Amazon SageMaker Security Features

Amazon SageMaker – Build, Train, and Deploy

SageMaker security features

Authorization access

Defense in depth

End to end encryption

Dedicated infrastructure

Network controls

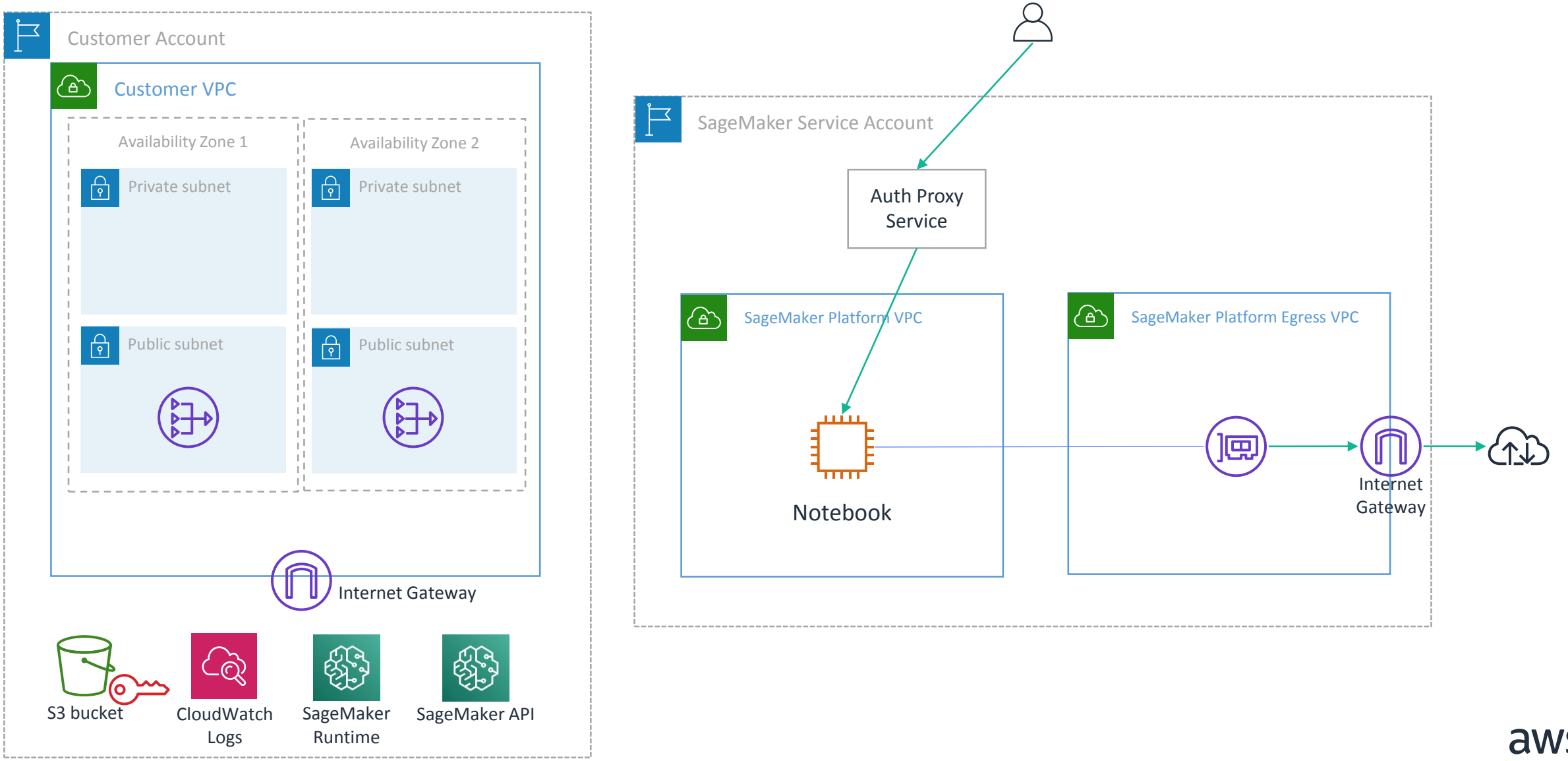
Private connectivity

OS customization

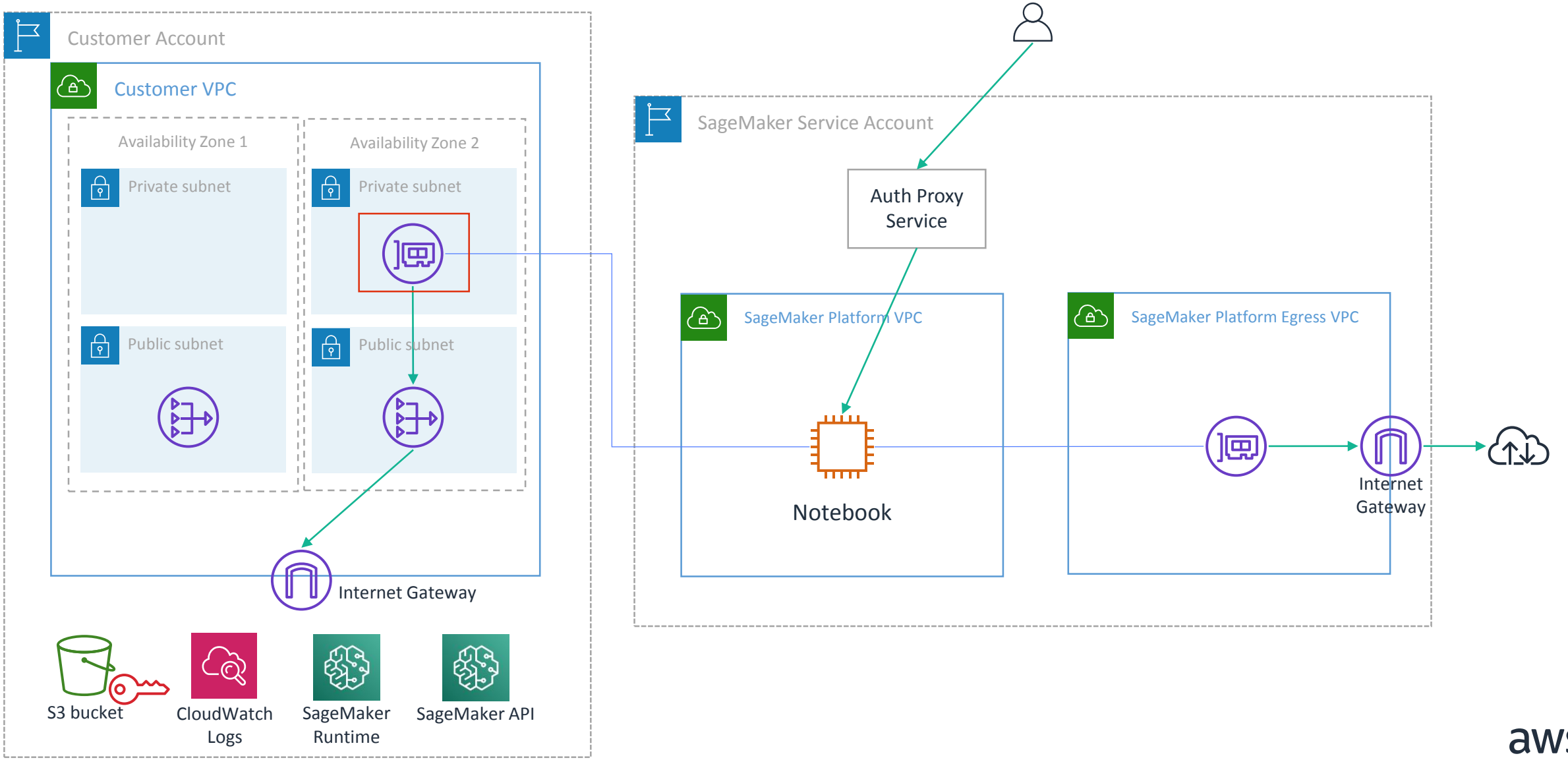
Logging and audit

SageMaker Networking

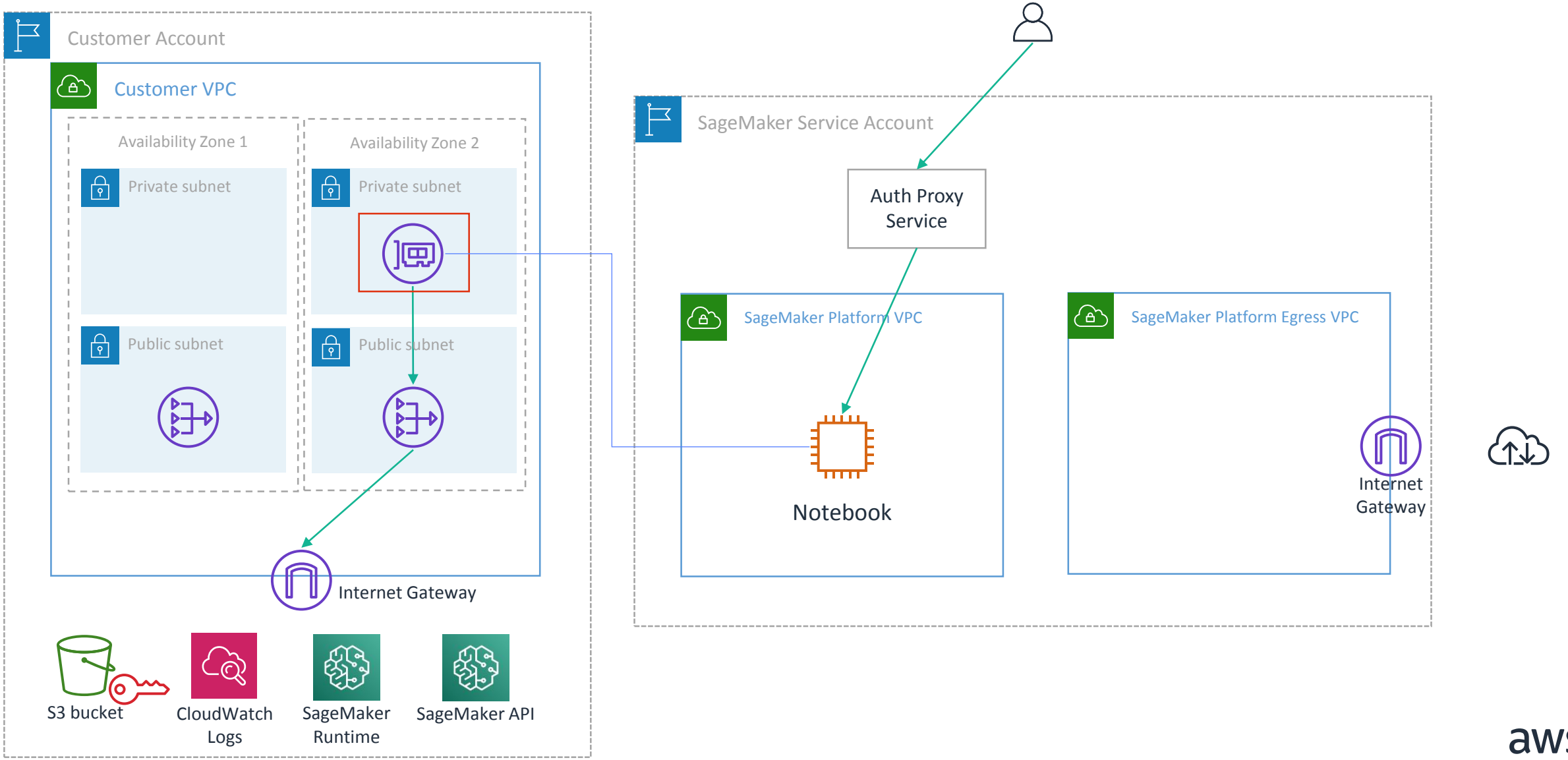
SageMaker notebook - SageMaker egress, no VPC connectivity



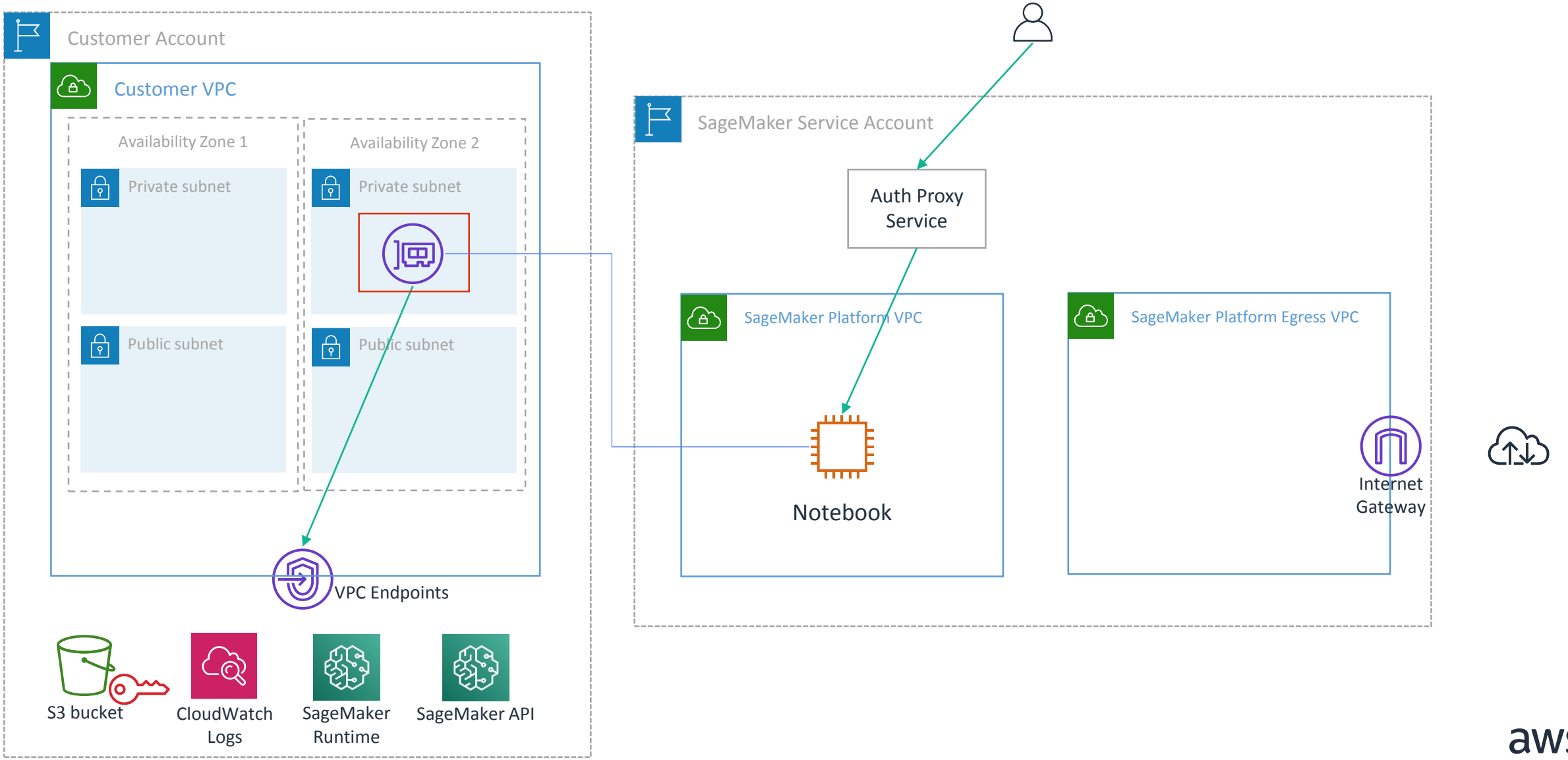
SageMaker notebook - SageMaker egress and VPC connectivity



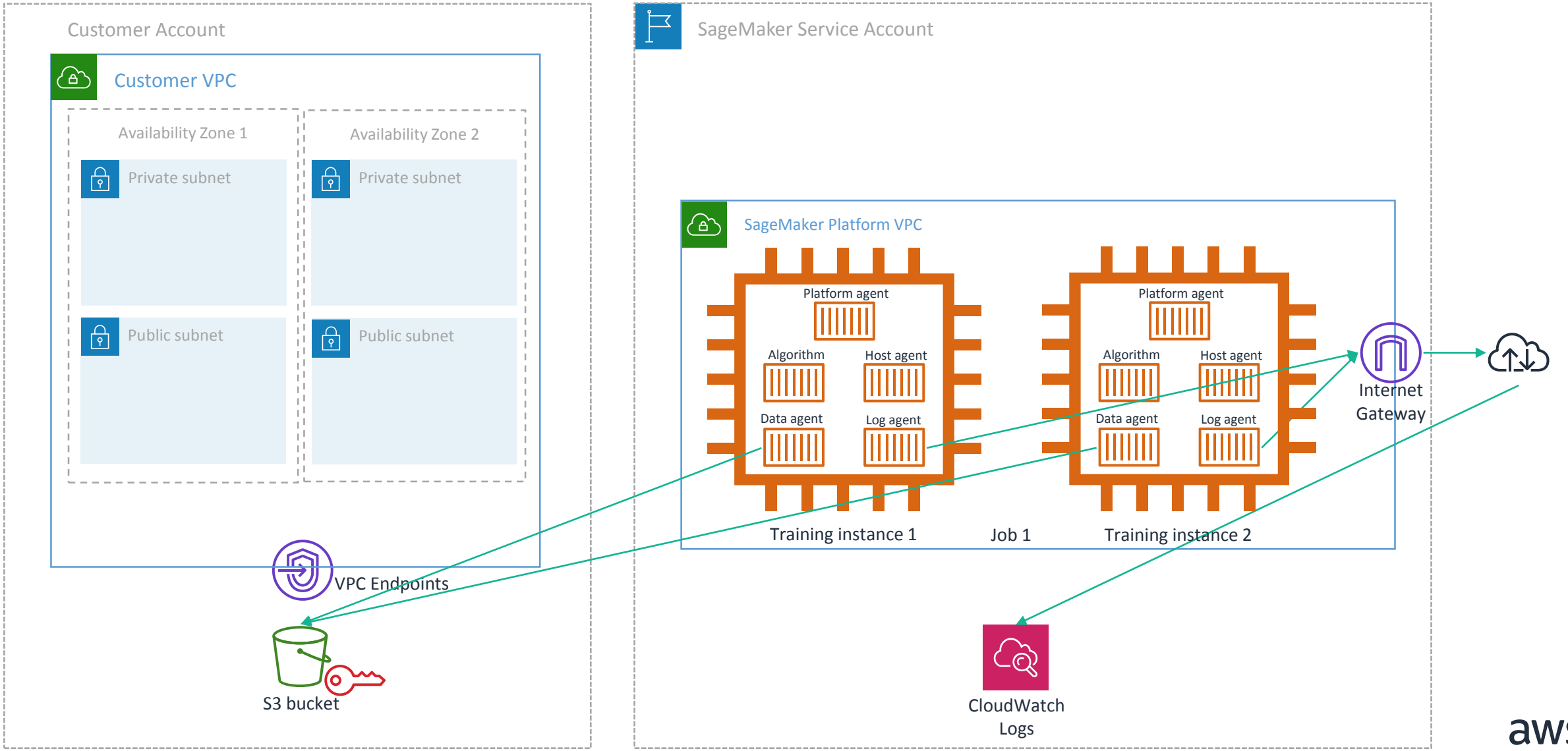
SageMaker notebook – no SageMaker egress, VPC connectivity



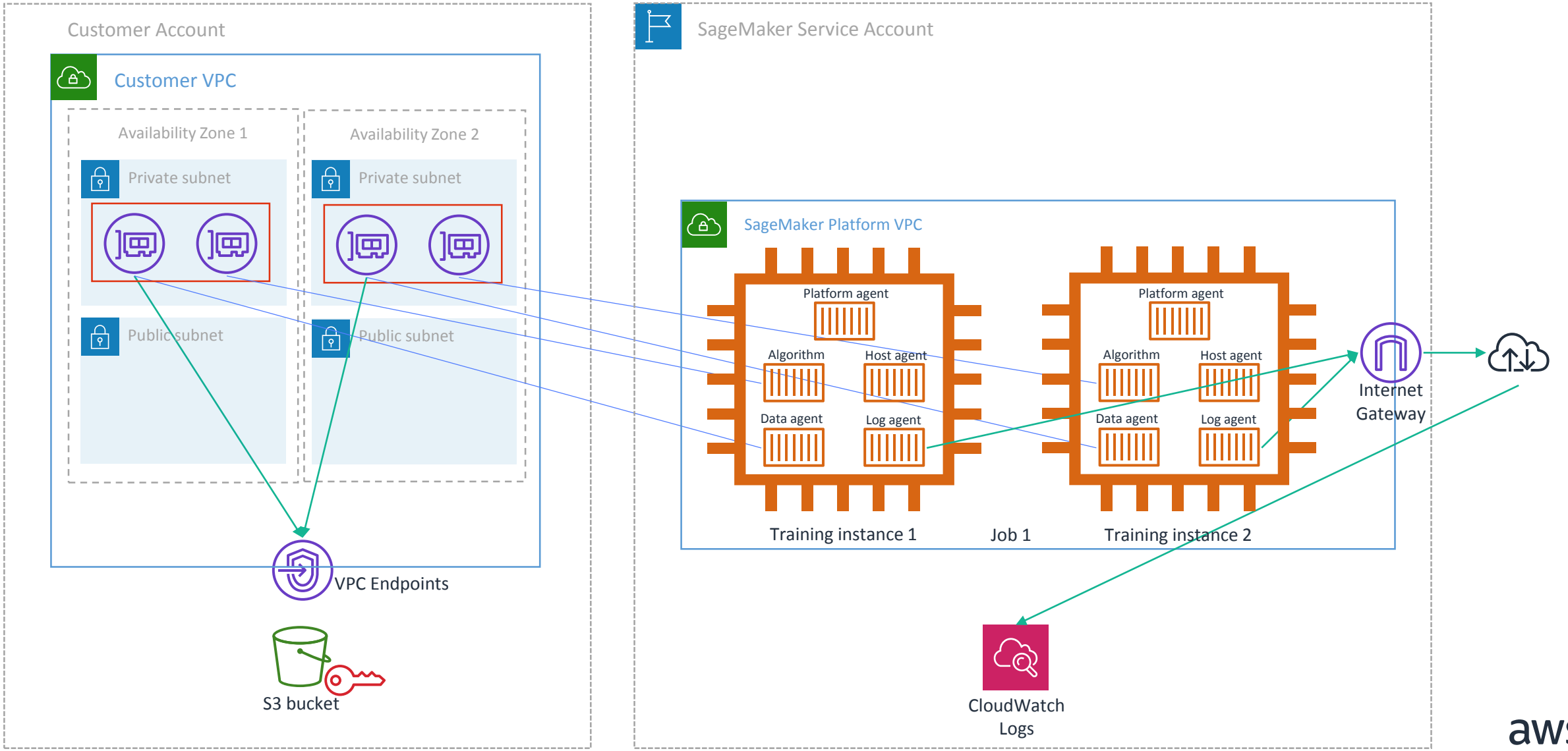
SageMaker notebook – VPC connectivity with VPC endpoints



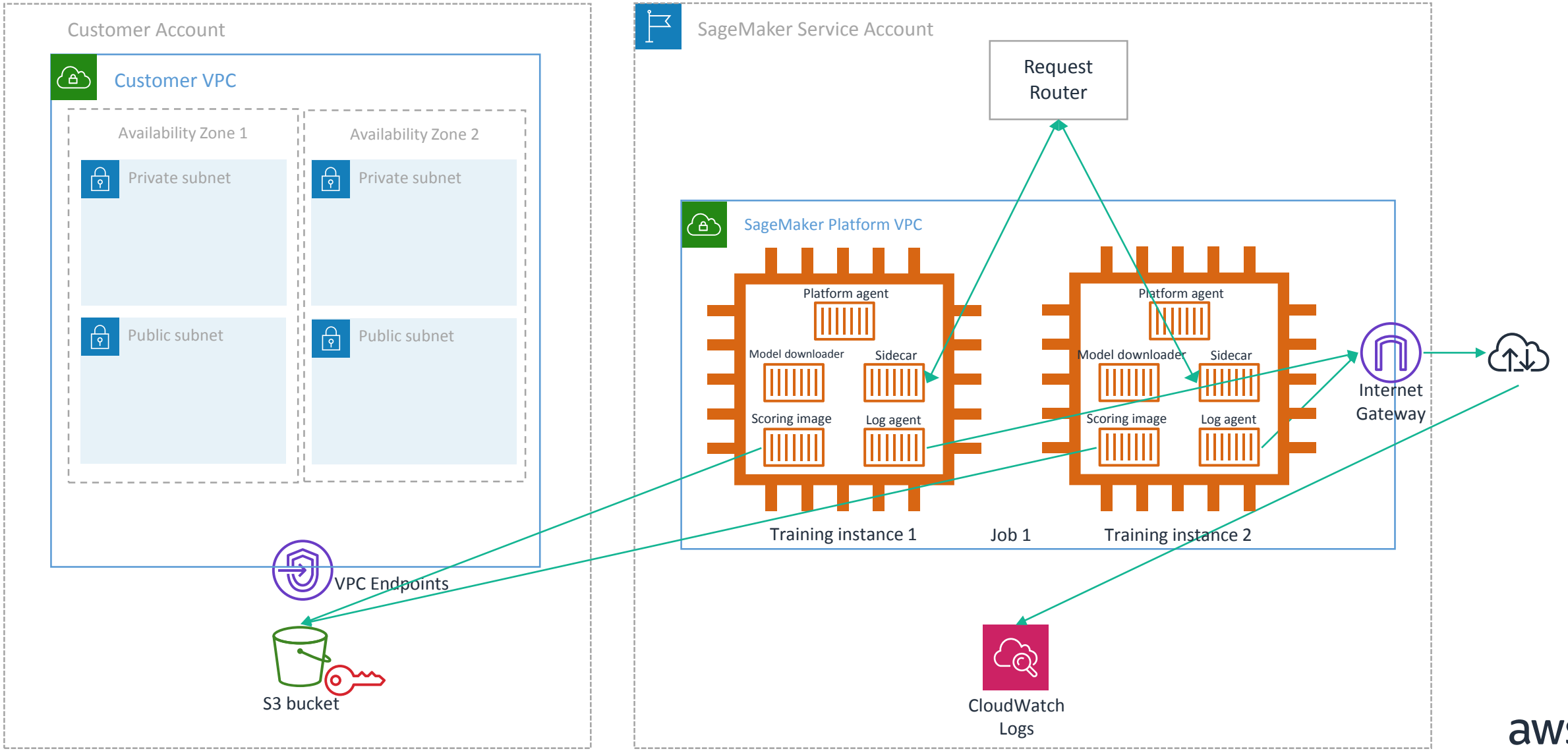
SageMaker training default deployment



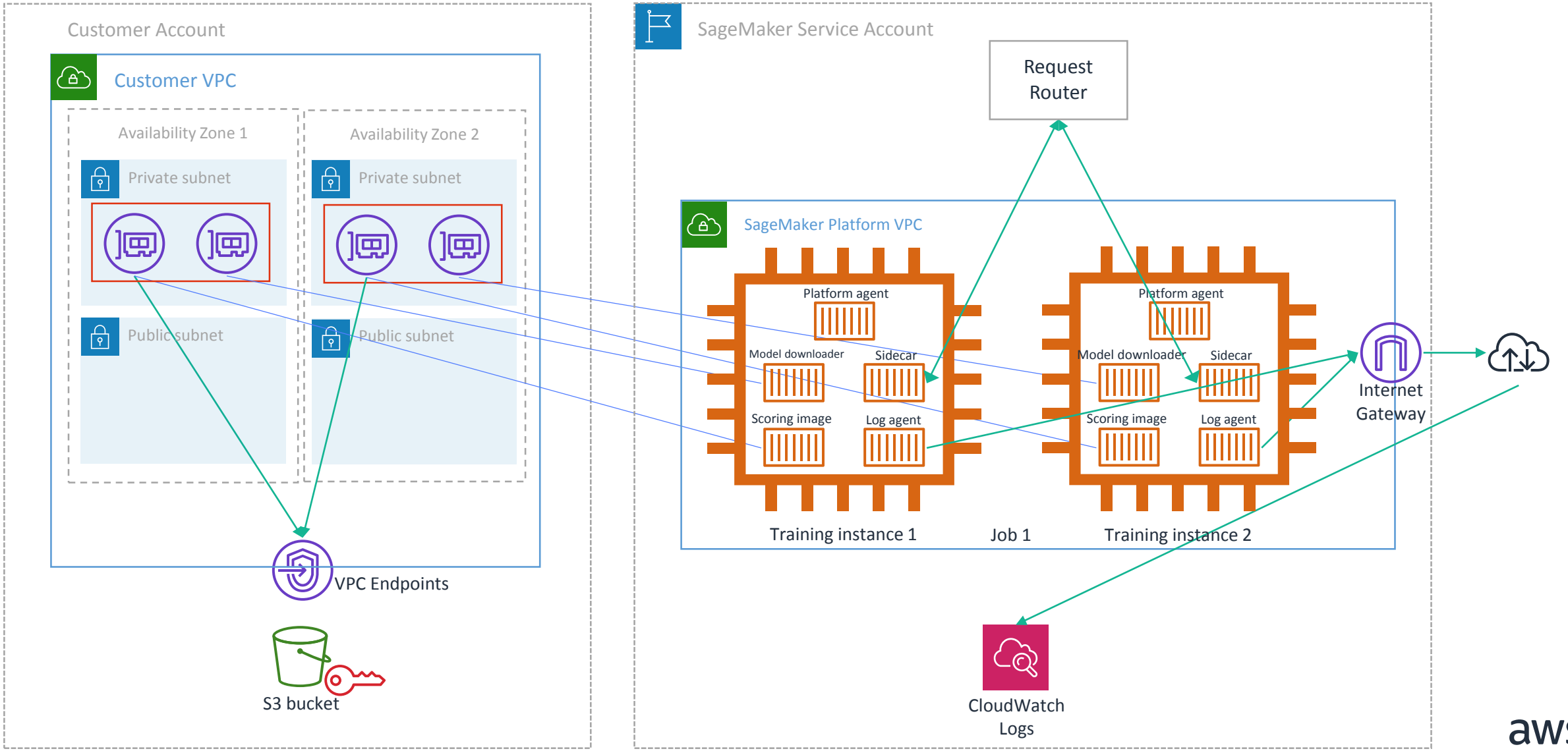
SageMaker training VPC deployment



SageMaker hosting default deployment



SageMaker hosting VPC deployment



Secure ML configurations

General

- Encrypt data at rest
- Encrypt data in transit

Network

- Network controls around compute
- Enforce AWS access using endpoint policies
- Private network connectivity using VPC endpoints
- No internet access
- Logging of all network traffic
- Secure access to environment without data egress

Data lake

- Disable public access to data lake
- Log access to data lake
- Make data lake read-only

Experimentation

- Private least-privilege access to notebook instances
- Apply IT policies to notebooks

Training

- Logging and monitoring of training

Hosting

- Authorize access to hosted models
- Private access to hosted models
- Logging and monitoring of models

Demonstration

Secure ML configurations

General

- Encrypt data at rest
- Encrypt data in transit

Network

- Network controls around compute
- Enforce AWS access using endpoint policies
- Private network connectivity using VPC endpoints
- No internet access
- Logging of all network traffic
- Secure access to environment without data egress

Data lake

- Disable public access to data lake
- Log access to data lake
- Make data lake read-only

Experimentation

- Private least-privilege access to notebook instances
- Apply IT policies to notebooks

Training

- Logging and monitoring of training

Hosting

- Authorize access to hosted models
- Private access to hosted models
- Logging and monitoring of models

SageMaker security summary

Authorization access

Defense in depth

End to end encryption

Dedicated infrastructure

Network controls

Private connectivity

OS customization

Logging and audit

Thank you

aws.amazon.com/sagemaker