How do I ensure the cloud is secure?

Vaughan Harper
Consulting IT Specialist
IBM Security Architect
vaughan_harper@uk.ibm.com

PCTY2012
Pulse Comes to You

Optimizing the World's Infrastructure

30 May, 2012 London

Please note:

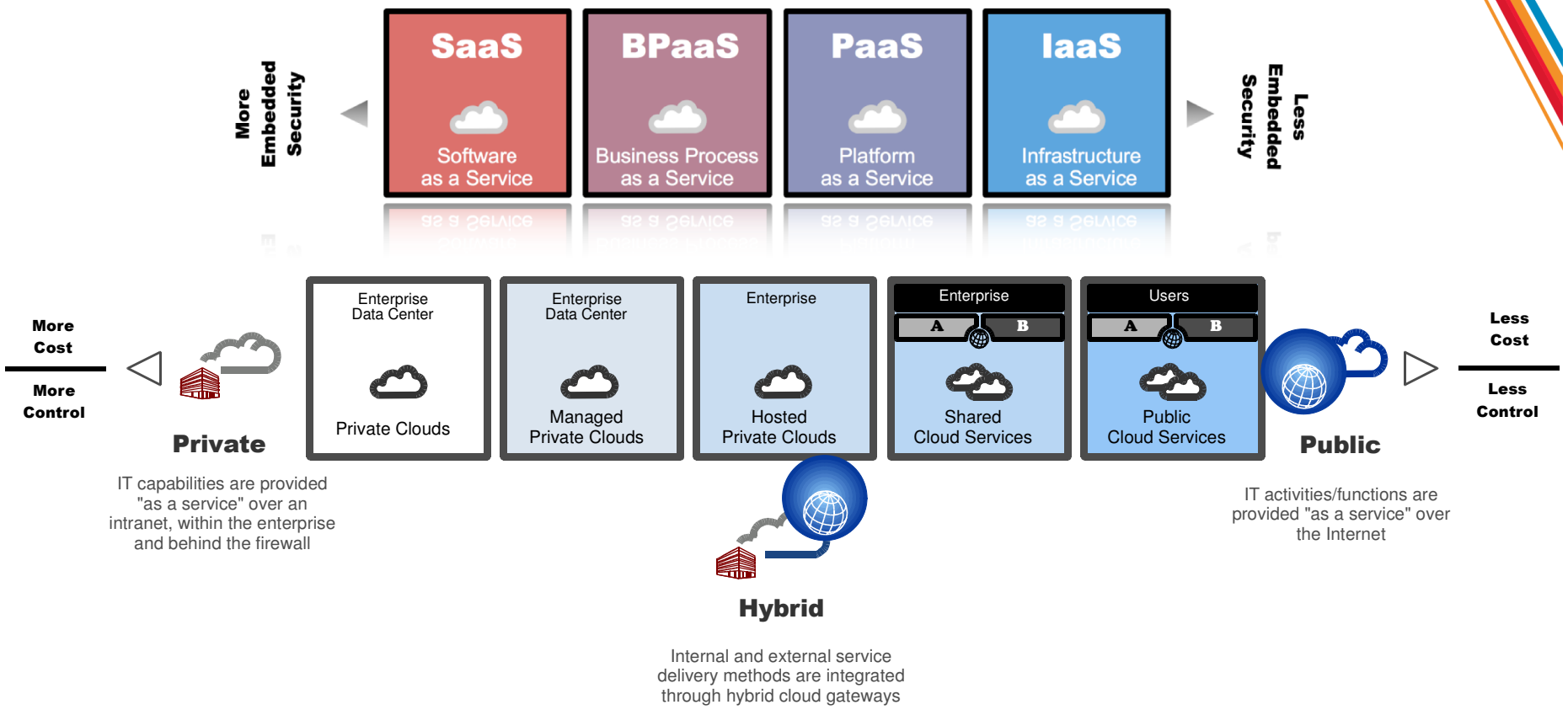
- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

What is Cloud Computing?

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models…"

- US National Institute of Standards and Technology (NIST), September 2011

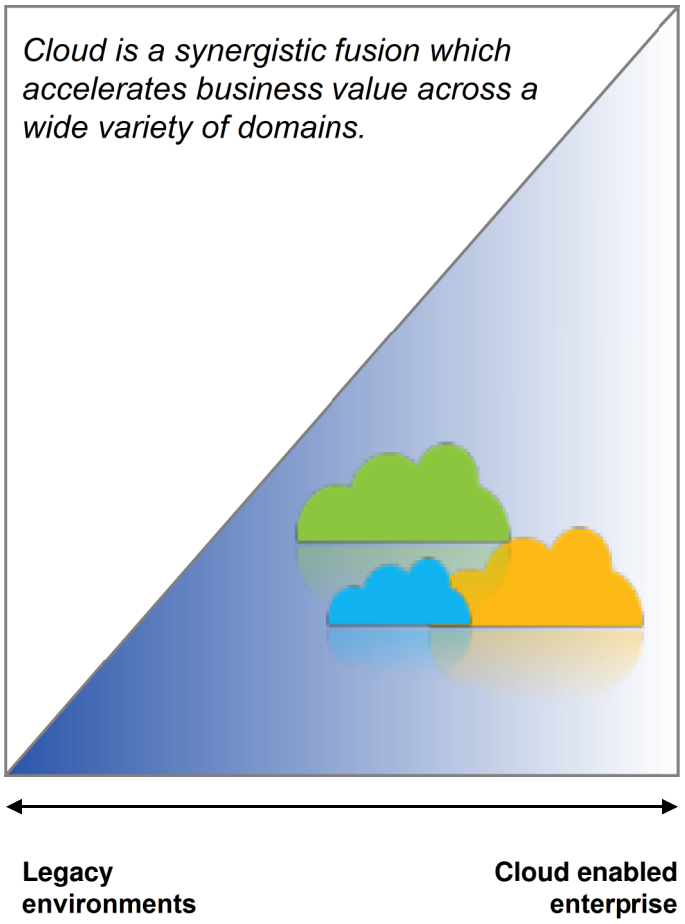
Cloud Deployment/Delivery and Security



Depending on an organization's readiness to adopt cloud, and appropriateness for a particular application, there are a wide array of deployment and delivery options

Why cloud?

Capability	From	To
Server/Storage Utilisation	10-20%	70-90%
Self service	None	Unlimited
Test Provisioning	Weeks	Minutes
Change Management	Months	Days/Hours
Release Management	Weeks	Minutes
Metering/Billing	Fixed cost model	Granular
Payback period for new services	Years	Months

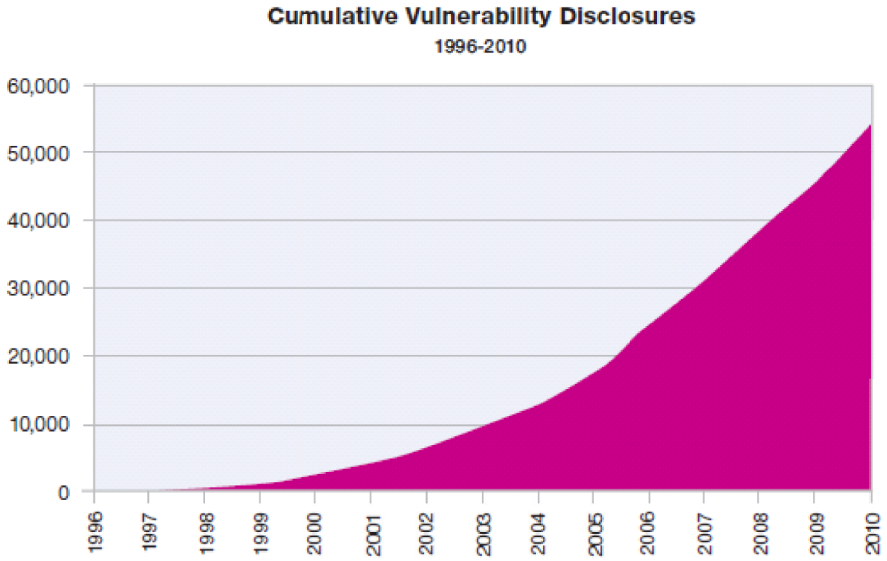


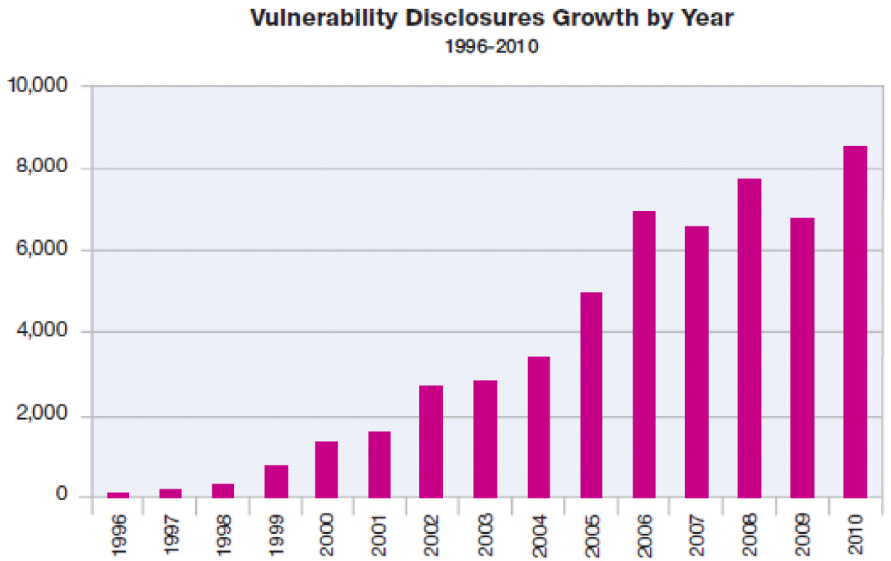
Security as a barrier to Cloud adoption

Over the past several years, **security concerns surrounding cloud computing** have become the most common 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.

What is the threat and where is it evolving…



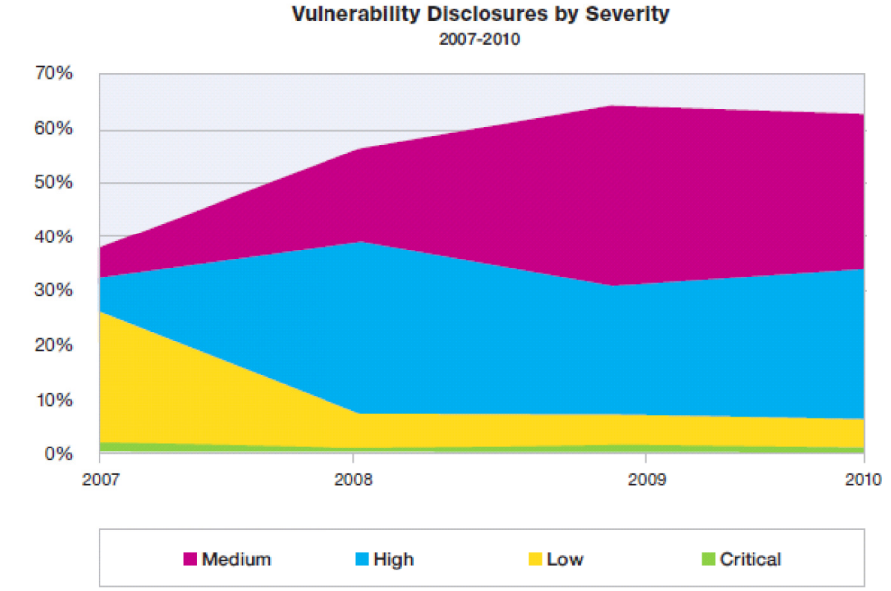


2010 = A record setting year had the largest number of vulnerability disclosures in history - 8,562.

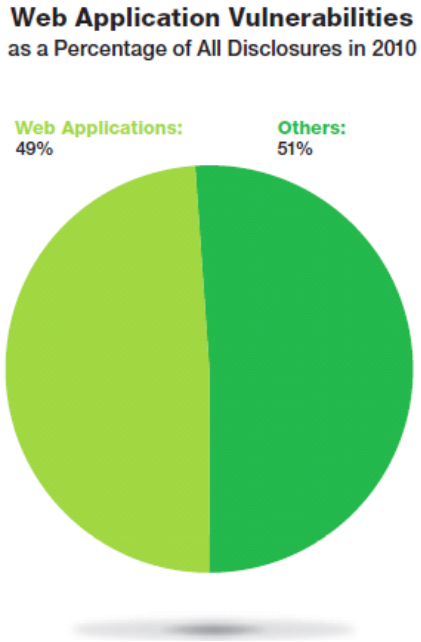
This is a 27 percent increase over 2009, and this increase has had a significant operational impact for anyone managing large IT infrastructures.

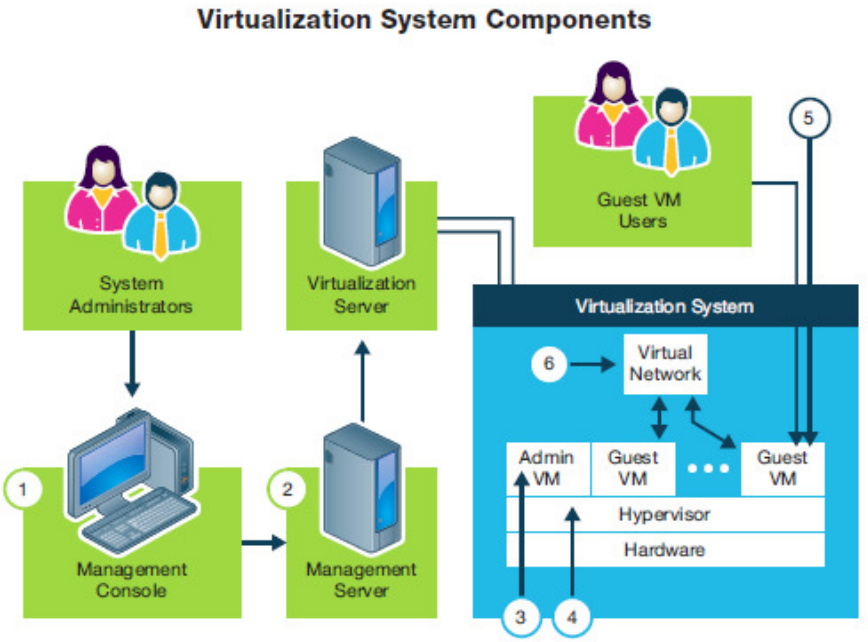
The relative mix of vulnerability severities has not changed substantially for the past three years.

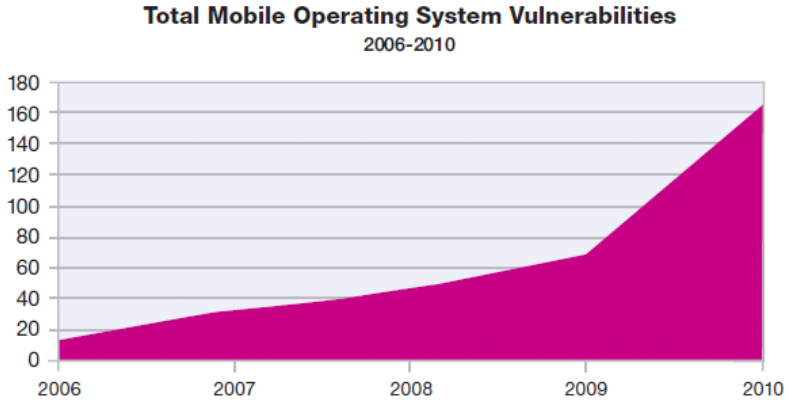
IBM X-Force® 2010 Trend and Risk Report



Implications for cloud….







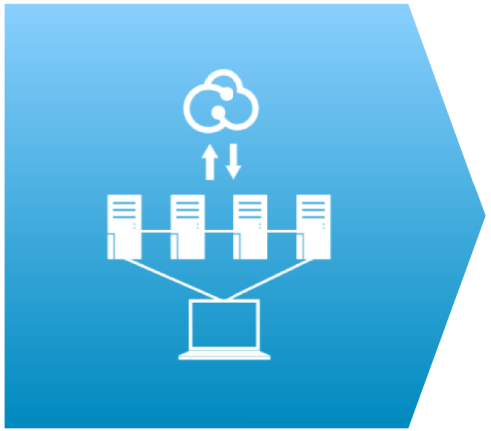
Distribution of Virtualization System Vulnerabilities
Indeterminate: 6.25% Hypervisor: 1.25%
Mgmt Server: 6.25%
Guest VM: 15%
Mgmt console: 16.25%
Admin VM: 17.5%
Hypervisor escape: 37.5%

IBM X-Force® 2010 Trend and Risk Report

Approaches to delivering security need to align with each phase of a client's cloud project or initiative

	Design	**Deploy**	**Consume**
	Establish a cloud strategy and implementation plan to get there.	Build cloud services, in the enterprise and/or as a cloud services provider.	Manage and optimize consumption of cloud services.
Cloud Security Approach	***Secure by Design*** *Focus on building security into the fabric of the cloud.*	***Workload Driven*** *Secure cloud resources with innovative features and products.*	***Service Enabled*** *Enable security through services and interfaces.*

Cloud computing impacts the implementation of security in fundamentally new ways



Security and Privacy Domains	To cloud
People and Identity	Multiple Logins, Numerous Roles
Data and Information	Multi-tenancy, Shared Resources
Application and Process	External Facing, Quick Provisioning
Network, Server and Endpoint	Virtualization, Reduced Access
Physical Infrastructure	Provider Controlled, Lack of Visibility
Governance, Risk and Compliance	Audit Silos, Logging Difficulties

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**.

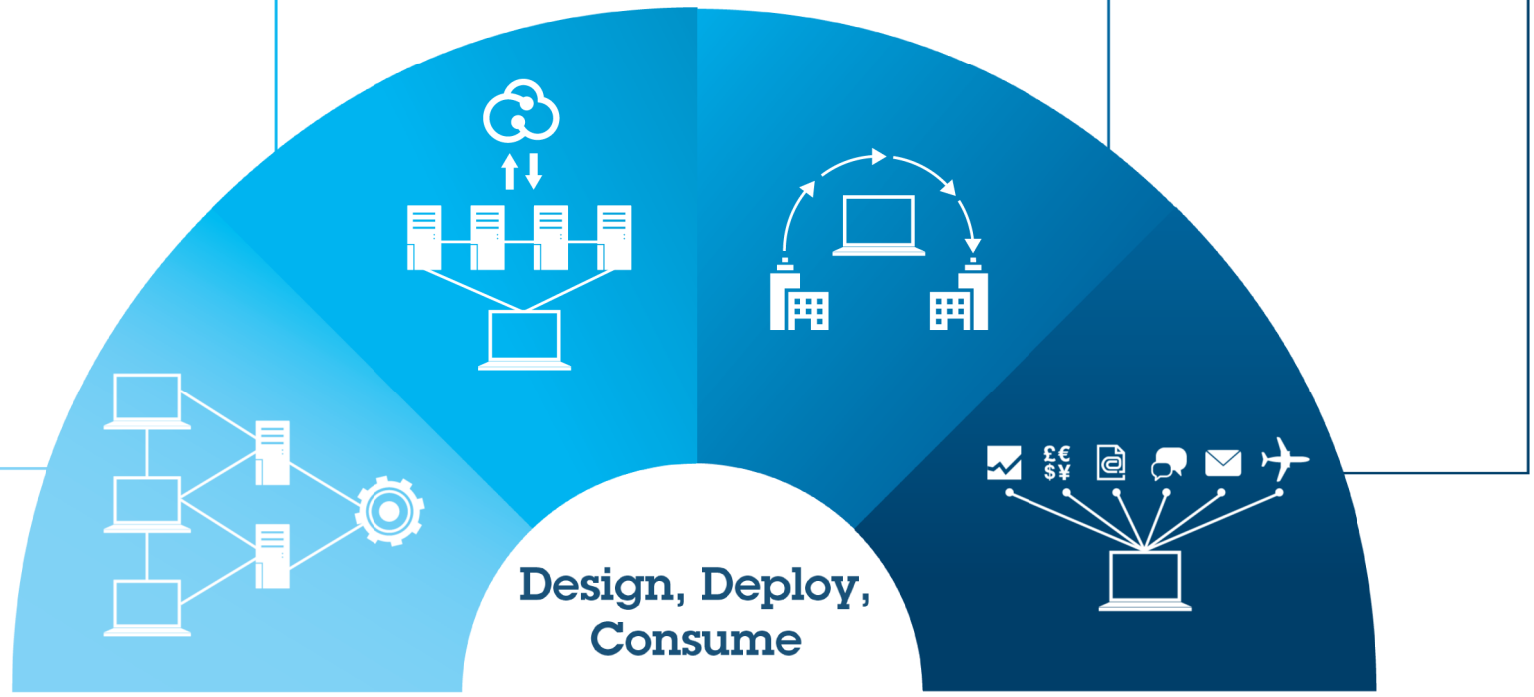
Adoption patterns are emerging for successfully beginning and progressing cloud initiatives

IaaS: Cut IT expense and complexity through a cloud enabled data center

PaaS: Accelerate time to market with cloud platform services

CSP: Innovate business models by becoming a cloud service provider

SaaS: Gain immediate access with business solutions on cloud



Each pattern has its own set of key security concerns

IaaS: Cut IT expense and complexity through a cloud enabled data center

PaaS: Accelerate time to market with cloud platform services

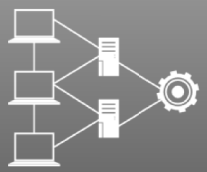
Innovate business models by becoming a cloud service provider

SaaS: Gain immediate access with business solutions on cloud

Cloud Enabled Data Center

Integrated service management, automation, provisioning, self service

- Logical and physical isolation
- Secure virtual machines
- Patch of default images
- Encrypt stored data
- Assess self service portals
- Monitor logs on all resources
- Defend network perimeters



Cloud Platform Services

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

- Harden exposed applications
- Use cloud APIs properly
- Protect private information
- Secure shared databases
- Manage platform identities
- Integrate existing security controls with the cloud

Cloud Service Provider

Advanced platform for creating, managing, and monetizing cloud services

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

Business Solutions on Cloud

Capabilities provided to consumers for using a provider's applications

- Federate identity between the cloud and on-premise IT
- Proper user authentication
- Audit and compliance testing
- Encrypt data, both in motion and at rest
- Integrate existing security

Understanding cloud security: using Cloud Reference Model with foundational security controls

Cloud Governance
Cloud specific security governance including directory synchronization and geo locational support

Security Governance, Risk Management & Compliance
Security governance including maintaining security policy and audit and compliance measures

Problem & Information Security Incident Management
Management and responding to expected and unexpected events

Identity and Access Management
Strong focus on authentication of users and management of identity

Discover, Categorize, Protect Data & Information Assets
Strong focus on protection of data at rest or in transit

Information Systems Acquisition, Development, and Maintenance
Management of application and virtual Machine deployment

Secure Infrastructure Against Threats and Vulnerabilities
Management of vulnerabilities and their associated mitigations with strong focus on network and endpoint protection

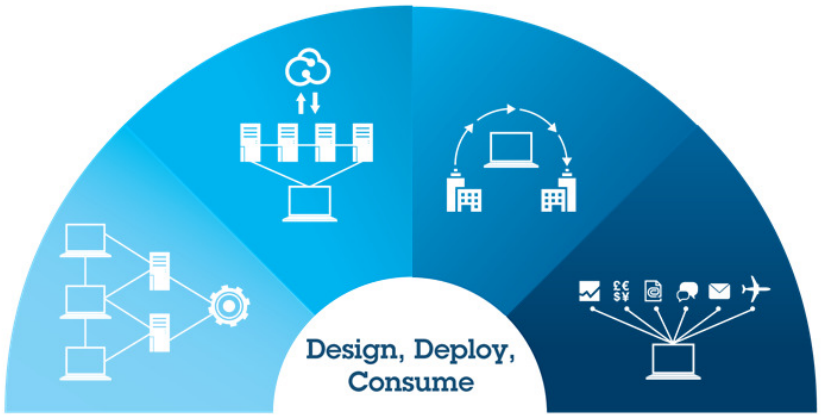
Physical and Personnel Security
Protection for physical assets and locations including networks and data centers, as well as employee security

IBM Cloud Reference Model

Protecting and risk management in the cloud building on traditional approaches, applied to new models. Each model has different aspects to consider.

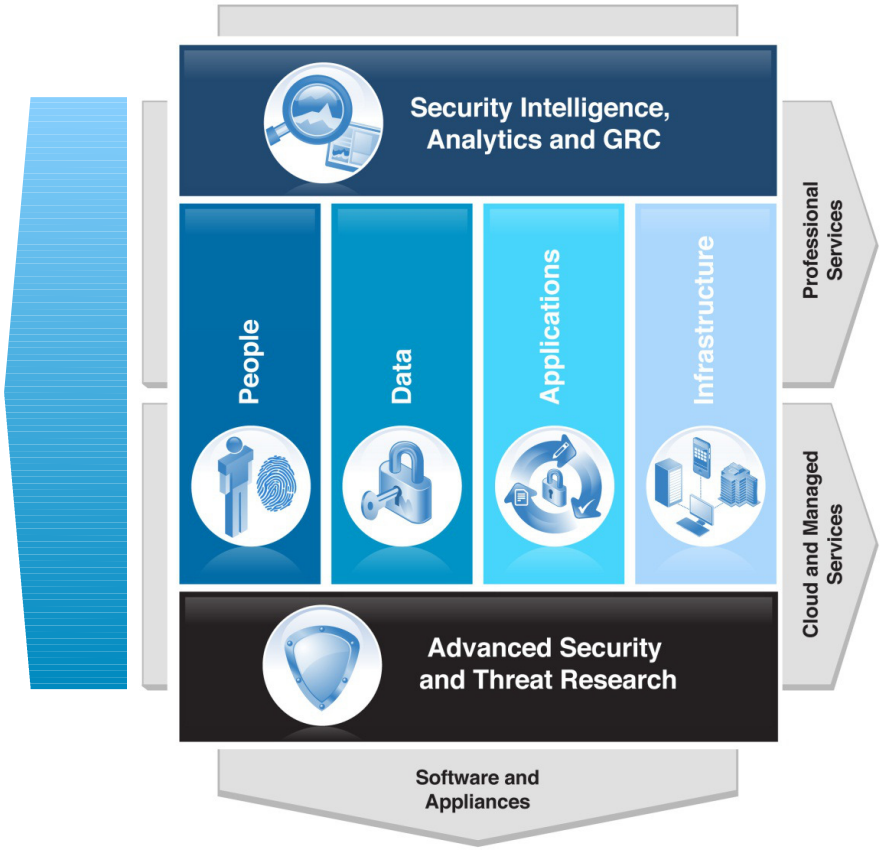
IBM Cloud Security

One Size Does Not Fit All

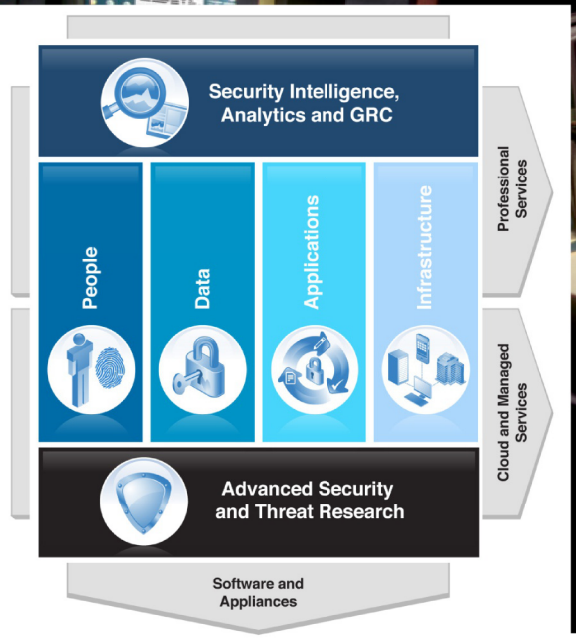


Different security controls are appropriate for different cloud needs - the challenge becomes one of integration, coexistence, and recognizing what solution is best for a given workload.

IBM Security Framework



Security GRC



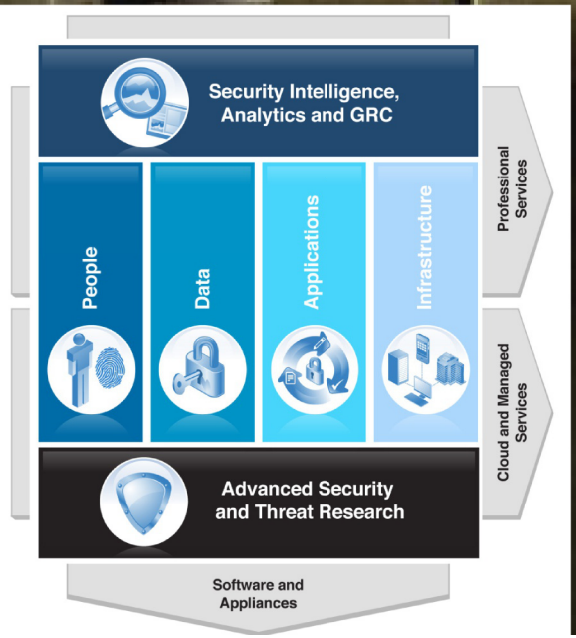
Solving the Urgent Questions

Am I compliant?

What controls are needed?

Can I prove it?

Identity and Access in a Smarter Planet



Solving the Urgent Questions

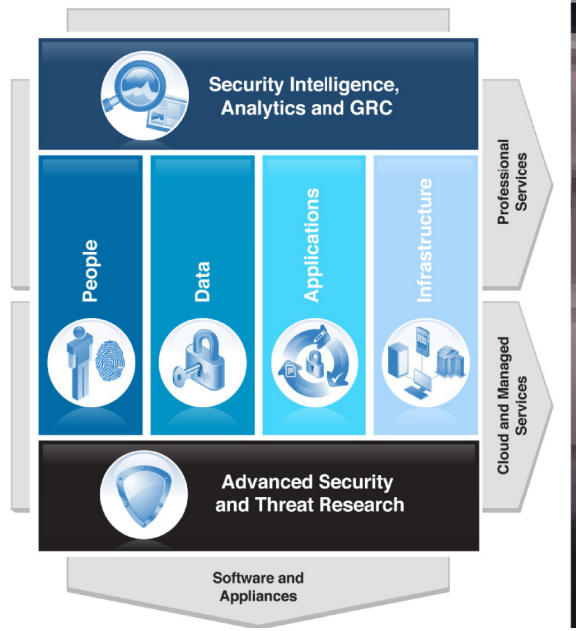
What's identity in the cloud?

Can I restrict privileged users?

Who has access?

How does Federation fit in?

Protect sensitive data from malicious activity



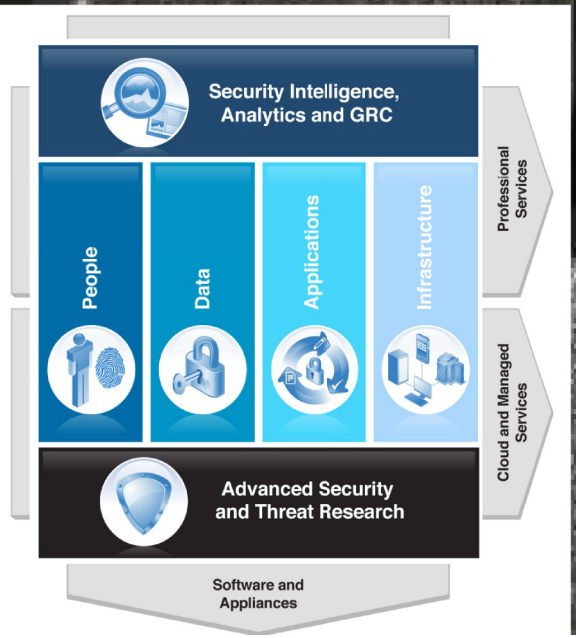
Solving the Urgent Questions

Where's my sensitive data?

How can I keep data secure?

What are DBAs doing?

Securing applications by design, not after disruption

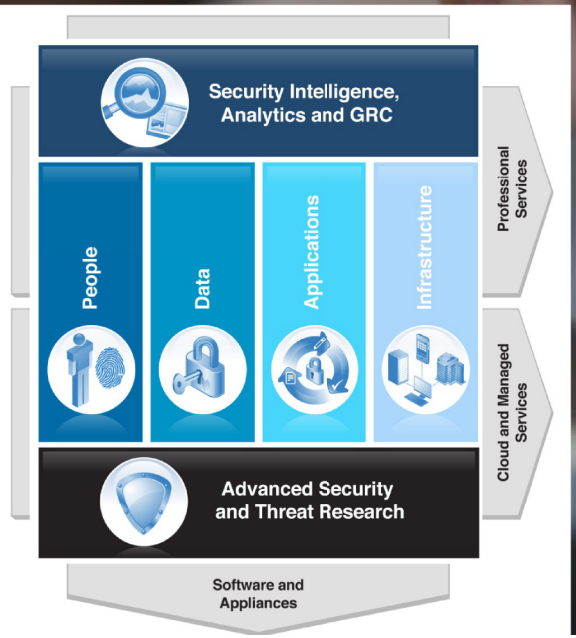


Solving the Urgent Questions

How do I develop apps securely?

How do I stop vulnerability exploitations?

A platform for converged endpoint

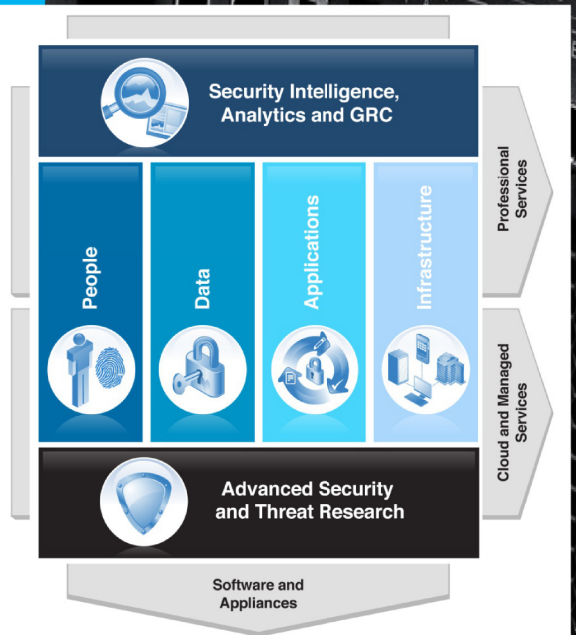


Solving the Urgent Questions

How do I manage all these devices?

How do I secure mobile devices?

Keep the bad guys out of the network



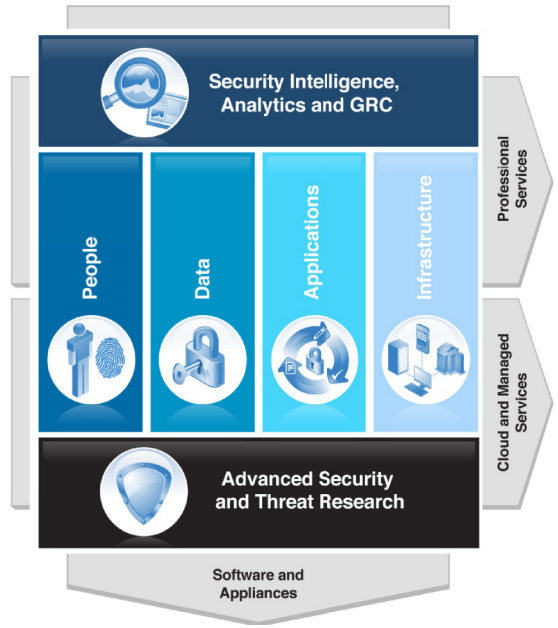
Solving the Urgent Questions

Who's attacking my system?

What's the latest threat intelligence?

How do I manage all the data?

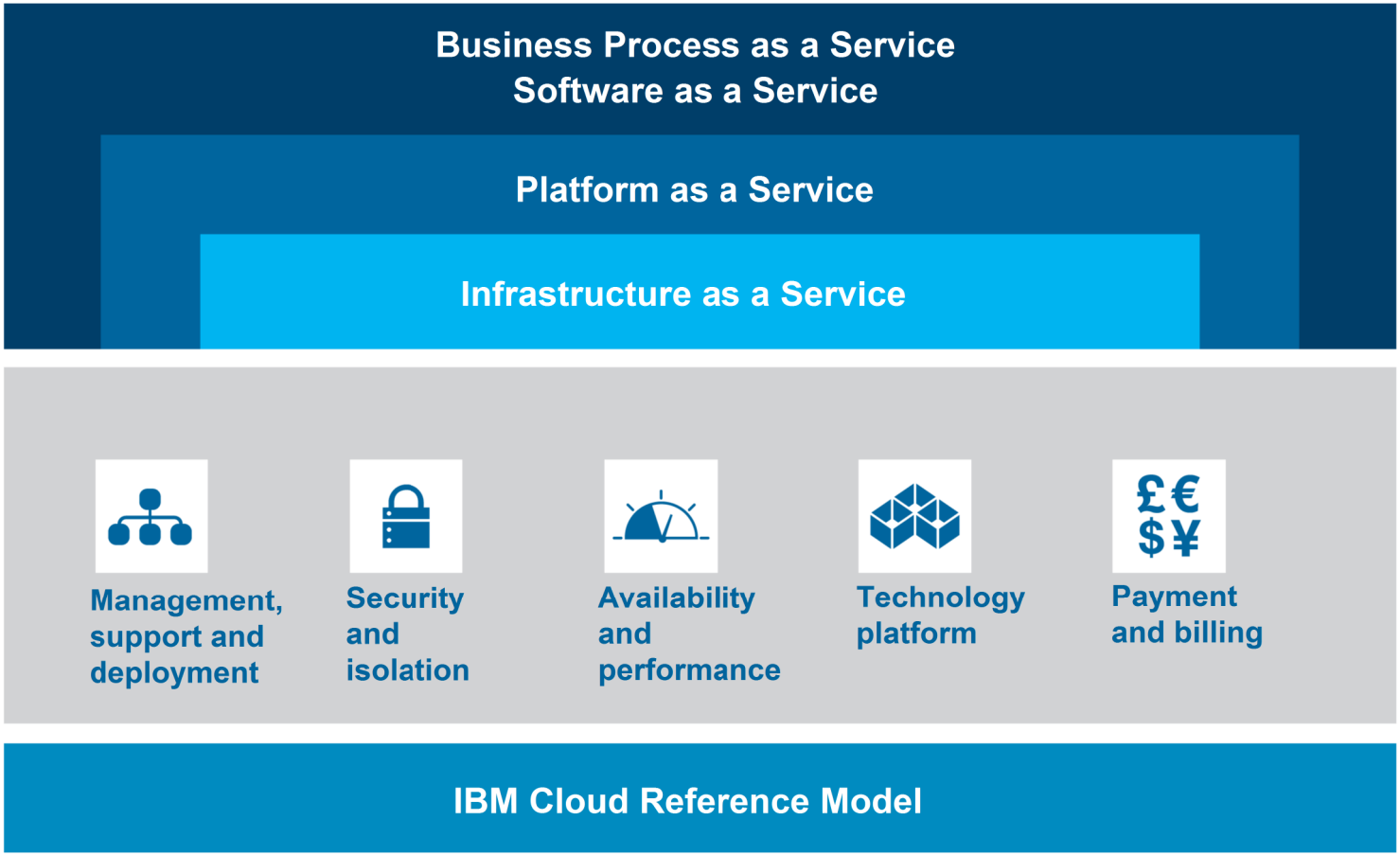
Modernize traditional surveillance systems



Solving the Urgent Questions

Can I automate my video surveillance?

Security in the context of a robust platform, secure by design, built on a cloud reference model



IBM has extensive real-world experience delivering public and private cloud services

2,000

successful private cloud engagements in 2010.

495M

daily client transactions through public cloud.

public cloud users.

1M

managed virtual machines.

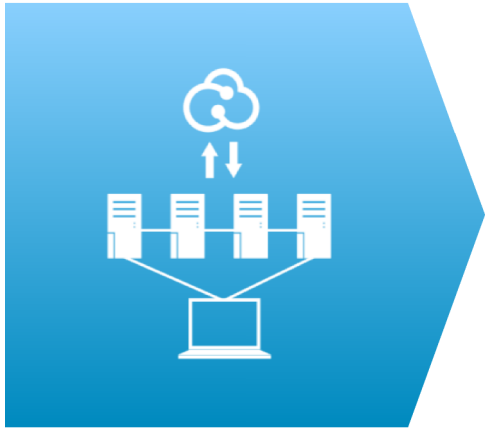
"IBM has one of the most comprehensive cloud portfolios, with the cloud integrated throughout its many lines of business. Moreover, IBM's consulting arm has put them in touch with numerous early adopters and special use cases—all of which helps the company stay ahead of competitors. "

– Jeff Vance, Datamation

PCTY2012

What are the issues we will face going forward…

Standardisation Interoperability Big Data Governance



Security and Privacy Domains

People and Identity

Data and Information

Application and Process

Network, Server and Endpoint

Physical Infrastructure

Governance, Risk and Compliance

Driven by multiple people accessing multiple devices via multiple clouds

In summary

Over the past several years, **security concerns surrounding cloud computing** have become the most common inhibitor of widespread usage.

This often translates to where is my data, who will be able to access, and how will I maintain oversight and governance?

Each cloud model has different features which changes the way security gets delivered which also changes the way we look at security governance and assurance.

Determining your desired security posture and enabling cloud in such a way that the new risks can be managed in a rapidly changing landscape....

Public cloud

Hybrid IT

Private cloud

Acknowledgements, disclaimers and trademarks

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

IBM, the IBM logo, ibm.com, Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml