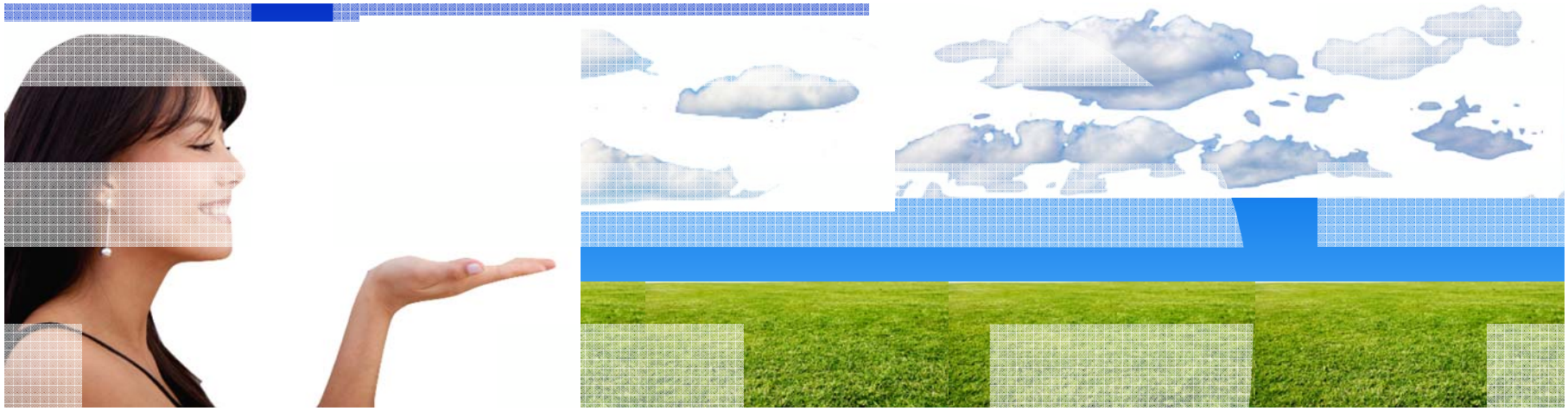
Cloud Computing: Getting the benefits by navigating the security challenges

Neil Readshaw, CISSP
Cloud Security Lead Architect
IBM Global Technology Services



Agenda

- Security Challenges in Cloud Computing
- Approaches for Cloud Security
- Example: Identity/Access Management and Cloud
- IBM Security Solutions for Cloud Computing

Security Challenges in Cloud Computing

Cloud security concerns

Less 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.

Data Security

Migrating workloads to a **shared** network and compute **infrastructure** increases the potential for **unauthorized exposure**. Authentication and access technologies become increasingly important.

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.

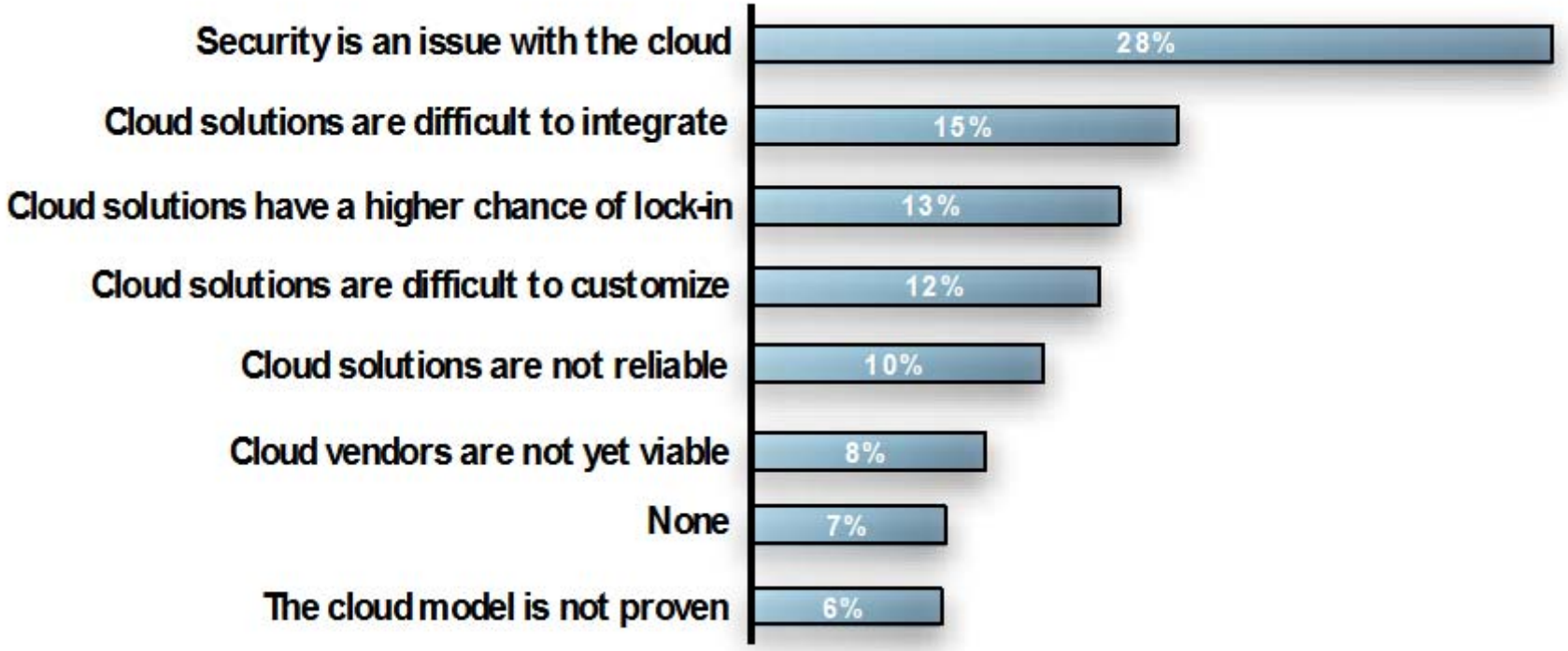
Compliance

Complying with SOX, HIPPA and other **regulations may prohibit** the use of clouds for some applications. Comprehensive auditing capabilities are essential.

Security Management

Providers must supply easy, visual controls to **manage firewall and security settings** for applications and runtime environments in the cloud.

What can we learn from companies who have already adopted public cloud solutions?



Appirio, State of the Public Cloud: The Cloud Adopters' Perspective, October 2010
http://thecloud.appirio.com/StateofthePublicCloudWhitepaper1.html

What is different about Cloud Security?

Consideration	What makes it different?
Data Locality	Data may no longer be protected by the same laws and regulations as if it was still in your on-premise environments.
Multi-tenancy	Workloads may be running on the same physical infrastructure as those of other organizations. Cloud management interfaces are used by multiple tenants to manage their use of the cloud.
Virtualization	The hypervisor adds an additional layer subject to its own threats and vulnerabilities.
Cloud Provider Administration	Cloud provider's administrators are not necessarily subject to the same controls as in the on-premise case.

The combination of these considerations is a consideration as well.

Approaches for Cloud Security

Consider cloud security from one or more of these perspectives

FOR the Cloud

- How to build clouds securely?
- How to evaluate and trust clouds and cloud providers?

WITH the Cloud

- How to use cloud based IT services securely?
- How to integrate security of on-premise and cloud based IT services?

FROM the Cloud

- How to leverage security services delivered via a cloud based model, for on-premise or cloud based IT?
- How to compare to equivalent on-premise security solutions?

Foundational controls for Cloud Security

1. Identity and Access Management

Strong focus on authentication of users and management of user identity

2. Discover, Categorize, Protect Data & Information Assets

Strong focus on protection of data at rest or in transit

3. Information Systems Acquisition, Development, and Maintenance

Management of application and virtual machine deployment

4. Secure Infrastructure Against Threats and Vulnerabilities

Management of vulnerabilities and their associated mitigations with strong focus on network and endpoint protection

5. Problem & Information Security Incident Management

Management and responding to expected and unexpected events

6. Physical and Personnel Security

Protection for physical assets and locations including networks and data centers. Employee security.

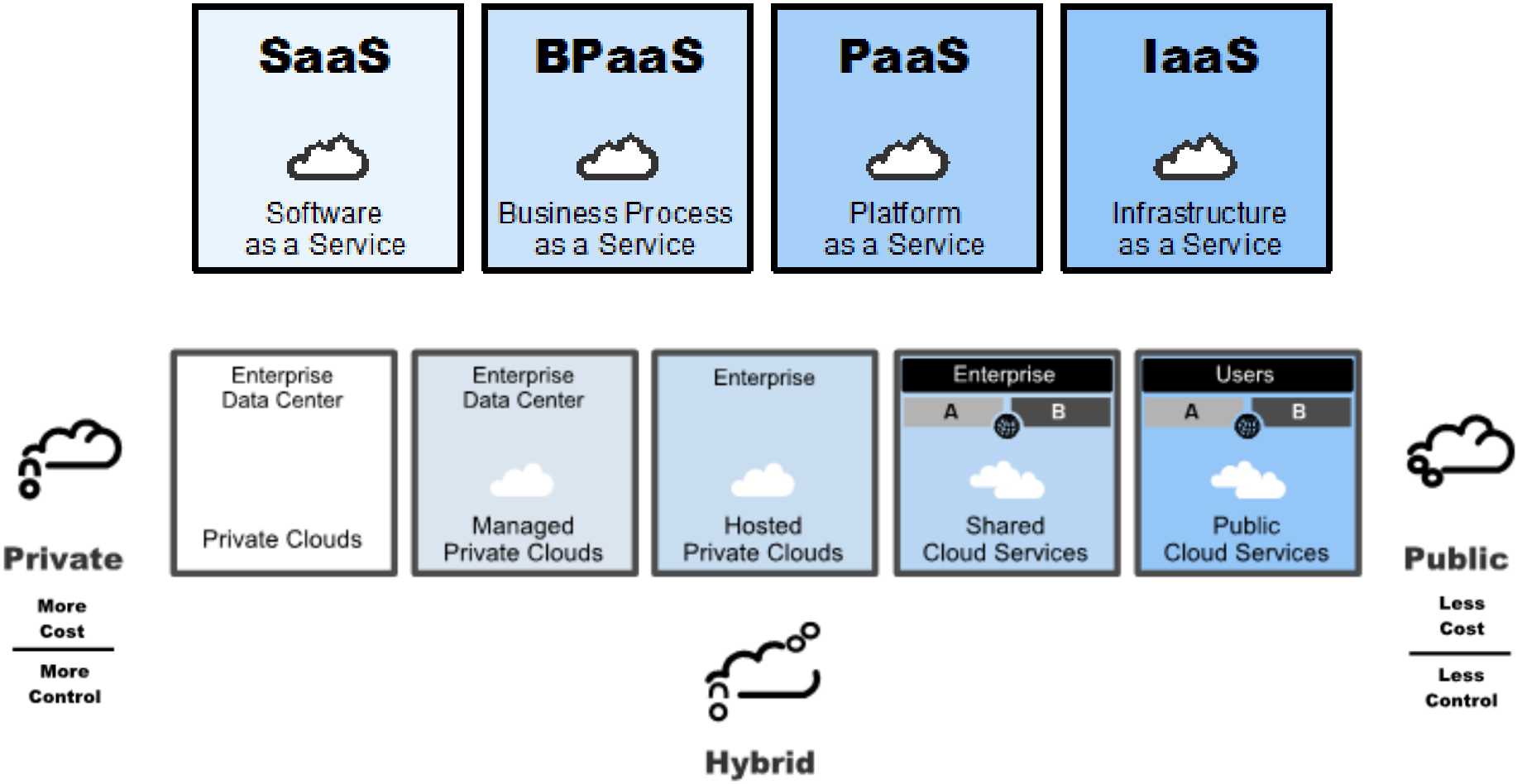
7. Security Governance, Risk Management & Compliance

Security governance including maintaining security policy and audit and compliance measures

8. Cloud Governance

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

Cloud deployment and delivery patterns influence the type and extent of security controls



There is no single product or service for Cloud Security

Cloud could be more secure than traditional enterprise IT in some cases

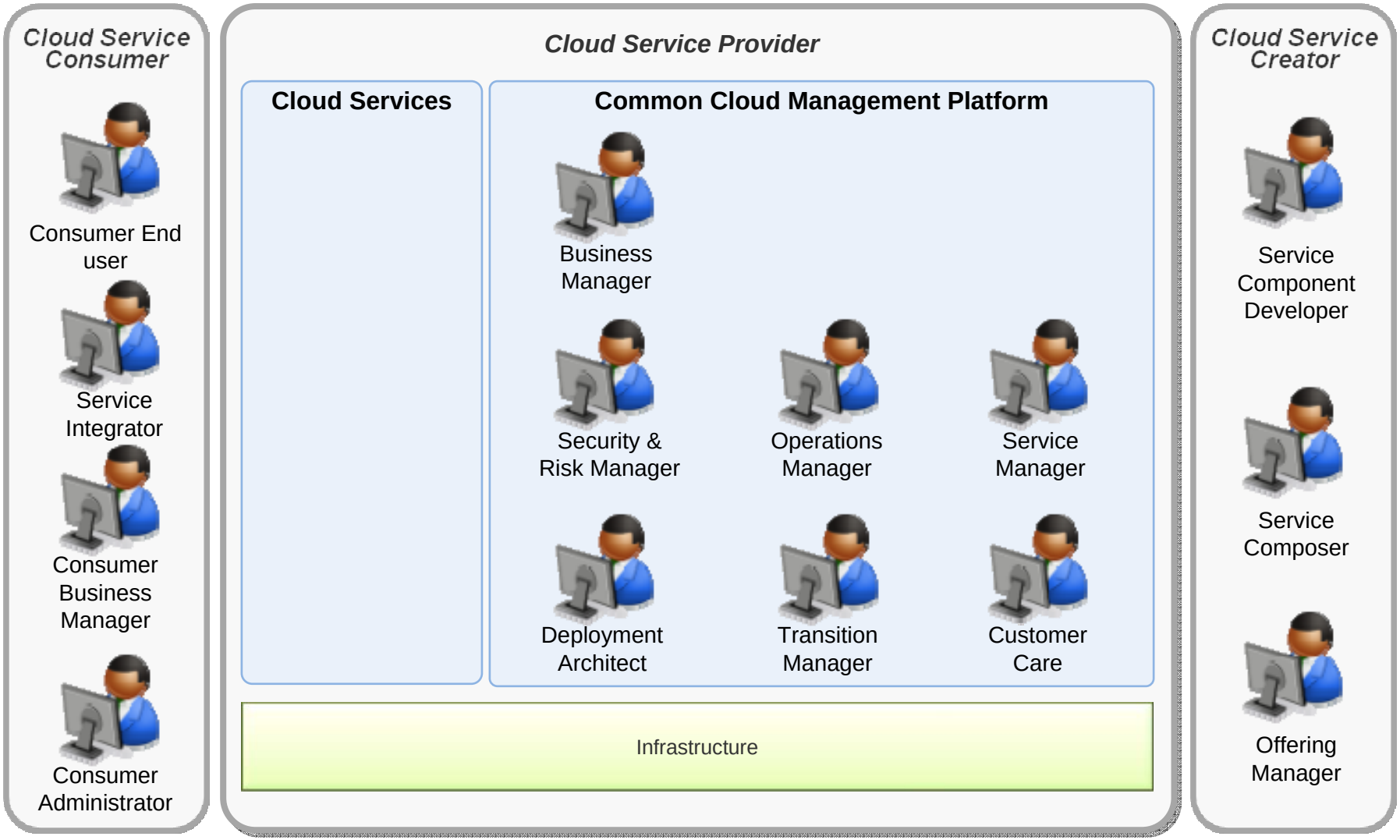
Security by Design

Security by Workload

New Security Efficiencies

Example: Identity/Access Management and Cloud

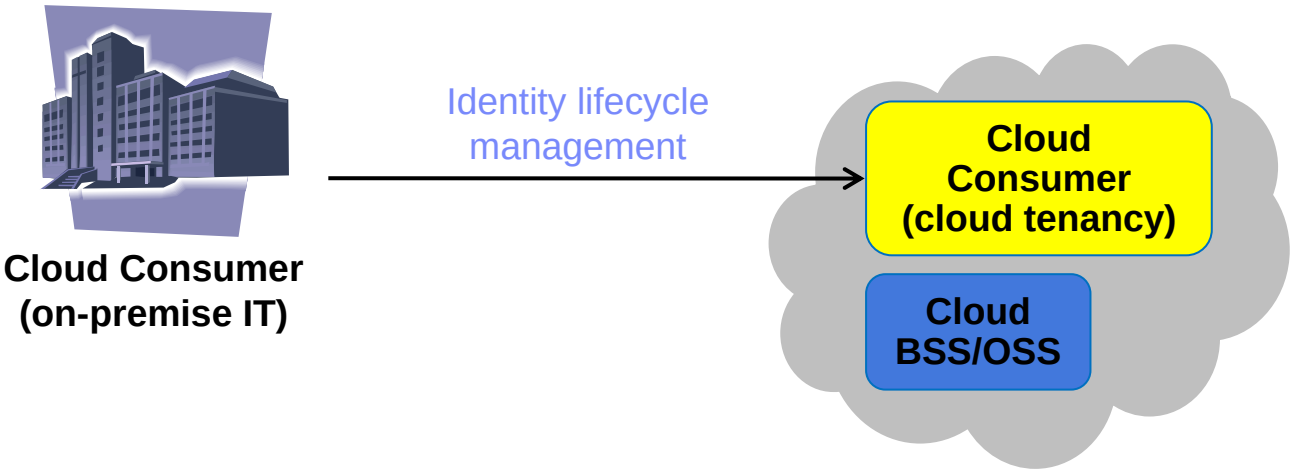
Identity/access model for a multi-tenant cloud must support a variety of roles and their entitlements



Identity Management and Cloud – Hype and Reality

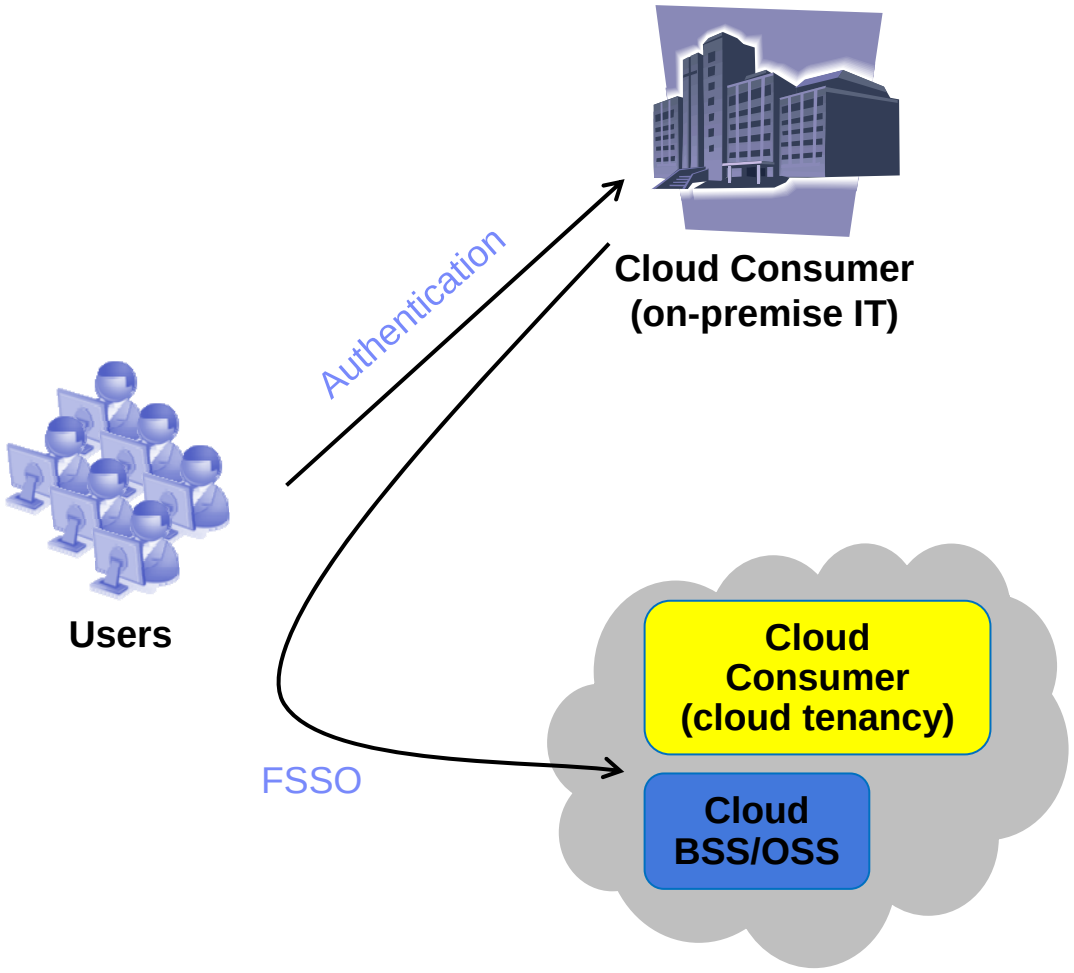
Hype	Reality
New identity management methods and tools are needed to support cloud deployments.	Customer are using enterprise identity management as an enabler for cloud services.
Only identity providers such as Google and Facebook are providing support for cloud deployments.	Customers are using existing enterprise access management systems to integrate enterprise and cloud identities.
Standards such as OpenID, OAuth, SPML are mandatory to integrate on-premise and cloud identities	Customers are determining the use of these standards based on the workload.

Integrate on-premise identity governance with the Cloud



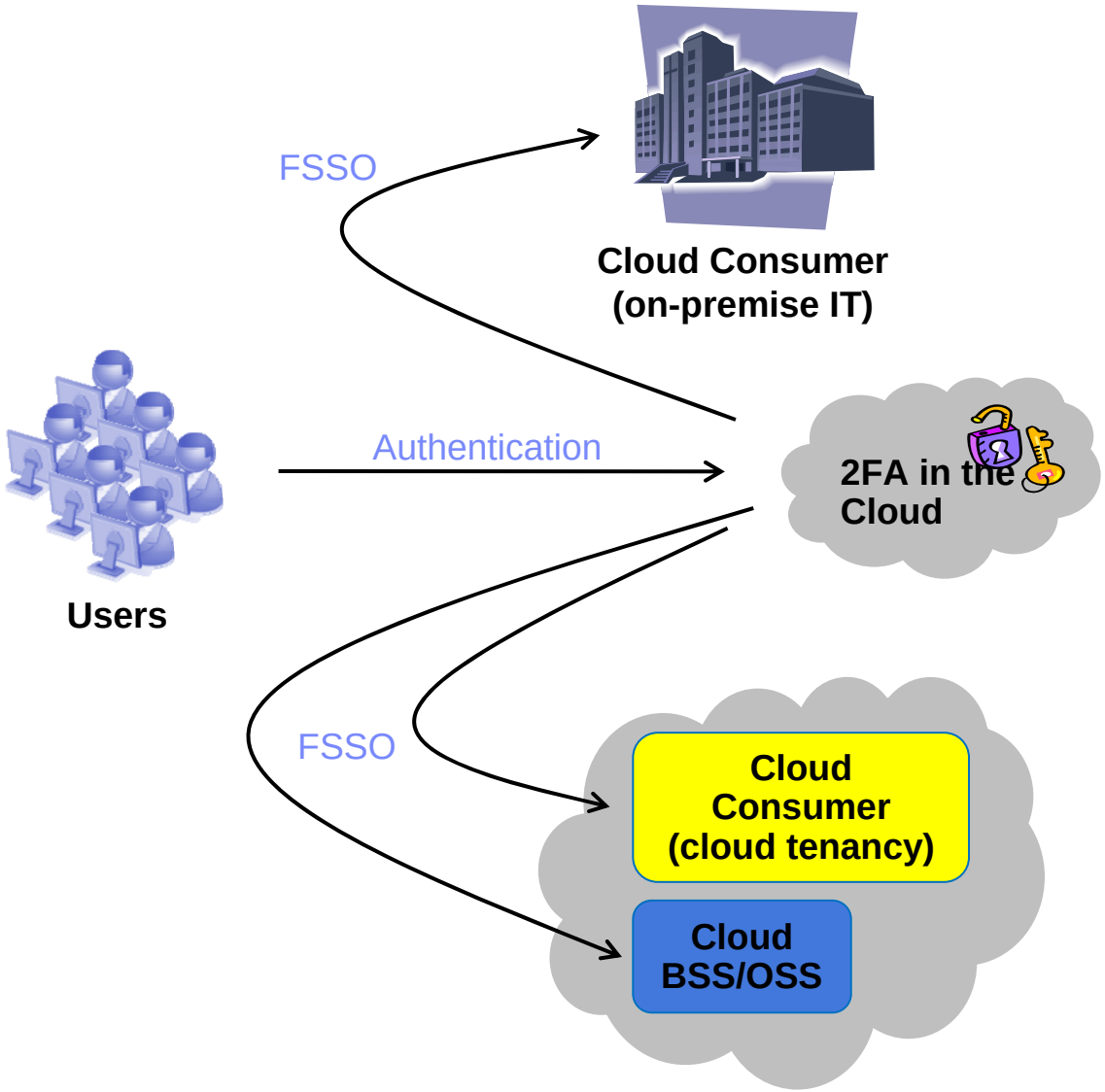
- Extend on-premise identity governance capabilities to IT services hosted in the Cloud
- Standards are not widely adopted at this time
  - SPML is one potential standard
- Example: Manage users and groups within a GoogleApps domain from on-premise identity lifecycle management

Integrate on-premise authentication with the Cloud



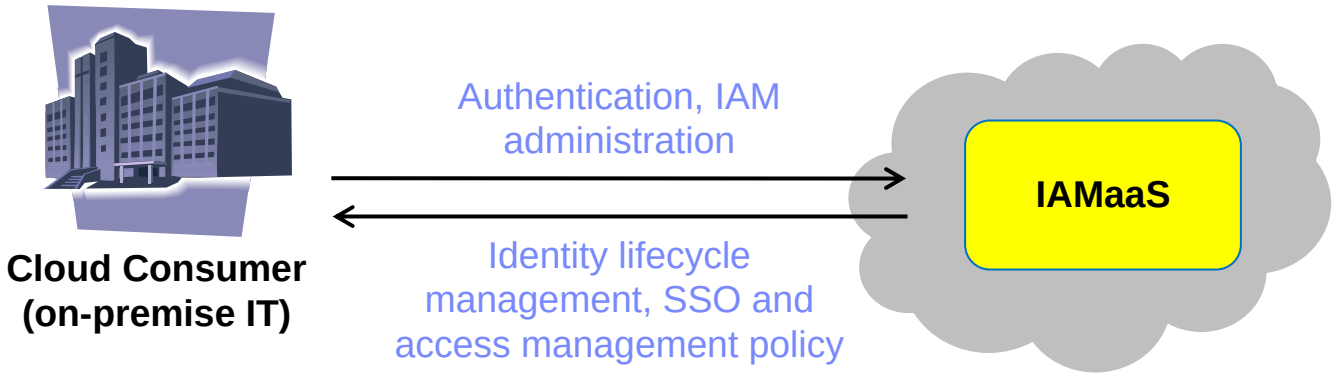
- Reuse existing on-premise identity and credential stores
- Federated Single Sign-on (FSSO) may be the integration approach
  - FSSO standards include SAML, WS-Federation
- Example: Use SAML to integrate with Salesforce.com

Strong authentication from the Cloud



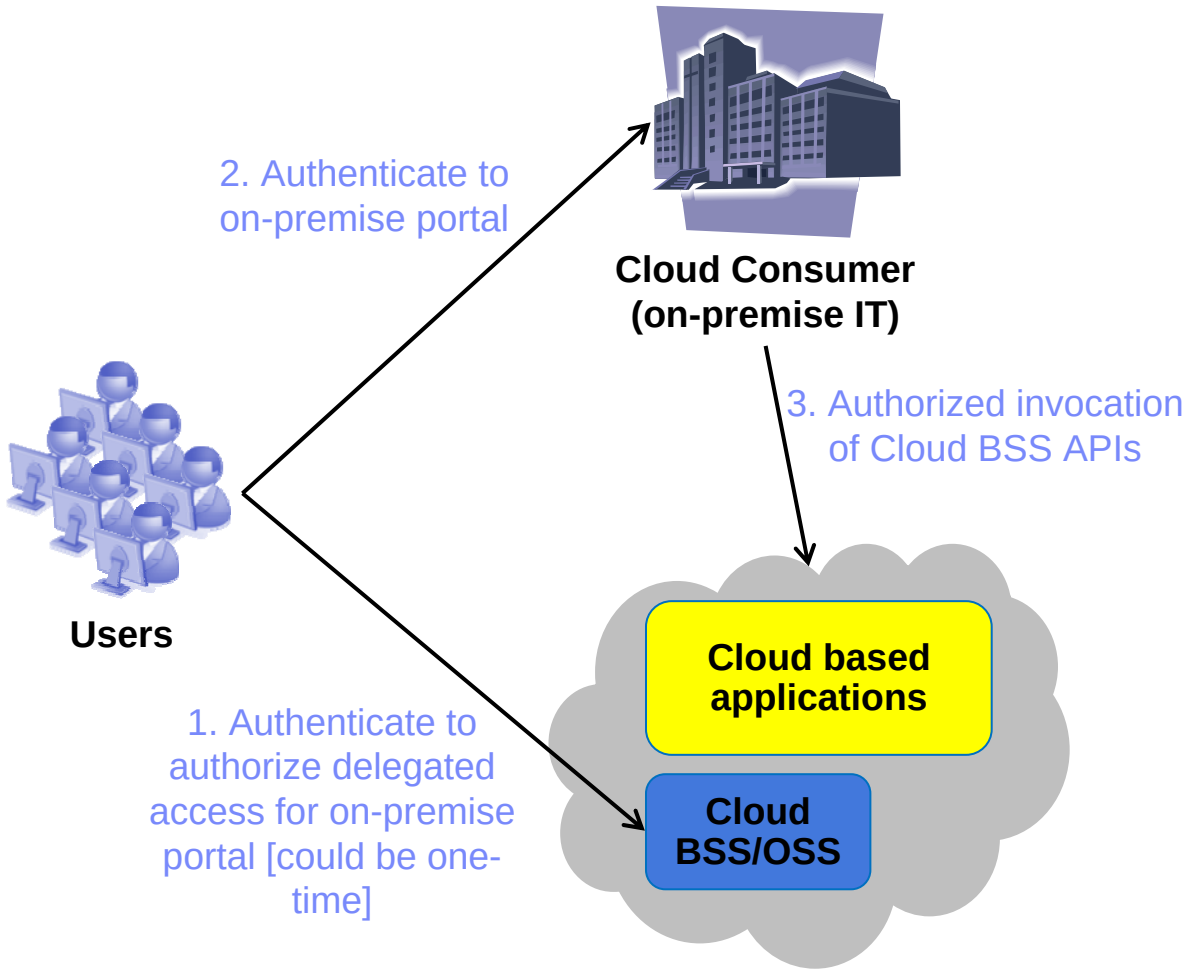
- Potential integration with on-premise or cloud IT
- Federated Single Sign-on (FSSO) may be the integration approach
  - FSSO standards include SAML, WS-Federation
- Example: authentication based on possession of a mobile device

Identity and access management from the Cloud



- An alternative model for delivery of IAM services, while retaining the rich capabilities of on-premise systems
- Suitable for many, but not all customers
- Example: IAMaaS delivered by traditional IAM vendors or their partners

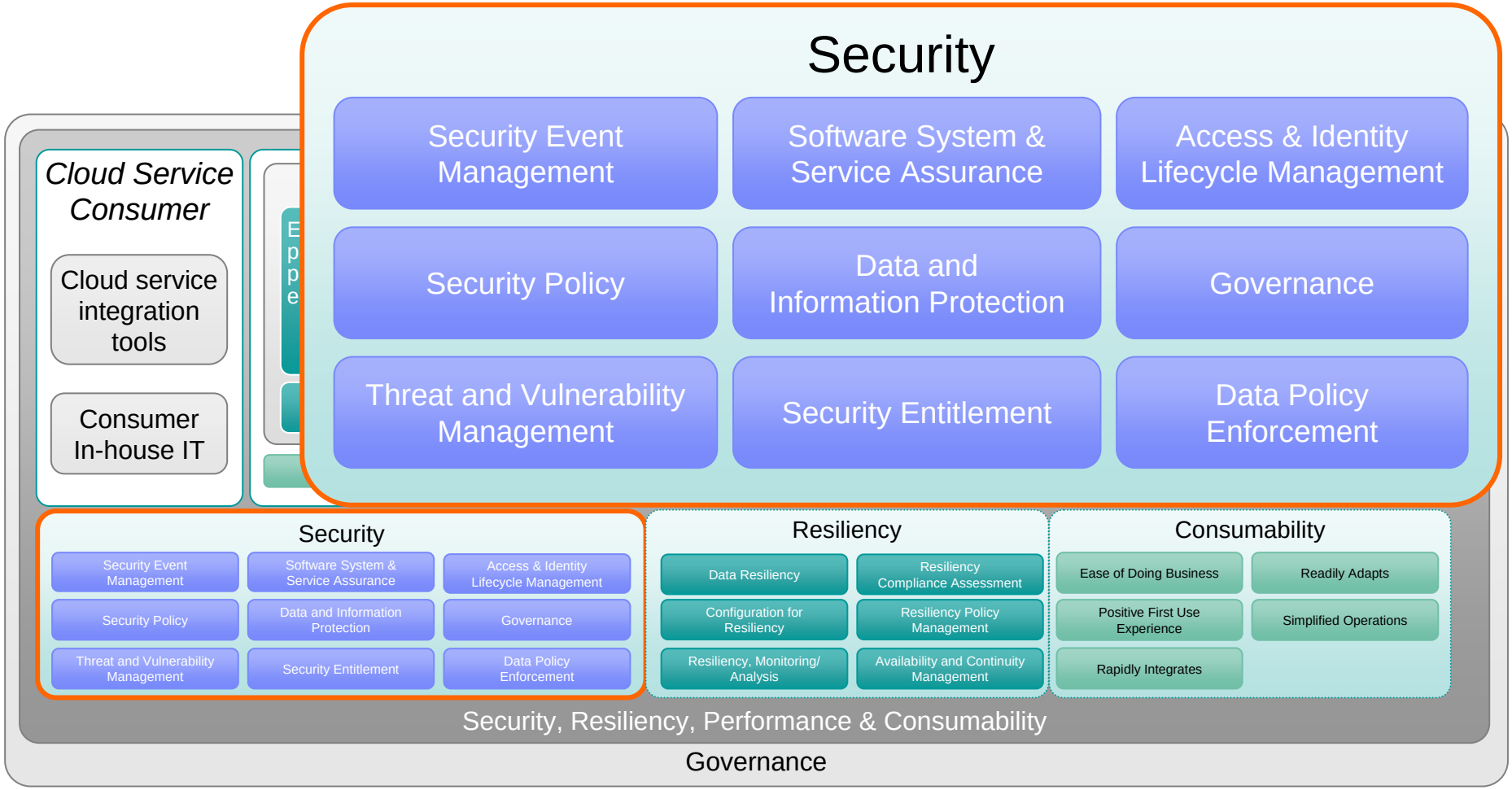
Integrate access management of on-premise portal with Cloud management platform



- On-premise portal aggregates across multiple cloud providers
- Use of Cloud APIs is authorized based on user identity, not just the enterprise's
- Example: Use OAuth for scoped, delegated authorization of Cloud BSS APIs

IBM Security Solutions for Cloud Computing

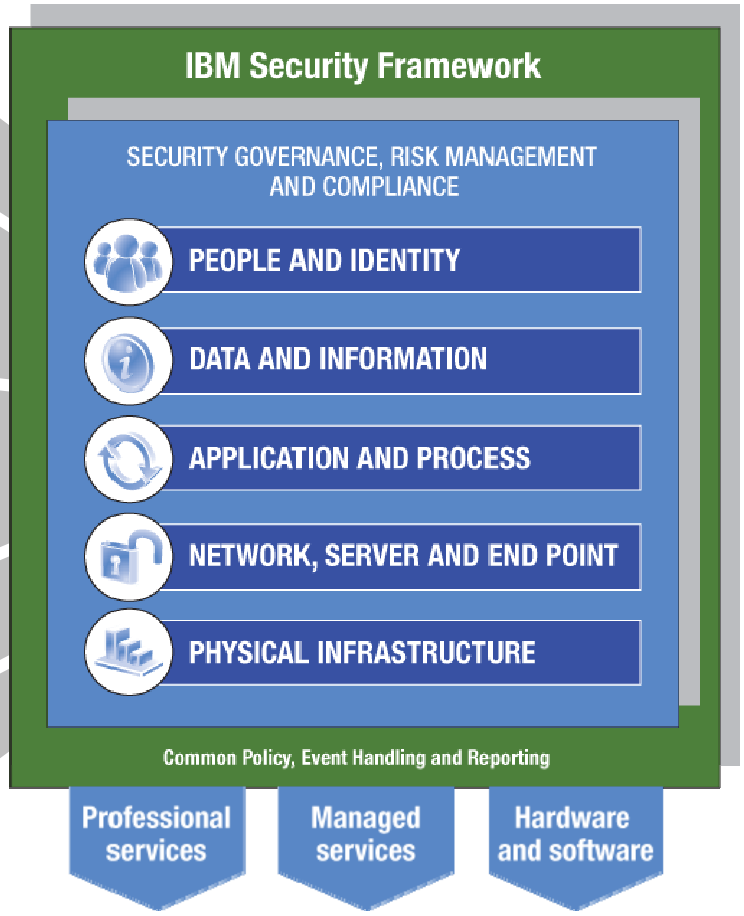
The IBM Cloud Computing Reference Architecture consolidates IBM wide expertise and experience



Security is a fundamental component in this architecture

Top security concerns for cloud computing map directly to the IBM Security Framework

- Privileged User Access
- Data Segregation
- Data Recovery
- Investigative Support
- Regulatory Compliance
- Data Location
- Disaster Recovery



Gartner: Assessing the Security Risks of Cloud Computing, June 2008

http://www.redbooks.ibm.com/abstracts/redp4528.html

Controls employed in IBM Clouds map to the IBM Security Framework

	Cloud Enabled Control(s)	Benefit
People and Identity	• Centralized IAM • Integration between on-premise and cloud identity	• Reduced risk of unauthorized access • Reduced operational cost
Information and Data	• Workloads running in isolated domains • Encryption of data in motion and at rest	• Reduced risk of data leak/loss
Process & Application	• Autonomous security policies and procedures • SLA-backed availability and confidentiality	• Improved protection of assets
Network Server and Endpoint	• Automated provisioning and reclamation of hardened runtime images • Multiple levels of intrusion management	• Improved forensics with ensemble snapshots • Reduced attack surface
Physical infrastructure	• Physical security of cloud data centers • Convergence of physical and logical identity and access systems.	• Improved ability to enforce access policy and manage compliance

Clients and IBM itself are implementing IBM Security solutions as foundational controls to address their cloud security needs

IBM Smart Cloud Enterprise LotusLive	**Business Challenge**	Secure IBM Public Cloud and SaaS offerings and help differentiate from its competitors
	IBM Solution	▪ IBM Security Network Intrusion Prevention System ▪ Tivoli Access Manager and Federated Identity Manager ▪ Tivoli Directory Integrator and Directory Server

IBM Smart Cloud Enterprise+	**Business Challenge**	Secure Hybrid/Private Cloud solution (in development) to share business services across the ecosystem
	IBM Solution	▪ Tivoli Access and Federated Identity Manager ▪ Tivoli Directory Integrator and Directory Server ▪ *IBM Security Virtual Server Protection (in plan)*

MOLSON Coors Vantis Life A better life experience.	**Business Challenge**	Adopt Tivoli IAM as SaaS to address the changing business needs, without having to maintain the infrastructure on premise
	IBM Solution	Lighthouse Gateway SaaS platform using ▪ Tivoli Identity, Access Manager and Federation ▪ Tivoli Directory Integrator and Server ▪ *Tivoli Security Information and Event Manager (in plan)*

Security services offer expertise for moving to secure cloud

IBM Professional Security Services
Security strategy roadmap for cloud computing

IBM Professional Security Services
Security assessment services for cloud computing

IBM Professional Security Services
Application security services for cloud computing

IBM Information Protection Services
IBM SmartCloud Managed Backup

IBM Managed Security Services
Hosted vulnerability management

IBM Managed Security Services
Hosted security event and log management

Conclusion

- Security solutions required for Cloud Computing vary, based on:
  - Cloud delivery model
  - Workload
  - Compliance requirements
- Security for Cloud Computing needs to be equivalent or better to security for traditional IT environments
  - Based on the same foundational controls
- Identity and access management is a logical starting point for integrating on-premise and cloud security services
- IBM Security solutions are being used today by customers and IBM itself to deliver secure solutions for, with and from the Cloud

References

References

- Cloud Computing Security Considerations, Australian Department of Defence
  - http://www.dsd.gov.au/infosec/cloudsecurity.htm
- Cloud Computing - Benefits, risks and recommendations for information security, European Network and Information Security Agency
  - http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
- Cloud Controls Matrix, Cloud Security Alliance
  - http://www.cloudsecurityalliance.org/cm.html
- Guidelines on Security and Privacy in Public Cloud Computing (SP 800-144), NIST
  - http://www.nist.gov/itl/csd/cloud-020111.cfm

Cloud Computing Whitepaper

IBM has a proven reference architecture for building and managing cloud solutions, providing an integrated approach that uses the same standards and processes across the entire portfolio of products and services.

IBM's expertise and experience in designing, building and implementing cloud solutions — beginning with its own — offers clients the confidence of knowing that they are engaging not just a provider, but a trusted partner in their IT endeavours.

The IBM Cloud Computing reference architecture builds on IBM's industry-leading experience and success in implementing SOA solutions.

http://www.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&appname=GTSE_CI_CI_USEN&htmlfid=CIW03078USEN&attachment=CIW03078USEN.PDF

IBM Cloud Security Guidance

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

Highlights a series of best practice controls that should be implemented

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

IBM

Redpaper

Axel Buecker
Koos Lodewijkx
Harold Moss
Kevin Skapinetz
Michael Waidner

Cloud Security Guidance

IBM Recommendations for the Implementation of Cloud Security

In this IBM® Redpapers™ publication, we provide a discussion about the IBM recommendations for the implementation of cloud security. To get started, let us begin with an introduction to cloud computing and cloud security in general.

Introduction to cloud computing

Cloud computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned *on demand*, regardless of the user location or device.

As a result, cloud computing gives organizations the opportunity to increase their service delivery efficiencies, streamline IT management, and better align IT services with dynamic business requirements. In many ways, cloud computing offers the *best of both worlds*, providing solid support for core business functions along with the capacity to develop new and innovative services.

Note: As an added benefit, cloud computing enhances the user experience without adding to its complexity. Users do not need to know anything about the underlying technology or implementations.

Both public and private cloud models are now in use. Available to anyone with Internet access, public models include *Software as a Service* (SaaS) clouds, such as IBM LotusLive, *Platform as a Service* (PaaS) clouds, such as Amazon Web Services, and *Security and Data Protection as a Service* (SDPaaS) clouds, such as IBM Security Event and Log Management Services.

Private clouds are owned and used by a single organization. They offer many of the same benefits as public clouds, and they give the owner organization greater flexibility and control.

http://www.redbooks.ibm.com/abstracts/redp4614.html?Open

Cloud Security Whitepaper

Trust needs to be achieved, especially when data is stored in new ways and in new locations, including for example different countries.

This paper is provided to stimulate discussion by looking at three areas:

- What is different about cloud?
- What are the new security challenges cloud introduces?
- What can be done and what should be considered further?

http://www-03.ibm.com/press/us/en/attachment/32799.wss?fileId=ATTACH_FILE1&fileName=10-0861_US%20Cloud%20Computing%20White%20Paper_Final_LR.pdf

Thank You

http://www.ibm.com/cloud

Backup

It’s time to start thinking differently about infrastructure

85% idle

In distributed computing environments, up to 85% of computing capacity sits idle.

70¢ per $1

70% on average is spent on maintaining current IT infrastructures versus adding new capabilities.

1.5x

Explosion of information driving 54% growth in storage shipments every year.

$40 billion

Consumer product and retail industries lose about $40 billion annually, or 3.5 percent of their sales, due to supply chain inefficiencies.

33%

33% of consumers notified of a security breach will terminate their relationship with the company they perceive as responsible.

Cloud Computing provides workload optimized models for delivery and consumption of IT services

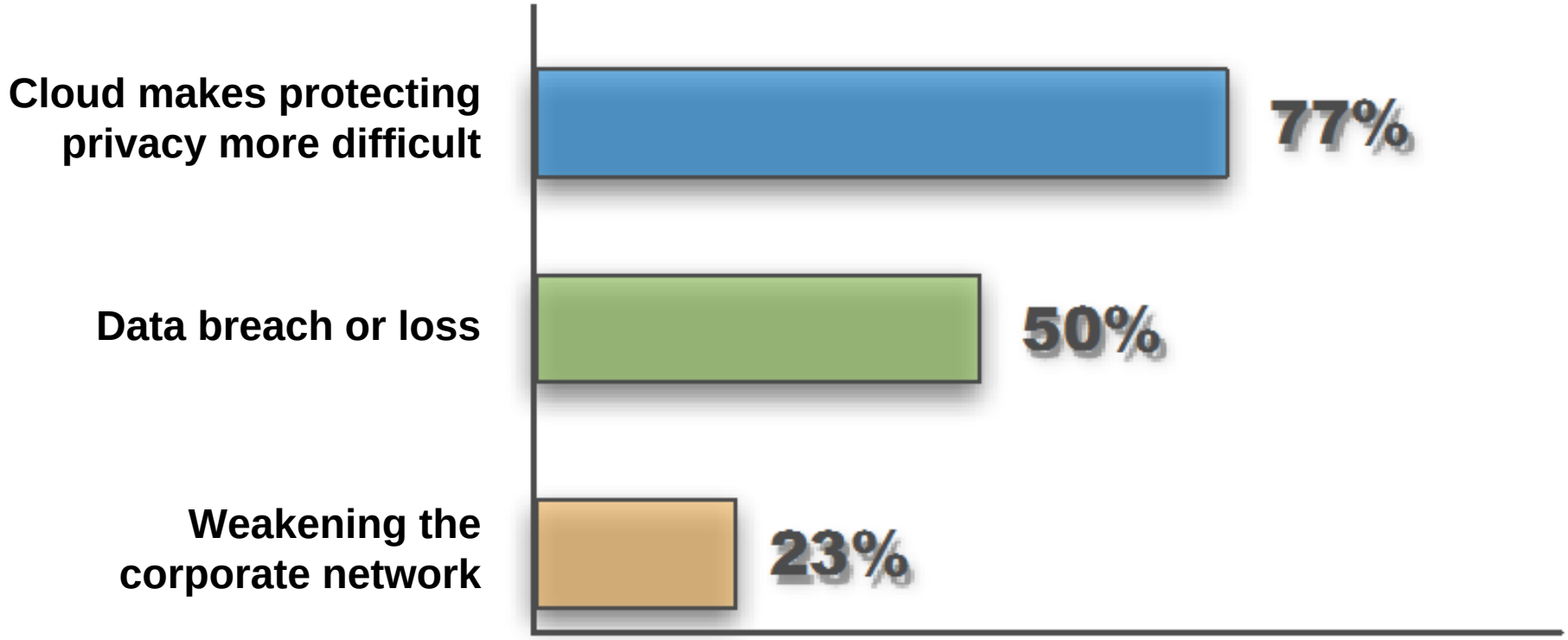
VIRTUALIZATION

AUTOMATION

STANDARDIZATION

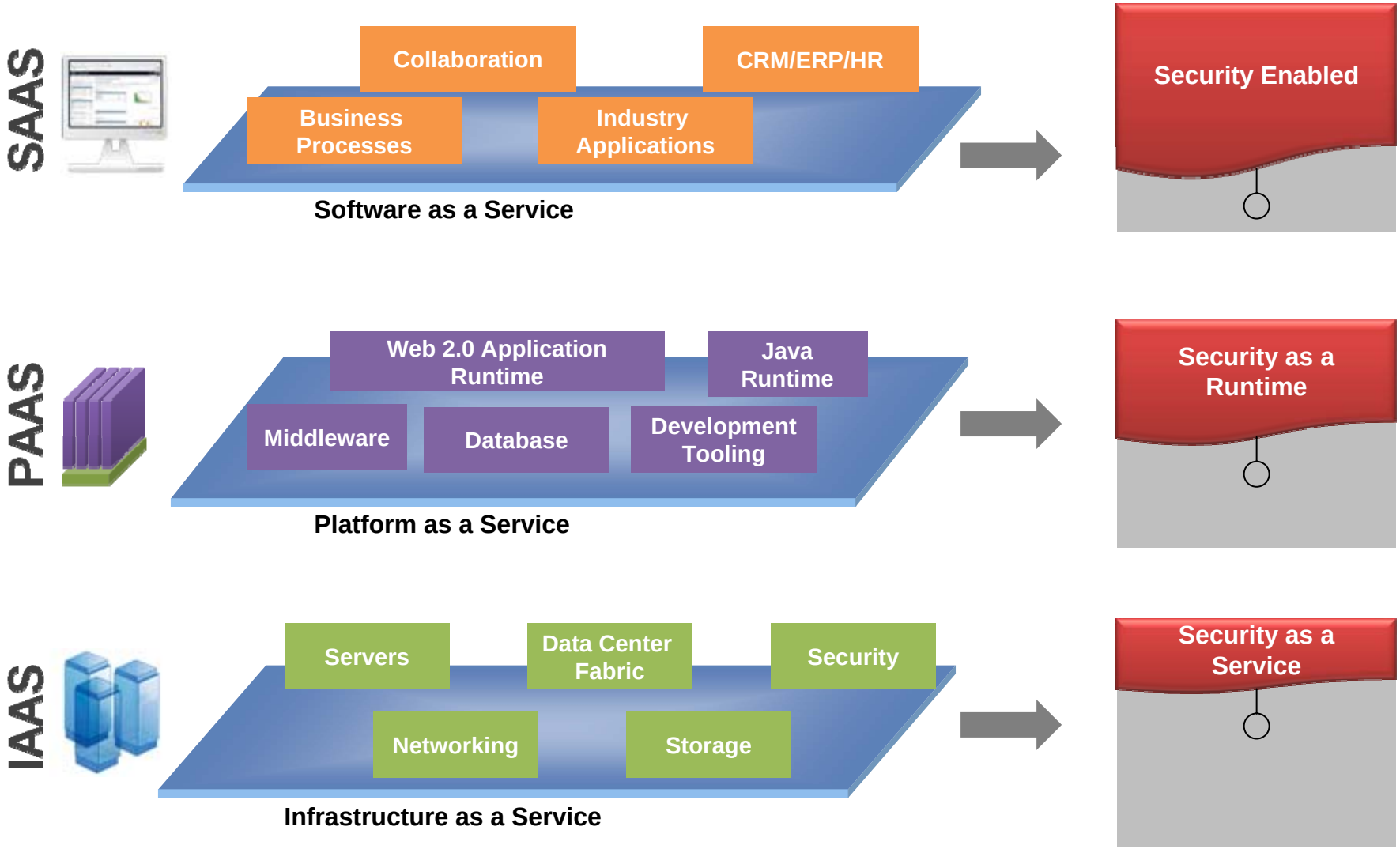
Attributes	Characteristics	Benefits
Advanced virtualization	IT resources can be shared between many applications. Applications can run anywhere.	Providing more efficient utilization of IT resources.
Automated provisioning	IT resources are provisioned or de-provisioned on demand.	Reducing IT cycle time and management cost
Elastic scaling	IT environments scale down and up as the need changes.	Increasing flexibility
Service catalog ordering	Defined environments can be ordered from a catalog.	Enabling self-service
Metering and billing	Services are tracked with usage metrics.	Offering more flexible pricing schemes
Internet Access	Services are delivered through the Internet.	Access anywhere, anytime

Cloud computing raised serious concerns among respondents about the use, access and control of data



Source: IBM Institute for Business Value 2010 Global IT Risk Study

Cloud deployment pattern influences the extent of security controls



Different workloads require different security controls in the Cloud

Simpler migration to the Cloud

- Analytics
- Infrastructure storage
- Industry applications
- Collaboration
- Workplace, desktop and devices
- Business processes
- Disaster recovery
- Development & Test
- Infrastructure Compute

New Business Model

- Collaborative health care
- Medical imaging
- Financial risk
- Energy management

Requires individual analysis

- Sensitive data
- Highly customized data
- Not yet virtualized software
- Legal restrictions
- Complex processes and transactions
- Regulation intensive systems
- Mature workload
- Isolated workload
- Preproduction systems
- Batch processing systems

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.