Experience with confidential computing

Discussions with end consumers across Asia Pacific

Dr Chris Butler

Red Hat

What has been driving these discussions?

- I am in the ‘Field CTO’ office for APAC focusing on platform layer conversations
- Most of the focus of the discussions have been on public sector.
- Telecommunications providers and banking as regulated industries.
- The conversations progress when their are strong constraints in what can be done today.
- Confidential containers has anchored conversations for commercial availability reasons.

Drivers of customer conversations

Size weight and power

Size weight and power is constraining designs, particularly at the edge.

End of life assets

Historical acquisitions using legacy or EoL technology is driving the desire for more standardized approaches

Capital constraints

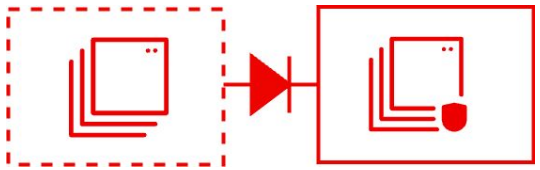
Recreating functionality in ‘secure’ regions is increasingly unaffordable.

Avoiding compliance

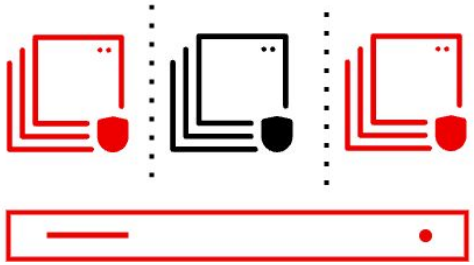
Service providers using confidential computing to push compliance obligations onto tenants

Use cases

Multi-level security



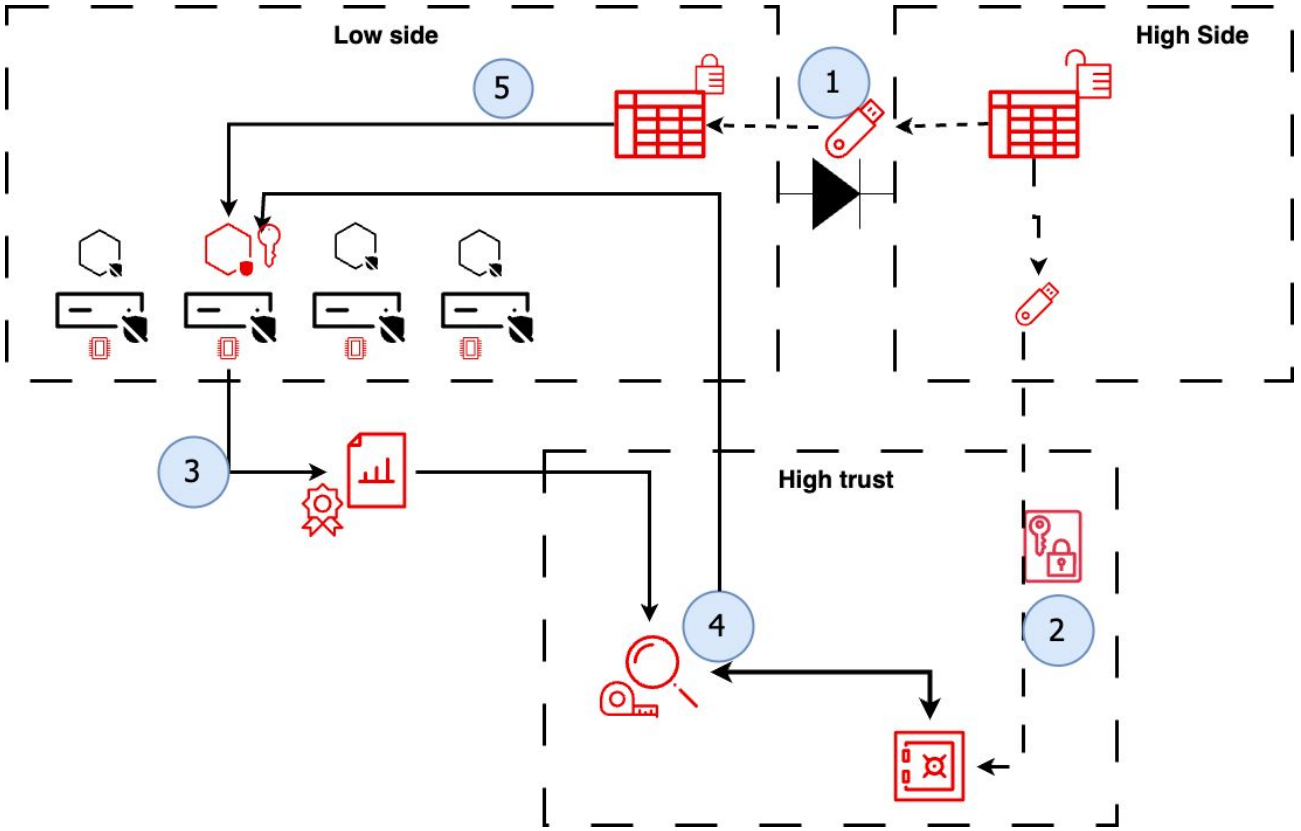
Compartmented data



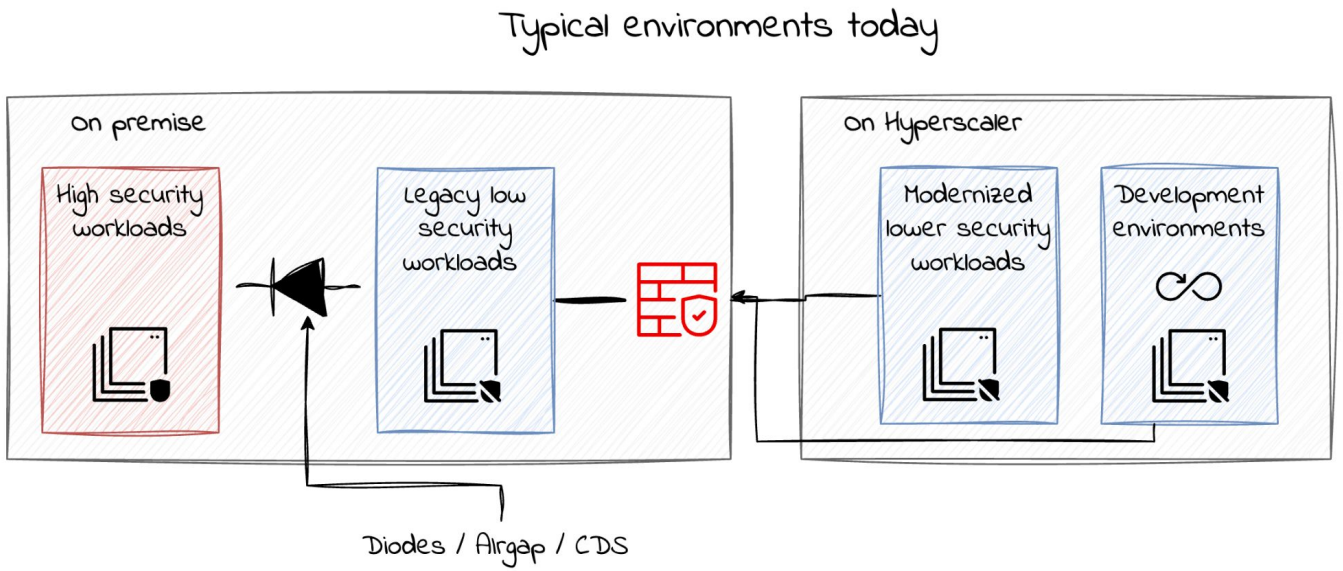
Physical asset compromise

High value asset compromise

Confidential computing to allow ‘multi-level security’ use of systems

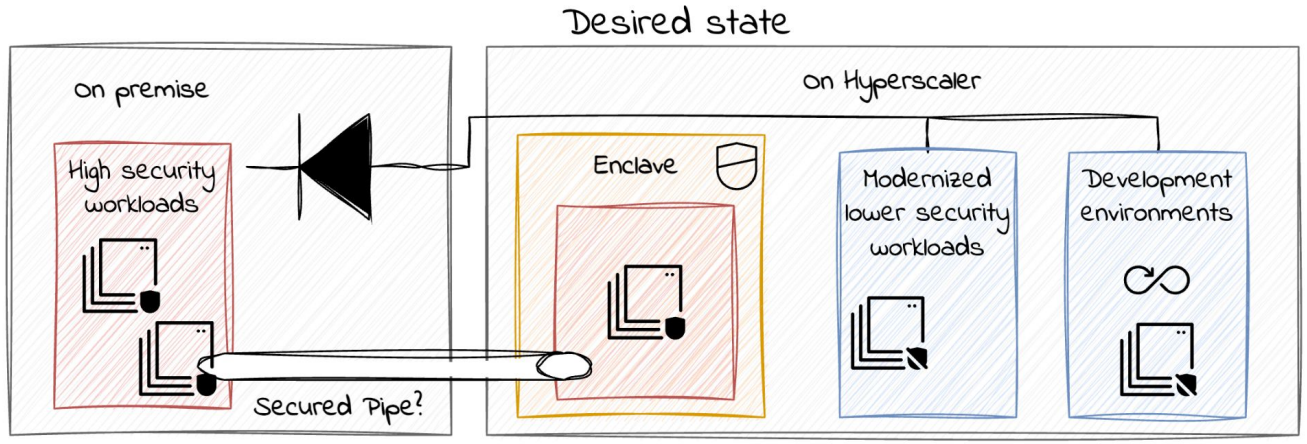


- Size Weight & Power is constraining the number of GPUs available in ‘secure’ zones
  - This translates to on-premise for enterprises
- System administrators are not trusted to handle data in the clear



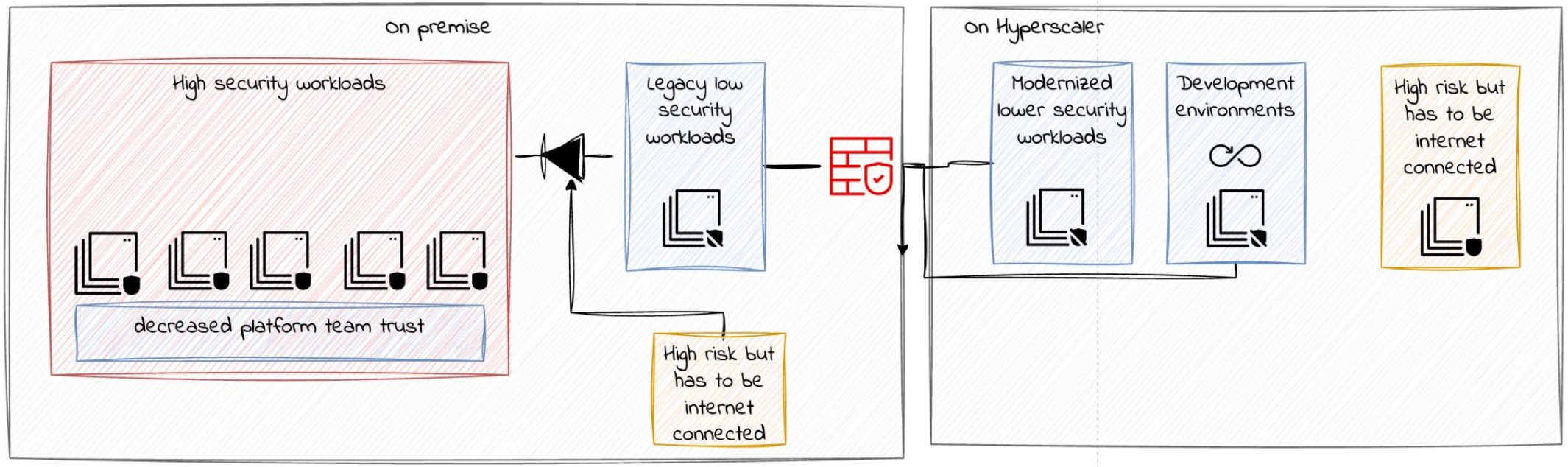
- Regulatory constraints restrict movement of data to the cloud

- The ability to extend their secure network into the cloud is desired



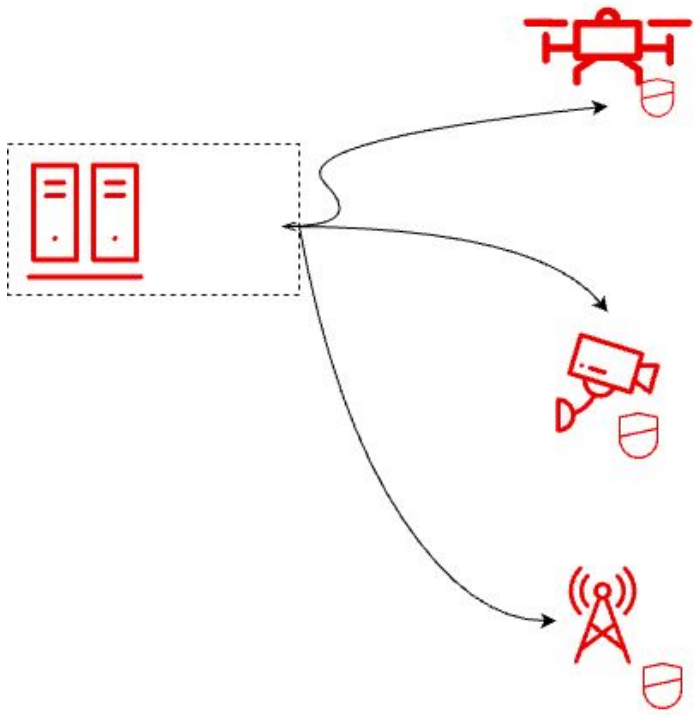
- Challenge occurs in how to operate in a way where the cloud network fabric is untrusted.

Red Hat



- Generally what is on the cloud providers today is viewed as being okay
- Internet connected workloads with significant IP / security impact are also a use-case
  - Challenging as often teams running these workloads are risk adverse
- Higher value use case is increasing common platform use on premise and/or decreasing platform team trust in organizations with compartmented workloads

Red Hat



- Edge devices are pushed into the field with limited compute and storage
- Communications back to the core may be limited intermittent.
- Challenge is continuity of operations which may limited remote attestation platform
- Fear of compromise of:
  - Software IP on the platform
  - Data on the platform
  - Communications channel compromise via endpoint compromise

Client deployment example

Red Hat

Red Hat Banking Client

- Large bank in south east Asia
- Large on premise deployments of Kubernetes within virtual machines in
- Significant regulatory pressure due to public failures of core banking system including retail functionality
- *Mix of on premise and hyperscaler deployments*

Crypto software solution provider

- Leading global cryptocurrency firm
- Acquired MetaCo a cryptocurrency custody platform
- Cryptocurrency custody platform is used by leading banks globally including HSBC; Citi; BNP Paribas among others.

Today the bank's Crypto cryptocurrency custody platform holds > $100M and is dependent on unsupported bespoke security appliances

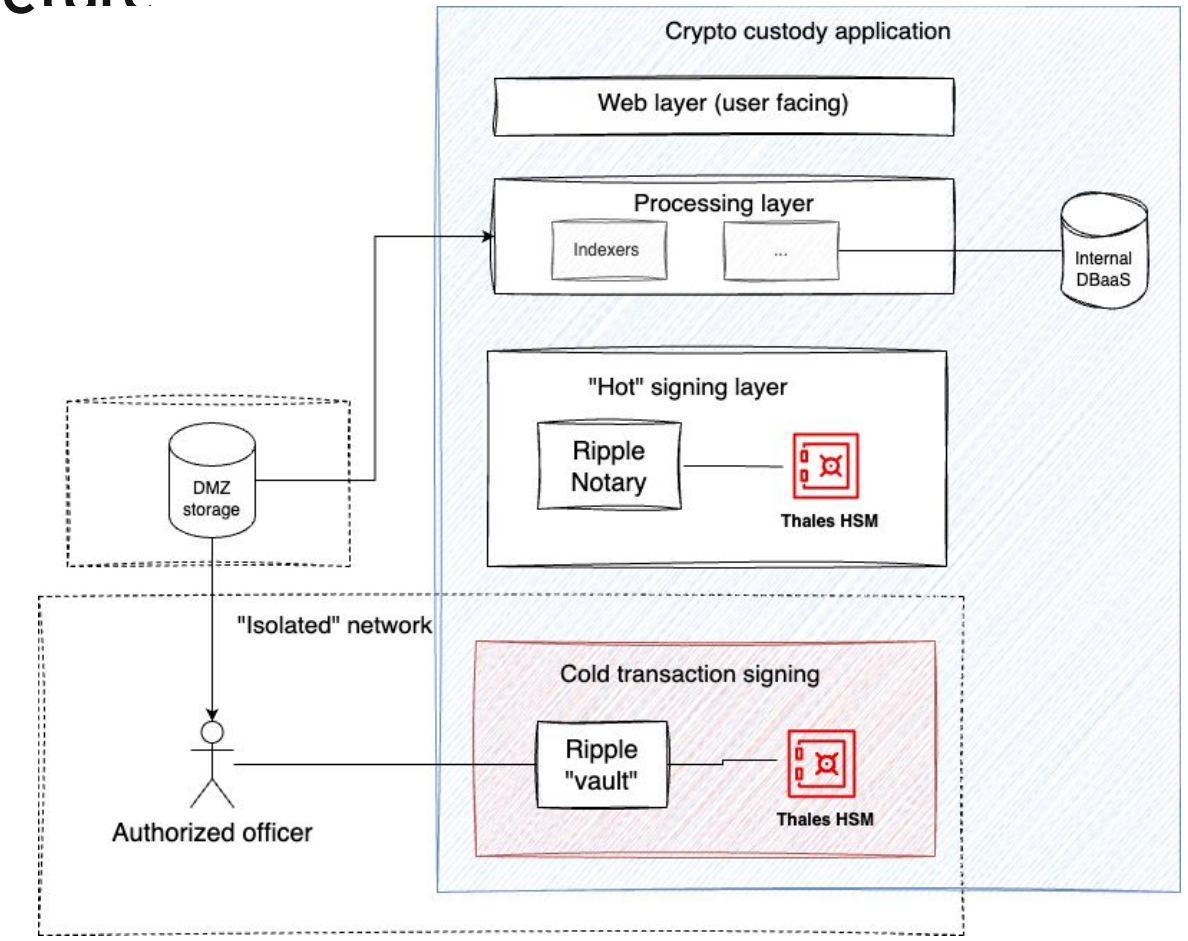
Ripple requires confidentiality of transaction processing infrastructure

Requirements Overview

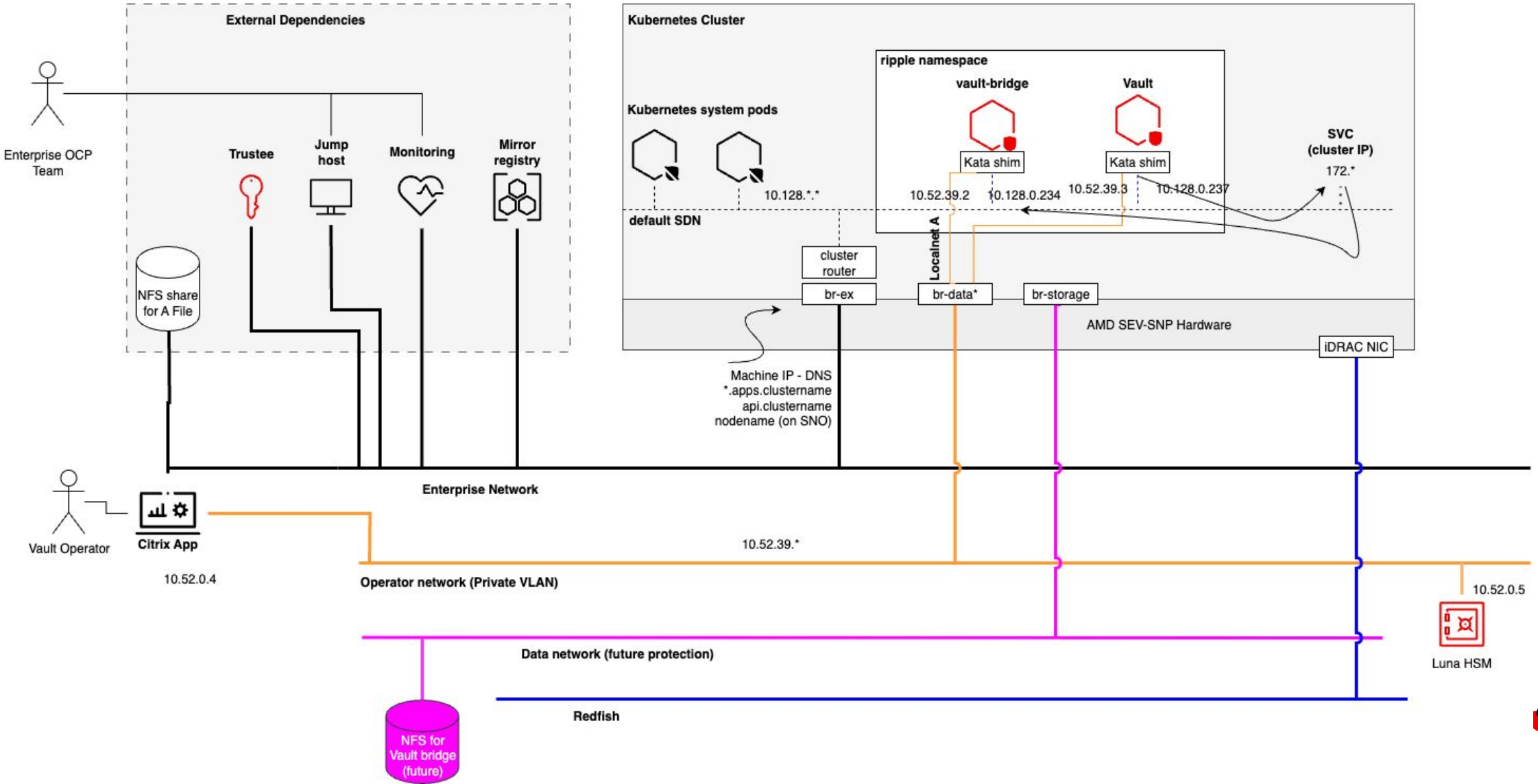
- Hardware Security Module (HSMs) are actually signing - protect the HSM
- Use confidential computing to protect against attacks which may manipulate memory
- Network segmentation requirements to isolate traffic for cold-vault signing and HSM access

Quality Goals

- Improve security and maintainability (no bespoke hardware platforms; enterprise standard monitoring)
- Decrease application team's burden (e.g. leverage enterprise infrastructure & platform teams)

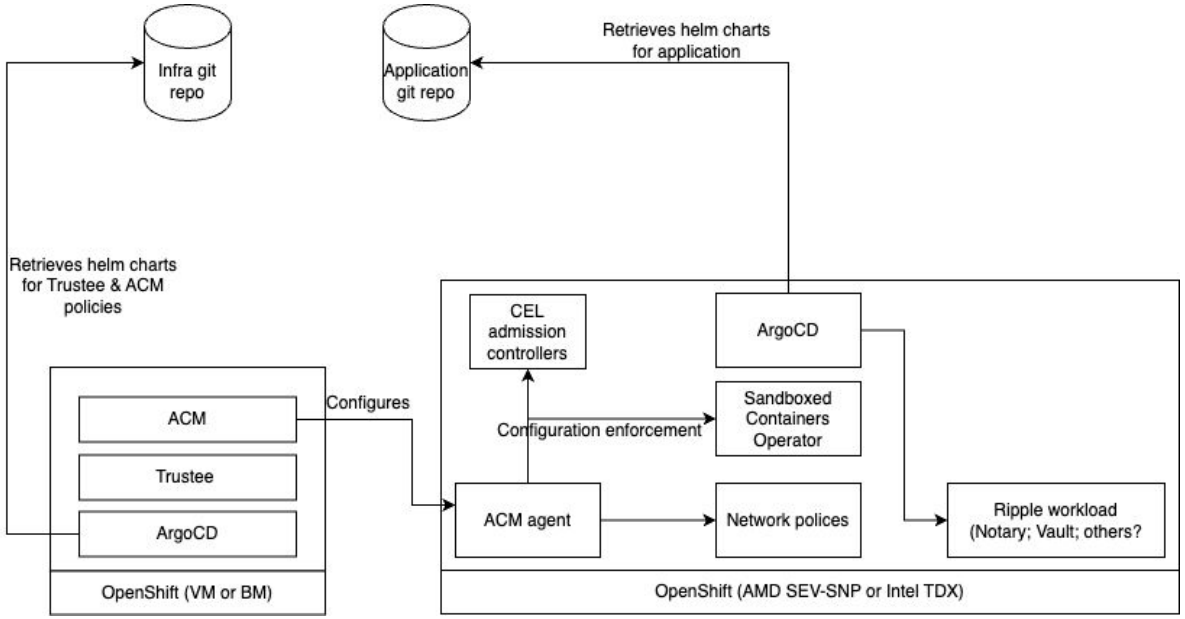


Resulting cluster architecture with 6 clusters deployed



Challenges & Opportunities

- Single largest challenge was explaining the value of remote attestation to all the parties. Encrypting memory in contrast was well understood.
- End to end deployment requires consistency across Trustee & CoCo including support for enterprise environments (air gaps / proxies) which is lagging upstream.
- Lack of supporting secure abstractions 'in-TEE' for both storage and networking
- Patterns for offline / cascading / multi-party attestation need to be refined to support complex use cases and high availability.



- Internally focusing on 'validated patterns' first for demonstrating then co-developing with partners https://github.com/validatedpatterns/coco-pattern

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


x.com/RedHat

Red Hat