

# IBM Perspectives on Cloud Security

Presented by: Donald Kneitel

North America Security Services Executive

[kneiteld@us.ibm.com](mailto:kneiteld@us.ibm.com), 678-644-9053



## Outline

- Introduction to Cloud Computing
- IBM Security and Cloud Workloads
- Example Cloud Patterns
- Considerations for Cloud Implementation

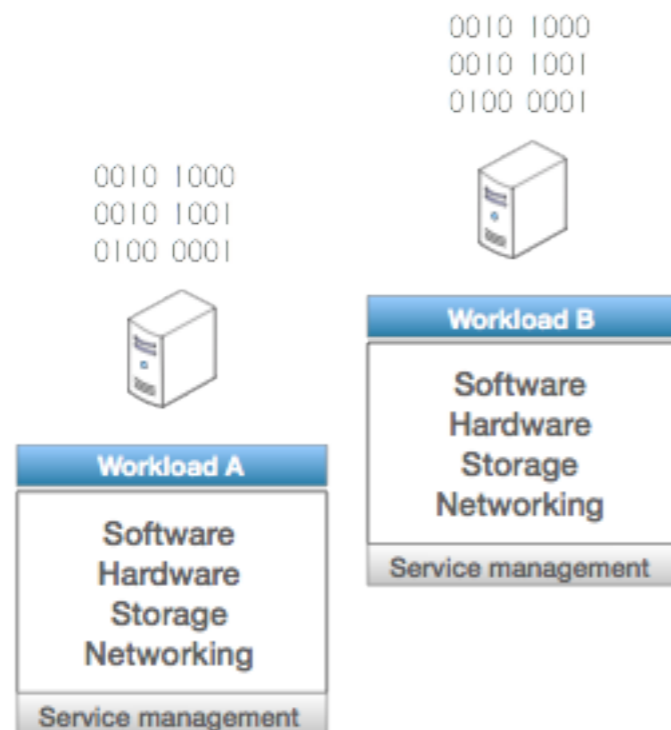


## Introduction to Cloud Computing

# Cloud: Consumption & Delivery Models Optimized by Workload

“**Cloud**” is a new consumption and delivery model inspired by consumer Internet services.

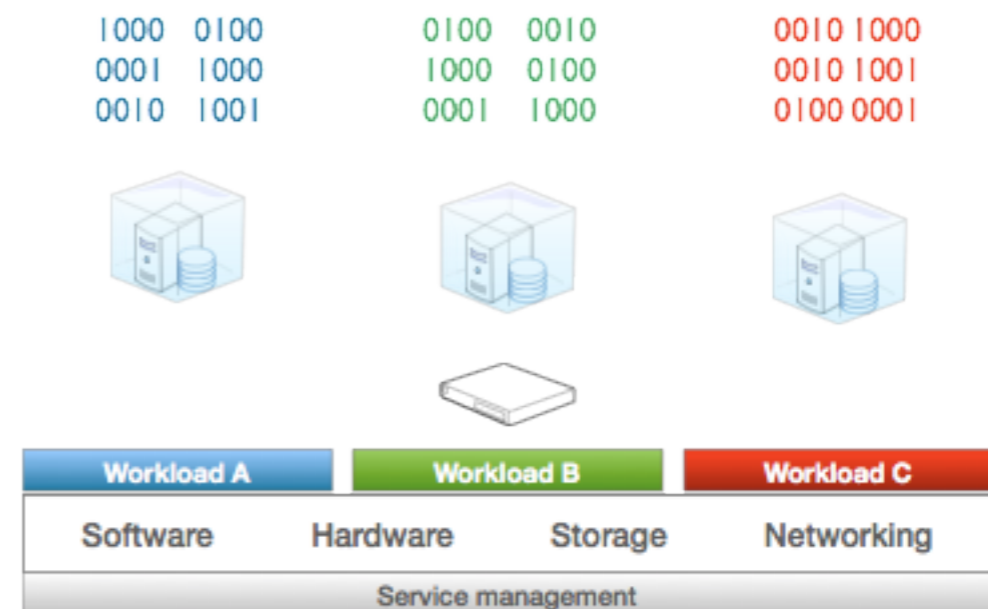
## Without Cloud Computing



## With Cloud Computing



- Virtualized resources
- Automated Service management
- Standardized services
- Location Independent
- Rapid Scale
- Self-service



# IT Benefits from Cloud Computing are Real...

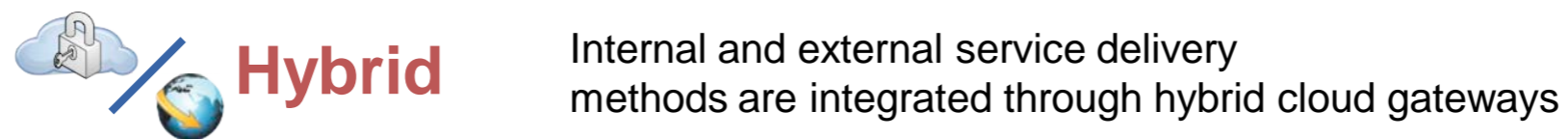
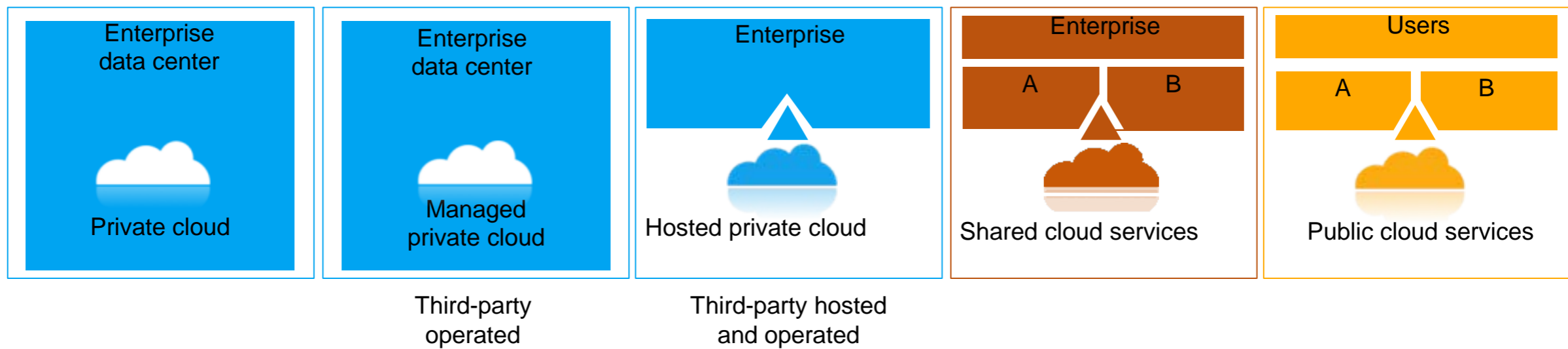
Results from IBM cloud computing engagements



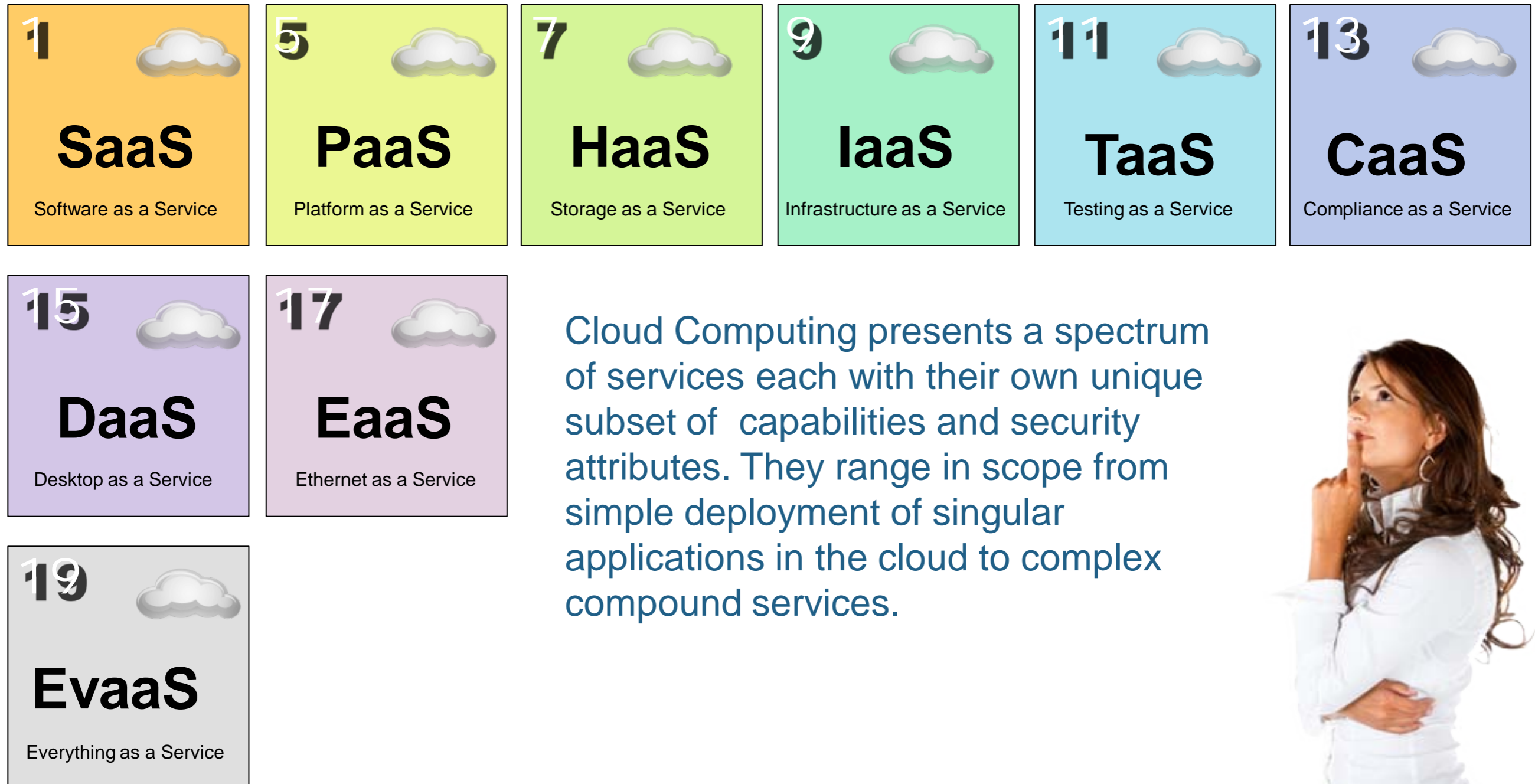
<b>Increasing speed and flexibility</b>	Test provisioning	Weeks	Minutes
	Change management	Months	Days/hours
	Release management	Weeks	Minutes
	Service access	Administered	Self-service
	Standardization	Complex	Reuse/share
	Metering/billing	Fixed cost	Variable cost
	<b>Reducing costs</b>	Server/storage utilization	10–20%
Payback period		Years	Months

Source: Based on IBM and client experience.

# Spectrum of Deployment Options for Cloud Computing

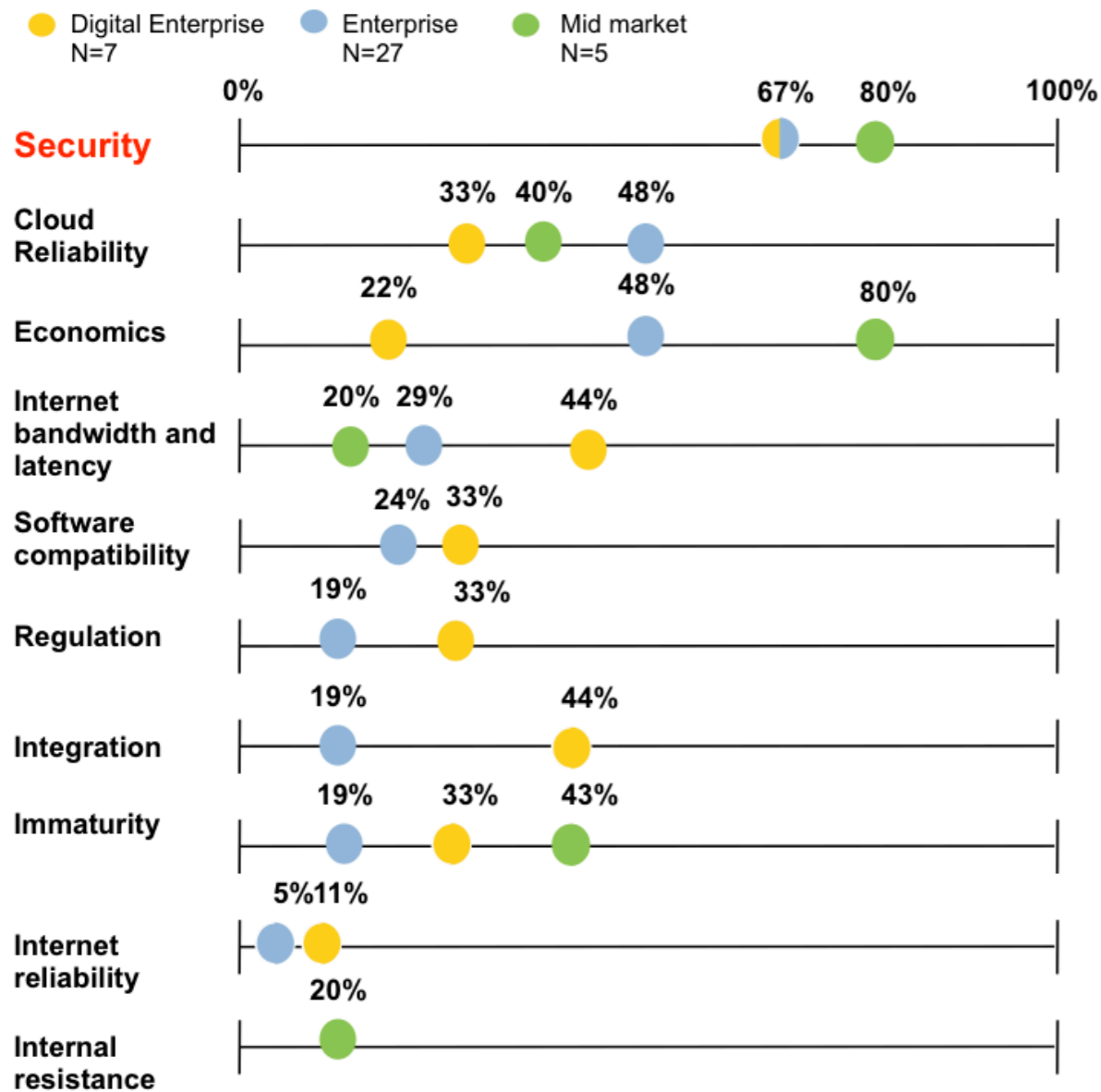


# Spectrum of Cloud based Services



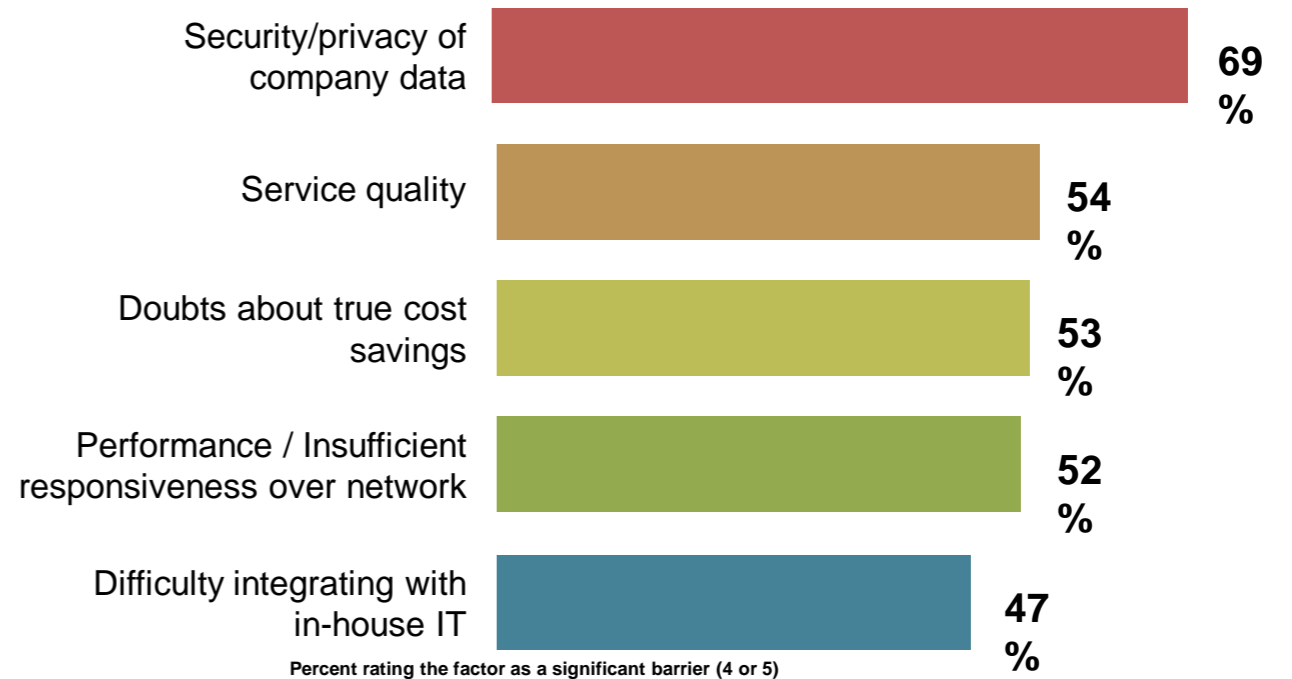
# Security is a top concern with cloud computing...

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?



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

# Cloud Security in the News

**“Organizations can easily lose 1-2% of revenues when mission-critical services go down even for a short amount of time.”**

<http://itmanagement.earthweb.com/netsys/article.php/3894891/Top-10-Reasons-Cloud-Computing-Deployments-Fail.htm>



Cloud-based note-taking service Evernote has admitted that a "series of hardware failures" means that around a fifth of its customers have lost some of their notes for good.

<http://www.bit-tech.net/news/bits/2010/08/11/evernote-coughs-to-data-loss/1>

Earlier this month a [security breach at AT&T](#) exposed the email addresses of more than 100,000 iPad users. Most customers blamed Apple, but the problem was with AT&T's cloud service.



<http://itmanagement.earthweb.com/netsys/article.php/3894891/Top-10-Reasons-Cloud-Computing-Deployments-Fail.htm>



Apple claims developer manipulated the system to make his books appear to forty two (42) of the top fifty (50) electronic books. While claiming the developer did not have access to personal data, Apple advised customers to watch for suspicious data.

<http://cloutage.org/incidents/100-apple-inc-apple-app-store>

Google reports massive compromise... Attack occurred through a zero-day hole in Microsoft Internet Explorer ...Google's cloud password system, "Gaia", had been compromised during the ordeal, potentially exposing the information of millions of google users.



<http://cloutage.org/incidents/4-google-inc-gmail>

**“Customers don't expect to be fully indemnified, but they want the penalty to hurt providers enough that they get motivated to prevent failures. The liability must be a deterrent to failure.**

Julio Gómez  
founderInnovation  
Councils LLC

# Risks introduced by cloud computing



# Some sources of Cloud threats

## Service Providers

Many product listings on Amazon.com were blank or partially there for more than a couple hours. During that time customers' shopping carts also displayed as being empty. The cause of the outage was not released by Amazon, but at a potential loss of \$51,400 a minute when their site is offline they were surely racing to get it back up.

[cloutage.org](http://cloutage.org)

## External Threats

With \$6 and a homemade "Thunder Clap" program, security experts David Bryan and Michael Anderson managed to take down their client's server with the help of Amazon's EC2 cloud infrastructure.

[http://blogs.computerworld.com/16708/thunder\\_in\\_the\\_cloud\\_6\\_cloud\\_based\\_denial\\_of\\_service\\_attack?source=rss\\_blogs](http://blogs.computerworld.com/16708/thunder_in_the_cloud_6_cloud_based_denial_of_service_attack?source=rss_blogs)

## Insider Threats

A recent survey ([PDF](#)) from Cisco ([News - Alert](#)) [found](#) that more employees are working around IT security policies to use personal hardware and software that's not sanctioned by the company.

<http://it.tmcnet.com/topics/it/articles/95585-employees-sneaking-past-it-run-unsupported-apps.htm>

## Service Level Agreements

**“We're in a progression of technology innovation, where we're only looking at the assets, capabilities and costs; but people are starting to realize there are higher consequences to a breach now than in 2005”**

Drew Bartkiewicz, vice president of technology and new media markets for The Hartford Financial Services Group



## IBM Security and Cloud Workloads

## Workload Centric Approach to Cloud Security

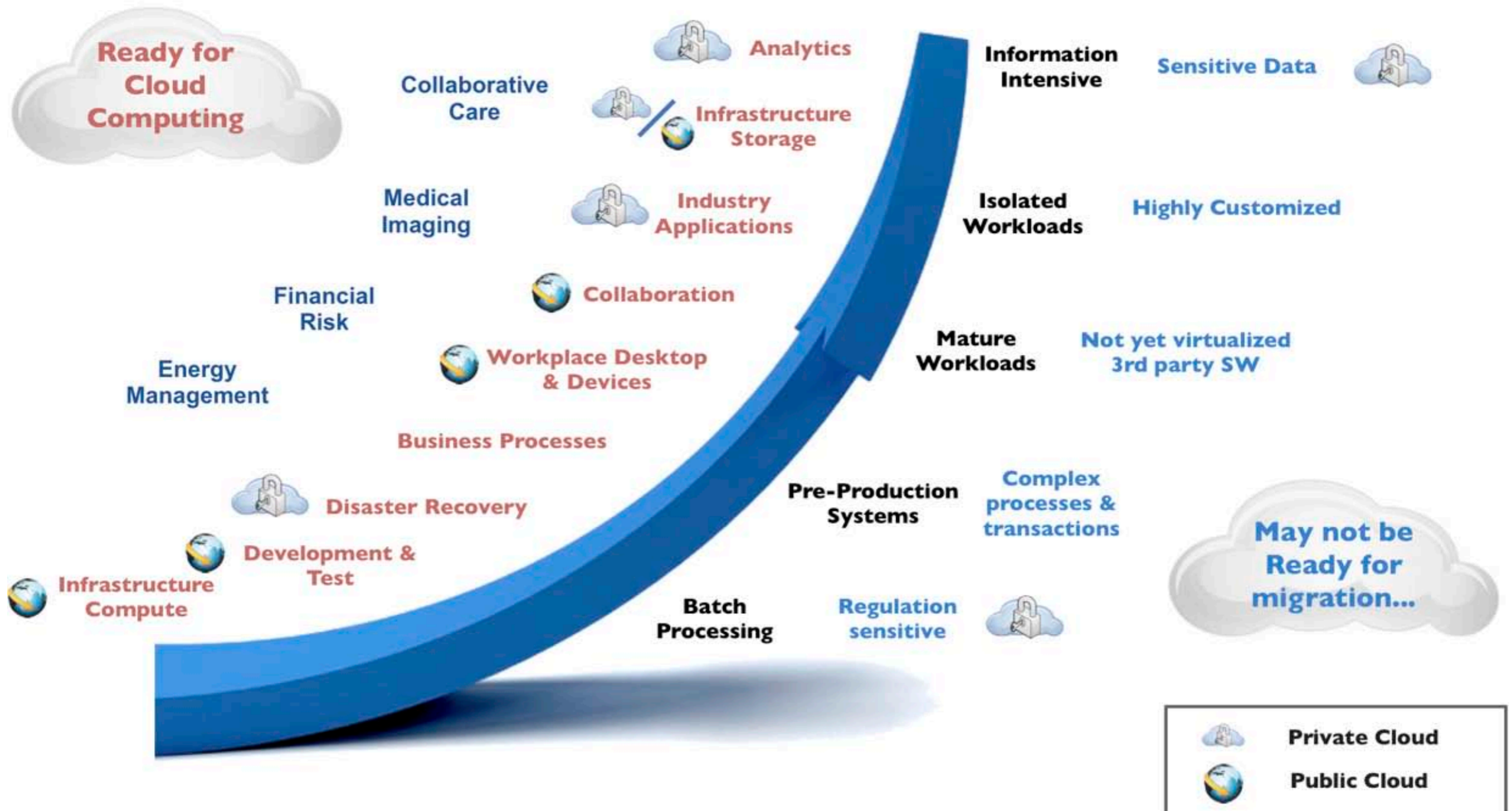
As cloud computing technology matures, organizations will shift from generic cloud security models to workload specific models. The concept being that the security needs of each organization are not based on the cloud type or vendor but on the data and the protections necessary to protect that data.

Some Industries which are already applying this concept are:

- **Healthcare**
- **Finance**
- **Government**



# Workloads may be at Different Levels of Cloud Readiness



## Example of Health Care related requirements

**Addressing Health Care data in the cloud boils down to a handful of key elements (*Data Protection, Audit and Logging, and Least Privileged management*)**

Example of requirements for Healthcare compliance:

- Encryption of Personal Data over public networks
- Mitigating controls or Encryption to protect data at rest
- Access Logging
- User Validation
- Forensic Capabilities
- Regular control audits.
- Data Protection and Isolation



## Example of Finance related requirements

**Financial Organizations have similar concerns to health care requirements.**

Example of requirements for PCI in the Cloud:

- Encryption of Personal Data over public networks
- Mitigating controls or Encryption to protect data at rest
- Access Logging
- User Validation
- Forensic Capabilities
- Regular control audits.

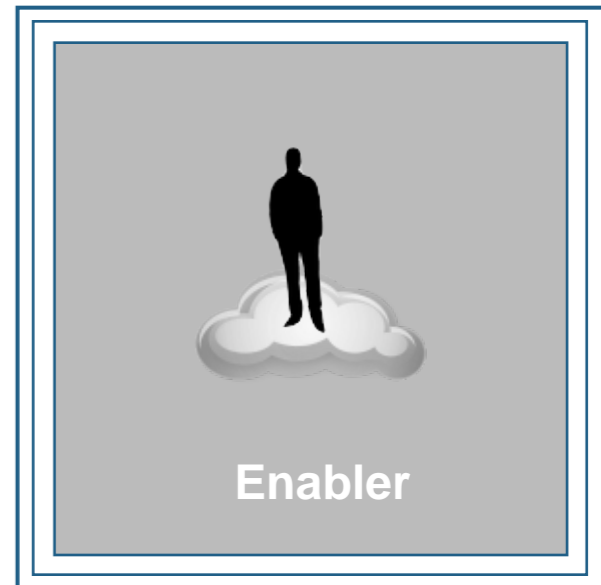


# IBM Strategy for Cloud Security

## IBM Security Framework: *Risk management-based approach to security*



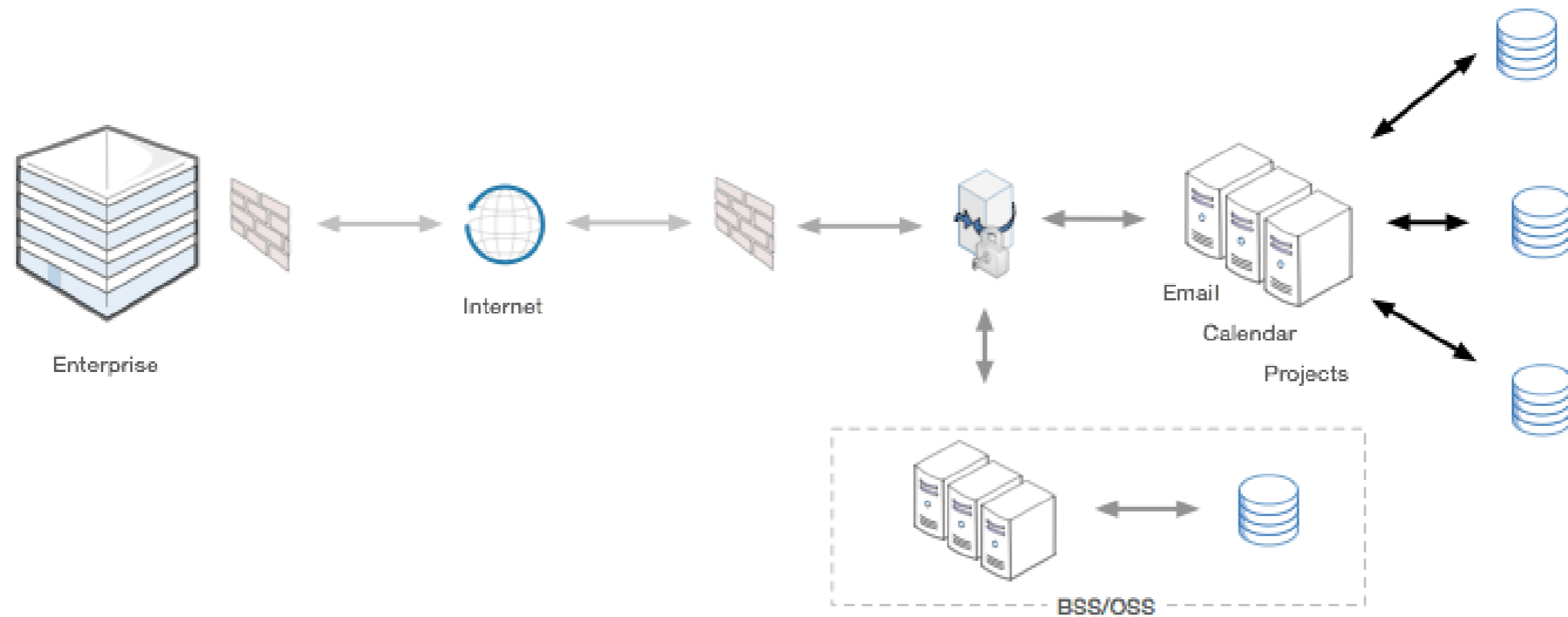
***Secure by Design...  
build security in  
from the beginning***





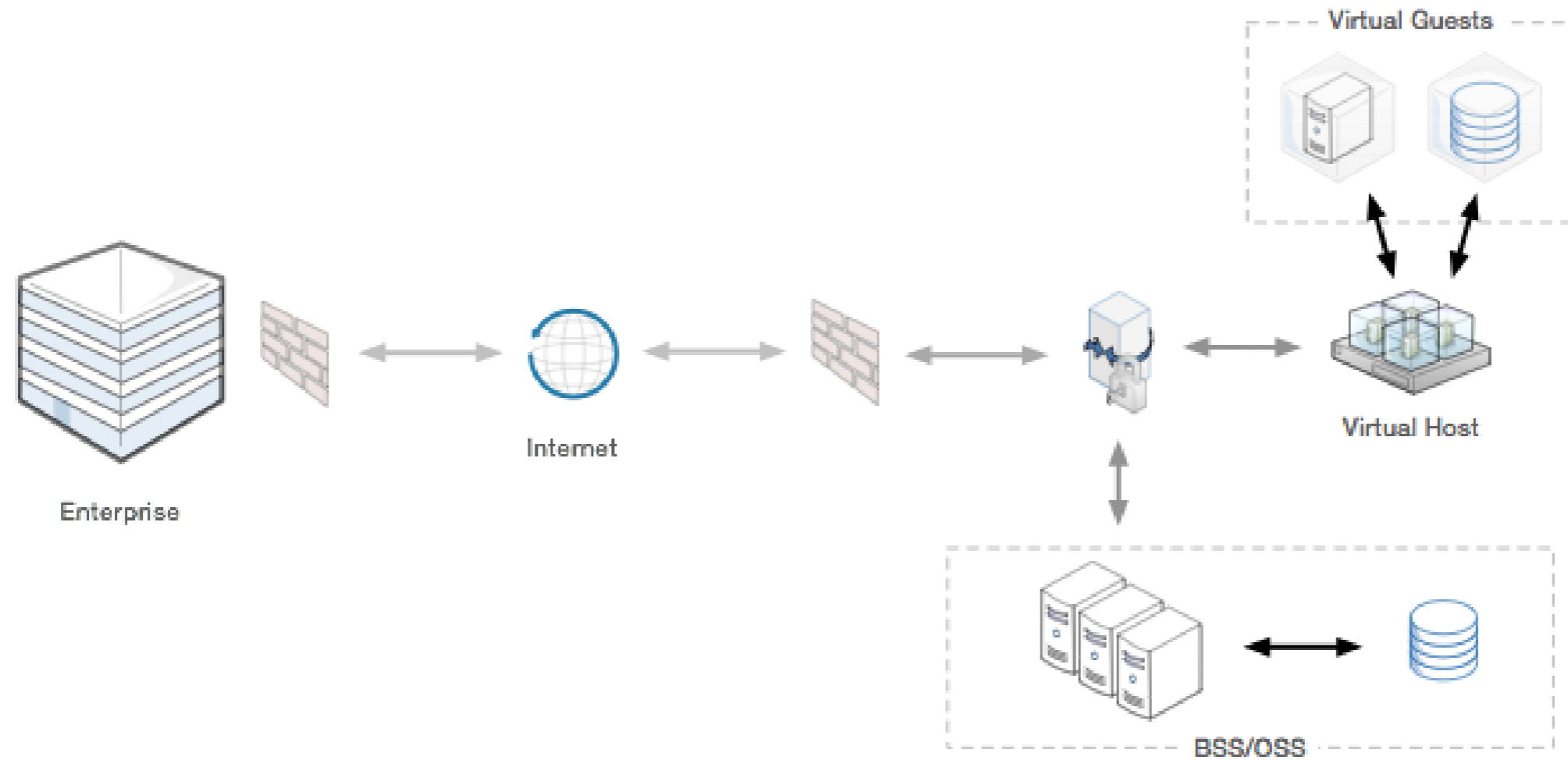
## Example Cloud Patterns

# Applying Security to Software as a Service



Governance & Compliance	People & Identity	Data & Information	Application & Process	Network, Server & Endpoint
<ul style="list-style-type: none"> <li>▪ Policy Management</li> <li>▪ Security Information Event Management</li> <li>▪ Directory Integration</li> <li>▪ Usage and Accounting</li> </ul>	<ul style="list-style-type: none"> <li>▪ Access Management</li> <li>▪ Application Gateway</li> <li>▪ User Management</li> <li>▪ Directory Services</li> <li>▪ Federated Identity</li> </ul>	<ul style="list-style-type: none"> <li>▪ Data Protection</li> <li>▪ Data Encryption</li> <li>▪ E-Discovery</li> <li>▪ Data Redaction</li> <li>▪ Resiliency Services</li> </ul>	<ul style="list-style-type: none"> <li>▪ Vulnerability Scanning</li> <li>▪ Anti-Spam</li> <li>▪ Anti-Virus</li> <li>▪ Application Acceleration and analysis</li> </ul>	<ul style="list-style-type: none"> <li>▪ Intrusion Prevention</li> <li>▪ Firewalls</li> <li>▪ Network Isolation/routing</li> <li>▪ VPN connectivity</li> <li>▪ Data Leakage Prevention</li> </ul>

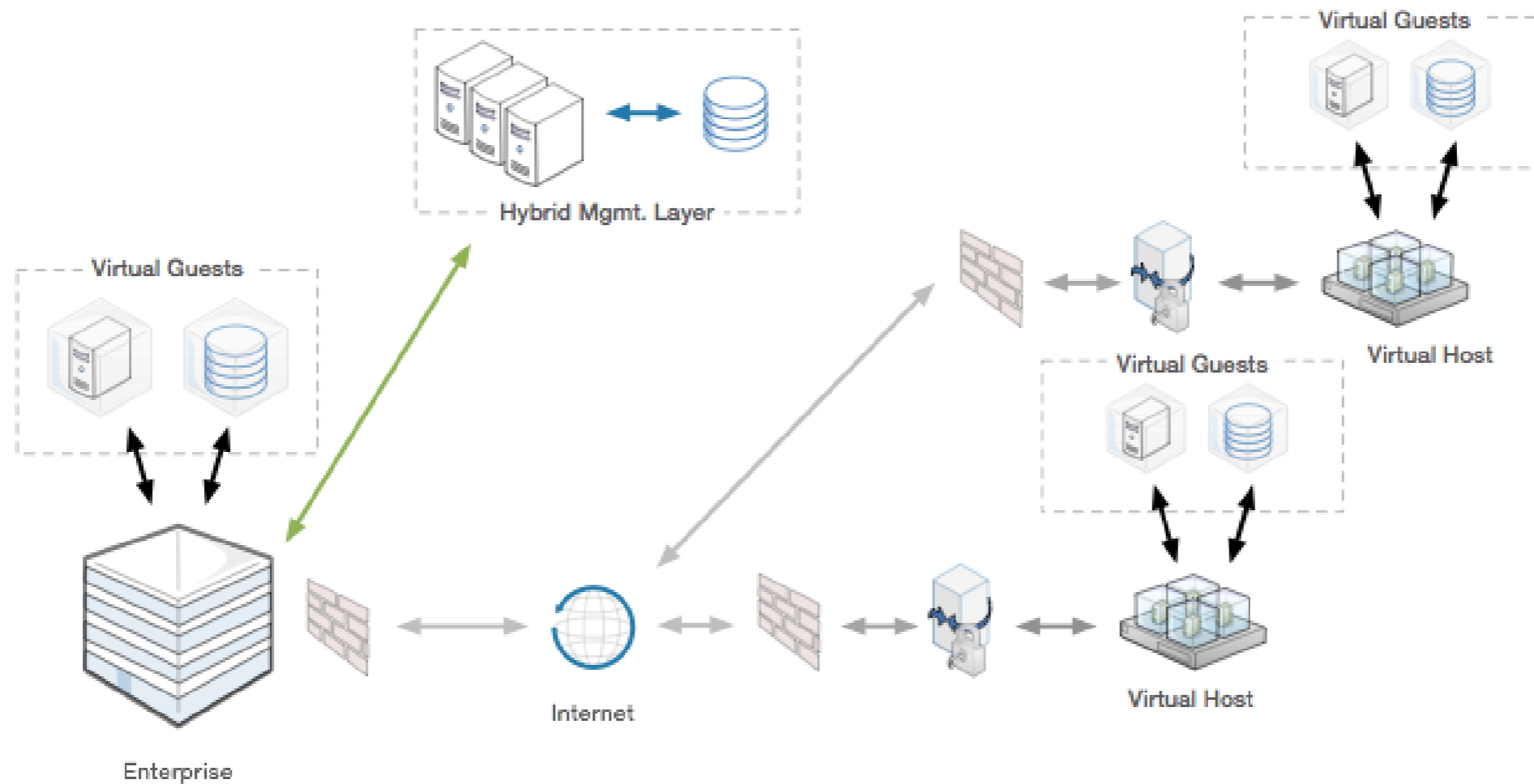
# Applying Security to Infrastructure as a Service



Governance & Compliance	People & Identity	Data & Information	Application & Process	Network, Server & Endpoint
<ul style="list-style-type: none"> <li>▪ Security Event Information Management</li> <li>▪ Security Policy Management</li> <li>▪ Directory Integration</li> <li>▪ Virtual Image Management</li> <li>▪ Utilization Monitoring</li> <li>▪ Integration API's</li> <li>▪ Image Migration Utilities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Tivoli Federated Identity Manager</li> <li>▪ Directory Services</li> <li>▪ Access Management</li> </ul>	<ul style="list-style-type: none"> <li>▪ Encryption Technologies</li> <li>▪ Data Protection Services*</li> <li>▪ E-Discovery Support</li> <li>▪ Image Destruction</li> <li>▪ Resiliency Services</li> </ul>	<ul style="list-style-type: none"> <li>▪ Vulnerability Scanning</li> </ul>	<ul style="list-style-type: none"> <li>▪ Intrusion Prevention</li> <li>▪ Data Leakage Prevention</li> <li>▪ Virtual Image Protection</li> <li>▪ Firewalls</li> <li>▪ Network Isolation/Routing</li> <li>▪ VPN Connectivity</li> <li>▪ Traffic Analytics</li> </ul>

\* optional based on virtual guest

# Hybrid as a Service and Security



Governance & Compliance	People & Identity	Data & Information	Application & Process	Network, Server & Endpoint
<ul style="list-style-type: none"> <li>▪ Security Event Information Management</li> <li>▪ Security Policy Management</li> <li>▪ Directory Integration</li> <li>▪ Virtual Image Management</li> <li>▪ Utilization Monitoring</li> <li>▪ Integration API's</li> <li>▪ Image Migration Utilities</li> </ul>	<ul style="list-style-type: none"> <li>▪ Tivoli Federated Identity Manager</li> <li>▪ Directory Services</li> <li>▪ Access Management</li> </ul>	<ul style="list-style-type: none"> <li>▪ Encryption Technologies</li> <li>▪ Data Protection Services*</li> <li>▪ E-Discovery Support</li> <li>▪ Image Destruction</li> <li>▪ Resiliency Services</li> <li>▪ Key Management</li> </ul>	<ul style="list-style-type: none"> <li>▪ Vulnerability Scanning</li> <li>▪ Asset management</li> <li>▪ License Management</li> </ul>	<ul style="list-style-type: none"> <li>▪ Intrusion Prevention</li> <li>▪ Data Leakage Prevention</li> <li>▪ Virtual Image Protection</li> <li>▪ Firewalls</li> <li>▪ Network Isolation/Routing</li> <li>▪ VPN Connectivity</li> <li>▪ Traffic Analytics</li> </ul>

\* optional based on virtual guest



## Considerations for Cloud Implementation

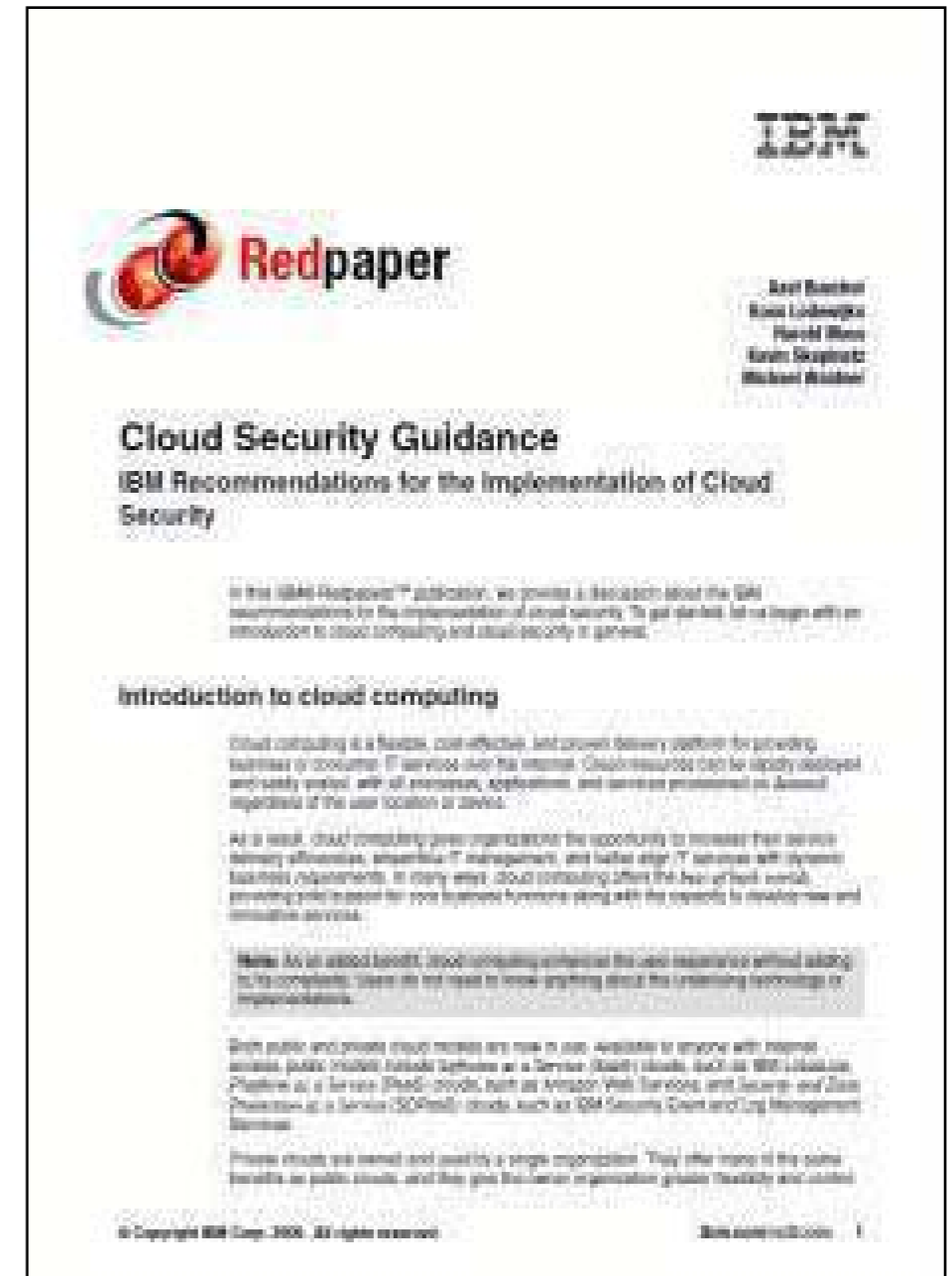
# IBM Cloud Security Guidance

Based on cross-IBM research and customer interaction on cloud security

Highlights a series of generic best practice controls, which can be further refined by workload

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



## Build a Security Program

Cloud Success is predicated on the creation of a holistic security approach which addresses not only the external cloud but the internal business requirements.

Key considerations are:

- Documented Security Plan
- Business Driven Security Requirements
- Service Level Agreement
- Vendor Compatibility
- Geo-Location Considerations

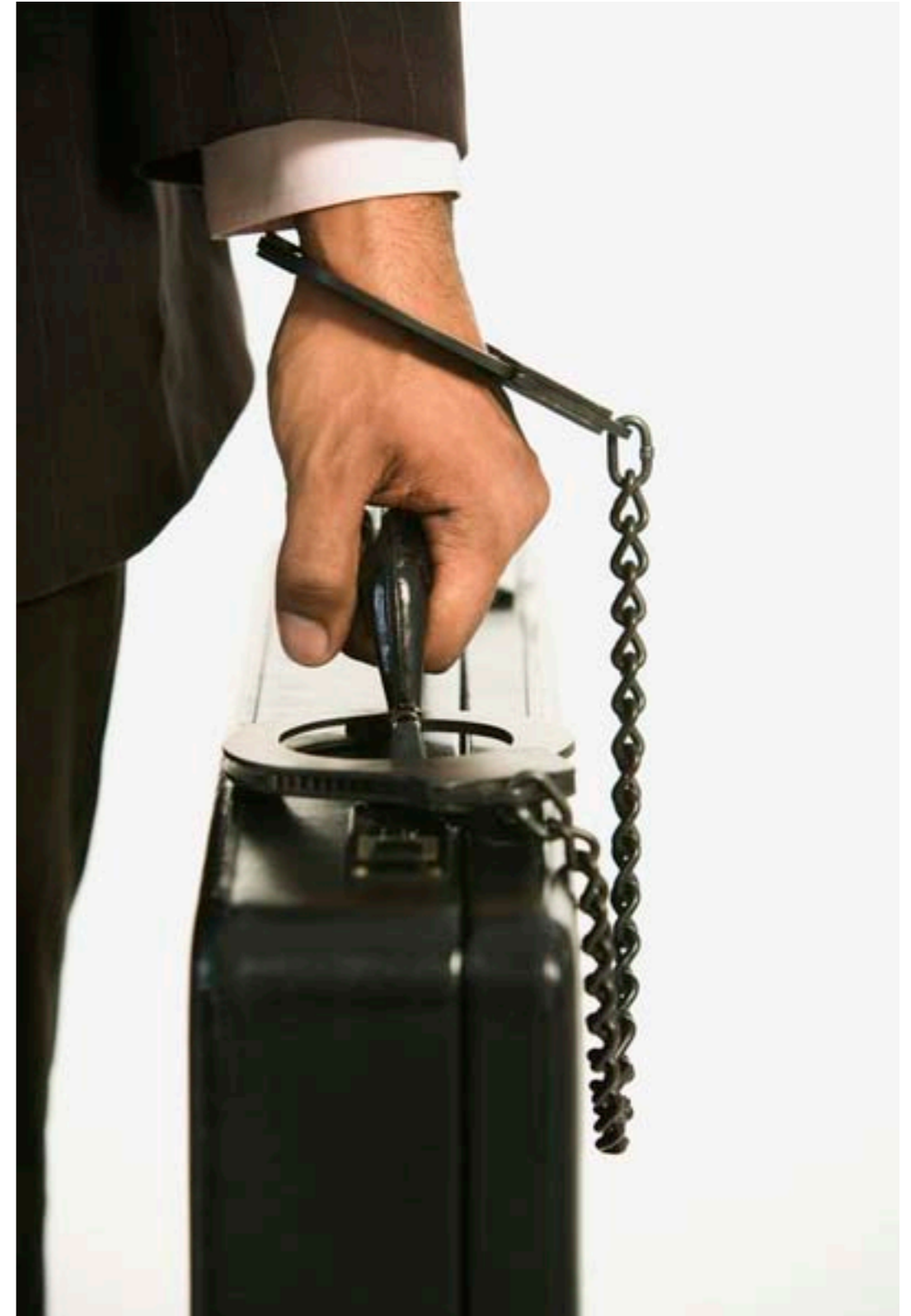


## Establish Data Security Requirements

Adoption of Cloud based technologies relies heavily on an organizations ability and confidence that it's data is protected in a trusted environment.

Key considerations are:

- Isolation Capabilities
- Encryption & Key Management
- Data Destruction and Handling
- Infrastructure Resiliency
- Data Portability



## Implement Strong Access and Identity

Identity and Access management form the foundation for any security program, in the cloud this becomes exponentially more difficult as cloud technologies could predicate multiple technologies.

Key considerations are:

- Federation of Identity
- Identity Synchronization
- Support for Least Privileged Access
- Host Access Privileges



## Application Provisioning and De-provisioning

Dependent on the cloud infrastructure type you may need to address provisioning and de provisioning of assets.

Key considerations are:

- Image Management
- Image Quality
- Image Destruction
- Patch/Version Management
- Portability of Image

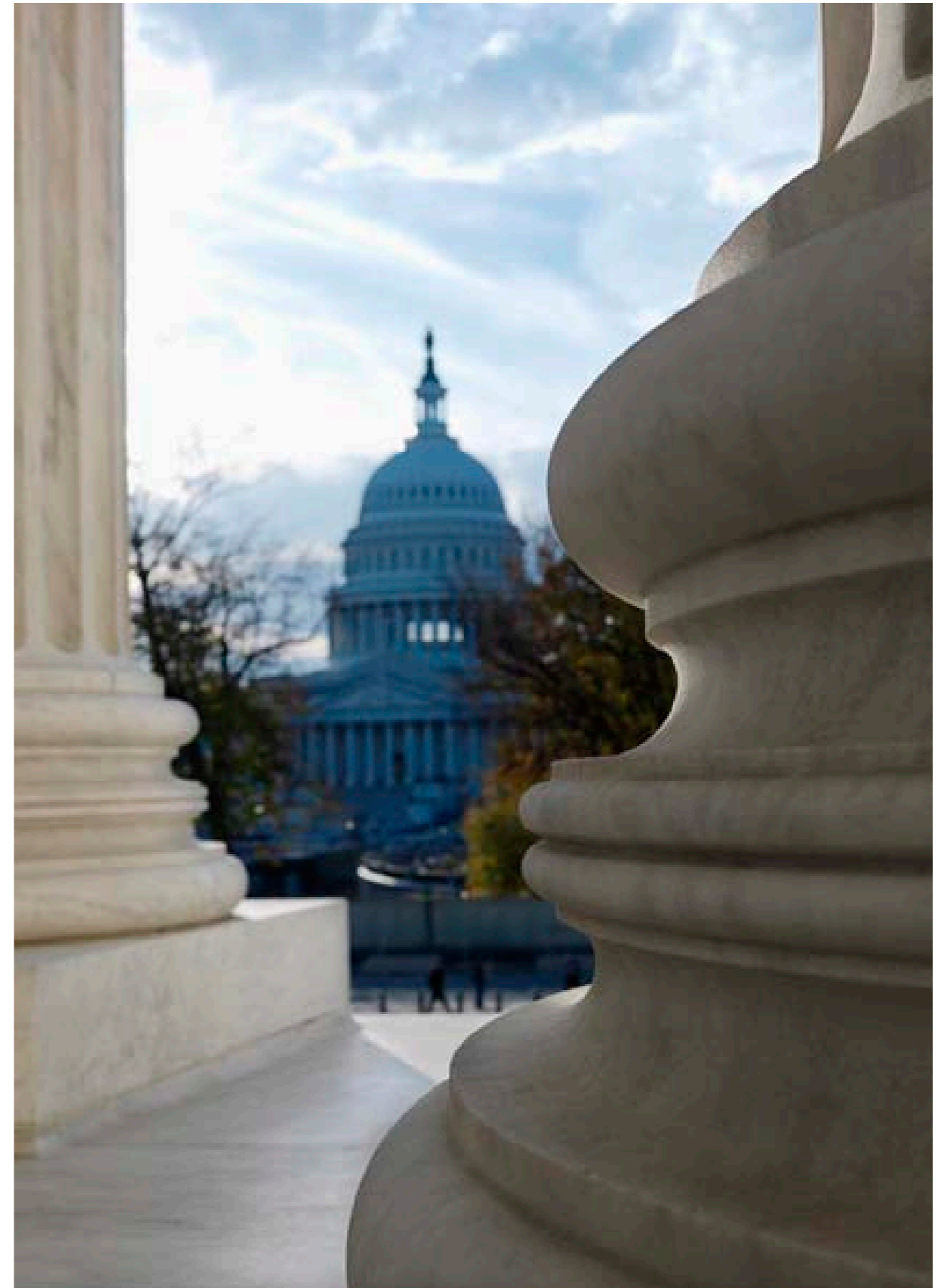


## Governance & Audit Management

Organizations are forced to adhere to numerous standards, movement to the cloud does not negate those requirements.

Key considerations are:

- Log Access
- Host standard Compliance
- Ability to Audit infrastructure
- Audit Integration
- Resiliency
- Business Efficacy



# Vulnerability Management

Vulnerability Management in the cloud provides a first line of defense protection.

Key considerations are:

- Firewalls
- Network Isolation/Security
- Intrusion Prevention
- Data Leakage Prevention
- Web App Gateway implementation



## Testing and Validation

Evaluating and Validating that the cloud infrastructure provides adequate protections.

Key considerations are:

- Vulnerability Scanning
- Security in Design
- Patch Management
- Asset Awareness

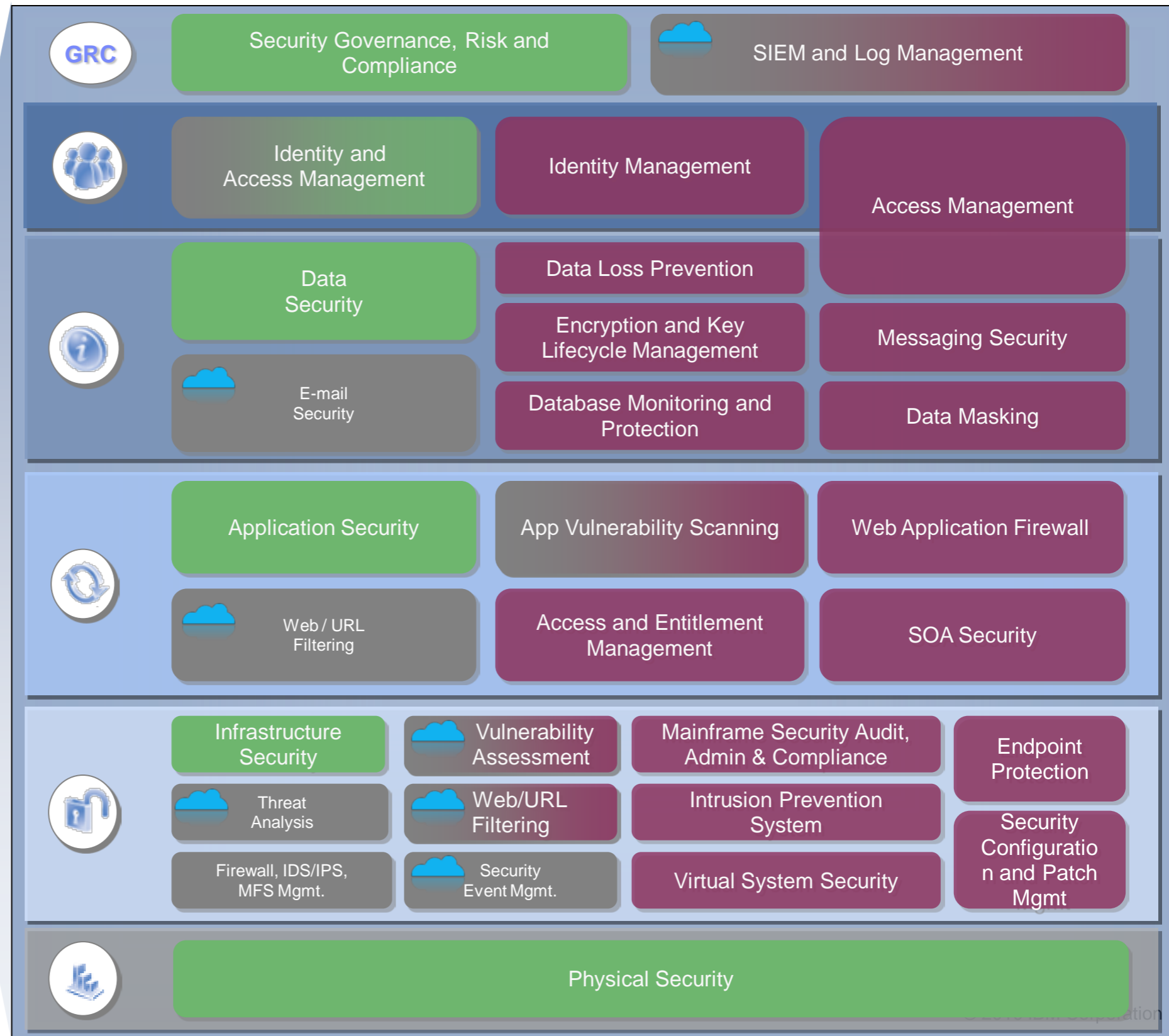


# IBM Security Solutions for the Cloud

= Professional Services

= Cloud-based & Managed Services

= Products



## Resources

- To learn more about IBM's cloud offerings...
  - Cloud computing: <http://www.ibm.com/ibm/cloud/>
  - Security solutions: <http://www-03.ibm.com/security/cloud-security.html>
- Whitepapers
  - [IBM Point of View: Security and Cloud Computing](#)
  - [Leveraging security from the cloud \(cloud-based security services\)](#)
  - [Cloud Security Guidance - IBM Recommendations for the Implementation of Cloud Security](#)

धन्यवाद

Hindi

多謝

Traditional Chinese

ขอบคุณ

Thai

Спасибо

Russian

Gracias

Spanish

---

**Thank You**

English

شكراً

Arabic

Merci

French

Obrigado

Brazilian Portuguese

Grazie

Italian

多谢

Simplified Chinese

Danke

German

நன்றி

Tamil

ありがとうございました

Japanese

감사합니다

Korean