# Pulse Comes to You 2012 Business without LIMITS

Aug 2012 | Bangkok, Hanoi

# **IBM Cloud Security**

Collin Penman

Business Unit Executive IBM Security Systems





# Cloud solutions accelerate the delivery of new business value and fundamentally change the economics of IT

Pulse Comes to You 2012

# **Tops Concerns for Cloud Adoption**

**80%** Of enterprises consider security the #1 inhibitor to cloud adoptions

48%

Of enterprises are concerned about the reliability of clouds

**33%** 

Of respondents are concerned with cloud interfering with their ability to comply with regulations "How can we be assured that our data will not be leaked and that the vendors have the technology and the governance to control its employees from stealing data?"

"Security is the biggest concern. I don't worry much about the other "-ities" – reliability, availability, etc."

"I prefer internal cloud to laaS. When the service is kept internally, I am more comfortable with the security that it offers."

Souper Britishe to Who Broger 12 and Computing, IBM Study (conducted by Oliver Wyman) May 2010 Security and Cloud Computing

Specific Customer Concerns Related to Security		
Protection of intellectual property and data	30%	
Ability to enforce regulatory or contractual obligations	21%	
Unauthorized use of data	15%	
Confidentiality of data	12%	
Availability of data	9%	
Integrity of data	8%	
Ability to test or audit a provider's environment	6%	
Other	3%	

Source: Deloitte Enterprise@Risk: Privacy and Data Protection Survey

### Pulse Comes to You 2012 May 2010

Security and Cloud Computing

# Cloud computing tests the limits of security operations and infrastructure

#### **Security and Privacy Domains**

	7
People and Identity	>
Data and Information	ĺ
Application and Process	?
Network, Server and Endpoint	>
Physical Infrastructure	>
Governance, Risk and Compliance	>
	>

Self-Service Highly Virtualized Location Independence Workload Automation Rapid Elasticity Standardization

# To cloud

Multiple Logins, Onboarding Issues Multi-tenancy, Data Separation External Facing, Quick Provisioning Virtualization, Network Isolation Provider Controlled, Lack of Visibility Audit Silos, Compliance Controls

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

## Pulse Comes to You 2012

# Simple Example

We Have Control

It's located at X.

Our uptime is sufficient.

The auditors are happy.

## **Today's Data Center**

## **Tomorrow's Public Cloud**



### Who Has Control?

Where is it located? Where is it stored? Who backs it up? Who has access? How resilient is it? How do auditors observe? How does our security team engage?

Business without LIMITS

#### Pulse Comes to You 2012 May 2010

Security and Cloud Computing

# Attributes and Benefits of Cloud Computing



	Attributes	Characteristics	Benefits
ALIZATION	Advanced virtualization	IT resources can be shared between many applications. Applications can run virtually anywhere.	Providing more efficient utilization of IT resources. Reducing hardware cost through economy of scale
	Automated provisioning	IT resources are rapidly provisioned or de-provisioned on demand.	Reducing IT cycle time (real-time provisioning) and management cost
AUTOMAT	Elastic scaling	IT environments scale down and up by large factors as the need changes.	Optimizing IT resources utilization Increasing flexibility
ATION	Service catalog ordering	Defined environments can be ordered from a catalog.	Enabling self-service, consumer concerns are abstracted from provider concerns through service interfaces
NDARDIZ	Metering and billing Flexible pricing	Services are tracked with usage metrics to enable multiple payment models.	Improving cost transparency Offering more flexible pricing schemes
vTS P⊷	Internet Access	Services are delivered through use of Internet.	Access anywhere, anytime

# **Cloud Computing Delivery Models**

## Private ...

- Access limited to enterprise and its partner network
- Dedicated resources
- Single tenant
- Drives efficiency, standardization and best practices while retaining greater customization and control
- Might be managed or hosted by third party

Customization, efficiency, availability, resiliency, security and privacy ... Cloud Services Cloud Computing Model

## Hybrid ...

 Private infrastructure, integrated with public cloud

## Public ...

- Access open to everybody, subject to subscription
- Shared resources
- Multiple tenants
- Delivers select set of standardized business process, application and/or infrastructure services on a flexible price per use basis
- Always managed and hosted by 3<sup>rd</sup> party

Standardization, capital preservation, flexibility and time to deploy ...

### Business without LIMITS

#### Pulse Comes to You 2012 May 2010

Security and Cloud Computing

# Categories of Cloud Computing Risk



9

## Control

Many companies and governments are uncomfortable with the idea of their information located on systems they do not control.

Providers must offer a high degree of security transparency to help put customers at ease.

# Reliability

High availability will be a key concern. IT departments will worry about a loss of service should outages occur.

Mission critical applications may not run in the cloud without strong availability guarantees.

## **Security Management**

Even the simplest of tasks may be behind layers of abstraction or performed by someone else.

Providers must supply easy controls to manage security settings for application and runtime environments.

## Compliance

Complying with regulations may prohibit the use of clouds for some applications.

Comprehensive auditing capabilities are essential.

May 2010

## Data

Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure.

Authentication and access technologies become increasingly important.



Pulse Comes to You 2012

# IBM Point of View: Cloud CAN be Secure.



As with most new technology paradigms, security concerns surrounding cloud computing have become the most widely talked about inhibitor of widespread usage.

To gain the **trust** of organizations, cloud services must deliver security and privacy expectations that meet or exceed what is available in traditional IT environments.

The same way transformational technologies of the past **overcame concerns** – PCs, outsourcing, the Internet.



# Different cloud deployment models also change the way think about security



## **Private cloud**

On or off premises cloud infrastructure operated solely for an organization and managed by the organization or a third party



## Hybrid IT

Traditional IT and clouds (public and/or private) that remain separate but are bound together by technology that enables data and application portability



## **Public cloud**

Available to the general public or a large industry group and owned by an organization selling cloud services.

### Changes in Security and Privacy

- Customer responsibility for infrastructure
- More customization of security controls
- Good visibility into day-to-day operations
- Easy to access to logs and policies
- Applications and data remain "inside the firewall"

## Pulse Comes to You 2012

- Provider responsibility for infrastructure
- Less customization of security controls
- No visibility into day-to-day operations
- Difficult to access to logs and policies
- Applications and data are publically exposed

# Each pattern has it own set of security concerns

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

#### **Cloud Enabled Data Center**

Integrated service management, automation, provisioning, self service

#### Key security focus:

#### Infrastructure and Identity

- Manage datacenter identities
- Secure virtual machines
- Patch default images
- Monitor logs on all resources
- Network isolation



### Pulse Comes to You 2012

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:

#### **Applications and Data**

- Secure shared databases
- Encrypt private information
- Build secure applications
- Keep an audit trail
- Integrate existing security



#### Innovate \_\_\_\_\_ business models by becoming a cloud service provider

#### **Cloud Service Provider**

Advanced platform for creating, managing, and monetizing cloud services

#### Key security focus:

#### **Data and Compliance**

- Isolate cloud tenants
- Policy and regulations
- Manage security operations
- Build compliant data centers
- Offer backup and resiliency



#### 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: Compliance and Governance

- Harden exposed applications
- Securely federate identity
- Deploy access controls
- Encrypt communications
- Manage application policies



# IBM Security Framework – Mapping into Cloud Security

IBM Cloud Security
One Size Does Not Fit All



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.



Business without LIMITS

## Pulse Comes to You 2012





# Network, Server and End Point

# Customers expect a **secure** cloud **operating environment**.

Del Terrent In Tank State 2, 2011 Byr	IBM
Redpaper	
	fore Lainville
Secure Cloud Guidance IBM recommendations for the implementation of o	ioud security
in the Perspect of the party is present on the statement of	alte 1948 Genel Mila Lege
Introduction to cloud computing	
Check comparing it a field in cash offician and protein delargy plattic barrange of constants of a section and the barrange. Check management and management of a section and proteining and a section protein regardless of our backless or design.	
(a s maybe chair comparing plans any index of a particle by the distance planets of the distance of the distance of the basic on explanation. In many lings, should compare grades the base providing with many the combinations. In many single distance of the same providing with many the combinations. In minimum large Bill for any consider provide.	an a
In an added lensel, shard anyoning estimates for our elipstence monoidity lines in not contributed anything about the animity of anythermitation.	When thing is in
Belle public med primite stand reaches are well in user. Available to any memory public methods include highware are a forward Pauli, should be Physican and a forware Pauli, should not an an an anomal Weil Forware, Protocolar are a forware (PEP-weil), should have BM Streamly There and Beauty.	and the balance and the second s
Provide classics are called and and by a single coperation. They also benefits as public shock, we first public classics expension provide Professions, printiple classics are provide bittle bittery through the periods. Usey regressions enhance but public and printiple classics.	and a second second
Constant Tel Colo 2006 All Igits Insuland	and a second

IBM Cloud Security Guidance Document

Pulse Comes to '

Maintain environment testing and vulnerability/intrusion management

Implement vulnerability scanning, anti-virus, intrusion detection and prevention on all appropriate images

- Ensure isolation exists between tenant domains
- Trusted virtual domains: policy-based security zones

A secure application testing program should be implemented.

Develop all Web based applications using secure coding guidelines.

Ensure external facing Web applications are black box tested





## **People and Identity**

# Customers require **proper authentication** of cloud users.

Dell'Annael le fanit Della (1.700 Ellija	IBM
Redpaper	
	Azel Backer Koon Lainvijin
Secure Cloud Guidance	
IBM recommendations for the Implementation of cit	oud security
in the Technese <sup>w</sup> ite an apply in practic pro Wite a descent deal management interaction for the top investigation of shard secondly. To put you at Wite as the shard second or any sharp and shard secondly in present	ter 1990 and to a tegin
Introduction to cloud computing	
Court are puting in a fulfilly, and off-the and puters defining platform balances of contracts of a processor part for balance. Chair manufacture are and and a solid. With all processors, applications and accelerate processor arguments of our definition or balance.	
for a result should compare give reprinting the provide by the loss	
instants any investigation of the second second system of the last providing and instants for our instants to start a start Will for any of boundary provides	find world: the looky setting
de an added interfét, sind comparing extension for our effective of completiby there is not contributed anything also the anticipage anythermatican.	and adding to the
The party and place and make an off is an Archite is appr	THE INCOME
Register and charter (Part), data and an instant with instant, and Property of a Charter (CPart), data in the Distance (Constant, Constant), Stream,	Character and Ch
Plants clock an attend and had be adopt oppointing. They after	and the second
Parlamente printe de la ser preció tille bien y l'an pala, de la	dara presi terte
Flagigi (Bligs 205 Align Instal	and shake 1

IBM Cloud Security Guidance Document

Implement strong identity and access management

- Implement least privilege model for user's access
- Strong Identity lifecycle management
- All administrative access over secure channels
- Privileged user monitoring, including logging activities, physical monitoring and background checking
- Utilize federated identity to coordinate authentication and authorization with enterprise or third party systems

Pulse Comes to '

A standards based, single sign-on capability



## **Application and Process**



# Customers require **secure cloud applications** and **provider processes**.

Dell'Instantio Table 18.7001 Bye	and the second
	EM
A Dednemer	
Correction Rectange	
	And Bascher ten Ladavijke
Secure Cloud Cuidence	
Secure crodu duruance	
IS M Recommendations for the implementation of cloud	soc unty
in the Teleport <sup>44</sup> for an party is providing with a decision density of measurements in the transmission of the decision of the transmission of the Without transmission is clear analysis, and the decision of parts	eð Fra hegt
Introduction to cloud computing	
Check computing is a field in cash of the day and proven defining platform for pr	and the second
and mady under 10th of processes, applications and provide problems for regardless of our backets or design.	(mark)
the a result of and comparing place any indices the superior by in increase it	Contraction of the local division of the loc
inations explorately is may large clear experts y down in the part (in the part of the second s	and and and
is an added interfit, class comparing estimates for our edgestrate filling monology (laws in our contribution) anything about the activity probability hyperconductors.	
Bell yields and primit shad reading an off in our Archite is argued the	1 to 1 to 1
montes, a platic constitute visitate industres en a clientate (Paral), chanda Rei (Birl, C. Fugliere et a Carriere (Paral), chanda a clientation (Paral), chanda Rei (Birl, Paratestan ara director (PCP-aral), chanda Rei (Birl Zenardy, David and Leg (Birl Benard).	and the second stress
Contractory and the second	to and
Parlament, printe deals an preside table table print paids dank deel periods Many organizations entreare balt paids and printe deal computing	to the party of the
• Capital INC Cal. 2015. Al Tatis Insulation	

IBM Cloud Security Guidance Document

Establish application and environment provisioning

Implement a program for application and image provisioning.

- Ensure provisioning management is strictly controlled
- Protect machine images from corruption and abuse

Ensure all changes to virtual images and applications are logged.

Ensure provisioned images apply appropriate access rights

Ensure destruction of outdated images

Pulse Comes to '. Ju 2012 May 2010





Data and Information

# Customers cite data protection as their most important concern.

<text><image><image><section-header><section-header><section-header><section-header><text><text><text><text><text><text><text>

IBM Cloud Security Guidance Document Ensure confidential data protection

Protect PII and Intellectual Property

Implement a secure key management program

Use a secure network protocol when connecting to a secure information store.

Implement a firewall to isolate confidential information, and ensure that all confidential information is stored behind the firewall.

Sensitive information not essential to the business should be securely destroyed.





## **Physical Security**



# Customers expect **cloud data centers** to be **physically secure**.

Dell'Assess to South Dates 202010 (pr	TRM
Redpaper	
	And Bascher Koon Laiseigen
Secure Cloud Guidand	æ
IBM recommendations for the imp	elementation of cloud security
in the Decision of the second se	ingen With a descention allend the 1988 of dataf secondly. In get you stand of the best pro- ceeded all neurologies generated.
Introduction to cloud computing	
Over expering to a fulfille, our effect bacteria or extension of annual sector and weak works. We also preserve any regardless of our backing or deter-	en en la companya de la companya de Receletar de la companya de la compa
the second state of the se	and an and the second of the second second
providing with appendix to combinational monotonic process	na i negato y den de las glindensis nationales y 10 de manipis designed na
is an added interfat, shad complete a sampleday threads of contribution any interfation.	danan baran diputan Mina abing tak ayilan dana baratisya jarinakya a
Ball public and priority dead reaching an accuracy public contribution (public) Ringbers are a limited (Paul), should be presented on a limited (Paul), should	will in our Archite to append With Marcall an Enroise (Deall) should be UNU course on an Enroise Web Enroise, and Enroy's and Data Section Security Developed and Enroy Security

IBM Cloud Security Guidance Document

Implement a physical environment security plan

Ensure the facility has appropriate controls to monitor access.

Prevent unauthorized entrance to critical areas within facilities e.g. servers, routers, storage, power supplies

Biometric access of employees

Ensure that all employees with direct access to systems have full background checks.

Provide adequate protection against natural disasters.

DUSINESS WILHOUL LIVILIS





Dell'Insurant la Tanta Colda 21.2008 Ellipsi	#Tipsetite
	IBM
Redpaper	
	fand Banchar Konn Ladawijka
Secure Cloud Guidance	
IBM recommendations for the implementation of d	foud security
is the final part of the set gain is previous. We a decrement of measurements in the input set of the decrements of the set of the	ative 1980 and for a longin
Introduction to cloud computing	
One of comparing it is fulfille, and official and protect datasy platform based on contactor IT annuals are the based. Could measure a set only waited with a processor application and annuals protec- ment of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of t	
(as a small of shared comparing plants may include the description of the state induces of these small states that it is the states of the state of the states based on a system with the states of the states and the states of the state possible of the states of the states induces a function as along the first states based on a state of the states.	
is an added insert, closel accepting enterous the care objective accepting these is not careful book anything about the activity asymmetry	and a string to be
Bell public and priority should reachly an well in case, Academic in any monte, public workshow have an algebra or algebra of David (status) for Fingleton and a first of Public (status) and the status of David (status) Properties are all strict of DDP-well (status) for DBM Strength (there are Strength and Strength (DDP-well) (status) for DBM Strength (there are Strength and Strength (DDP-well) (status) for DBM Strength (there are Strength and Strength (DDP-well)) (status) for DBM Strength (there are Strength and Strength (DDP-well) (status) for DBM Strength (there are Strength and Strength (DDP-well) (status) for DBM Strength (there are Strength and Strength (DDP-well) (status) for DBM Strength (there are Strength and Strength (there are all strength (there are al	an Web Scienced Web Local An And Science System (Com- log Web ageneral
Provide classific and effect and participal regression. They also benefits as public classific and participal for allow a specializing participal Professional priority classific and provide fails being that public of profession. Many approximation without fails public of participality and	
• Capital IN Los XXX Al Istochast	

IBM Cloud Security Guidance Document

Pulse Comes to

May 2010

Security governance, risk management and compliance

# Customers require **visibility** into the security posture of their cloud.

Implement a governance and audit management program

Establish 3rd-party audits (ISO27001, PCI)

Provide access to tenant-specific log and audit data

- Create effective incident reporting for tenants
- Visibility into change, incident, image management, etc.
- Create policies for PII and for data crossing International boundaries
- •Understand applicable regional, national and international laws

Security and Cloud Computing

# **IBM Providing Cloud Leadership**



# Summary

- "Cloud" is a new consumption and delivery model inspired by consumer Internet services.
- Security Remains the Top Concern for Cloud Adoption
- One sized security doesn't fit all
- Take a structured approach to securing your cloud environment
- Documented guidance is available for download to assist you in securing your cloud environment



