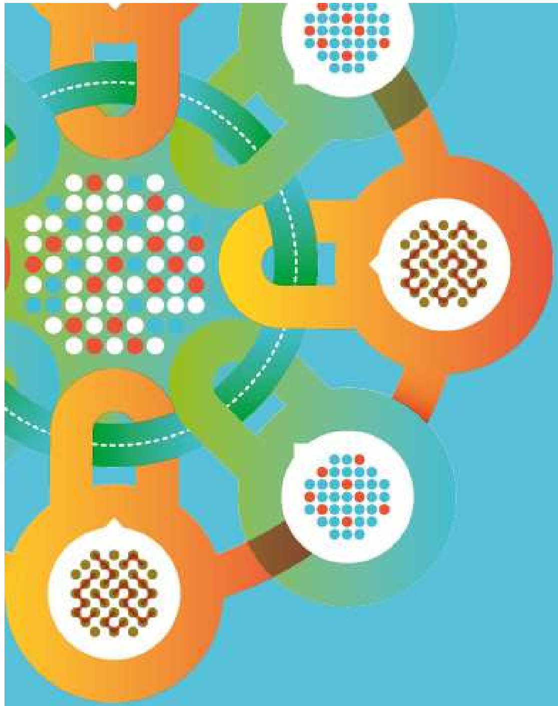


IBM Forum Segrate - Milano

18 settembre:
Missione Sicurezza

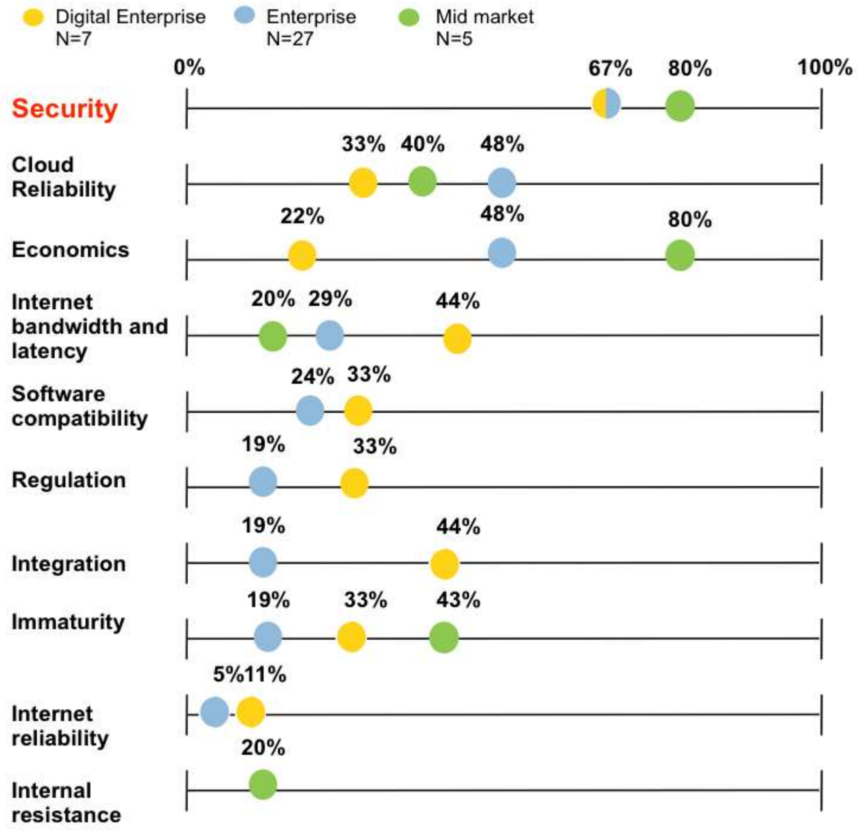
Identifica e combatti i rischi con la Security Intelligence IBM

Tiziano Airoldi

Security in the move to Cloud

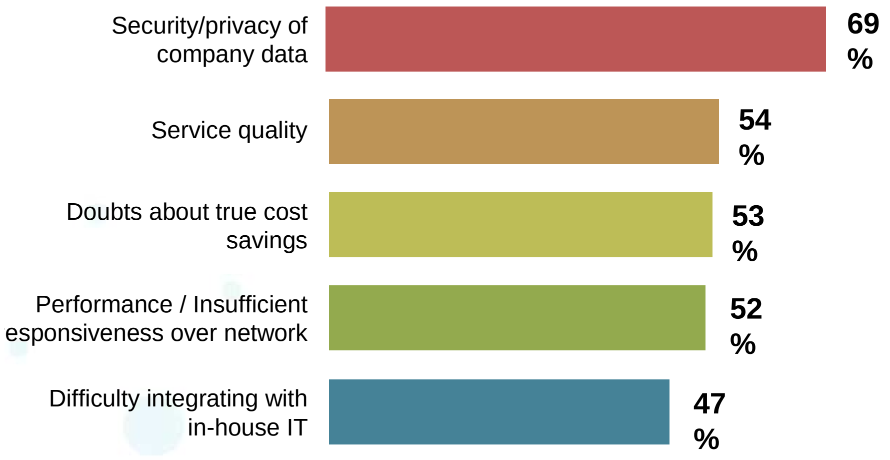
Security is a top concern with cloud computing…

The tale of two studies shows that Security is the number one inhibitor to customers adopting cloud technologies.



Source: Oliver Wyman Interviews

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

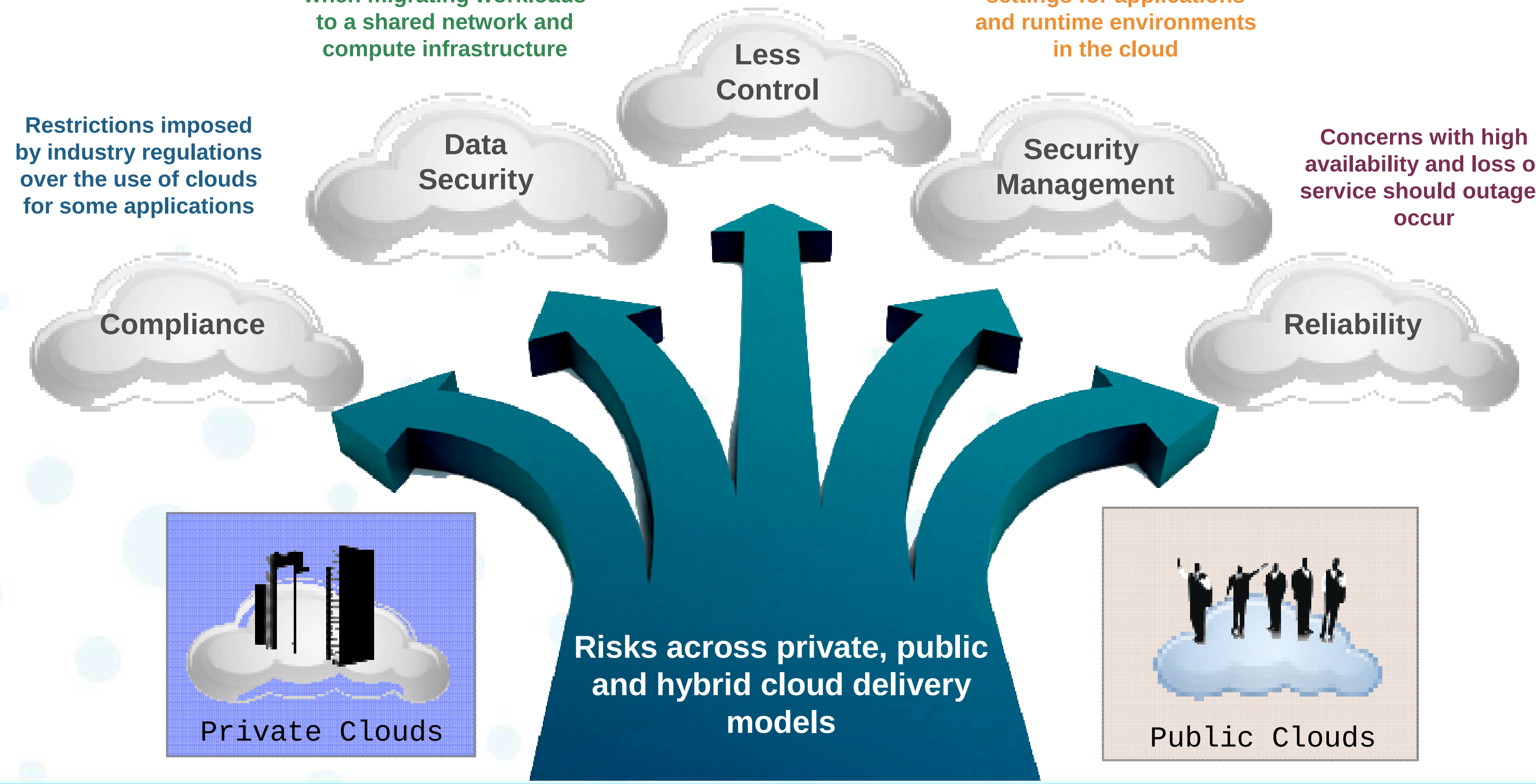


Percent rating the factor as a significant barrier (4 or 5)

Respondents could select multiple items

Source: IBM Market Insights, *Cloud Computing Research*, July 2010. n=1,090

New Risks introduced by cloud computing



Restrictions imposed by industry regulations over the use of clouds for some applications

Compliance

Challenges with an increase in potential unauthorized exposure when migrating workloads to a shared network and compute infrastructure

Data Security

Where the information is located and stored, who has access rights, how access is monitored & managed, including resiliency

Less Control

Control needed to manage firewall and security settings for applications and runtime environments in the cloud

Security Management

Concerns with high availability and loss of service should outages occur

Reliability

Private Clouds

Risks across private, public and hybrid cloud delivery models

Public Clouds

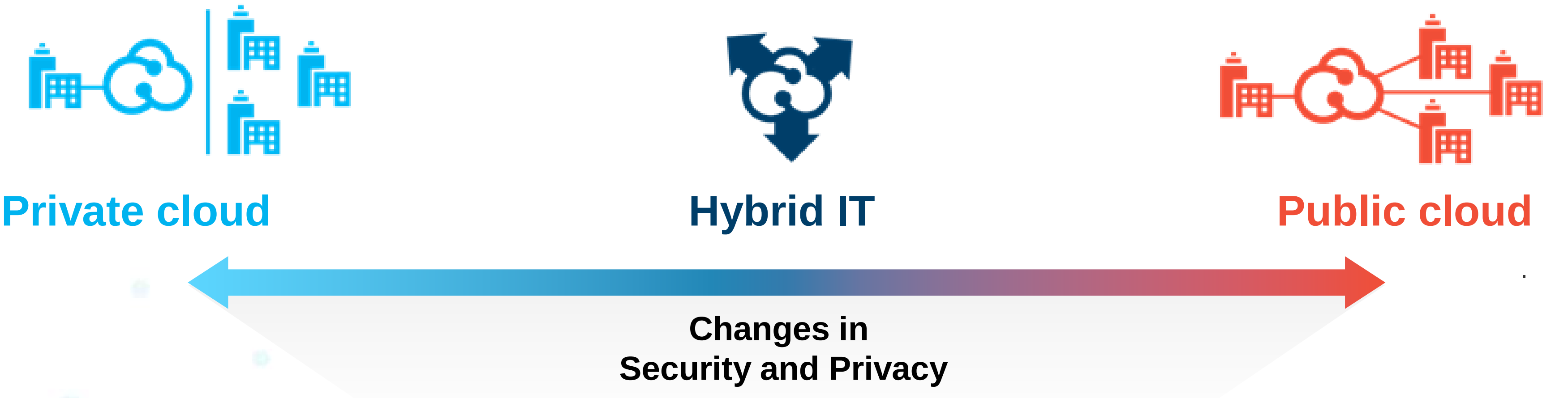
Some Worry about cloud & security ….

Cloud computing raises questions about maintaining the security and privacy of information assets

- How can I find out **where** data is located?
- How can I make sure data isn't **lost**? Is data portable?
- Data sensitivity vs data **persistence**?
- How does the cloud deal with **encryption**?
- How do we ensure that only the **right people** see the right information? **Insider threats**?
- How do auditors observe **what is going on**?
- Who is responsible for **compliance** audits?
- What happens if authentication **requirements** are stronger than the cloud?
- What if **corporate security** settings (FW, AV, IDS, etc.) are different than the cloud?
- How do you **integrate** legacy content in the cloud?
- How about **isolation failure** between tenants?
- Is the **management** web interface secure?
- How about Cloud **downtime**? They do happen!
- Am I **locked-in** ?
- .....

Cloud computing changes the way we think about security

In a cloud environment, access expands, responsibilities change, control shifts, and the speed of provisioning IT resources increases - **greatly affecting all aspects of security**



While the security concerns are often shared across the different cloud models the responsibility changes from consumer to provider and this can present unique challenges.

- *High multi-tenancy and data separation*
- *Image management and compliance*
- *Security of the virtual / hypervisor layer*
- *Virtual network visibility*
- *Need for Service level agreements (SLAs)*

- *Provider responsibility for infrastructure*
- *Customization of security controls*
- *Visibility into day-to-day operations*
- *Access to logs and policies*
- *Applications and data are publically exposed*

Adoption patterns are emerging and each pattern has its own set of key security concerns

Infrastructure as a Service (IaaS): Cut IT expense and complexity through cloud data centers

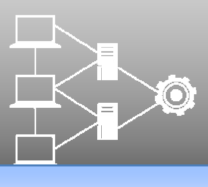
Cloud Enabled Data Center

Integrated service management, automation, provisioning, self service

Key security focus:

Infrastructure

- Logical & physical isolation
- Manage datacenter identities
- Secure virtual machines
- Encrypt stored data
- Patch default images
- Monitor logs on all resources
- Defend network perimeters



Platform-as-a-Service (PaaS): Accelerate time to market with cloud platform services

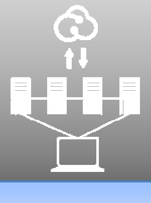
Cloud Platform Services

Pre-built, pre-integrated IT infrastructures tuned to application-specific needs

Key security focus:

Data and Information

- Secure shared databases
- Protect private information
- Build secure applications
- Keep an audit trail
- Integrate existing security
- Manage platform identities
- Harden exposed applications



Innovate business models by becoming a cloud service provider

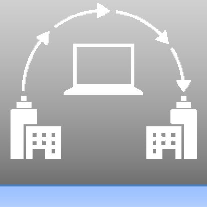
Cloud Service Provider

Advanced platform for creating, managing, and monetizing cloud services

Key security focus:

Governance and Compliance

- Isolate multiple cloud tenants
- Secure portals and APIs
- Manage security operations
- Build compliant data centers
- Offer backup and resiliency
- Integrate system management & security



Software as a Service (SaaS): Gain immediate access with business solutions on cloud

Business Solutions on Cloud

Capabilities provided to consumers for using a provider's applications

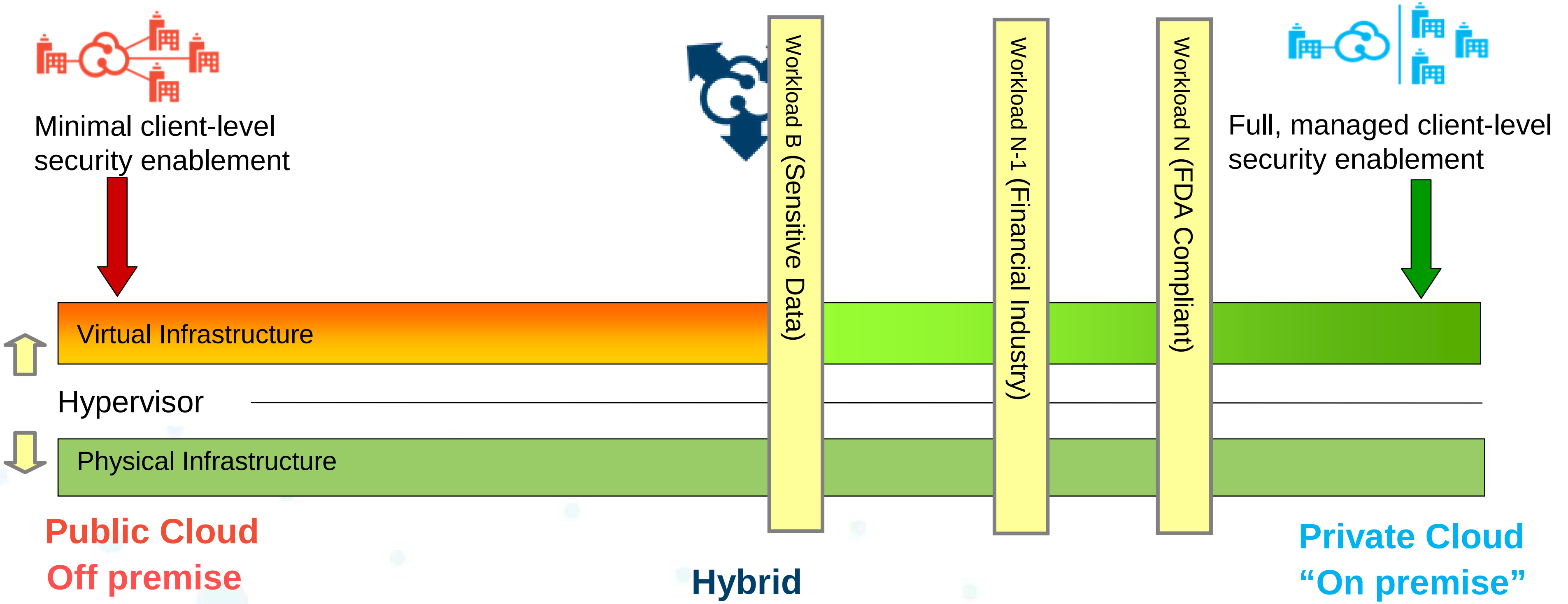
Key security focus:

Applications and Identity

- Proper user authentication
- Harden exposed web apps
- Securely federate identity
- Deploy access controls
- Encrypt communications
- Encrypt data (motion/rest)
- Manage application policies
- Audit & compliance testing

Security Intelligence – threat intelligence, user activity monitoring, real time insights

Security "sophistication" increases with workload deployment



Minimal client-level security enablement

Full, managed client-level security enablement

Workload B (Sensitive Data)

Workload N-1 (Financial Industry)

Workload N (FDA Compliant)

Virtual Infrastructure

Hypervisor

Physical Infrastructure

Public Cloud
Off premise

Hybrid

Private Cloud
"On premise"

With more sophisticated & complicated workloads, we see an increase in the need for

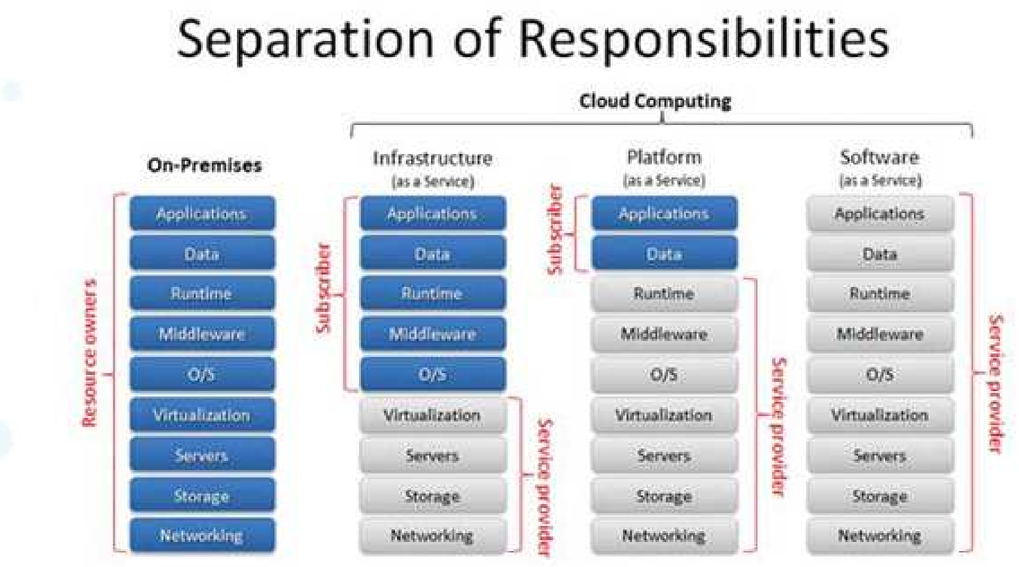
- a risk base approach is needed
- security to be enabled & integrated across cloud infrastructure
- seamless transition from one environment to another (hybrid enablement)
- regulatory compliance & certification requirement to be considered

Security responsibilities in the Cloud

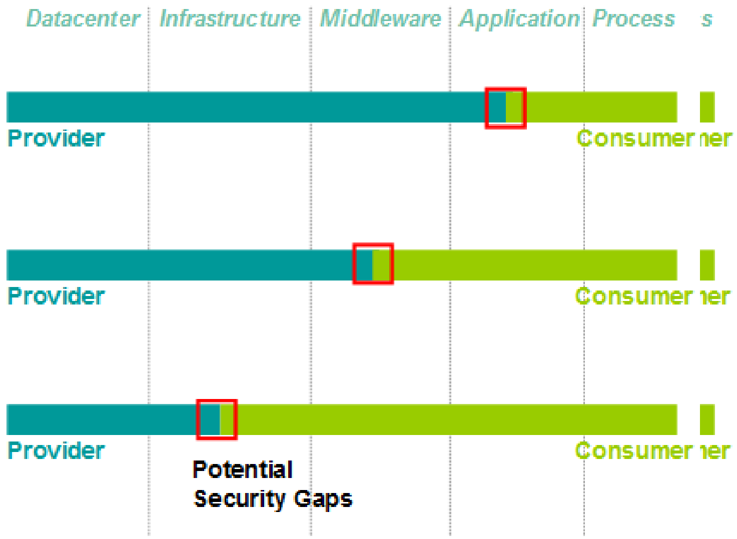
Cloud security is more a relationship issue than a technical issue

Interested parties need to really look at the diligence of the cloud provider and also the cloud provider has to meet the customer half way in terms of being flexible and transparent about their approach to security

Getting effective cloud security has to do with the health of the relationship between the customer and the provider and their ability to work together to address security risks



Cloud Patterns



Minimizing the risks of cloud computing requires a strategic approach

Define a cloud strategy with security in mind

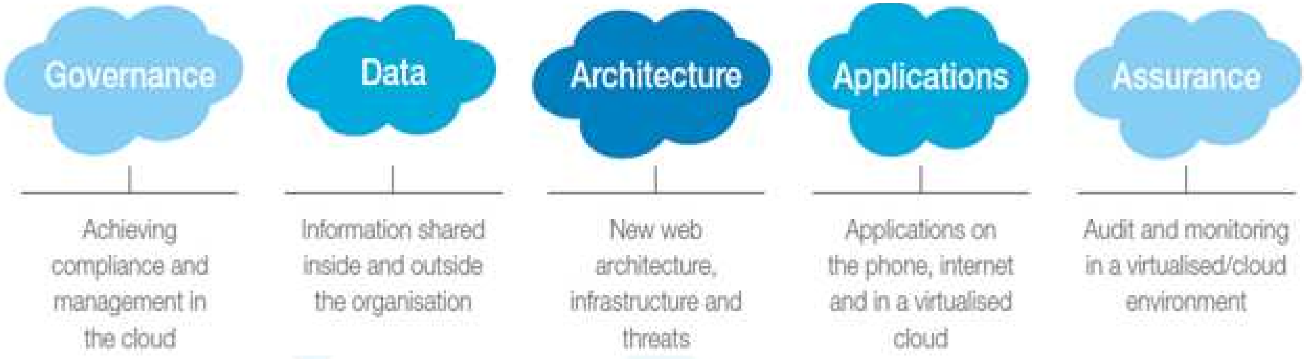
- Identify the different workloads and how they need to interact
- Which models are appropriate based on their security and trust requirements and the systems they need to interface to?

Identify the security measures needed

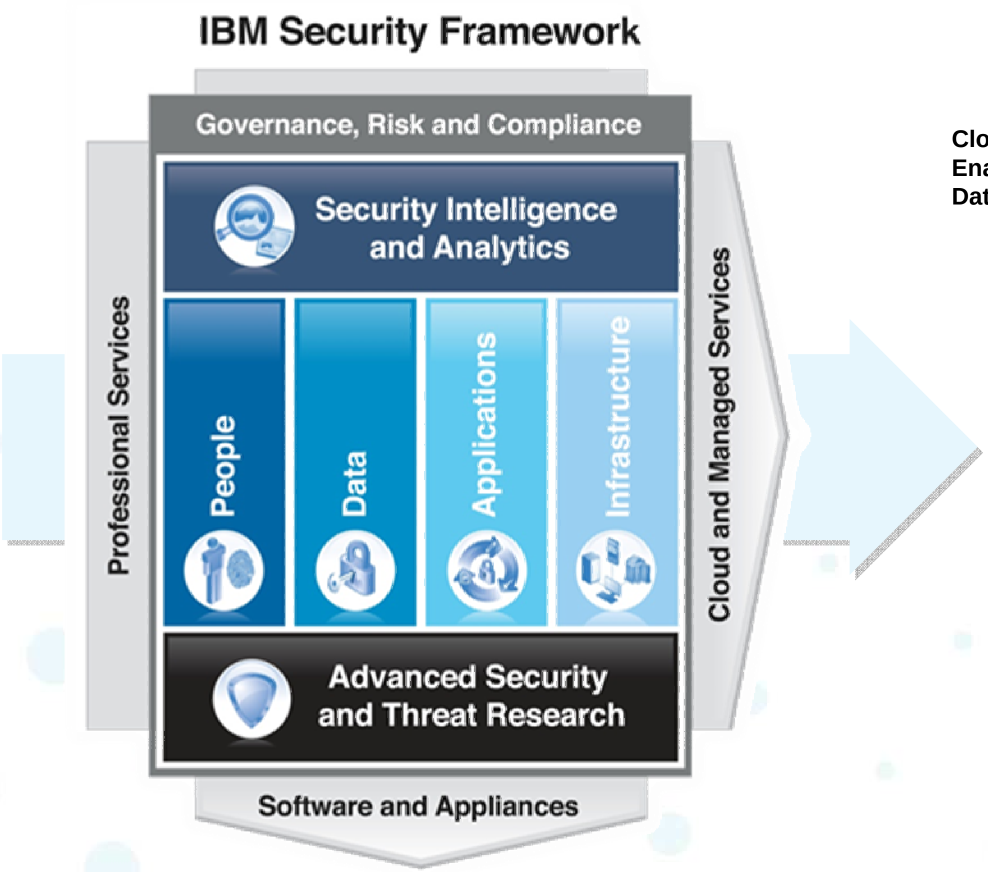
- Using a methodology such as the IBM Security Framework allows teams to measure what is needed in areas such as governance, architecture, applications and assurance

Enabling security for the cloud

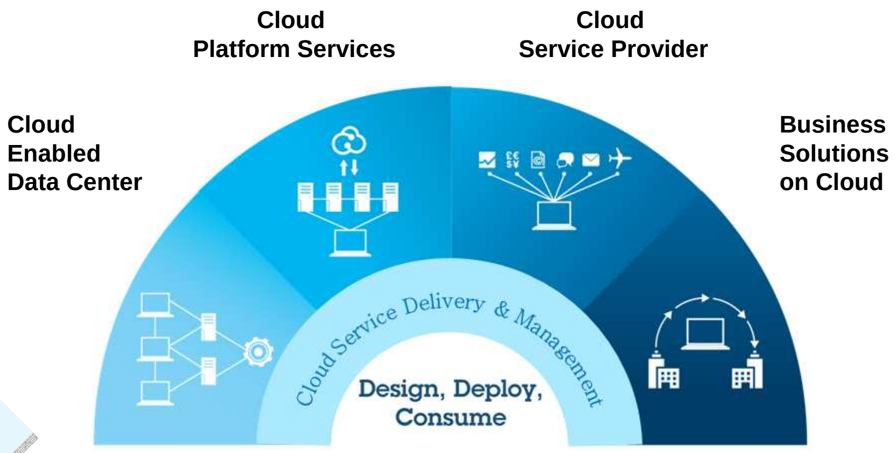
- Define the upfront set of assurance measures that must be taken
- Assess that the applications, infrastructure and other elements meet the security requirements, as well as operational security measures


Governance
Achieving compliance and management in the cloud
Data
Information shared inside and outside the organisation
Architecture
New web architecture, infrastructure and threats
Applications
Applications on the phone, internet and in a virtualised cloud
Assurance
Audit and monitoring in a virtualised/cloud environment

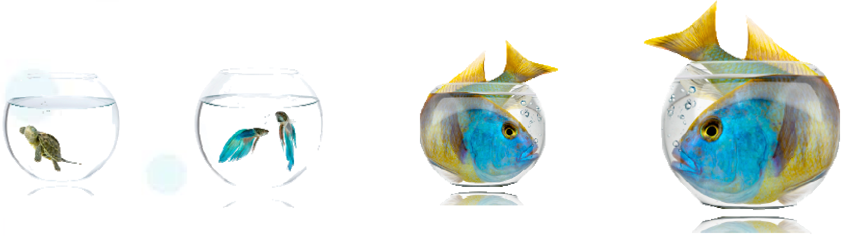
IBM's breath of experience and security capabilities are being applied to all cloud adoption patterns


IBM Security Framework
Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

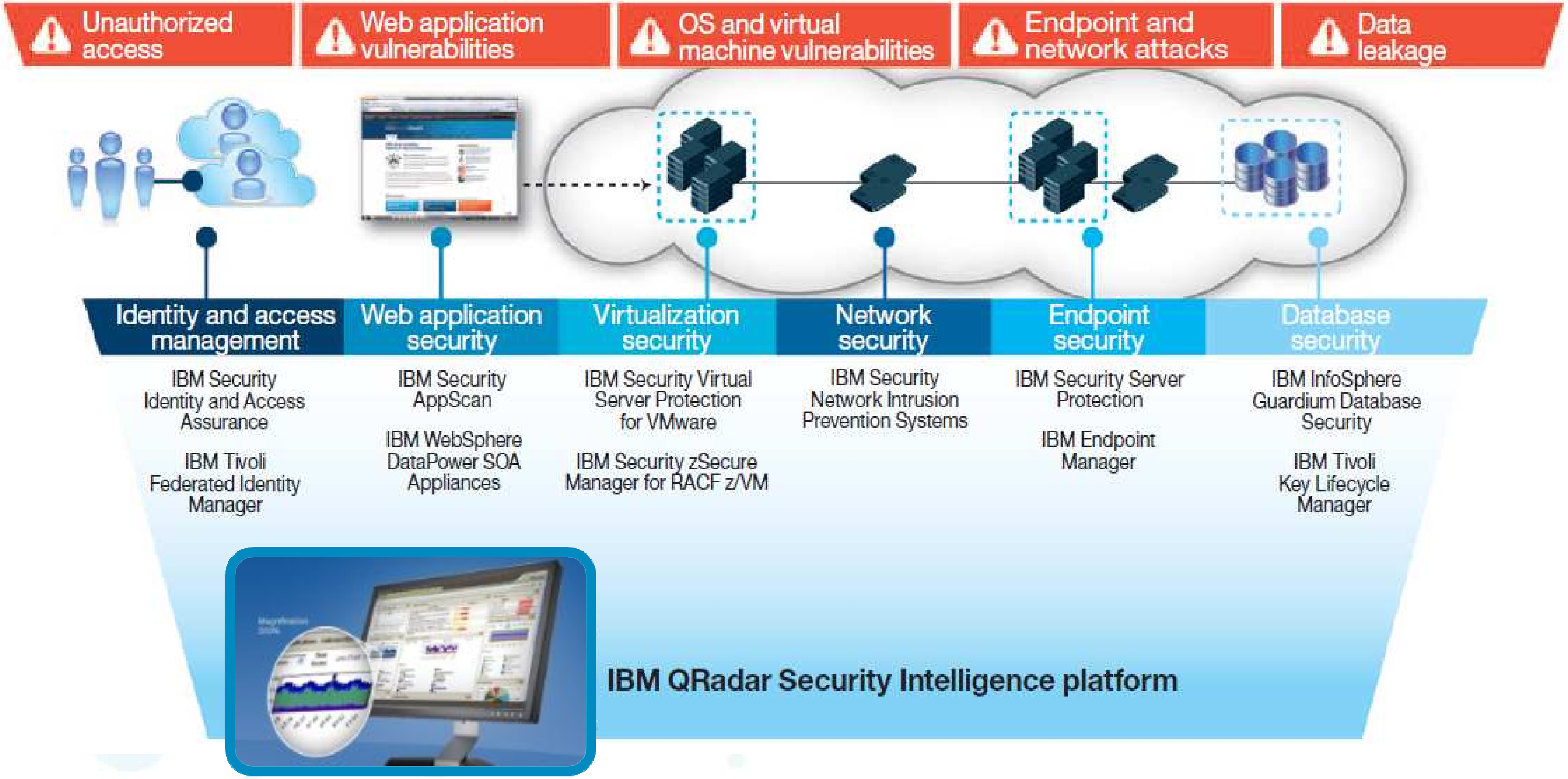
IBM Cloud Security
One Size Does Not Fit All


Cloud Enabled Data Center
Cloud Platform Services
Cloud Service Provider
Business Solutions on Cloud
Cloud Service Delivery & Management
Design, Deploy, Consume

Different security controls are appropriate for different cloud needs - the challenge becomes one of integration, coexistence, and recognizing what solution is best for a given workload.



IBM safeguards the cloud with flexible, layered security solutions



Unauthorized access

Web application vulnerabilities

OS and virtual machine vulnerabilities

Endpoint and network attacks

Data leakage

Identity and access management

IBM Security Identity and Access Assurance

IBM Tivoli Federated Identity Manager

Web application security

IBM Security AppScan

IBM WebSphere DataPower SOA Appliances

Virtualization security

IBM Security Virtual Server Protection for VMware

IBM Security zSecure Manager for RACF z/VM

Network security

IBM Security Network Intrusion Prevention Systems

Endpoint security

IBM Security Server Protection

IBM Endpoint Manager

Database security

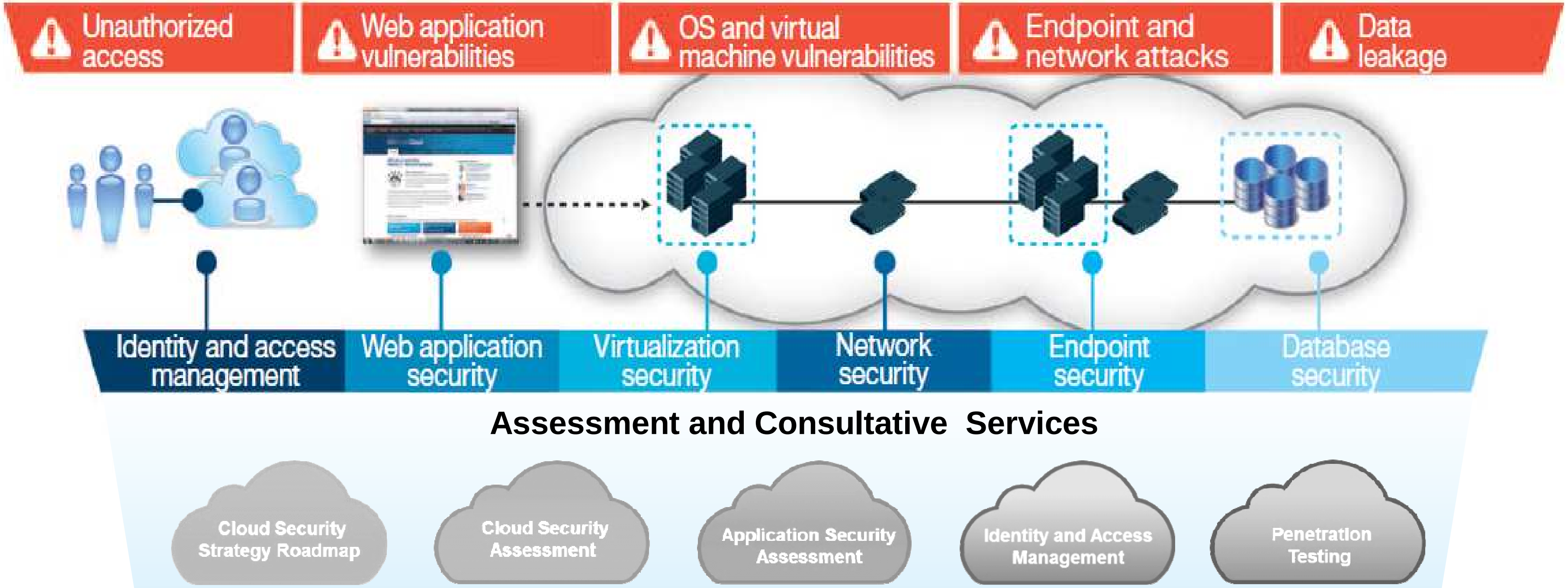
IBM InfoSphere Guardium Database Security

IBM Tivoli Key Lifecycle Manager

IBM QRadar Security Intelligence platform

Protect against threats, regain visibility and demonstrate compliance with activity monitoring and security intelligence

IBM provides consulting, assessment, and managed services for enterprises and Cloud service providers



Unauthorized access
Web application vulnerabilities
OS and virtual machine vulnerabilities
Endpoint and network attacks
Data leakage
Identity and access management
Web application security
Virtualization security
Network security
Endpoint security
Database security

Assessment and Consultative Services

Cloud Security Strategy Roadmap
Cloud Security Assessment
Application Security Assessment
Identity and Access Management
Penetration Testing

Managed Security Services for Cloud Environments

- Secure Network Communications
- Critical Server Protection
- Vulnerability Scanning
- User Activity Monitoring
- Identity and Access Management
- Incident Response
- 24x7 Security Management

How to start …. some advices

1. Look at your workloads with a risk base approach
   - workload risk profile vs service criticality
   - data sensitivity
   - availability requirements
   - compliance requirements
   - security requirements (CIA) vs internal & external compliance mandates
2. Consider to engage expertise to help build your security cloud strategy
3. Negotiate good SLA .. for you ☺
4. Evaluate cloud provider backup and recovery capabilities
5. Consider where are they located in the world
6. Evaluate data persistency
7. Evaluate your way out conditions ☺
8. Assess internet management application for vulnerability

IBM is working with clients as both a cloud service provider and trusted advisor for cloud security strategy & design

Secure IBM Clouds

IBMSmartCloud

Reduce costs.
Improve service delivery.
Enable business innovation.

Leveraging IBM's deep security skill set, hosting and strategic outsourcing experience, broad security portfolio, history of security innovation, and commitment to client trust as the foundation for building security into all cloud offerings.

IBM Cloud Reference Model
(Foundational Security Controls)

Capabilities

Knowledge

IBM Security Solutions

New Customer Initiatives Require Enhanced Security

Leading portfolio of products and services to help secure cloud environments. Allows customers to address concerns when adopting private, public and hybrid cloud services by adopting security controls to match requirements of the workload.

IBM Security Framework
(Cloud Security On Ramps)

Tiziano Airoldi

IBM Senior Certified Executive Architect

Global Technology Services
Security & Privacy

IBM Italia S.p.a

Mobile: +39-335.7506675
Mail: *tiziano.airoldi@it.ibm.com*