Moving to the Cloud in an Azure Sky

A Security View

Dominik Zemp
TSP Security
Microsoft Switzerland Ltd Liab. Co.
dominik.zemp@microsoft.com

General Trends

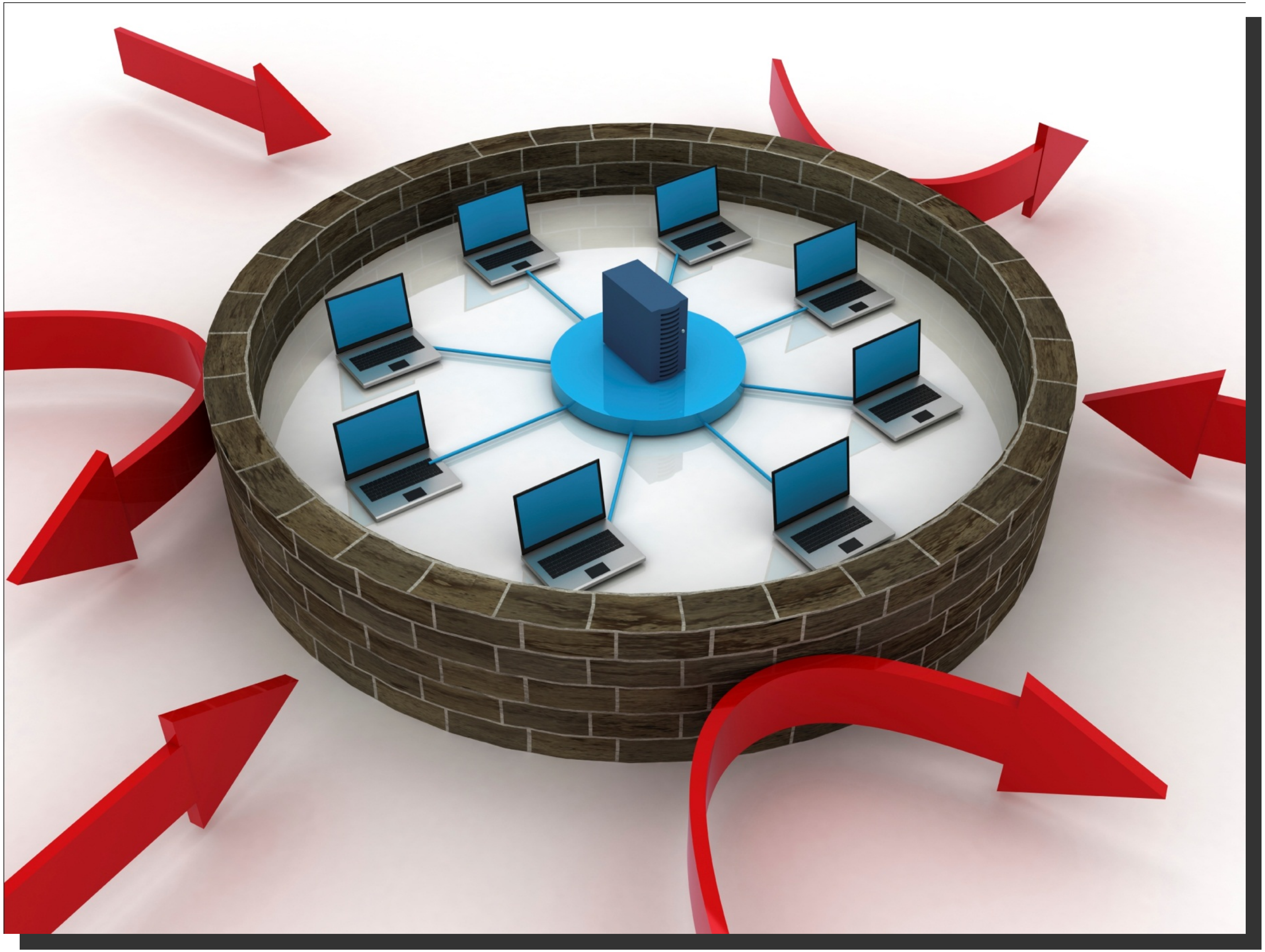
What is “The Cloud”?

Opportunities and Challenges

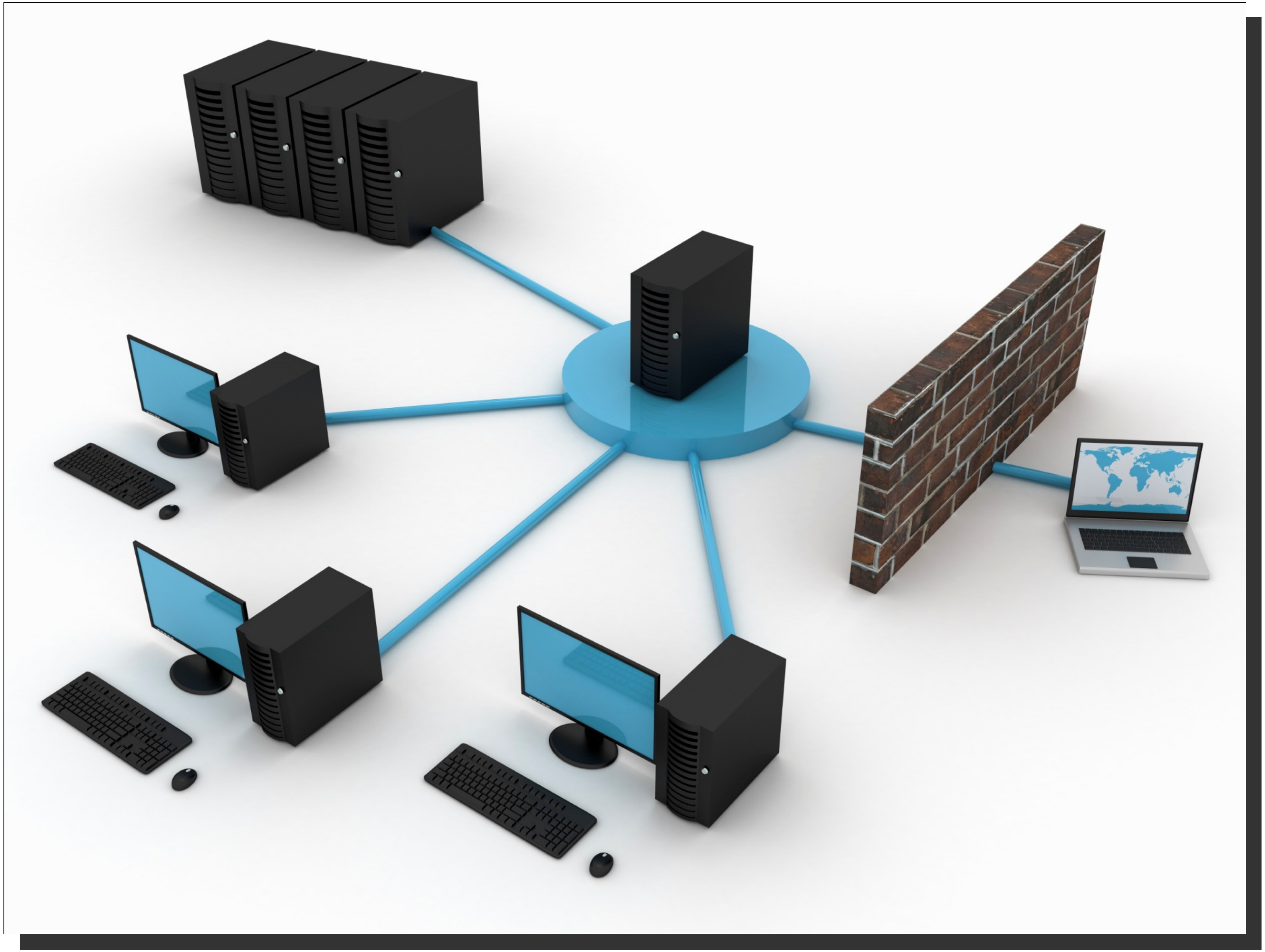
The 5 Considerations

Recommendations

Your Network Has to Adapt



Your Network Has to Adapt



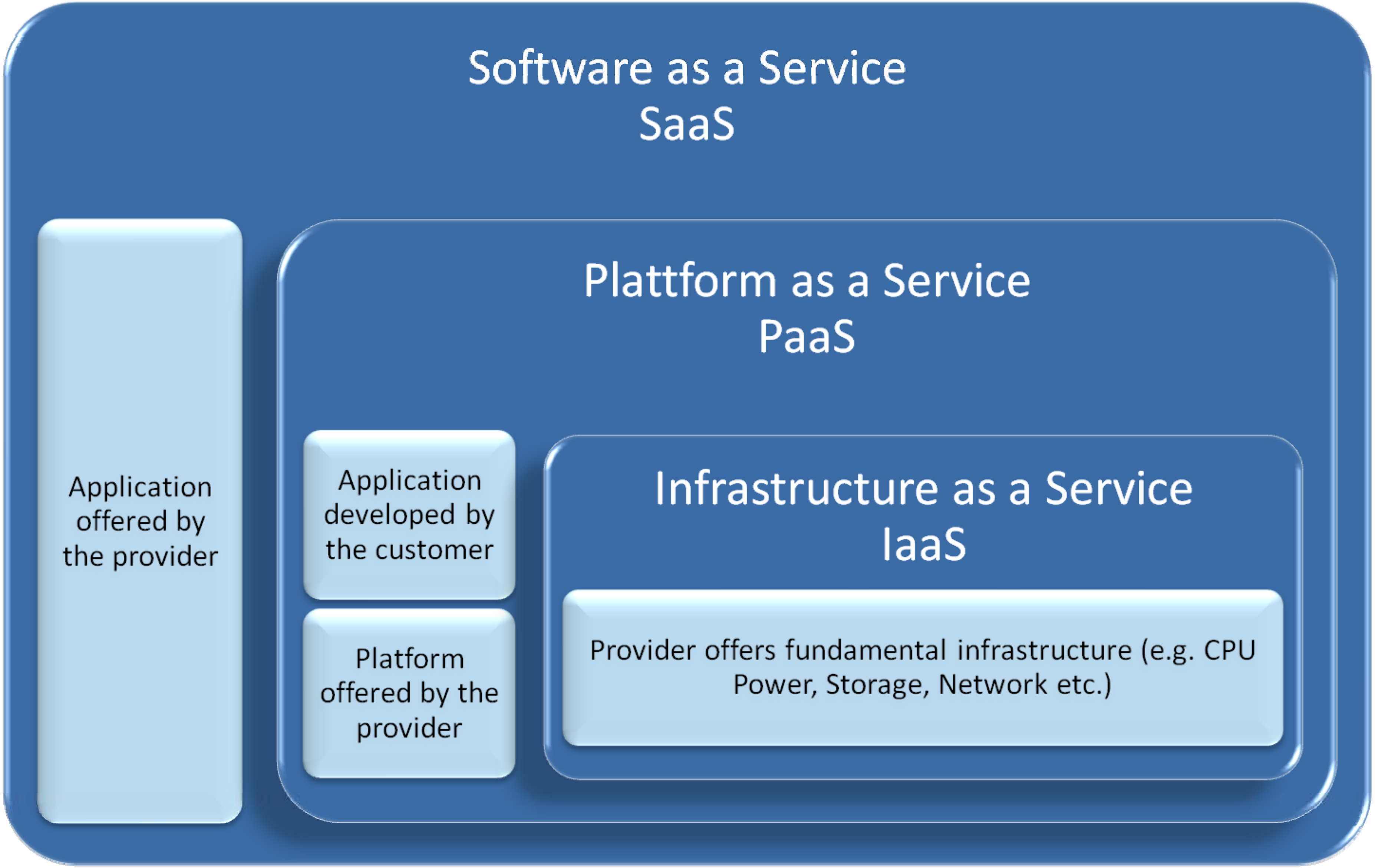
Your Network Has to Adapt

Essential Cloud Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
  - Location independence
- Rapid elasticity
- Measured Service

Source: NIST (http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc)

Cloud Service Models



Software as a Service
SaaS

Application offered by the provider

Plattform as a Service
PaaS

Application developed by the customer

Platform offered by the provider

Infrastructure as a Service
IaaS

Provider offers fundamental infrastructure (e.g. CPU Power, Storage, Network etc.)

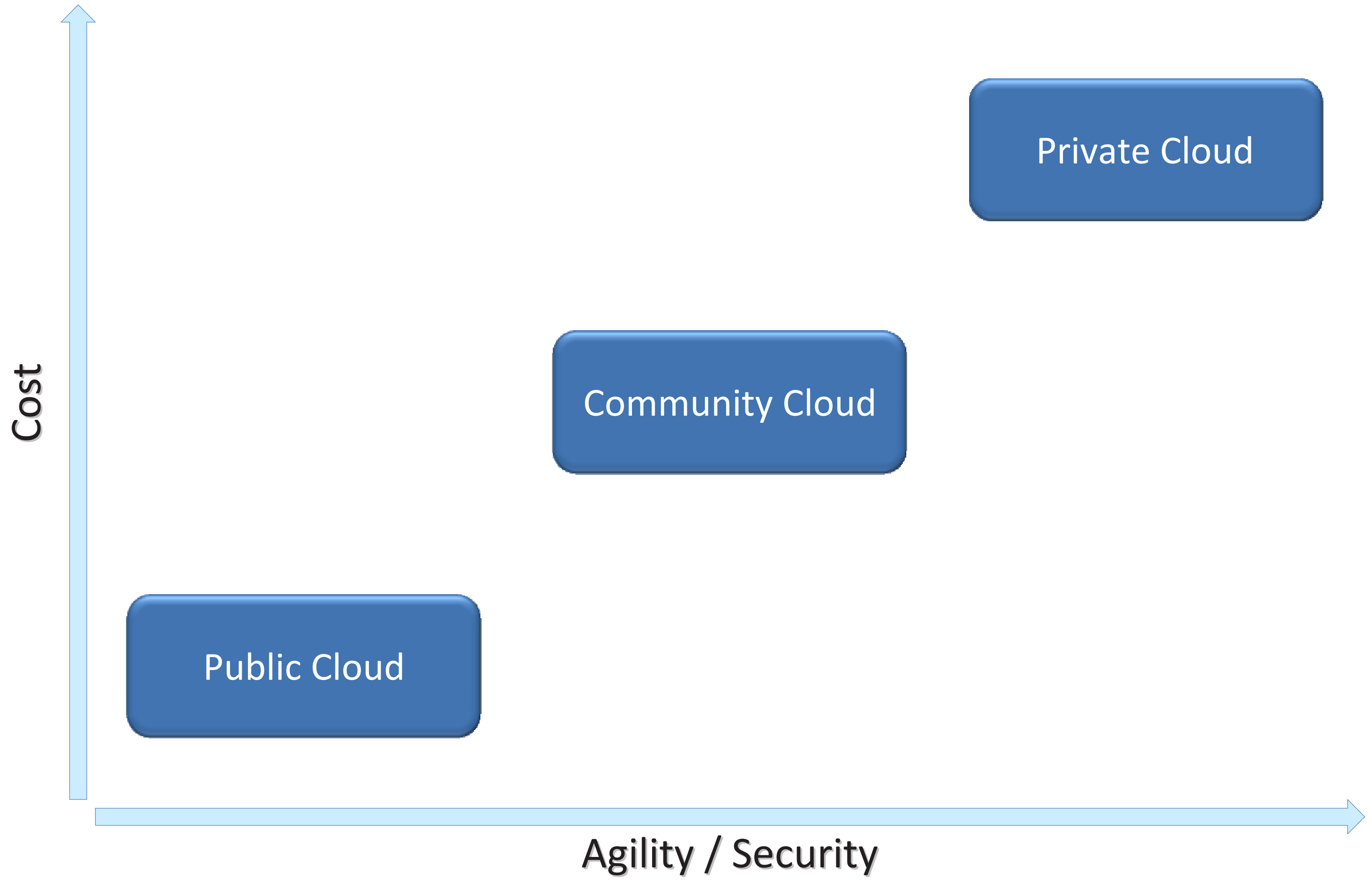
Source: NIST (http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc)

Cloud Deployment Models

- Private Cloud
  - Owned by or operated for one enterprise
- Community Cloud
  - Shared infrastructure by a community
- Public Cloud
  - Offered to the public, wide scale
- Hybrid Cloud
  - Composition of two or more models

Source: NIST (http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc)

Cloud Deployment Models



Opportunities and Challenges

- Information under the provider’s control
  - Not limited by space or geography
- Changes in IT processes
  - Provider can have better security processes
  - Physical security will be managed by the cloud provider
  - Legal sovereignty challenges
- Centralized Storage of Data
  - Economy of Scale
  - Attractive for Criminals
- Privacy Issues
- Forensics

Cloud Security Considerations

Compliance and Risk Management

Identity and Access Management

Service Integrity

Endpoint Integrity

Information Protection

Compliance and Risk Management

- Compliance is still the duty of the Customer
- Sound Risk Management encompassing the Cloud is needed
- Collaboration between Customer and Provider is essential
  - Need of a certain level of Process Transparency
- Strong Internal Team needed
  - Contract Negotiation
  - Definition of Controls and Metrics
  - Integration of Controls into own processes

*Compliance requirements can be fulfilled by a **skilled internal team** and a certain level of **process transparency** by the cloud provider(s).*

Identity and Access Management

- Cross-Domain Collaboration requires secure identities
  - People and Devices
- Based on In-Person Proofing or similar
- Claims-Based
- Based on interoperable standards
- Privacy vs. Authentication has to be balanced
- Processes have to be able to include several providers

Any digital identity system for the cloud has to be ***interoperable*** *across different organisations and cloud providers and based on strong processes.*

Service Integrity

- Service Engineering and Development
  - Strong and Transparent Engineering Processes Needed
    - Requirements
    - Design
    - Implementation
    - Verification
    - Release
    - Response
  - Proofed
  - Based on Threat Models or similar

The provider should follow a ***clear, defined, and provable process*** *to integrate security and privacy in the service from the beginning and for the whole lifecycle.*

Service Integrity

- Service Delivery
  - Internal processes have to be able to cover multiple provider
    - Security Monitoring
    - Auditing
    - Forensics
    - Incident response
    - Business Continuity
    - Etc.
  - Requirements depend on application and information needs

The service delivery capabilities of the provider and the security management and auditing needs of the customer must be aligned.

Endpoint Integrity

- Is part of the delivery chain
- Often subject to social engineering attacks (and similar)
- Review today’s processes and policies

It is very important to ***include the end point*** *in any security consideration for cloud-based services.*

Information Protection

- Data Classification is the foundation
  - Requirements
  - Legal Needs
- Persistent Data Protection needed
  - Encryption/Rights Management
- Has to cover the whole transaction
  - Data in transit
- «New» Challenges
  - Data Sovereignty
  - Access to Information
  - Data Partitioning and Processing

Implemented Data Classification *helps to decide which data is ready for the cloud, under which circumstances, and with which controls.*

Recommendations

- Well-Functioning Risk and Compliance Programs are a must
- Data classification is the base
- Choose the right Deployment Model (Private, Community, or Public)
- Strong, cloud trained, Internal Team still needed
- Process Transparency, Compliance Controls, and Auditability by the Provider
- Implement a Secure Development Lifecycle and evaluate the Provider and their vendors as well
- Stronger federated identity and access controls
- Information Lifecycle Controls
- Access controls to operate across organisational boundaries without surrendering identity ownership

Microsoft®