Cloud or Hell Computing ?

Os desafios da Segurança em Cloud Computing

Cezar Taurion
Technical Evangelist
ctaurion@br.ibm.com

Marcus Vinicius Itala Ferreira
Arquiteto de Segurança
marcusv@br.ibm.com

The significance of Cloud Computing

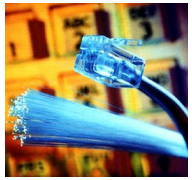
Cloud Computing changes IT services delivery in the same way that the *ATM changed banking* and the *internet changed commerce*

Seismic Shifts: What the Industrial Revolution has to do with the Evolution of Modern IT

- Industrial Revolution – **no single event**, but an evolution of events and inventions over many decades
- **Standardized processes** in product manufacturing brought about **significant changes in labour**
- Cloud is the “Spinning Jenny” or “Watt’s Steam Engine” of its time: an essential part to the history of IT, but only a part of a much wider narrative
- How this narrative will play out over the next decade really is anyone’s guess
- **There will be winners and losers**

Mainframe Era

PC / Client-Server Era



The Network Era

Cloud Computing Era

1960s 1970s 1980s 1990s 2000s 2010s+

- In just the last decade, we’ve moved from static websites and slow internet modem dial-up to $$$Bn e-commerce, pervasive mobile and “tweeting” the world! In the next decade, we may have witnessed a dramatic transformation in the way IT is bought / consumed, to a highly flexible, pay-as-you-go, standardised model. All bets are off !

A cloud computing primer – your 60 second guide

Start

A new model of IT delivery and consumption…

…inspired by internet services in the consumer space

Key ingredients:
- elasticity
- PAYG
- on-demand self-service

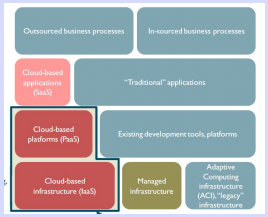
Analogies - electricity generation and The Model-T Ford

Evolutionary, not revolutionary – time sharing, hosting, ASP

A "confluence of technologies" – virtualization, SOA, multi-tennancy

Variants – public, private, hybrid, community, G-cloud add to confusion

Get to know the Cloud stack



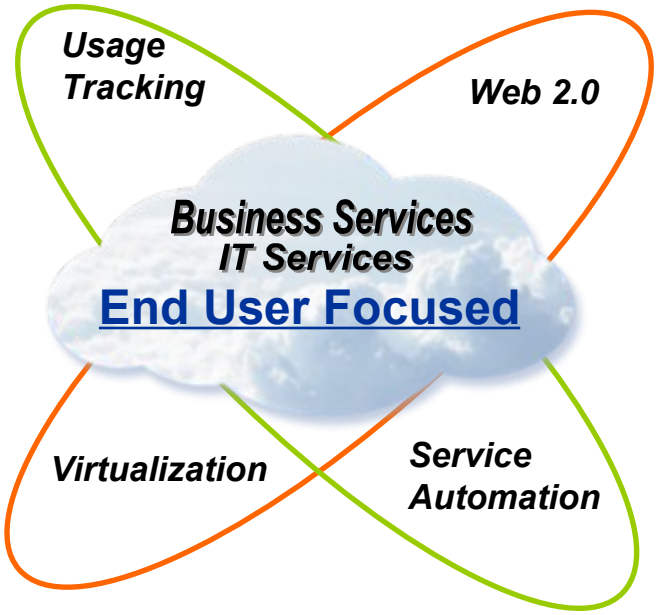
Near-term adoption overstated, long-term impact underestimated – **all bets are off !**

Finish

Source: Market Insights

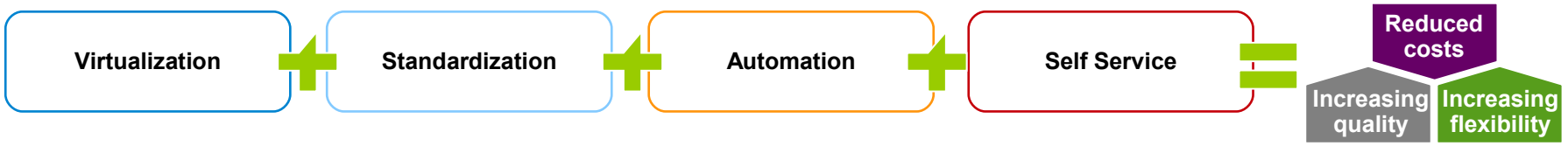
Cloud Computing Definition

Cloud computing is a **new consumption and delivery model** inspired by consumer internet services and driven by client needs

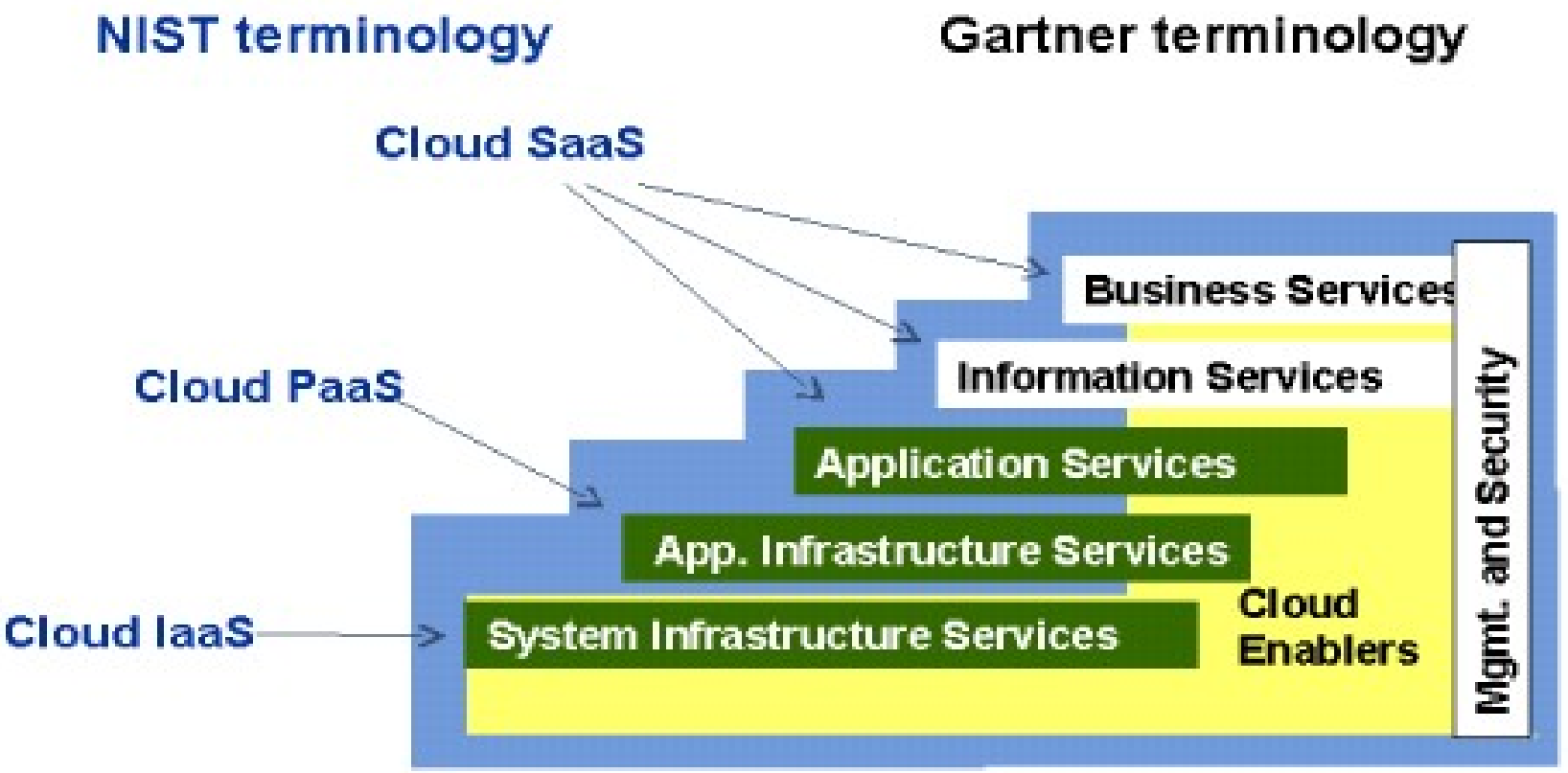


Cloud computing has **5 key characteristics**:

1. “Always on” network access
2. On-demand self-service
3. Location independent resource pooling
4. Rapid elasticity – grow & shrink easily
5. Flexible pricing models



Cloud Service Types



Source: "Government in the Cloud" Gartner Webinar, Sept. 8, 2010

A range of deployment options

Private

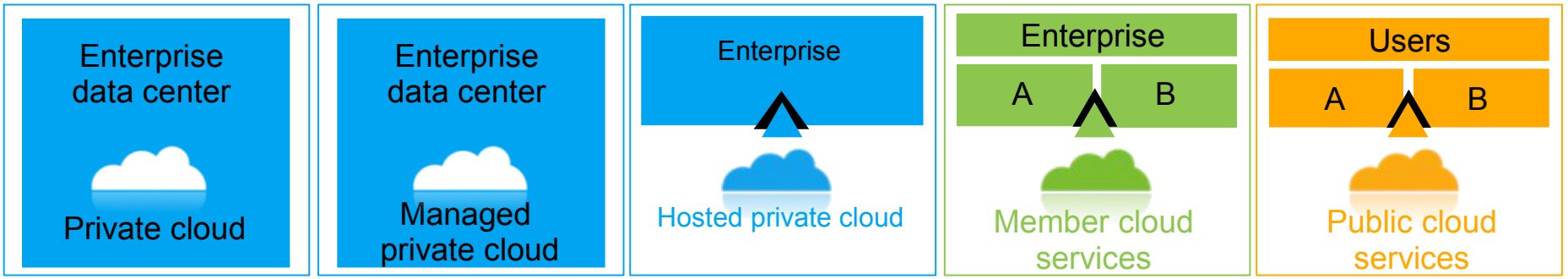
IT capabilities are provided "as a service," over an intranet, within the enterprise and behind the firewall

Hybrid

Internal and external service delivery methods are integrated

Public

IT activities / functions are provided "as a service," over the Internet



- Private
- On client premises
- Client runs/ manages

- Third-party operated
- Client owned
- Mission critical
- Packaged applications
- High compliancy
- Internal network

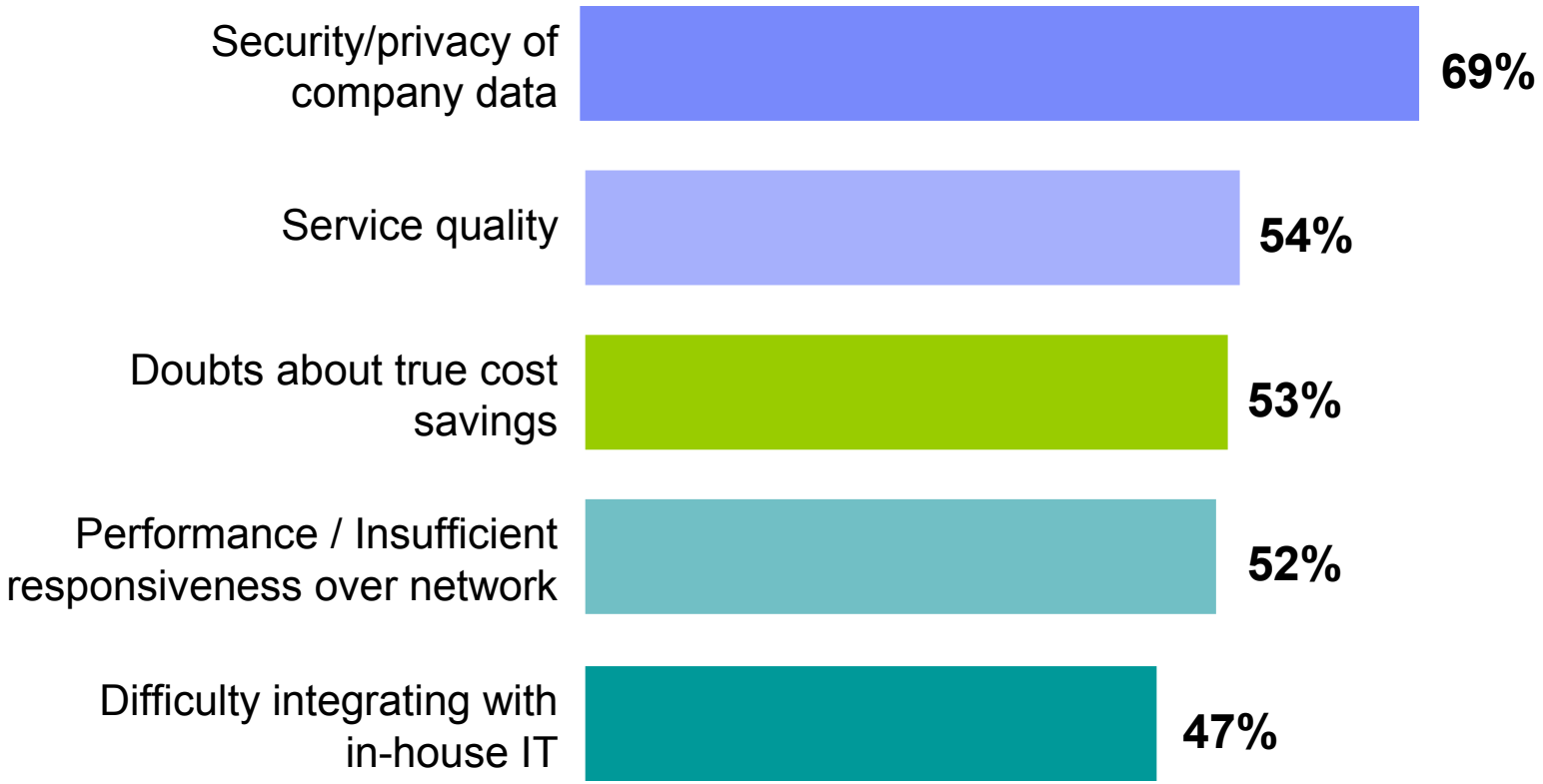
- Third-party owned and operated
- Standardization
- Centralization
- Security
- Internal network

- Mix of shared and dedicated resources
- Shared facility and staff
- Virtual private network (VPN) access
- Subscription or membership based

- Shared resources
- Elastic scaling
- Pay as you go
- Public Internet

Concerns about data security and privacy are the primary – but not the only - barriers to public cloud adoption

What, if anything, do you perceive as actual or potential barriers to acquiring public cloud services?



Source: IBM Market Insights, *Cloud Computing Research*, July 2009. n=1,090

Cloud attributes that greatly affect information security:

INTERNAL DELIVERY → EXTERNAL DELIVERY

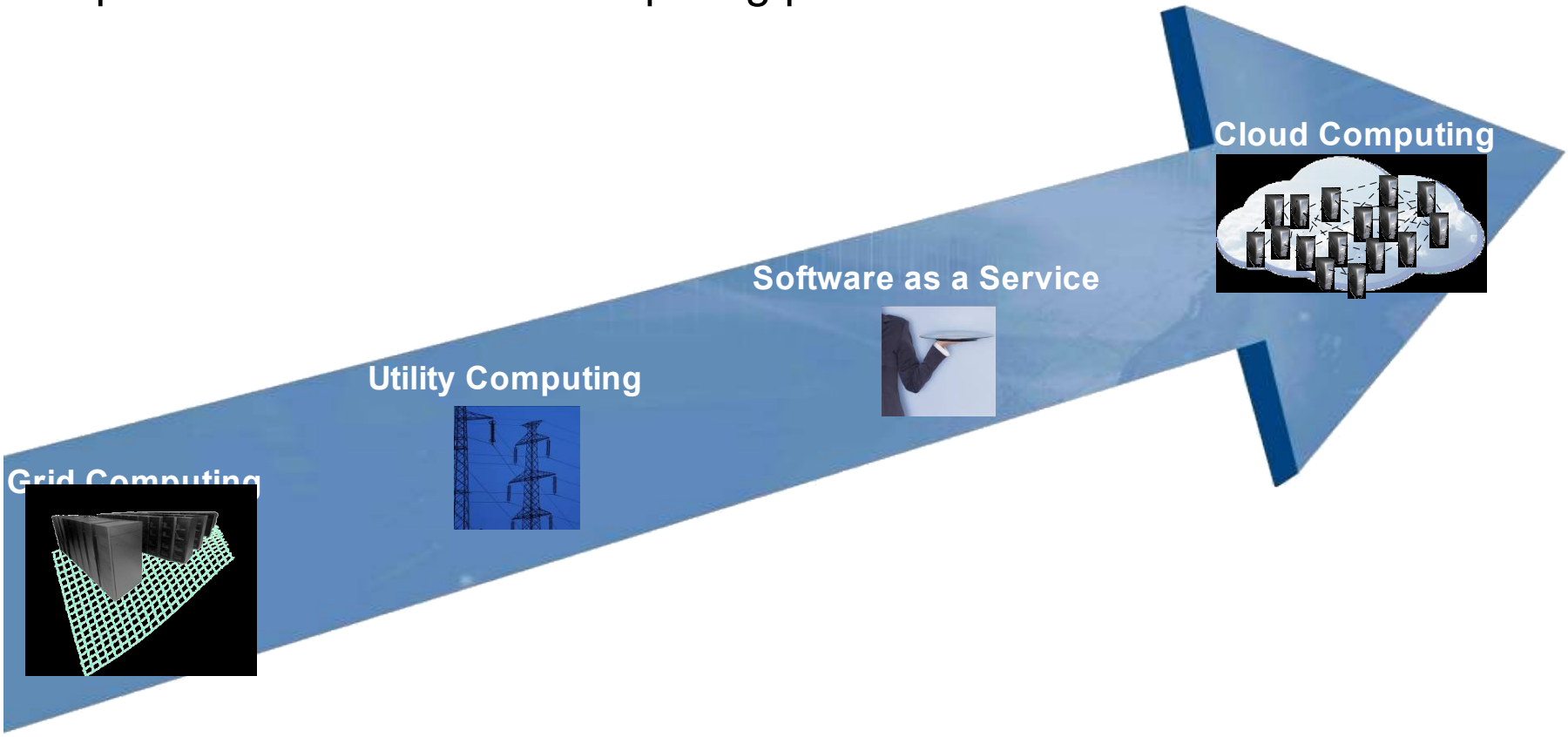
SINGLE-TENANCY → MULTI-TENANCY

IT-SERVICE → SELF-SERVICE

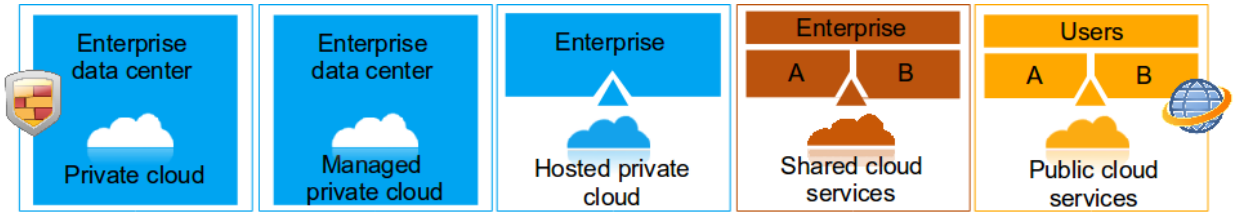
SLOW PROVISIONING → RAPID PROVISIONING

What is Cloud Security?

Ensure confidenciality, integrity and availability of critical IT resources which are stored or processed in a Cloud Computing platform.



Where is the information?



We have control
It is stored on .....
We have backups.
We control administrative access.
Auditors are happy.
Security team is involved.

Who has control?
Where is it stored?
Who is responsible for backup?
Who has access to the data?
How is it audited?
How is the security team involved?

33%

Answered that are concerned with compliance with regulations in a cloud environment

48%

of the corporations are worried with the reliability of cloud environments

80%

of the corporations consider security as the #1 inhibitor for the cloud model

Source: Driving Profitable Growth Through Cloud Computing, IBM Study, 2008 (conducted by Oliver Wyman)

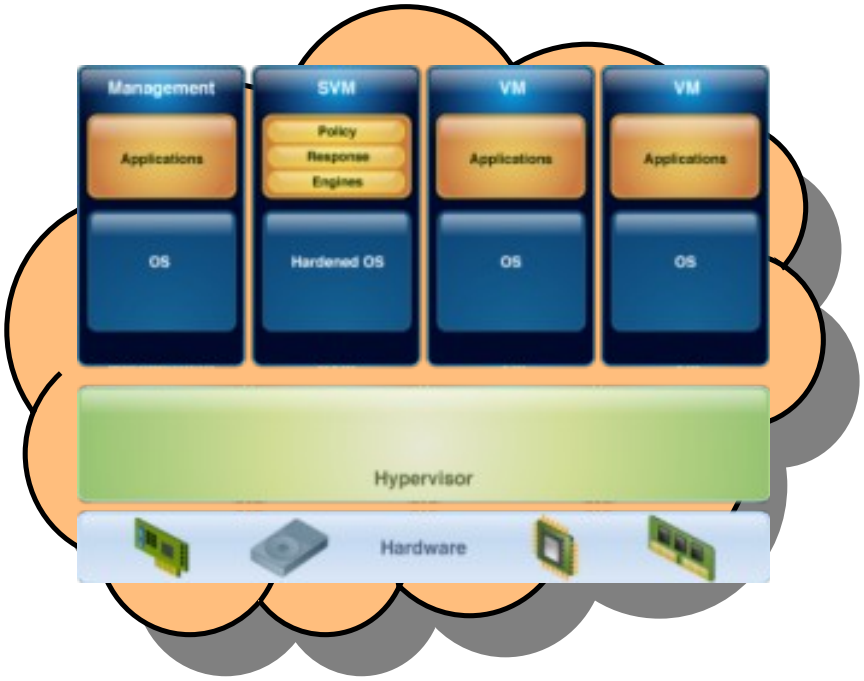
Security complexities raised by Cloud

- New complexities
  - Dynamic relocation of VMs
  - Increased infrastructure layers to manage and protect
  - Multiple operating systems and applications per server
  - Elimination of physical boundaries between systems
  - Manually tracking software and configurations of VMs

Before Cloud

- 1:1 ratio of OSs and applications per server

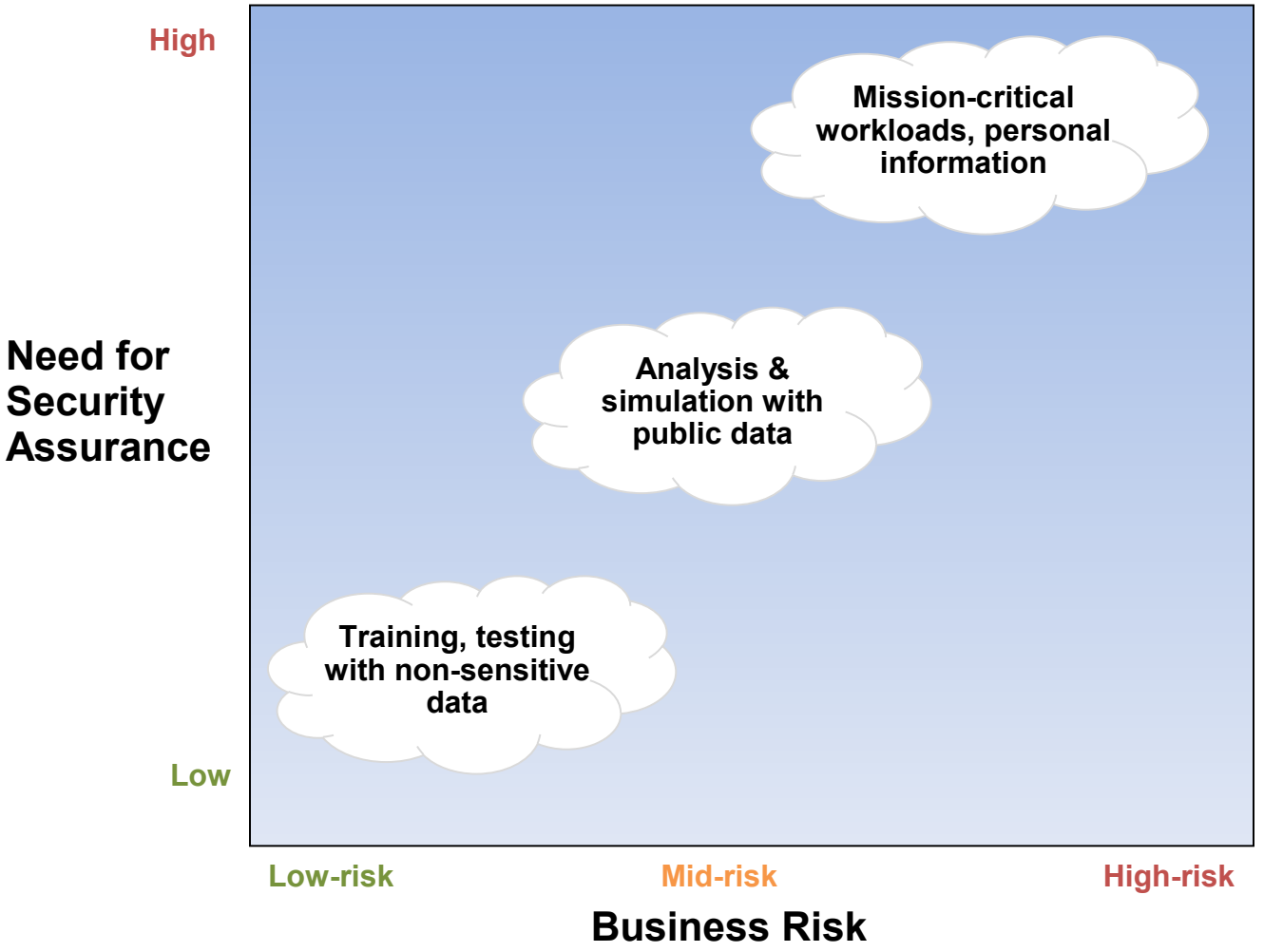
After Cloud



- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure

One size does not fits all

Different cloud workloads have different risk profiles



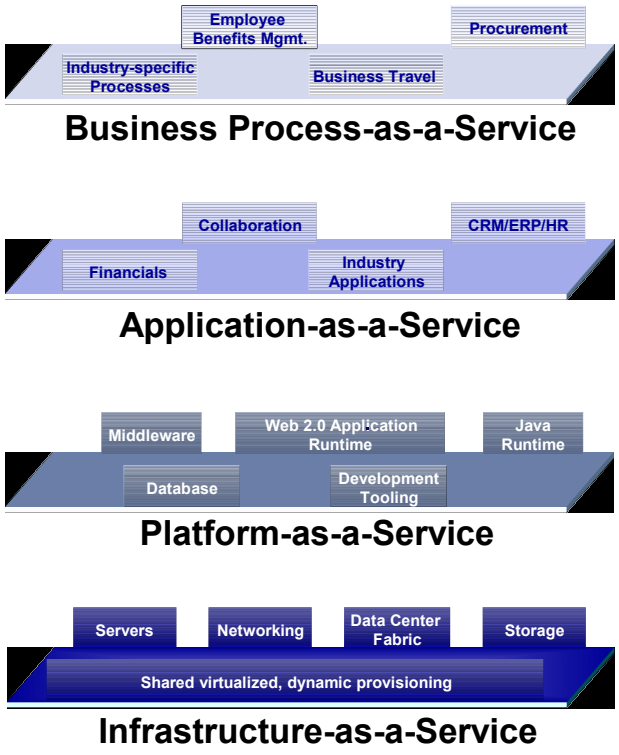
Tomorrow's high value / high risk workloads need:

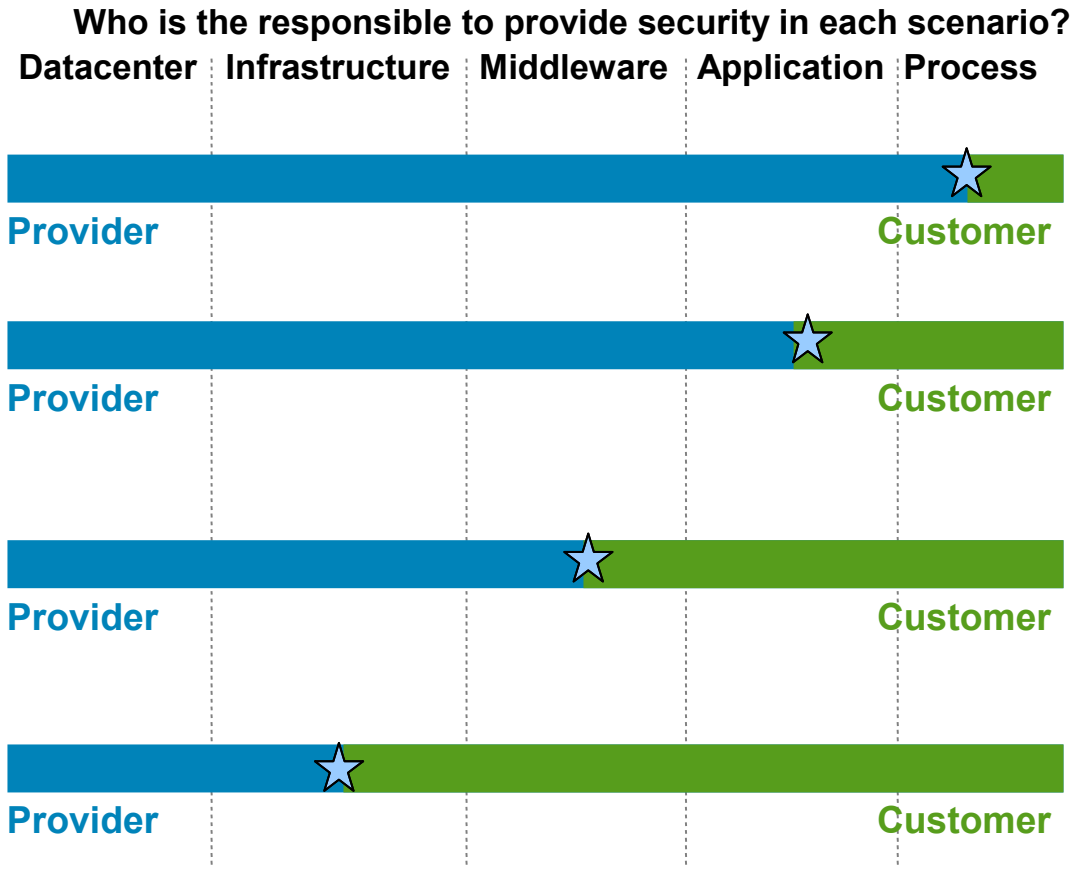
- Quality of protection adapted to risk
- Direct visibility and control
- Significant level of assurance

Today's clouds are primarily here:

- Lower risk workloads
- One-size-fits-all approach to data protection
- No significant assurance
- Price is key

The responsiblity to provide security depends on the cloud service model





SLA between Provider and Customer determines the responsibility

Typical Security Requirements for Cloud Environments

Governance, Risk Management and Compliance

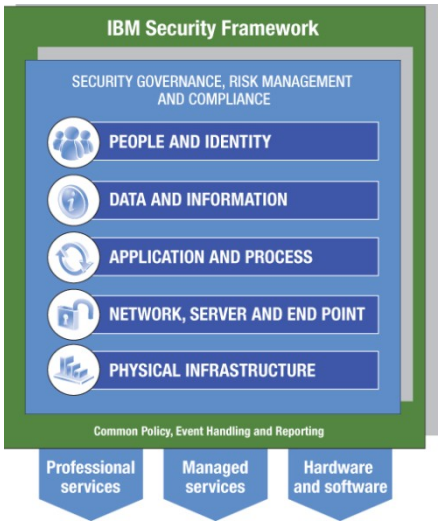
- **External Auditing** (SAS 70(2), ISO27001, PCI)
- **Data access and auditing logs segregated by customer**
- **Effective reporting of security incidents by individual customer**
- Visibility for change and incident management processes
- SLAs, risk transfer from customer to provider
- Forensics support

Application and Process

- Specific security requirements for applications developed for cloud environments
- Compliance with application development best practices

Physical Infrastructure

- Physical access control and monitoring



People and Identities

- **Privileged user monitoring**
- **Identity Federation:** coordination of authentication and authorization processes with the corporation or third parties
- **Single Sign-on**

Data and Information

- **Data segregation**
- Control of the geographical location of the data

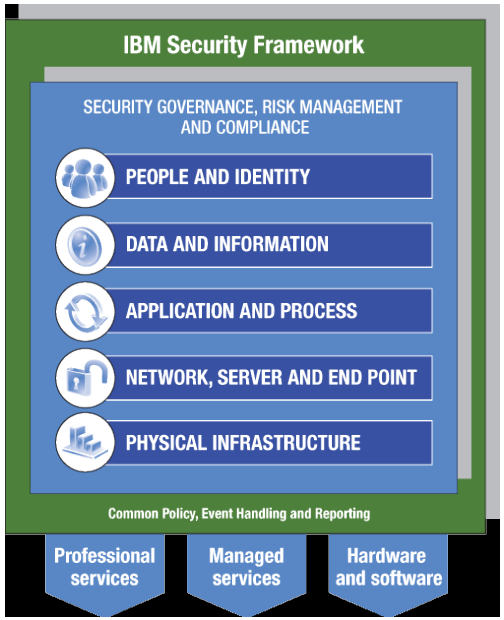
Network, Server and endpoint

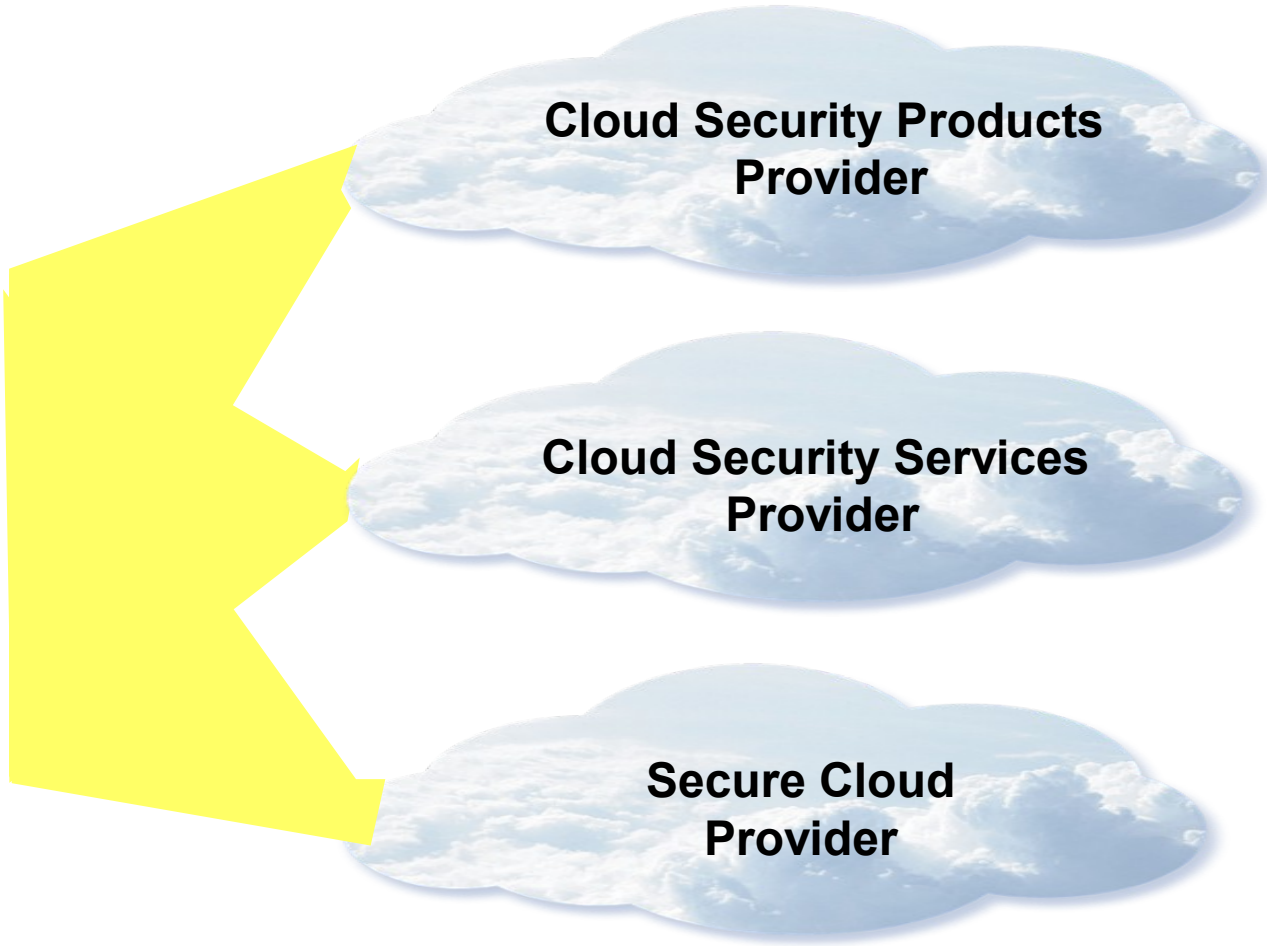
- **Isolation** among domains from different customers
- **Virtual domains:** domains with different security policies
- Intrusion detection and prevention capabilities
- Vulnerability management

Based on customer interviews and analyst reports

IBM Strategy for Cloud Security

IBM Security Framework





IBM Cloud Security Guidance document

- Based on cross-IBM research and customer interaction on cloud security
- Highlights a series of best practice controls that should be implemented
- Broken into 7 critical infrastructure components:
  - *Building a Security Program*
  - *Confidential Data Protection*
  - *Implementing Strong Access and Identity*
  - *Application Provisioning and De-provisioning*
  - *Governance Audit Management*
  - *Vulnerability Management*
  - *Testing and Validation*

Obrigado!

- Cezar Taurion
- **ctaurion@br.ibm.com**
- **www.ibm.com/developerworks/blogs/page/ctaurion**
- **www.computingonclouds.wordpress.com**
- **@ctaurion**
- **Facebook, Linkedin**

- Marcus Vinicius Itala Ferreira
- **marcusv@br.ibm.com**
- **www-03.ibm.com/security/cloud-security.html**