

Cloud Security Styles

Caribbean Telecommunications Union
9th Ministerial Strategic Seminar
December 7th – 8th, 2011

Cloud
Computing.
The complete
picture.



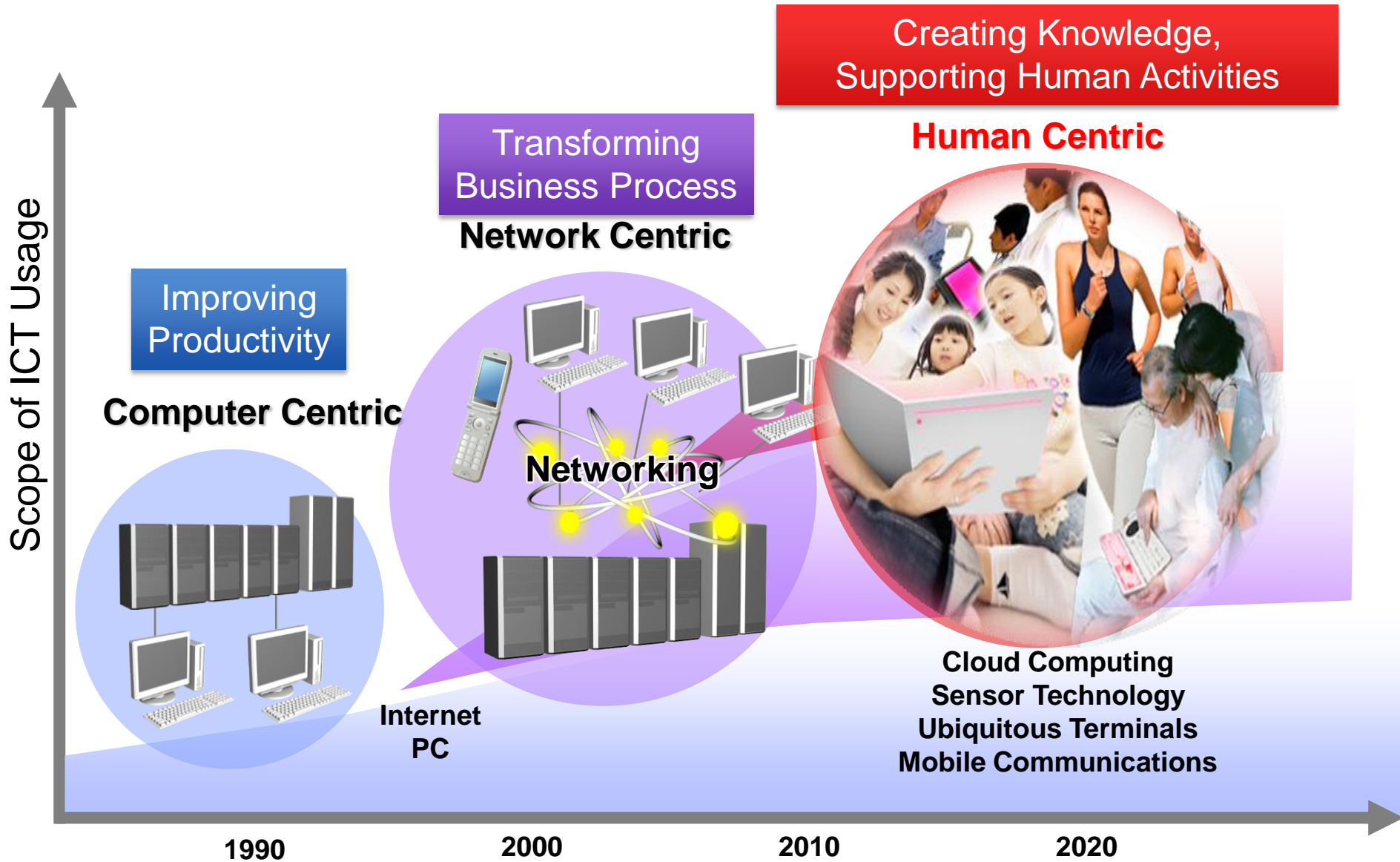
Concerns we hear from you..

- Trust
- Compliancy and regulations
- Security
- Data Sovereignty / Data location
- Long-term viability

What are we afraid of...?

“Cloud computing has “unique attributes that require risk assessment in areas such as data integrity, recovery, and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance, and auditing” - Gartner

Entering the Human Centric era



Technology – the New Way



Accessible to all



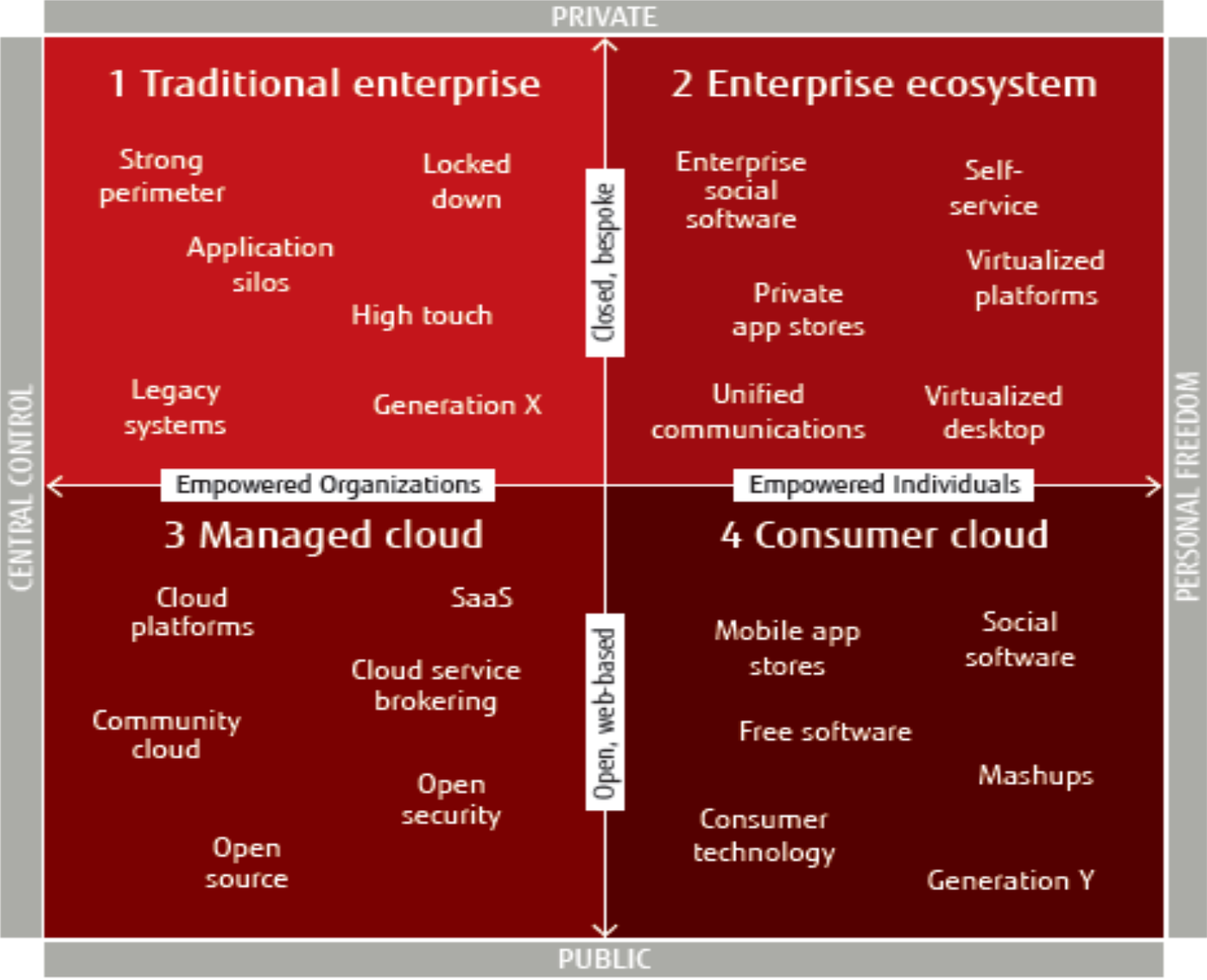
Commoditized

On-demand



Stateless

Scenarios for the future

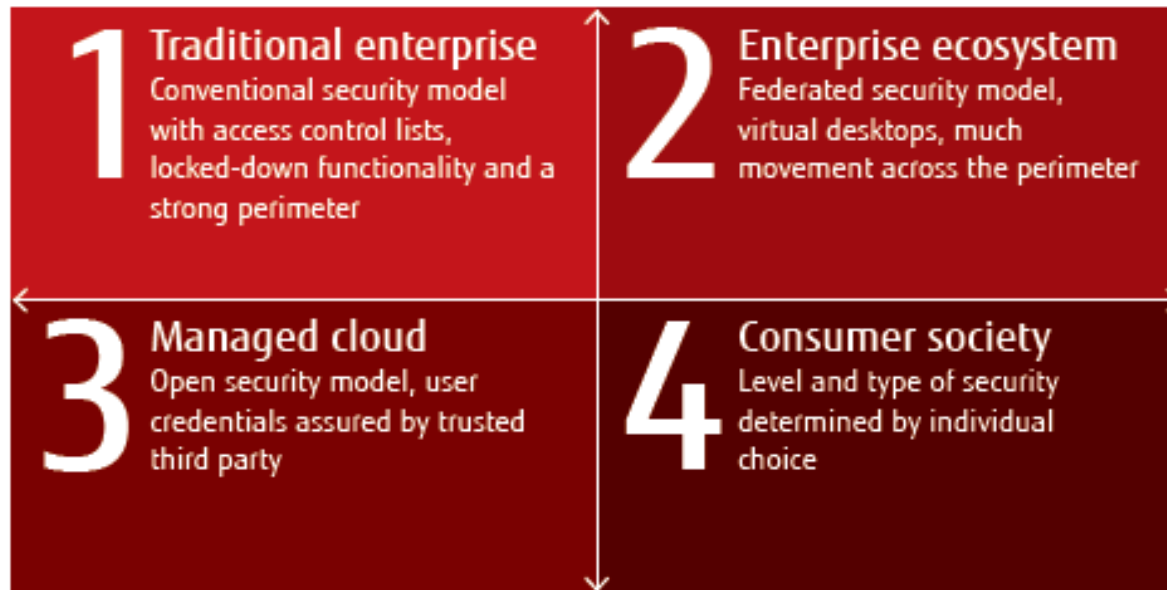


Financial model	CA PEX mainly
Commercial model	Fixed spend
Client devices	Locked down
Applications	Monolithic
Collaboration	Low
Information	Siloed + secured
Security	Traditional
Relevance of perimeter	High
Standards	Across the board
Service model	Bespoke
Choice	Limited
IT buyer	IT function

Financial model	Cap Ex + Op Ex
Commercial model	Fixed + variable
Client devices	Virtualized + thin client
Applications	Virtualized
Collaboration	Intra-organization
Information	Shared + secured
Security	Federated
Relevance of perimeter	Medium
Standards	Minimum needed
Service model	Self service
Choice	... of client devices
IT buyer	IT function + Individuals

Financial model	Op Ex only
Commercial model	Variable
Client devices	Browser-based
Applications	SaaS
Collaboration	Inter-organization
Information	Shared + trusted
Security	Open
Relevance of perimeter	Weak
Standards	For security + software interfaces
Service model	Commoditized
Choice	... of services
IT buyer	Business function

Financial model	Op Ex + free
Commercial model	Pay-as-you-go
Client devices	Anything goes
Applications	App stores
Collaboration	Everywhere
Information	Public
Security	As offered
Relevance of perimeter	Irrelevant
Standards	None
Service model	As offered
Choice	High
IT buyer	Individuals



Gartner sees 3 broad styles of security:

- Rely on security built into the cloud infrastructure
- Run your own security controls in the cloud
- Require all security controls to run separately from the cloud

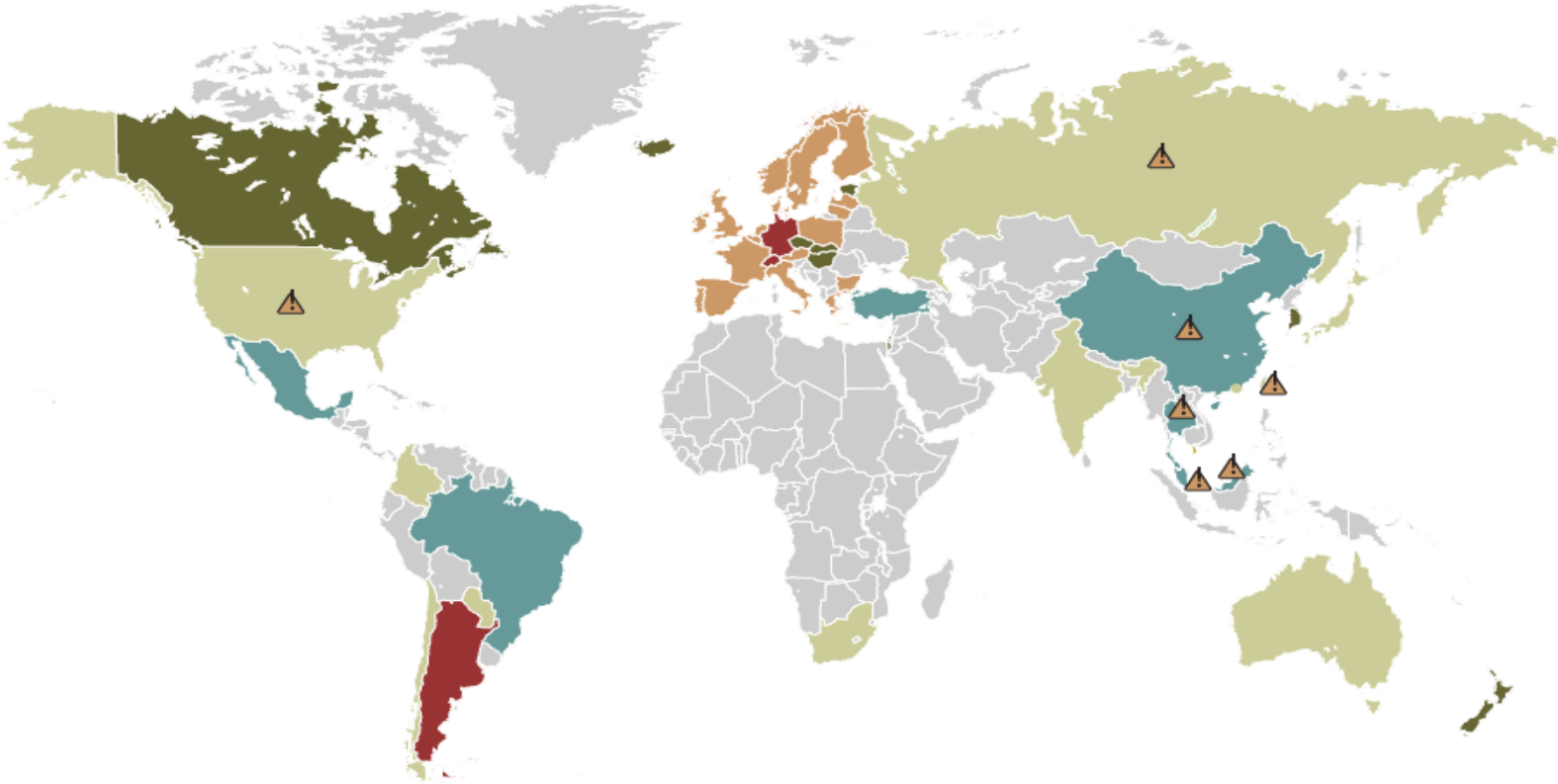
Matching the security level of workload/application to the Cloud Security Style

	Low	Medium	High
Public Cloud	<ul style="list-style-type: none">• Security built into the cloud is used• Statement on Auditing Standards (SAS) 70 sufficient	<ul style="list-style-type: none">• Third-party security running in cloud is used• Custom/industry security assessment	<ul style="list-style-type: none">• Security is performed outside the cloud• No trust of the cloud
Private Cloud	<ul style="list-style-type: none">• Security built into a VM is used• Accept vendor security claims	<ul style="list-style-type: none">• Third-party security running on the VM is used• Certification/accreditation assessment	<ul style="list-style-type: none">• Security is performed outside of the VM• Security product certification

Source: Gartner (August 2010)

Global data protection regulations

- Most restrictive
 - Restrictive
 - Some restrictions
 - Minimal restrictions
 - Pending legislation
 - No legislation or no information
- ⚠ Caution due to government surveillance

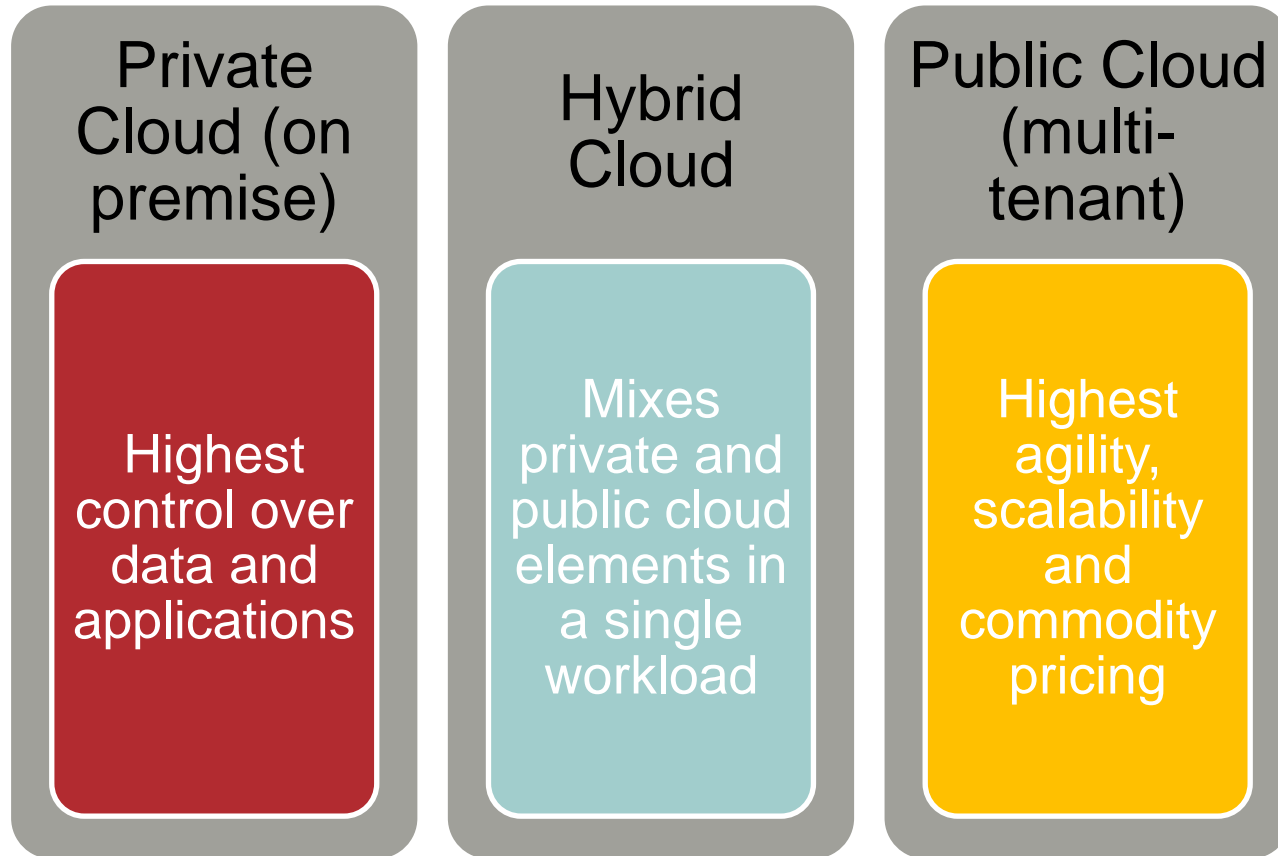


Source: US Department of Commerce and country specific-legislation

Source Forrester: <http://www.forrester.com/cloudprivacyheatmap>

Driving cloud in the enterprise

- Most enterprise cloud business will be driven by a hybrid approach



Fujitsu Dynamic Cloud

Your Gateway
to Success



@abayrd

@Fujitsu_Carib

adrian.bayrd@caribbean.fujitsu.com