Building Secure And Reliable Cloud Services: The Microsoft Story

Alan Chan
National Technology Officer
Microsoft Hong Kong Limited
Businesses are taking advantage of Cloud computing

- 50% more than half of surveyed CIO company's business to be running over public cloud by 2020 –Gartner
- 70% of CIOs will embrace a “cloud first” strategy in 2016 –IDC
- 45% of total IT services spent on cloud services by 2020 –Forrester

Cloud innovation

OPPORTUNITY FOR SECURITY & COMPLIANCE BENEFITS

Pre adoption concerns

60% cited concerns around data security as a barrier to adoption

45% concerned that the cloud would result in a lack of data control

Benefits realized

94% experienced security benefits they didn’t previously have on-premise

62% said privacy protection increased as a result of moving to the cloud

SECURITY
- Design/Operation
- Infrastructure
- Network
- Identity/access
- Data

PRIVACY

COMPLIANCE

Barriers to Cloud Adoption study, ComScore, September 2013
Cloud security and reliability challenges

- Growing interdependence amongst cloud providers and customers
- Complex global regulatory requirements and industry standards
- Evolving technologies, massive scale, changing business models, dynamic hosting environments
- Continuous and increasing sophistication of attacks
5.8+ billion worldwide queries each month

2.4+ million emails per day

250+ million active users

400+ million Active accounts

8.6+ trillion objects in Windows Azure storage

50+ million active users

48+ million users in 41 markets

1 in 4 Enterprise customers

50+ billion

Minutes of connections handled each day

50+ million active users

1+ billion customers · 20+ million businesses · 90+ markets worldwide

200+ Cloud Services
Microsoft’s cloud environment

Software as a Service (SaaS)
- Consumer and Small Business Services
- Enterprise Services
- Third-party Hosted Services

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Global Foundation Services

Microsoft Dynamics CRM, Bing
Outlook, Office 365

Windows Azure

“99.9% Uptime $$ Backed SLAs for Office 365 and Azure”
Cloud reliance – Security and compliance

Microsoft Cloud Services rely on GFS Infrastructure Audits to satisfy their own compliance obligations.

For some controls and DCs, GFS relies on 3rd Party DC Certifications.

Third Party Datacenters (DCs)
Microsoft Security Development Lifecycle
Security by design - Reduce vulnerabilities, limit exploit severity

**Education**
- Administer and track security training
- Training
- Requirements

**Process**
- Guide product teams to meet SDL requirements
- Design
- Implementation
- Verification

**Accountability**
- Establish release criteria and sign-off as part of FSR
- Release
- Incident Response (MSRC)
- Response

Ongoing Process Improvements

Defense-in-depth: infrastructure security

- Physical Security
- Network Security
- Host Security
- Application Security
- Data Security

- Identity and access management
- Configuration and Vulnerability Scanning
- 24x7x365 Incident Response
Infrastructure compliance capabilities

(as of January 2014)

<table>
<thead>
<tr>
<th>Certification/Compliance</th>
<th>✔️</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO / IEC 27001:2005 Certification</td>
<td>✔️</td>
</tr>
<tr>
<td>SSAE 16/ISAE 3402 SOC 1, AT101 SOC 2 and 3 Attestation</td>
<td>✔️</td>
</tr>
<tr>
<td>HIPAA/HITECH</td>
<td>✔️</td>
</tr>
<tr>
<td>PCI Data Security Standard Certification</td>
<td>✔️</td>
</tr>
<tr>
<td>FISMA Certification &amp; Accreditation</td>
<td>✔️</td>
</tr>
<tr>
<td>FedRAMP P-ATO by the Joint Authorization Board</td>
<td>✔️</td>
</tr>
<tr>
<td>Various State, Federal, and International Privacy Laws (95/46/EC—aka EU Data Protection Directive; California SB1386; etc.)</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Datacenter evolution

1989-2005 • 2007 • 2009 • 2012 • Future

Generation 1
- 2.0+ PUE
- Colocation
  - Server Capacity
  - 20 year Technology

Generation 2
- 1.4 – 1.6 PUE
- Density
  - Rack Density & Deployment
  - Minimized Resource Impact

Generation 3
- 1.2 – 1.5 PUE
- Containment
  - Containers, PODs
  - Scalability & Sustainability
  - Air & Water Economization
  - Differentiated SLAs

Generation 4
- 1.12 – 1.20 PUE
- Modular
  - ITPACs & Colocations
  - Reduced Carbon
  - Right-Sized
  - Faster Time-to-Market
  - Outside Air Cooled

Generation 5
- 1.07 – 1.19 PUE
- Integrated
  - Integrated System
  - Resilient Software
  - Common Infrastructure
  - Operational Simplicity
  - Flexible & Scalable

Future
Case Study
Hurricane Sandy
Power outage

About 8.6 million citizens lost electricity in the U.S. during the storm.

Source: U.S. Department of Energy, Office of Electricity Delivery and Reliability situation reports. Chart data reflect situation posted at 3:00 PM EST on November 9, 2012.
Contingency & business continuity measures

Hurricane Sandy was meticulously managed end-to-end

- Initiated a proactive war room with monitoring and control
- Delivered internal communications
  - Latest developments on hurricane status
  - Health of services
  - Contingency plans
- BCP implemented on all Edge services and properties
- Supply of fuel to generators on regular basis
- Worked with service providers for restoration of internet circuits
Impact to infrastructure & services

Infrastructure Challenges

- **Drop in capacity** via network provider fiber cut
- **Water flooding** caused partial failure of communications lines
- **Water leakages** during storm period at facilities
- **Core network device outages** due to combination of power, network, and load issues

Services

Microsoft services were migrated to avoid service impact

- bing
- Windows Azure
- XBOX LIVE
- Outlook.com
- Office 365
- SharePoint
- Skype
- SkyDrive
Results

- Successful implementation of Business Continuity and Disaster Recovery Plans
- No major service impact to customers
- No significant impact to the datacenter or assets
- Increased resources to aid local relief efforts
- Excellent overall coordination among internal and external teams for combined execution to ensure minimal impact
Considerations for choice in cloud services provider

Require that the provider has attained third-party certifications and audits, e.g., ISO/IEC 27001:2005

Know the value of your data and processes and the security and compliance obligations you need to meet

Ensure a clear understanding of security and compliance roles and responsibilities for delivered services

Consider the ability of vendors to accommodate changing security and compliance requirements

Ensure data and services can be brought back in house if necessary

Require transparency in security policies and operations