

The background features a dark blue gradient with abstract, glowing geometric shapes. A large, bright magenta/pink semi-circle is prominent in the lower right, with a smaller, darker blue semi-circle above it. Thin, light blue lines intersect diagonally across the scene.

AWS re:Invent

DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

AIM344 - R

Understanding the deep security controls within Amazon Q Business

Dr. Andrew Kane

(he/him)

WW Tech Lead (Gen AI Security & Compliance)
Amazon Web Services

Gabrielle Dompereh

(she/her)

AI/ML Specialist Solutions Architect
Amazon Web Services



© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

01 What is Amazon Q Business?

02 Data privacy and protection

03 AWS Identity and Access Management (IAM)

Followed by optional sections



Amazon Q Business features

AWS IAM
Identity
Center

Admin flows

Guardrails

Repository
connectors

01 What is Amazon Q Business?

Amazon Q

AMAZON Q BUSINESS



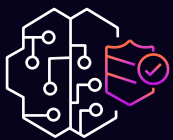
AMAZON Q DEVELOPER

AMAZON Q
IN QUICKSIGHT

AMAZON Q
IN CONNECT

AMAZON Q
IN SUPPLY CHAIN

Safety and security



Use pre-built guardrails for toxicity



Restrict responses to enterprise content only



Specify blocked words or phrases that never appear in responses



Define special topics and configure guardrails for such topics



Use AWS PrivateLink to access Amazon Q Business securely in your VPC environment using a VPC endpoint



Integrates with IAM Identity Center for easier management, auditability, and control



Integrated with AWS CloudTrail to record actions taken by a user, role, or an AWS service

FIPS

Support for Federal Information Processing Standard (FIPS) endpoints

AWS generative AI stack

APPLICATIONS TO BOOST PRODUCTIVITY



Amazon Q Business
INSIGHTS AND AUTOMATION



Amazon Q Developer
SOFTWARE DEVELOPMENT LIFECYCLE

MODELS AND TOOLS TO BUILD GENERATIVE AI APPS

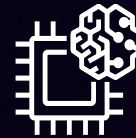


Amazon Bedrock
AMAZON MODELS | PARTNER MODELS

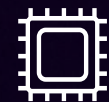
INFRASTRUCTURE TO BUILD AND TRAIN AI MODELS



Amazon SageMaker
MANAGED INFRASTRUCTURE



AWS Trainium
AWS Inferentia



GPUs

HIGH PERFORMANCE COMPUTE

Find accurate and referenceable answers

BOOST YOUR WORKFORCE PRODUCTIVITY WITH GENERATIVE AI



Trusted answers generated from enterprise data



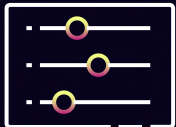
In-context conversations



Source references for fact-checking



Conversation history



Tune the relevance of results with index boosting

data durability, which means the data is redundantly stored across multiple Availability Zones that are physically separated within an AWS Region . [1] [2] The source also states that S3 is resilient to AZ failures and stores data across multiple AZs, resulting in high data durability . [3] Additionally, the Resilience Hub assessment shows that S3 does well in terms of resiliency, with the S3 bucket being resilient to AZ failures . [3]

Sources ▾

👤 Tell me more about availability zones

🔍 Availability Zones are distinct locations within an AWS Region that are engineered to be isolated from failures in other Availability Zones. [1] [2] Each Availability Zone provides inexpensive, low-latency network connectivity to other Availability Zones in the same AWS Region. [1] [2] By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location. [1] [2] AWS maintains multiple Availability Zones in each Region, and these Availability Zones are physically isolated from each other but united by private, low-latency, high-throughput, and highly redundant network connections. [3] [4] This enables AWS to provide very high levels of availability and redundancy, while also minimizing latency. [3] [4]

Sources ▾

👍 🗨️ 📄

🔗 Enter a prompt

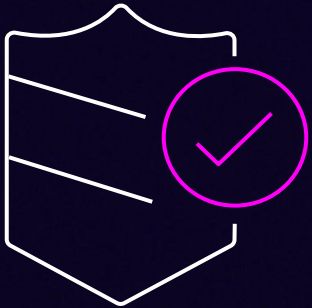
Responding from approved sources

Amazon Q Business uses generative AI. You may need to verify responses for accuracy. [AWS Responsible AI Policy](#)

aws

02 Data privacy and protection

Data privacy and localization



You are always in control of your data

- Amazon Q Business uses **pre-trained LLMs** for inference
- Amazon Q Business **does not use** customer data for **service improvement** or for improving any of the **underlying** LLMs
- All customer model data usage (prompts, responses) are **isolated per customer**
- All data used in the API **remain in the AWS Region** where they were created unless you explicitly use a cross-Region feature

Data security

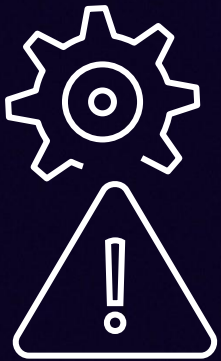


You are always in control of your data

- Customer data is always **encrypted in transit** with a minimum of TLS1.2 and AES-256 **encrypted at rest** using AWS KMS managed data encryption keys
- FIPS endpoints are available in **us-east-1** and **us-west-2** Regions
- Use your symmetric AWS KMS keys to add a **second layer of encryption** over the existing AWS-owned encryption, such as your data and any child resources in an Amazon Q Business application environment **
- Integration with **AWS Identity and Access Management (IAM)** to manage access to Amazon Q Business, manage plugins, access the AWS Console, etc.

*** Enterprise index only*

Governance and auditability support



Comprehensive monitoring and logging capabilities

- Track **usage metrics** and build customized dashboards using Amazon CloudWatch
- **Monitor API activity** and **troubleshoot issues** as you integrate other systems into your applications using AWS CloudTrail, supporting application, data-source and index events
- Compliance standards: GDPR, HIPAA BAA

03 AWS Identity and Access Management (IAM)

Amazon Q Business – IAM

ALLOW A USER TO CONVERSE WITH AMAZON Q BUSINESS

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": [  
      "qbusiness:ChatSync",  
      "qbusiness:ListMessages",  
      "qbusiness:ListConversations",  
      "qbusiness:DescribeExperience",  
      "qbusiness>DeleteConversation"  
    ],  
    "Resource": [  
      "arn:aws:qbusiness:<REGION>::<ACCOUNT>:application/<APPLICATION ID>"  
    ]  
  }  
]
```


Amazon Q Business – IAM

ALLOW A USER TO MANAGE PLUG-INS IN A CHAT APPLICATION

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": [  
      "qbusiness:CreatePlugin",  
      "qbusiness:ListPlugins",  
      "qbusiness:GetPlugin",  
      "qbusiness:UpdatePlugin",  
      "qbusiness>DeletePlugin"  
    ],  
    "Resource": [  
      "arn:aws:qbusiness:<REGION>::<ACCOUNT>:application/<APPLICATION ID>"  
    ]  
  }  
]
```

Amazon Q Business – IAM

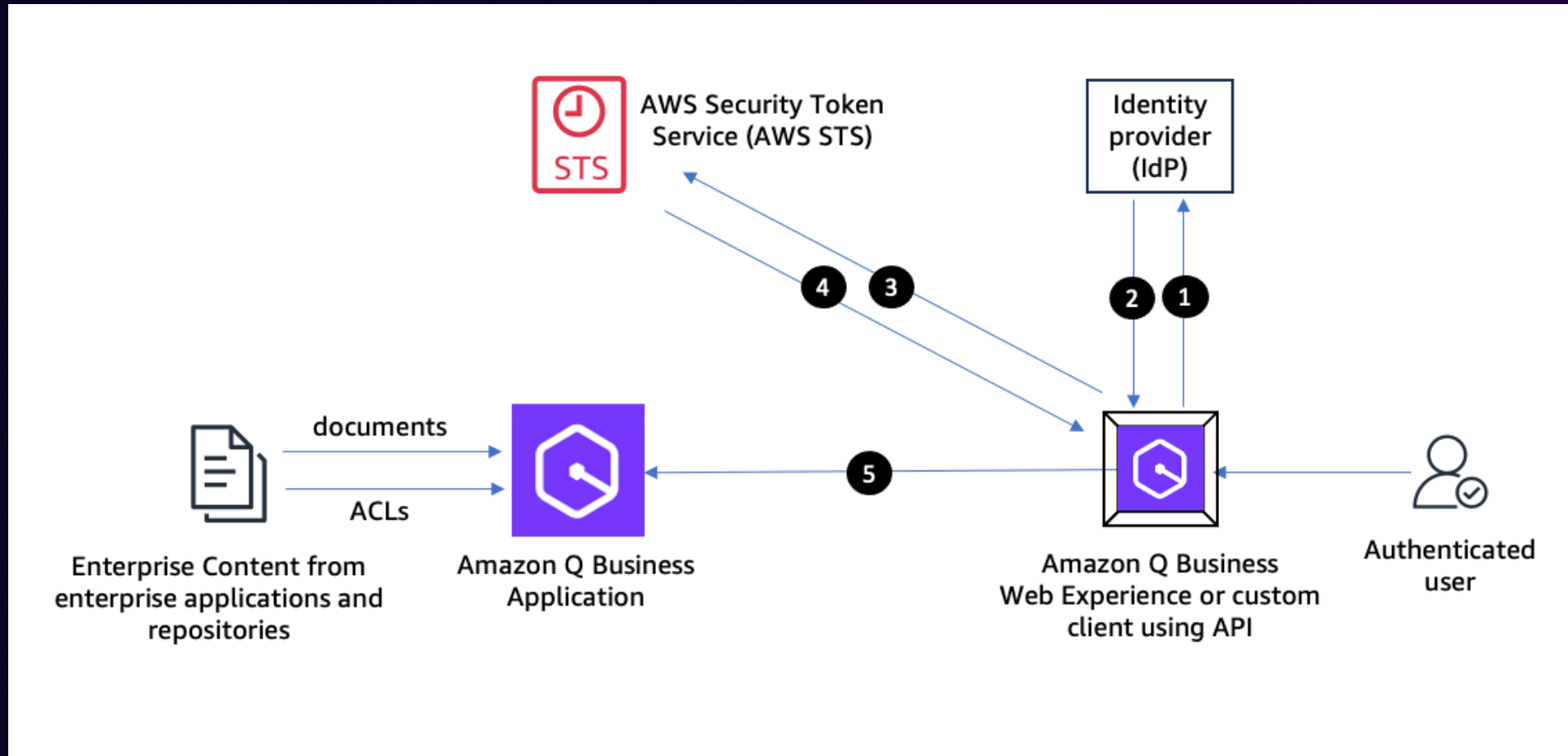
ALLOW A USER TO MANAGE A SPECIFIC PLUG-IN IN A CHAT APPLICATION

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": [  
  
      "qbusiness:GetPlugin",  
      "qbusiness:UpdatePlugin",  
      "qbusiness:DeletePlugin"  
    ],  
    "Resource": [  
      "arn:aws:qbusiness:<REGION>::<ACCOUNT>:application/<APPLICATION ID>",  
      "arn:aws:qbusiness:<REGION>::<ACCOUNT>:application/<APPLICATION ID>/plugin/<PLUGIN ID>"  
    ]  
  }  
]
```


04 IAM Identity Center

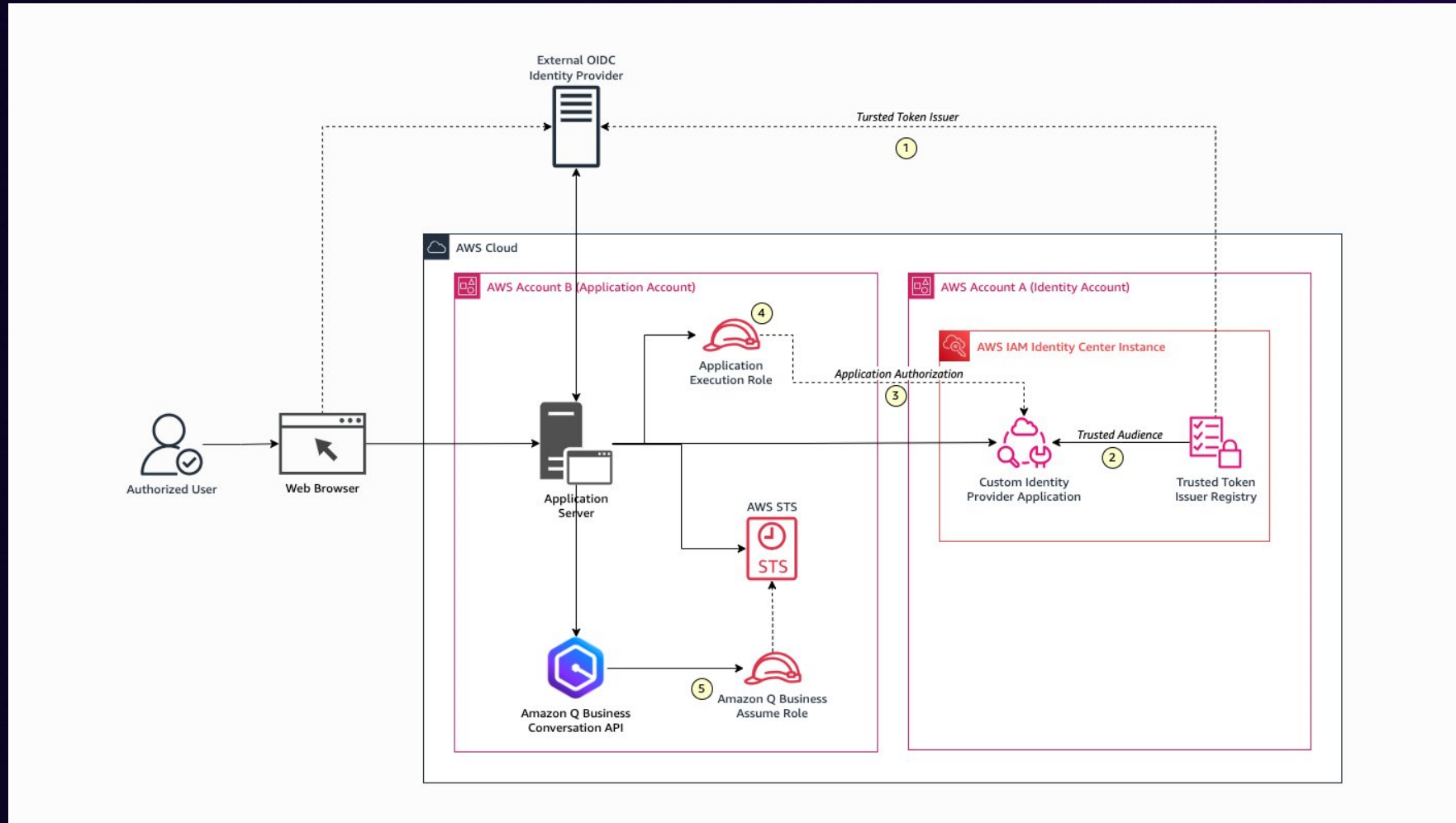
Authentication workflow

AUTHENTICATION VIA IAM FEDERATION



Authentication workflow

AUTHENTICATION VIA TRUSTED IDENTITY PROPAGATION



Guide to choosing a user access mechanism

HOW THE CHOICE AFFECTS YOUR SUBSCRIPTION COSTS

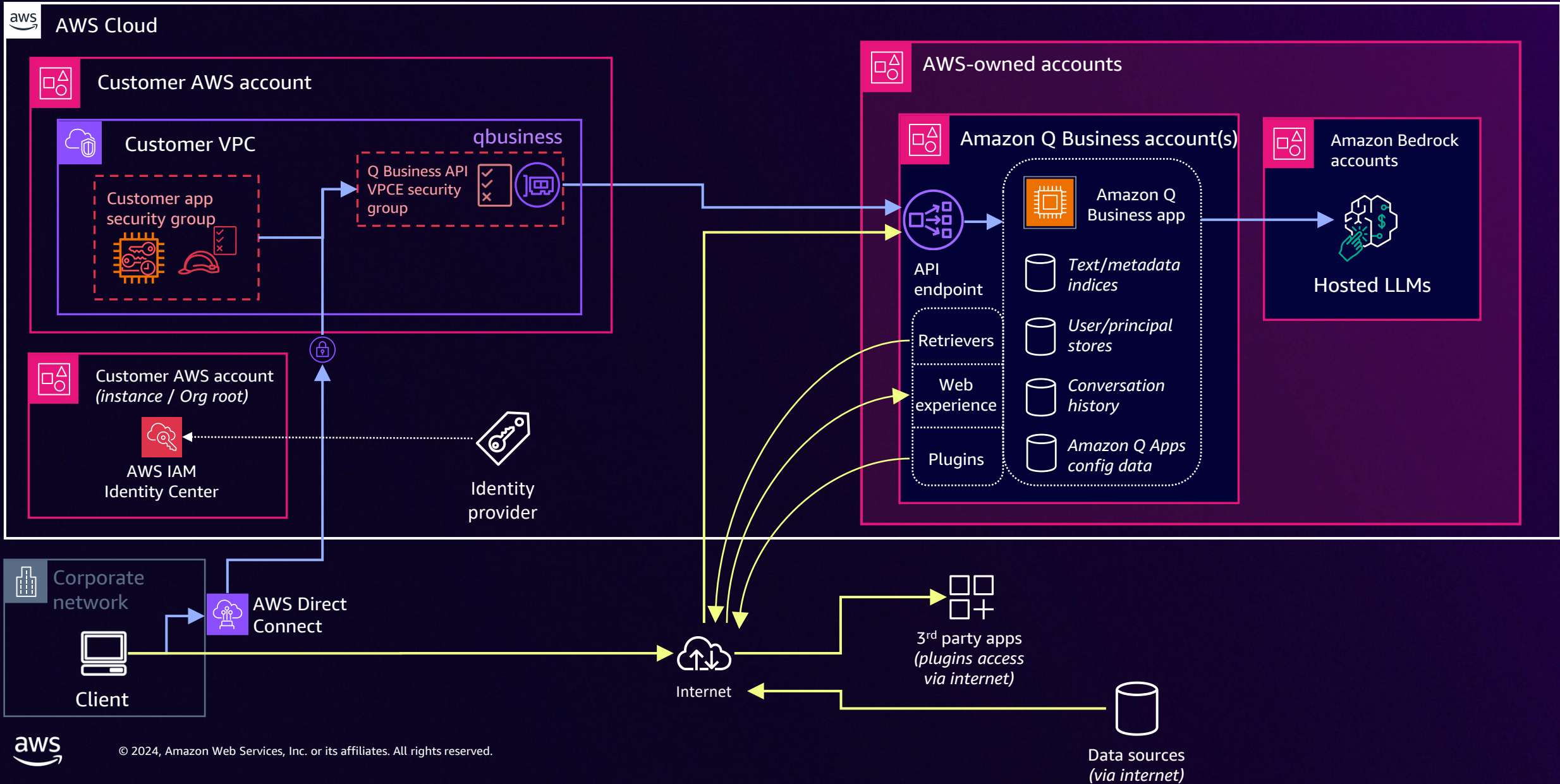
Access Mechanism	Configuration	App1 in AC1 Reg1	App2 in AC1 Reg1	App3 in AC1 Reg2	App4 in AC2 Reg2
IAM Identity Center (Org)	Per AWS Org	\$\$	---	---	---
IAM Identity Center (Instance)	Per account/region	\$\$	---	\$\$	\$\$
IAM Federation	Per account/IDP	\$\$	---	---	\$\$

1. Use AWS Organizations with IAM Identity Center
2. Use an IAM Identity Center instance
 - Proofs of concept or temporary trials
 - IAM Identity Center is not yet deployed in your AWS Organization and you do not wish to delay
 - You want application(s) to be outside of the AWS Organization instance of IAM Identity Center
 - Your organization does not have a single identity provider or store with the userbase you need
3. Use IAM Federation if IAM Identity Center is not an option

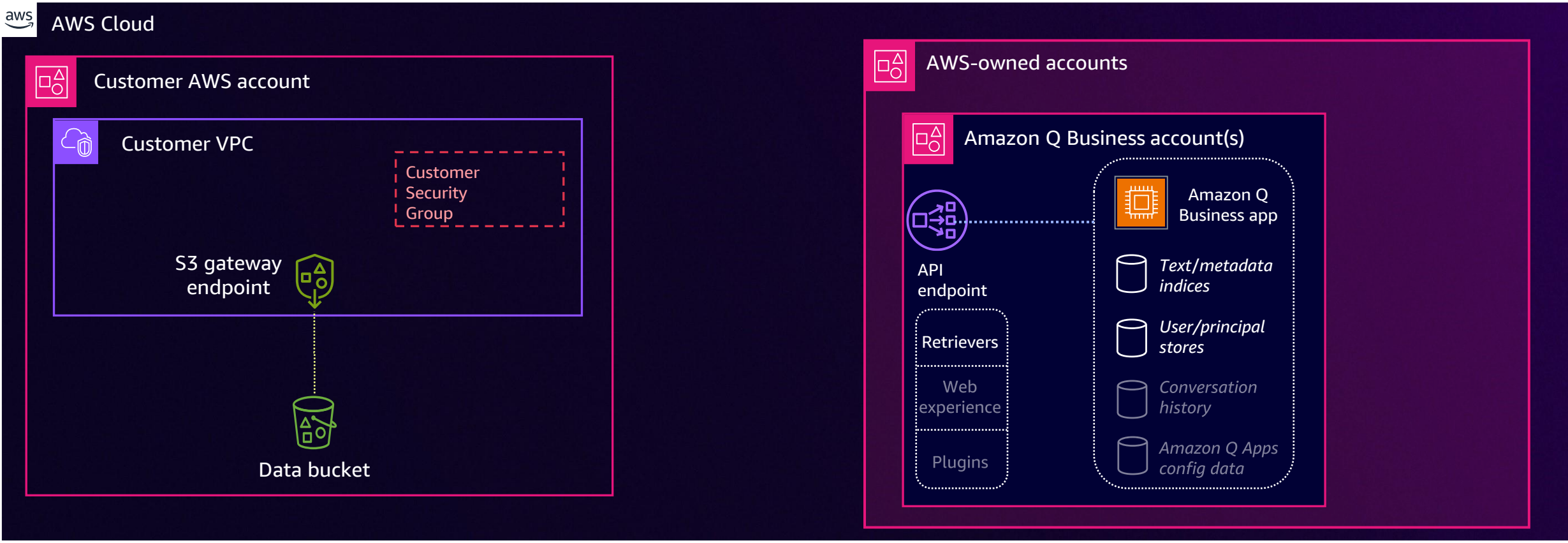


05 High-level administration flows

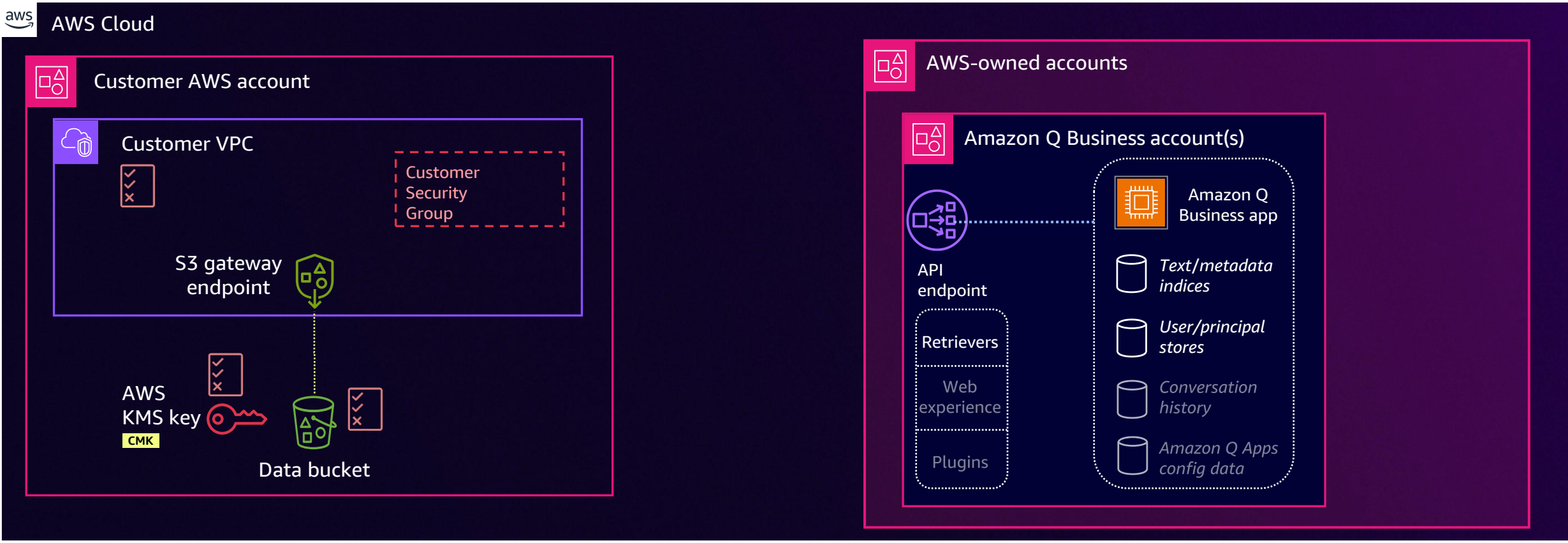
Amazon Q Business architecture overview



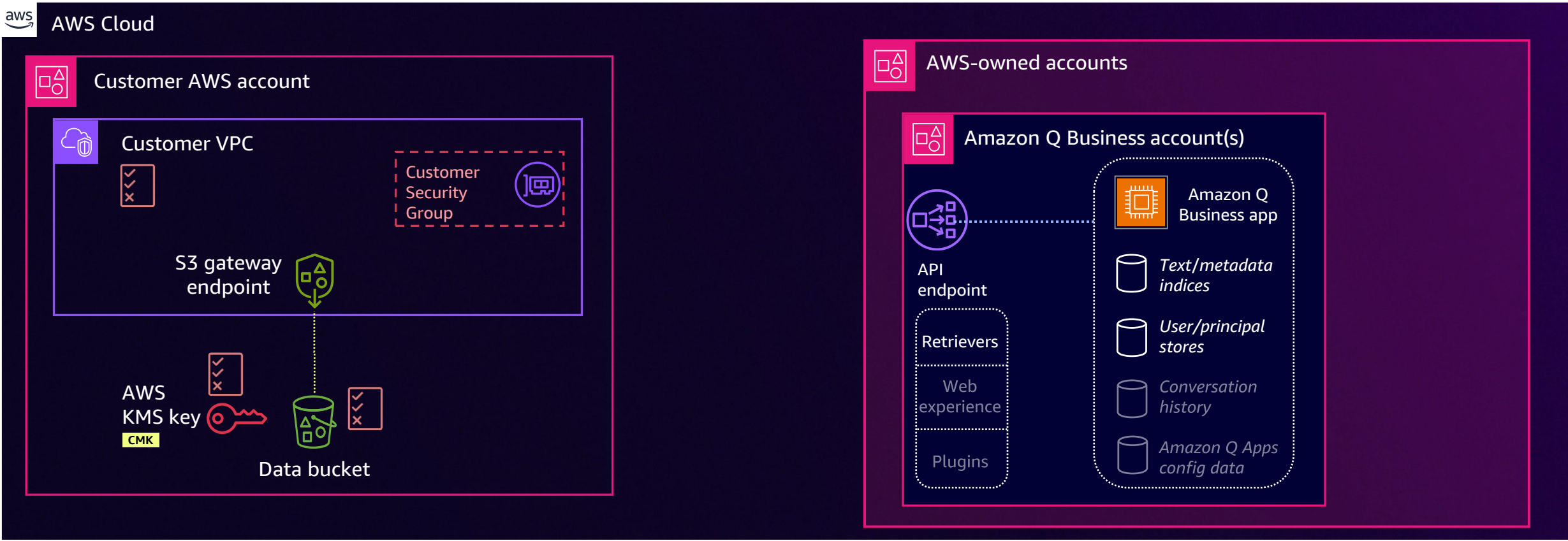
Native retriever flow – Amazon S3



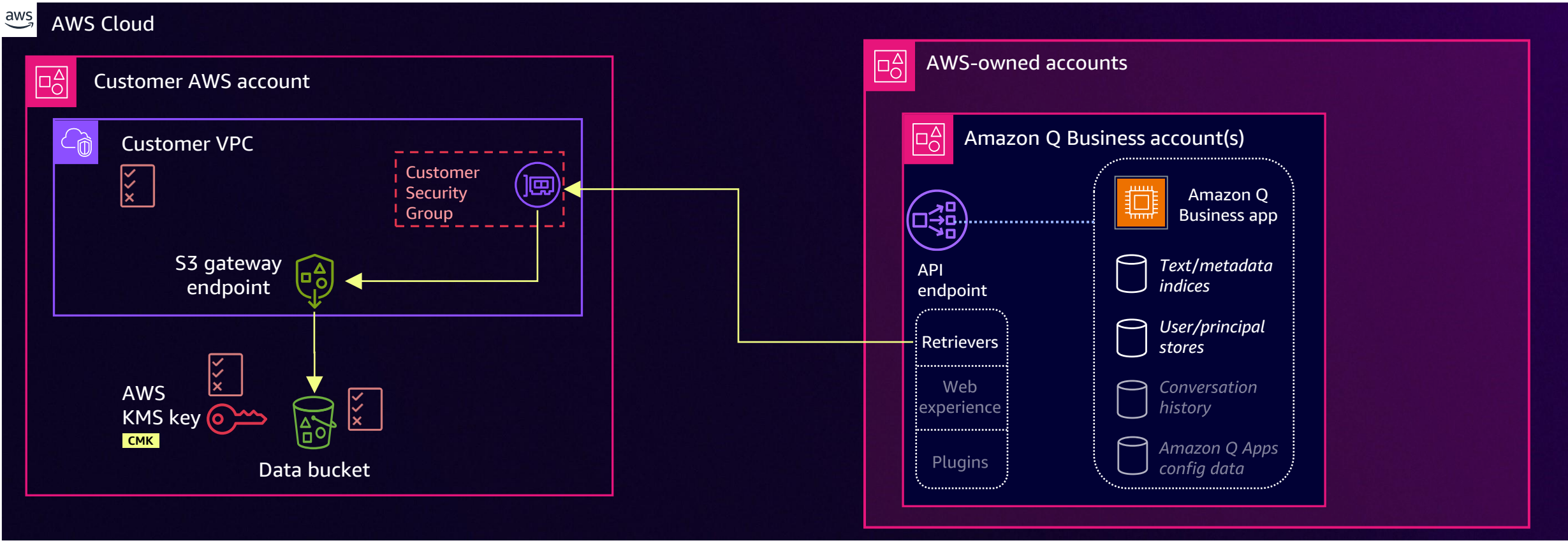
Native retriever flow – Amazon S3



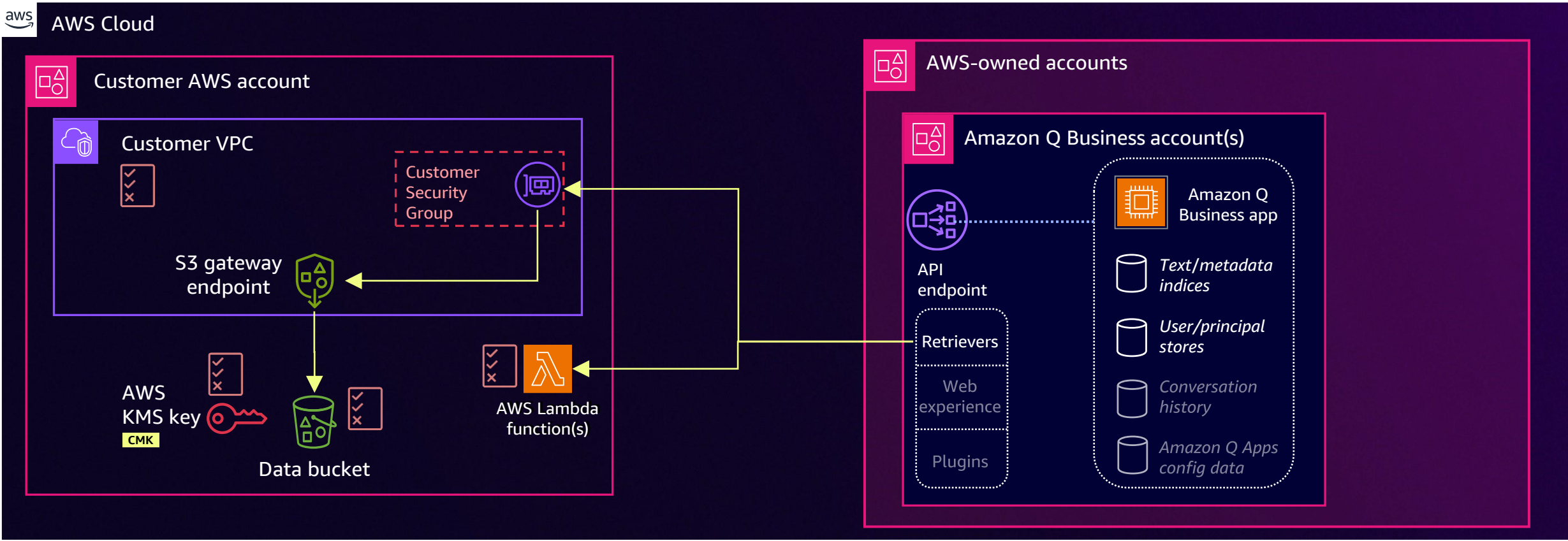
Native retriever flow – Amazon S3



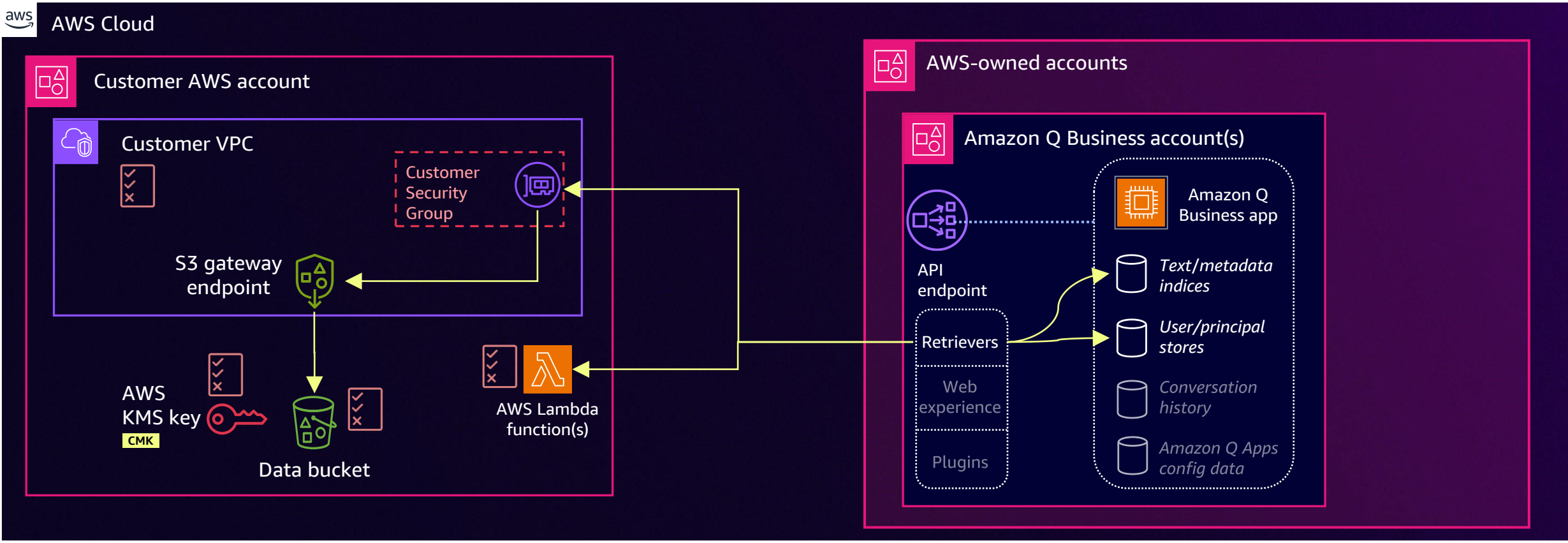
Native retriever flow – Amazon S3



Native retriever flow – Amazon S3



Native retriever flow – Amazon S3



06 Guardrails

Controls and guardrails

CUSTOMIZE AND CONFIGURE THE END USER CHAT EXPERIENCE



Global controls

Applies to **all conversations**

- Use of base LLM knowledge (*query/fallback*)
- Personalize responses (*IDC only*)
- Allow file uploads
- Blocked words (*20 phrases*)

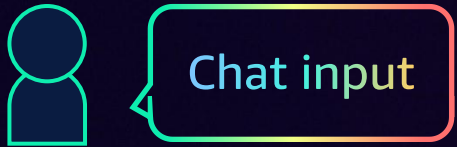


Topic-level controls

Applies to **specific topics** (*max of 2*)

- Name
- Description
- Example chat message (*max of 5*)
- Rules (*max of 5*)
 - Behavior (*block or restrict to ENT data*)
 - Sources (*if ENT data*)
 - User groups (*include/exclude*)

Controls and guardrails flow



Controls and guardrails

Toxicity filter**

Special topics

Words/phrases

*** on output only*

Chat output

Controls and guardrails flow



Controls and guardrails

Toxicity filter**

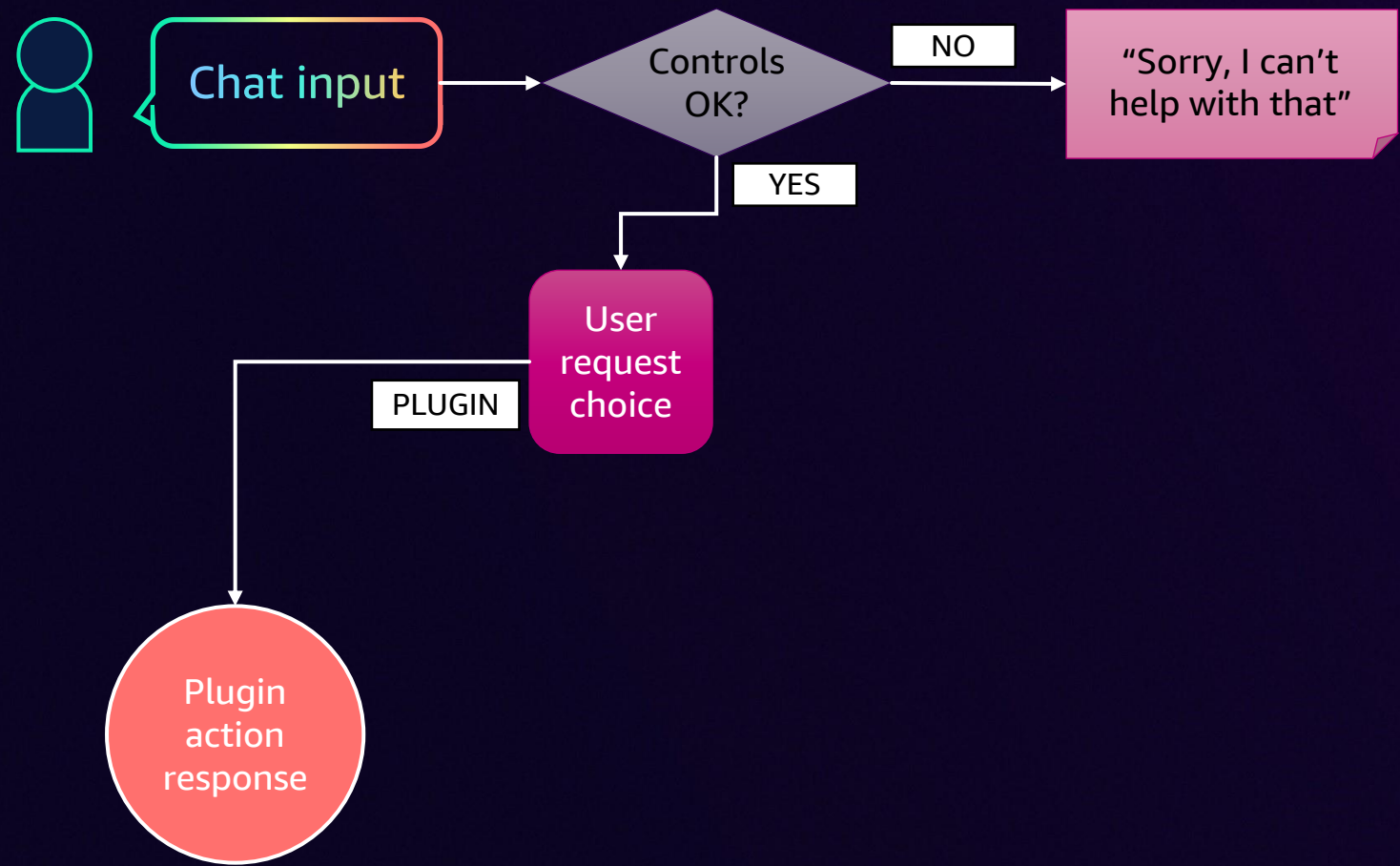
Special topics

Words/phrases

** on output only

Chat output

Controls and guardrails flow



Controls and guardrails

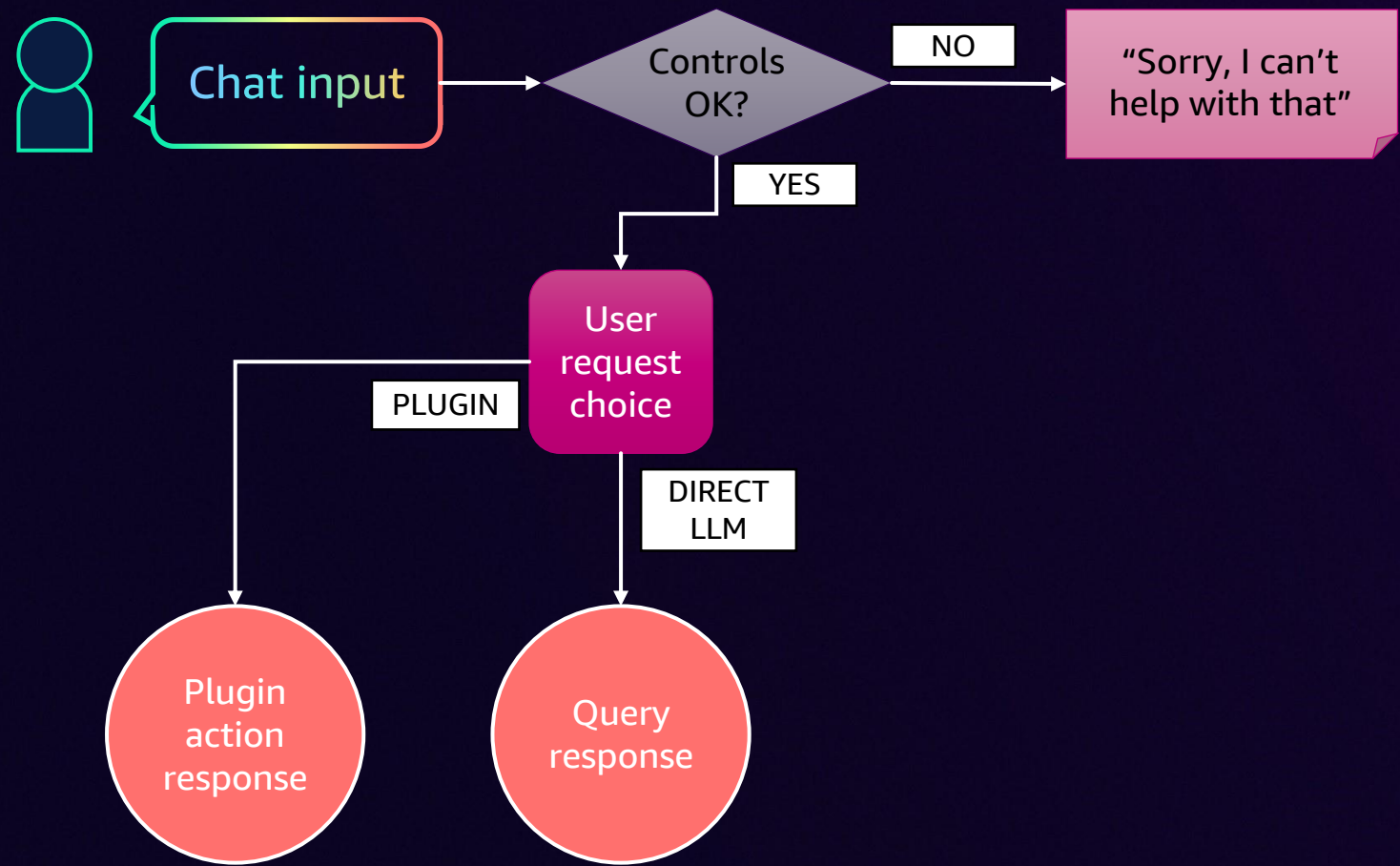
Toxicity filter**

Special topics

Words/phrases

** on output only

Controls and guardrails flow



Controls and guardrails

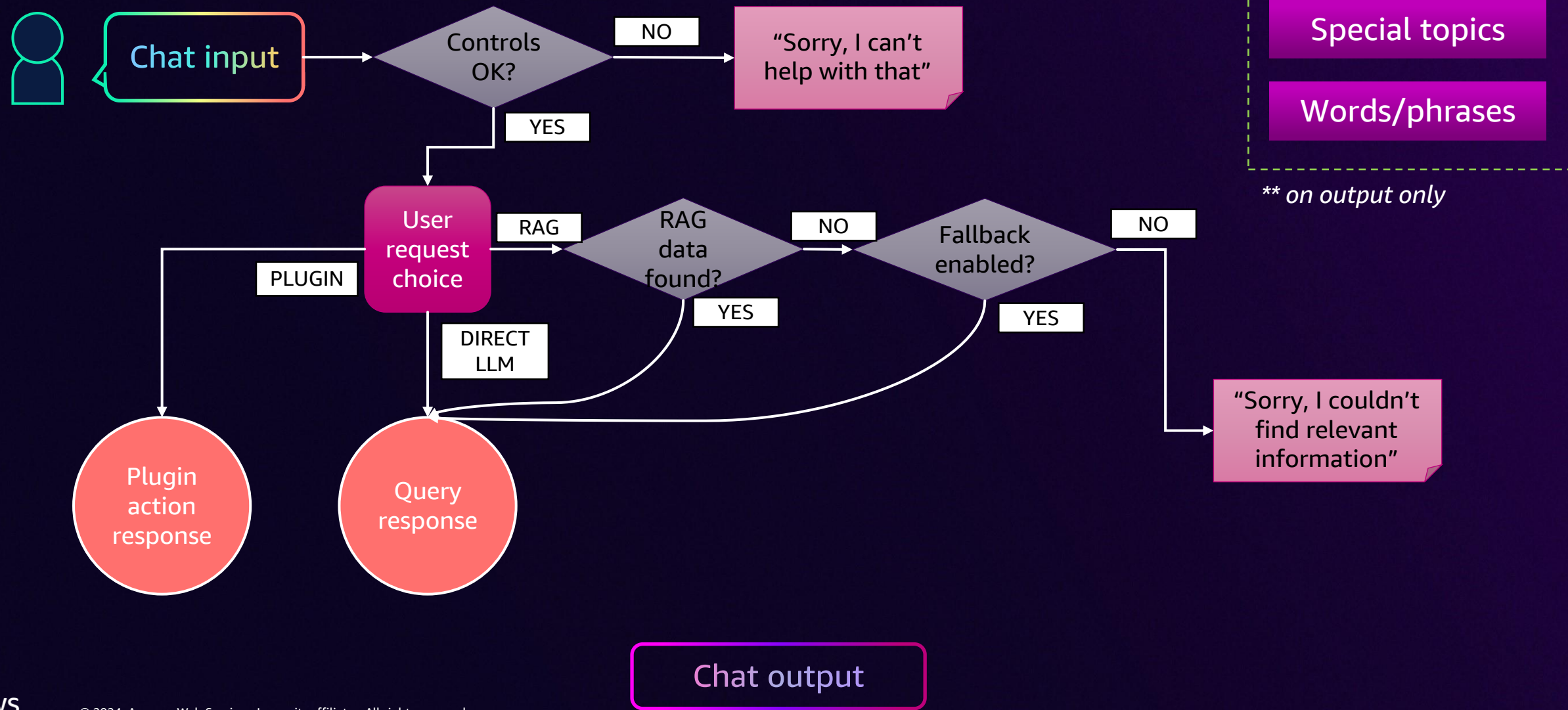
Toxicity filter**

Special topics

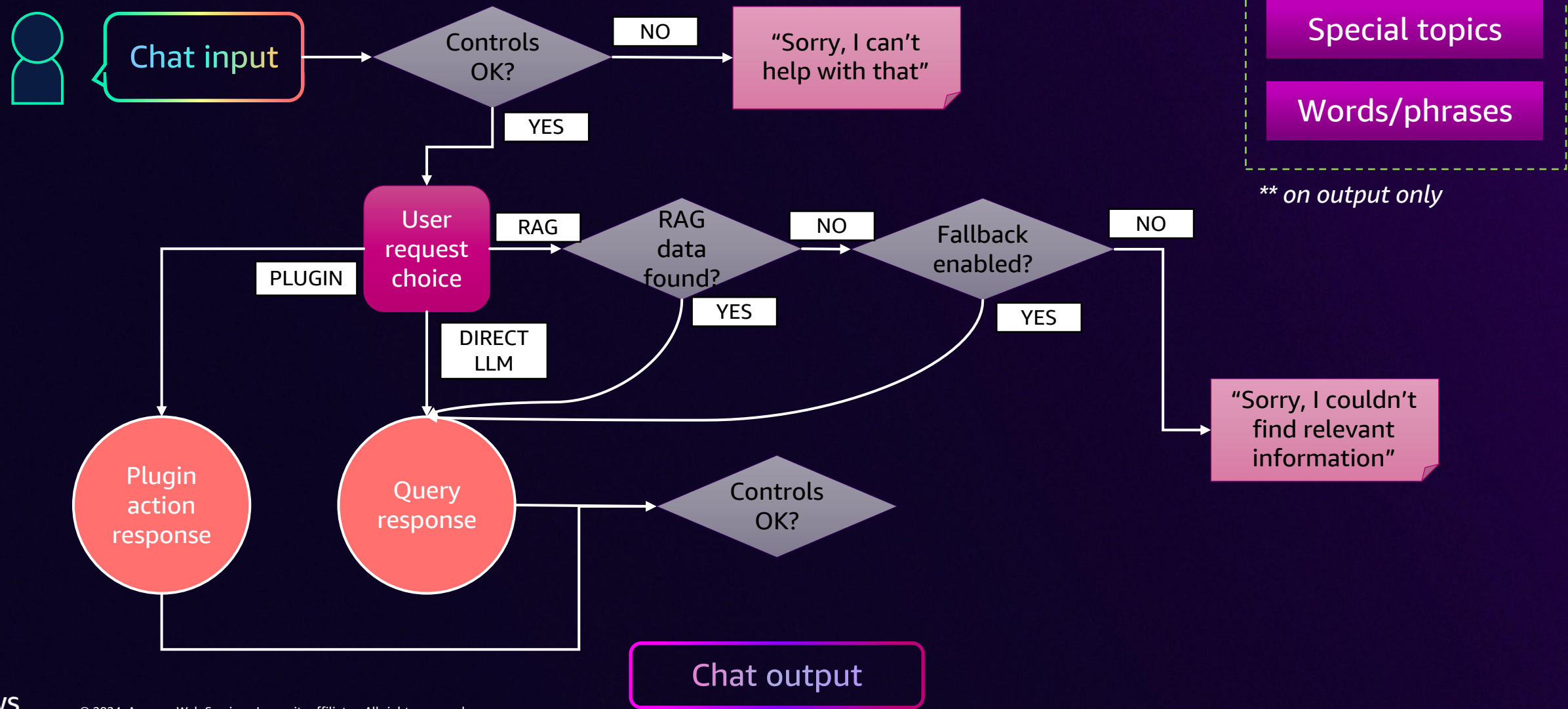
Words/phrases

** on output only

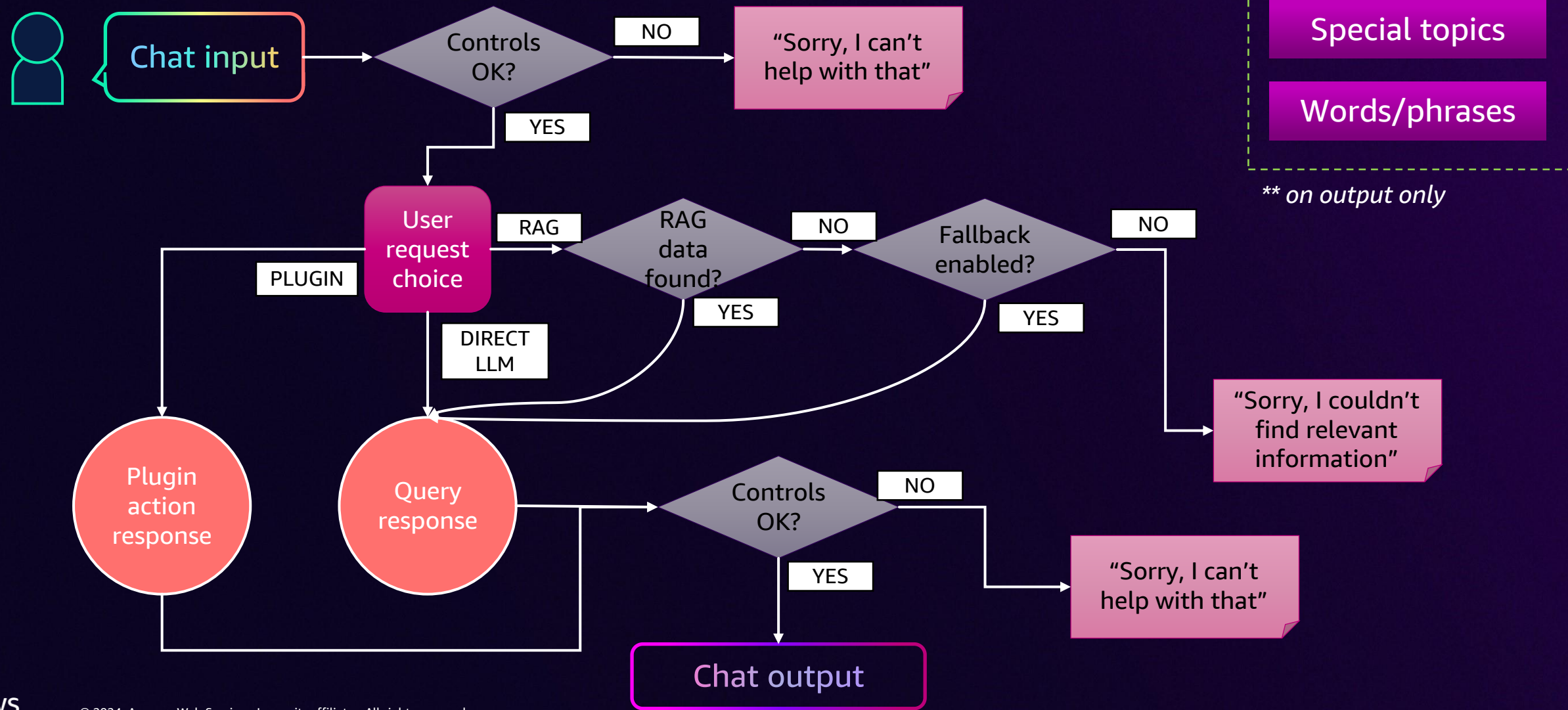
Controls and guardrails flow



Controls and guardrails flow



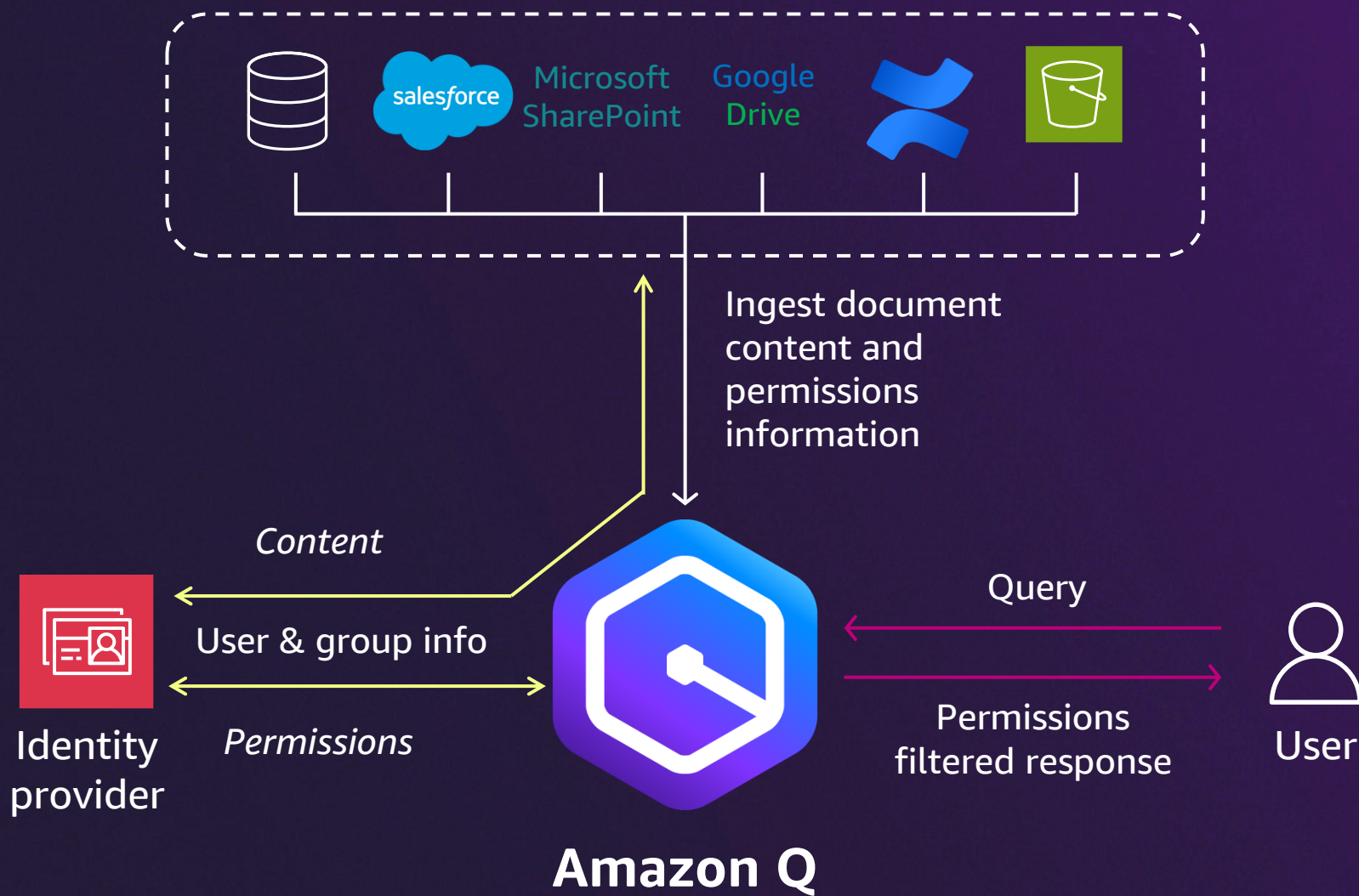
Controls and guardrails flow



07 Repository connectors

Safety and security

AMAZON Q BUSINESS IS
AWARE OF ENTERPRISE USER
PERMISSIONS



Connector security

VARIATIONS OF CONNECTOR SECURITY AND DATA CONFIGURATIONS

	Amazon S3	Confluence (cloud)	Jira	Microsoft Teams	Salesforce online	Slack
Authentication	AssumeRole	Basic, OAuth2	Basic	OAuth2	OAuth2	Token
Credentials	n/a	User/pass, app key/secret	Jira ID, Jira token	Client ID + secret	URL + keys + secrets	Workspace ID + bot or user token
Identity crawl	No	Yes	No	Yes	Yes	Yes
ACL crawl	Yes	Yes	Yes	Yes	Yes	Yes
Metadata crawl	Yes	Yes	Yes	Yes	Yes	No
Entities	Document	Space, page, blog, comment, attachment	Projects, issues, comments, attachments, worklogs	Wiki, channel posts/files, 2 x chat, 4 x meeting	~20 entities	Pub/priv channels, 4 x messages



Thank you!

Dr. Andrew Kane

✉ andkane@amazon.co.uk
in andrewjkane

Gabrielle Dompreh

✉ domprehg@amazon.co.uk
in gabrielledomp reh



Please complete the session survey in the mobile app