How to build a successful hybrid cloud strategy without compromising on security and managability

Martin Borrett
IBM Distinguished Engineer
CTO IBM Security EMEA

Security must enable your journey to hybrid cloud

80%

of workloads have not yet migrated to cloud[1]

94%

of organizations have multiple clouds[2]

85

security products across 40 different vendors[3]

99%

of cloud failures will be customers' fault[4]

32%

of organizations publicly exposed at least one cloud storage service[5]

1 Forrester, The Public Cloud Market Outlook 2019-2022
2 Cloud Computing Trends: 2019 State of the Cloud Survey, Flexera
3 Thousands of IBM Security Services engagements
4. Gartner, is the cloud secure.
5. Analytics Insight, cloud security threats

Today's hybrid, multicloud reality presents several challenges

How can I integrate my native security tools into my overall security operations?

What are my security responsibilities vs. my Cloud Service Provider's?

How do I secure my critical data on cloud?

How can I get visibility into and manage Shadow IT usage?

How can I ensure my native security tools are properly configured?

How do I centrally manage policy across my on-premise and cloud environments?

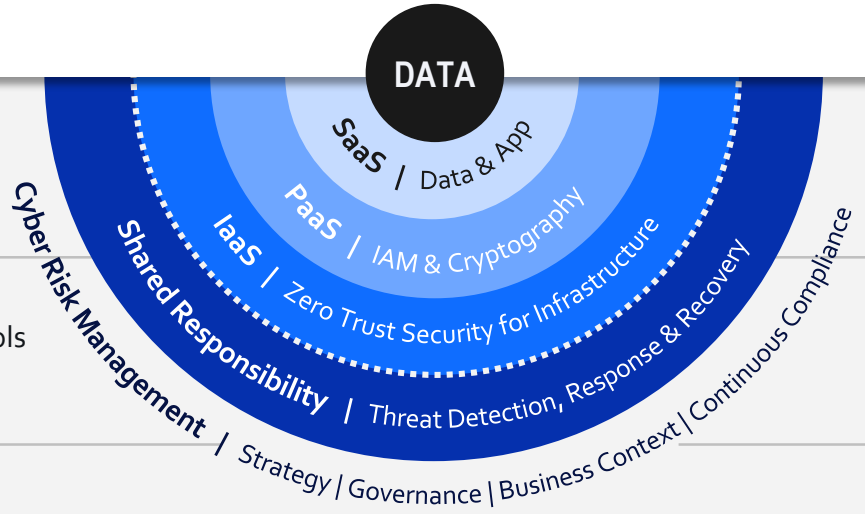
How do I develop cloud applications that are secure by design?

How do I secure access to my cloud workloads?

How do I keep up with changing compliance regulations?

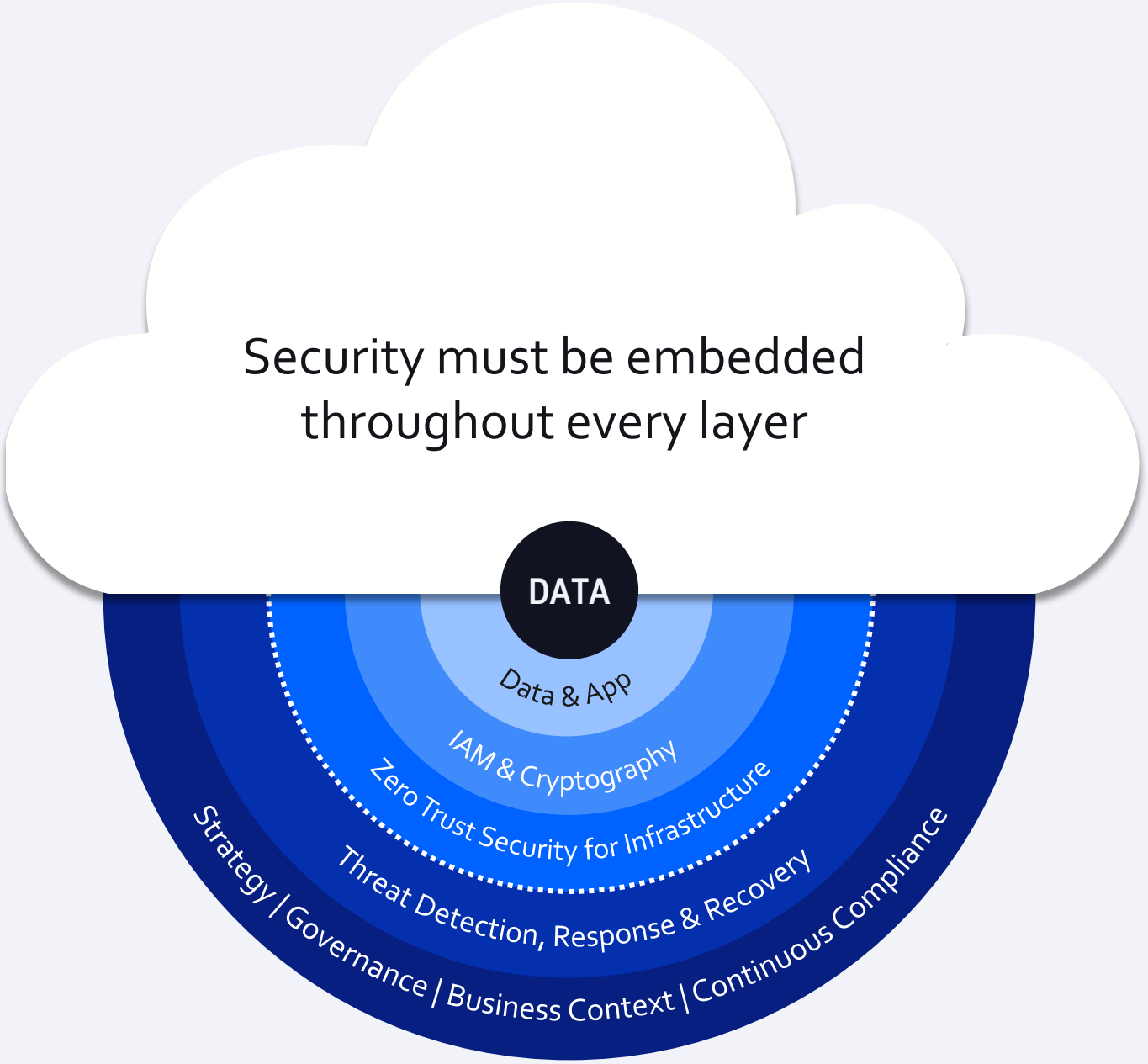
How can I apply security without impacting the speed of business innovation?

We're hearing a lot of new cloud security concerns from customers
Where do they start?



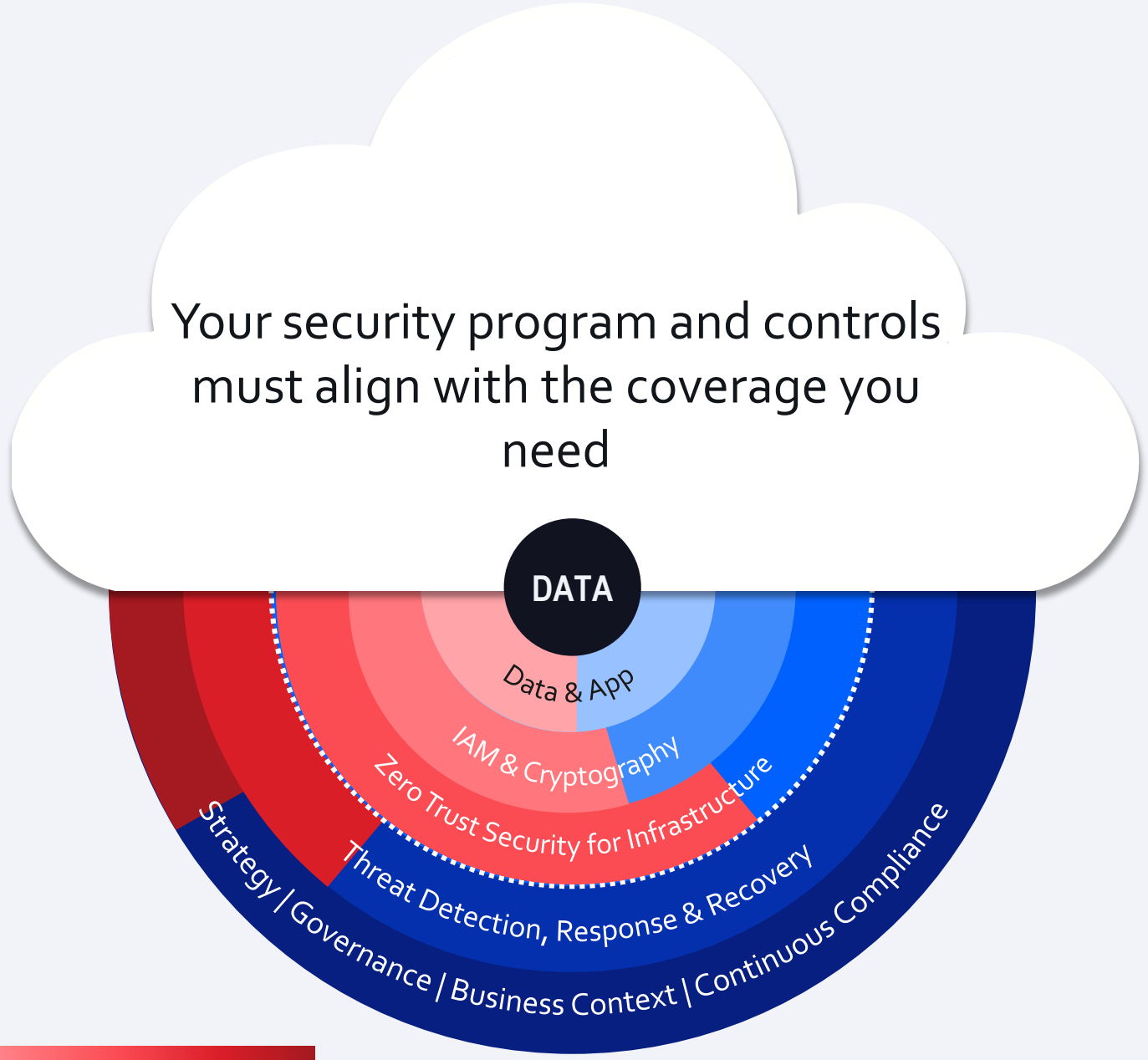
Securing Enterprise Hybrid Cloud requires a comprehensive security program

It should span across all layers, with data as the center of the universe.

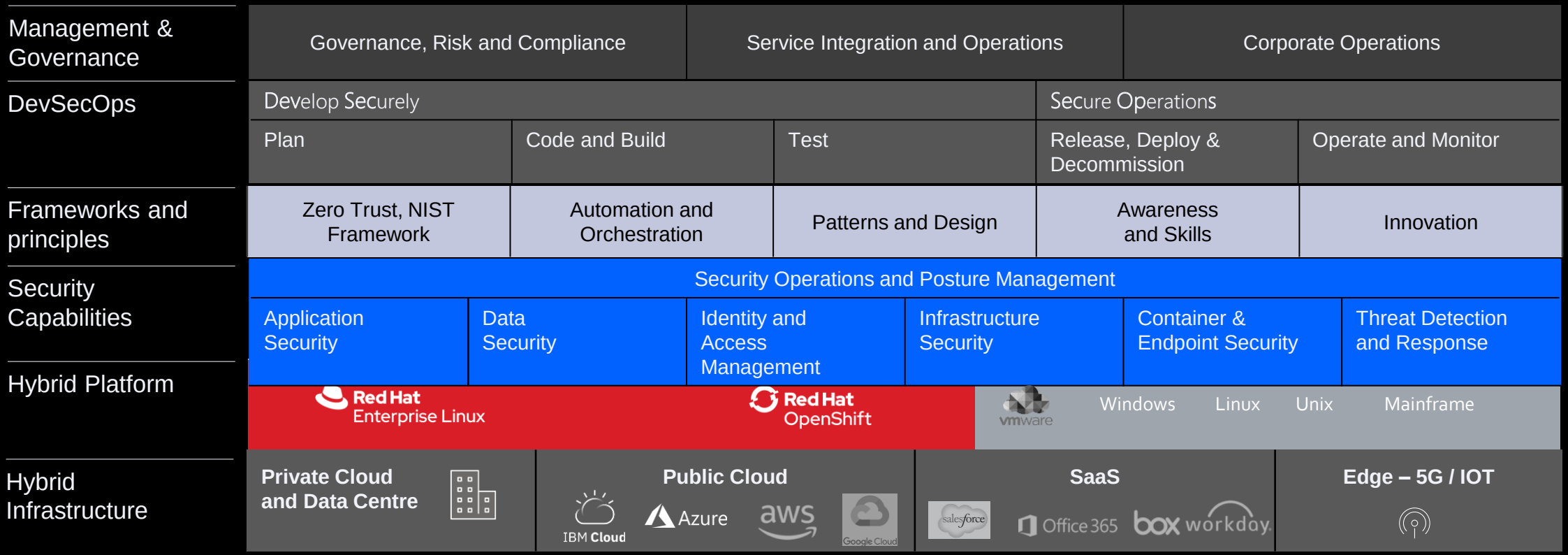


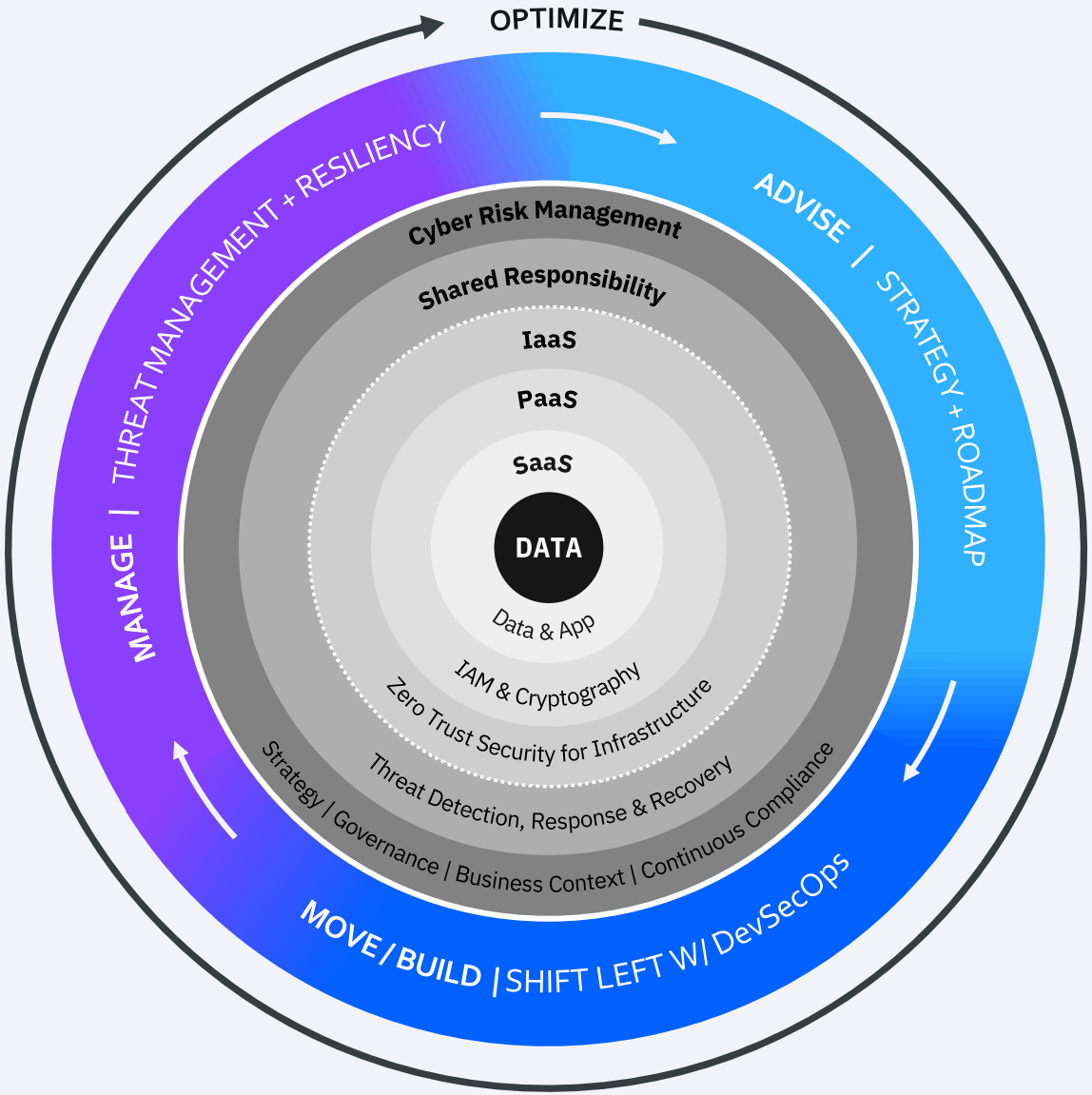
Don’t the cloud providers already have security?

Cloud native security controls are helpful but not typically enough, especially across hybrid or multi-cloud environments



Tiered Approach towards enabling hybrid cloud security





A successful journey to the cloud contains security and resiliency throughout.

ADVISE
Security & Compliance at the Core of Your Cloud Transformation Strategy

MOVE / BUILD
Building Applications Based On A Secure Environment & Secure Best Practices

MANAGE
Continuous Security & Compliance Monitoring with a Resilience plan in place

IBM Cloud Pak for Security

An open multicloud platform to gain security insights, take action faster, and modernize your architecture

Modular security capabilities

- Threat Management
- Data Security
- Identity & Access Management
- Open Security Ecosystem

Platform services

- Data connection
- Asset enrichment
- Case management
- Orchestration
- Automation
- Development tools

Open and integrated hybrid multicloud platform

SIEM tools | EDR tools | Cloud repositories | Data lakes | Database protection | Network protection | Additional point solutions

On premise | Hybrid Cloud | Multicloud

IBM Cloud: The most open and secure public cloud for business

Open innovation

- API services that are cloud delivered applications
- Kubernetes on IBM Cloud™: 1,000-plus clients, 21,000-plus clusters in production
- Major contributor to cloud-native open source work: Istio, Knative, Razee and more

Security leadership

- Highest compliance for data encryption
- Configurable so that even IBM cannot see your data
- Edge-to-cloud threat management with security integration from IBM

Enterprise grade

- #1 VMware public cloud, with 2,000 clients
- Cloud migration for IBM Power® AIX®, IBM i, IBM Z®, SAP and mission-critical applications
- Broadest portfolio of compute instances, including Power and x86

Highest level of encryption
FIPS 140-2 Level 4

Isolation for cloud native
ROKS and containers on bare metal

No data egress charges with Cloud Databases
No vendor lock in and lower TCO

No-cost bandwidth between regions
Significantly lower TCO

Enhanced availability SLAs
HA: 99.99%, Non-HA: 99.9%

Higher SLA payouts versus market
25% of monthly at 60 minutes

Audit transparency to bare metal
Traceable serial number compliance

Full control to bare-metal level
Full admin control of compute

World's first financial services-ready public cloud with Bank of America

2019 IBM WINNERS
GOOD DESIGN AWARD WINNER
Good Design Award for VPC

DESIGN AWARD 2019
Good Design Award for IBM API Connect®

Gartner peerinsights customers' choice
Customer Choice Award for Cloud IaaS

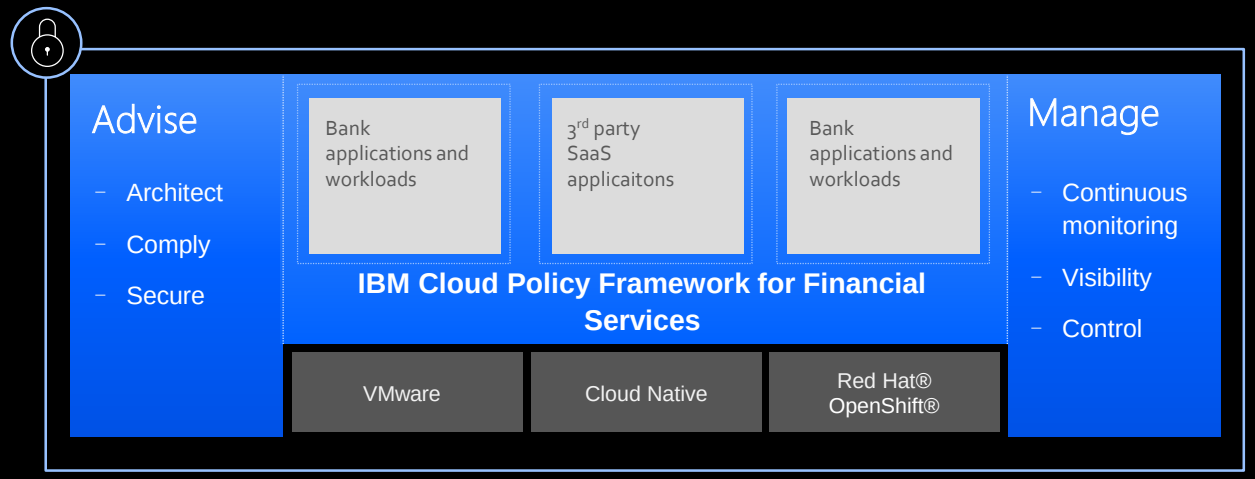
STRATUS 2019 AWARD
Stratus Award for User Experience

IBM Cloud for Financial Services

Achieve private cloud-security in a public cloud and demonstrate regulatory compliance faster, more efficiently

Financial Services key program elements:

- Industry-informed common criteria to enable the ecosystem (Cloud, FIs, ISVs) to transact and operate securely, fluidly
- Intelligent monitoring and enforcement of security and compliance profiles
- Mainframe-level data security, and compute and network isolation
- Innovation lab to connect FIs with IBM Research team and portfolio to build skills and learn in cloud



IBM Cloud for Financial Services

Financial Services Advisory Council:

Bringing together FIs to help drive strategic evolution of cloud security and advise on the advancement of IBM Cloud Policy Framework for Financial Services.

That's a lot to consider!

How can we help you get started?

01. Assess your current environment & strategy

Cloud Security Strategy Assessment

02. Understand what and where your critical data is

Cloud Data Discovery & Classification

03. Review your current cloud compliance posture

Security Posture Management for Cloud

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

IBM Security

IBM