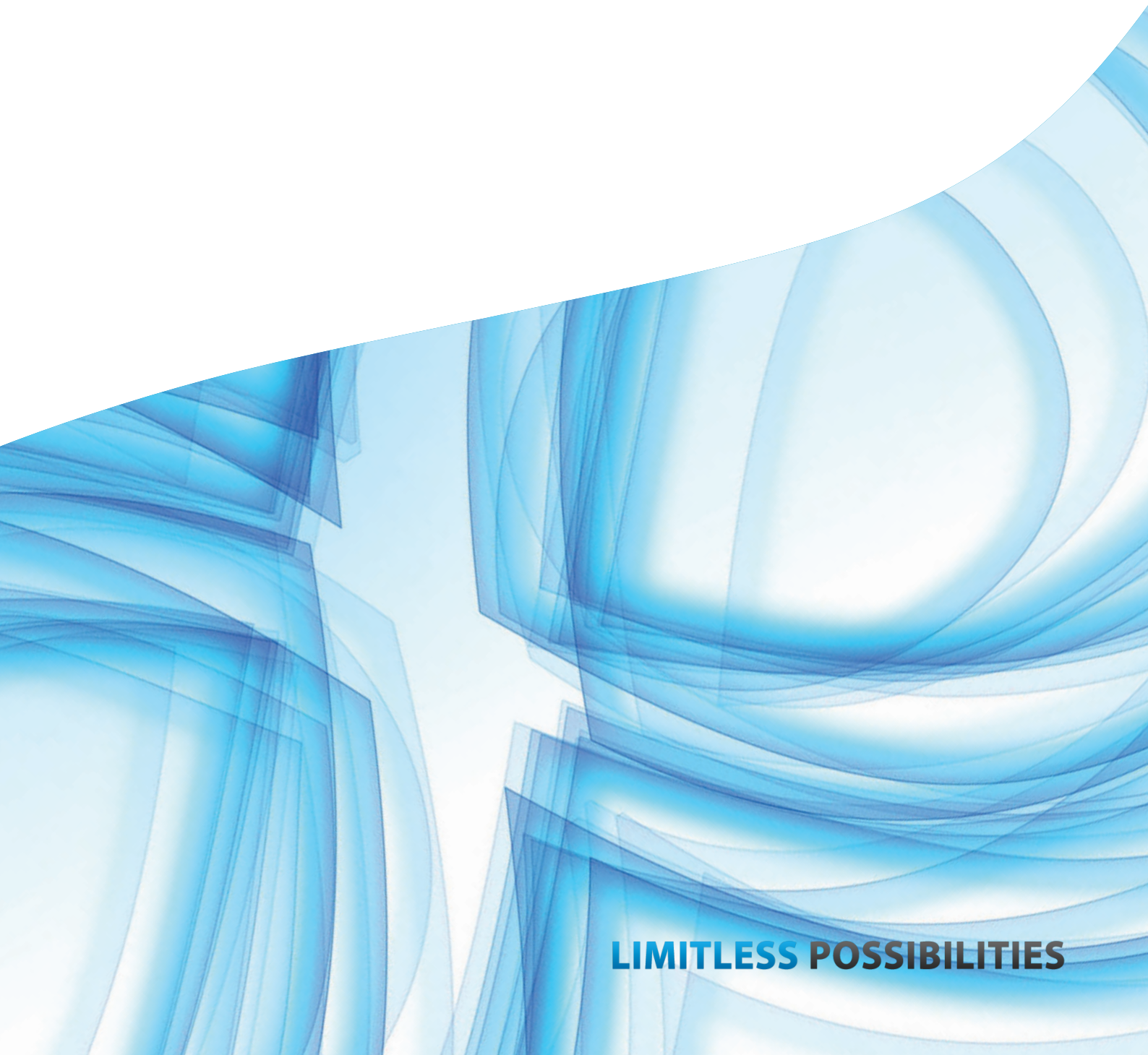
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Microsoft® Windows Azure™

Building Secure Cloud Applications

On the Microsoft Windows Azure platform



LIMITLESS POSSIBILITIES

Contents

1	Security and the cloud	3
	1.1 General considerations	3
	1.2 Questions to ask	3
2	The Windows Azure platform	4
	2.1 Inside the platform	5
	2.2 The data centre : who has access?	6
3	Application development	8
	3.1 Development practices	8
	3.2 Integration practices	8
	3.3 Operations: Application Lifecycle Services	9
4	Making the move: Capgemini can help	10
	4.1 The need for a trusted advisor	10
	4.2 Contact Capgemini	10

1. Security and the cloud

1.1 General considerations

Security requirements for applications and for data have always been critical components in software development and for on-premises software delivery. As you consider moving your applications and services to the Windows Azure cloud platform, you will find that security requirements are much the same, but there are some key differences that will be helpful to understand.

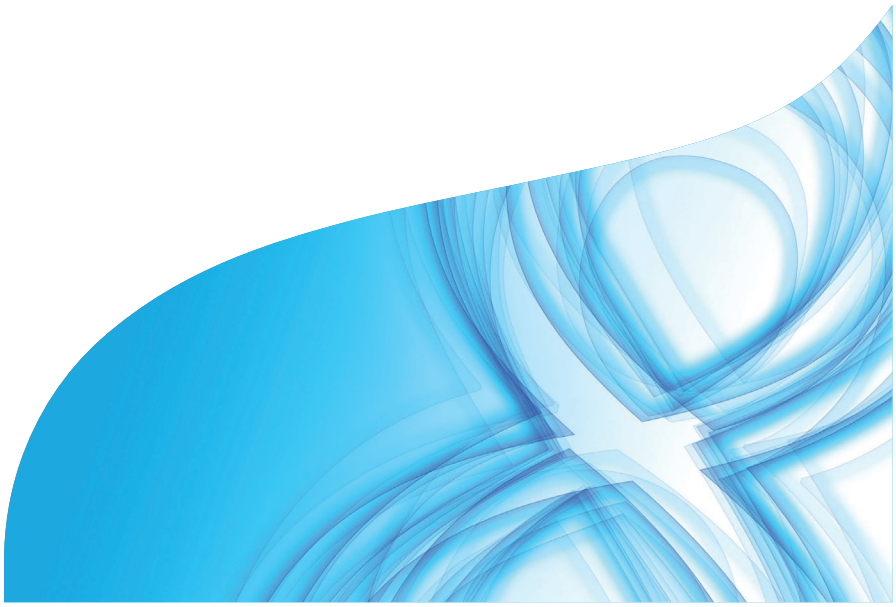
When you build your application on the Windows Azure platform, Microsoft hosts data and applications that belong to you and your customers. This means that Windows Azure must address information security challenges above and beyond traditional on-premises or off-premises IT scenarios. The responsibilities are split between Microsoft and you. Microsoft is responsible for the physical hosting of the data as well as platform capabilities. You are responsible for how you choose to use the platform and for the application you build.

The purpose of this paper is to clarify what moving to the cloud and Windows Azure means with regard to security and how Capgemini can help you make the right security decisions for your business.

1.2 Questions to ask

Before you move to the cloud, you should be very clear on what the security risks are. Cloud security covers a wide territory. Some of the questions that you will need to ask yourself include:

- Where is my data stored?
- Can anyone physically access my data?
- Can I actually lose my data?
- Is my customer information safe?
- Is my application in compliance with local and industry regulations?
- What steps does Microsoft take to provide a secure environment for my data?



2. The Windows Azure platform

Why Windows Azure?

Microsoft is one of a small number of cloud vendors. It has a long track record in enterprise software and a proven understanding of what security means to an enterprise.”

Microsoft has hosted cloud services for many years and currently hosts over 200 such services, from Xbox to Office 365. Not only does it have a great deal of experience in hosting large-scale secured services, it also offers years of experience in helping to define security and compliance.

With the Windows Azure platform, developers can build applications that span from consumer to enterprise scenarios. The key components of the Windows Azure platform are:

- **Windows Azure:** Windows Azure is the development, service hosting, and service management environment for the Windows Azure platform. It provides developers with on-demand compute instances, storage, bandwidth, content delivery, middleware and access control, as well as marketplace capabilities to build, host, and scale web applications through Microsoft data centers. With Windows Azure, your application is deployed on virtual machines (VM). Each deployment, or instance, has the same capabilities and security.

- **Microsoft SQL Azure:** Microsoft SQL Azure is a self-managed, multitenant relational cloud database service built on Microsoft SQL Server technologies. It provides built-in high availability, fault tolerance, and scalable database capabilities, as well as cloud-based data synchronization and reporting,

to build custom enterprise and web applications and extend the reach of data assets.

The Windows Azure platform provides a solid foundation to help prevent security breaches, and the necessary services to assist you in developing secure applications on top of it.

2.1 Inside the platform

Windows Azure helps provide confidentiality, integrity, and availability of customer data. It also provides transparent accountability, which enables customers and their agents to track administration of services. It is designed with the objective that customer data must be secure, data must be available 24 hours a day, seven days a week, and applications must be compliant with security standards for cloud applications.

2.1.1 Confidentiality

The Windows Azure operating system provides secure protocols for all communications within the Windows Azure platform. You can also use these e-protocols for external communications if your business requires it. All of the encrypted protocols that are available in the Windows Server operating system are also available with Windows Azure. All the encryption algorithms that developers are familiar with from Windows Server for developing for on-premises can be used to encrypt data in Windows Azure.

2.1.2 Integrity

One of the key capabilities of Windows Azure is that it provides isolation between services on the platform. This is done at several levels.

- At the network level, Windows Azure separates your application instances from other companies' applications, using virtual networks so that communication can only occur between instances of your own application.

- At the instance level, your service operates within a guest virtual machine. The Windows Azure Hypervisor isolates your VM from all others operating on that hardware.

- Windows Azure itself employs many levels of protection against hosted applications interfering with or taking control of it.

All these countermeasures greatly reduce the risk to your applications, as well as to the Windows Azure platform itself, helping to ensure the integrity of your data at all levels.

2.1.3 Availability

The Windows Azure platform is designed to be highly available. It provides numerous levels of redundancy to ensure maximum availability of customers' data.

For example, data in Windows Azure and SQL Azure storage is replicated within the platform to three separate nodes in such a way that the impact of hardware failures is minimized. This mechanism helps protect your data against hardware failure. In the event of a failure, Windows Azure automatically handles the issue and re-replicates the data if required. While this helps protect you against hardware failure, it is your responsibility to maintain backup copies of data beyond what Windows Azure offers.

Windows Azure is responsible for the health of all instances and will automatically replace instances that are not responding due to software or hardware failure.

The platform is designed to monitor that all instances of your application are healthy at the application instance level. If one goes down, a new instance is brought up automatically.

.

2.1.4 Accountability

The Windows Azure platform implements multiple levels of monitoring, logging, and reporting. The monitoring agent gathers monitoring and diagnostic log information from many places, such as the Fabric Controller and Operating System, and writes it to log files. It eventually pushes a digested (summarized) subset of the information into a preconfigured Windows Azure Storage account. In addition, the Monitoring Data Analysis Service is a freestanding service that reads various monitoring and diagnostic log data and summarizes the information, writing it to an integrated log. This combined information will help you investigate what happens in case of an anomaly, as you would in an on-premises environment, and it helps you to determine who is accountable for it as well. Windows Azure provides logs for both storage operations services and the management API.

Microsoft Support Services is also available to assist with troubleshooting services that run on Windows Azure. With your permission, it can help diagnose runtime issues.

2.2 The data center : who has access?

The security of your data depends on the strength of several separate factors, including:

- The physical security of the location of your data
- The confidentiality of your information
- The compliance of your application to global security standards

Windows Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24 hours a day, seven days a week, and employs various measures to help protect operations from power failure, physical and virtual intrusion, and network outages. These data centers comply with industry standards for physical security and reliability and they are managed, monitored, and administered by Microsoft operations personnel. They are designed for “lights out” operation, which means that almost all the management tasks are automated. Access is very limited and only people with a valid business justification have access.

The data center’s perimeter itself is protected by physical security controls, including intrusion detection systems and biometric identification devices. These systems have been designed to “fail closed” in case of power outages or incidents, which means that these devices will close the environment down in case of an incident.

Inside the data centers, access is controlled and logged to all server areas. In addition to the physical aspects of securing the data centers, processes are also important in the overall security scheme. The way the operational staff works on a day-to-day basis determines in large part how secure the data center is itself.

To ensure that the data is not compromised in the data center, all operational staff are screened and educated, and their tasks are subjected to rigorous operational procedures with regard to such things as systems' end-of-life. All Microsoft Online Services must follow the processes outlined in the security development lifecycle (SDL) and must conduct security threat analysis throughout the lifecycle of the service.

3. Application development

Application Lifecycle Services

Many management questions can be answered by the Capgemini Application Lifecycle Services offering, which is a managed service for all or part of your application landscape, including your cloud assets.

3.1 Development practices

Software architects and developers must understand the security threats to software developed for the cloud and use appropriate secure design and implementation practices to counter those threats in the cloud environment. The progression from classic, client-server computing to web-enabled applications to applications hosted in the cloud has changed the boundaries of applications. These boundary shifts make it all the more important to understand the security threats to software based on Windows Azure.

Your development team must ensure a secure and compliant development lifecycle by applying the correct development practices and coding standards. This lifecycle needs to include, among others, threat identification and mitigation so that software vulnerabilities are detected early and the attack surface of the application is greatly reduced. For more information, see Security Development Lifecycle[1].

Windows Azure provides built-in defenses against some attacks. Also, several platform services and security functions are available to your development team to help them build more secure applications. However, it is ultimately the business's responsibility to ensure the security and compliance of the applications. The key to security is in the design of the application itself.

3.1.1 Identity issues

One of the central issues facing developers of cloud applications is how to allow access for authorized clients and customers while meeting basic security requirements for confidentiality, availability, and integrity. The Windows Azure platform provides tools to aid in solving this problem. Identity management can be handled effectively by incorporating such key tools as:

- Windows Identity Foundation
- Active Directory Federation Services 2.0
- Windows Azure Access Control

Key questions about identity that your development team should ask include:

- How do I achieve single sign on for my applications?
- Should I implement Windows Identity Foundation?
- How should I integrate with other identity providers?
- Where does Windows Azure Access Control fit in?

3.2 Integration practices

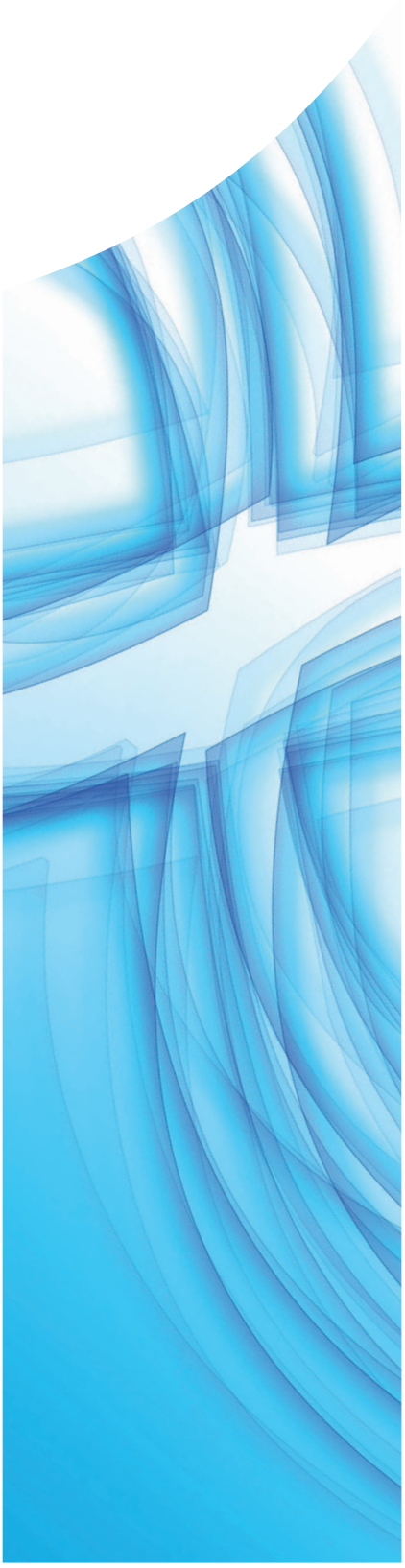
The integration points between your cloud applications and your existing on-premises assets require attention as well. Your security model needs to take into account the on-premises security requirements. In building your system, you will want to ensure that integration points between on-premises and cloud applications provide for security.
However, your on-premises development teams should treat the content of any incoming traffic as hostile by default and build in logic to validate the authenticity of the requests. For more information, see Security Best Practices for Developing Windows Azure Applications[2].

1- www.microsoft.com/security/sdl/default.aspx
2- www.globalfoundationservices.com/security/documents/SecurityBestPracticeswindowsazureApps.pdf

3.3 Operations: Application Lifecycle Services

As you can see, the Windows Azure platform offers many services that you can use to help create systems that are both secure and compliant with a wide range of regulations.
When you build an application using Windows Azure, you may encounter additional management questions that need to be answered, including:

- How do I manage identity providers, certificates, and access keys?
- How do I make changes to my application when it should be always available?
- How do I mitigate human mistakes?
- How do I replicate data across data centers without violating regulations?
- How do I properly manage my diagnostics and system information?
- Do I understand the impact of my legal and industry compliance obligations on my application?



4. Making the move: Capgemini can help

> **Our cloud advisory consultants have the technical capabilities to select the services that you require from the platform plus in-depth knowledge about local laws and industry-specific regulations, so they can guide you in your first steps to the cloud.**

> **Windows Azure ADCs**
>
> **Currently, Capgemini is in the process of training 1500 developers and architects for development on the Windows Azure platform with special attention to the characteristics specific to a cloud platform, including security, elasticity, and operational costs.**
>
> **Capgemini is also in the process of establishing a Windows Azure Center of Excellence in India.**

The Windows Azure platform provides a solid foundation on which to build your secure applications and systems, but ultimately the responsibility is yours for building and running a secure application that complies with the regulations required by your application.

4.1 The need for a trusted advisor

Businesses that provide services on the web need to make many complex choices. The Windows Azure platform is designed to support the needs of a global economy, which means that it supports highly available, highly scalable, and global web applications.

The needs of your applications may contradict the laws and regulations that you are subject to. You will need to carefully investigate regulations to determine how to proceed. Ultimately, it is up to you and your advisors to select a combination of services from the Windows Azure platform that provide you with the capabilities you need and that are in compliance with the rules and regulations to which your business is subject.

The services of a trusted advisor such as Capgemini can be invaluable, especially in the area of service selection. Our cloud advisory consultants have the technical capabilities to select the services that you require, plus in-depth knowledge about local laws and industry-specific regulations, so they can guide you in your first steps to the cloud. Accelerated Windows Azure delivery centers

Properly designing and implementing secure applications in the cloud requires a specific skillset that is not easily found on the market today. Currently, Capgemini is training 1,500 developers and architects for development on the Windows Azure platform with special attention to the characteristics specific to a cloud platform, including security, elasticity, and operational costs.

These people will specialize in custom software development and integration as a service using the Windows Azure platform. They will be working from several Accelerated Delivery Centers (ADCs) around the world, with a core Center of Excellence located in India.

4.2 Contact Capgemini

Capgemini can assist you in multiple ways:

- Our cloud advisory consultants can help you select the appropriate services to meet your application's needs while staying compliant to regulations.
- Our developers and architects can help you ensure that your application is designed, built and integrated in a secure way.
- We can manage your cloud application's lifecycle for you entirely, if you prefer. Capgemini Application Lifecycle Services offering, which is a managed service for all or part of your application landscape, including your cloud assets. It covers all stages of an application's lifecycle, from application conception, design, and deployment through service, renewal, and disposal.

About Capgemini

With around 115,000 people in 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2010 global revenues of EUR 8.7 billion Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at www.capgemini.com

For more information on any of these offerings, visit www.capgemini.com

Contact:

Yves Goeleven
Solution Architect
Capgemini
Yves.goeleven@capgemini.com

Krystianne Avedian
Global Leader Microsoft Sector and Field Alignment
Capgemini
Krystianne.avedian@capgemini.com

Special thanks to Yves Goeleven of Capgemini for his contributions to this document.

Yves Goeleven is a solution architect at Capgemini, located in Belgium, with over a decade of experience in designing and implementing enterprise applications and systems with Microsoft software and services, both on-premises and in the cloud. In 2011 he has been recognized as a Most Valuable Professional for the Windows Azure Platform by Microsoft.

Thanks also to Microsoft Windows Azure Technical Specialist David Aiken for his contributions to this paper.