Cloud computing
White paper
November 2009

IBM Point of View: Security and Cloud Computing

Table of Contents

Introduction

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 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.

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 like IBM LotusLive™, Platform as a Service (PaaS) clouds such as IBM Computing on Demand™, and Security and Data Protection as a Service (SDPaaS) clouds like the IBM Vulnerability Management Service.

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. Furthermore, private clouds can provide lower latency than public clouds during peak traffic periods. Many organizations embrace both public and private cloud computing by integrating the two models into hybrid clouds. These hybrids are designed to meet specific business and technology requirements, helping to optimize security and privacy with a minimum investment in fixed IT costs.

Although the benefits of cloud computing are clear, so is the need to develop proper security for cloud implementations. The following pages provide an overview of key security issues related to cloud computing, concluding with the IBM Point of View on a secure cloud architecture and environment.

Address cloud security—the grand challenge

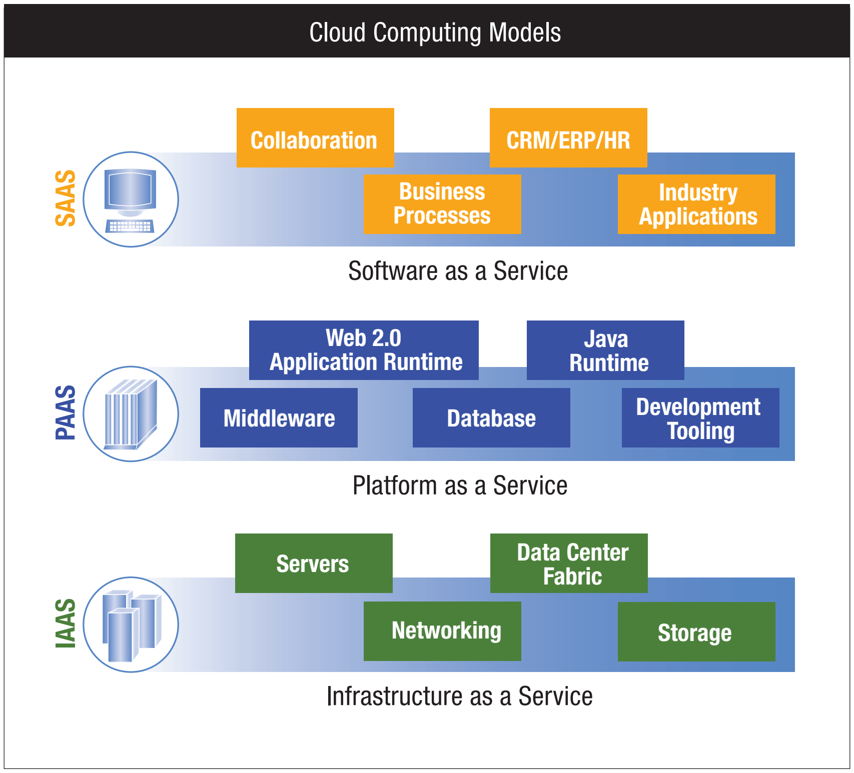
In addition to the usual challenges of developing secure IT systems, cloud computing presents an added level of risk because essential services are often outsourced to a third party. The "externalized" aspect of outsourcing makes it harder to maintain data integrity and privacy, support data and service availability, and demonstrate compliance.

In effect, cloud computing shifts much of the control over data and operations from the client organization to their cloud providers, much in the same way that organizations entrust part of their IT operations to outsourcing companies. Even basic tasks, such as applying patches and configuring firewalls, can become the responsibility of the cloud service provider, not the end user. As a result, clients must establish trust relationships with their providers and understand risk in terms of how these providers implement, deploy and manage security on their behalf. This "trust but verify" relationship between cloud service providers and clients is critical because the clients are still ultimately responsible for compliance and protection of their critical data, even if that workload has moved to the cloud. In fact, some organizations choose private or hybrid models over public clouds because of the risks associated with outsourcing services.

Other aspects about cloud computing also require a major reassessment of security and risk. Inside the cloud, it is difficult to physically locate where data is stored. Security processes that were once visible are now hidden behind layers of abstraction. This lack of visibility can create a number of security and compliance issues.

In addition, the massive sharing of infrastructure with cloud computing creates a significant difference between cloud security and security in more traditional IT environments. Users spanning different corporations and trust levels often interact with the same set of compute resources. At the same time, workload balancing, changing service-level agreements (SLAs) and other aspects of today's dynamic IT environments create even more opportunities for misconfiguration, data compromise and malicious conduct.

Infrastructure sharing calls for a high degree of standardized and process automation, which can help improve security by eliminating the risk of operator error and oversight. However, the risks inherent with a massively shared infrastructure mean that cloud computing models must still place a strong emphasis on isolation, identity and compliance.



Evaluate different models of cloud computing

Different models of cloud computing have various ways of exposing their underlying infrastructure to the user. This influences the degree of direct control over the management of the computing infrastructure and the distribution of responsibilities for managing its security.

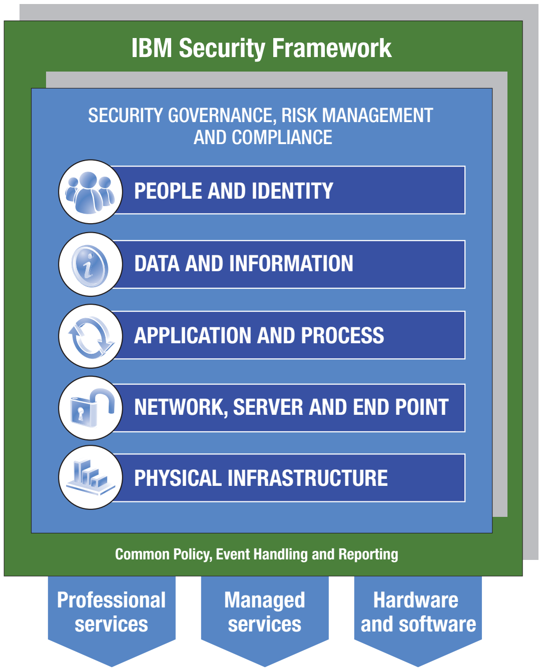
With the SaaS model, most of the responsibility for security management lies with the cloud provider. SaaS provides a number of ways to control access to the Web portal, such as the management of user identities, application level configuration and the ability to restrict access to specific IP address ranges or geographies.

Cloud models like Platform as a Service allow clients to assume more responsibilities for managing the configuration and security for the middleware, database software and application run-time environments. The Infrastructure as a Service (IaaS) model transfers even more control—and responsibility for security—from the cloud provider to the client. In this model, access is available to the operating system supporting virtual images, networking and storage.

Organizations are intrigued with these cloud computing models because of their flexibility and cost-effectiveness, but they are also concerned about security. Recent cloud adoption studies by industry analysts and articles in the press have confirmed these concerns, citing the lack of visibility and control, concerns about the protection of sensitive information and storage of regulated information in a shared, externally managed environment.

A mass adoption of external, massively shared and completely open cloud computing platforms for critical IT services is considered to be still a few years away.

In the near term, most organizations are looking at ways to leverage the services of external cloud providers. These clouds would be used primarily for workloads with a low-risk profile, where a one-size-fits-all approach to security with few assurances is acceptable, and where price is the main differentiator. For workloads with a medium- to high-risk profile involving highly regulated or proprietary information, organizations are choosing private and hybrid clouds that provide a significant level of control and assurance. These workloads will be shifting into external clouds as they start offering tighter and more flexible security.



Examine the IBM Security Framework

The IBM Security Framework was developed to describe security in terms of the business resources that need to be protected, and it looks at the different resource domains from a business point of view.

Based on the IBM Security Framework and informed by extensive discussions with IBM clients, the following section provides a list of major security requirements in enterprise-class cloud computing today. (For more information, *see IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*, IBM RedGuide REDP-4528-00, July 2009.)

Security governance, risk management and compliance

Organizations require visibility into the security posture of their cloud. This includes broad-based visibility into change, image and incident management, as well as incident reporting for tenants and tenant-specific log and audit data.

Visibility can be especially critical for compliance. The Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), European privacy laws and many other regulations require comprehensive auditing capabilities. Since public clouds are by definition a “black box” to the subscriber, potential cloud subscribers may not be able to demonstrate compliance. (A private or hybrid cloud, on the other hand, can be configured to meet those requirements).

In addition, providers sometimes are required to support third-party audits, and their clients can be directed to support e-Discovery and forensic investigations when a breach is suspected. This adds even more importance to maintaining proper visibility into the cloud.

In general, organizations often cite the need for flexible SLAs that can be adapted to their specific situation, building on their experiences with strategic outsourcing and traditional, managed services.

People and identity

Organizations need to make sure that authorized users across their enterprise and supply chain have access to the data and tools that they need, when they need it—all while blocking unauthorized access. Cloud environments usually support a large and diverse community of users, so these controls are even more critical. In addition, clouds introduce a new tier of privileged users: administrators working for the cloud provider. Privileged-user monitoring, including logging activities, becomes an important requirement. This monitoring should include physical monitoring and background checking.

Identity federation and rapid on-boarding capabilities must be available to coordinate authentication and authorization with the enterprise back-end or third-party systems. A standards-based, single sign-on capability is required to simplify end-user logons for both internally hosted applications and the cloud, allowing end users to easily and quickly leverage cloud services.

Data and information

Most organizations cite data protection as their most important security issue. Typical concerns include the way in which data is stored and accessed, compliance and audit requirements, and business issues involving the cost of data breaches, notification requirements and damage to brand value. All sensitive or regulated data needs to be properly segregated on the cloud storage infrastructure, including archived data.

Encrypting and managing encryption keys of data in transit to the cloud or at rest in the service provider's data center are critical to protect data privacy and comply with compliance mandates. The encryption of mobile media and the ability to securely share those encryption keys between the cloud service provider and consumer is an important and often overlooked need. Because moving large volumes of data quickly and cheaply over the Internet is still not practical in many situations, many organizations must send mobile media, such as an archive tape, to the cloud provider. It is critical that the data is encrypted and that only the cloud provider and client have access to the encryption keys.

Significant restrictions regarding data collocation can arise with cloud computing, depending on an organization's location, the type of data it handles and the nature of its business. Several member states of the European Union (EU), for example, expressly forbid the nonpublic personal information of its citizens to leave their borders.

A number of U.S. state governments do not allow the nonpublic personal information of its employees to be sent offshore.

Additionally, a cloud deployment can raise export-law violation issues relative to encrypted information, and the deployment can potentially expose intellectual property to serious threats. The organization's legal counsel must perform a thorough review of all these requirements prior to cloud deployment, making sure the organization can maintain control over the geographic location of data in the provider infrastructure.

In areas involving users and data with different risk classes that are explicitly identified (such as public and financial services), organizations need to maintain cloudwide data classification. The classification of the data will govern who has access, how that data is encrypted and archived, and how technologies are used to prevent data loss.

Application and process

Clients typically consider cloud application security requirements in terms of image security. All of the typical application security requirements still apply to the applications in the cloud, but they also carry over to the images that host those applications. The cloud provider needs to follow and support a secure development process. In addition, cloud users demand support for image provenance and for licensing and usage control. Suspension and destruction of images must be performed carefully, ensuring that sensitive data contained in those images is not exposed.

Defining, verifying and maintaining the security posture of images vis-à-vis client-specific security policies is an important requirement, especially in highly regulated industries. Organizations need to ensure that the Web services they publish into the cloud are secure, compliant and meet their business policies. Leveraging secure-development best practices is a key requirement.

Network, server and endpoint

In the shared cloud environment, clients want to ensure that all tenant domains are properly isolated and that no possibility exists for data or transactions to leak from one tenant domain into the next. To help achieve this, clients need the ability to configure trusted virtual domains or policy-based security zones.

As data moves further from the client's control, they expect capabilities like Intrusion Detection and Prevention systems to be built into the environment. The concern is not only intrusions into a client's trusted virtual domain, but also the potential for data leakages and "extrusions"—that is to say, the misuse of a client's domain to mount attacks on third parties. Moving data to external service providers raises additional concerns about internal and Internet-based denial of service (DoS) or distributed denial of service (DDoS) attacks.

> *Because information security is a moving target, the environment must be reviewed on a regular basis against prevalent threats and common vulnerabilities.*

In a shared environment, all parties must agree on their responsibilities to review data and perform these reviews on a regular basis. The organization must take the lead in terms of contract management for any risk assessments or controls deployment that it does not perform directly.

Where image catalogs are provided by the cloud provider, clients want these images to be secure and properly protected from corruption and abuse. Many clients expect these images to be cryptographically certified and protected.

Physical infrastructure

The cloud's infrastructure—including servers, routers, storage devices, power supplies and other components that support operations—should be physically secure. Safeguards include the adequate control and monitoring of physical access using biometric access control measures and closed circuit television (CCTV) monitoring. Providers need to clearly explain how physical access is managed to the servers that host client workloads and that support client data.

Understand the IBM Point of View on cloud security

IBM offers an informed perspective on cloud security based on extensive experience in the design, implementation and support of cloud computing solutions across a range of vertical industries.

No "one size fits all" for security

> *There is no one-size-fits-all model for security in the cloud. Organizations have different security requirements that are determined by the unique characteristics of the business workload they intend to migrate to the cloud.*

Organizations have many different requirements for integration between the cloud environment and their enterprise back-end systems. Some organizations are developing entirely new applications and are prepared to build their cloud environment to be independent from any existing operations, but most enterprise clients will start with a hybrid or private cloud where integration with their enterprise systems is a central requirement.

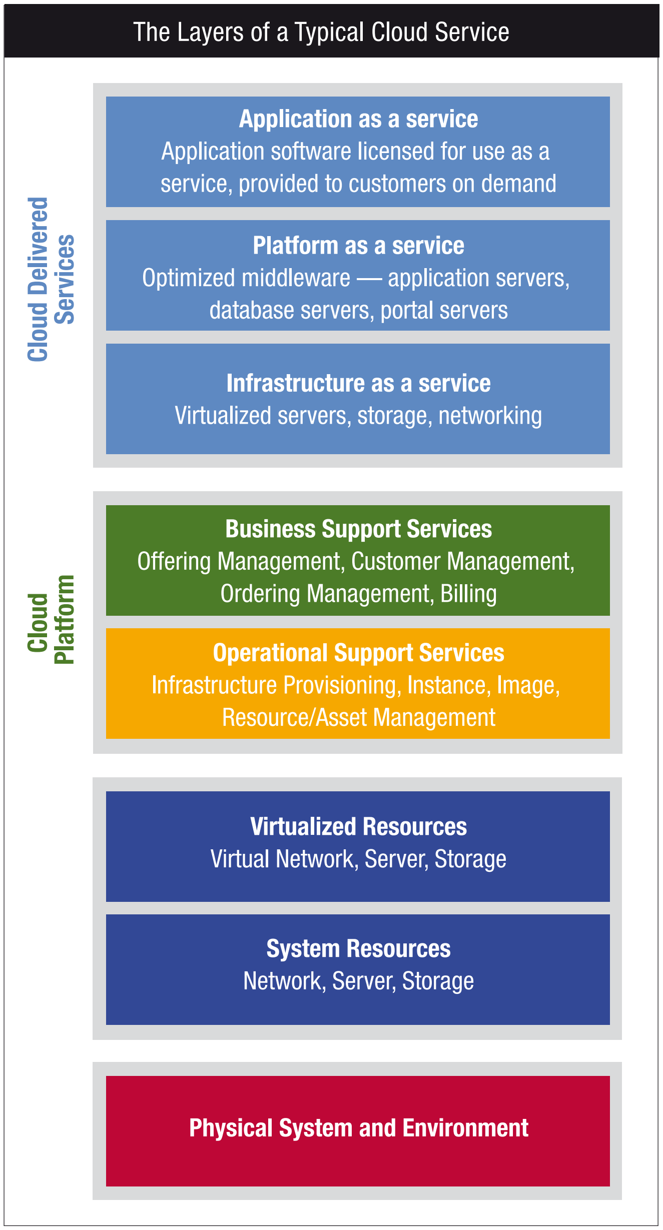
In this context, the ease with which the existing security management infrastructure can be extended into the cloud—and, in particular, the use of federation protocols—are important contributors to a successful deployment. Identity federation protocols such as OpenID and Security Assertion Markup Language (SAML) receive a great deal of public attention and play an important role for public clouds, but in the enterprise a variety of other protocols need to be supported. These protocols all have the objective of quickly moving data from the enterprise back-end systems into the private or hybrid cloud.

Different types of workloads require different levels of security. One of the top requirements is the need for a third-party security audit or validation, and governments are even expressing a need for formal validation and certification. The strength of identity proofing—making sure that the users who log on to the service are really who they claim they are—and the strength of authentication mechanisms will vary depending on the workload type. In response, new public services for identity verification are being set up, offering varying degrees of service quality.

Encryption requirements are very different from one client to another. Certain clients mandate the use of specific crypto-algorithms and require very high restrictions on who can have access to the keys, while other clients may demand encryption only for specific data and may want to delegate key management to a trusted cloud service provider.

There is a large variation in availability requirements, including the time allowed for the provider to react to and recover from failure. Requirements also vary for the intervals at which security and compliance checks are performed.

It is IBM's point of view that a provider of enterprise-class cloud services must support a range of security and service-level options, as well as an extensible and industry standards-based security infrastructure that makes it easy to integrate with existing operations. In addition, the service provider must integrate with and extend the client's cloud security capabilities as needed.


The Layers of a Typical Cloud Service
Cloud Delivered Services
Application as a service
Application software licensed for use as a service, provided to customers on demand
Platform as a service
Optimized middleware — application servers, database servers, portal servers
Infrastructure as a service
Virtualized servers, storage, networking
Cloud Platform
Business Support Services
Offering Management, Customer Management, Ordering Management, Billing
Operational Support Services
Infrastructure Provisioning, Instance, Image, Resource/Asset Management
Virtualized Resources
Virtual Network, Server, Storage
System Resources
Network, Server, Storage
Physical System and Environment

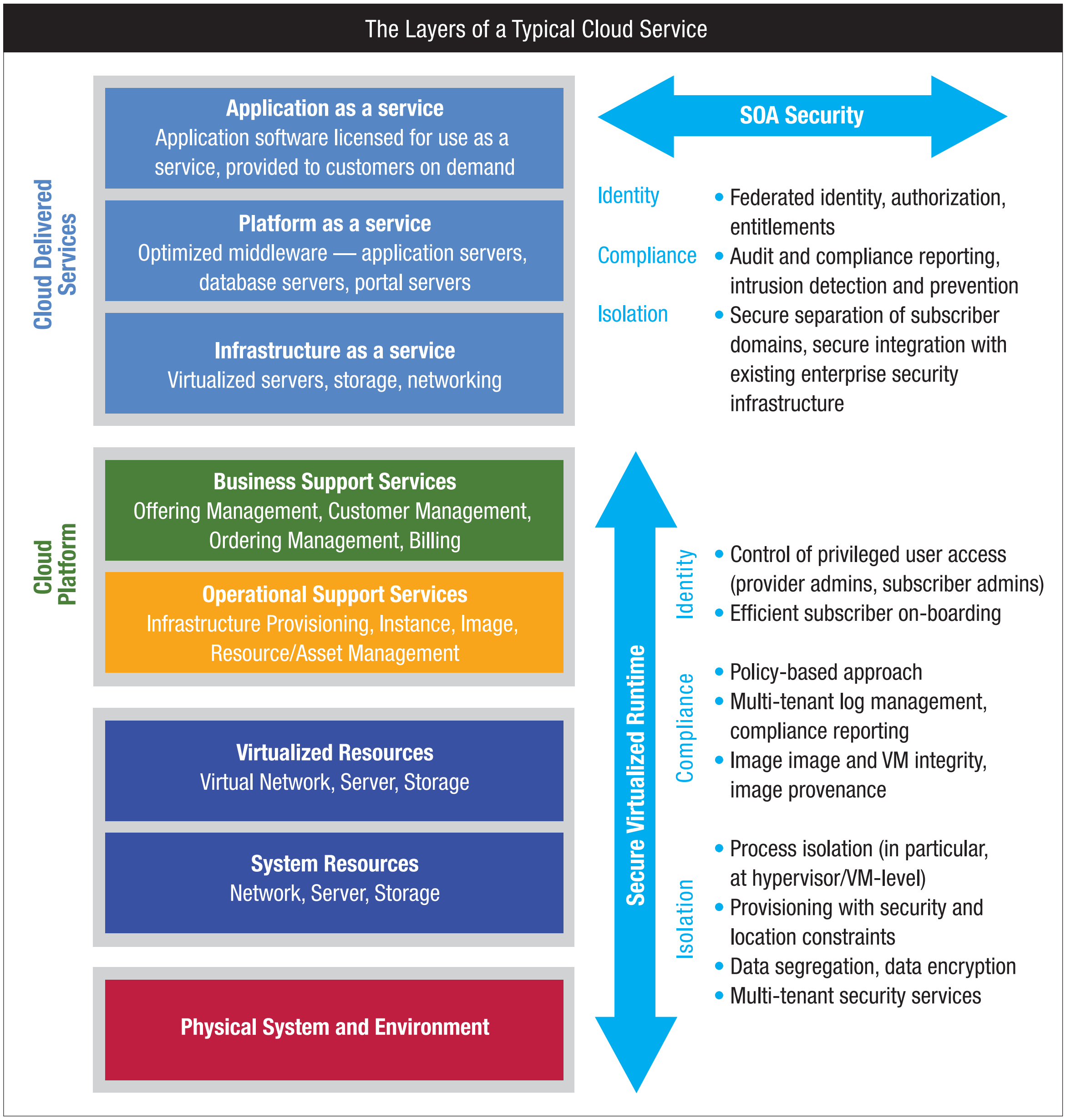
A basic architectural model for cloud computing

A basic architectural model for cloud computing consists of a stack of layered services. The physical system layer describes normal data center requirements, mandating access control measures and monitoring of the facility. The system resources layer governs network, server and storage infrastructure. The virtualized resources layer introduces strong isolation as the core property of virtualization security: isolating processes through hypervisors and data segregation.

The next layers are the operational support services (OSS) and business support services (BSS) that define the cloud management platform. At the top are the various cloud-delivered services of Infrastructure as a Service, Platform as a Service and Application as a Service.

Security requirements exist at each layer of this architecture, and it is critical to maintain consistency among these layers. For example, if a security policy at the highest level of the stack defines that customer information cannot leave the country, then at the lower level of physical resources, disk space must be allocated in-country that will store that data.

The Layers of a Typical Cloud Service



Cloud Delivered Services
Application as a service
Application software licensed for use as a service, provided to customers on demand
Platform as a service
Optimized middleware — application servers, database servers, portal servers
Infrastructure as a service
Virtualized servers, storage, networking
Cloud Platform
Business Support Services
Offering Management, Customer Management, Ordering Management, Billing
Operational Support Services
Infrastructure Provisioning, Instance, Image, Resource/Asset Management
Virtualized Resources
Virtual Network, Server, Storage
System Resources
Network, Server, Storage
Physical System and Environment
SOA Security
Secure Virtualized Runtime
Identity
Compliance
Isolation

SOA Security

- Identity: Federated identity, authorization, entitlements
- Compliance: Audit and compliance reporting, intrusion detection and prevention
- Isolation: Secure separation of subscriber domains, secure integration with existing enterprise security infrastructure

Secure Virtualized Runtime

Identity
- Control of privileged user access (provider admins, subscriber admins)
- Efficient subscriber on-boarding

Compliance
- Policy-based approach
- Multi-tenant log management, compliance reporting
- Image image and VM integrity, image provenance

Isolation
- Process isolation (in particular, at hypervisor/VM-level)
- Provisioning with security and location constraints
- Data segregation, data encryption
- Multi-tenant security services

Cloud security and SOA

The cloud architecture described here allows us to construct a very simple model of cloud security consisting of two main concepts: an SOA security layer that resides on top of a new Secure Virtualized Runtime layer.

The Cloud Delivered Services layer is a complex, distributed SOA environment. Different services can be spread across different clouds within an enterprise. The services might be in different administrative or security domains that connect together to form a single cloud application. The SOA Security Model fully applies to the cloud. The Web Services (WS) protocol stack forms the basis for SOA security and, therefore, also for cloud security. This security model is fully supported across the IBM software stack. (For more information on these products and the SOA security model, refer to IBM Redbook SG24-7310-01, *Understanding SOA Security*). A solution such as IBM Tivoli® Federated Identity Manager provides broad, standards-based support for bridging various security domains to deliver seamless user access to cloud services. This is especially important when tying together internal IT resources with third-party cloud services in a hybrid cloud model, or when packaging several third-party services in a branded offering to end customers.

One of the key aspects of SOA is the ability to easily integrate different services from different providers. Cloud computing is pushing this model one step further than most enterprise SOA environments, since a cloud sometimes supports a very large number of tenants, services and standards. This support is provided in a highly dynamic and agile fashion, and under very complex trust relationships. In particular, a cloud SOA sometimes supports a large and open user population, and it cannot assume a pre-established relationship between cloud provider and subscriber.

Many cloud implementations focus on specific protocols, such as OpenID for identity federation, and favor specific architectural styles, such as representational state transfer (REST). It is IBM's point of view that enterprise-class cloud computing must not limit its users to a specific protocol or style, but rather, offer flexibility and choice. While IBM supports REST-based interfaces and protocols where appropriate, SOA security needs the full range of security services as described in the SOA Security Reference Model.

A basic concept in SOA is to externalize security into services, and make these available for use by other services.

Standards-based proofing, enrollment and authentication of users to cloud services represent only the tip of the iceberg for ensuring that the right users have access to the right resources. Consistent policies for entitlements and access control are needed to ensure that all underlying components of a cloud service maintain data confidentiality and adhere to compliance regulations. For example, a medical research application pulls data from clinical and billing services from multiple hospitals, so patient names and other personally identifiable information must be removed from all sources. A centralized entitlements management service, like IBM Tivoli Security Policy Manager, can help ensure that common policy is defined and enforced to protect patient confidentiality across all cloud services.

Cloud providers can support SaaS and IaaS within and across clouds. The provider should adhere to implementation best practices and provide clients with maximum visibility into the security and compliance posture of cloud services. The IBM Rational® AppScan® portfolio can help support application security. IBM Tivoli Security Information and Event Manager provides consolidated views of security audit logs and prepackaged reports that can be used to demonstrate compliance efforts and identify threats from privileged insiders. The ability to monitor and respond to threats posed by privileged IT administrators takes on heightened importance in the public cloud model, where third-party administrators have access to the data of many different organizations.

The Secure Virtualized Runtime layer on the bottom is a virtualized system that runs the processes that provide access to data on the data stores. This run time differs from classic run-time systems in that it operates on virtual machine images rather than on individual applications. It provides security services such as antivirus, introspection and externalized security services around virtual images.

While the foundations of Secure Virtualized Runtime predate SOA security and are built on decades of experience with mainframe architectures, the development of Secure Virtualized Runtime is still very much in flux. IBM continuously invests in research and development of stronger isolation at all levels of the network, server, hypervisor, process and storage infrastructure to support massive multitenancy.

The provisioning of virtual resources enforces security domains and location constraints. Virtual resources must be grouped based on policy, and the automation of security configuration management helps ensure consistency.

Within Secure Virtualized Runtime, security services are also increasingly externalized through SOA services, providing identity, audit, key management, policy and other services. The IBM Proventia® Virtualized Network Security Platform is an extensible virtual security platform that provides threat management capabilities like intrusion prevention, Web application protection and network policy enforcement.

An opportunity to simplify security controls and defenses

While cloud computing is often seen as increasing security risks and introducing new threat vectors, it also presents an exciting opportunity to improve security. Characteristics of clouds such as standardization, automation and increased visibility into the infrastructure can dramatically boost security levels.

For example, the use of a defined set of cloud interfaces, along with centralized identity and access control policies, will reduce the risk of user access to unrelated resources. Running computing services in isolated domains, providing default encryption of data in motion and at rest, and controlling data through virtual storage have all become activities that can improve accountability and reduce the loss of data. In addition, automated provisioning and reclamation of hardened run-time images can reduce the attack surface and improve forensics.

IBM researchers, developers and security experts around the world have been awarded over 3,000 security and risk management patents.

IBM offers an unparalleled capacity to focus on driving business innovation and securing operational processes across all risk domains. Its comprehensive solutions and services enable organizations to reduce the complexity of security within their enterprise and implement a holistic security management strategy.

With IBM, organizations can develop comprehensive, scalable, standards-based solutions across the enterprise, supporting their security needs both now and in the years ahead.

For more information

To learn more about security for cloud computing, contact your IBM representative or IBM Business Partner, or visit **ibm.com**.

Readers can also consult *Cloud Security Guidance, IBM Recommendations for the Implementation of Cloud Security* (REDP-4614). This IBM RedGuide provides more information about cloud protection, responses to threats and a line of accountability for the management of events.

Additional information about cloud security can be found at the following sites:

IBM Cloud Computing: **ibm.com**/cloudcomputing

IBM Enterprise Security: **ibm.com**/security

IBM Internet Security Systems: **ibm.com**/services/security

IBM X-Force® Security Alerts and Advisories: xforce.iss.net

Additionally, IBM Global Financing can tailor financing solutions to your specific IT needs. For more information on great rates, flexible payment plans and loans, and asset buyback and disposal, visit: **ibm.com**/financing

© Copyright IBM Corporation 2009

Produced in the United States of America
November 2009
All Rights Reserved

IBM, the IBM logo, ibm.com, and Tivoli are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at **ibm.com**/legal/copytrade.shtml

Other product, company or service names may be trademarks or service marks of others.

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.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED “AS IS” WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

The customer is responsible for ensuring compliance with legal requirements. It is the customer’s sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

Recyclable, please recycle