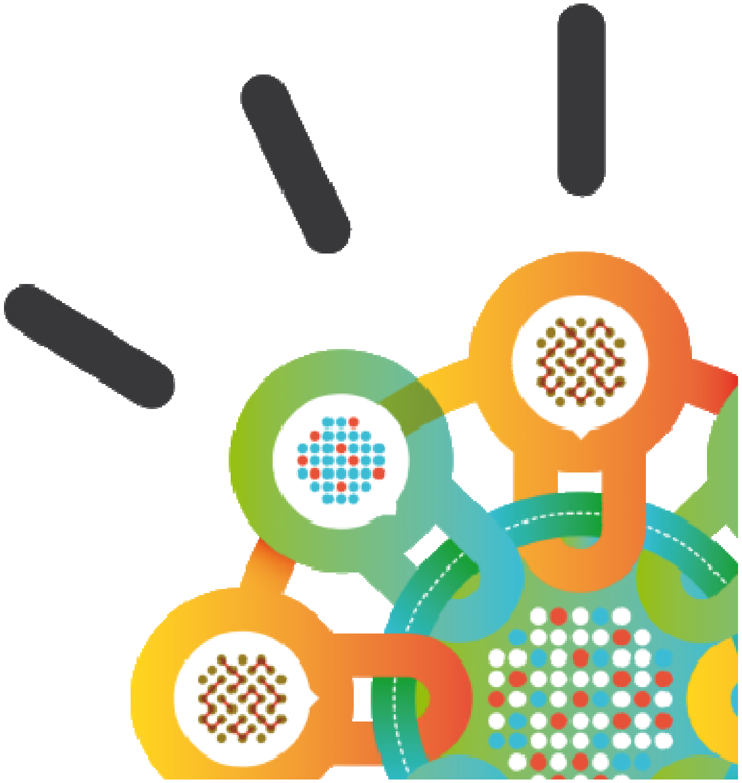
Security Intelligence.
Think Integrated.

Securing the Cloud with IBM Security Systems

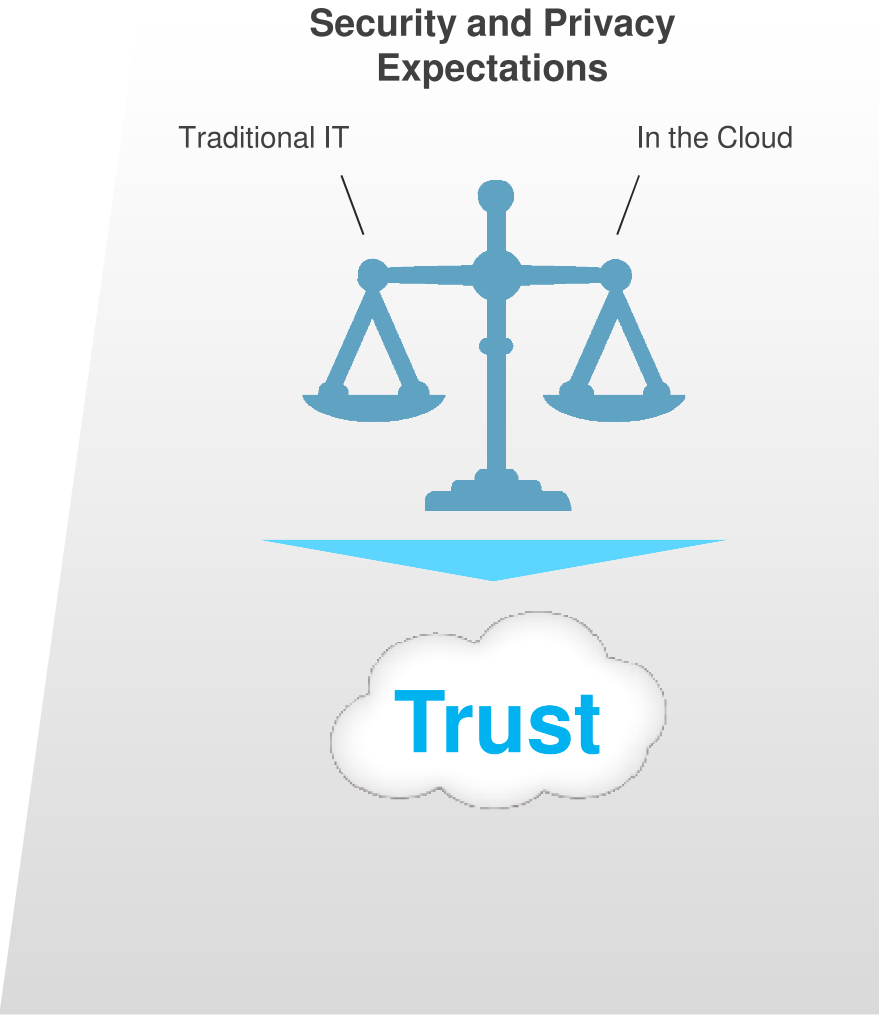


IBM Point of View: Cloud can be made secure for business

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

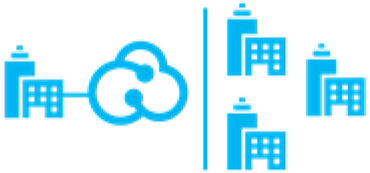
To gain the **trust** of organizations, cloud services must deliver security and privacy expectations that meet or exceed what is available in traditional IT environments.

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



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**

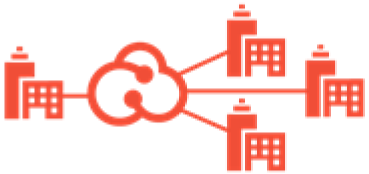


Private cloud

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”*

- *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*

Minimizing the risks of cloud computing requires a strategic approach

Define a cloud strategy with security in mind

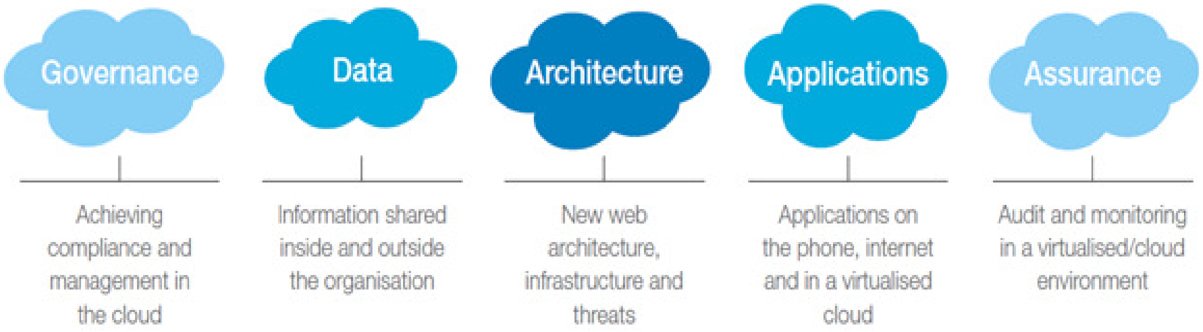
- Identify the different workloads and how they need to interact.
- Which models are appropriate based on their security and trust requirements and the systems they need to interface to?

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

Our approach to delivering cloud security aligns with each phase of a clients 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.
IBM 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*** *Govern the cloud through ongoing security operations and workflow.*
Example security capabilities	▪ Cloud security roadmap ▪ Secure development ▪ Network threat protection ▪ Server security ▪ Database security	▪ Application security ▪ Virtualization security ▪ Endpoint protection ▪ Configuration and patch management	▪ Identity and access management ▪ Secure cloud communications ▪ Managed security services

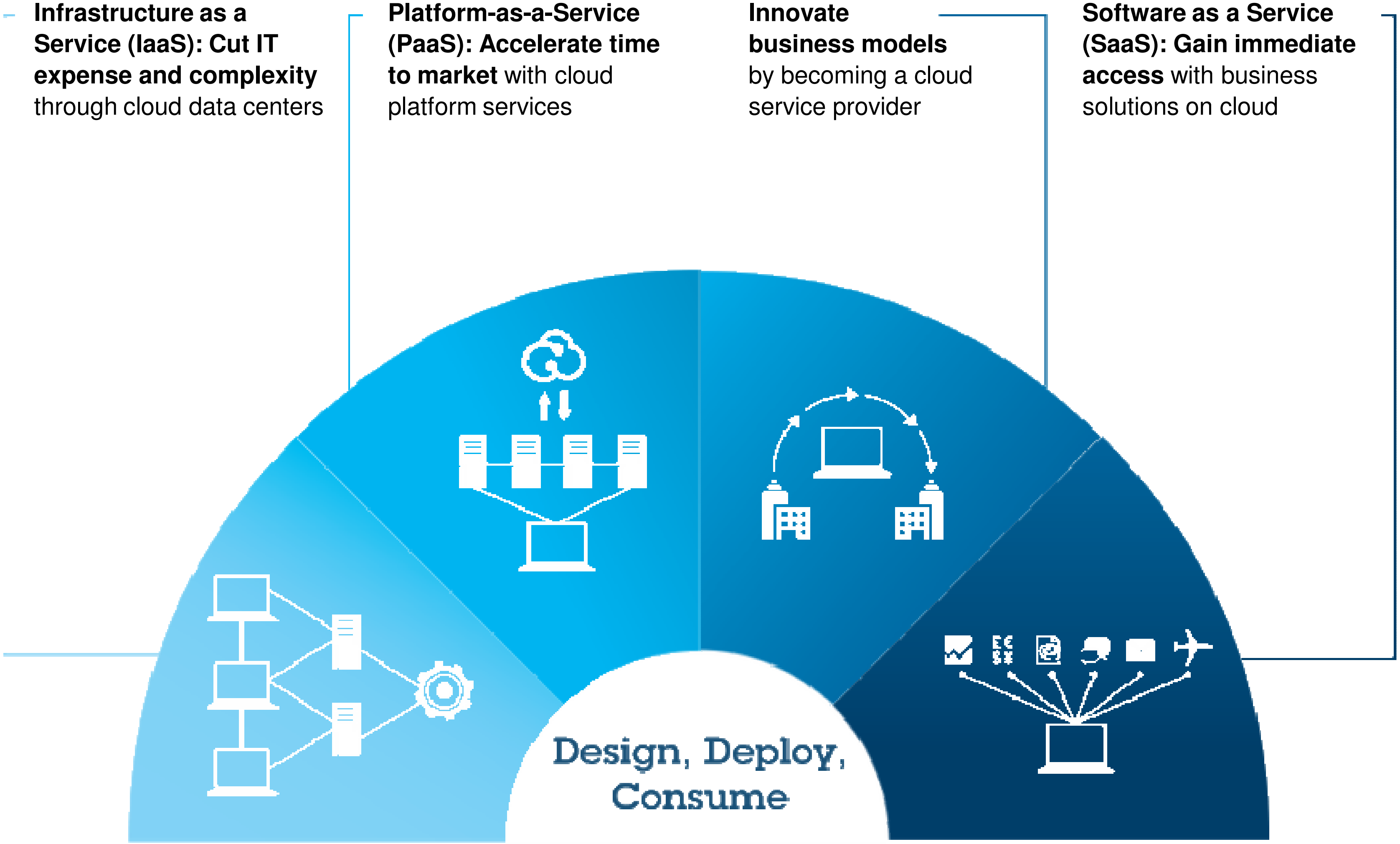
Adoption patterns are emerging for successfully beginning and progressing cloud initiatives

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

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

Innovate business models by becoming a cloud service provider

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



Each pattern has its own set of key security concerns

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

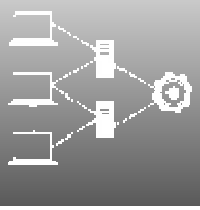
Cloud Enabled Data Center

Integrated service management, automation, provisioning, self service

Key security focus:

Infrastructure and Identity

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



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

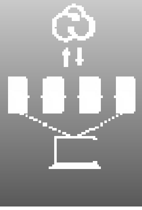
Cloud Platform Services

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

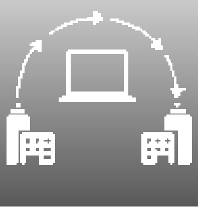
Cloud Service Provider

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

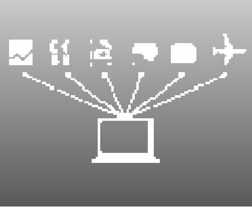
Business Solutions on Cloud

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 Cloud Security helps customers regain visibility and control

End-to-end coverage for securing private, hybrid and public clouds.

IBM is the only vendor with products, services and expertise to secure critical dimensions of cloud - spanning **users, data, applications** and **virtualized infrastructure.**

- **Enterprise-class** security across all cloud domains
- **Visibility** into the security of cloud environments
- **Secure access** to cloud applications
- **Data protection** for in motion and at rest.
- **Threat and vulnerability management** solutions for applications and infrastructure.
- **Services** specifically designed for securing the cloud

SC MAGAZINE AWARDS 2012 WINNER

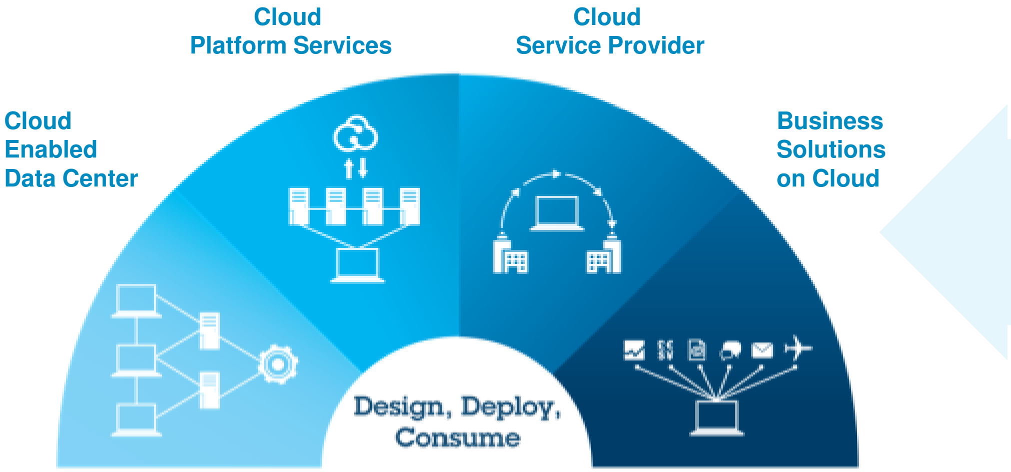
Honored in the U.S.

Best Cloud Computing Security

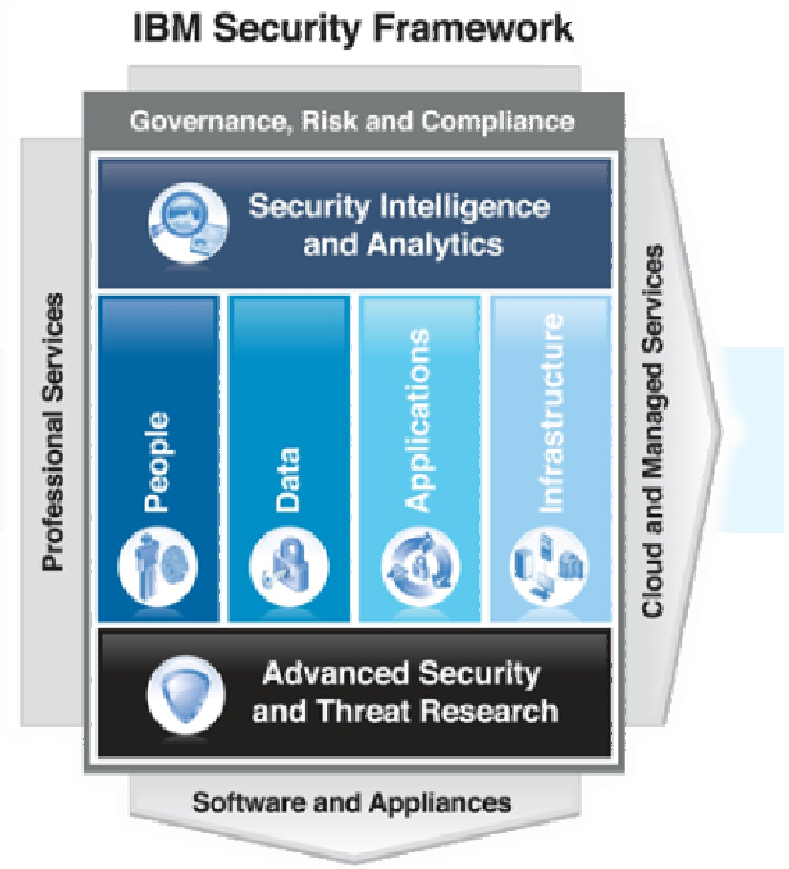
IBM's breath of experience and security capabilities are being applied to all cloud adoption patterns

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.

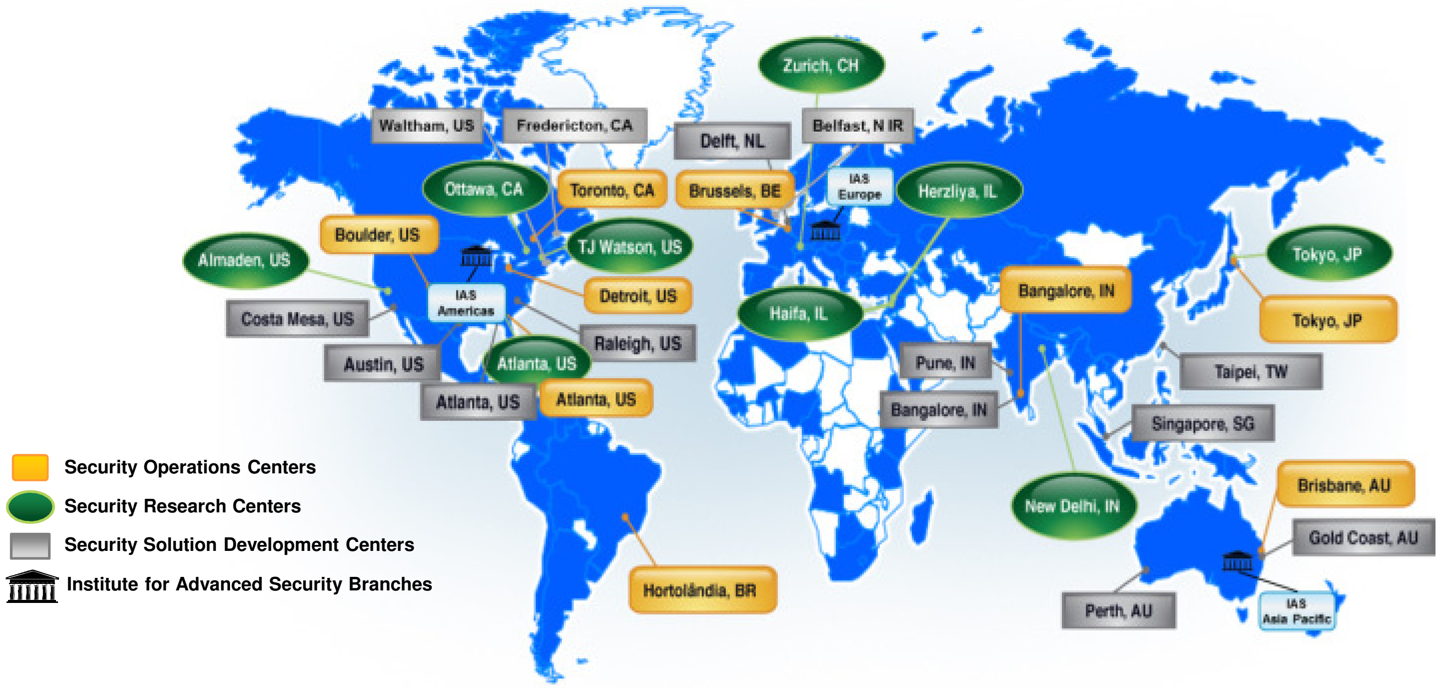

IBM Security Framework
Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

And we’ve developed a set of cloud security controls to get started

Cloud Security On Ramps

			Design	Deploy	Consume
Security Intelligence	▪ Total visibility into virtual and cloud environments	**IBM QRadar Security Intelligence Platform (SIEM, Risk Manager)**	X	X	X
People	▪ Enable single sign on across multiple cloud services	**IBM Federated Identity Manager Business GW**			X
Data	▪ Protect and monitor access to shared databases	**IBM InfoSphere Guardium**	X	X	
Applications	▪ Scan cloud deployed web applications	**IBM Rational AppScan Suite**		X	
Infrastructure	▪ Defend users and apps from network attacks	**IBM Security Network Intrusion Prevention System**	X		
	▪ Protect VMs and hypervisor from advanced threats	**IBM Virtual Server Protection for VMware**	X	X	
	▪ Provide patch and config management of VMs	**IBM Tivoli Endpoint Manager for Security and Compliance**		X	X
Services	▪ Understand the concerns of your unique cloud initiative	**IBM Cloud Security Roadmap Service**	X		

IBM also offers unmatched global coverage and security research



IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration

10B analyzed Web pages & images

150M intrusion attempts daily

40M spam & phishing attacks

46K documented vulnerabilities

Millions of unique malware samples

X-FORCE

World Wide Managed Security Services Coverage

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 13B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)

IBM continues to research, test and document more focused approaches to cloud security

IBM Research

Special research concentration in cloud security

IBM X-Force

Proactive counter intelligence and public education

Customer Councils

Real-world feedback from clients adopting cloud

Standards Participation

Client-focused open standards and interoperability

IBM Institute for Advanced Security

Collaboration between academia, industry, government, and the IBM technical community

Cloud computing
White paper
November 2009

IBM Point of View:
Security and Cloud Computing

Redpaper

Axel Buecker
Koos Lodewijks
Harold Moss
Kevin Skapinetz
Michael Waidner

Cloud Security Guidance
IBM Recommendations for the Implementation of Cloud Security

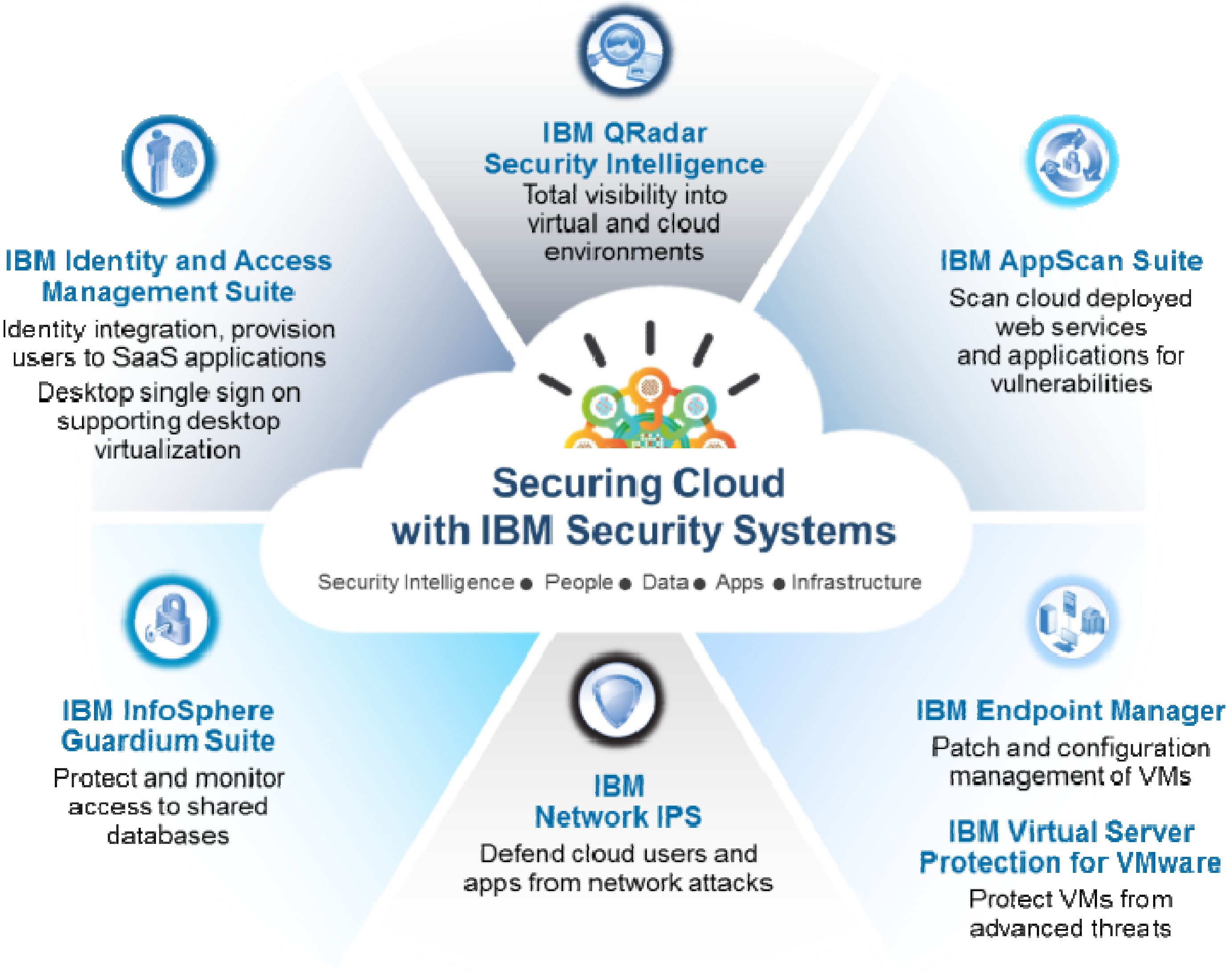
Thought Leadership White Paper

Cloud Computing

Cloud Security
Who do you trust?

Nick Coleman, IBM Cloud Security Leader
Martin Borrett, IBM Lead Security Architect

IBM has a broad portfolio of products and services to help satisfy these key security concerns



IBM QRadar Security Intelligence
Total visibility into virtual and cloud environments

IBM Identity and Access Management Suite
Identity integration, provision users to SaaS applications
Desktop single sign on supporting desktop virtualization

IBM AppScan Suite
Scan cloud deployed web services and applications for vulnerabilities

Securing Cloud with IBM Security Systems
Security Intelligence ● People ● Data ● Apps ● Infrastructure

IBM InfoSphere Guardium Suite
Protect and monitor access to shared databases

IBM Network IPS
Defend cloud users and apps from network attacks

IBM Endpoint Manager
Patch and configuration management of VMs

IBM Virtual Server Protection for VMware
Protect VMs from advanced threats