Section 3 Design 2

- Confluent Cloud is a SaaS for Apache Kafka. This service is chosen over self-hosted Kafka implementations for the easier architecture management and maintenance.
- This design assumes the resources are within a Virtual Network with an NSG rule which allows outbound TCP connection to Confluent Cloud.
- API calls to Web Application 1 will go through the App Gateway. The App Gateway will enforce the HTTPS connection, redirecting the user to use the HTTPS connection if they are not on it. Otherwise, the App Gateway will act as the reverse proxy and forward the request to Web Application 1 for processing the image uploaded by the user.
- The Web Application Firewall should also be configured on the App Gateway and be on **Prevention** mode to detect and block any anomaly and malicious requests after they meet the recommended threshold.

(*) CONFLUENT

Confluent Cloud

User

(PC or Mobile)

3 Web Application requires

authenticated through

Organisation's Tenant

Service hosting the Web

configured to managed

process automatically.

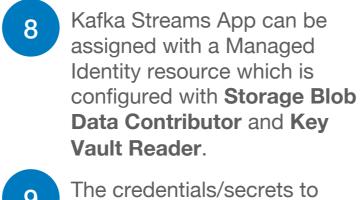
Directory. The App

Application 1 can be

this authentication

the User to be

AAD using the



Azure

- establish the connection to Confluent Cloud can be retrieved from Key Vault. Engineers can manage the secrets without downtime.
- The App Service hosting the Kafka Streams App will be configured to Scale Out based on the CPU utilisation rate over a defined period of time. This can help alleviate pressure on the resources as the organisation grows.

App Gateway + WAF

Azure Active Directory

(Organisation's Tenant)

With Lifecycle Management for Storage Account, a Rule can be created against all Base Blobs (images) stored in the containers, which will delete the Base Blob after the 7th day since creation. This will align with the privacy and compliance requirements. Azure Storage Service Encryption (SSE) can automatically encrypt data before it is stored, and it automatically decrypts the data when retrieving it.

Image Container

Storage Account

Power BI is the Business Intelligence tool of choice as it can integrate with data sources from Azure resources including Azure Cosmos DB and Blob storage.

> **Shared Access Signatures** (SAS) can be generate from Storage Account Containers and they can be configured to be read-only, suitable for analytical purposes. Power BI can connect to the blob storage container using the generated SAS.

Metadata Store

Power BI on Azure

12 13

Processing Script

Azure Functions

Azure Cosmos DB Processed image metadata is

stored in NoSQL database for analysis. Data is configured with 7 days TTL to purge expired data completely after retention period. Encryption at rest is implemented by secure key storage systems, encrypted networks, and cryptographic

Image processing script deployed to Azure Functions will react to file uploads or changes in blob storage. Processed images are stored in blob storage and corresponding metadata is stored in Cosmos DB. Can be

scaled to meet demand.

Azure Functions Sink Connector for Confluent Platform configured with SSL is used to ingest real-time incoming images and metadata.

Web Application 1

Managed Identity (Storage Blob Data Contributor Role)

8 9 10

Managed Identity

(Storage Blob Data

Contributor + Key Vault

Reader)

0------

Key Vault

Kafka Streams App

App Service

App Service

alleviate pressure on the resource if the organisation expanded. Web Application 1 App Service can be assigned with a Managed Identity resource. The Managed Identity can configured with the Storage

Blob Data Contributor Role which allows Web Application 1 to add images to the storage account container. Managed Identities do not require secrets management.

The App Service hosting the

based on the average number

incoming requests over the

number of instances of the

define period of time. This

Autoscaling configuration can

Web Application 1 over a

Web Application 1 will be

configured to Scale Out

Legend

- AAD Azure Active Directory
- SaaS Software as a Service
- Apache Kafka for Confluent Cloud is an Azure Marketplace offering that provides Apache Kafka as a service that is readily integrated with Azure Cloud.
- NSG Network Security Groups
- TTL Time to live (Defines retention period of data)
- SSL Secure Socket Layer (Provides secure network communication)
- SAS Shared Access Signatures (Provides secured delegated access to resources)