Flexibility, Resilience, and Security: IBM's Hybrid Cloud

Ziqi Liao

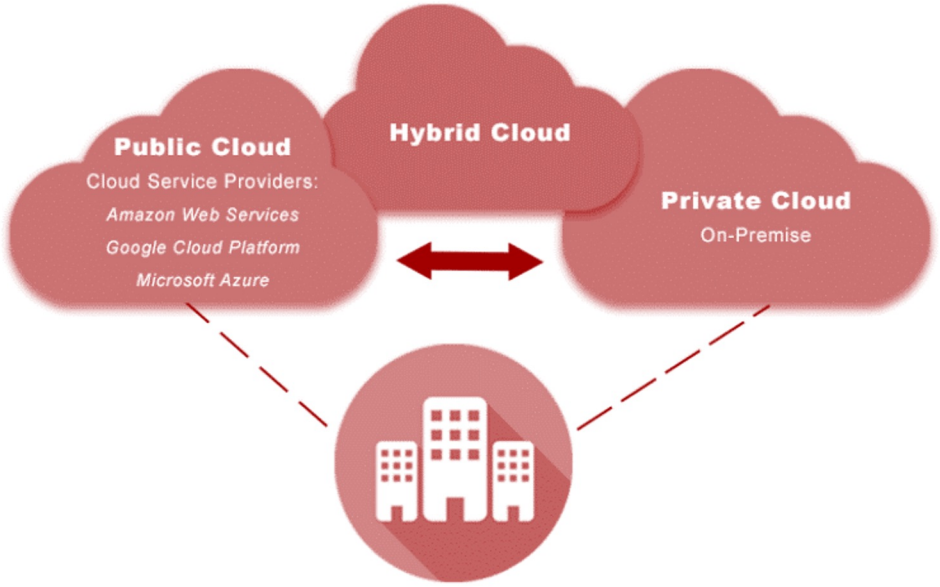
November 8, 2023

What is Hybrid Cloud?

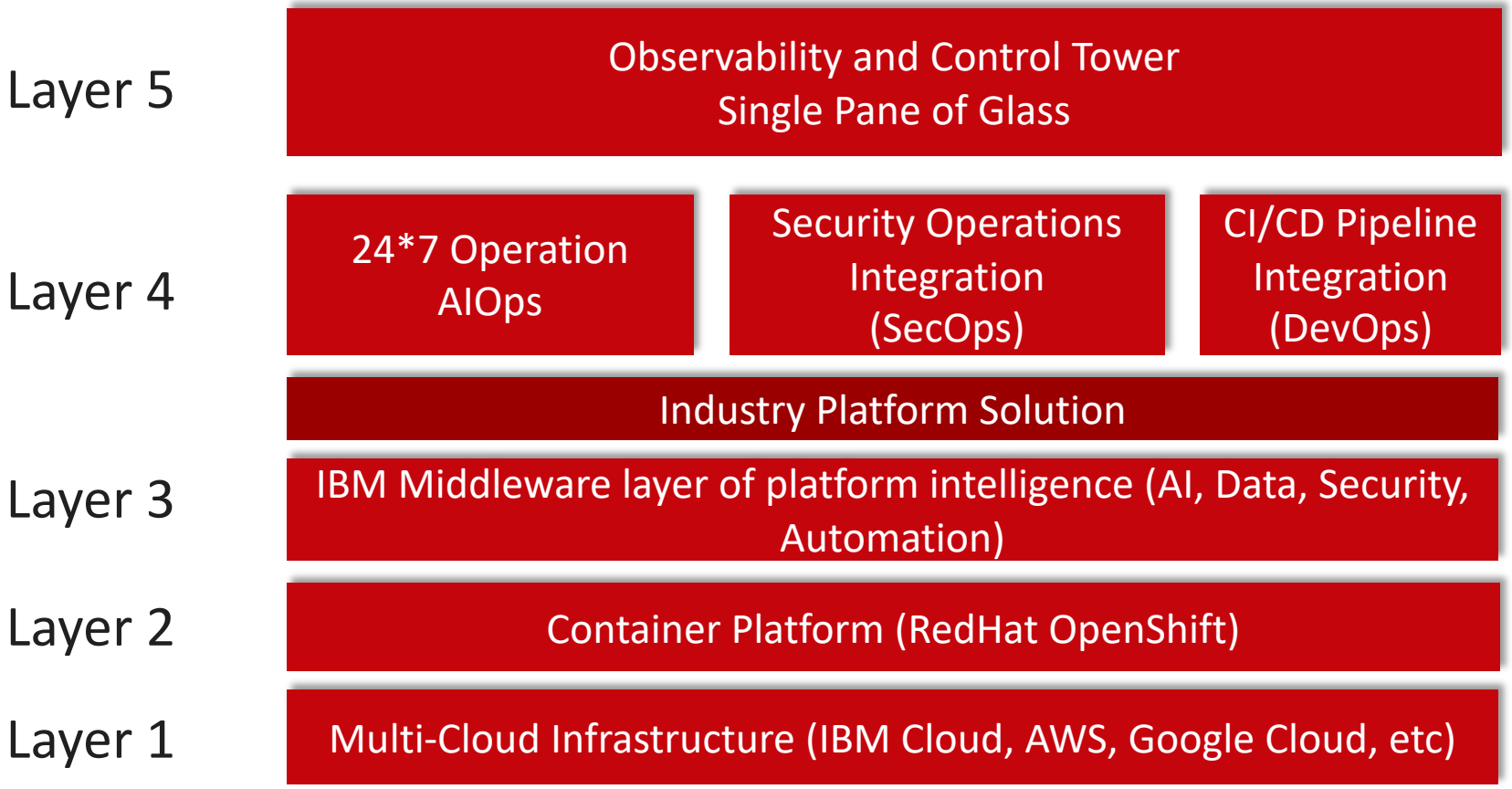
- Hybrid cloud combines and unifies public cloud, private cloud and on-premises infrastructure to create a single, flexible, cost-optimal IT infrastructure.

Benefits of a unified hybrid cloud platform

- ✓ Improved developer productivity
- ✓ Greater infrastructure efficiency
- ✓ Improved regulatory compliance and security
- ✓ Overall business acceleration



5 layers of the hybrid cloud architecture framework



Modern hybrid cloud infrastructure

- Support for cloud-native application development and deployment across all cloud types (public and private) and cloud providers
- A single operating system across all environments
- A container orchestration platform–typically Kubernetes–that automates the deployment of applications across cloud environments

Key differentiators of IBM Hybrid Cloud

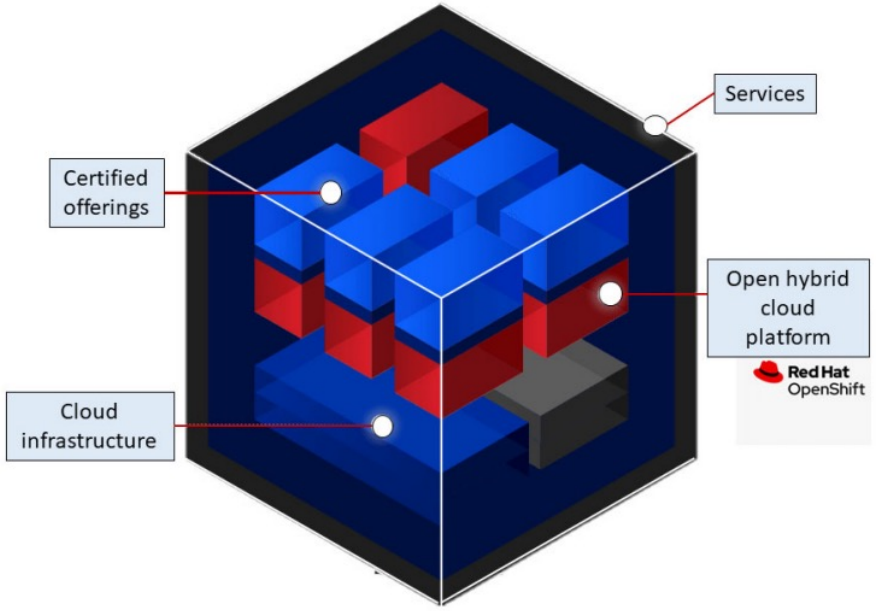
- **Scalability: built on Red Hat OpenShift**
- **Location access (60 data centers worldwide)**
  - Multi-zone regions (MZRs)
  - Single-zone regions (SZR)
  - Data centers
  - By IBM Cloud Satellite
- **Cloud security:**

IBM Cloud data protection

IBM Security Guardium® Data Encryption

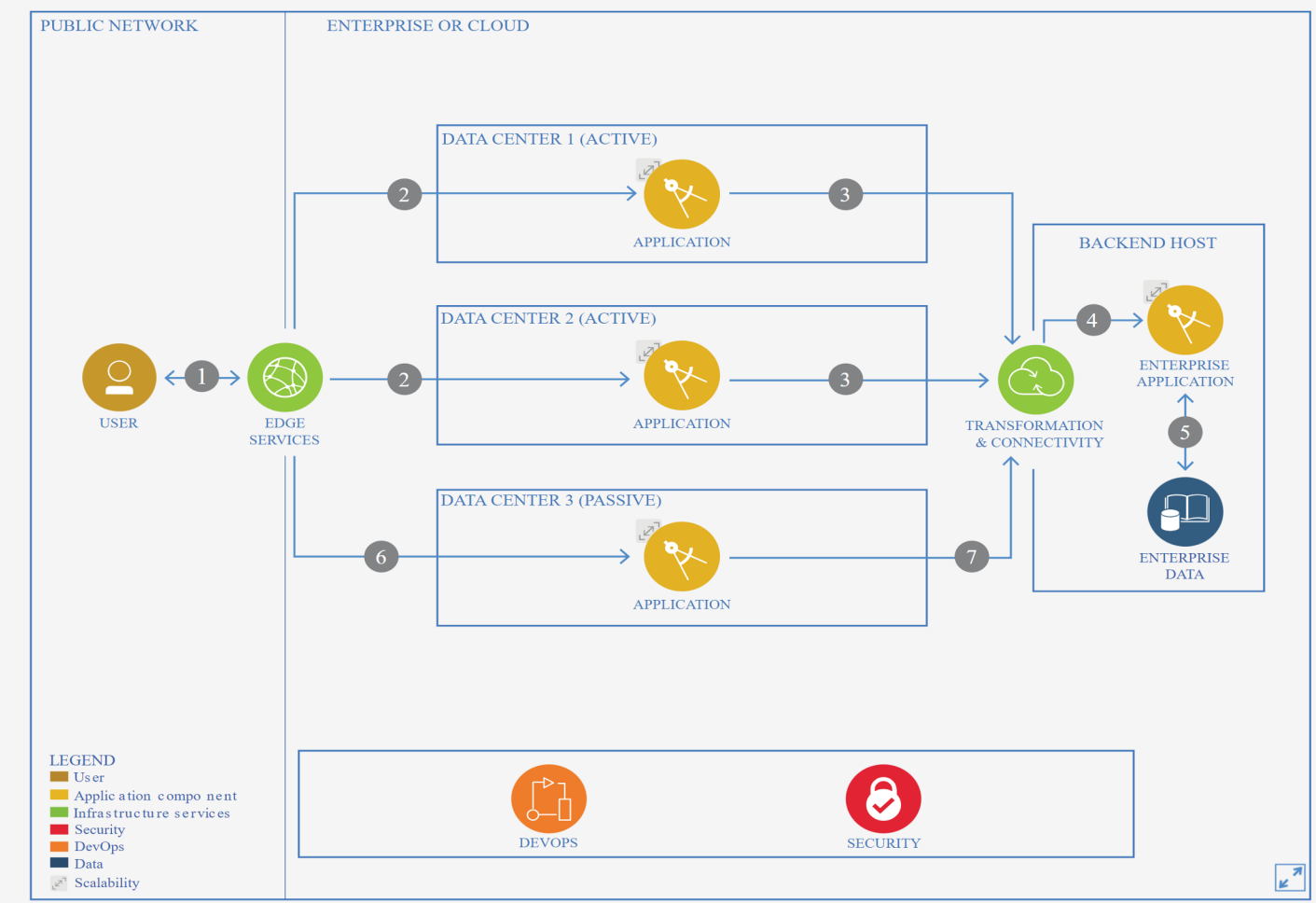
IBM Cloud for Financial Services

- **Leveraging innovation**
- **Multi-Cloud and open source flexibility**



IBM wide range of portfolio offerings

Cloud reliability and disaster recovery

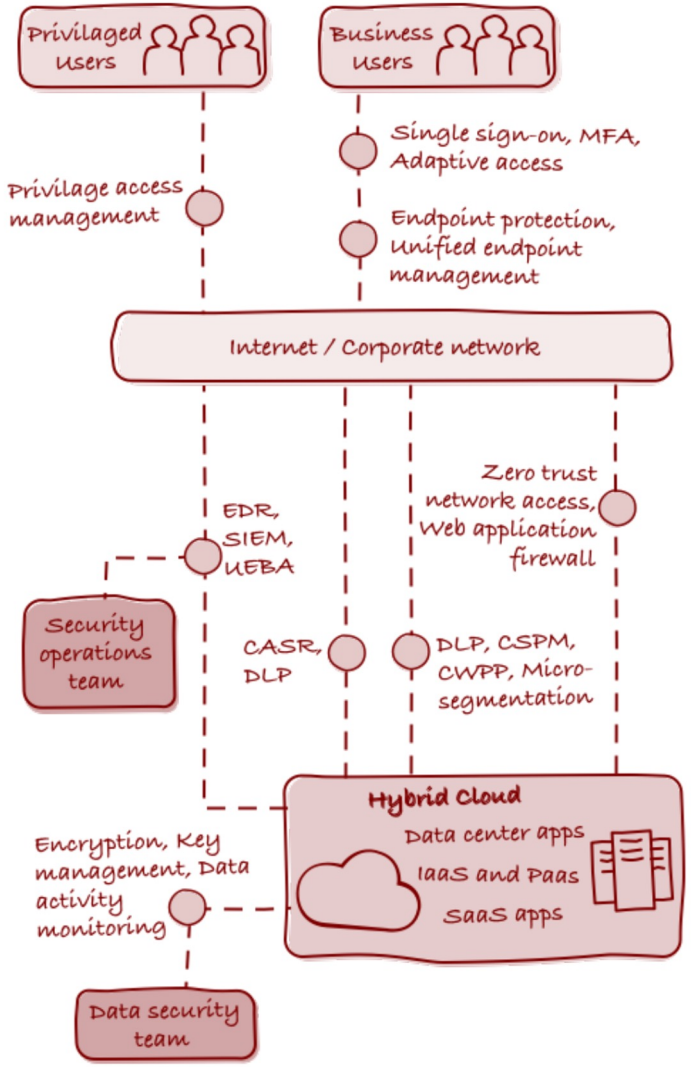


- Data center 1/2 provide high availability
- Data center 3 provides disaster recovery

Security Mechanisms in IBM Hybrid Cloud

- Zero-Trust Model
  - Assume breach
  - Continuous Verification
  - Enable least privilege

- Encryption and Access Management
  - Data encryption in transit
  - Utilizing industry-standard protocols
  - Identity and Access Management (IAM)



Security and Compliance

Security domains	Security capabilities				
Governance, risk, and compliance	**Strategy architecture, and governance**	**Security policy and processes**	**Risk and compliance**	**Audit and regulatory**	**Security awareness and education**
Application security	Secure development lifecycle	Threat modeling and requirements management	Application urntime security	Application security testing	Application defect and risk management
Data security	Data lifecycle management	Data loss prevention	Data access, integrity, and monitoring	Encryption	Key and certificate lifecycle management
Identity and access management	Identity lifecycle management	Identity governance	Access and role management	Privileged identity and access management	Secrets management
Infrastructure and endpoint security	Platform protection	Endpoint protection	Edge protection	Core network protection	Multi-environment security management
Detect and respond	Vulnerability lifecycle management	Security testing	Threat detection	Threat investigation and response	Threat intelligence and hunting

Challenges and Considerations

Challenges	Considerations
Moving from legacy to cloud and AI models	• Modernize applications • Keep IT available • Navigate security and compliance concerns
Creating truly hybrid architectures	• Simplifying the experience of using and Managing of both infrastructure and data
Streamlining security and compliance	• From manual exercises to software-defined approaches
Identifying the next frontiers of technology	• Network and storage • Quantum computing and AI accelerators • Optimized for large-scale and performance-Sensitive workloads

Questions?