

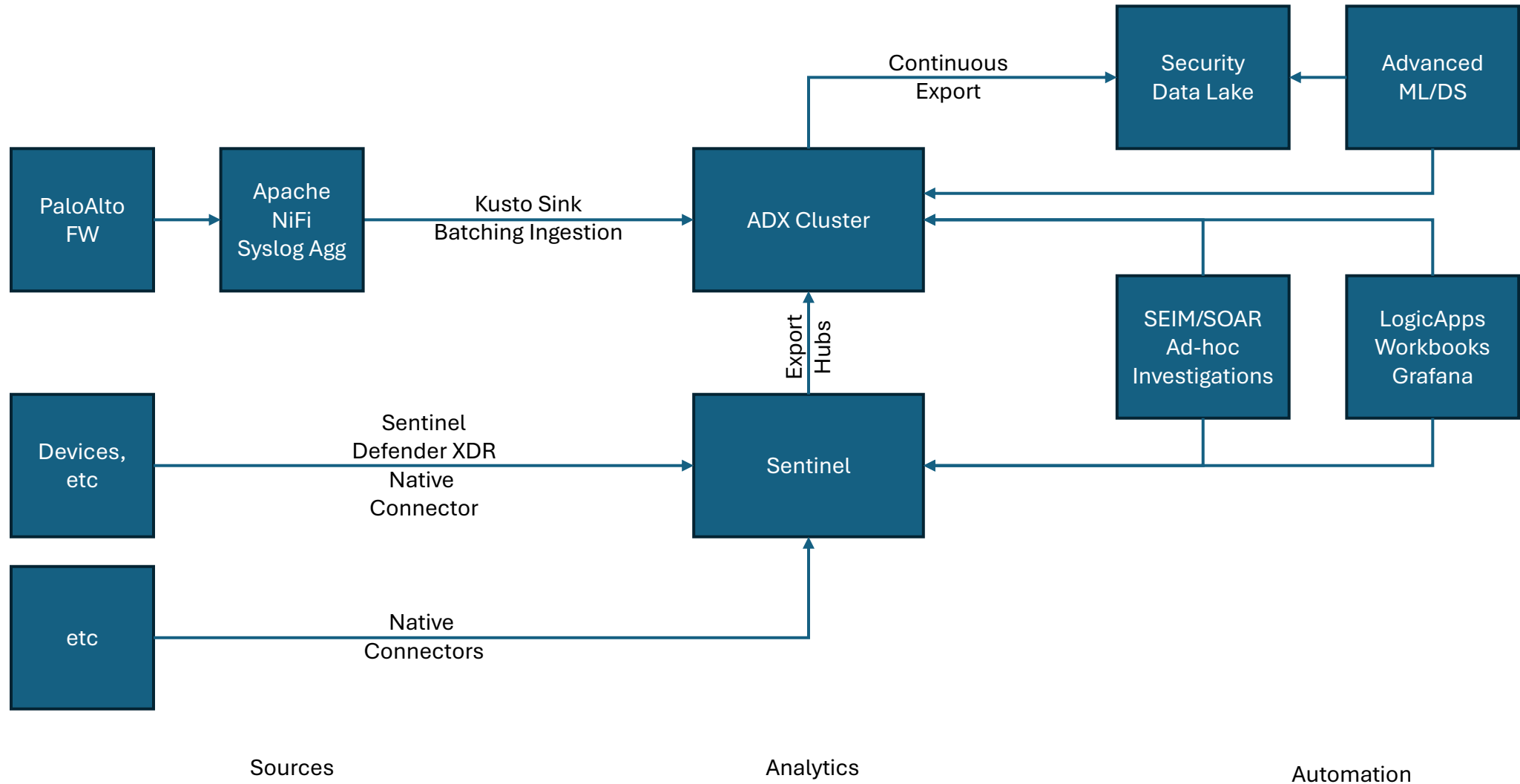
CAF – ILZ Fed Customer

RTI Nomination

Partner: Cloud Fit Software

High-level Architecture Diagram

Cyber Workflow w/ available features in Gov Cloud



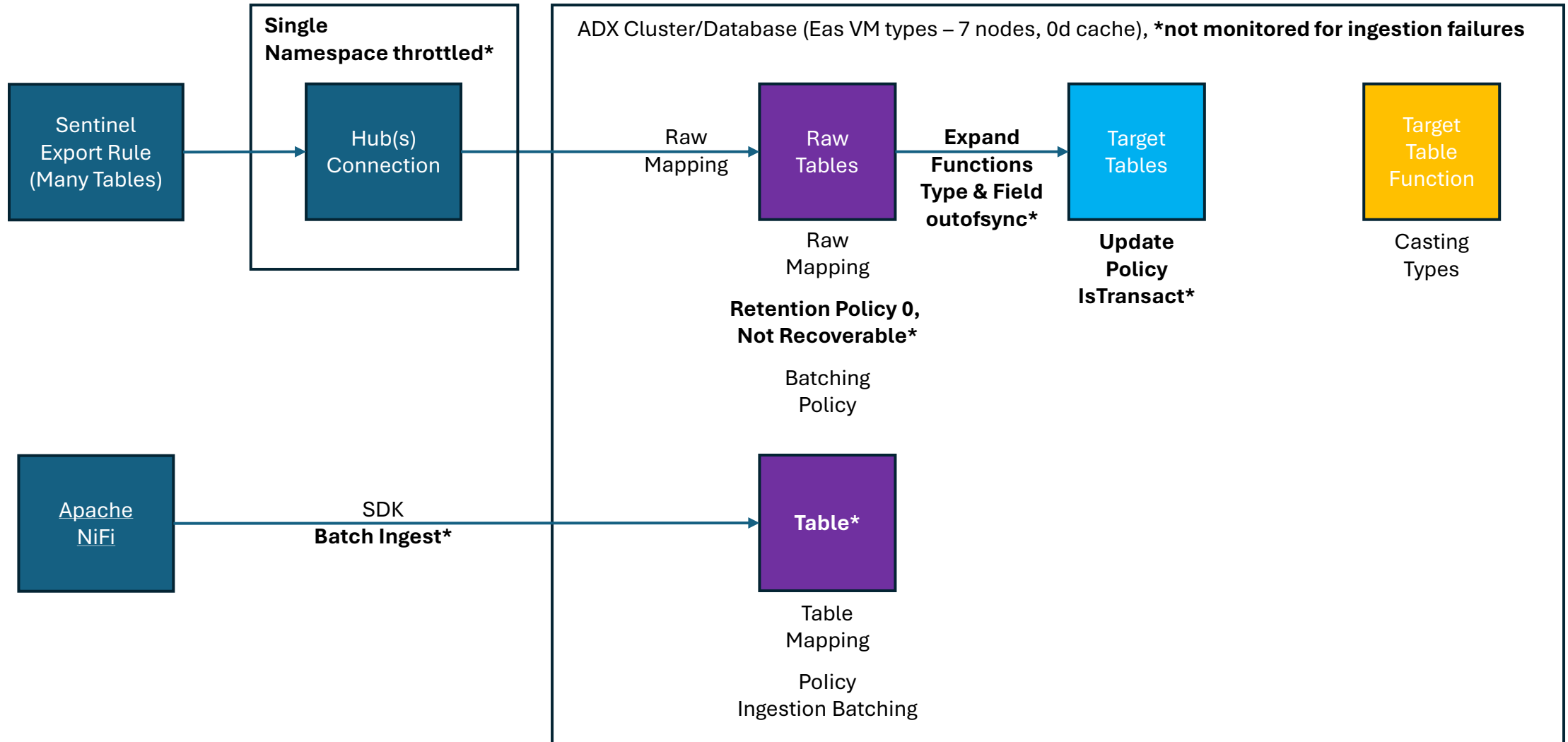
Sentinel + ADX

Considerations

- 10 export rules per LAW workspace (10 tables per rule), 10 hubs per namespace. Reference [Sentinel Tools ADX guide](#).
- Sentinel Export API payloads differs Sentinel table schemas as some columns are internal for Sentinel-only billing.
- Sentinel custom tables are not supported by Continuous Export feature.
- Use premium hubs and **monitor** for throttling.
- Scale by adding partitions, PUs, namespaces and/or hubs.
- Sentinel data not intended to ever be read/queried should be exported to blob storage to lower costs, instead of hubs & ADX.
- Land data raw then use update policy to flatten. If you choose to flatten on ingestion is simpler but use DropMappedFields mapping option to catch full record. Objective is to have ability to revert to the full-record.
- Minimize caching for raw layer. Maximize caching for silver & gold layers. ie. Target tables or materialized-views used for queries/reporting.
- Increase retention policy.
- Use Las vm-sku types if available in your region. Scale by adding nodes.
- Enable diagnostics and Optimized Auto-Scale.
- Monitor ADX using system views, Insights Blade and Azure Advisor.

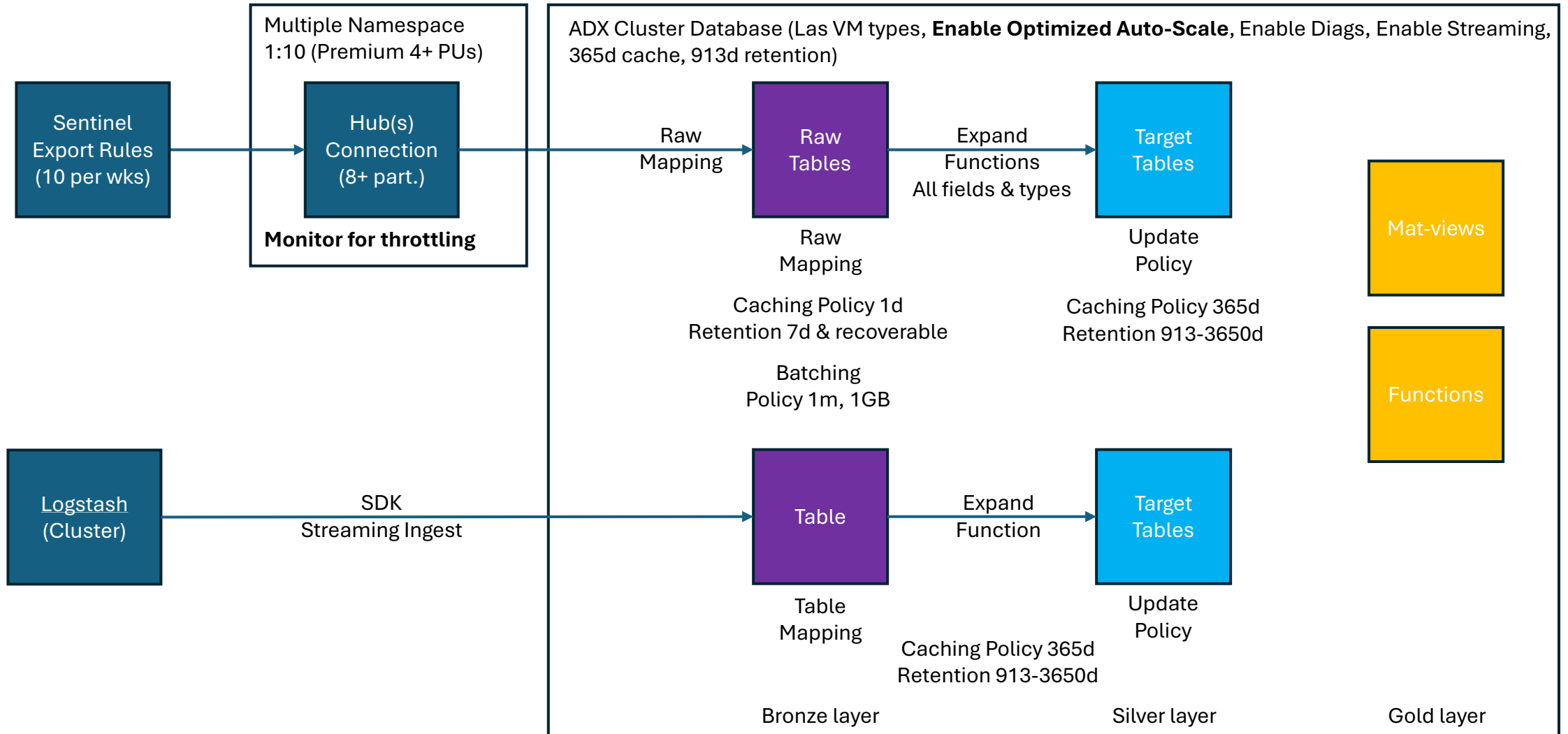
ADX Dataflow (Before)

Cyber Workflow w/ available features in Gov Cloud



ADX Dataflow (After)

Cyber Workflow w/ available features in Gov Cloud



Validations

- Get count for both systems (Sentinel vs ADX) where ingestion_time()>=ago(10m). This should match...very very closely in reference to the particular exported table. ie.

rawtable ... targettable | where ingestion_time() >=(10m) | count

- PS > LAW table 50 cols > get schema > generates expand function dynamically. > generates the target dynamically.
- LAW Export API > outputs payload schema > raw > expect the expand function > flatten all fields to target.
- Raw Payload if 43 > all 43 fields expanded to target. (Get Data UI preview should show them populated for a recent raw json, therefore target should show them populated also)
- Check table(s) retention, cache, update policy is(not)transact, hub partitions, namespace is prem/stand – sku, PUs, etc, check for requests, **throttling**.
- Check adx metric insights blade – no failures and using system view .show ingestion failures | where FailedOn >=ago(10m)
- Scripts located [here](#).