Cloud Security: Developing a Secure Cloud Approach

Critical questions you should ask your cloud provider

Businesses are facing IT and data management challenges unlike those they’ve ever experienced. Big data and the globalisation of the business landscape, coupled with increased time-to-market pressures and budget restrictions, have resulted in ad hoc infrastructure build-outs and high levels of complexity.

This hampers the IT organisation’s ability to function efficiently. The cloud has become a perceived panacea for all these problems, but the journey to the cloud isn’t one that should be undertaken lightly. There are many potential pitfalls along the road, the most prominent of which is security.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>01</td>
</tr>
<tr>
<td>Cloud breaks the traditional security model</td>
<td>01</td>
</tr>
<tr>
<td>Taking a layered approach to securing the cloud</td>
<td>01</td>
</tr>
<tr>
<td>Client and cloud provider accountability</td>
<td>02</td>
</tr>
<tr>
<td>The cloud provider’s role in delivering secure cloud computing</td>
<td>02</td>
</tr>
<tr>
<td>Security questions you should ask your cloud provider</td>
<td>03</td>
</tr>
<tr>
<td>Summary</td>
<td>04</td>
</tr>
</tbody>
</table>
Executive summary

Businesses are facing IT and data management challenges unlike those they’ve ever experienced. Big data and the globalisation of the business landscape, coupled with increased time-to-market pressures and budget restrictions, have resulted in ad hoc infrastructure build-outs and high levels of complexity. This hampers the IT organisation’s ability to function efficiently. The cloud has become a perceived panacea for all these problems, but the journey to the cloud isn’t one that should be undertaken lightly. There are many potential pitfalls along the road, the most prominent of which is security.

Gartner analyst Jeffrey Wheatman comments in a recent research note that:

“Security requirements and drivers in the cloud are different from those in traditional data center environments… The dynamic nature of the cloud, coupled with the lack of customer ownership of infrastructure and limited transparency, has essentially broken traditional security models and architectures.”

This paper examines the differences between cloud and on-premise security requirements and discusses what organisations should consider to securely and confidently make the shift to the cloud.

Cloud breaks the traditional security model

As enterprise networking technology has evolved, so too have the requirements for enterprise security. What began simply as setting up a perimeter around the network using security tools like firewalls and e-mail gateways has evolved to the deployment of a wide range of tools. These include virtual private networks (VPNs) and intrusion detection systems (IDS) needed to handle the continuously growing number of threats to the network. For many IT departments, the idea of moving this established infrastructure into the cloud is a daunting proposition. Although the cost and scalability benefits of the cloud are appealing, the perceived lack of security and control has prevented organisations from taking the plunge.

Taking a layered approach to securing the cloud

The solution lies in taking a layered or ‘defense in depth’ approach to enterprise-class security. An effective hosted cloud service involves much more than migrating sensitive data into an environment, simply wrapping a virtual perimeter around it and calling it secure. Unfortunately, this is precisely what many public cloud offerings consider ‘security’. Businesses should give thought to how to best secure each layer of the cloud environment, including the infrastructure, operating system, application and network layers. They need an integrated approach that considers networking and security together, in order to provide security for the overall functionality of the application and data to be migrated to the cloud.

Layered security requires enterprise IT teams to understand both the applications and data they intend to move to the cloud and the capabilities of the cloud infrastructure to which they’re moving. Any cloud infrastructure will have some differences from the organisation’s on-premise infrastructure. Understanding these differences is important in designing a security approach that replicates the level of control an organisation has over its own on-premise infrastructure. Because cloud environments are more dynamic than on-premise infrastructures, security approaches need to provide automated adaptability, as new assets are provisioned or removed from the environment. If the target cloud architecture provides programmatic controls that support automation, IT can use these interfaces to enable the business to adapt and evolve its security ‘on the fly’, rather than attempting to duplicate a mirrored image of a relatively static environment.

Another important element of securing data in the cloud is the division of the cloud into separate network segments. With this model, data is categorised and organised in the same way it would be in a local data centre. This enables enterprises to benefit from the scalability, flexibility and cost benefits of the public cloud, without sacrificing the control of effective multi-layer security. This network separation enables IT to secure data by network segment as opposed to software group.

This layered cloud approach enables each network segment to function as its own ‘stream’, but also builds in the intelligence for secure inter-network communication, enabling organisations to seamlessly scale their cloud presence simply by adding new streams. Regardless of the number of cloud segments, each one acts as a single extension of the in-house IT structure, replicating all security functions regardless of location.

The public cloud offers enticing cost and scalability benefits, but until recently the potential security risks have eclipsed them. Businesses handling sensitive data were vulnerable to compliance issues stemming from the weak security capabilities. With a reconfigured view of the public cloud, IT departments can implement the appropriate layered security to make the cloud a true extension of the corporate infrastructure.

Big data and the globalisation of the business landscape, coupled with increased time-to-market pressures and budget restrictions, have resulted in ad hoc infrastructure build-outs and high levels of complexity.
Client and cloud provider accountability

Control over security, compatibility with existing systems, business continuity and compliance are the most commonly expressed concerns when organisations consider adopting a cloud-based strategy. However, as we’ll explain in the following section, these concerns can be mitigated with a subtle shift in thinking, a greater understanding of the division of responsibilities between cloud host and business client, and some informed decisions about network architecture.

There are three distinct models for cloud computing service – infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Each offers a different balance of control and responsibility between the host and the client business, making it more or less appropriate to a particular set of business requirements:

In an IaaS model, virtual or physical hardware resources are provided as a service, making significant use of server virtualisation. The cloud provider is responsible for security, management and control of the underlying cloud infrastructure that includes operating systems, virtualisation technology, computer servers, storage and networking components (e.g. switches, load balancers and firewall modules). The remainder of the stack – the middleware, applications, run-time components and the data – is the client’s responsibility. This means that any measures a business would take to protect its data on-premise can be implemented in the cloud – anti-malware, data leak prevention, security information and event management (SIEM), monitoring, auditing, logging, and more.

PaaS is a cloud platform for the development and deployment of application software. PaaS offerings are designed to support the entire application development lifecycle. The cloud provider is responsible for security, management and control of networking components, storage, servers, virtualisation technology, operating systems, specific middleware and any run-time components deployed. The client is only responsible for securing the applications and the data. In this scenario, third-party security and monitoring are more challenging to deploy and are highly dependent on the availability of appropriate application interfaces (APIs).

SaaS is the cloud computing model that’s most familiar – a hosted application accessed through a web browser, such as Gmail or Salesforce.com. In a SaaS environment, the service provider is responsible for the security, management and control of the entire stack. The client’s responsibility is limited to negotiating the appropriate services, service levels, privacy and compliance with the provider. If multiple SaaS solutions are in use, as is the case for most businesses, establishing a standardised approach for data monitoring may require the involvement of a third-party application broker, which in turn can introduce higher levels of risk for the data.

The cloud provider’s role in delivering secure cloud computing

Security in a cloud environment requires a multi-faceted approach. In an IaaS offering, much of the overall security burden rests with the client, who’s responsible for its network configurations and maintenance of the underlying applications and virtual server operating systems. The cloud provider plays an important role in securing both the overall infrastructure and the cloud orchestration software.

The cloud provider’s platform should comprise cloud hardware and software from industry-leading providers and a pre-integrated cloud management system. The cloud management system should provide automation of provisioning, orchestration and billing.

The user interface should allow end users to configure their cloud-based infrastructure to meet their requirements, in the same manner as they would with an on-premise network but with cloud-specific safeguards:

- Cloud servers should be assigned private IP addresses that isolate them from the rest of the Internet in a public cloud setting. Connectivity with the Internet should only occur when the client maps public IP addresses on the cloud network to the cloud server using VIP or NAT functions.
The cloud platform should offer clients a fully managed, secure foundation upon which to establish and grow their cloud strategies.

A cloud provider’s security model should include:

**Physical security:**
- All areas within the data centre are monitored 24x7x365 by closed-circuit cameras and on-site guards.
- Data centre space is physically isolated and accessible only by authorised administrators.
- Access is restricted to authorised personnel by two-factor biometric authentication
- CCTV digital cameras cover the entire centre, including cages, with 24x7 surveillance and audit logs.

**Software security:**
- Cloud orchestration technology should enforce multi-tenant security across all cloud functions; it should support role-based permissions, enabling clients to define which functions can be managed by which users within their organisation.
- A fully managed intrusion detection system using signature, protocol and anomaly-based inspection provides network intrusion detection monitoring.
- No passwords are stored in clear text on any system.

**Infrastructure security:**
- Edge-to-edge security, visibility and carrier-class threat management and remediation compares real-time network traffic against baseline definitions of normal network behaviour, immediately flagging all anomalies due to security hazards such as:
  - Denial of service and distributed denial of service attacks, worms or botnets; and
  - Network issues such as traffic and routing instability, equipment failures, or misconfigurations
- Infrastructure systems are fully updated and patched at all times. This approach ensures both the infrastructure and operating system images remain up to date.
- A security incident response team should handle reports of security incidents, escalating incidents to law enforcement and/or executive management as agreed with the client.
- All firewalls and VPNs receive 24x7x365 support and maintenance.

Security questions that you should ask your cloud provider

In order to evaluate the security approach of a cloud provider, enterprises should ask the following questions of their cloud providers:

**Network security:**
- Do you provide dedicated physical or virtual LANs to your clients?
- How does your data centre architecture contribute to client security?
- Are clients able to define their own authorisation and access control lists?
- How can clients ensure that their networks are secure?

**Secure user access:**
- How do you provide secure access (SSL-based VPNs) to your clients?
- How do you provide account-based security?
- Do you support role-based access controls?
- Do you support the addition and removal of ACL firewall rules directly in addition to host-level security?
- How do you monitor and report on usage and activities for audit purposes?

**Compliance:**
- What compliance certifications does your company hold, and how often do you undertake a compliance audit?
- Do you permit clients to audit your security controls?
- How do you address requests for location-specific storage to abide by data sovereignty requirements?
- Can a client’s data be prevented from being moved to a non-compliant location?

**Virtual machine security:**
- What protocols do you use to secure applications running on a virtual machine?
- How do you secure virtual machines in your cloud?
- How do you isolate one or a logical group of virtual machines from one other?
- Do clients have visibility into their virtual machines and servers running in their cloud and, if so, what monitoring tools do you provide?
Data security:
- What mechanisms are in place to prevent the co-mingling of data with other cloud users?
- What data security technologies are supported (tokenisation, encryption, masking, etc.)?
- Describe your encryption services.

Disaster recovery and business continuity:
- Do you provide backup and restore services?
- Can clients select a specific separate location for backup/replication?

Physical security:
- How is your data centre physically secured?

Summary
Businesses are facing a new set of complex data storage and management challenges. The cloud offers a path to efficiency and control; however, there are a number of potential challenges, including security. According to Gartner analyst Jeffrey Wheatman, the cloud “has essentially broken the traditional security models and architecture.”

Taking a layered or ‘defense in depth’ approach to cloud security is a natural extension of enterprise security models. Organisations demand more granularity in their control of the network, and only an integrated approach that considers networking and security together can provide this degree of custom functionality.

A layered approach to security enables enterprise IT to easily replicate the level of control it has over its own on-premise networks, extending user access controls and network permissions into the cloud. IT teams can do so directly, from their own, familiar user interface, which enables the organisation to adapt and evolve its security ‘on the fly’, essentially working with a mirrored image of an environment that’s already familiar.

Organisations should select their cloud providers with care to ensure that their security approach addresses common concerns regarding physical, software and infrastructure security.

* Data Security Monitoring in the Cloud: Challenges and Solutions, by Jeffrey Wheatman, 23 April 2012