
AWS
re:Inforce
JULY 26 – 27, 2022 | BOSTON, MA

IAM306

Managing B2B identity at scale: Lessons from AWS and Trend Micro

Suresh Sridharan (he/him)

Product Manager
AWS
@s_sridharan

Geoff Baskwill (he/him)

Software Architect
Trend Micro
@geoff_baskwill

Agenda

★**Introductions**

About Trend Micro Cloud One: where we were

About Amazon Cognito and multi-tenant SaaS solutions

Trend Micro Cloud One’s journey to Amazon Cognito

Key takeaways and additional resources

Introductions

Suresh Sridharan (he/him)
Product Manager, AWS
@s_sridharan

Geoff Baskwill (he/him)
Software Architect, Trend Micro
@geoff_baskwill

Agenda

Introductions

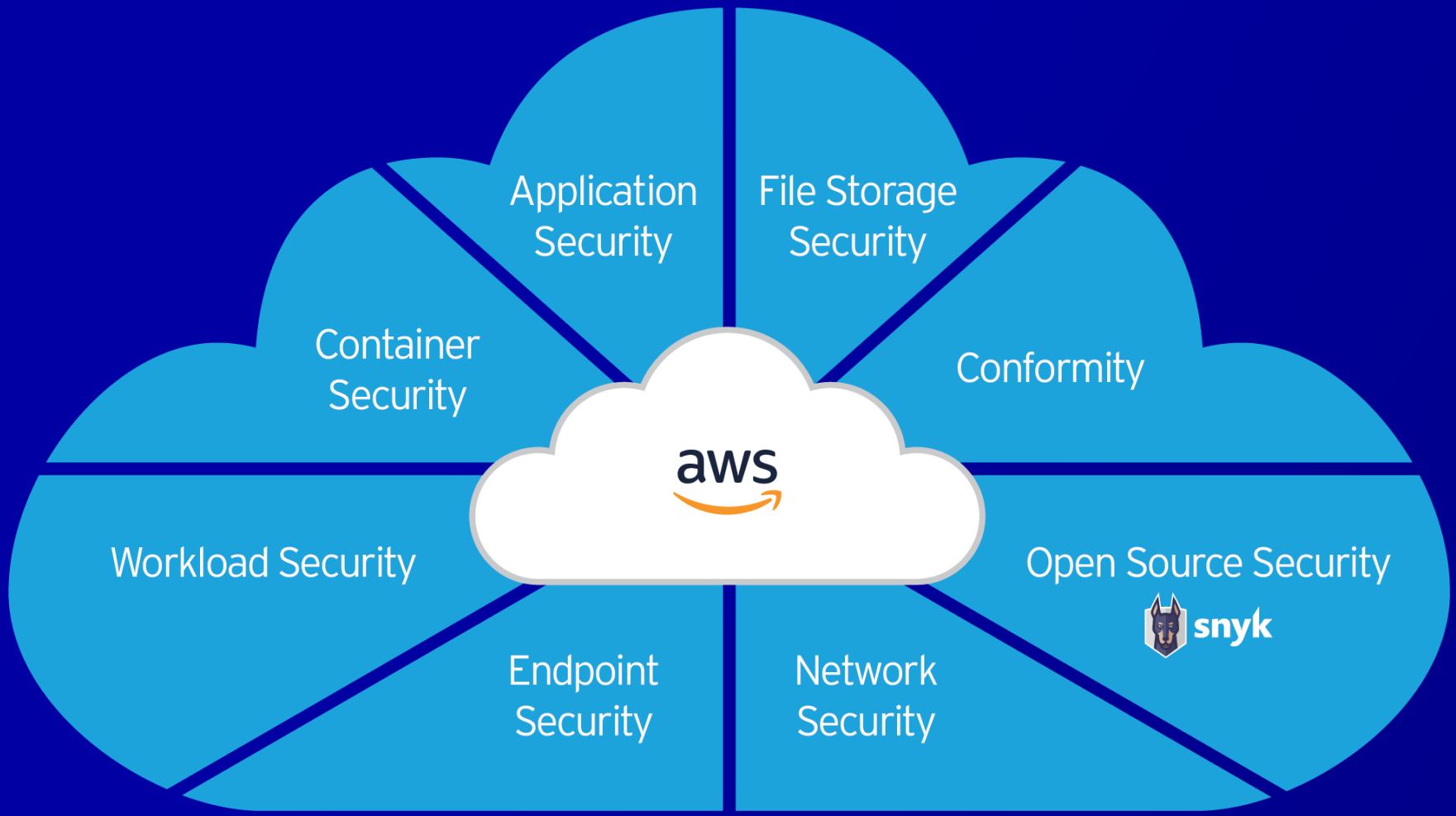
★**About Trend Micro Cloud One: where we were**

About Amazon Cognito and multi-tenant SaaS solutions

Trend Micro Cloud One’s journey to Amazon Cognito

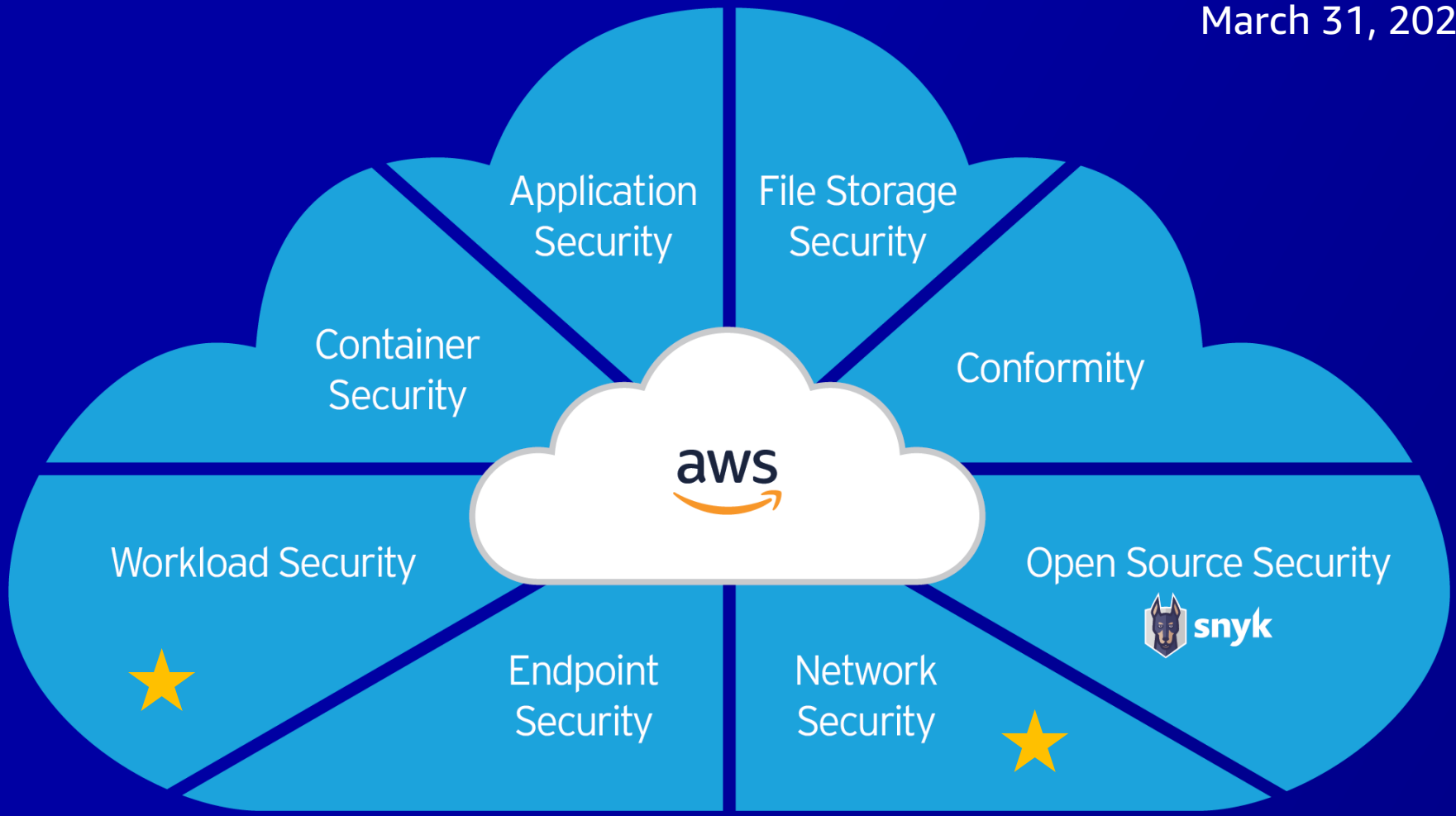
Key takeaways and additional resources

About Trend Micro Cloud One



About Trend Micro Cloud One

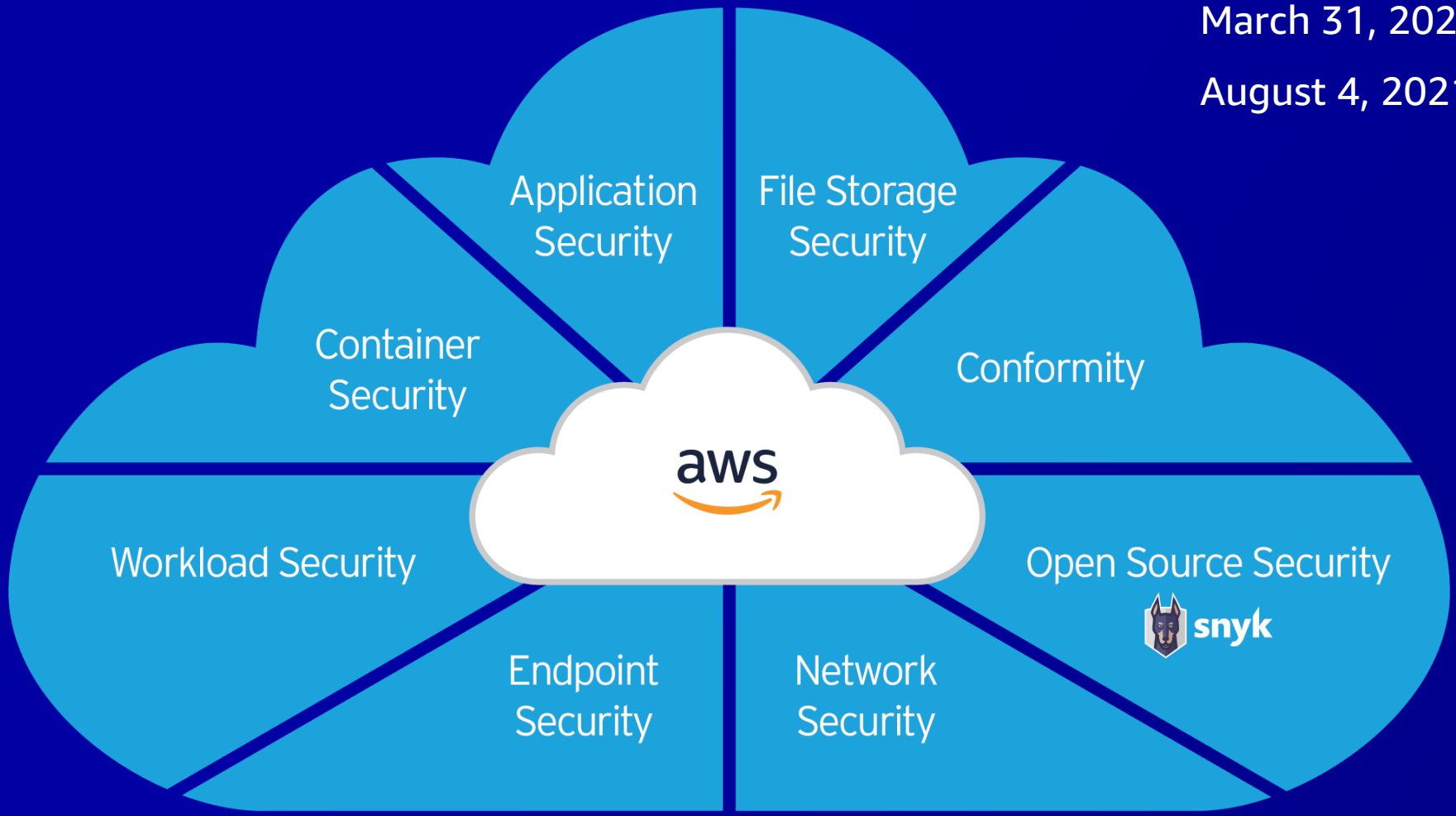
March 31, 2020: Launched with old identity



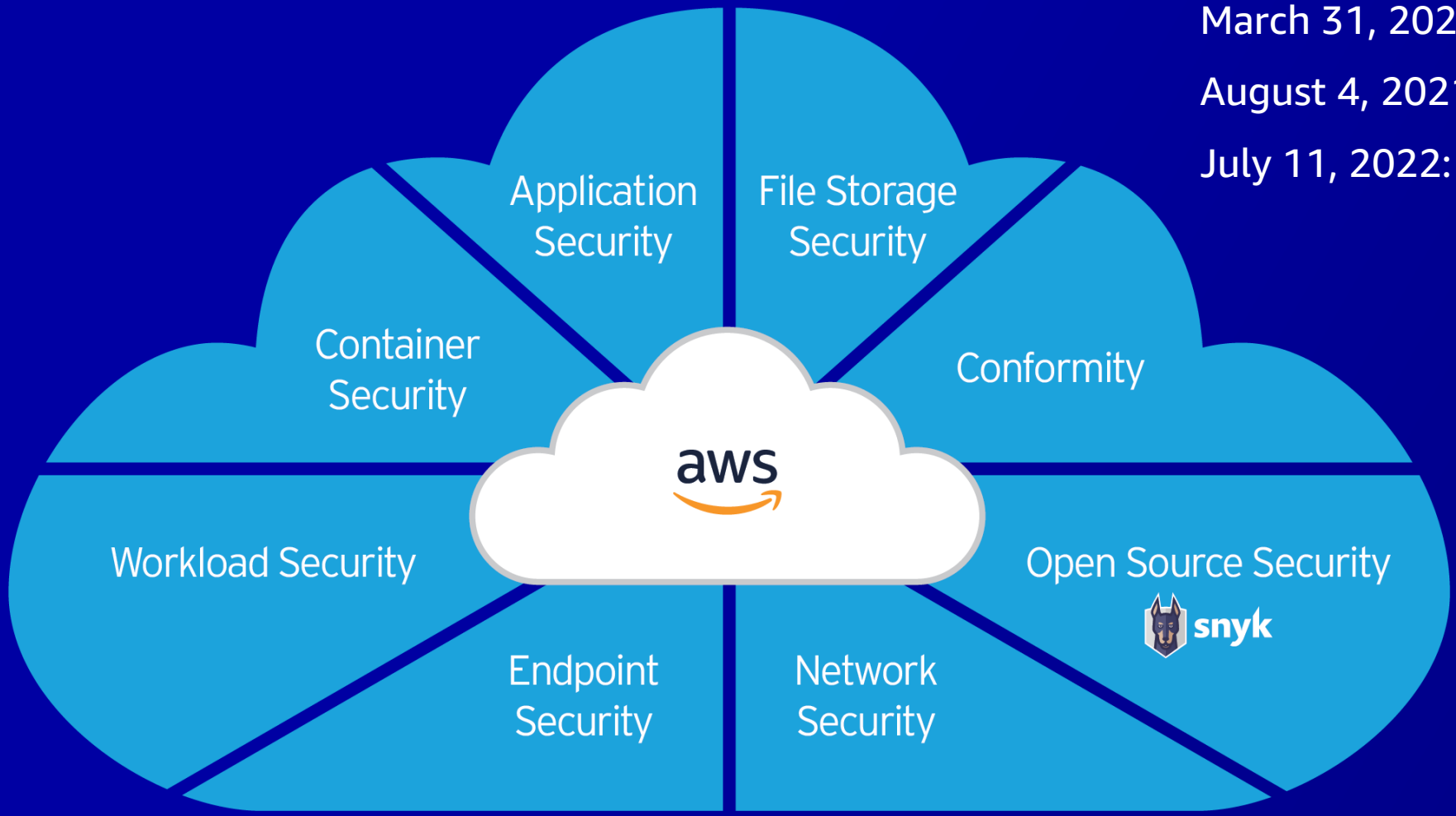
About Trend Micro Cloud One

March 31, 2020: Launched with old identity

August 4, 2021: Integrated Amazon Cognito



About Trend Micro Cloud One



March 31, 2020: Launched with old identity

August 4, 2021: Integrated Amazon Cognito

July 11, 2022: Decommissioned old identity

An opportunity to improve

Where we were

- Homegrown identity system

Where we wanted to be

- Partner with an identity provider

An opportunity to improve

Where we were

- Homegrown identity system
- Awkward to switch between tenant accounts
- Separate credentials in each tenant

Where we wanted to be

- Partner with an identity provider
- Easy account switching
- Consolidated user credentials

An opportunity to improve

Where we were

- Homegrown identity system
- Awkward to switch between tenant accounts
- Separate credentials in each tenant
- Few verified user identities; limited ability for outreach

Where we wanted to be

- Partner with an identity provider
- Easy account switching
- Consolidated user credentials
- Verified contact details for all users

An opportunity to improve

Where we were

- Homegrown identity system
- Awkward to switch between tenant accounts
- Separate credentials in each tenant
- Few verified user identities; limited ability for outreach
- Customizable per-tenant user policies

Where we wanted to be

- Partner with an identity provider
- Easy account switching
- Consolidated user credentials
- Verified contact details for all users
- Simplified self-serve user management

Agenda

Introductions

About Trend Micro Cloud One: where we were

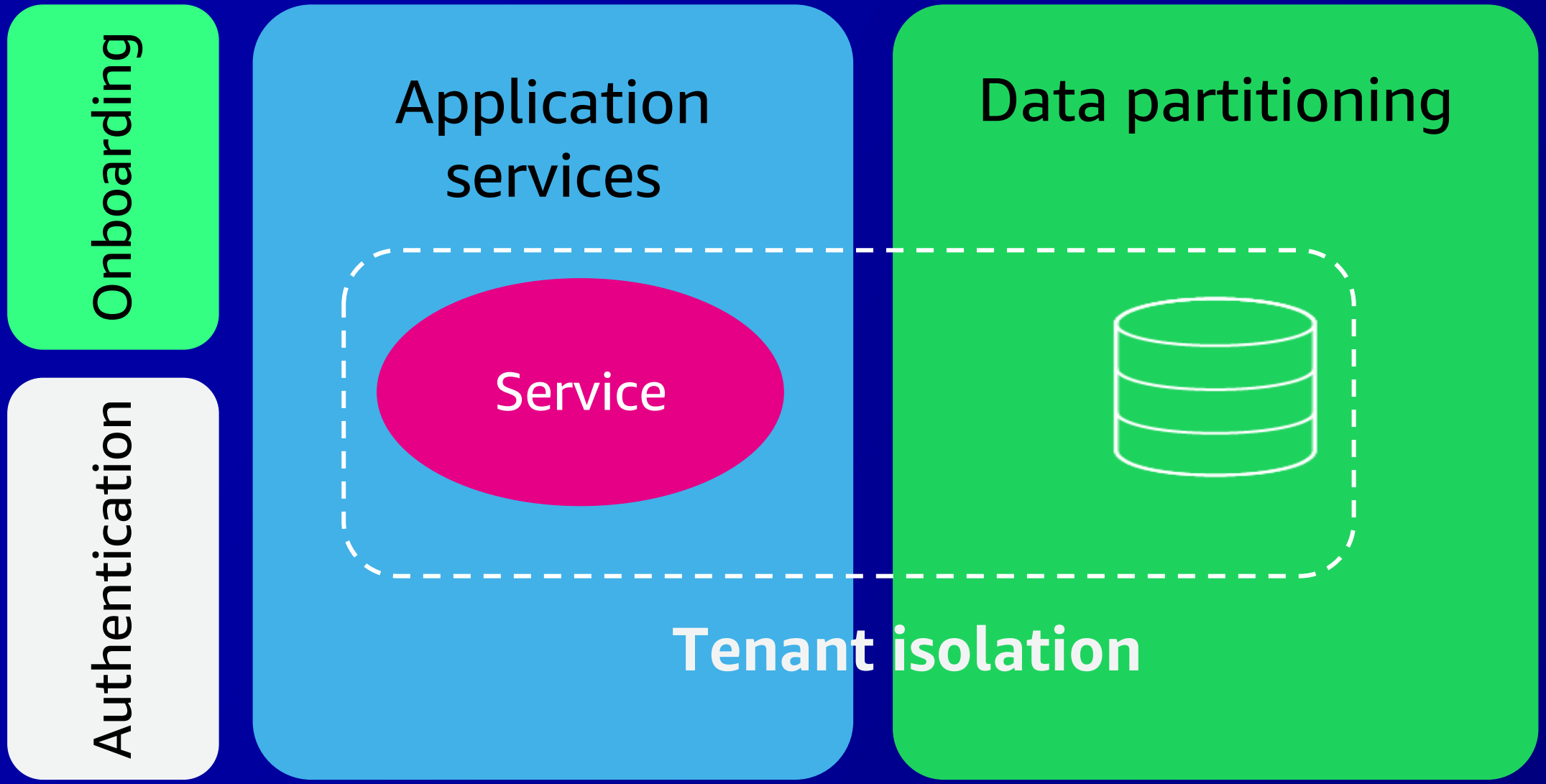
★**About Amazon Cognito and multi-tenant SaaS solutions**

Trend Micro Cloud One’s journey to Amazon Cognito

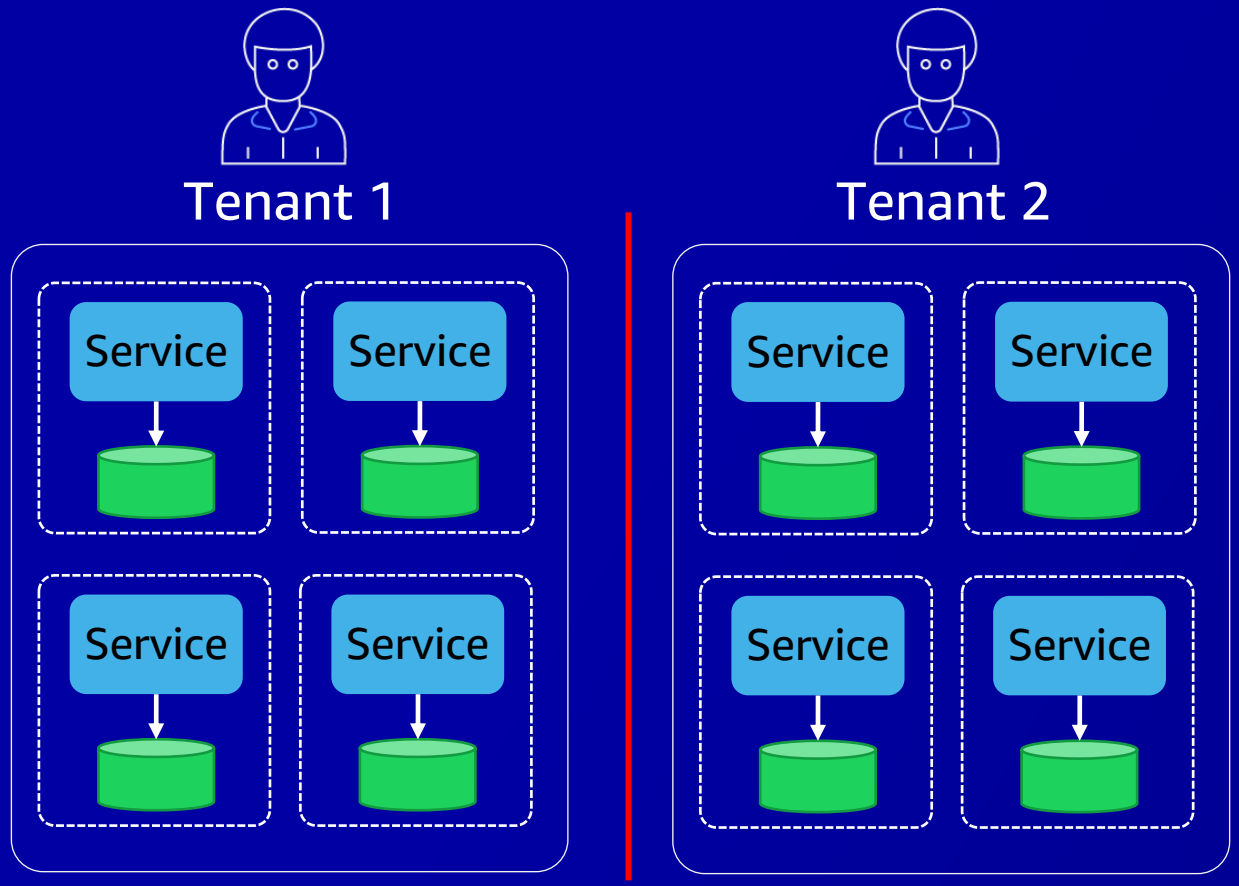
Key takeaways and additional resources

About Amazon Cognito and multi-tenant SaaS solutions

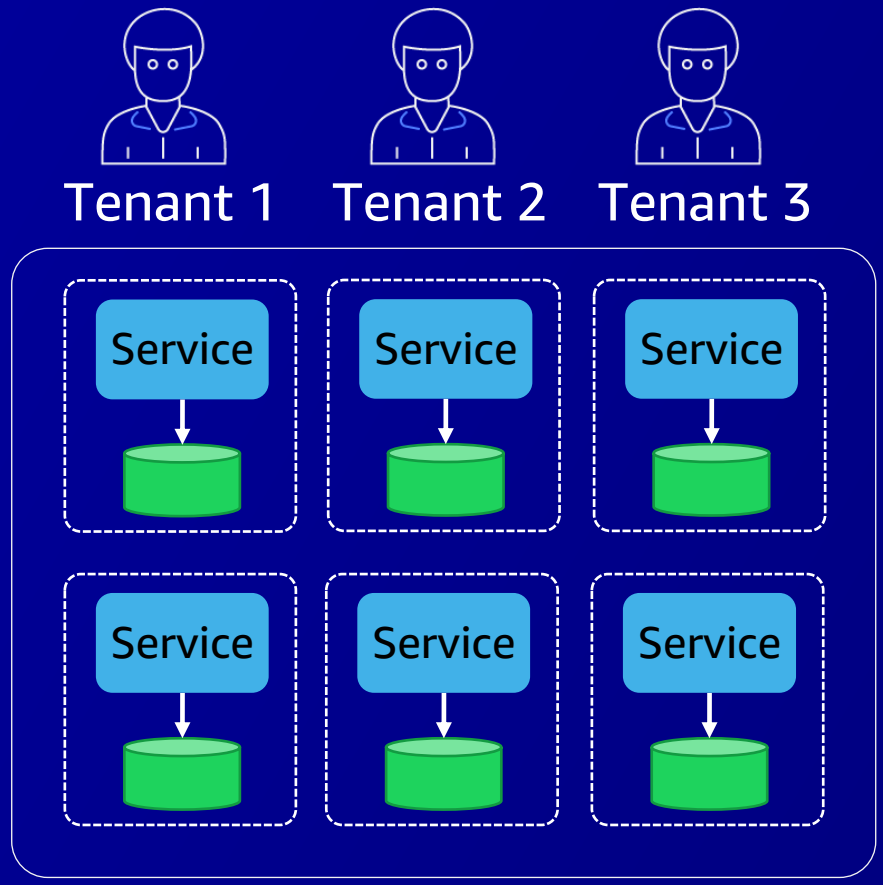
SaaS basics



Multiple flavors of isolation



Isolation through siloed infrastructure
(silo model)



Isolation through runtime policies
(pool model)

Weighing your isolation options

Silo isolation

Pros

- Coarse-grained isolation
- Customer acceptance
- Better tool alignment

Cons

- Deployment
- Cost optimization
- Manageability
- Account limits

Policy-based isolation

Pros

- Fine-grained isolation
- Enables resource pooling
- Flexibility

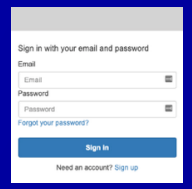
Cons

- Customer acceptance
- Relies on convention
- Mix of technologies
- Account limits

Amazon Cognito: Introduction

User pools
Directory for your identities

- User directory for web/mobile app
- Issue tokens
- OAuth2
- Client credentials



Hosted UI

Issues

JSON
Web tokens (JWTs)

Federation

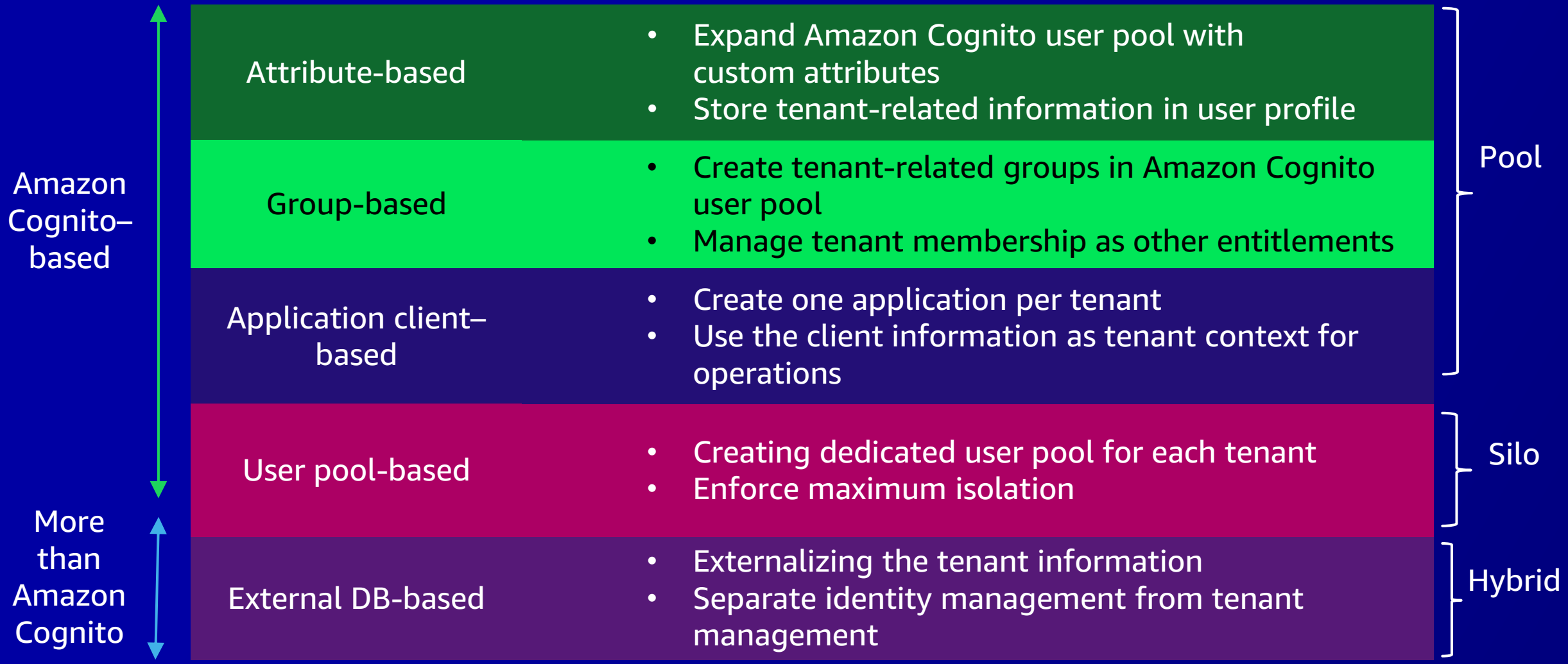
Identity pools
Access control for AWS resources

- Federated identities
- Credentials broker
- Guest access
- Authenticated access
- Fine-grained access

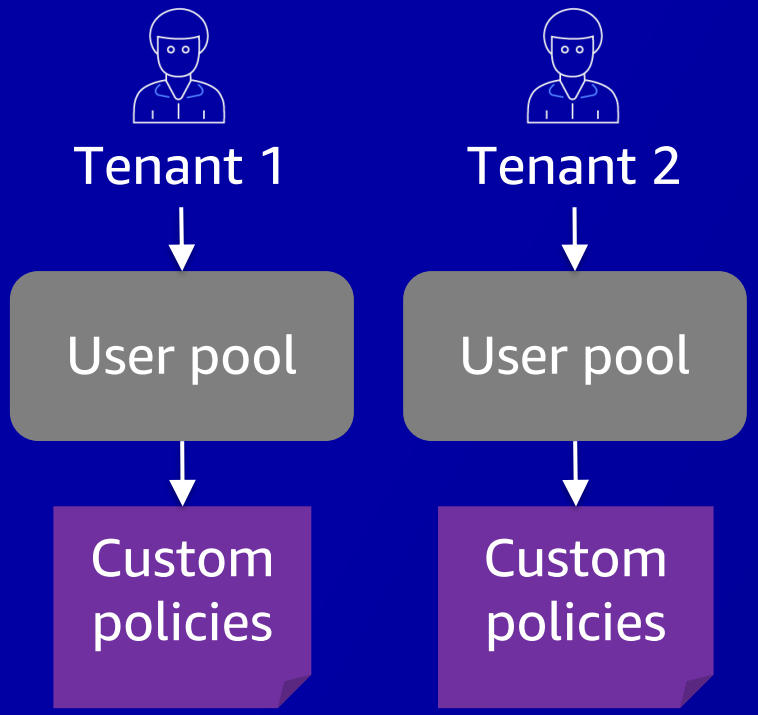
Provides

AWS temporary credentials

Approaches to multi-tenancy in Amazon Cognito



Tenant isolation with Amazon Cognito

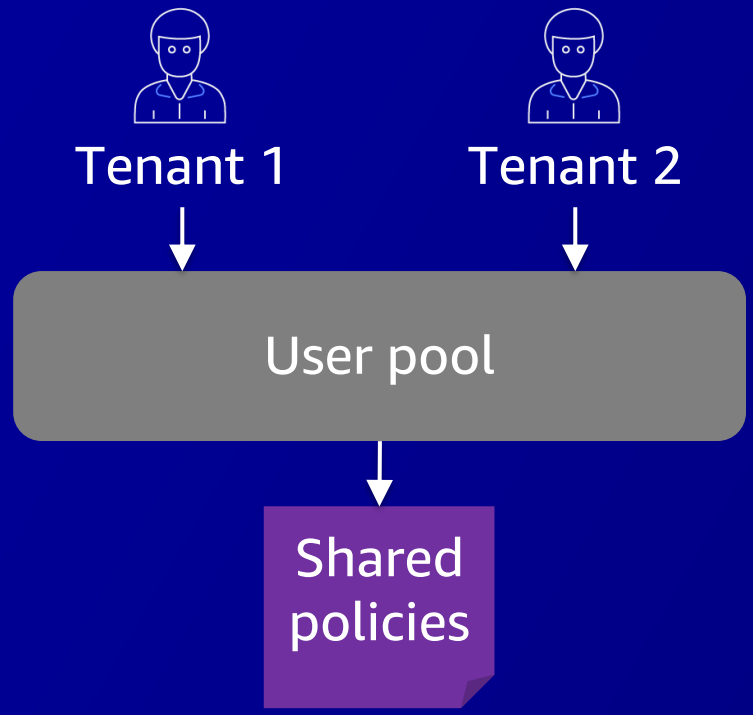


Pros

- Separate policies
- Better isolation

Cons

- Mapping required
- Scale
- Atypical OAuth flow



Pros

- No mapping
- Better OAuth flow
- Scale (maybe)

Cons

- No custom policies
- Isolation story

Agenda

Introductions

About Trend Micro Cloud One: where we were

About Amazon Cognito and multi-tenant SaaS solutions

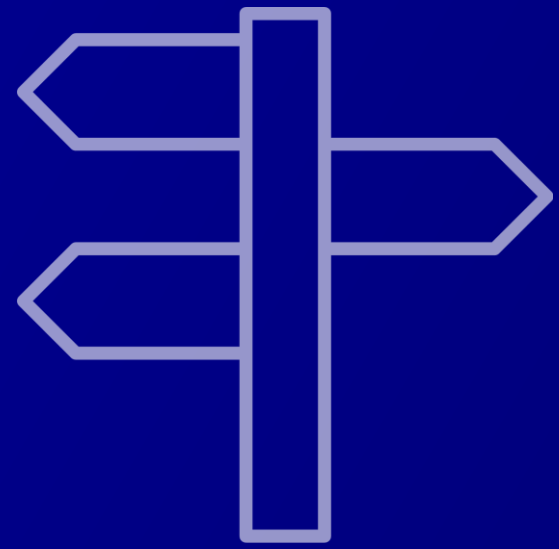
★**Trend Micro Cloud One’s journey to Amazon Cognito**

Key takeaways and additional resources

Trend Micro Cloud One’s journey to Amazon Cognito

Decision points before setting out

1. Which identity provider should we use?
2. What multi-tenancy approach should we use?
3. Whose token should we use?

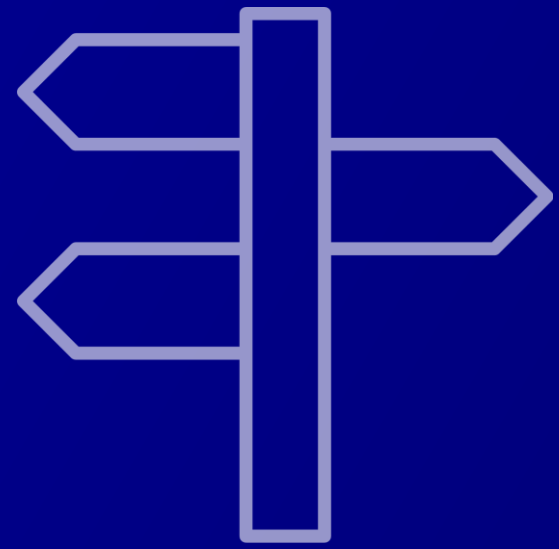


Which identity provider should we use?

Which identity provider should we use?

CRITERIA

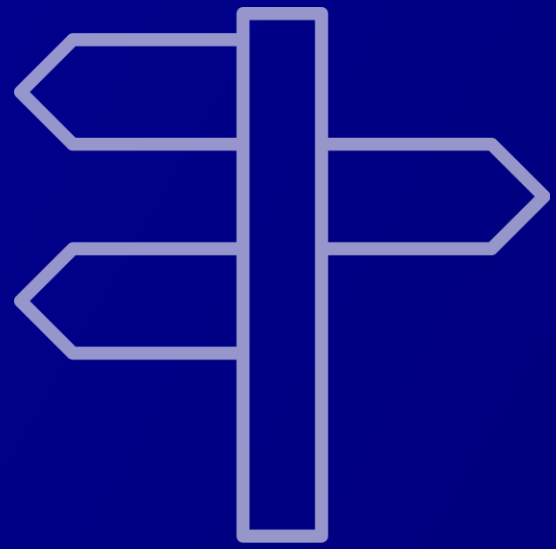
1. Not homegrown



Which identity provider should we use?

CRITERIA

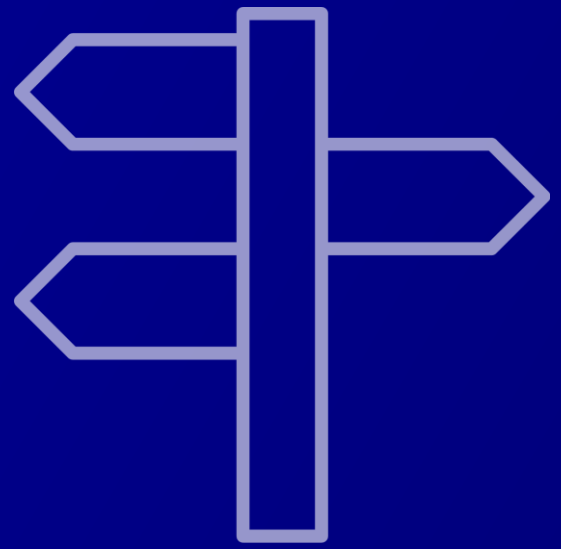
1. Not homegrown
2. Meets our security and compliance needs
    - Data sovereignty/residence, automatic user migration (including MFA), user limits, identity provider limits, user lockout/re-enable, max session duration, token encryption, cookies for browser sessions, password history, customizable sign-up challenges (CAPTCHA), customizable workflow UIs, login on page, sample code, pricing model, estimated cost



Which identity provider should we use?

CRITERIA

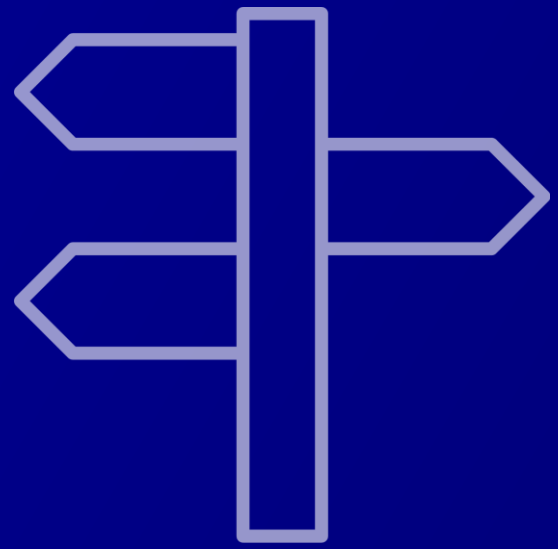
1. Not homegrown
2. Meets our security and compliance needs
   - Data sovereignty/residence, automatic user migration (including MFA), user limits, identity provider limits, user lockout/re-enable, max session duration, token encryption, cookies for browser sessions, password history, customizable sign-up challenges (CAPTCHA), customizable workflow UIs, login on page, sample code, pricing model, estimated cost
3. Fits with how we work on AWS
   - Lead time, infrastructure as code, SLA, high availability, disaster recovery, backup/restore, support, compliance artifacts



Which identity provider should we use?

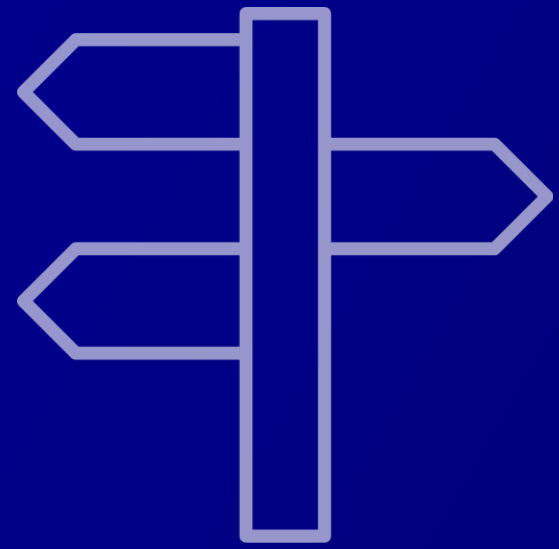
CRITERIA

1. Not homegrown
2. Meets our security and compliance needs
   - Data sovereignty/residence, automatic user migration (including MFA), user limits, identity provider limits, user lockout/re-enable, max session duration, token encryption, cookies for browser sessions, password history, customizable sign-up challenges (CAPTCHA), customizable workflow UIs, login on page, sample code, pricing model, estimated cost
3. Fits with how we work on AWS
   - Lead time, infrastructure as code, SLA, high availability, disaster recovery, backup/restore, support, compliance artifacts



Spoiler alert: we chose Amazon Cognito

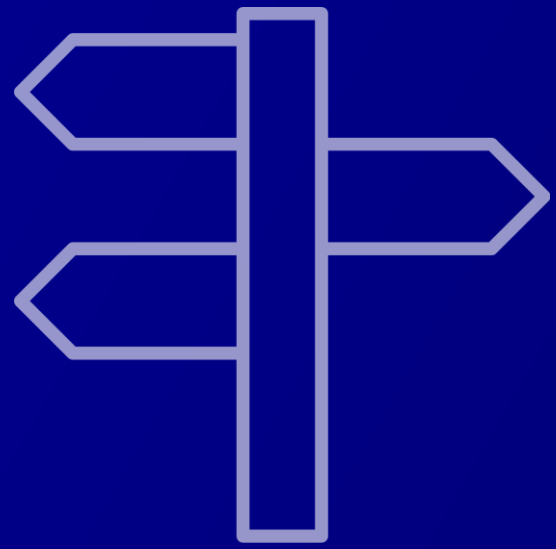
What multi-tenancy approach should we use?



What multi-tenancy approach should we use?

CRITERIA

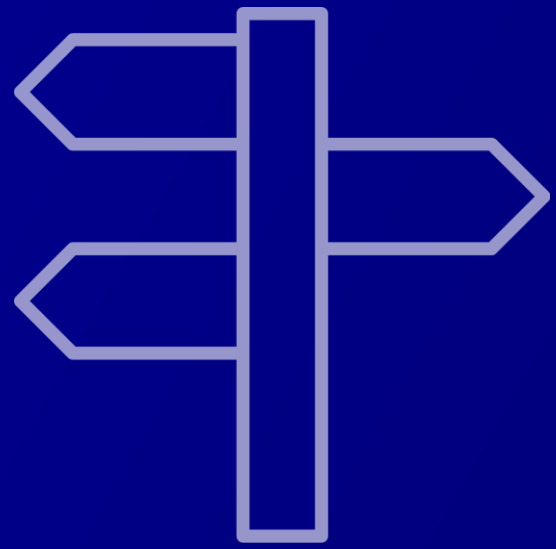
1. 100% self-serve



What multi-tenancy approach should we use?

CRITERIA

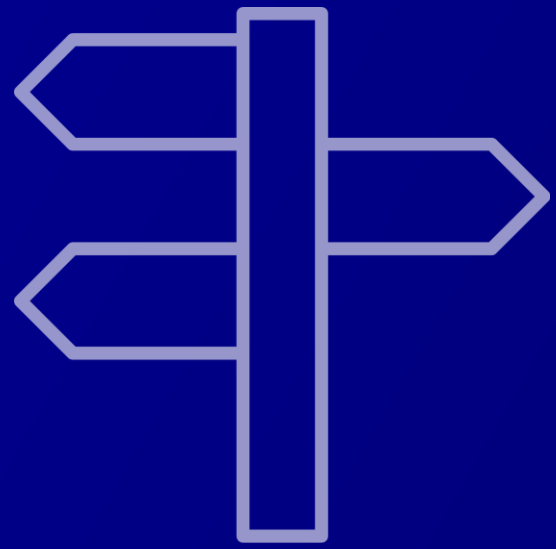
1. 100% self-serve
2. Allow users to sign in once and switch between accounts



What multi-tenancy approach should we use?

CRITERIA

1. 100% self-serve
2. Allow users to sign in once and switch between accounts
3. Support tens of thousands of customers,
   thousands of accounts for each customer,
   hundreds of users per account

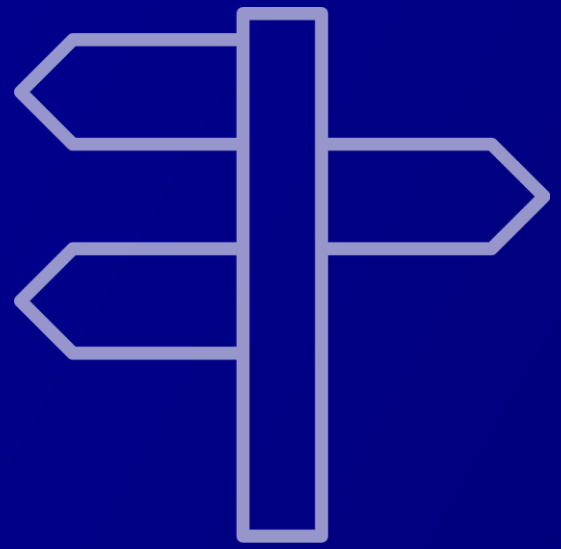


What multi-tenancy approach should we use?

CRITERIA

1. 100% self-serve
2. Allow users to sign in once and switch between accounts
3. Support tens of thousands of customers,
   thousands of accounts for each customer,
   hundreds of users per account

Our choice: authenticate into a single user pool
(and single group), manage multi-tenancy in service

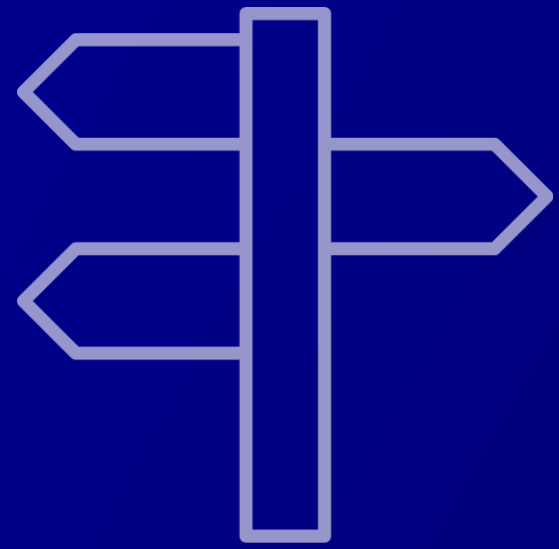


This is not our data model

EXAMPLE DATA MODEL

Primary key		Attributes	
Partition key: pk	Sort key: sk		
glb@example.com	012345678901	role	name
		full-access	Geoff
	023456789012	role	name
		read-only	Geoff
suresh@example.com	03456789013	role	name
		full-access	Suresh

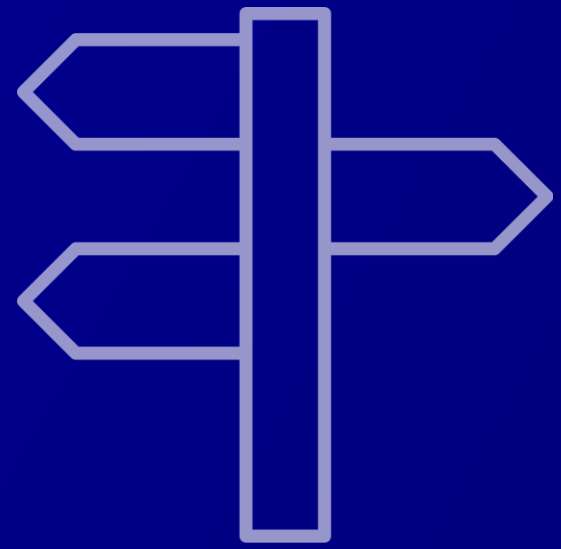
Which token should we use?



Which token should we use?

CRITERIA

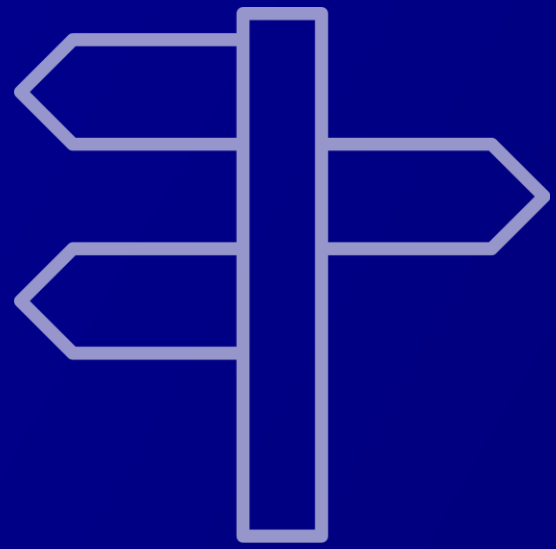
1. Support gradual migration from our preexisting identity system



Which token should we use?

CRITERIA

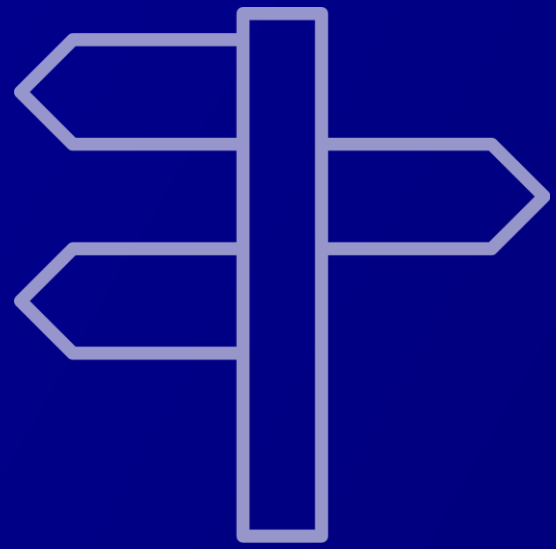
1. Support gradual migration from our preexisting identity system
2. Incorporate chosen account and selected role



Which token should we use?

CRITERIA

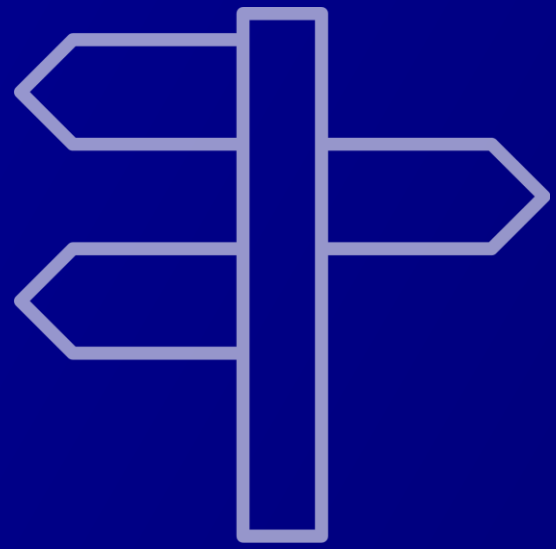
1. Support gradual migration from our preexisting identity system
2. Incorporate chosen account and selected role
3. Limit the scope of exposure for personally identifiable information



Which token should we use?

CRITERIA

1. Support gradual migration from our preexisting identity system
2. Incorporate chosen account and selected role
3. Limit the scope of exposure for personally identifiable information

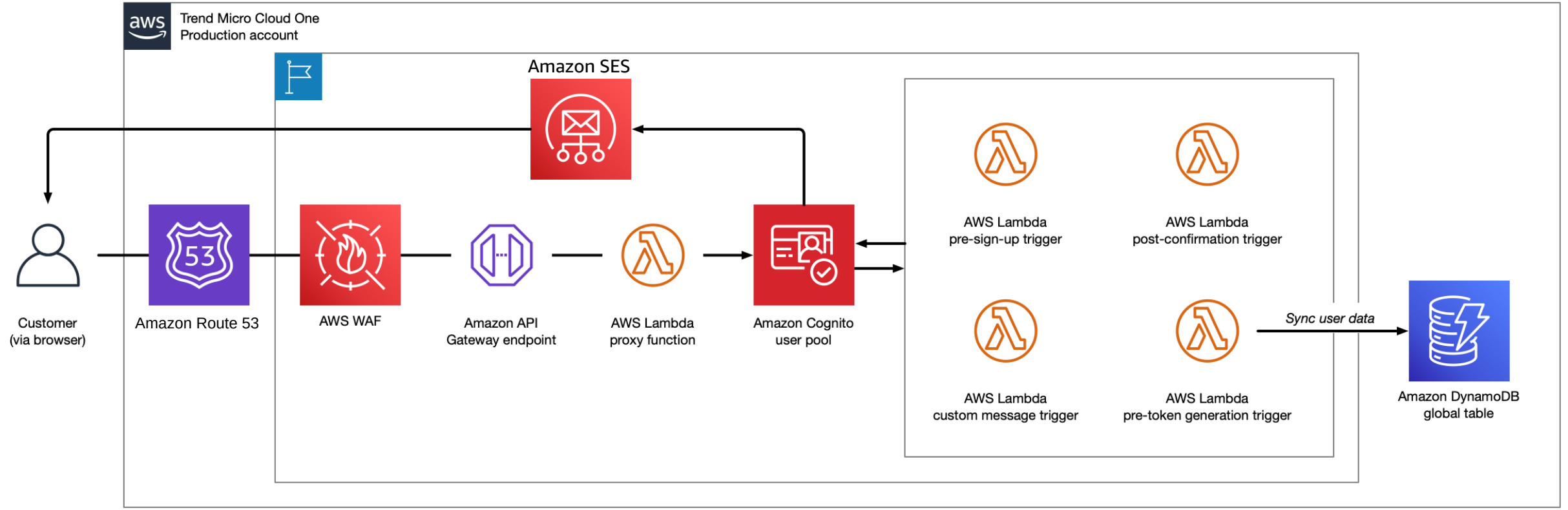


Our choice: issue our own token with selected details

Architecture

Trend Micro Cloud One and Amazon Cognito

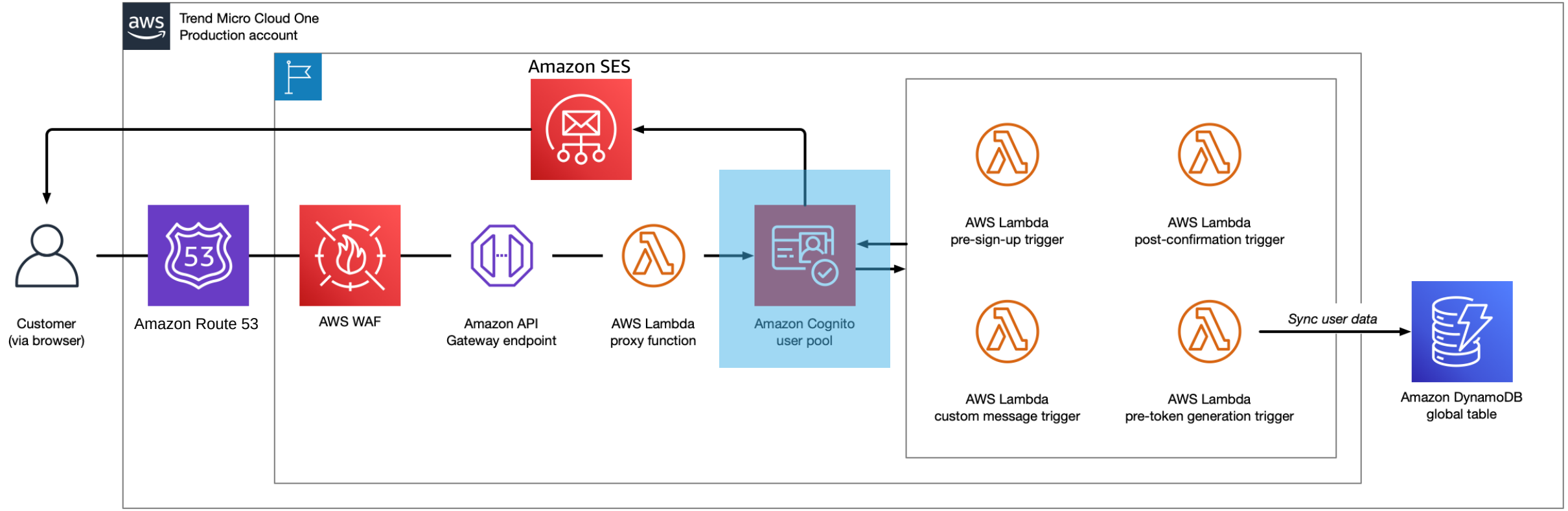
STEP 1: SIGN UP AND SIGN IN



Proxy blog post:
go.aws/39Aq5DS

Trend Micro Cloud One and Amazon Cognito

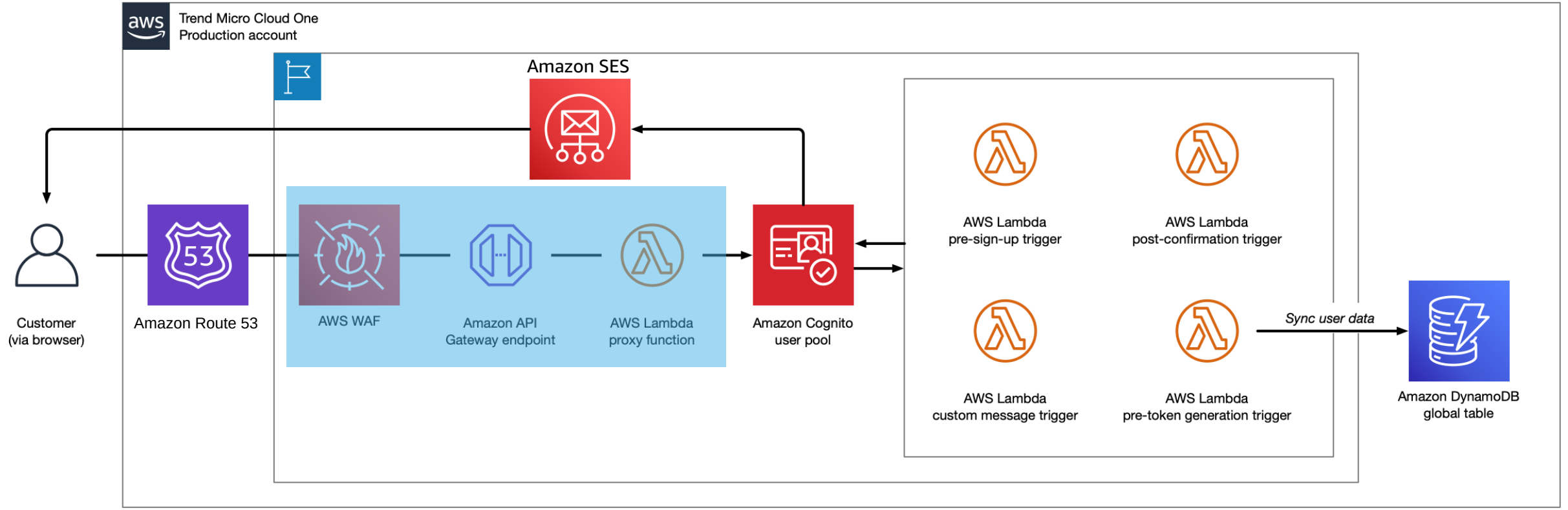
STEP 1: SIGN UP AND SIGN IN



Proxy blog post:
go.aws/39Aq5DS

Trend Micro Cloud One and Amazon Cognito

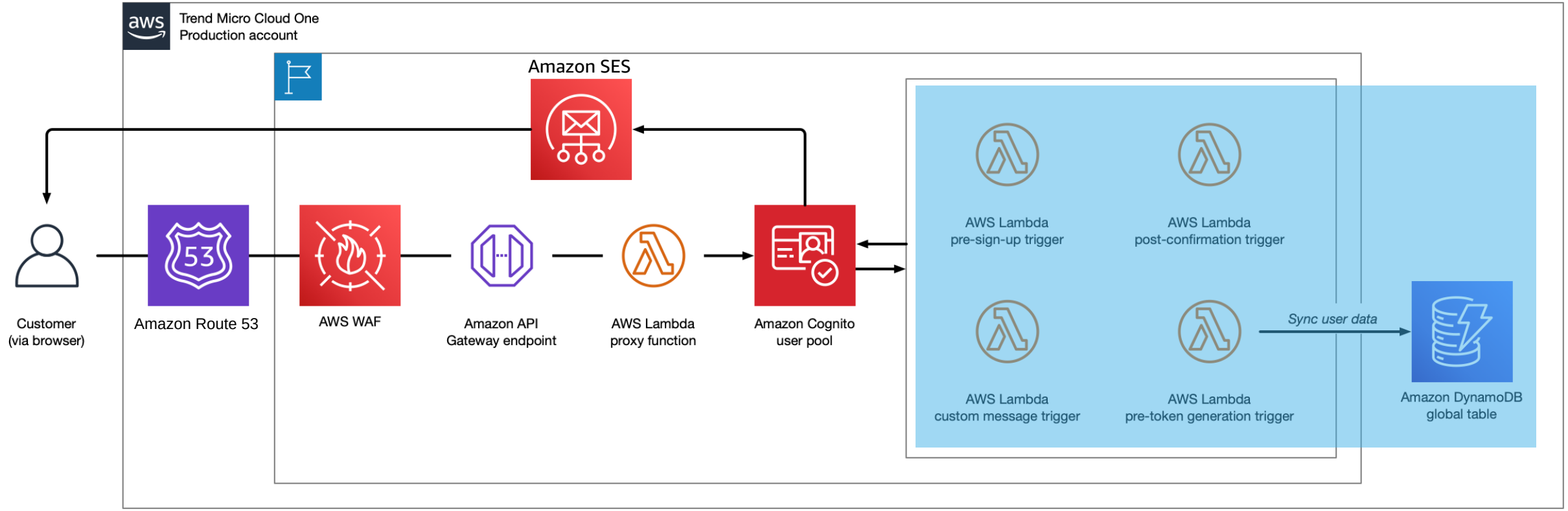
STEP 1: SIGN UP AND SIGN IN



Proxy blog post:
go.aws/39Aq5DS

Trend Micro Cloud One and Amazon Cognito

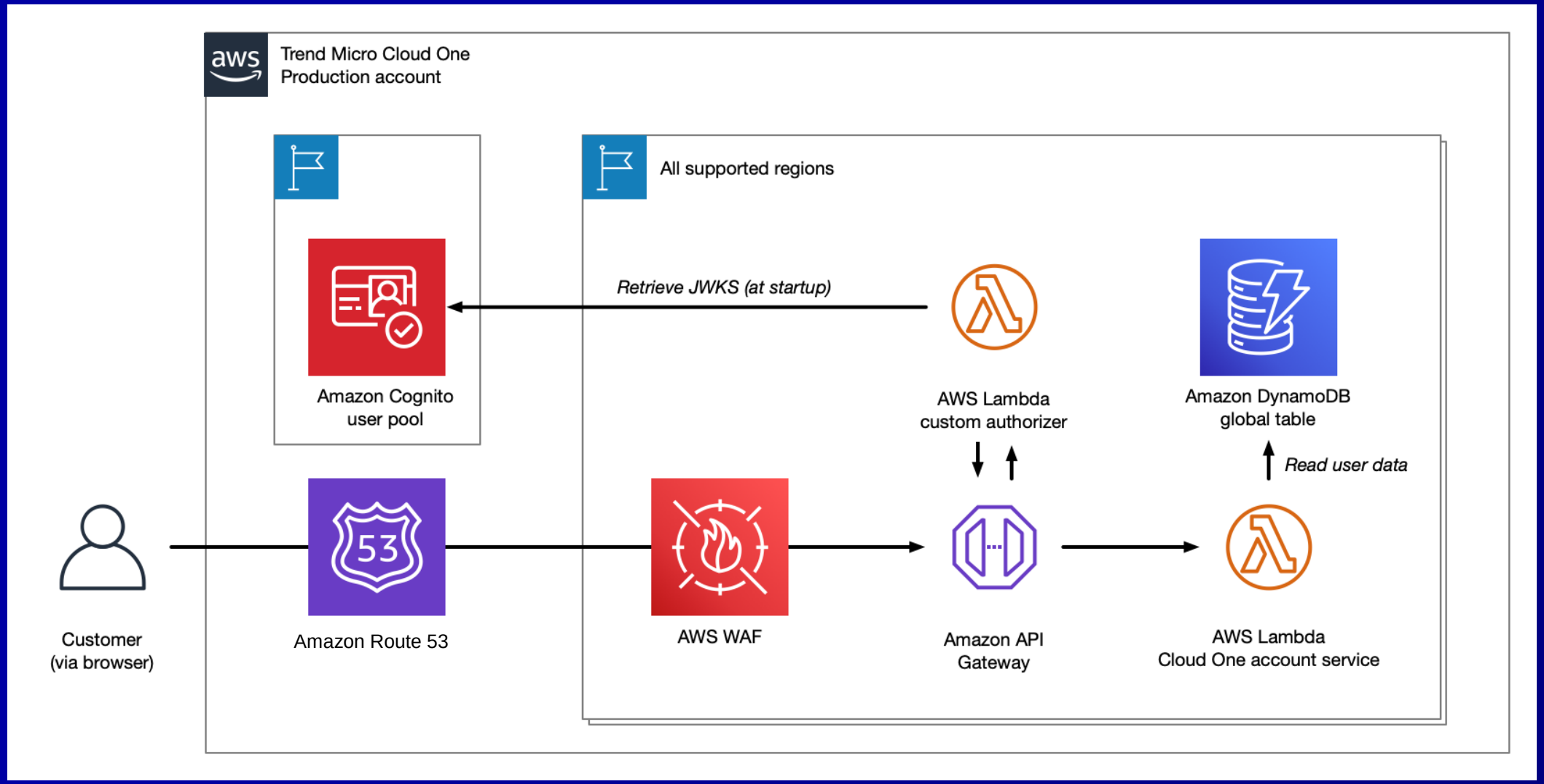
STEP 1: SIGN UP AND SIGN IN



Proxy blog post:
go.aws/39Aq5DS

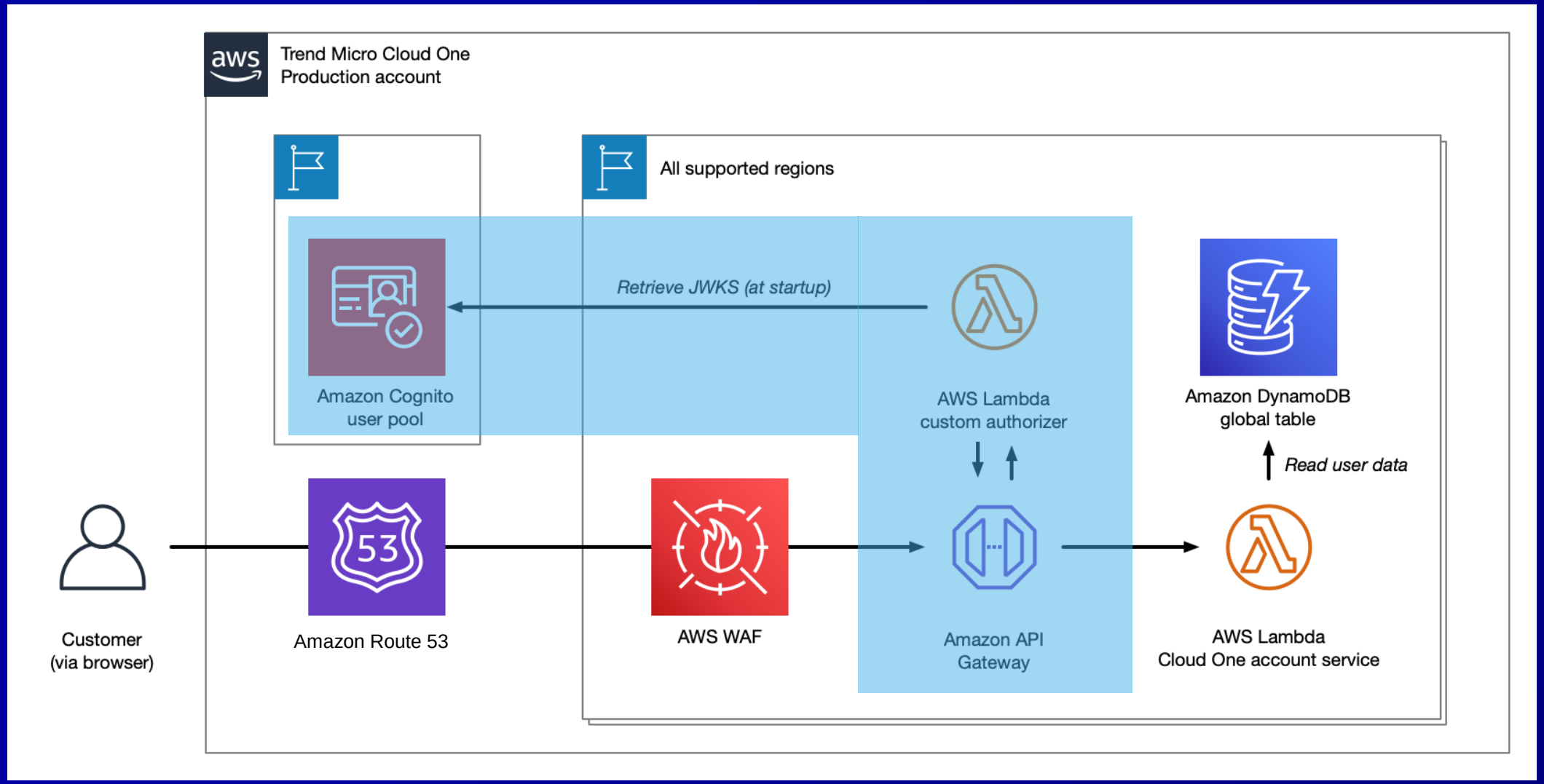
Trend Micro Cloud One and Amazon Cognito

STEP 2: ACCOUNT SELECTION AND ACCESS TOKEN GENERATION



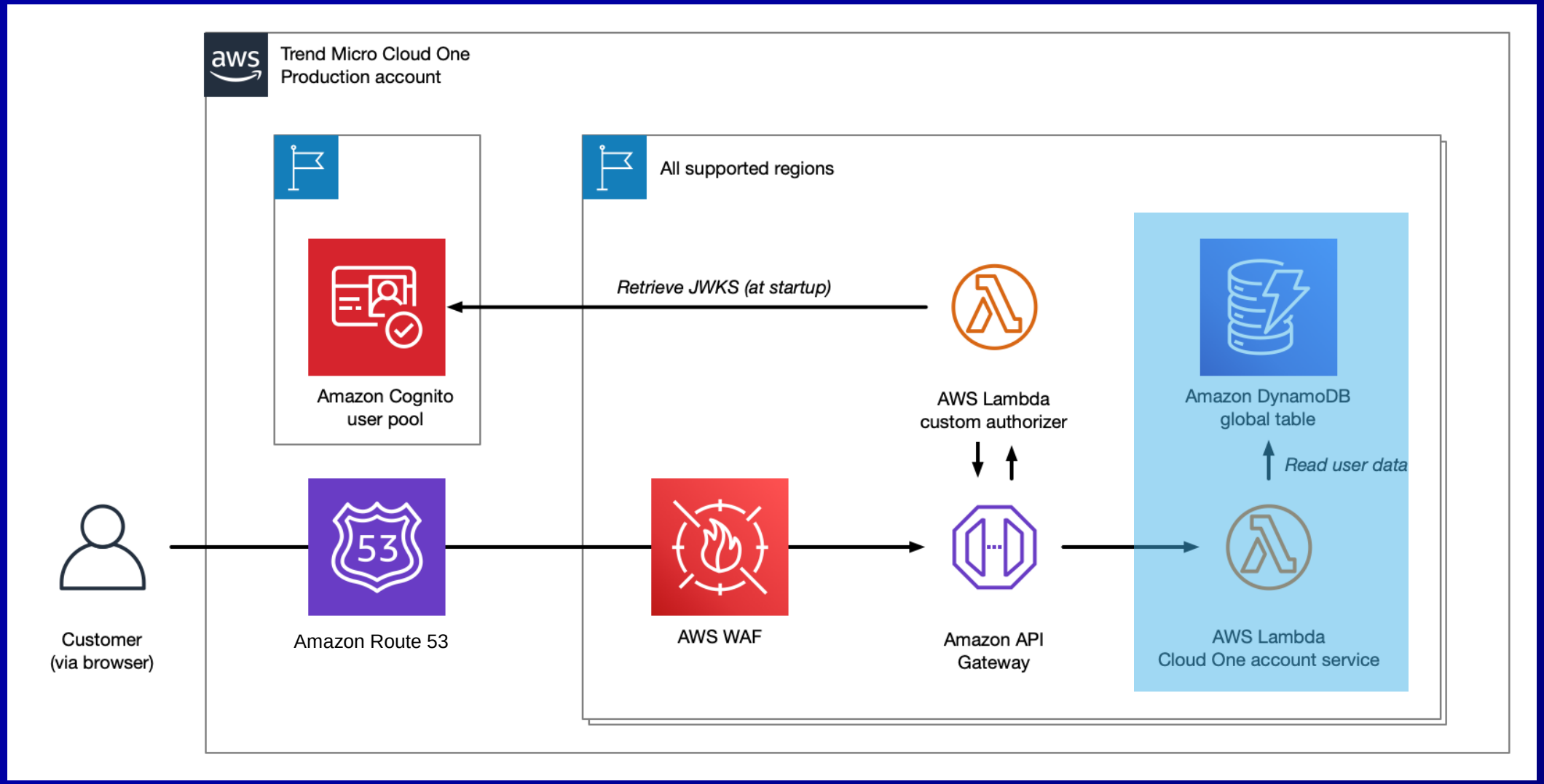
Trend Micro Cloud One and Amazon Cognito

STEP 2: ACCOUNT SELECTION AND ACCESS TOKEN GENERATION



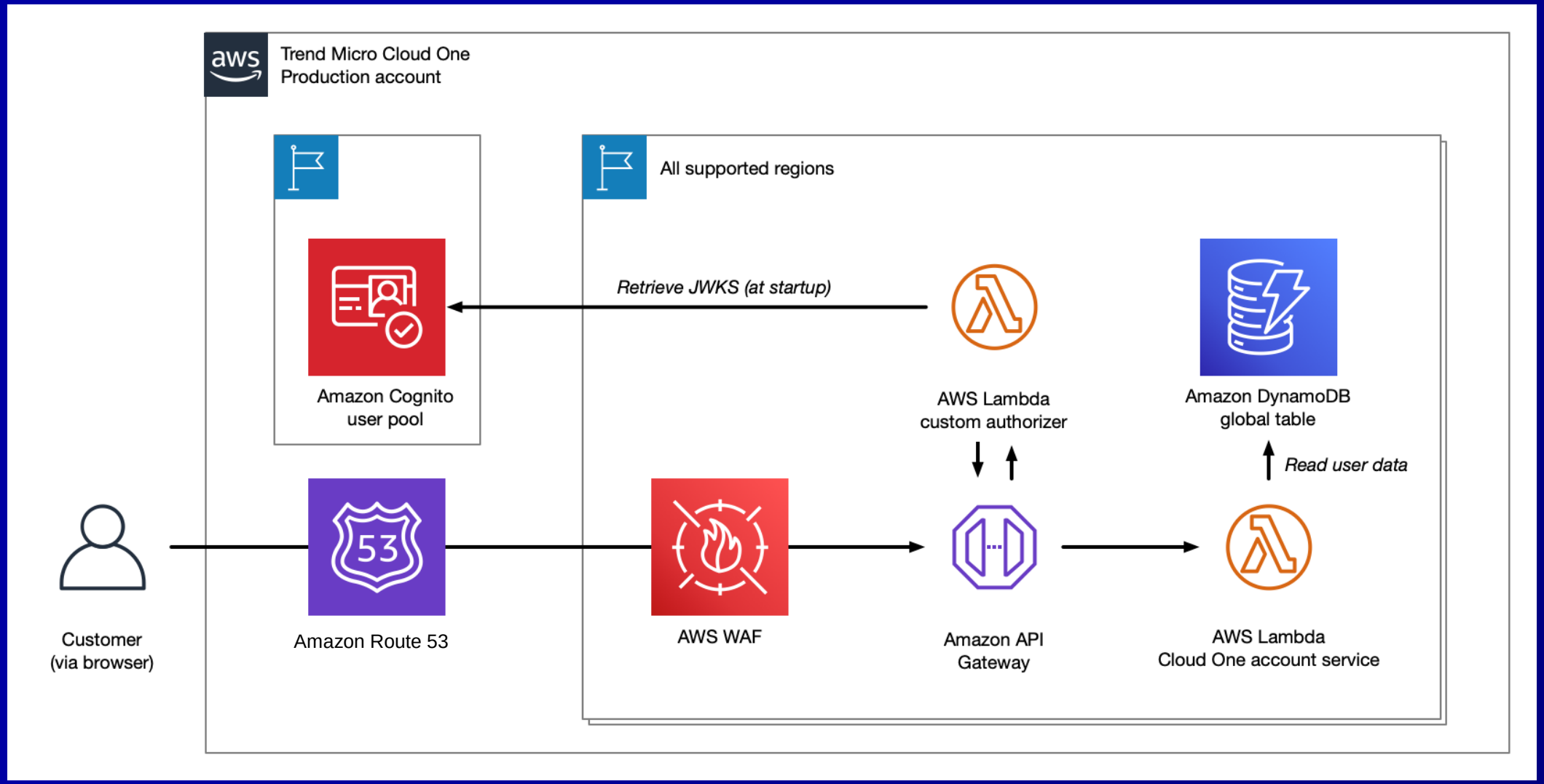
Trend Micro Cloud One and Amazon Cognito

STEP 2: ACCOUNT SELECTION AND ACCESS TOKEN GENERATION



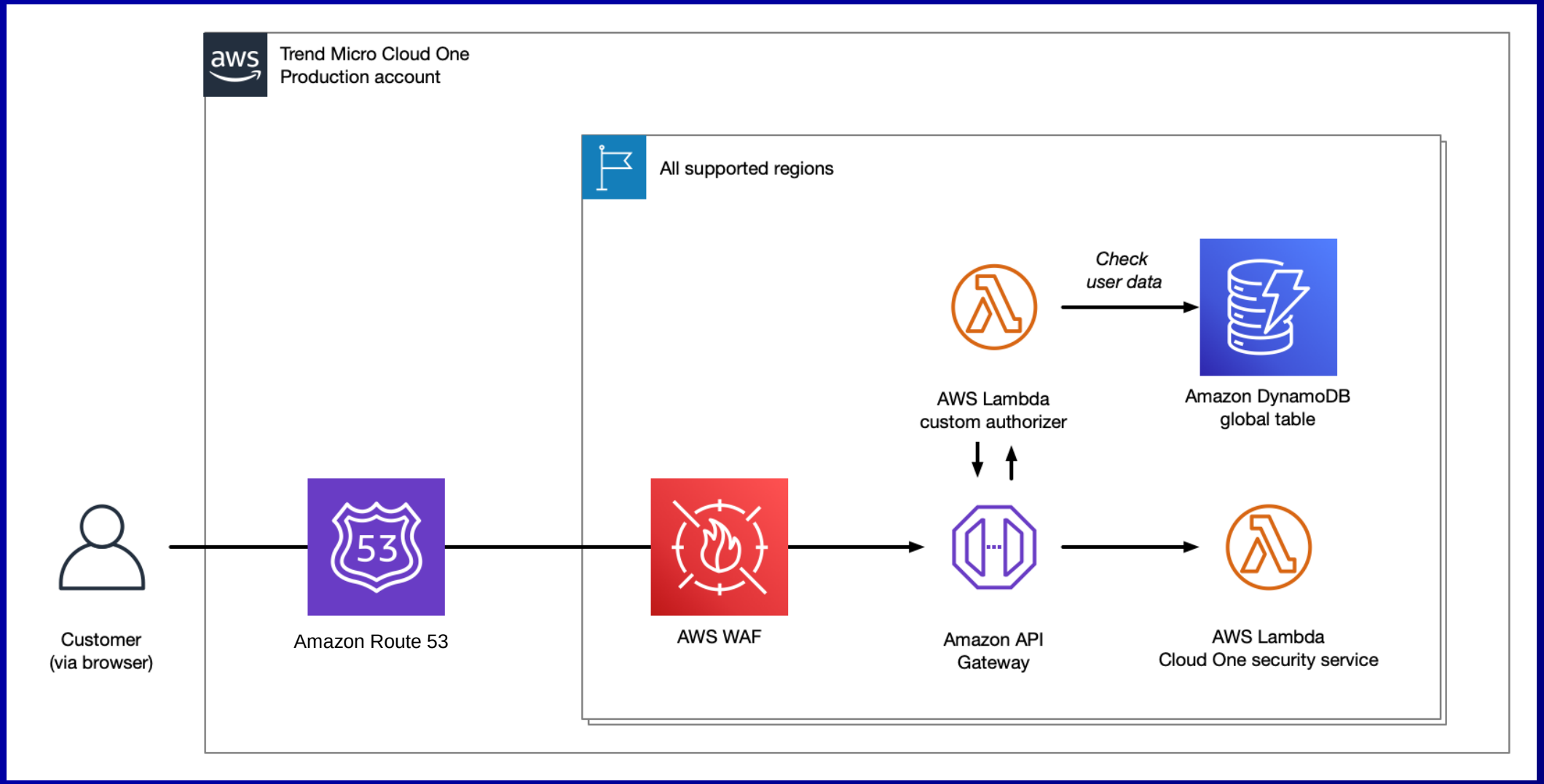
Trend Micro Cloud One and Amazon Cognito

STEP 2: ACCOUNT SELECTION AND ACCESS TOKEN GENERATION



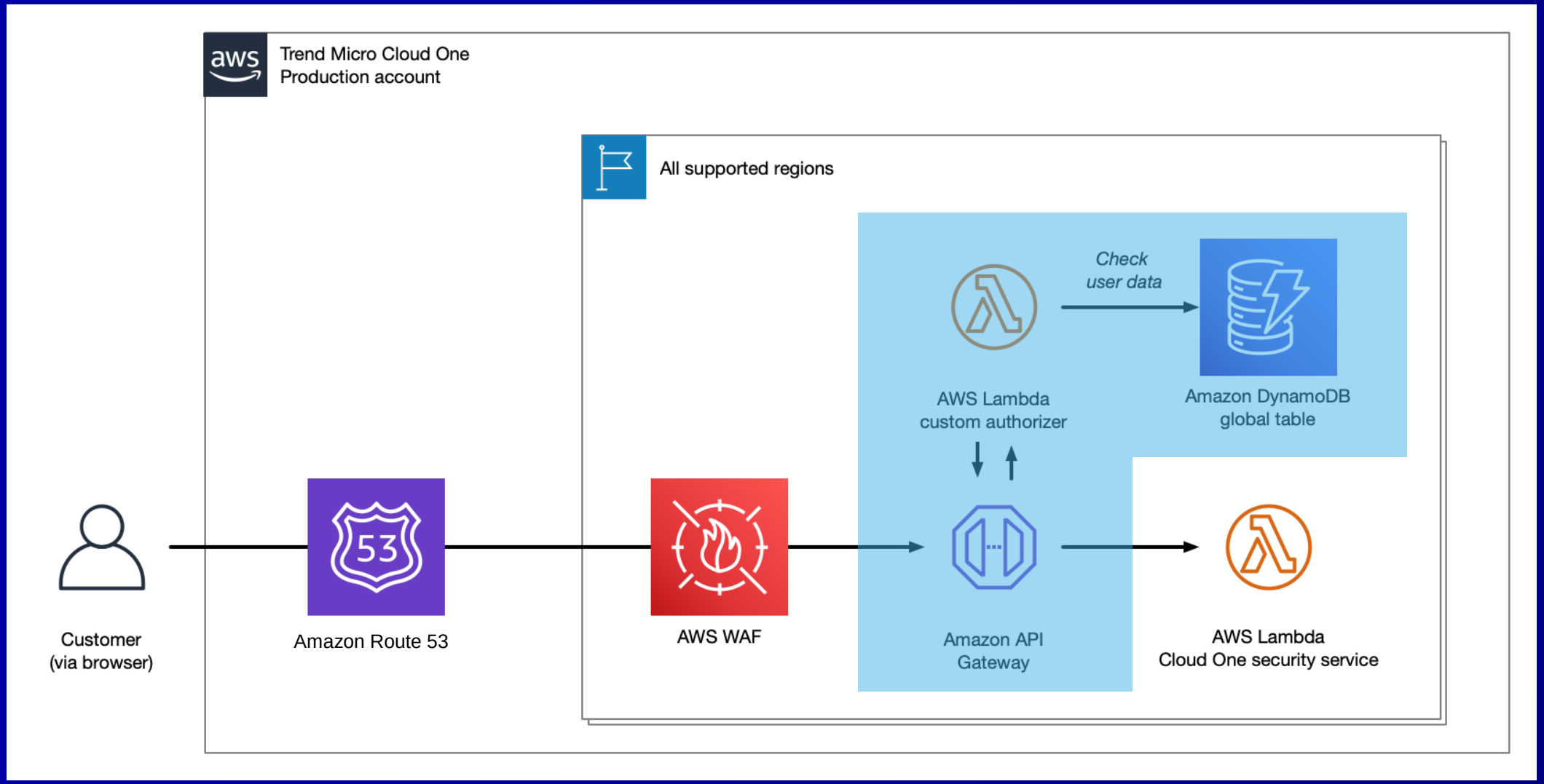
Trend Micro Cloud One and Amazon Cognito

STEP 3: SERVICE INTERACTIONS



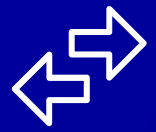
Trend Micro Cloud One and Amazon Cognito

STEP 3: SERVICE INTERACTIONS



Architecture summary

Authenticate with Amazon Cognito



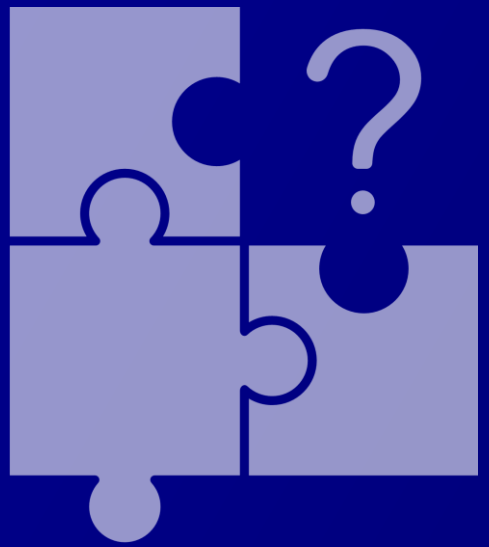
Exchange Amazon Cognito token for Cloud One token

Perform authorized operations

Challenges

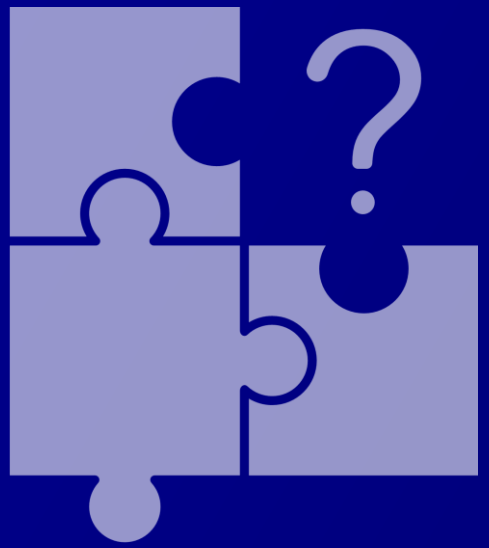
Some of the challenges we encountered

1. Single user pool = single password policy



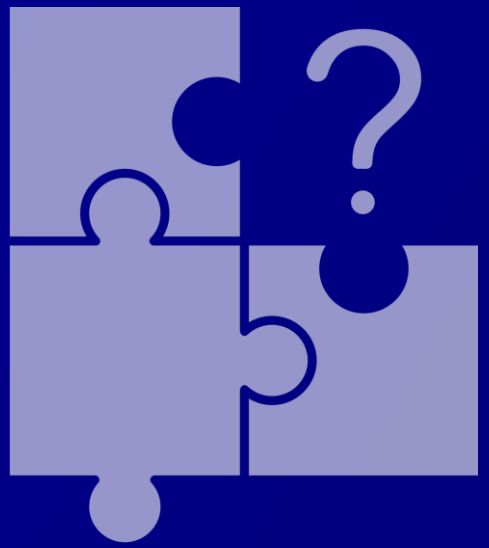
Some of the challenges we encountered

1. Single user pool = single password policy
2. User-visible change = customer pain



Some of the challenges we encountered

1. Single user pool = single password policy
2. User-visible change = customer pain
3. Identity federation and multi-tenancy = complexity



Agenda

Introductions

About Trend Micro Cloud One: where we were

About Amazon Cognito and multi-tenant SaaS solutions

Trend Micro Cloud One’s journey to Amazon Cognito

★**Key takeaways and additional resources**

Key takeaways

Things to consider

- Are you building entirely new or starting from an existing system?
- Can a single user be in multiple tenants?
- What tenant onboarding model do you want – full self-serve or supported?
- Will tenants need control over password policies?
- How does federated identity/SSO/SAML fit into your multi-tenancy model?

Things to consider

- Are you building entirely new or starting from an existing system?
- Can a single user be in multiple tenants?
- What tenant onboarding model do you want – full self-serve or supported?
- Will tenants need control over password policies?
- How does federated identity/SSO/SAML fit into your multi-tenancy model?

- Talk to the Amazon Cognito solution architecture team!

Additional resources

Multi-tenant application best practices
Learn more about different multi-tenancy approaches using Amazon Cognito

https://go.aws/3B6jhsT

Enriching Amazon Cognito features with an Amazon API Gateway proxy
Learn how to implement a proxy function to extend Amazon Cognito

https://go.aws/3Osnvhx

Trend Micro Cloud One
Secure your cloud infrastructure with clarity and simplicity

https://bit.ly/3PI5koY

Thank you!

Suresh Sridharan
@s_sridharan

Geoff Baskwill
@geoff_baskwill