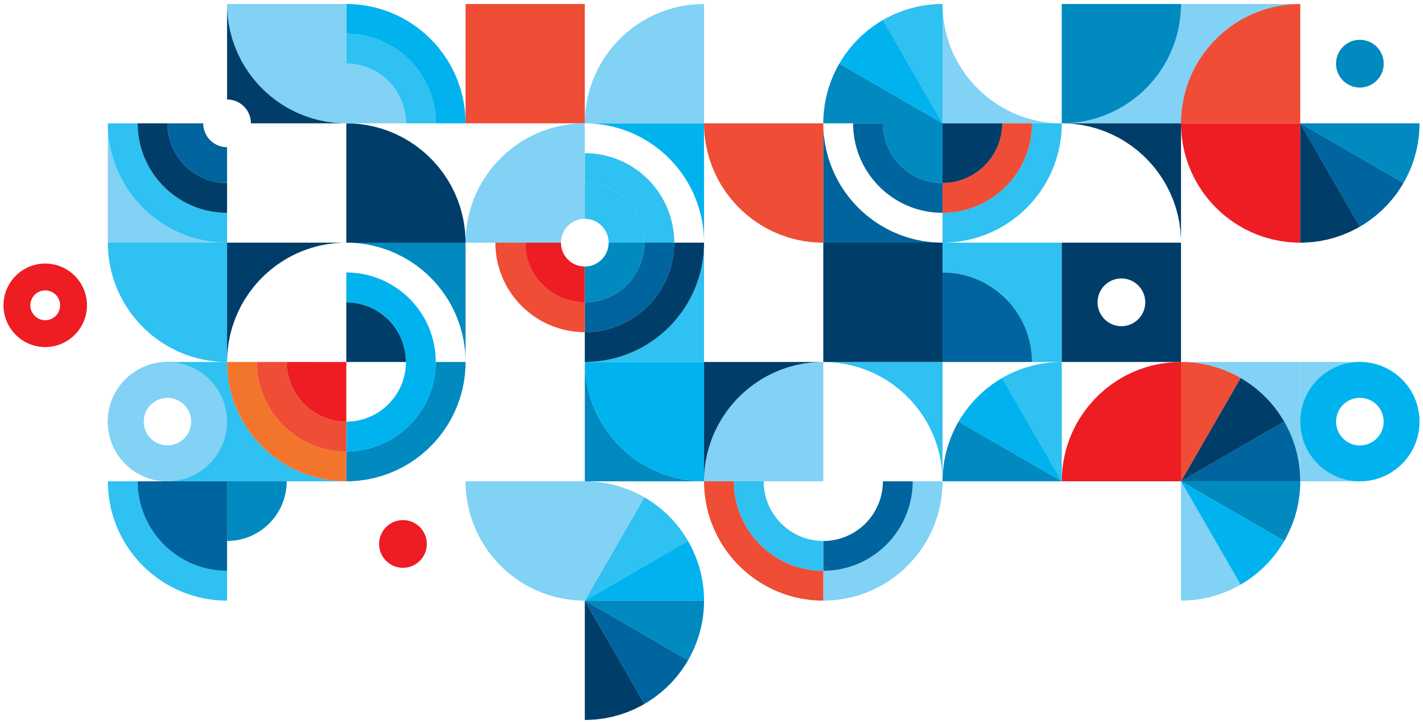
SmartCloud

How does IBM deliver cloud security?

An IBM paper covering SmartCloud Services[1]



IBM

Contents

Introduction

Cloud computing is changing the way we use computing and has the potential for significant economic and efficiency benefits. But the speed of adoption depends on how quickly trust in new cloud models can be established. Some of the growing cloud security concerns include: security of highly virtualized environments from targeted threats and attacks, enabling secure collaboration, protection of the data (isolation, sharing) in a rapid provisioning and de-provisioning environment while experiencing the loss of direct control of security compliance, and privacy parameters.

In order to build this trust, IBM has written this paper to enable discussion around the new security challenges cloud introduces and how these are addressed by IBM's cloud offerings. We highlight the approach IBM takes to secure cloud services delivered from IBM delivery centers.

In delivering security for its cloud offerings, IBM looks to and relies upon its strong security heritage and expertise. IBM has more than 6,000 security engineers and consultants around the world, designing, building and running security solutions for its customers and helping them address their challenges in this space. It has a portfolio of more than 3,000 security patents, with 100 new patents in 2011 alone. IBM also has the largest vulnerability database in the industry and manages over 13 billion security related events every day for existing customers.

IBM's security strategy is based on the IBM Security Framework[2], IBM provides security solutions that span this framework and works with organizations to take a holistic and risk-based approach to security. IBM has extensive experience of delivering in an outsourced and managed services environment and of having those services internally and externally audited to recognized industry standards.

The approach IBM takes to delivering cloud services to its customers is anchored in the IBM Security Framework and the associated IBM Security Blueprint. By using this proven framework and blueprint approach, we have created a set of foundational controls specific to cloud. These Cloud Security Foundation Controls have been developed from the foundational security management layer of the blueprint and are used to communicate with customers, partners and other stakeholders about how we approach security in our cloud models.

In this paper we present some of the measures that we take in relation to these foundational controls. This paper is not intended to be exhaustive and does not describe every procedure and technical detail for each cloud offering.

1. Cloud governance

Governance, risk and compliance are common issues raised by stakeholders. IBM has many managed services operations in countries around the globe. IBM's cloud governance builds on that extensive IBM governance structure. We recognize that taking advantage of cloud requires new considerations for governance and that there are important questions about how data will be managed in the cloud. In order to assist transparency, IBM aligns its approach to recognized industry standards.

- IBM has internal security policies, standards and processes consistent with the ISO 27001 framework and control areas. In our delivery organization we also regularly submit these policies, standards and processes to both internal audits and external certifications.
- IBM also maintains many industry related certifications such as ISO 9001, ISO 20000 and CMMI across many data centers. For example a customer using SmartCloud Services from IBM's data center in Ehningen, Germany can expect that it has both ISO 27001 and ISAE3402 covering the physical controls.

IBM has a comprehensive Service Organization Controls (SOC) reporting program and is undergoing several SSAE16 or equivalent audits covering many IT services and associated controls, from managed services delivery through to managed security services. We continue to develop this external auditing approach to cover our cloud services as they evolve and to stay in line with the standards' requirements.

2. Security governance, risk management and compliance

As a large enterprise and a service provider, our cloud solutions reflect our understanding of organizational needs. We have a robust security compliance program that has governance over IBM internal security policies, standards and processes.

- IBM has an Information Technology (IT) Security Compliance management system which entails adherence to predefined requirements. These include physical access controls, logical access controls (including user ID administration) and security health checking. Our internal and external audit partners regularly review these controls.
- Our processes and controls have evolved through thousands of engagements around outsourcing, hosting and other services. They have been further developed with the aim of meeting the needs of cloud environments.

We have incorporated governance and risk management best practices and lessons learned through implementing our own cloud solutions and building solutions for other large enterprise customers – and applied them to our cloud offerings.

IBM has extensive experience designing and delivering in multi-tenant environments. Security governance has also been enabled through the way we design, build and deliver solutions guided by an approach called, 'Secure by Design'.

3. Problem and information security incident management

In the event of a problem or incident occurring in the cloud, formal response processes, aligned to the overall IBM Corporate Incident Management Processes, are executed and records retained. IBM has extensive experience of environments with shared users and incident management is handled to best efforts to ensure that customers and their data are protected.

- IBM has documented policies and procedures relating to the management and monitoring of security events within its offerings and infrastructure, including policies on escalation and resolution of incidents.
- In order to maintain the integrity of these security policies and procedures, and thereby protect our customers, these policies are not divulged outside IBM. Procedures are, however, subjected to internal and external audits on a regular basis.

In the case of a security event, IBM will evaluate the situation, and where an issue has a material impact on a customer, will notify them of such incidents. IBM also protects its infrastructure by shutting down instances that violate acceptable use policy. In addition, IBM has put in place log-management of its infrastructure, including network traffic and administrative functions, to ensure issues can be investigated. IBM customers can be assured that the cloud infrastructure monitoring does not capture or retain logs of customer data, other than metadata.

4. Identity and access management

To ensure that only those who need to access cloud environments do so, IBM has developed processes to ensure that access is tightly controlled. IBM maintains robust access control and privileged user monitoring to ensure enforcement and compliance regarding access to customer content and information.

- Access to any system managed by IBM begins with a formal access request and management approval process. Once approved, access is revalidated on a periodic basis, at least annually, to ensure users still require the level of access they have been granted. Systems are also in place to ensure that those who leave IBM have their access rights removed.
- IBM Administrators of the cloud have to authenticate to the management environment and to the management tools in order to gain access to functionality. These activities are monitored and logged to prevent unauthorized access to customer virtual environments.
- All customer content managed by IBM is strictly controlled and actively monitored. Only those personnel with appropriate authorization from IBM Corporation have access to host management systems.

5. Discover, categorize, and protect data and information assets

One often cited concern about cloud is that it places data in new and different places. This applies not just to the user data, but also to the application (source) code.

IBM has invested in cloud data centers in geographic regions across the globe with customers able to specify the cloud data center location they wish to use. Mechanisms for protecting data, such as encryption, may also be possible.

- We have enabled customers to configure encryption – for example, of persistent storage – within their guest workloads. Customers retain key management responsibility to support the security of these processes.
- Encryption can also be built into some applications deployed on our cloud services, for example IBM DB2® can encrypt local databases and support the encryption of customer information. For some solutions this can also be achieved at the file system level.
- At the infrastructure level there are additional controls such as encrypting backup media, protection of data on portable media, as well as during the disposal of storage devices.

Processes are also in place to ensure any media removed from the data center is encrypted for transport, and securely deleted at the end of its use. In addition, in our standard operating procedures, customer data is not removed from the data center without a customer's permission.

IBM, as an international company with global customers, has substantial experience collecting, storing and working with personally identifiable information – and it has applied these rules within its managed infrastructure.

Governments have long had the authority to request access to data for law enforcement and national security reasons and such a request can extend to any company doing business within that country, regardless of where the company is based or where the data is stored.

IBM will thoroughly evaluate its obligations in order to provide the minimum data necessary to comply with legal requests, from governmental authorities for access to data.

IBM recommends that customers review the legal and business requirements relative to their data and works with them to architect solutions that meet their privacy and security needs.

6. System acquisitions, development and maintenance

Ensuring that the systems are built with security controls in mind, and that these controls are maintained throughout the operation of the system, is not a new concept to IBM.

- Our extensive experience in managing infrastructure means that cloud operational processes have been built, to enable that security is applied to the environment throughout its lifecycle.
- Hypervisors are Common Criteria certified, for example, VMware ESX, PowerVM® and KVM are EAL 4+ certified. KVM is deployed on hardened SELinux servers, which provides additional isolation capabilities over KVM itself.
- Procedures to maintain the security of the infrastructure such as standard infrastructure patch management for cloud infrastructure.

7. Secure infrastructure against threats and vulnerabilities

Securing any infrastructure requires a defense in depth approach and IBM uses a number of different processes and procedures to protect cloud infrastructures. These are underpinned with people and technology to secure the infrastructure against threats and vulnerabilities.

- The solutions have been designed with isolation built in at different levels – at the network, hypervisor and storage layers. Management and infrastructure components are compartmentalized into security zones based on function, data types and access requirements, and storage networks and guest networks are physically separated. The zone design, as well as network flows, requires formal review and approval through architecture governance processes.
- Management infrastructure is regularly scanned for vulnerabilities using industry standard tools and master images are regularly updated to the latest security fix/patch level.
- Intrusion detection and prevention systems (IDPS) are utilized at boundaries to the Internet, IBM employs an approach that does not rely on signature-based vulnerability detection alone. This capability allows protection against previously unseen threats based on behavior and not just signatures.
- All management systems and underlying infrastructure periodically undergo security configuration checking to ensure system security settings continue to be configured in-line with security standards and policy. Host-based firewalls within the customer Virtual Machines (VMs) can, and should, also be configured to achieve defense in depth.

8. Physical and personnel security

One concern often raised is where the data is located and how it will be controlled in the data center. IBM cloud delivery centers are located within established IBM data centers and the company has extensive experience in managing data centers.

- IBM has data centers with strong physical controls including, but not limited to, CCTV, biometric authentication mechanisms, resiliency tools and door alarms. All IBM personnel undergo background checks prior to being hired.
- IBM does allow accompanied visitation of its site facilities by its customers, however no persons, other than IBM personnel and agents working on behalf of IBM, are allowed access to the data center facilities beyond those areas specified for visitors. Access to the IBM data center floor is strictly restricted to authorized IBM personnel only and those permitted to carry out work on behalf of the company.
- IBM requires employees to go through training in the handling of customer data and to demonstrate understanding of those policies. The IBM business conduct guidelines oversee expectations and requirements of employees including the handling of customer data. All IBM employees are required to re-certify understanding in these areas on a yearly basis.

Summary

Cloud computing offers new possibilities and new security 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.

IBM has extensive experience of delivering in shared environments, a common characteristic of cloud. This experience ranges from managed services, through to infrastructure as a service and platform as a service.

This paper introduces IBM's approach to delivering cloud security for infrastructure services. However it is not intended to be exhaustive and does not describe every procedure and technical detail for each cloud offering.

The key to establishing trust in these new models is choosing the right cloud computing model for your organization, and being able to deploy workloads using a delivery model with the appropriate security controls.

We understand this is not just a technical challenge but a challenge of governance and compliance, applications and infrastructure, and assurance.

Author

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

Acknowledgments

Neil Readshaw
IBM Senior Technical Staff Member

Martin Borrett
Director of the IBM Institute for Advanced Security Europe

References

1 IBM SmartCloud Enterprise and Enterprise Plus
ibm.com/cloud-computing/us/en/iaas.html

2 IBM Security Framework
www.redbooks.**ibm.com**/abstracts/redp4528.html

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

Produced in the United States of America
May 2012
All Rights Reserved

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

Information may be changed or updated without notice. IBM may also make improvements and/or changes in the products, practices and/or the programmes described in this information at any time without notice. This paper should not be seen as a contractual agreement or indication of terms of service.

Please Recycle