

Building Cloud Trust

Ioannis Stavrinides
Technical Evangelist
MS Cyprus

“If you’re resisting the cloud because of security concerns,
you’re running out of excuses.”

FORRESTER®

“The question is no longer: ‘How do I move to the cloud?’
Instead, it’s ‘Now that I’m in the cloud, how do I make sure
I’ve optimized my investment and risk exposure?’”



“By 2020 clouds will stop being referred to as ‘public’ and ‘private’. It will simply be the way business is done and IT is provisioned.”





My first question
Do you use Cloud today?

Microsoft Cloud Magnitude



200+ Cloud Services
1+ million Servers
\$15B+ Infrastructure Investments



1 Billion Customers
20+ million Businesses
90 Countries Worldwide



380+ Active
Subscriptions in Cyprus

57%
of Fortune 500
10,000 new subscribers per week
Microsoft Azure

2000+
Businesses in Cyprus
From 2 to 3500 users

1.2 billion
worldwide users

 Office 365



3.5 million

Active users

 Microsoft Dynamics CRM Online

5.5+ billion
Queries per month



300+ million
Users per month



48 million
Members in 57 countries



450+ million
Unique users each month





Privacy & Control

Refers to **what** is protected and the determination of **who** is permitted to use, disclose or access that information.





Security

Refers to **how** private information is safeguarded – Ensuring Privacy by controlling access to information and protecting it from inappropriate disclosure and accidental or intentional destruction or loss.

Compliance

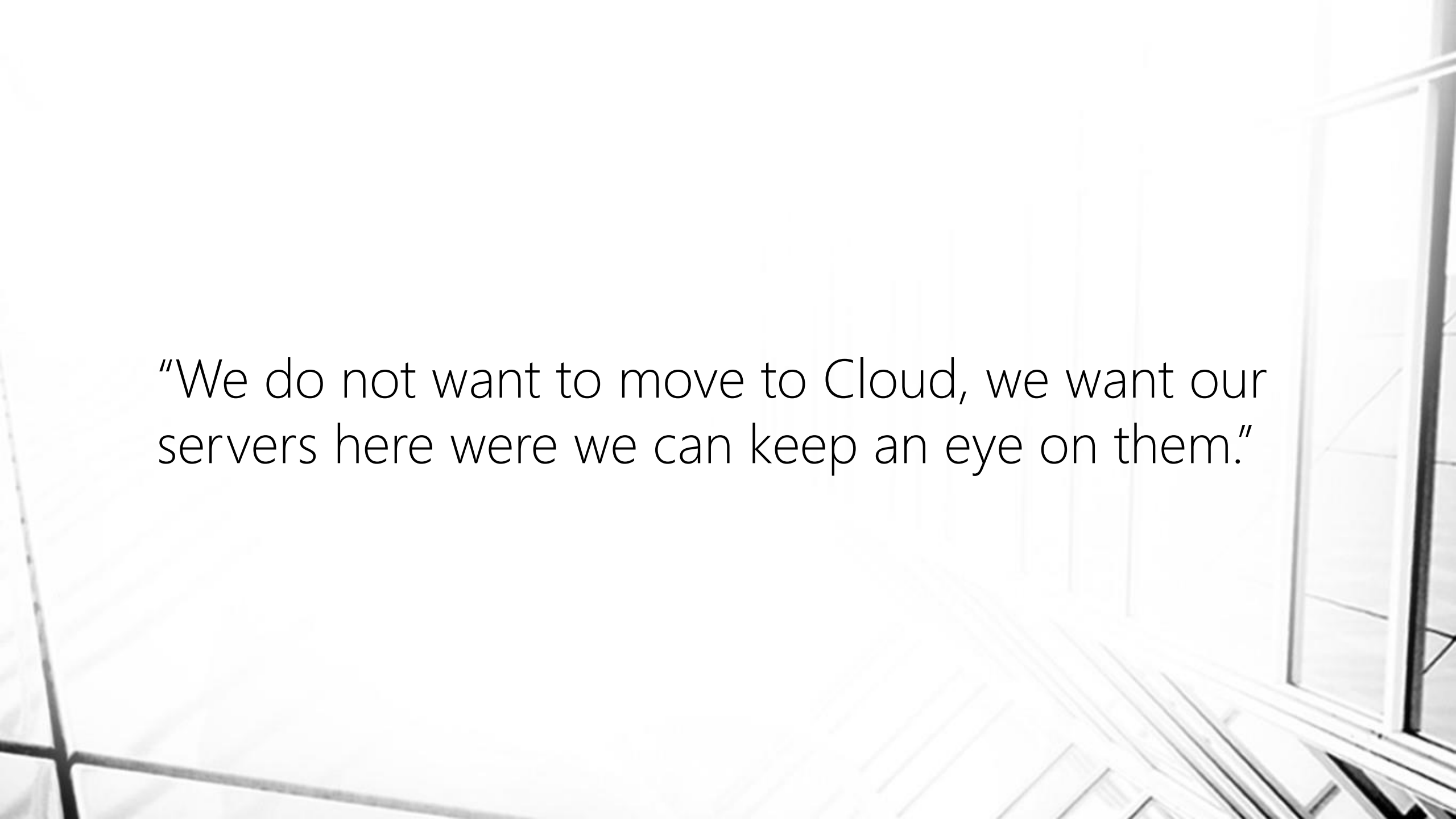


Describes the goal that organizations aspire to **achieve** in their efforts to ensure that they are aware of and take steps to comply with relevant laws and regulations.



Transparency

Describes the level of **detail in disclosing** of the data protection policies and practices that govern customer data and its location, use of subcontractors, access and handling of data, and related issues.



“We do not want to move to Cloud, we want our servers here were we can keep an eye on them.”

Azure Security Design and Operations

We make security a priority at every step, from code development to incident response.



Security Development Lifecycle (SDL) and Operations Security Assurance (OSA)

Company-wide, mandatory development and operations processes that embeds security into every phase of development and ops process.

Assume breach simulation

Dedicated security expert "Red Team" that simulate real-world attacks at network, platform, and application layers, testing the ability of Azure to detect, protect against, and recover from breaches.

Incident response

Global, 24x7 incident response service that works to mitigate the effects of attacks and malicious activity.



"A very important point to remember is how much can a customer secure their infrastructure, considering their budget and expertise, compared to what Microsoft invests, their technical ability to execute and their Enterprise-focused legacy."



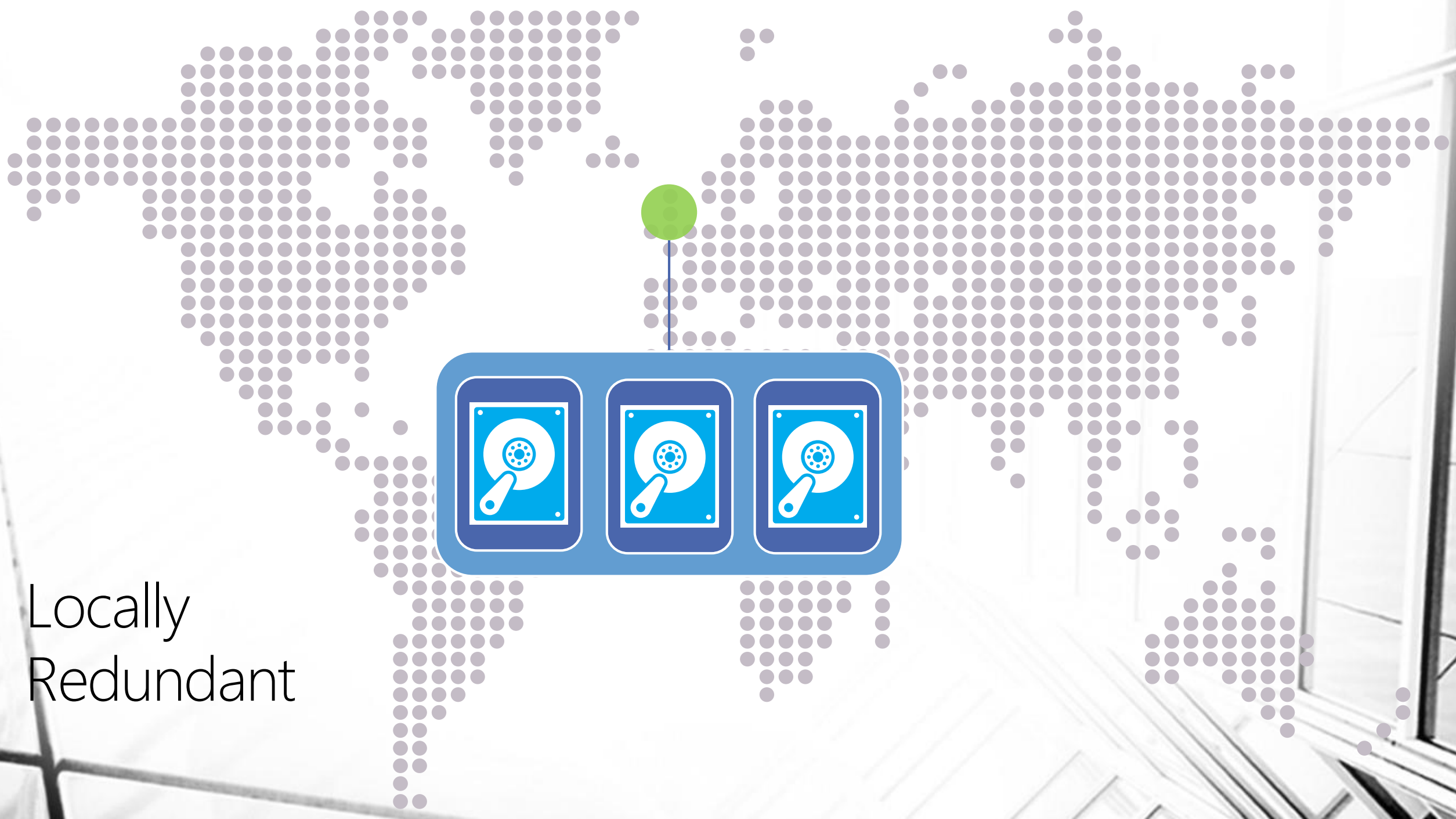
“What guarantees my data will not be lost?”

In Microsoft Azure, Microsoft ensures business continuity

For Office 365, guarantees 14-30 day retention policy

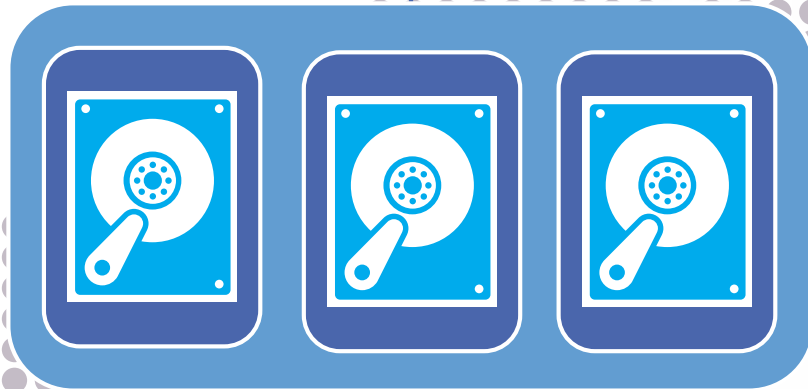
Understanding Business Continuity compared to Retention Policy and Backup

Understanding the impact in a cloud vendor's business if they loose and render customer data irretrievable



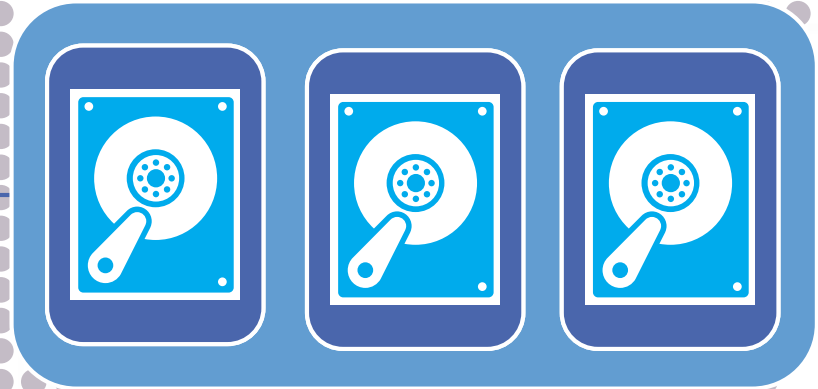
Locally
Redundant

Zone
Redundant





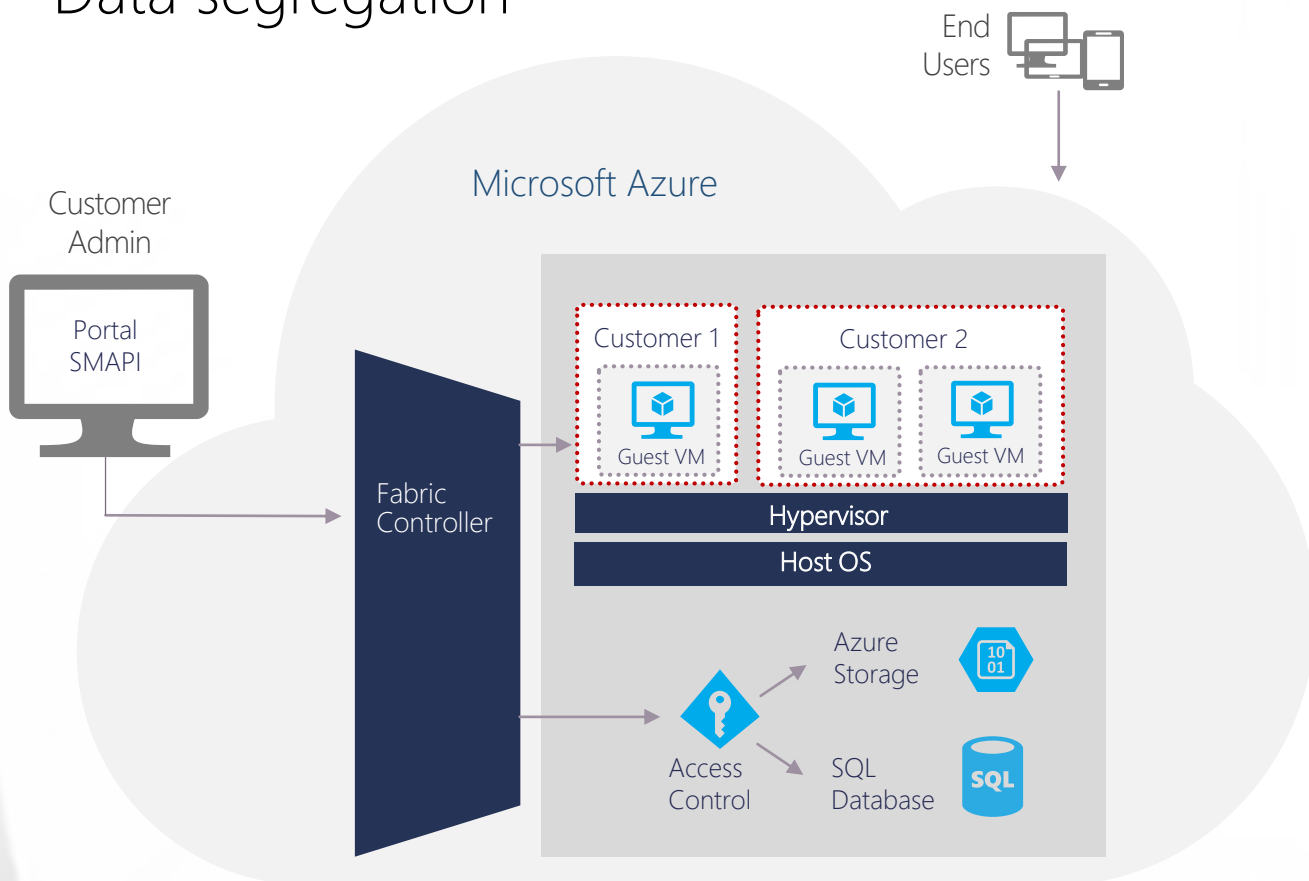
Geo
Redundant





“How do I know another one of Microsoft’s customers will not see my stuff?”

Data segregation



Storage isolation:

- Access is through Storage account keys and Shared Access Signature (SAS) keys
- Storage blocks are hashed by the hypervisor to separate accounts

SQL isolation:

- SQL Database isolates separate databases using SQL accounts

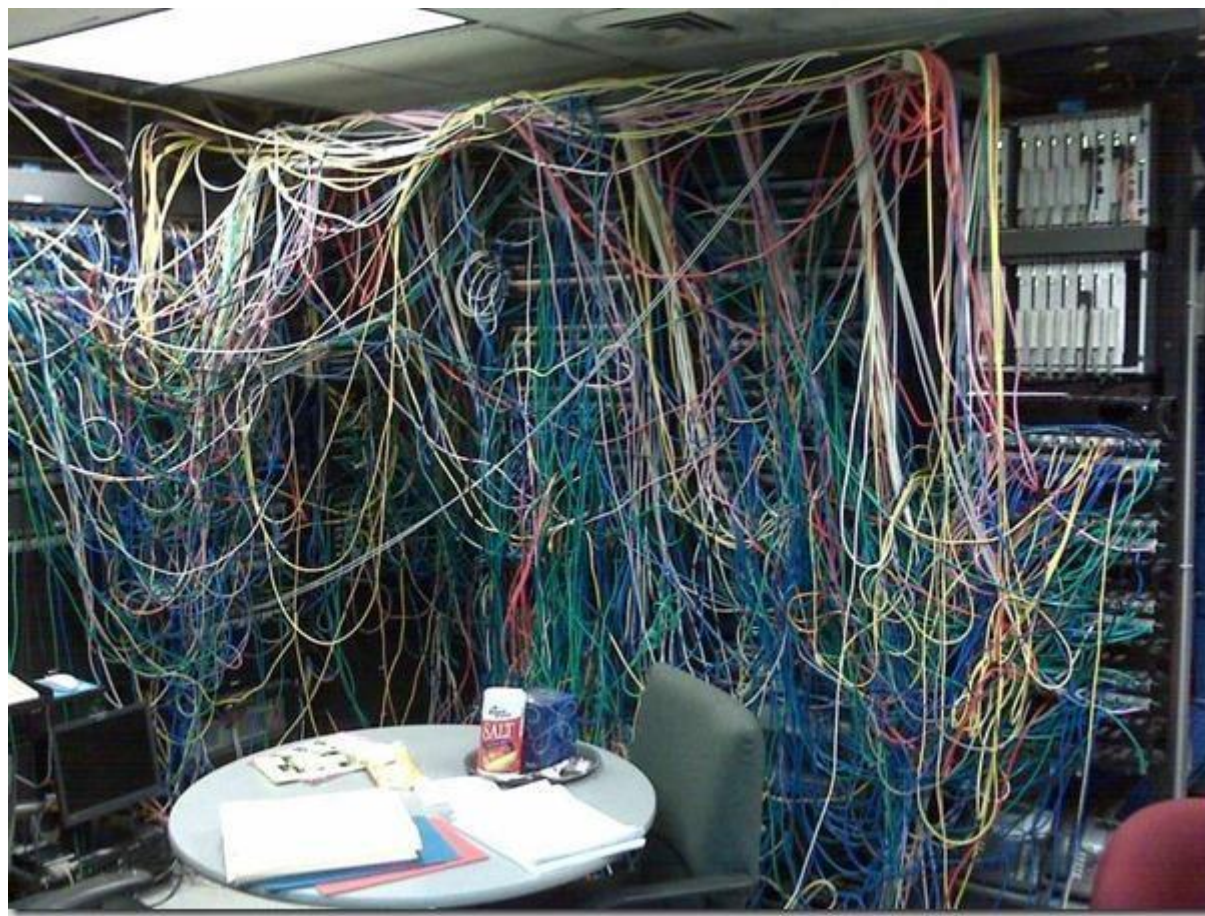
Network isolation:

- VM switch at the host level blocks inter-tenant communication



"I think it is not safe to go Cloud, here is better."

The "Here"





"I think it is not safe to go Cloud, here is better."

Microsoft Datacenters

Cameras

24X7 security staff

Barriers

Fencing

Alarms

Two-factor access control:
Biometric readers & card
readers

Security operations center

Seismic bracing

Days of backup power



Perimeter



Building



Computer room



"I think it is not safe to go Cloud, here is better."

Understanding security risks before allowing misconceptions affect strategy decisions
The following are the most frequent reasons for corporate data theft:

Top Risk: Disgruntled Employees

2nd highest Risk: Careless or Uninformed Employees

3rd highest Risk: Mobile Devices (BYOD)

4th Risk: Unpatched Devices



"I think it is not safe to go Cloud, here is better."





“Do outages happen?”

Yes, there is no 100% bulletproof system, 99.9% SLA is the best you can find in the Market. Last major outage occurred November 2014 and it involved temporary access issues to data (not data loss)

“What did Microsoft do?”

Gave back affected customers a lot of Money or free services, respective of impact. The outage did not result in loss of customer base



Operational Security summary

Data & Keys

Data Protection
Access control,
encryption, key
management



User

Admin Access Identity
management, dual-
factor authentication,
training and awareness,
screening, Least and
Temporary Privilege



Application

Application Security
Access control,
monitoring, anti-
malware, vulnerability
scanning, patch and
configuration
management



Host System

Host Protection
Access control,
monitoring, anti-
malware, vulnerability
scanning, patch and
configuration
management



Internal Network

Network Security
Segmentation, intrusion
detection, vulnerability
scanning



Network Perimeter

Network Security
Edge ACLs, DOS,
intrusion detection,
vulnerability scanning



Facility

Physical Security
Physical controls, video
surveillance, access
control





Privacy & Control



“Where will my data be?”

CREATE A VIRTUAL MACHINE

Virtual machine configuration

CLOUD SERVICE [?]

Create a new cloud service

CLOUD SERVICE DNS NAME

keithwstpvm01 .cloudapp.net

REGION/AFFINITY GROUP/VIRTUAL NETWORK [?]

East US

STORAGE ACCOUNT

Use an automatically generated storage account

AVAILABILITY SET [?]

(None)





“Where will my data be?”

Where is my data?

These interactive data maps provide specific geographic details about where customer data is stored in Office 365 and Microsoft Dynamics CRM Online.

Specifically, they provide information regarding the locations of our datacenters throughout the world for the Office 365 and Microsoft Dynamics CRM Online services.

Europe, Middle East, Africa ▾



o365datacentermap.azurewebsites.net



“Who is the owner of the data?”

Microsoft clearly states repeatedly...

Customer Data.

Microsoft will process Customer Data in accordance with the provisions of this Amendment and, except as stated in the Agreement and this Amendment, Microsoft (1) will acquire no rights in Customer Data and (2) will not use or disclose Customer Data for any purpose other than stated below. <cont>

From: Microsoft Online Services Data Processing Agreement (Mar2013) – page 2

You own your own data.

With Microsoft Azure, you are the owner of your customer data.

We define customer data as all data, including text, sound, video, or image files and software, that are provided to Microsoft by you, or on your behalf, through use of Azure. For example, it includes data that you upload for storage or processing and applications that you or your end users upload for hosting on Azure.

<https://azure.microsoft.com/en-us/support/trust-center/privacy/>



“What stops Microsoft from using my data?”

Within the Microsoft Online Services Terms:

Use of Customer Data

Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer. This paragraph does not affect Microsoft’s rights in software or services Microsoft licenses to Customer.



“What stops Microsoft from using my data?”

To put it blunt..

\$20B+ in investments /year on cloud technology and infrastructure
in a highly competitive landscape





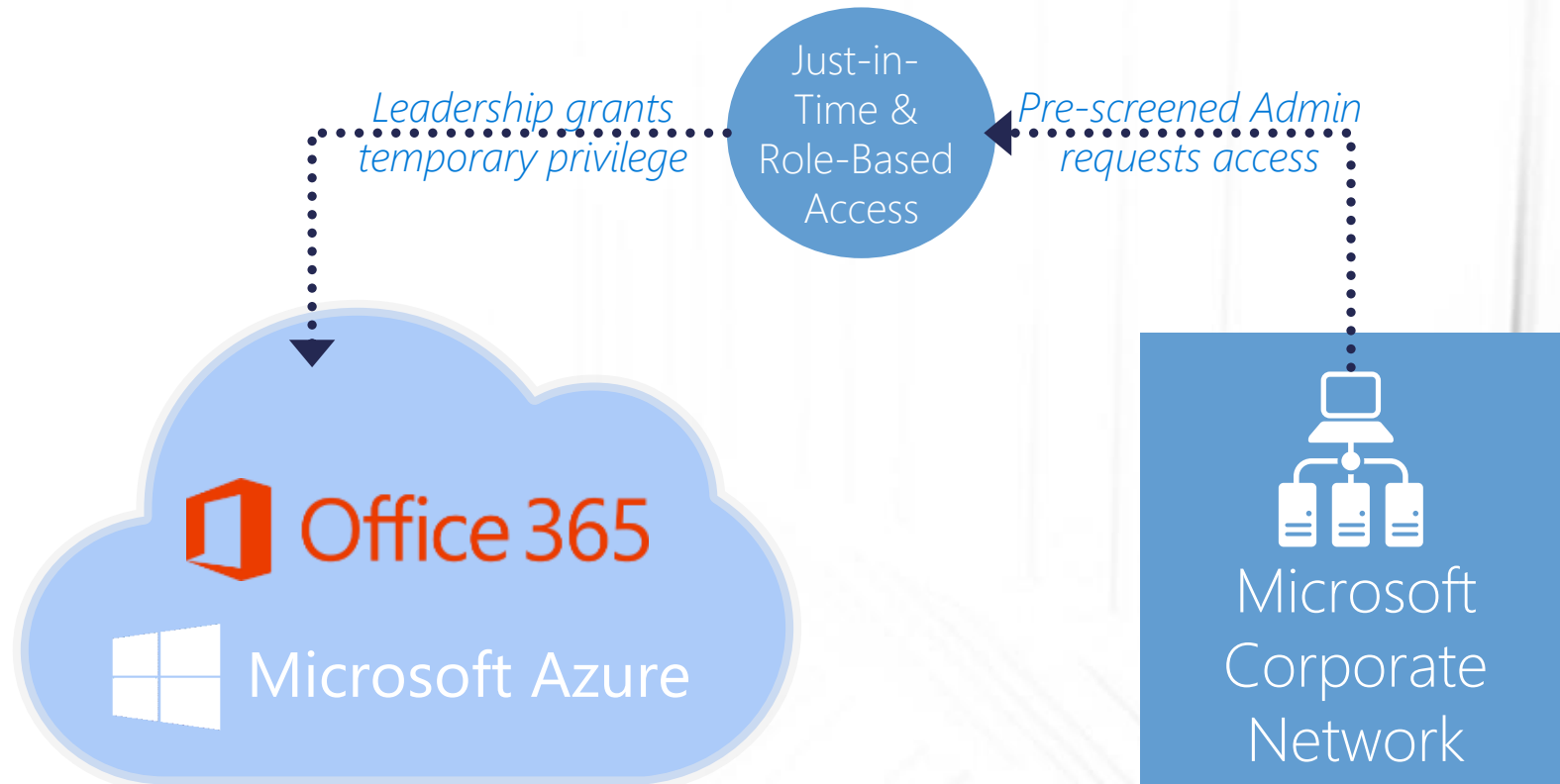
"Are you telling me a Microsoft employee can't just log in and snoop around my files?"

No standing access to the customer data

Grants least privilege required to complete task

Multi-factor authentication required for all administration

Access requests are audited, logged, and reviewed





“Microsoft will disclose my data to anyone with a legal demand”

Microsoft will not disclose Customer Data to law enforcement unless required by law. Should law enforcement contact Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Microsoft may provide Customer’s basic contact information to the agency. If compelled to disclose Customer Data to law enforcement, Microsoft will use commercially reasonable efforts to notify Customer in advance of a disclosure unless legally prohibited.

From: Microsoft Online Services Data Processing Agreement (Mar2013) – page 2



On Law enforcement requests

Microsoft does not disclose customer data to law enforcement unless as directed by customer or required by law, and will notify customers when compelled to disclose, unless prohibited by law.

The Law Enforcement Request Report discloses details of requests every 6 months.

Microsoft doesn't provide any government with direct or unfettered access to customer data.

Microsoft only releases specific data mandated by the relevant legal demand.

If a government wants customer data it needs to follow the applicable legal process.

Microsoft only responds to requests for specific accounts and identifiers.





“NSA or Equivalent is monitoring Microsoft’s Datacenters”

We do not offer direct access to customer data. We believe that you should control your own data. Microsoft does not give any third party (including law enforcement, other government entity, or civil litigant) **direct or unfettered access to customer data except as you direct.**

From: <http://www.microsoft.com/en-us/trustcenter/privacy/responding-to-govt-agency-requests-for-customer-data>



“What happens when I delete my data?”

Data Deletion

- Index immediately removed from primary location
- Geo-replicated copy of the data (index) removed asynchronously
- Customers can only read from disk space they have written to

Disk Handling

- Wiping is NIST 800-88 compliant
- Defective disks are destroyed at the datacenter



“I do not want my email on cloud where it could be possible for someone to read them”

Fact:

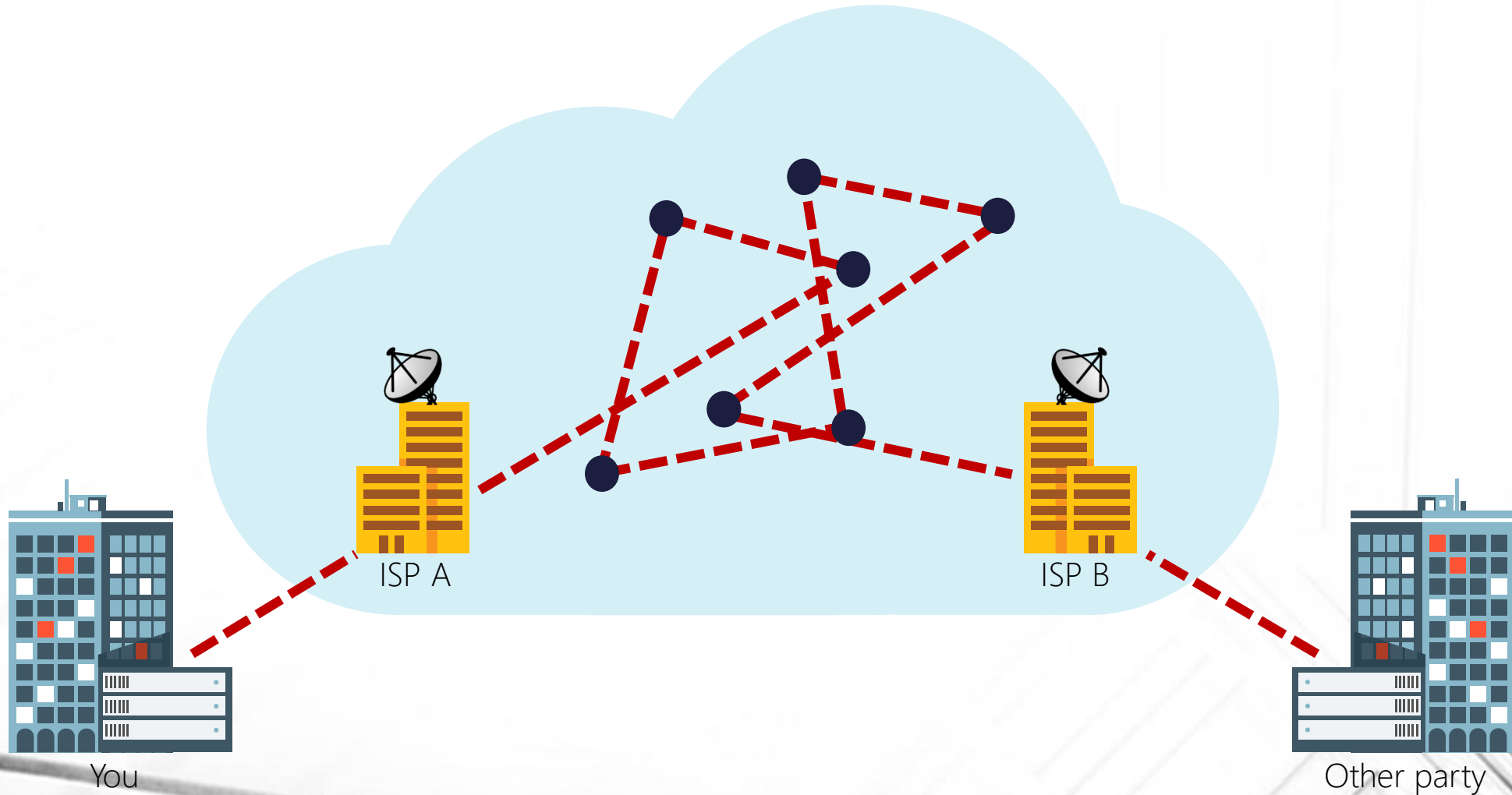
Email is asynchronous and unencrypted means of communication.

Meaning:

Anyone standing within the network between you and your other party
Could potentially read your email.

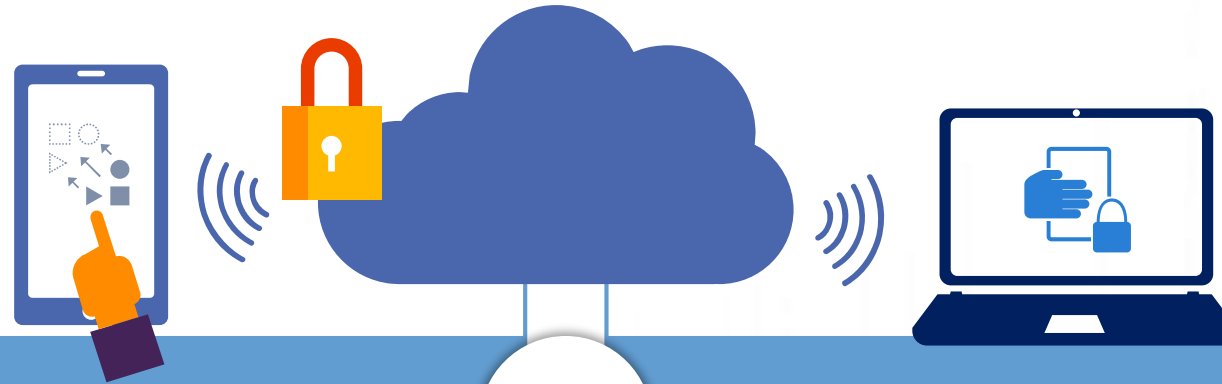


"I do not want my email on cloud where it could be possible for someone to read them"





Regarding Customer data – Summarizing



Control over data location



Customers choose data location and replication options.

Control over access to data



Strong authentication, carefully logged “just in time” support access, and regular audits.

Encryption key management



Customers have the flexibility to generate and manage their own encryption keys.

Control over data deletion



When customers delete data or leave Azure, Microsoft follows procedures to render the previous customer’s data inaccessible.



Compliance



The most relevant question to compliance I have heard was:

“Should I add a disclaimer in our users signature about our email hosted on Office 365?”



To give you the foundation to achieve that compliance, Microsoft puts serious effort to help ensure that compliance controls are current and that we build and maintain a dynamic compliance framework. Ultimately, it is up to you to determine whether our services comply with the specific laws and regulations applicable to your business and satisfy your legal requirements.

From: <http://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx>



CDSA



China GB 18030



China MLPS



CJIS



DISA Level 2



EU Model Clauses



FDA



FedRAMP

FedRAMP



FERPA



FIPS 140-2



FISC



HIPAA



MTCS



CCSL (IRAP)



IRS 1075



ISO/IEC 27001



ISO/IEC 27018



PCI-DSS



NZCC Framework



Section 508 VPATs



SOC 1 & SOC 2



GOV.UK

UK G-Cloud



ISO/IEC 27018

Microsoft is the first major cloud provider to adopt the first international code of practice for governing the processing of personal information by cloud service providers.

Prohibits use of customer data for advertising and marketing purposes without customer's express consent.

Prevents use of customer data for purposes unrelated to providing the cloud service.





HIPAA / HITECH

The Health Insurance Portability and Accountability Act (HIPAA) is the US law that regulates patient Protected Health Information (PHI). Microsoft enterprise cloud services offer customers a HIPAA Business Associate Agreement (BAA) that stipulates adherence to HIPAA's security and privacy provisions.





Compliance “as a Service”

Some technologies and solutions offer significant value in terms of achieving compliance for a customer’s organization with minimal effort or investment.



Compliance “as a Service” through Office 365

Elaborate on In-place Hold & e-Discovery

Explain Data Loss Prevention

Describe Rights Management Services



Compliance “as a Service” through Enterprise Mobility Suite

Policy enforcement on Mobile Devices and BYOD

User Centric approach to accessing corporate resources

Advanced Threat Analytics



Transparency



Transparency

You know what we do to help secure your data

You know where your data is stored and how it used

You know who can access your data and under what conditions

We are transparent about how we respond to government requests for your data

You can review the standards certifications for Microsoft cloud services



Law Enforcement Request Reports

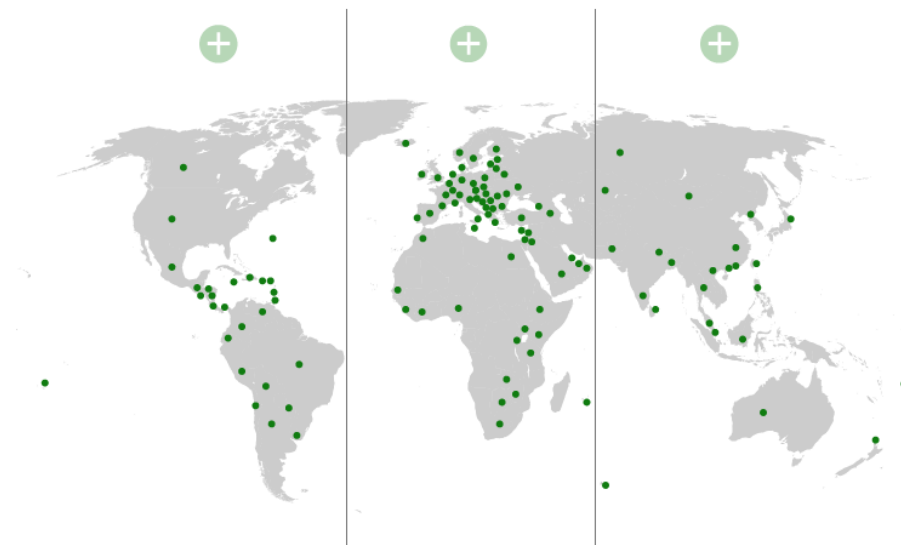
Requests by country

2015 (JAN-JUN) 2014 (JUL-DEC) 2014 (JAN-JUN) 2013 (JUL-DEC) 2013 (JAN-JUN)

Show global results

Select a region

Select a country



Global

Requests

Total number of requests

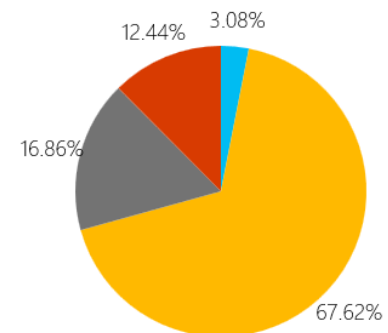


Accounts/users specified in request



Disclosures

- % Disclosed content
- % Only subscriber/transactional data
- % No data found
- % Rejected





Principles, Policies and Practices FAQ

We believe that our customers deserve and need to understand our policies. Increased transparency may also help advocates and policymakers better arrive at an appropriate balance between public safety and customer privacy.



What is the process for disclosing customer information in response to government legal demands?



Microsoft requires an official, signed document, issued pursuant to local law and rules. Specifically, we require a subpoena or equivalent before disclosing non-content, and only disclose content in response to a warrant or court order. Microsoft's compliance team reviews government demands for user data to ensure the requests are valid, rejects those that are not valid, and only provides the data specified in the legal order.



What laws apply to Microsoft customer records and content?



For data hosted in the U.S., Microsoft follows the Electronic Communications Privacy Act. We require at least a subpoena before turning over non-content records, such as basic subscriber information or IP connection history, and we require a court order or warrant before producing content. Irish law and European Union directives apply to the Hotmail and Outlook.com accounts hosted in Ireland. Skype is a wholly-owned, but independent division of Microsoft, headquartered in and operating pursuant to Luxembourg law.



How does Microsoft determine what countries are able to request data?



Microsoft produces certain data in response to valid legal requests from governmental entities for data we host in those countries. Additionally, Microsoft may disclose non-content data in response to a valid legal request. For our Microsoft services, we only comply after it is validated locally and transmitted to our compliance teams. When legal demands are served directly on Microsoft's local subsidiaries in other countries, a local team or individual (typically a lawyer or someone operating under legal guidance) will receive and authenticate the legal demand. If it complies with local law, then it will be translated and sent to the appropriate compliance team for review and processing.



Office 365 status reports

Current status



Last refreshed: 00:29, 16 December 2015

[View history for past 30 days](#)

Service	Today	DEC 15	DEC 14	DEC 13	DEC 12	DEC 11	DEC 10
Exchange Online ▲							
E-Mail and calendar access	✓	ⓘ	ⓘ	✓	✓	✓	✓
E-Mail timely delivery	✓	✓	✓	✓	✓	✓	✓
Management and Provisioning	✓	✓	✓	✓	✓	✓	✓
Sign-in	✓	✓	✓	✓	✓	✓	✓
Voice mail	✓	✓	✓	✓	✓	✓	✓
Identity Service ▼	✓	✓	✓	✓	✓	✓	✓
Mobile Device Management	✓	✓	✓	✓	✓	✓	✓
Office 365 Portal ▲							
Administration	✓	✓	✓	✓	ⓘ	ⓘ	ⓘ
Portal	✓	✓	✓	✓	✓	✓	ⓘ
Office Subscription ▼	✓	✓	✓	✓	✓	✓	✓
Power BI	✓	✓	✓	✓	✓	✓	✓
Rights Management Service	✓	✓	✓	✓	✓	✓	✓
SharePoint Online ▼	✓	✓	✓	✓	✓	✓	✓
Skype for Business ▼	✓	✓	✓	✓	✓	✓	✓
Sway	✓	✓	✓	✓	✓	✓	✓
Yammer Enterprise	✓	✓	✓	✓	✓	✓	✓

✓ Normal service

ⓘ Investigating

⬇ Service interruption

↔ Service degradation

⏸ Restoring service

⌚ Extended recovery

✓ Service restored

ⓘ Additional information

☐ PIR published

[Learn more about service health status](#)



Office 365 uptime reports

Recent worldwide uptimes:

2014				2015		
99.99%	99.95%	99.98%	99.99%	99.99%	99.95%	99.98%
Q1	Q2	Q3	Q4	Q1	Q2	Q3

<https://products.office.com/en-us/business/office-365-trust-center-operations>

The image shows a bright, overexposed interior space, likely a modern building. On the right side, there is a large window with a white frame. In the foreground, a dark metal railing is visible, suggesting the viewer is looking out from an elevated position. The overall scene is very bright and lacks detail due to overexposure.

Cloud is already here



Microsoft is a Trusted Cloud Provider

Thank you very much!

