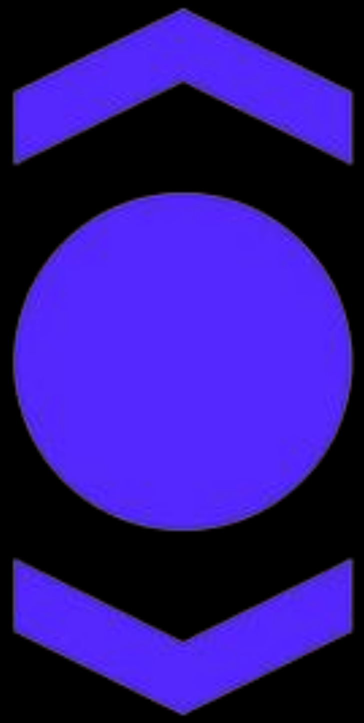
Privacy Concerns

To The Rescue

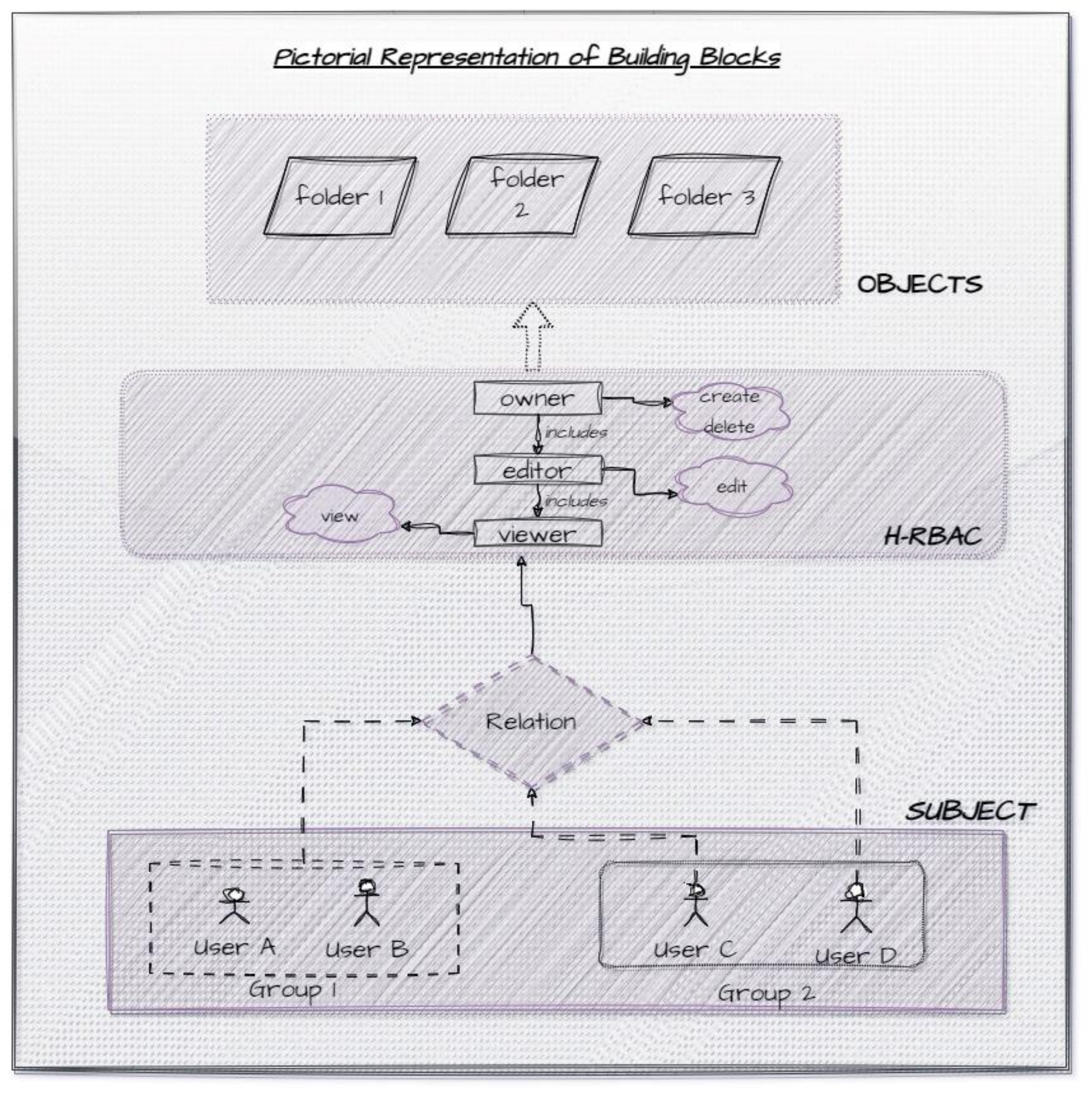
ORY – Keto | OPA

ORY – Keto

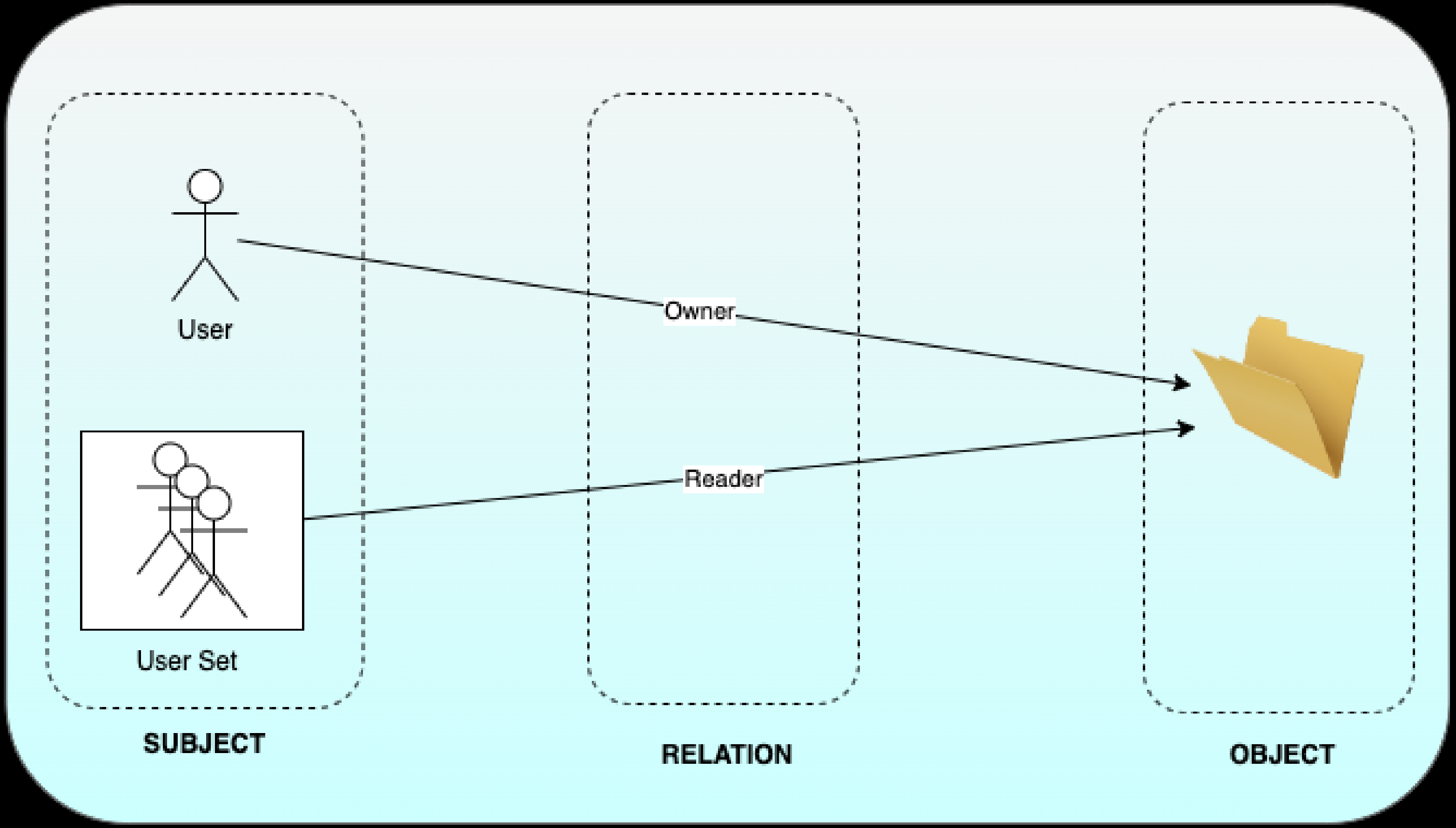
- Based on Google’s Zanzibar paper(2019).
- Subset implementation of Zanzibar.
- Array of services focused on enterprise authorization.
- Open-source - Self-hosted, Managed Services.



ORY – Keto - Primer



ORY – Keto - Primer



ORY - Keto’s way

Problems:

- Complex and inconsistent access definitions.
- Inconsistent & scattered implementation

ORY’s solution:

- Keto’s server answering the authz calls. - Avoiding scattered implementations
- ORY Permission Language - Effort to standardize permission definition.

ORY - Keto’s way

Problems:

- Performance and scalability.

ORY’s solution:

- Based on Zanzibar, which is built for internet scale with a 99.9th percentile of 93ms.

ORY - Keto’s way

Problems:

- Cost of development

ORY’s solution:

- Proven design available for use.
- Array of tools to secure enterprise systems.
- Managed service available to minimize OPS efforts.

ORY - Keto

ORY - Keto

ORY - Keto - Catches

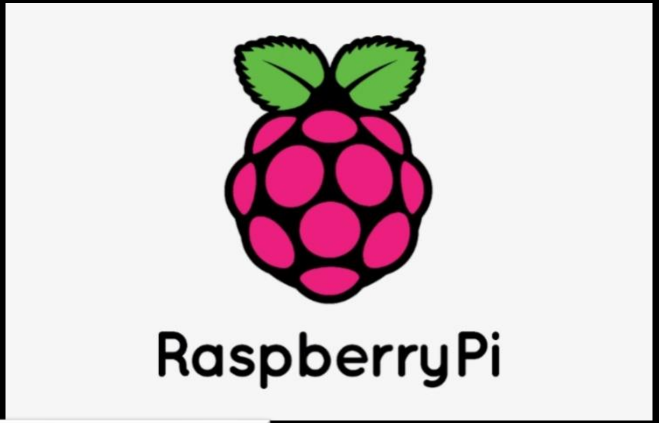
- Based on Google’s Zanzibar paper (2019). - But not Zanzibar yet.
- The claim of 93ms at 99.9 percentile comes from running server in the magnitude of 10,000 X.
- With a single-server setup of 100 users and 200 resources we got 95th percentile as 15.1s (not ms!)

ORY - Keto - When not to use?

You “might” not need when “ALL” the below conditions are met

- Your authz rules can be kept in-memory.
- Getting your context data is not costly(For example, ACL type list containing list of allowed users is costly to get).
- When you need dynamic resource types and rules, ORY Keto is still evolving on this front.

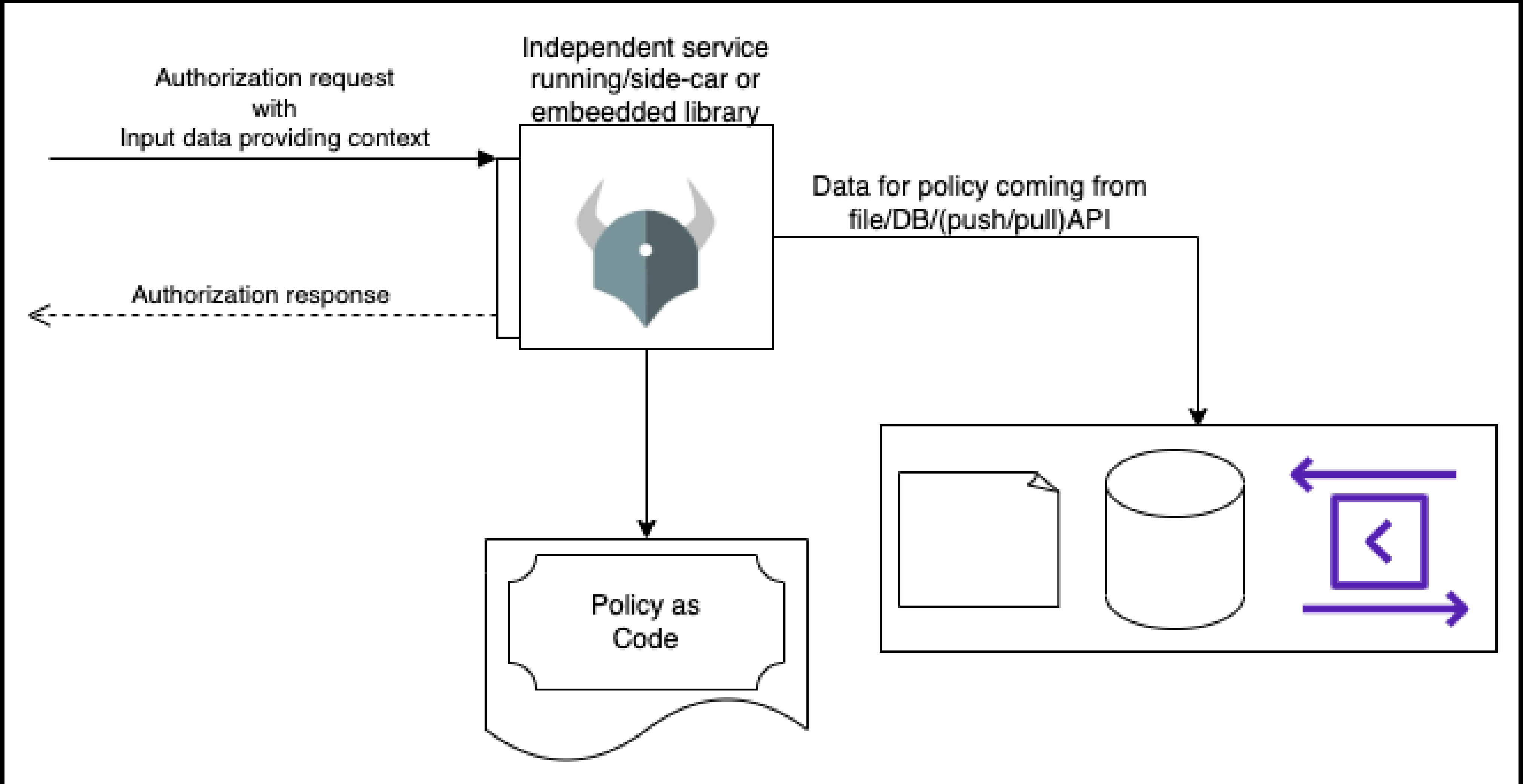
Companies using ORY Keto



OPA(Open Policy Agent)

- CNCF support project(“Graduated” level)
- General purpose policy engine.
- Supported modes - Embedded, side-car, Individual service.

OPA - Primer



Independent service running/side-car or embeedded library

Authorization request with Input data providing context

Authorization response

Data for policy coming from file/DB/(push/pull)API

Policy as Code

OPA’s way of solving

Problems:

- Complex and inconsistent access definitions.
- Inconsistent & scattered implementation

OPA’s solution:

- OPA server answering the authz calls. - Avoiding spread-across implementations
- Rego - Permission DSL.
- Testing frameworks - Helps on catching ambiguous definitions upfront.

OPA’s way of solving

Problems:

- Cost of development

OPA’s solution:

- Matured policy engine, available for use right away.
- Ecosystem of tools helps in fast and stable progress of authz definitions.

OPA’s way of solving

Problems:

- Performance and scalability

OPA’s solution:

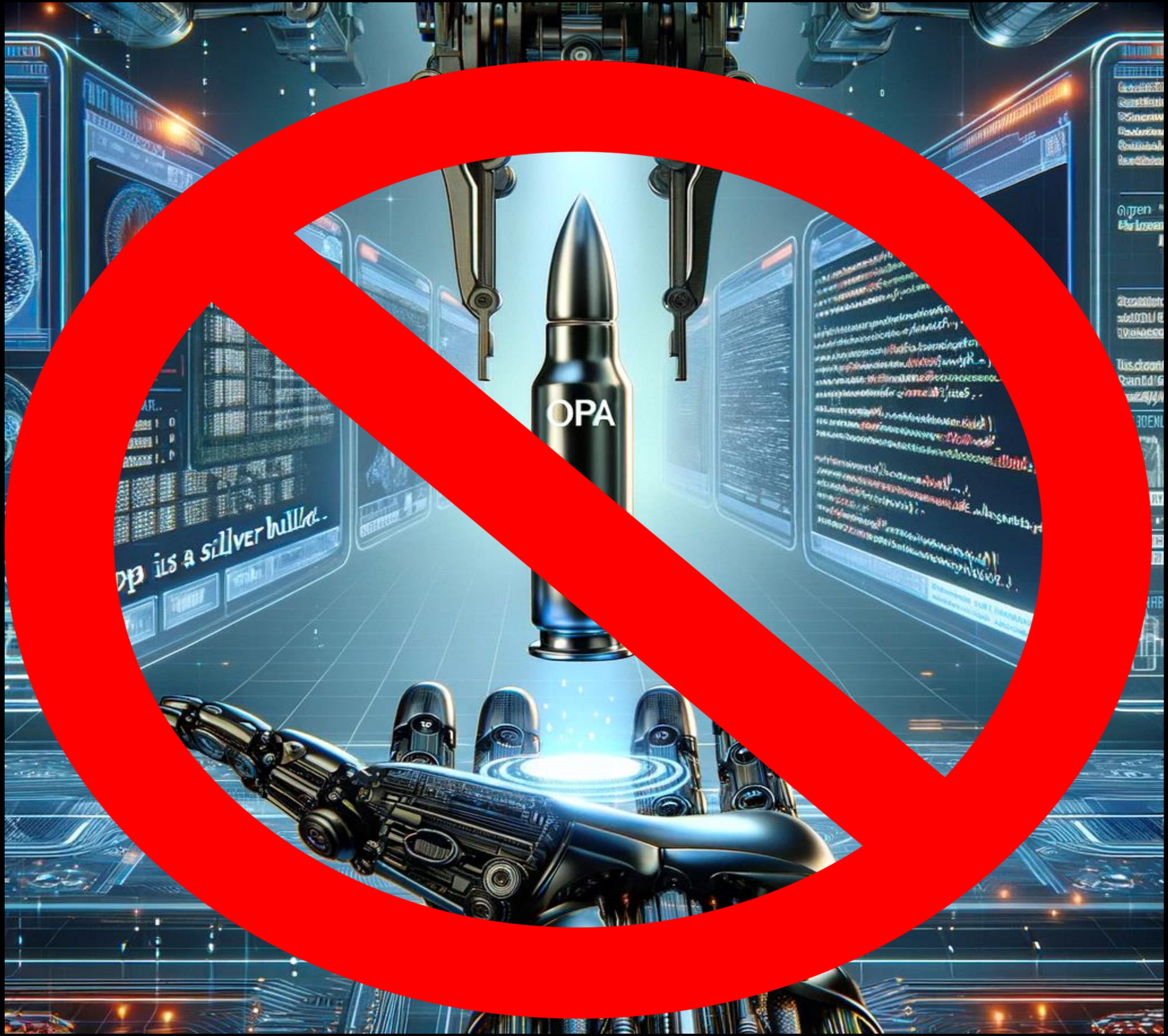
- In-memory policy engine.
- Sidecar/embedded packaging.

OPA - Other advantages

- Tools like Rego playground, IDE plugin.
- Compilation of policies in to WASM module.
- Enterprise microservice ecosystem integrations eg Envoy, Istio, K8S, etc

OPA - A silver Bullet?

OPA - A silver Bullet?



TechConative

OPA - When not to use?

Handling Huge Context Data

- Having the policies and (context) Data in-memory poses practical challenges.
- Not ideal for designs like ACLs(Access Control List).

Companies using OPA

Honourable Mentions

Gold Partner

PRESIDIO®

Silver Partner

ManageEngine
Site24x7
Crafted at ZOHO Corp.

SAGENT

Securra Health

kÿn
Where we belong

Syncfusion®

PRO

Q & A

Thank You!

TechConative

Vivek Dhayalan

Founder

Kannan Ramamoorthy

Co-Founder