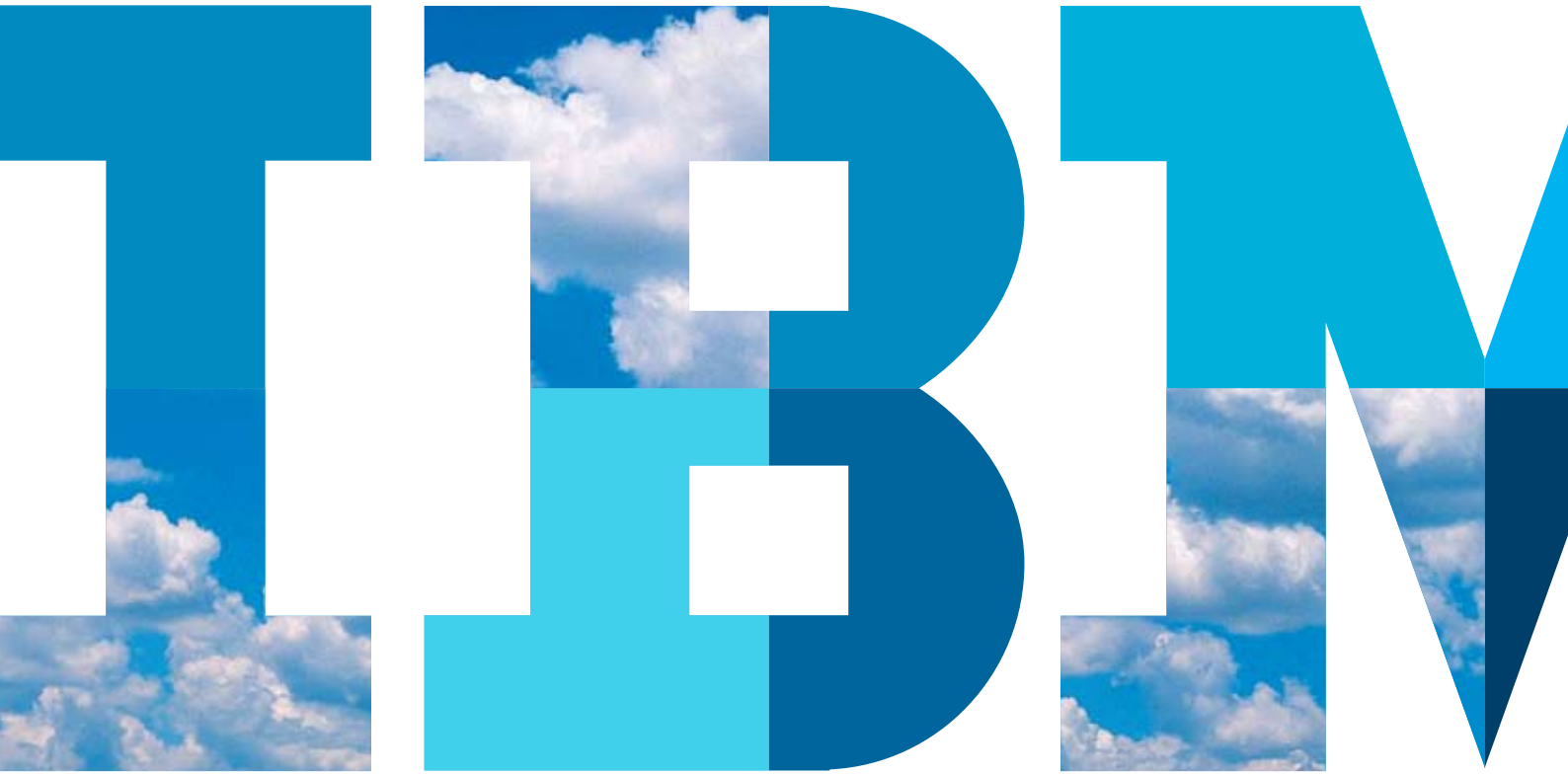
Cloud Security
Who do you trust?

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



IBM

In this paper we will explain why trust, reliability and security decisions are central to choosing the right model. Consider for example:

- **How easy would it be to lose your service if a denial of service attack is launched within your cloud provider?**
- **Will you suffer a data security breach when an administrator can access multiple stores of data within the virtualized environment they are controlling?**
- **Could you lose your service when an investigation into data loss of another customer starts to affect your privacy and data?**

Cloud Security – Who do you trust?

Cloud computing offers to change the way we use computing with the promise of significant economic and efficiency benefits. The speed of adoption depends on how trust in new cloud models can be established.

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:

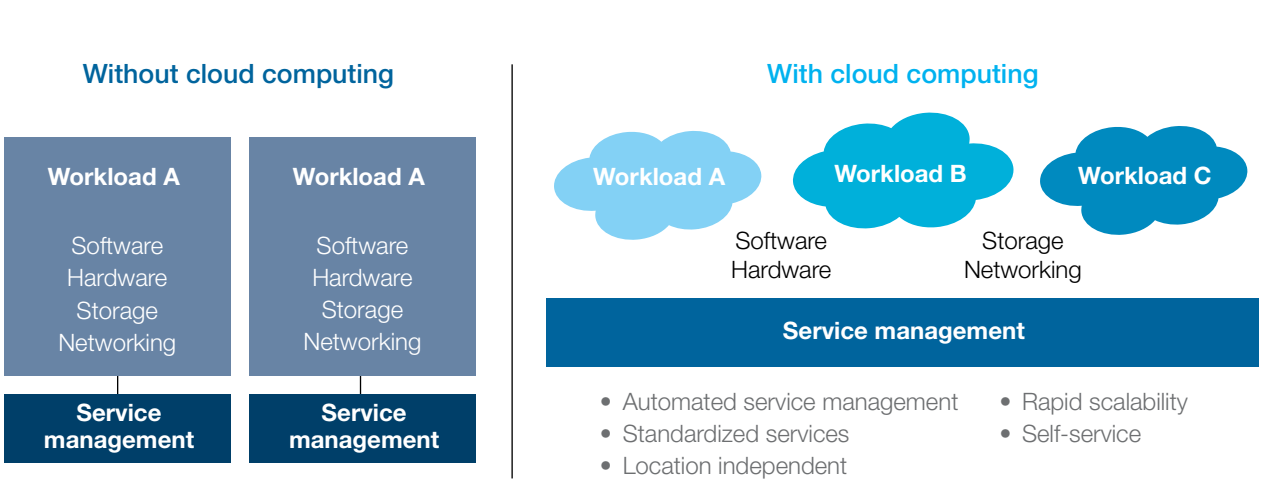
- What is different about cloud?
- What are the new security challenges cloud introduces?
- What can be done and what should be considered further?

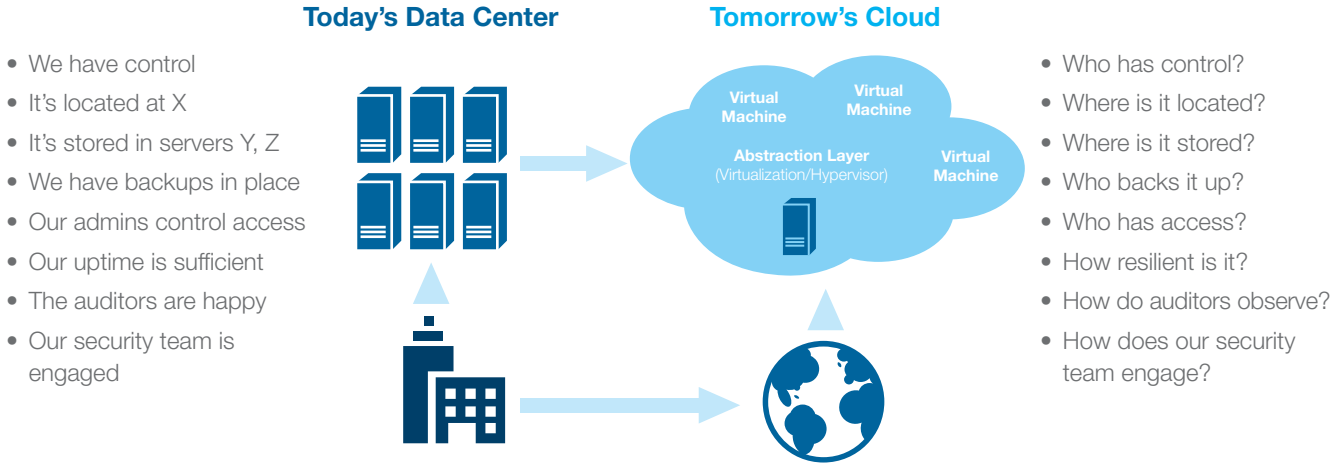
What is different about cloud?

Cloud computing moves us away from the traditional model, where organizations dedicate computing power to a particular business application, to a flexible model for computing where users access business applications and data in shared environments.

Cloud is a new consumption and delivery model; resources can be rapidly deployed and easily scaled (up and down), with processes, applications and services provisioned 'on demand'. It can also enable a pay per usage model.

In these models the risk profile for data and security changes and is an essential factor in deciding which cloud computing models are appropriate for an organization.





What are the security challenges cloud introduces?

There are existing security challenges, experienced in other computing environments, and there are new elements which are necessary to consider. The challenges include:

- Governance
- Data
- Architecture
- Applications
- Assurance

These five categories are described in the rest of this section in more detail so that the complexity of these issues can be better understood.

"⅔ of organizations identify security as their top concern when considering cloud."

Driving Profitable Growth Through Cloud Computing, IBM Study (conducted by Oliver Wyman) published Nov 2008.

Governance

Achieving and maintaining governance and compliance in cloud environments brings new challenges to many organizations. (This paper should not be seen as legal advice or guidance specific to any one organization.) Things you might need to consider include:

Jurisdiction and regulatory requirements

- Can data be accessed and stored at rest within regulatory constraints?
- Are development, test and operational clouds managing data within the required jurisdictions including backups?

Complying with Export/Import controls

- Applying encryption software to data in the cloud, are these controls permitted in a particular country/jurisdiction?
- Can you legally operate with the security mechanisms being applied?

Compliance of the infrastructure

- Are you buying into a cloud architecture/infrastructure/service which is not compliant?

Audit and reporting

- Can you provide the required evidence and reports to show compliance to regulations such as PCI and SOX?
- Can you satisfy legal requirements for information when operating in the cloud?

Data

Cloud places data in new and different places, not just the user data but also the application (source) code. Who has access, and what is left behind when you scale down a service? Other key issues include:

Data location and segregation

- Where does the data reside? How do you know?
- What happens when investigations require access to servers and possibly other people's data?

Data footprints

- How do you ensure that the data is where you need it when you need it, yet not left behind?
- How is it deleted?
- Can the application code be exposed in the cloud?

Backup and recovery

- How can you retrieve data when you need it?
- Can you ensure that the backup is maintained securely, in geographically separated locations?

Administration

- How can you control the increased access administrators have working in a virtualized model?
- Can privileged access be appropriately controlled in cloud environments?

Architecture

Standardized infrastructure and applications; increased commoditization leading to more opportunity to exploit a single vulnerability many times. Looking at the underlying architecture and infrastructure, some of the considerations include:

Protection

- How do you protect against attack when you have a standard infrastructure and the same vulnerability exists in many places across that infrastructure?

Hypervisor vulnerabilities

- How can you protect the hypervisor (a key component for cloud infrastructures) which interacts and manages multiple environments in the cloud? The hypervisor being a potential target to gain access to more systems, and hosted images.

Multi-tenant environments

- How do you ensure that systems and applications are appropriately and sufficiently isolated and protecting against malicious server to server communication?

Security policies

- How do you ensure that security policies are accurately and fully implemented across the cloud architectures you are using and buying into?

Identity Management

- How do you control passwords and access tokens in the cloud?
- How do you federate identity in the cloud?
- How can you prevent user IDs/passwords being passed and exposed in the cloud unnecessarily, increasing risk?

Providing Software as a service (SaaS), Infrastructure and hardware as a service (IaaS) and Platform as a service (PaaS), either individually or in different combinations

Applications

There has been a significant increase in web application vulnerabilities, so much so that these vulnerabilities make up more than half of the disclosed vulnerabilities over the past 4 years.

"67% of all web application vulnerabilities had no patch in 2009."

Source: IBM Security Solutions X-Force 2009 Trend and Risk Report, published Feb 2010.

Software Vulnerabilities

- How do you check and manage vulnerabilities in applications?
- How do you secure applications in the cloud that are increasing targets due to the large user population?

Patch management

- How do you secure applications where patches are not available?
- How do you ensure images are patched and up to date when deployed in the cloud?

Application devices

- How do you manage the new access devices using their own new application software?
- How do you ensure they are not introducing a new set of vulnerabilities and ways to exploit your data?

Assurance

Challenges exist for testing and assuring the infrastructure, especially when there is no easy way for data center visits or penetration (pen) tests.

Operational oversight

- When logs no longer just cover your own environment do you need to retrieve and analyse audit logs from diverse systems potentially containing information with multiple customers?

Audit and assurance

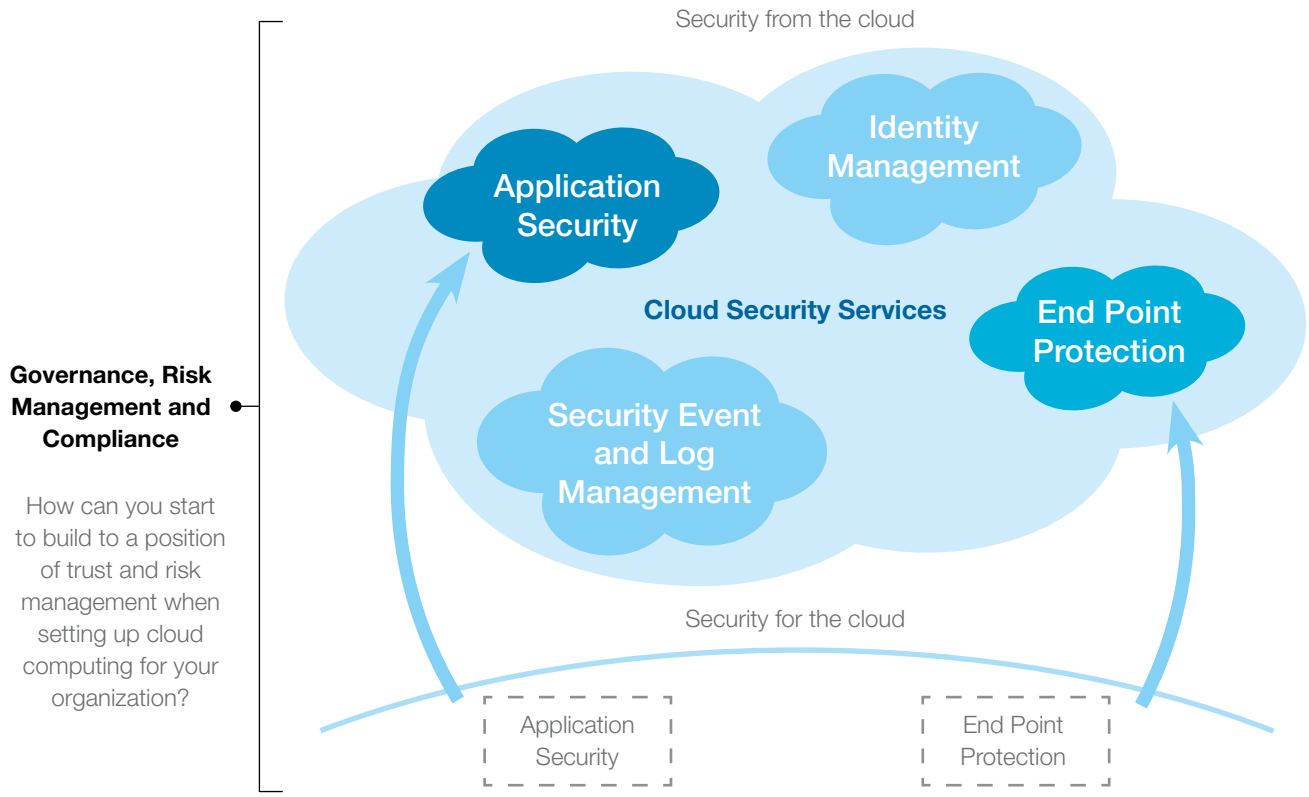
- What level of assurance and how many providers will you need to deal with?
- Do you need to have an audit of every cloud service provider?

Investigating an incident

- How much experience does your provider have of audit and investigation in a shared environment?
- How much experience do they have of conducting investigations without impacting service or data confidentiality?

Experience of new cloud providers

- What will the security of data be if the cloud providers are no longer in business?
- Has business continuity been considered for this eventuality?



What can be done and what should be considered further?

Many of the risks identified can be managed through the application of appropriate security and governance measures.

Which risks you choose to address will be different depending on your business, your appetite for risk and how costly these measures are.

In many cases the complexity of securing cloud comes not just from the individual application but how it integrates into the rest of the organization.

Delivering security for the cloud

Working out where and how to apply security is core to delivering security for the cloud.

Security itself can be delivered from within the cloud. Elements such as Event and Log Management, Identity Management, End Point Protection and Application Security are increasingly delivered as cloud security services. Security for the cloud will be down to what can be delivered in the cloud and what needs to supplement that delivery framework.

Getting started:

1. 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?

2. Identify the security measures needed

Using a framework such as the one IBM uses, the IBM Security Framework and Blueprint, allows teams to capture the measures that are needed in areas such as governance, architecture, applications and assurance.

3. Enabling security for the cloud.

The upfront set of assurance measures you will want to take. Assessing that the applications, infrastructure and other elements meet your security requirements, as well as operational security measures.

Cloud security can be delivered as part of the cloud service and also as specific components added in to enhance security. Depending on your cloud provider it may be that a combination of both of these approaches is necessary.

The fundamental principles of security and risk management still apply. The approach IBM is using is based on IBM's Security Framework and Blueprint which provides a comprehensive framework to address all aspects of security.

In summary

Cloud computing offers new possibilities and new challenges. These challenges range from governance, through to securing application and infrastructure. Fundamentally it is important to be able to assure the security of these new models in order to build trust and confidence.

The key to establishing trust in these new models is choosing the right cloud computing model for your organization. Place the right workloads in the right model with the right security mechanisms.

- For those planning to consume cloud services looking for trust and assurance from the cloud provider; understanding the service level agreements and the approaches to security is key. Assessing that this can be delivered, including what assurances can be provided will be important.

- For those providing or building a cloud infrastructure, using a proven methodology and technologies that can deliver appropriate security is key.

This is not just a technical challenge but a challenge of governance and compliance; applications and infrastructure; and assurance. This paper is written to stimulate discussion of the challenges and ways to start to address these challenges in securing cloud computing.

The Authors

Nick Coleman
IBM Cloud Security Leader.
Email: coleman@uk.ibm.com
Twitter: twitter.com/teamsecurity

Martin Borrett
IBM Lead Security Architect
Email: borretm@uk.ibm.com

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United Kingdom
October 2010

Please Recycle

10-0861 (10/10) CL