Securing IBM SmartCloud Services

Neil Readshaw
Worldwide Chief Architect – Cloud Security
IBM Global Technology Services

Pulse2012
Meet the Experts. Optimise your infrastructure.

May 31 – June1
Sheraton on the Park Hotel, Sydney

Agenda

- IBM point of view on Cloud Security
- Securing IBM SmartCloud Services
- IBM as a consumer of SmartCloud Services

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.

This is no different to how transformational technologies of the past **overcame concerns** – PCs, outsourcing, the Internet.

Each cloud deployment model has different security considerations

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*

The IBM approach is to align security 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.
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

Each cloud adoption pattern has its own set of key security concerns

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
Cloud Enabled Data Center	**Cloud Platform Services**	**Cloud Service Provider**	**Business Solutions on Cloud**
Integrated service management, automation, provisioning, self service	***Pre-built, pre-integrated IT infrastructures tuned to application-specific needs***	***Advanced platform for creating, managing, and monetizing cloud services***	***Capabilities provided to consumers for using a provider's applications***
Key security focus: **Infrastructure and Identity**	Key security focus: **Applications and Data**	Key security focus: **Data and Compliance**	Key security focus: **Compliance and Governance**
▪Manage datacenter identities ▪Secure virtual machines ▪Patch default images ▪Monitor logs on all resources ▪Network isolation	▪Secure shared databases ▪Encrypt private information ▪Build secure applications ▪Keep an audit trail ▪Integrate existing security	▪Isolate cloud tenants ▪Policy and regulations ▪Manage security operations ▪Build compliant data centers ▪Offer backup and resiliency	▪Harden exposed applications ▪Securely federate identity ▪Deploy access controls ▪Encrypt communications ▪Manage application policies

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

IBM is working with clients as both a cloud service provider and trusted advisor

Secure IBM Clouds

IBMSmartCloud

Reduce costs.
Improve service delivery.
Enable business innovation.

Leveraging IBM's deep security skillset, 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

Capabilities

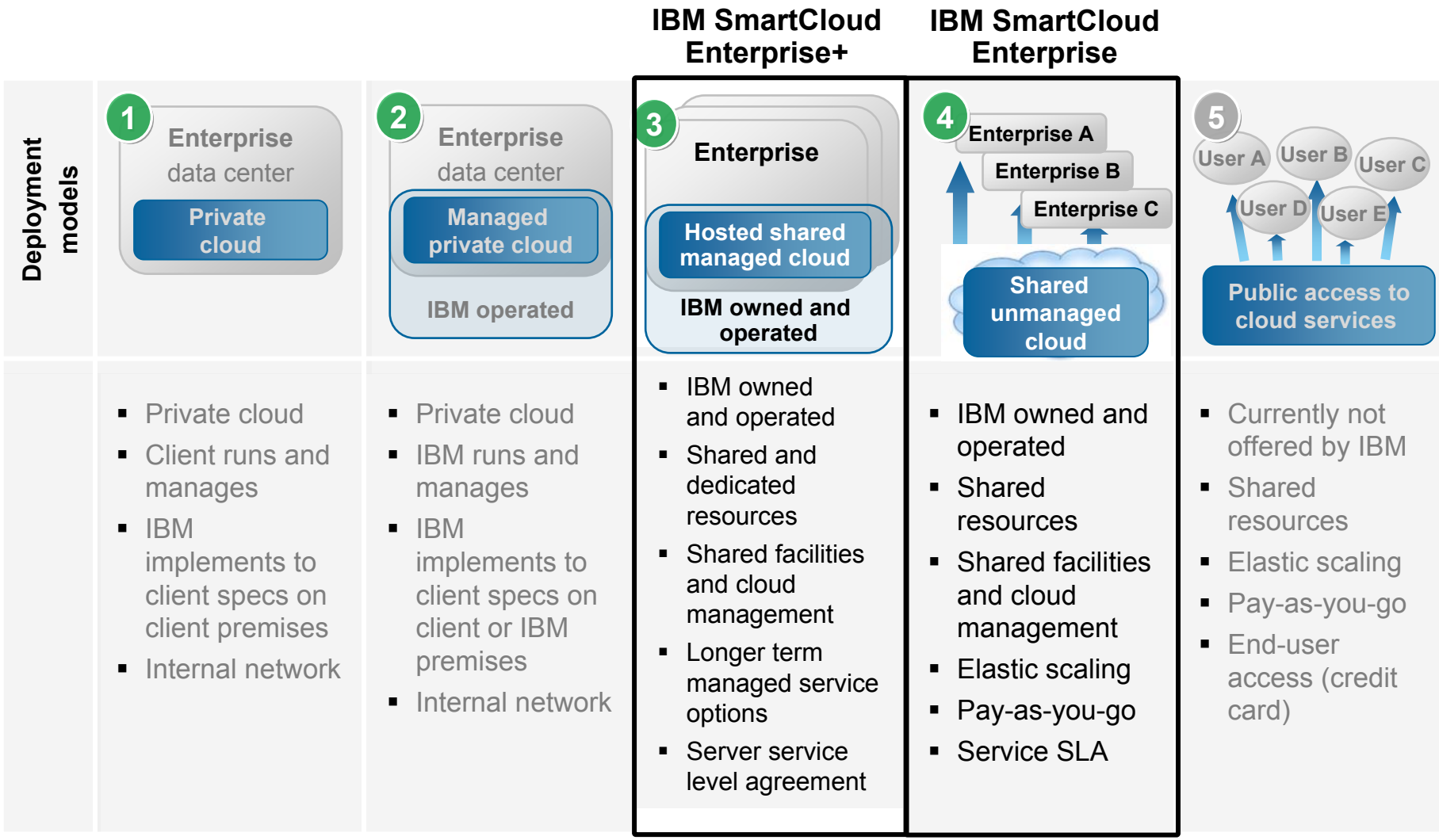
Knowledge

IBM Security Solutions

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

IBM SmartCloud Services offer a broad choice of delivery models

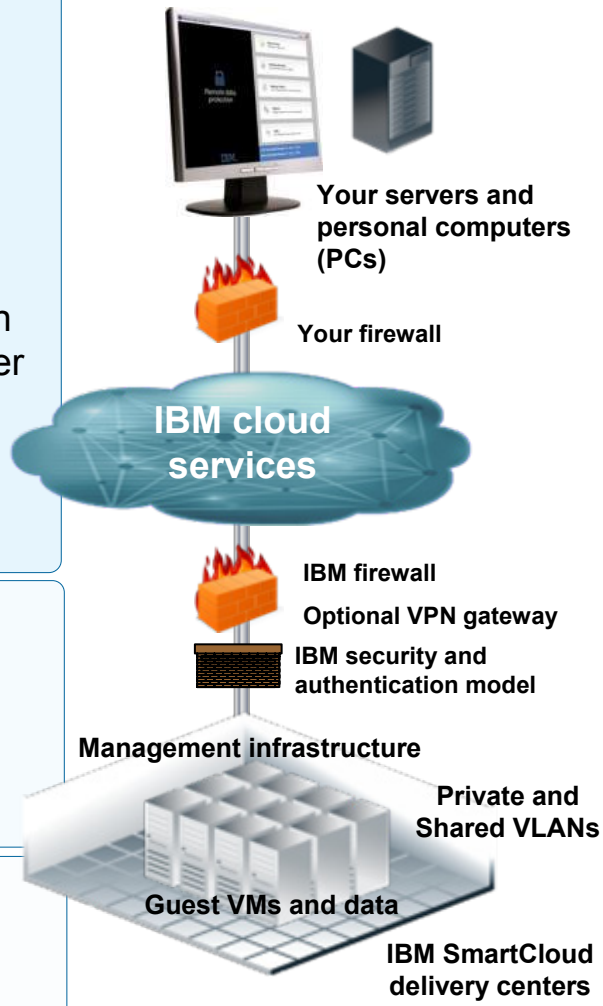


Security is built into IBM SmartCloud Enterprise

Virtual infrastructure
- Hypervisor-based isolation with customer configurable firewall rules
- Physical firewall and intrusion prevention service/intrusion detection service (IPS/IDS) between guest virtual machines (VMs) and Internet
- Multiple IP addresses per instance with which to enable security zones
- Optional virtual private network (VPN) and virtual local area network (VLAN) isolation of account instances
- Connections may be encrypted and IBM is isolated from VMs by design (using secure shell keys in Linux® and Microsoft® Windows® Server user access control)
- Client has root access to guest virtual machines allowing further hardening of VMs, e.g. in-guest encryption
- Shared images are patched and scanned regularly

Management infrastructure
- Access to the infrastructure is only enabled using IBM Web Identity through the user interface portal or application programming interfaces
- Complies with IBM security policies, including regular security scans
- Controlled and audited administrative actions and operations

Delivery centers
- Customer data and VMs are kept in the data center where provisioned
- Physical security same as for IBM's internal data centers

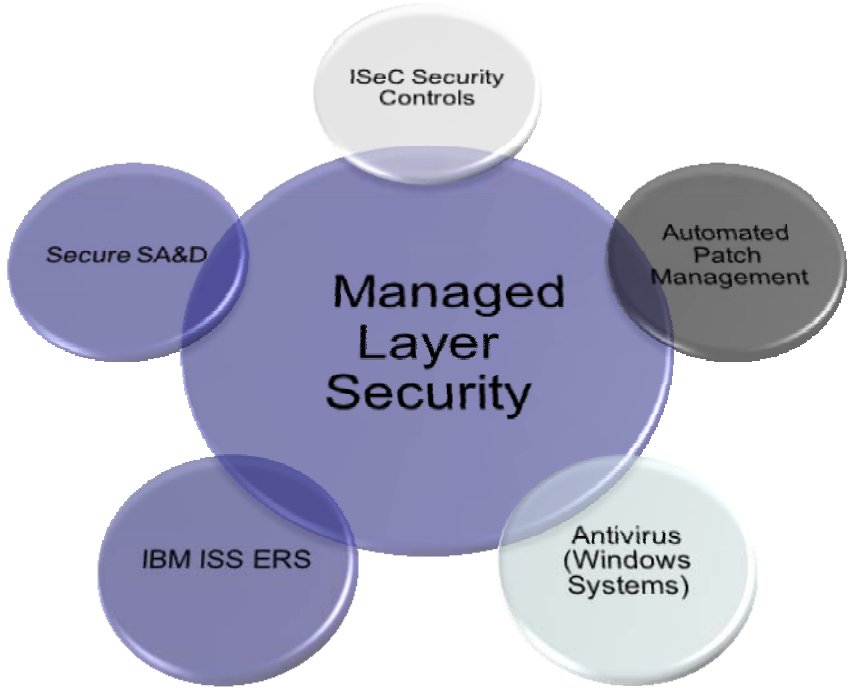


IBM SmartCloud Enterprise+ implements security controls that meet or exceed industry best practices at the Management layer

- Built on secure building blocks from IBM's experience in strategic outsourcing
- Network isolation using :
  - 802.1q (secure trunking)
  - 802.3ad (channelling)
  - VLAN
- Separate VLAN for access to management infrastructure
  - Storage is separated using zoning + hypervisor isolation
- Regular validation of security parameters and policies using strategic IBM tools
- Strict adherence to IBM corporate patch and vulnerability scanning management practices
- Standard methods to support the customer's existing Enterprise Directory (AD, LDAP, etc)
- Hosted in a Tier 3 (UTI-3) data center
- Regular vulnerability scanning

IBM SmartCloud Enterprise+ managed environment adopts standard IBM security controls which have been used to secure thousands of customers across the globe

- ISO/IEC 27001/2 based security policy which supports industry and regulatory requirements
- Hardened OS images, validated using strategic IBM tools
- Securely configured middleware, based on security policy specifications
- Automated validation against defined security controls
- Automated processes for Service Activation and Deactivation (SA&D) and patch management
  - Activation
    - Patch installation
    - Security control applied
  - Deactivation
    - Zeroing of virtual disk
    - Invalidation of previous backups



IBM Security Solutions used in SmartCloud Services today

- Cloud Management Portal uses IBM Security Access family for web access management

- Network intrusion detection/prevention uses IBM Security Network IPS
  - Consumed as a managed service

- IAM solution for privileged administrator access to cloud infrastructure uses Tivoli Identity Manager
  - Reusing a standard solution in-place

- Rational AppScan is used for web application vulnerability testing
  - Integrated with the development process

- Security compliance management of client workloads uses Tivoli Endpoint Manager (SCE+ only)

Emerging requirements driving SmartCloud Services security roadmap

- Security intelligence

- IAM integration with external entities
  - On-premise enterprise IAM
  - Multi-factor authentication

- Delegated authorization for REST APIs

- Additional defense in depth for workload isolation
  - Hypervisor security, storage encryption

Lessons learned/re-affirmed from IBM internal adoption of SmartCloud Services

- Make CIO Office/Cybersecurity policies and procedures ‘cloud aware’
  - Governance on which workloads run in which clouds
  - Security incident management

- Make workload owners aware of their security management responsibilities
  - Ongoing education and awareness on what cloud provides and what they must do themselves
  - Integration with existing IBM systems supporting security and compliance
  - Automating compliance management

Questions?

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

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 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 throughput or performance improvements equivalent to the ratios stated here.

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.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.