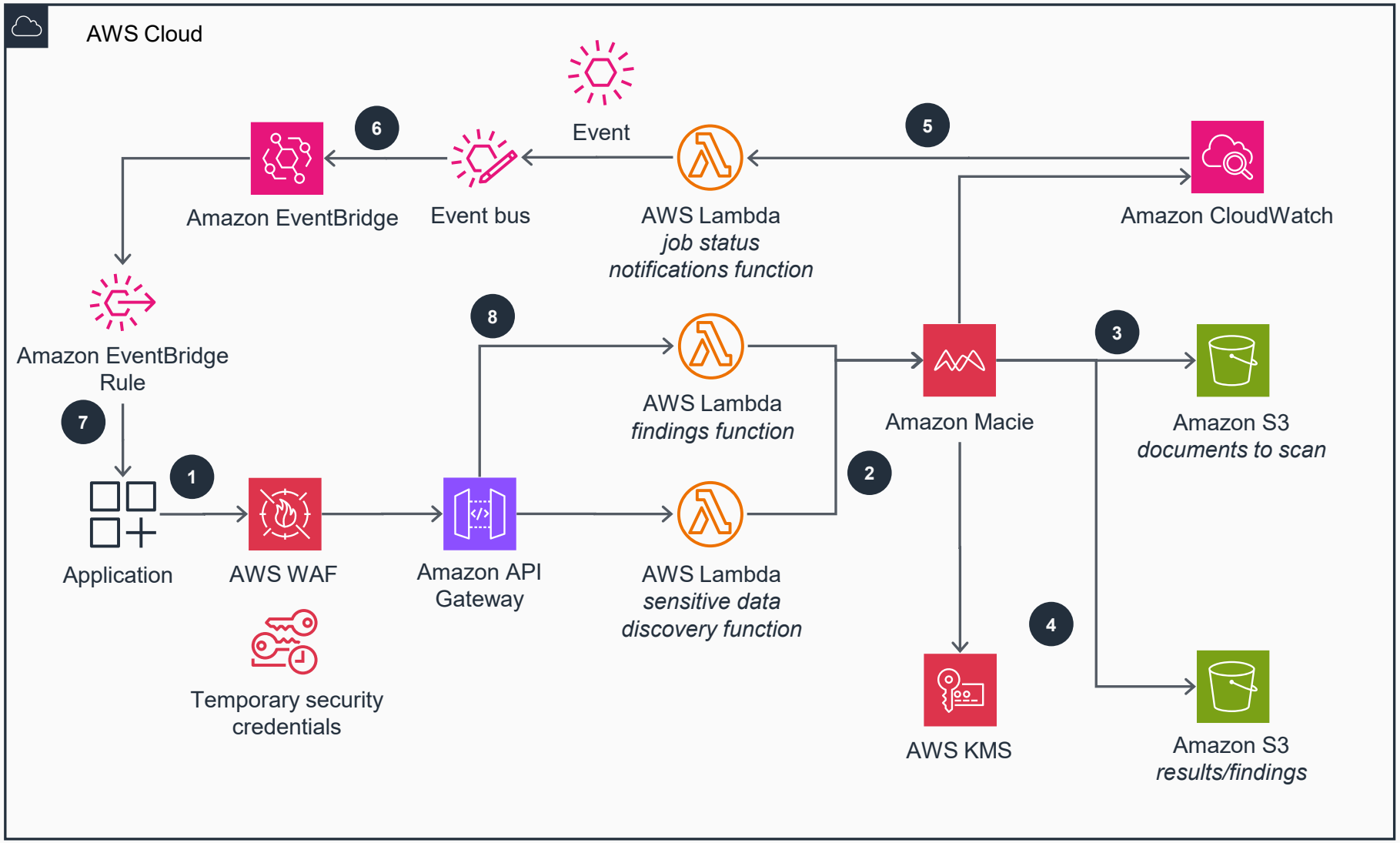
Guidance for Sensitive Information Scanning with Amazon Macie

This architectural diagram demonstrates how customer applications can scan artifacts for PII, financial information or credentials, and other sensitive information with Amazon Macie.



1. The application initiates an **Amazon Macie** scan request and subscribes to **Amazon Macie** job completion events by providing a pre-created **Amazon EventBridge** Event bus ARN. The application calls **Amazon API Gateway** using Temporary security credentials. **AWS Web Application Firewall (AWS WAF)** protects calls to **API Gateway**.
2. An **AWS Lambda** function creates a sensitive data discovery job by invoking the **Macie** API.
3. **Macie** scans all objects in the specified **Amazon S3** *documents to scan* bucket to look for sensitive information. **Macie** uses the customer managed **AWS Key Management Service (AWS KMS)** key(s) to decrypt the **Amazon S3** objects.
4. **Macie** stores the scan results and findings in the **Amazon S3** *results/findings* bucket and encrypts the results/findings using a customer managed **AWS KMS** key.
5. An **Amazon CloudWatch** subscription filter invokes an **Lambda** *job status notifications* function.
6. The *job status notifications* **Lambda** function sends an event on the **EventBridge** Event bus.
7. The **EventBridge** Rule triggers the application.
8. The application makes an API call to get the results/findings.

Reviewed for technical accuracy July 24, 2025

AWS Reference Architecture