YOTTA

cloud STACK COLLABORATION CONFERENCE

Cloud Compliance and Security

Kaushik Bora
Principal Solution Architect
Yotta

Topics to Cover in this Session

A brief discussion on Cloud Compliance and Security Requirement

A few real-life challenges

Apiculus@Yotta along with CloudStack help mitigating the Challenges

Cloud Compliances

Key aspects of Cloud Compliance

Industry Regulations and Standards

Different industries have specific compliance frameworks, including:

GDPR (General Data Protection Regulation)

European Union regulation for data protection and privacy.

MEITY (Ministry of Electronics & Information Technology in India)

MEITY defines **The National cyber security policy** which should be implemented in all Public/Private Cloud deployments for the Central and State Govt. in India.

HIPAA (Health Insurance Portability and Accountability Act)

US regulation for healthcare data protection.

NCA

The Saudi Arabia National Cybersecurity Authority (NCA) develops policies to protect the Kingdom's critical information infrastructure, enhance the nation's cybersecurity capabilities, and promote a secure digital environment for government.

Key aspects of Cloud Compliance

Industry Regulations and Standards

Different industries have specific compliance frameworks, including:

PCI DSS (Payment Card Industry Data Security Standard)

A global standard for securing payment card information.

SOC 2 and SOC 3

Frameworks used for assessing the controls related to security, availability, processing integrity, confidentiality, and privacy in the cloud.

ISO 27001

International standard for information security management.

Key aspects of Cloud Compliance

Data Residency

Cloud customers must ensure that their data is stored in regions that meet regulatory requirements. Some laws require data to stay within certain geographic borders

Audit and Reporting

Cloud providers often offer tools to assist with compliance audits. Businesses must implement tracking and reporting mechanisms to demonstrate compliance to regulatory bodies.

Continuous Compliance

Compliance is not a one-time effort; it requires ongoing assessments and adjustments. Cloud environments change frequently, so businesses must continuously monitor and adjust their security controls to remain compliant.

Cloud Security

Key aspects of Cloud Security

Data Protection

Encryption: Ensures data is protected both at rest (when stored) and in transit (when moving between servers).

Access Controls: Strong authentication mechanisms (e.g., Multi-Factor Authentication - MFA) and strict access control policies to ensure only authorized users can access cloud resources.

Identity and Access Management (IAM)

IAM tools allow businesses to define and enforce who can access cloud resources and what actions they can perform. Role-based access control (RBAC) is commonly used to limit privileges based on user roles.

YOTTA

Key aspects of Cloud Security

Network Security

Protecting cloud infrastructure from external and internal network threats. Techniques include firewalls, VPNs (Virtual Private Networks), and segmentation of the network into separate security zones.

Security Monitoring and Incident Response

Continuous monitoring of cloud environments to detect potential threats or anomalies. This includes intrusion detection, logging, and security event management.

Incident response plans ensure that businesses can quickly respond to breaches or security incidents.

Key aspects of Cloud Security

Threat Detection and Vulnerability Management

Regular scanning and vulnerability assessments help identify and mitigate risks in cloud infrastructure. Automated tools help ensure up-to-date security patches and fixes.

Data Availability and Disaster Recovery

Ensuring business continuity through redundancy, backup solutions, and disaster recovery plans. Cloud providers often offer Service Level Agreements (SLAs) to guarantee uptime and availability.

A Few Real Life Challenges

Security Controls and Encryption

Identity and Access Management (IAM)

CloudStack’s IAM is relatively basic compared to AWS IAM or Azure AD, offering fewer controls for user management, role-based access control (RBAC), and multi-factor authentication (MFA) natively.

Data Encryption

Although CloudStack supports data encryption, it lacks fine-grained encryption options across all hypervisors and does not provide key management solutions.

Network Security

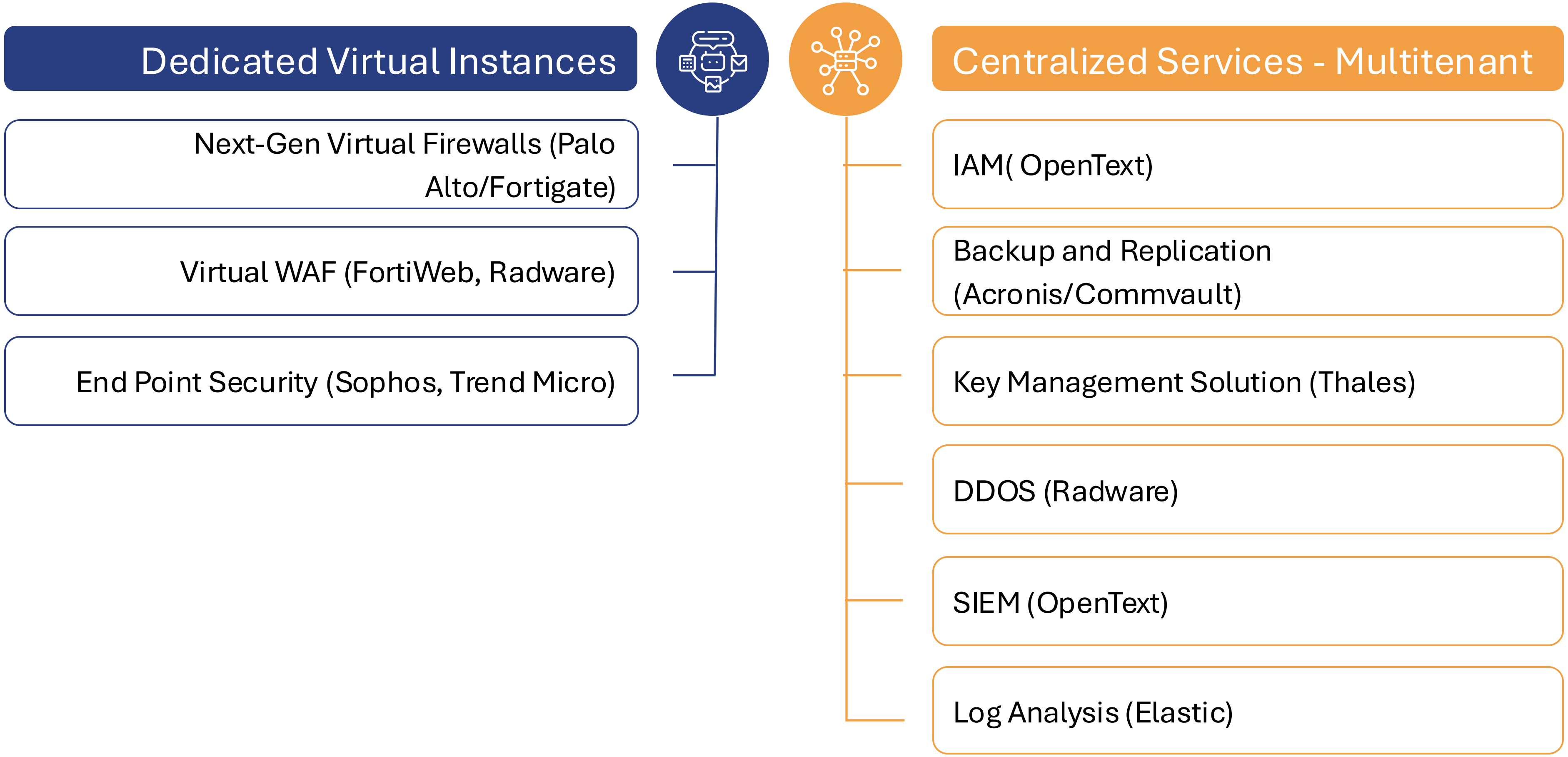
While CloudStack has now come up with VNF support, this seems to be still in initial stages and limit its security framework when dealing with complex network requirements.

Audit and Logging

CloudStack has some auditing capabilities, however; this is limited to the management side and lacks the comprehensive logging from the user traffic/data perspective.

Mitigating the Challenges

Building Integrations with Multiple Security Solutions



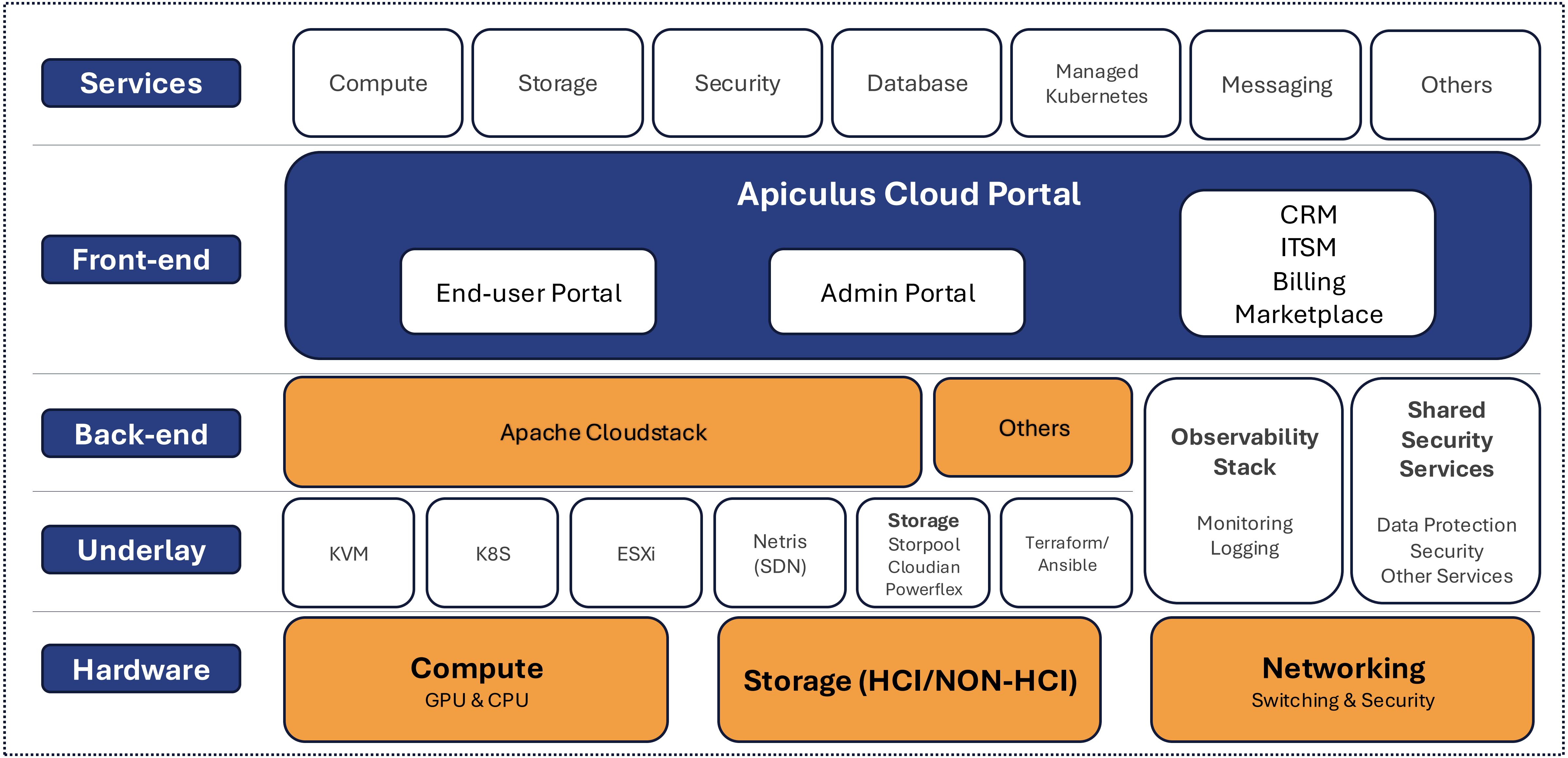
Dedicated Virtual Instances

- Next-Gen Virtual Firewalls (Palo Alto/Fortigate)
- Virtual WAF (FortiWeb, Radware)
- End Point Security (Sophos, Trend Micro)

Centralized Services - Multitenant

- IAM(OpenText)
- Backup and Replication (Acronis/Commvault)
- Key Management Solution (Thales)
- DDOS (Radware)
- SIEM (OpenText)
- Log Analysis (Elastic)

A High-Level View of the Apiculus Architecture



Services

Compute

Storage

Security

Database

Managed Kubernetes

Messaging

Others

Front-end

Apiculus Cloud Portal

End-user Portal

Admin Portal

CRM
ITSM
Billing
Marketplace

Back-end

Apache Cloudstack

Others

Observability Stack

Monitoring
Logging

Shared Security Services

Data Protection
Security
Other Services

Underlay

KVM

K8S

ESXi

Netris (SDN)

Storage
Storpool
Cloudian
Powerflex

Terraform/ Ansible

Hardware

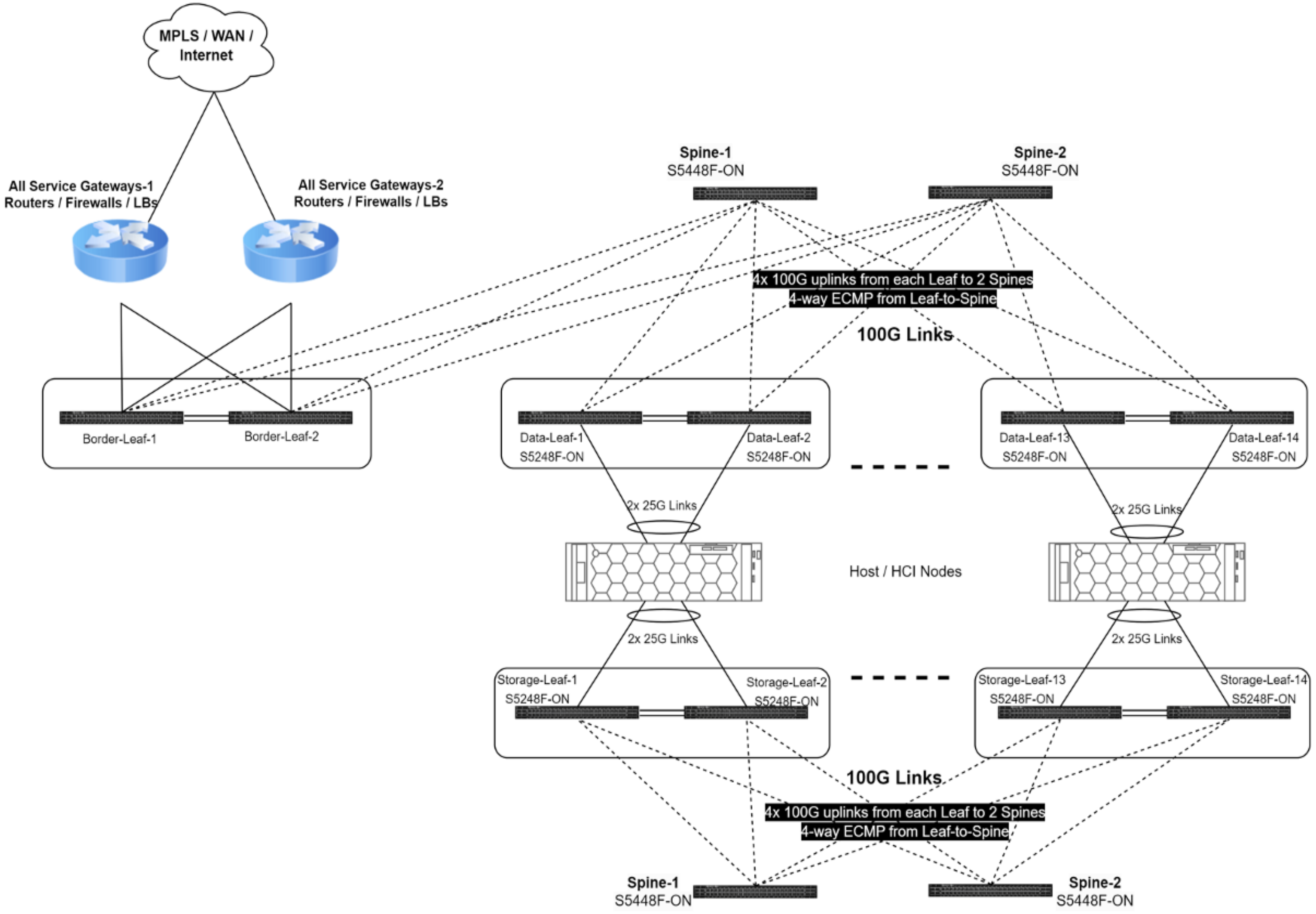
Compute
GPU & CPU

Storage (HCI/NON-HCI)

Networking
Switching & Security

YOTTA

Leaf-Spine Vxlan-EVPN based Architecture



Leaf Switch Pair (Data / Storage)

- MLAG / EVPN Multihoming without Interconnect Links
- Anycast IP / VRRP for Server / Host gateway
- VXLAN VTEP Discovery using BGP EVPN
- DHCP Relay & Server Traffic protection using Storm Control & BPDU Guard Features

Leaf – Spine Connectivity on 100G

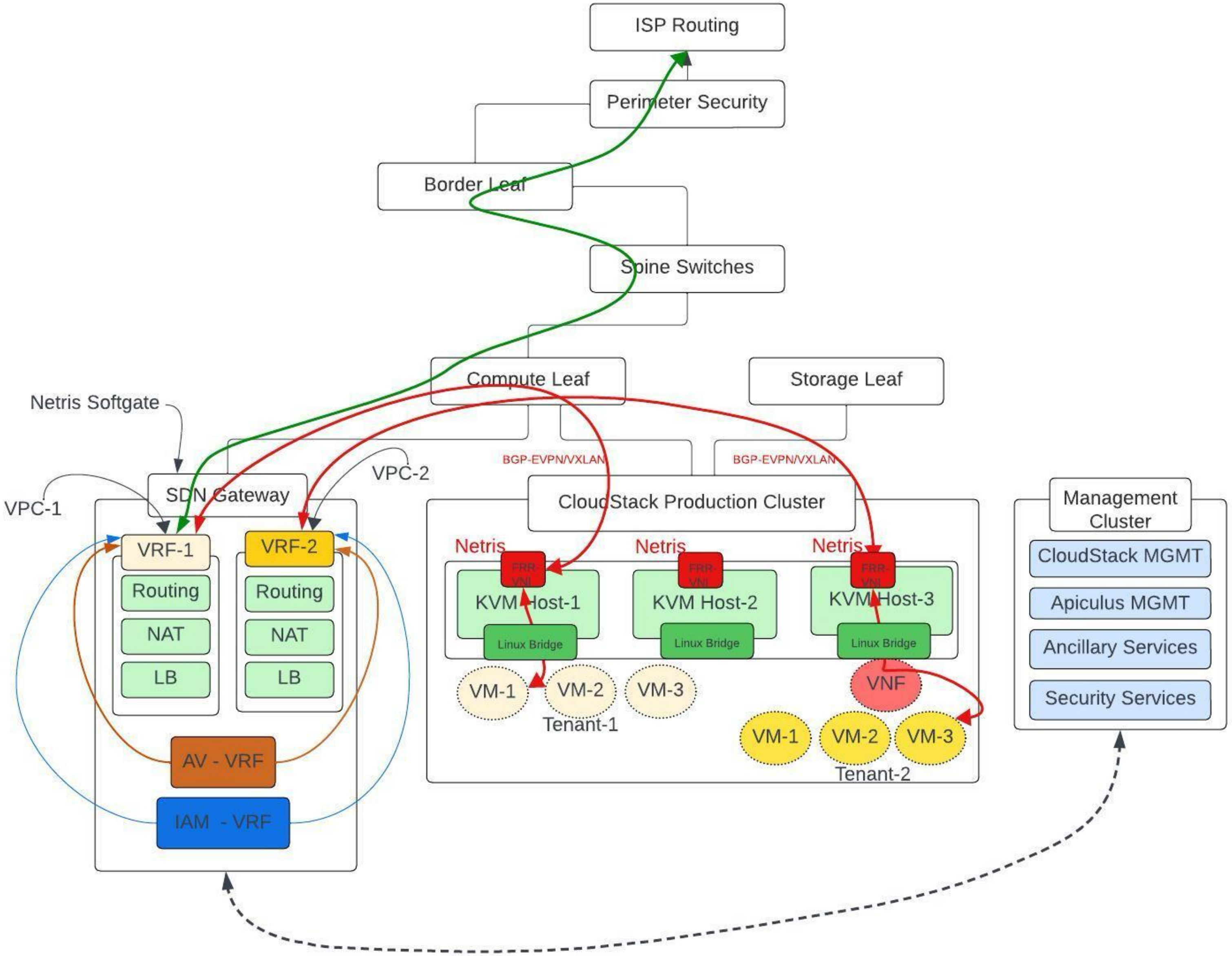
- Unnumbered IPv6 on the Leaf – Spine Links
- Using BGP between Leaf and Spine underlay
- IPv4 BGP sessions between Leaf and Spine Switches
- 128-way ECMP and resilient Hashing
- 400G connectivity for future connectivity to Super Spine

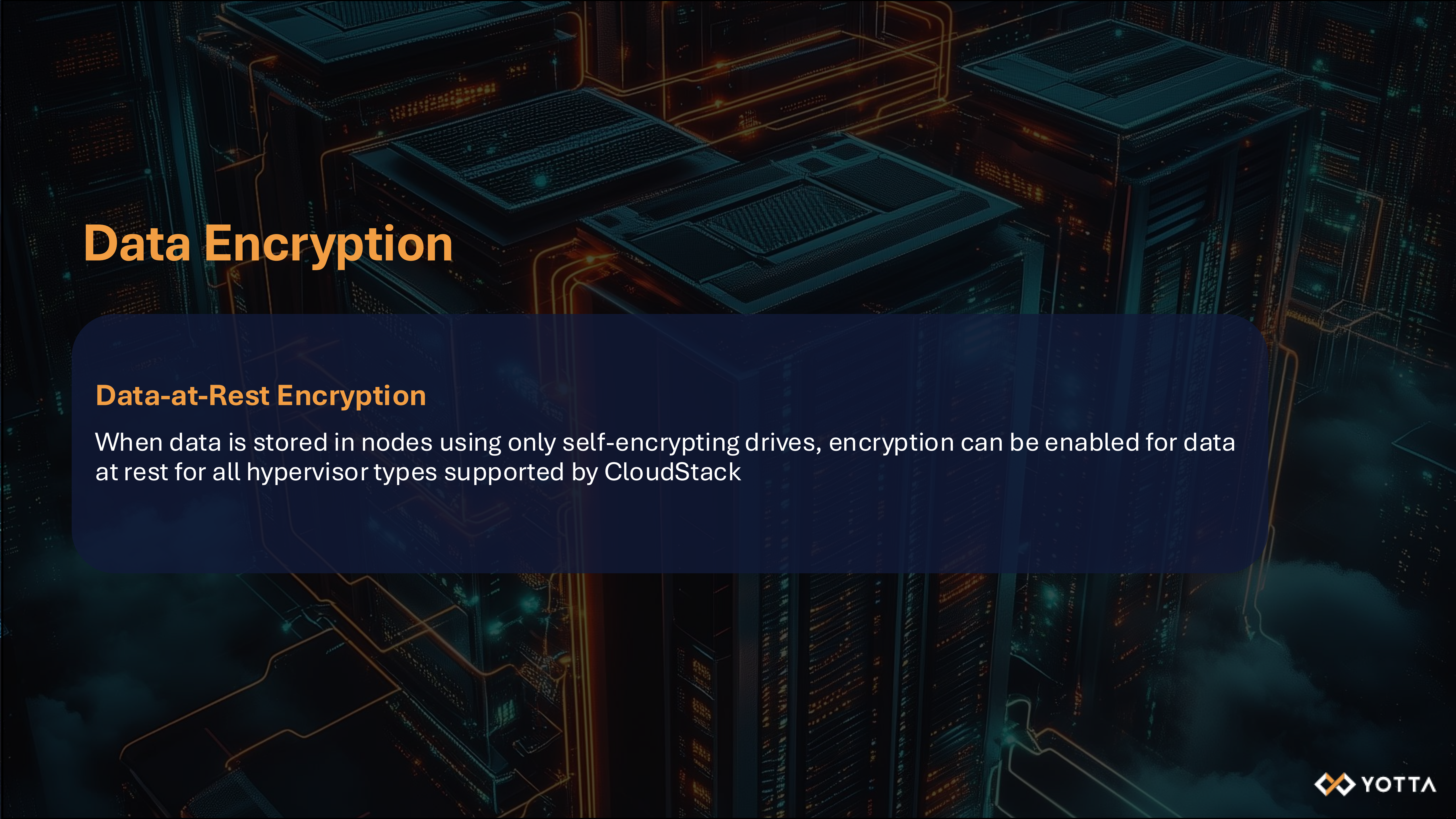
Data and Storage Leaf Traffic handling

- Traffic arriving from Border Leaf will only go to Data Leaf
- HCI to use separate NIC for Data and Storage
- Physically separated networks

YOTTA

Single SDN Controller for Underlay and Overlay





Data Encryption

Data-at-Rest Encryption

When data is stored in nodes using only self-encrypting drives, encryption can be enabled for data at rest for all hypervisor types supported by CloudStack

Conclusion

Our primary goal is to enhance the network and infrastructure capabilities to ensure the delivery of Cybersecurity and Analytics services to Guest VMs for a specific VPC environment, addressing and mitigating compliance requirements effectively.

YOTTA | cloud STACK COLLABORATION CONFERENCE

Thank You