金融業雲端API管理轉型實戰經驗

Kai Lin, Yien Liu / Cathayholdings

國泰金控
Cathay Financial Holdings

Agenda

01 API Application Strategies

API Management Platform Selection and Implementation Strategies

02 API Management System

API Security Challenges and Protection Strategies

03 APIM Architecture Evolution

APIM Architecture Creation and Changes

04 APIM Problem-Solving

APIM Problem-solving

05 APIM Future Enhancement

APIM Future Enhancement

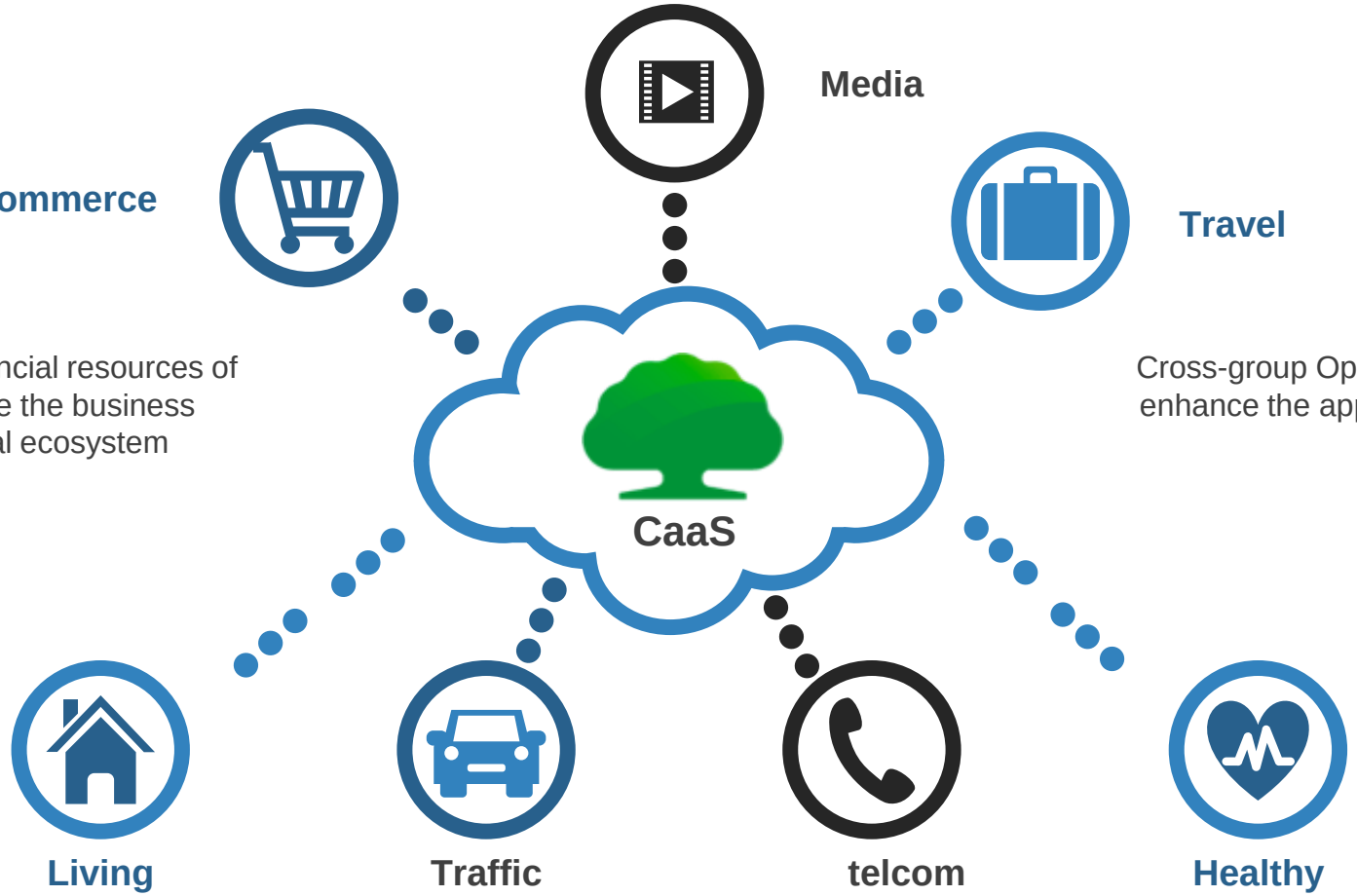
國泰金控
Cathay Financial Holdings

API Application Strategies

CaaS - your best ecosystem partner

國泰金控
Cathay Financial Holdings

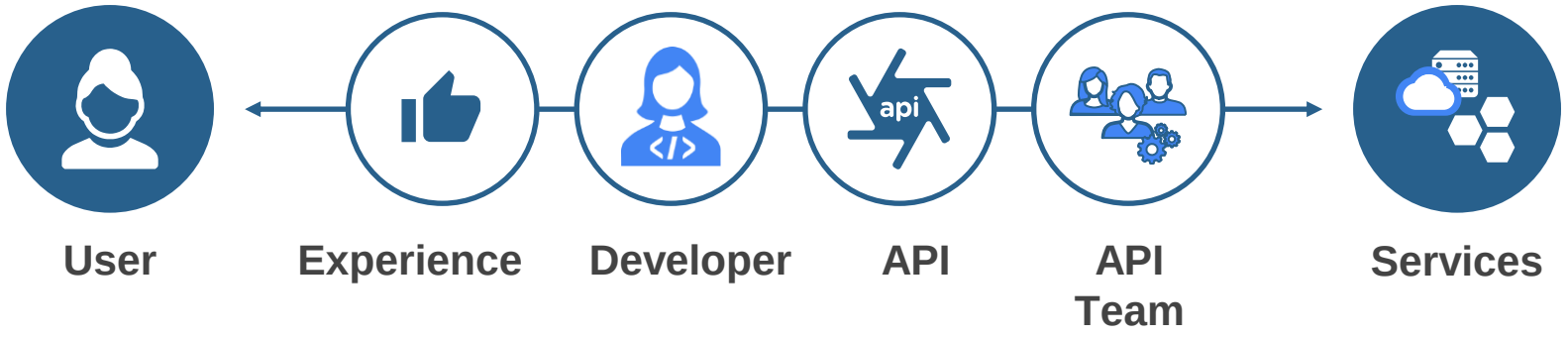
Integrated Platform as a Service



Only by integrating the financial resources of the group is able to promote the business development of the financial ecosystem

Cross-group Open API application is able to enhance the application development of the common financial circle

Security and Governance



Threat Protection

Behavior Based
Signature Based
Payload Complexity
Spikes OWASP (SQL injection, input validation, etc.)

Access Controls

OAuth2 API Keys
Products Scopes
Quota/Spike Arrest
Logging

Self Service & SSO

IAM Integration Prov. & DeComm OpenId Connect JWT SAML

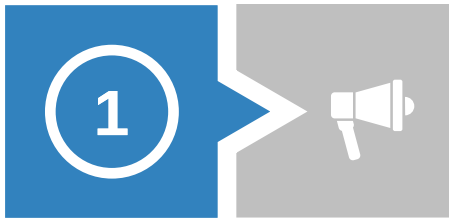
Security Governance

Global Policies RBAC management Data Masking Compliance: ISO, PCI-DSS, HIPAA, SOC1&2

Data Security

TLS Two-way TLS IP Access Control Encrypted Data Store and Cache

Cathay Finance Group APIM Structure



Open Banking

Build the external API management system, and must comply with Open Banking regulations and future development

Integration

- Integrate the business governance process to facilitate the horizontal use of business among subsidiaries
- Integrate API listing registration and version control mechanism
- Integrate the audit and off-shelf process of each subsidiary

Portal

Manage group API information and usage methods, and provide a unified entrance for external access

Monitoring

Monitor internal and external API usage to make expansive and efficient use of resources

Right Solution Fits Our Needs For “Open Banking”

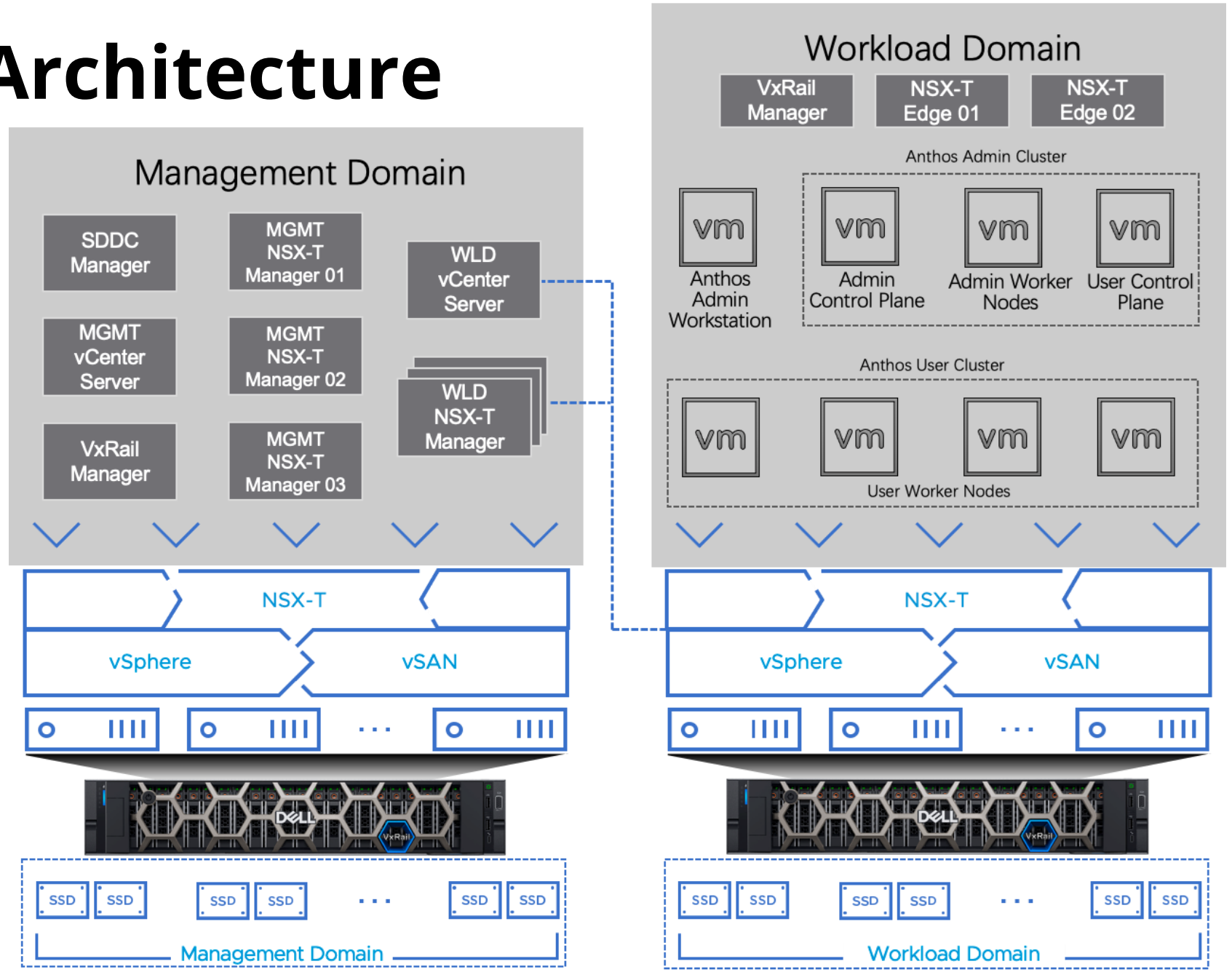
Hybrid

Get the added benefits of a cloud-hosted API platform for managed design, analytics and documentation plus the autonomy to deploy a runtime wherever you’d like.

In compliance with regulatory requirements, seek the best scalable, safe and reliable API service platform

To accommodate hybrid and multi-cloud deployments, API management platforms must support a **biplane architecture** with distinct control plane and data plane elements.

Hybrid Architecture



國泰金控
Cathay Financial Holdings

Photo from vmware

API Management System

Authentication
Authorization

Firewall
(OWASP)

API Secure

API Security Challenges and Protection Strategies

End to End Security

Traffic Management

Content-based Security

Extension

Securing a proxy

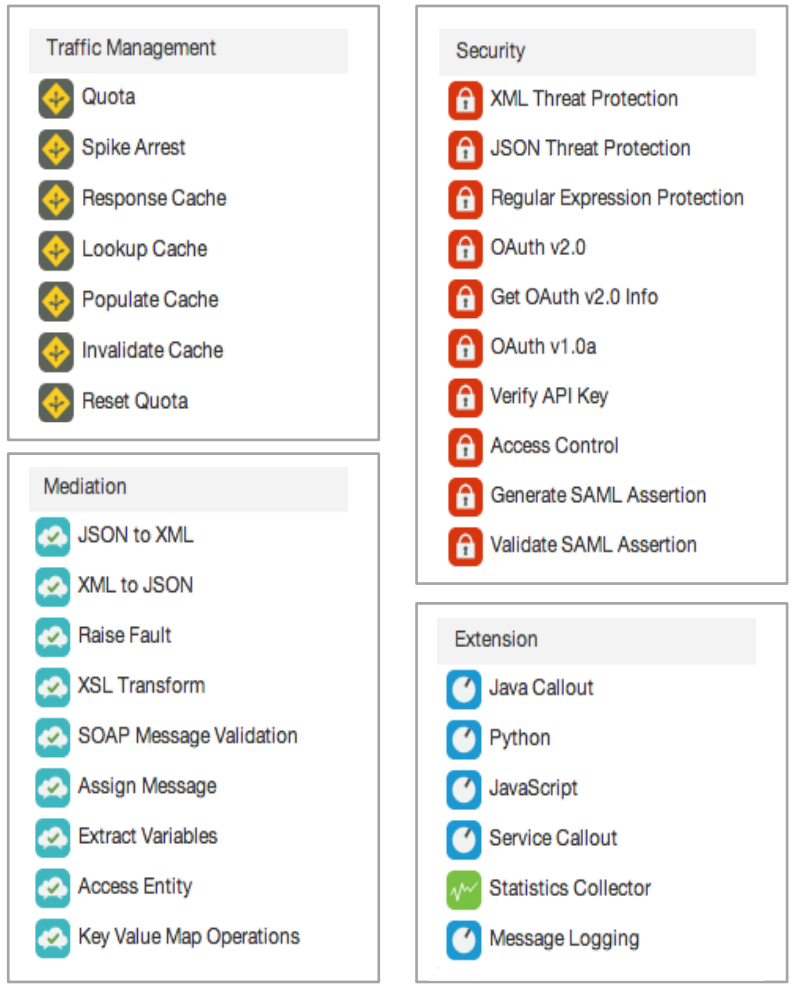
API security protects your backend services against direct access, guards against malicious message content, accesses and masks sensitive encrypted data at runtime,

國泰金控
Cathay Financial Holdings

Configurable API Policies

Manage interactions with API consumers and optimize performance

Transform, translate and reformat data for easy consumption



Secure APIs and protect back-end systems from attack

Extend with programming when you need it

APIM Architecture Evolution

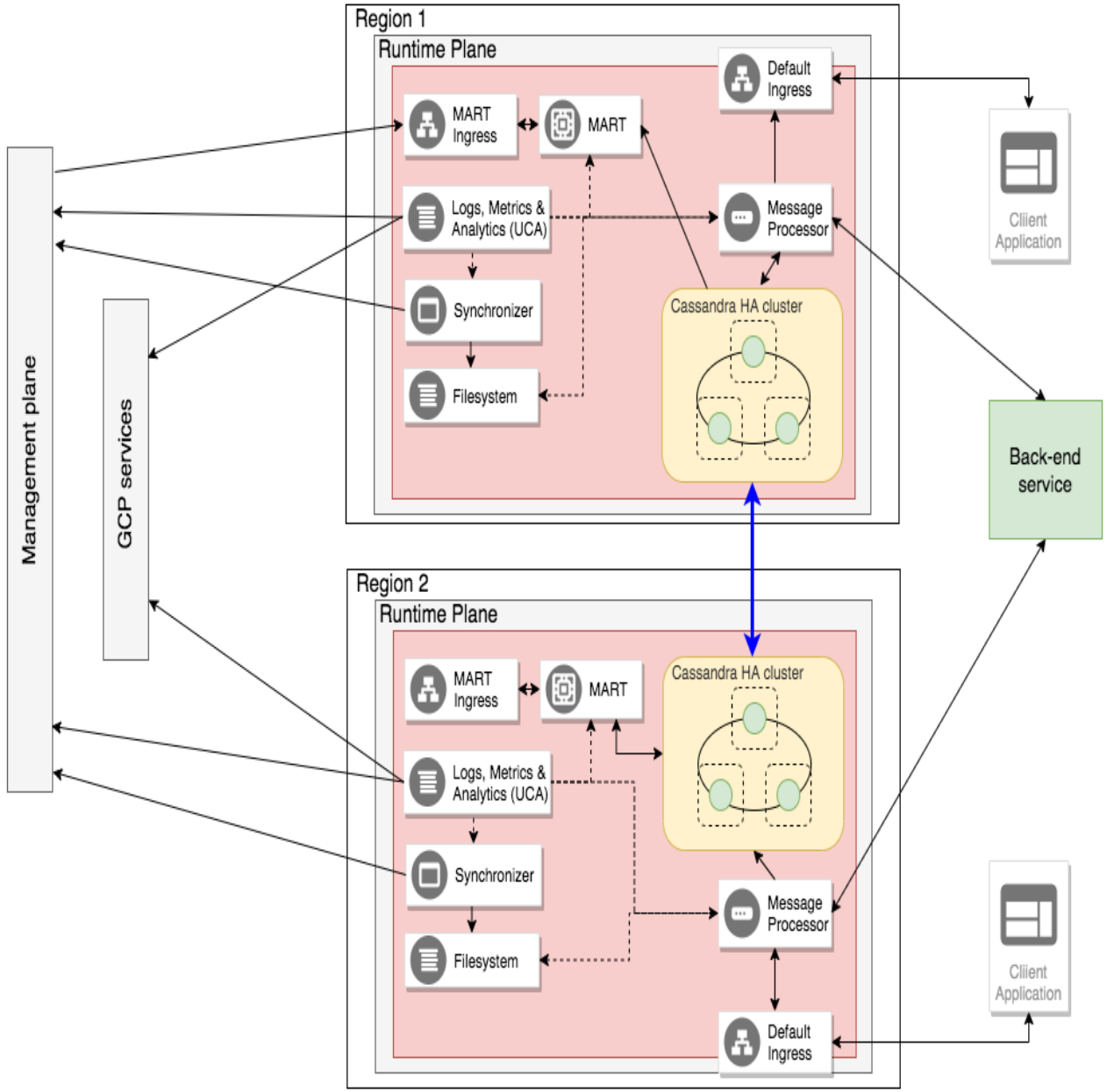
Scalability and Reliability for API Management

國泰金控
Cathay Financial Holdings

Stable Services By Highly Available

Expand organization across multiple regions

- High availability: increasing the overall availability of your APIs.
- High capacity: increasing the overall capacity of your APIs.
- Low latency: Additional regions can lower the overall transaction latency for clients by serving their requests in a geographically closer region.



國泰金控
Cathay Financial Holdings

APIM Problem Solving

Learning from Failure

Incidents and outages are inevitable given our scale and velocity of change. When an incident occurs, we fix the underlying issue, and services return to their normal operating conditions.

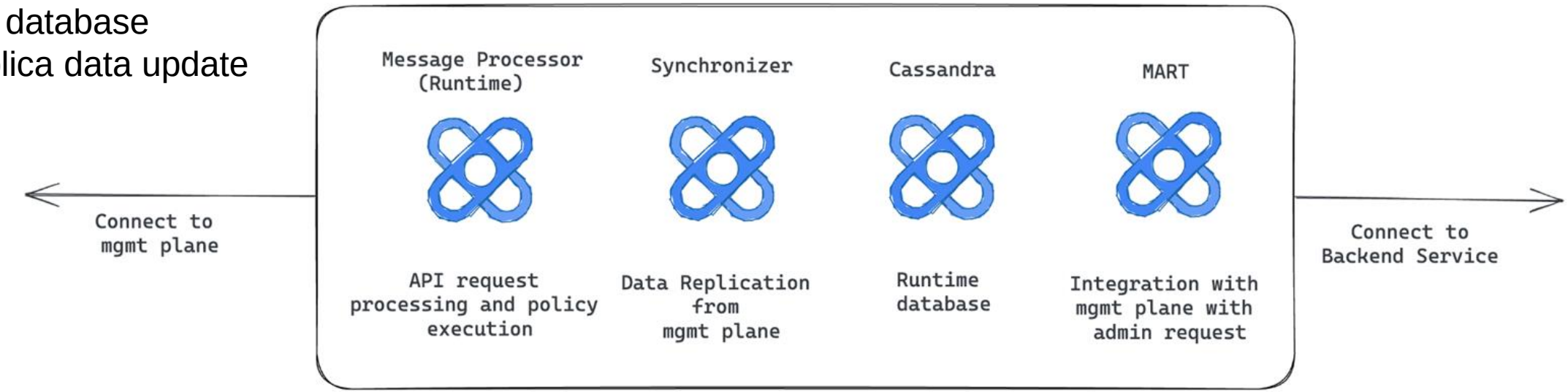
by SRE Postmortem Culture

國泰金控
Cathay Financial Holdings

Unsynchronized Status

Uncoordinated

- Can’t request the MART component for configuration changes.
- Fail r/w database
- No Replica data update



The Influence of **TLS Certificates**

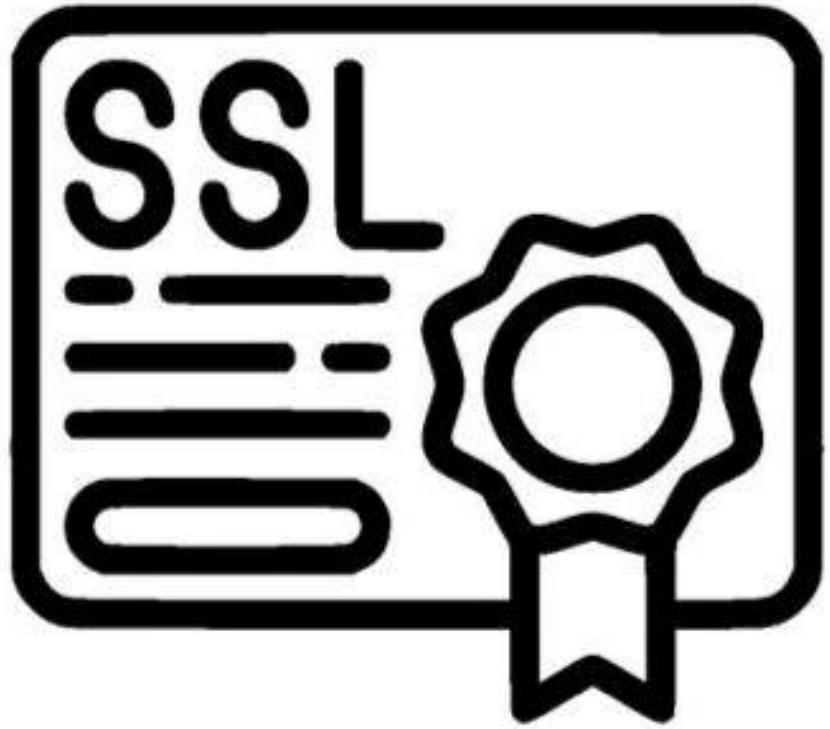
Certificate increases security and also increases maintenance cost

ssl/tls certificate expired, and broke the communication between components

Certificate handshake failure, because replaced certificate by egress proxy

Ingress gateway supports TLS1.2 only.

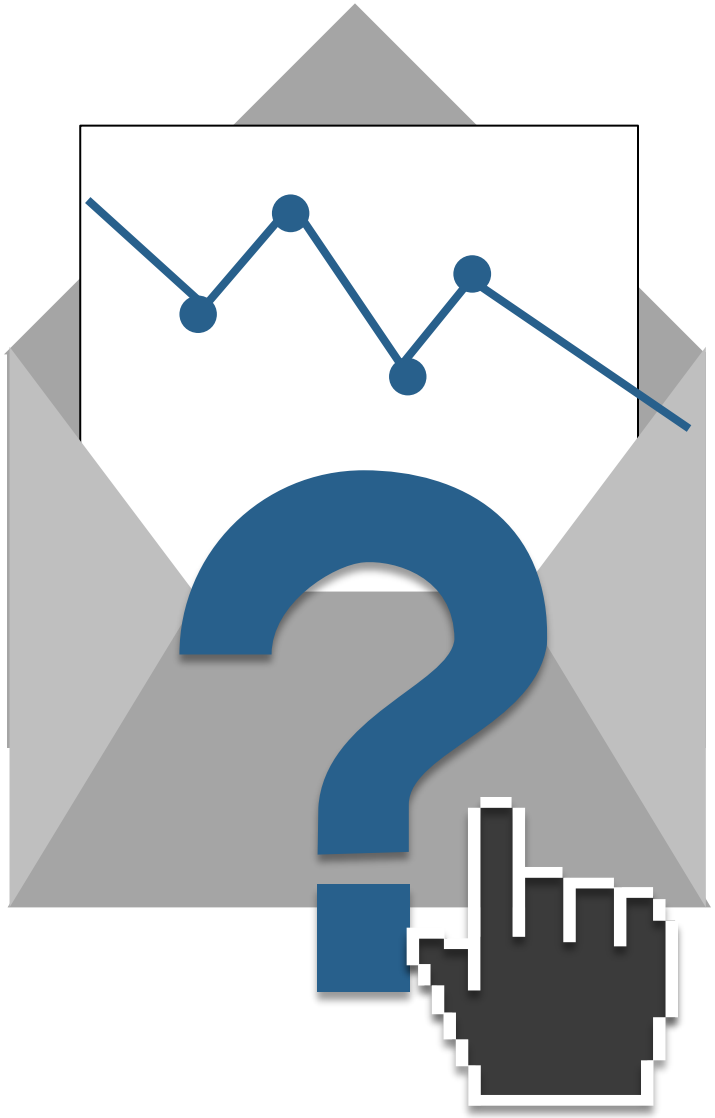
Egress gateway verify certificate failed from IPs.



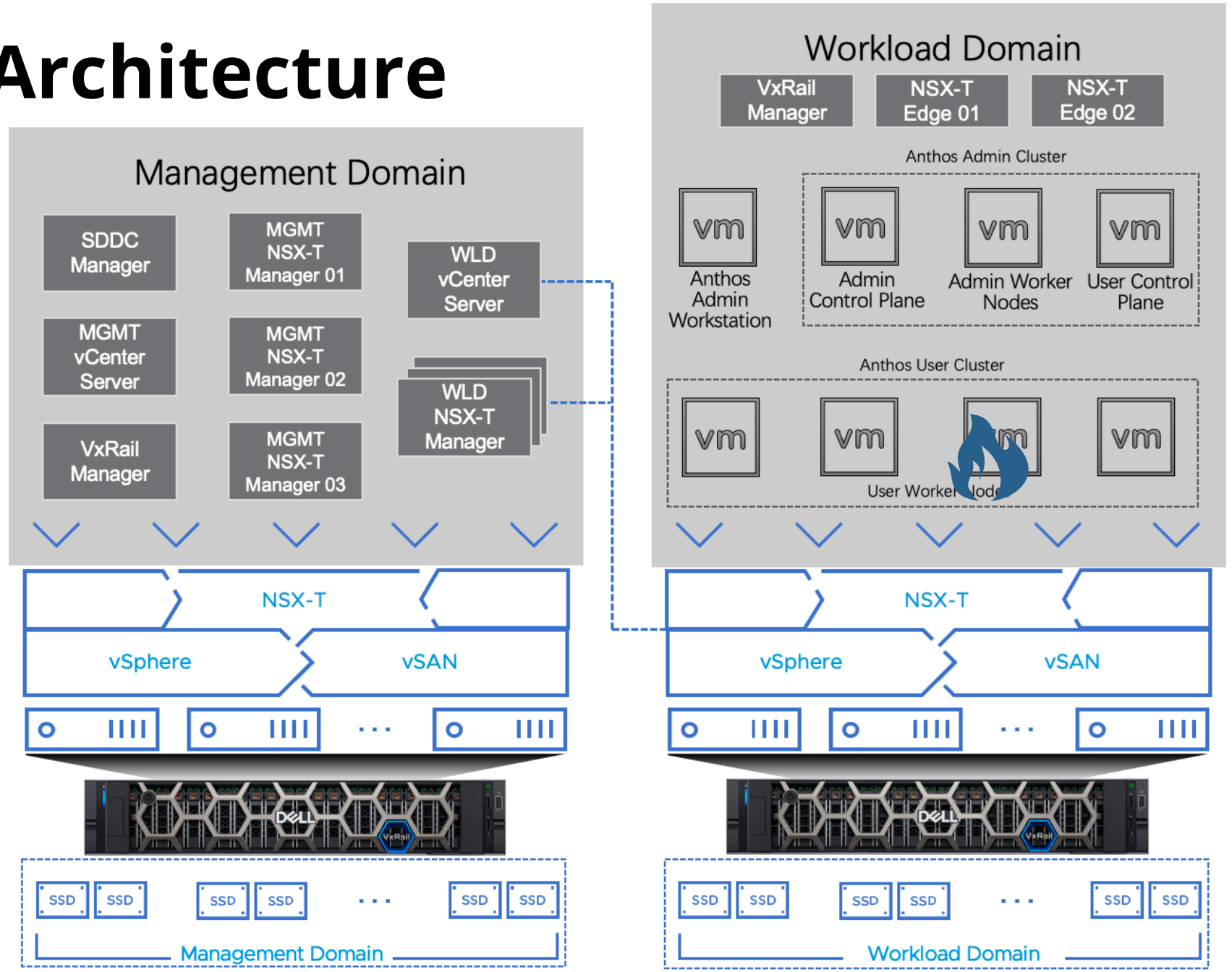
Resource Management

The Unexpected Resource Status

1. **Zombie Pods**
   An unhealthy pod ain’t able to drop out automatically
2. **Resource Capacity**
   Unexpected resource usage exhausts the capacity causing further issues.
3. **Unhealthy Auto-Scaling**
   Unexpected pod autoscaling occurred



Hybrid Architecture



國泰金控
Cathay Financial Holdings

Photo from vmware

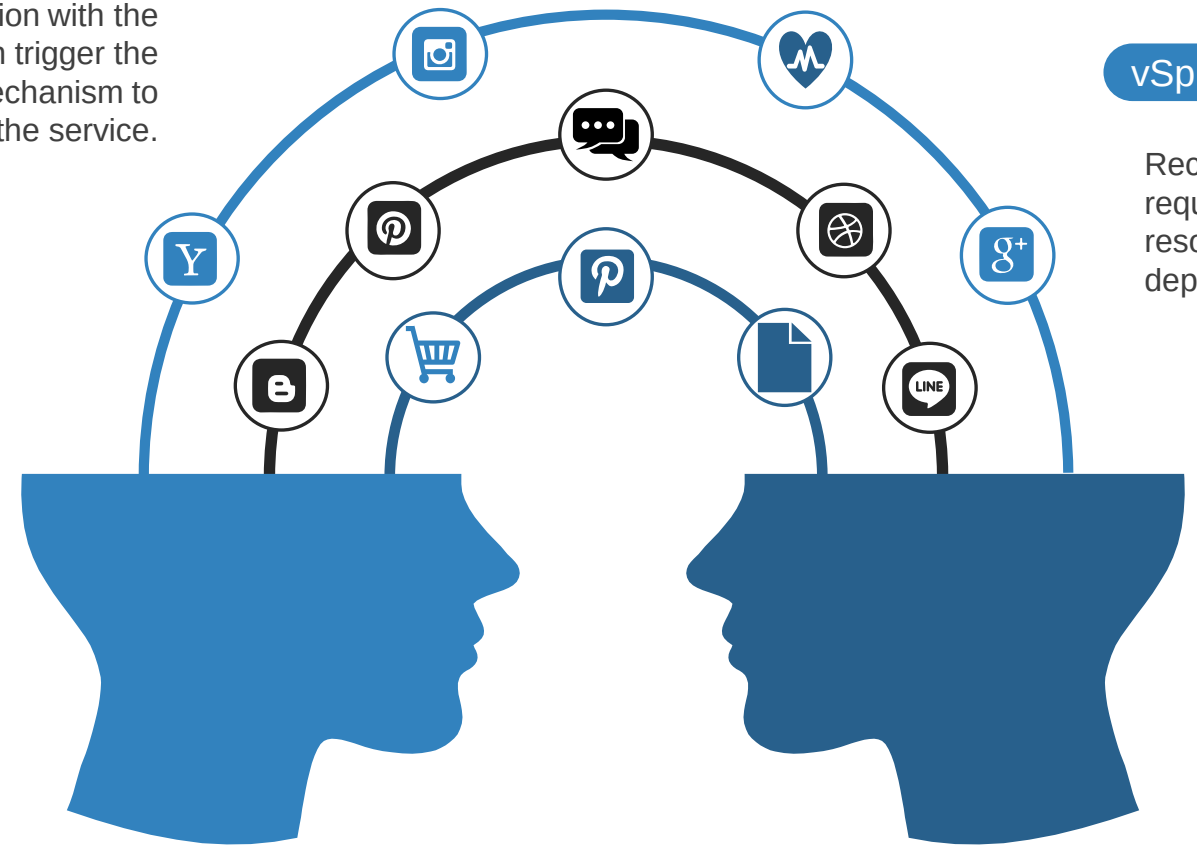
Competition for Resources

Anthos admin node

After losing connection with the worker node, then trigger the auto-repair mechanism to rescue the service.

Anthos worker node

Losing the volume, the node can’t create successfully



vSphere environment

Receive the Anthos' requirement to provide the resource til the own space was depleted

APIM Future Enhancement

Increase reliability for our service, and seek for ha availability architecture

Implement a strategy to ensure availability during an outage or disaster affecting an APIM

Communicate and keep rolling with the latest stable version to avoid service corruption

To seek a highly stable architecture without any infrastructure issues, plan to migrate to APIM SaaS

國泰金控
Cathay Financial Holdings

國泰金控 | 60 ANNIVERSARY

國泰徵才中 SRE科技人才最佳舞台

[Join Us]

掃我看更多 國泰精選職缺

【金控】

〈雲端SRE工程師〉

雲端架構整合、配置管理與維運。實現可觀察性監控、警報和指標報告。提供可靠的大規模部署技術服務。

Thank You

國泰金控
Cathay Financial Holdings