NARUC

Winter Committee Meetings

Staff Subcommittees on Electricity & Electric Reliability

Cloud Service for Electric Utilities

Moderator: *Sheree Kernizan*, Georgia PSC

If you have not done so already, please download the NARUC app, so you can participate in our polling questions!

Panelists:

- *Dr. Arshad Mansoor*, EPRI
- *Felek Abbas*, NERC
- *Jianhui Wang, PhD*, Argonne National Labs
- *Joe Joyce*, Microsoft Azure

NERC CIP Standards

The Cloud, Virtualization, and CIP

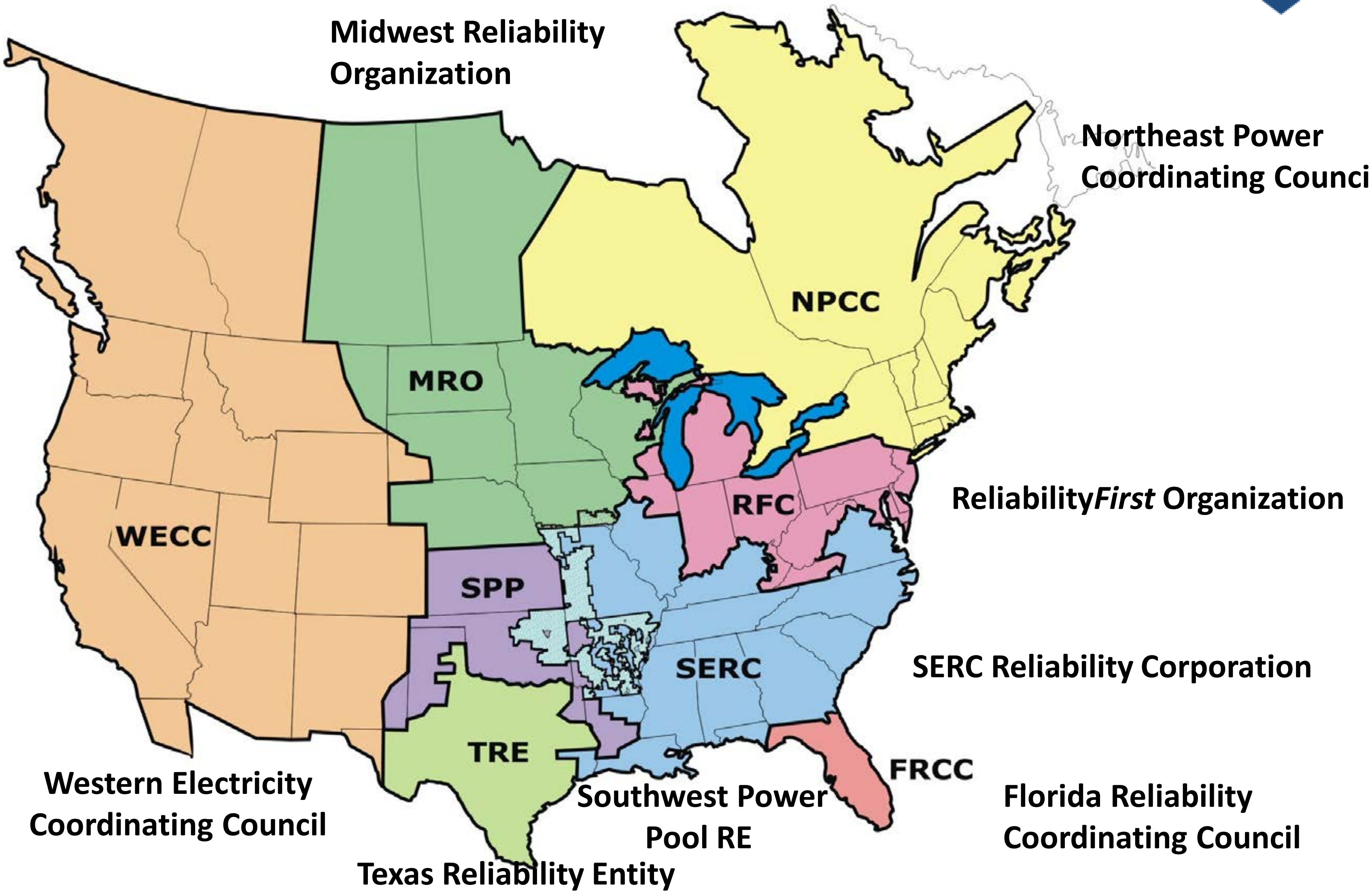
Felek Abbas, Senior CIP Compliance Advisor
NARUC Cloud Services Panel
February 12, 2017

RELIABILITY | ACCOUNTABILITY

NERC Mission

- To ensure the reliability of the Bulk-Power System in North America
  - Develops and enforces Reliability Standards
  - Annually assesses seasonal and long-term reliability
  - Monitors the Bulk-Power System
  - Educates, trains, and certifies industry personnel
- Subject to oversight by the Federal Energy Regulatory Commission in the United States
- Designated by Department of Energy (DOE) as the Electricity Information Sharing and Analysis Center (E-ISAC)

NERC Regions



CIP Standards – Version History

Urgent Action 1200
- BOT Approved 07/2003
- Renewed 2005

CIP Version 1
- BOT Approval 05/2006
- FERC Approval 01/2008

CIP Version 2
- BOT Approval 05/2009
- FERC Approval 09/2009

CIP Version 3
- BOT Approval 12/2009
- FERC Approval 03/2010

CIP Version 4 (Surpassed by CIP Version 5)
- BOT Approval 01/2011
- FERC Approval 04/2012

CIP Version 5 Currently Effective
- BOT Approval 11/2012
- FERC Approval 11/2013
- FERC Approval 01/2016

Cloud services rely on virtualization technology for:

- Scalability
  - Storage
  - Computation
  - Instantiation

Cloud services rely on virtualization technology for:

- High Availability
  - Redundancy
  - Geographic Diversity
- Security
  - Patching
  - Network Monitoring

CIP Standards Approach to Security

The CIP Standards were developed with physical systems in mind:

- Identify BES Cyber Assets
- Group them into BES Cyber Systems
- Place them inside an Electronic Security Perimeter
- Place everything inside a Physical Security Perimeter

Cyber Asset

- Cyber Asset Definition:

  Programmable electronic devices, including the hardware, software, and data in those devices.

The Cloud and Mixed-Trust

Mixed-Trust virtualization introduces unique risks.

- Resource misuse
- Resource starvation
- Promiscuous mode

- Compromises of the host OS and hypervisor from lower-trust guests
- Privileged position threat vectors

Virtualization and Audits

Virtualized environments must be able to:

- Identify all the hardware used in the virtual environment – CIP-002-5.1a
- Classify them as BES Cyber Systems – CIP-002-5.1a
- Protect them inside an Electronic Security Perimeter – CIP-005-5

Virtualization and Audits

- Virtualized environments must be able to:
  - Protect them inside a Physical Security Perimeter – CIP-006-6
  - Perform personnel risk assessment for all employees who have access to the systems or their perimeters – CIP-004-6
  - Secure their data – CIP-011-2 and future standards

The Future of Virtualization & CIP

The Standards Drafting Team for FERC Order No. 822 is currently evaluating whether modifications to the CIP standards are necessary to change the manner in which those standards address virtualization.

Questions and Answers

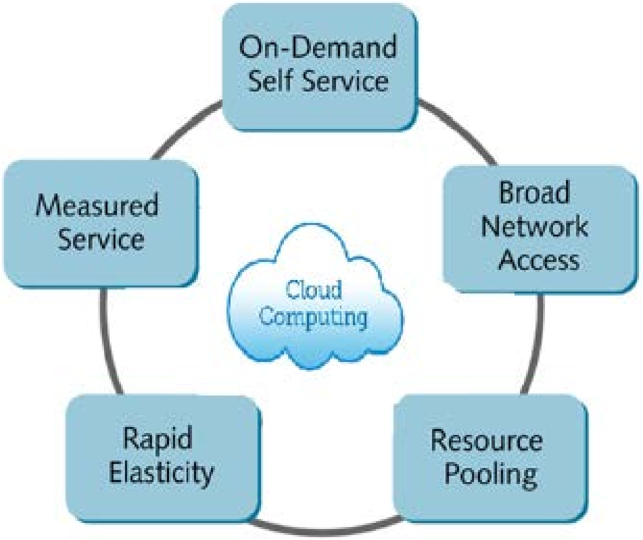
Cloud and Outsourcing Security for Power Grid Applications

Jianhui Wang
Energy Systems Division
Argonne National Laboratory

NARUC Winter Meeting 2017
February 12, 2017

Essential Characteristics of Cloud Computing

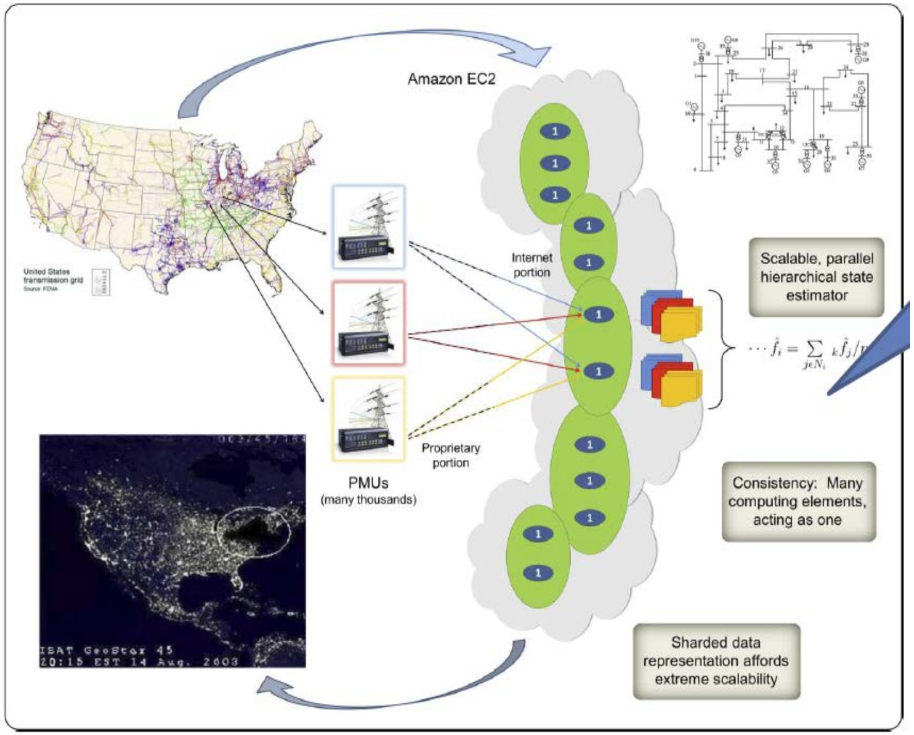
1. **Resource Pooling**
   – No need to have servers in-house
   – Reduce the need for advanced hardware in-house
   – Cloud platforms hide the complexity of the underlying infrastructure from users by providing simple graphical interfaces
2. **Broad Network Access**
   – Data is available anytime, anyplace, and anywhere
   – Secure backup and disaster recovery of data
1. **Rapid Elasticity and High Cost-effectiveness**
   – Quickly scale operations & powerful computational capacit
3. **On-demand Self Service**
   – Pay for only what you use
4. **Measured Service**
   – Resource usage can be monitored, controlled, and reported
   – Transparency



Characteristics defined by NIST

The Need for Cloud Computing for Power Grid Applications

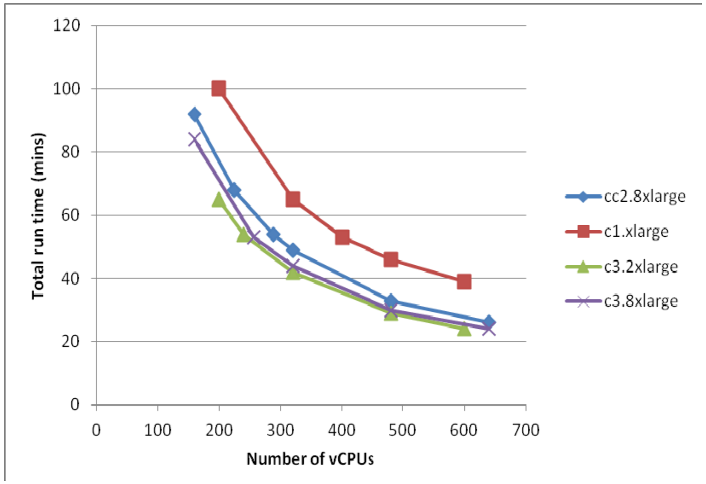
- Many power grid applications are computationally intensive including:
  - Wide-area state estimation
  - Contingency analysis
  - Security-constrained economic dispatch (SCED)
  - Security-constrained unit commitment (SCUC)
  - Faster-than-real-time grid dynamic simulation and analysis
  - Production cost simulation
  - On-line stability analysis
- In-house computing infrastructure is not flexible to solve such intensive applications
- Computational complexity hinders market development



Courtesy of Ken Birman

Current State-of-Art of Cloud Computing for Grid Applications

- ISO-NE is at the forefront of cloud-hosted grid applications[1]
  - Platform for real-time PMU data collection, storage, and processing to achieve Wide Area Monitoring
  - HPC platform for large-scale simulations
    - Transmission Planning Studies (stability analysis, etc.)
    - Resource Adequacy studies
  - Software on the cloud: TARA, GE MARS, PSS/E, TSAT
- Majority of applications is focused on Grid Planning as opposed to Grid Operations



Total runtime for 7,090 TARA N-1-1 Planning Studies performed by ISO-NE

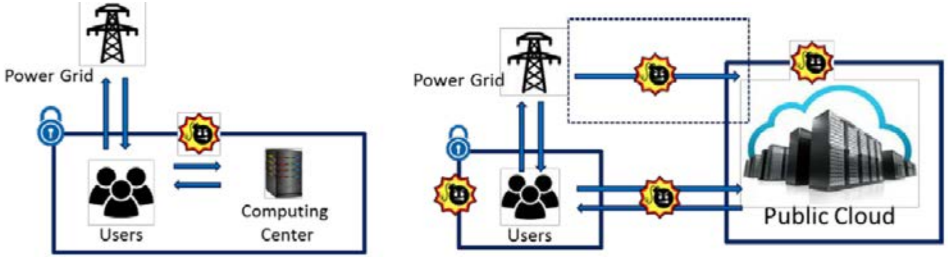
- Research and development of cloud-based operation models (e.g., SCUC, SCED) is needed

1 E. Litvinov, F. Ma, Q. Zhang, and X. Luo, “Cloud-based next-generation IT paradigm for the operations of future power systems,” in 2016 Power Systems Computation Conference (PSCC), June 2016, pp. 1–7.

Challenges in Cloud Computing for Grid Operations

Infrastructure Security

- Confidentiality and integrity of data-in-transit to and from cloud providers
- Outside attackers could compromise data in transmission
- Inside attackers could compromise a user or a cloud provider



Traditional Scenario vs. Cloud Scenario

Data Confidentiality

- Grid data must be kept confidential
- Grid data must remain unaltered

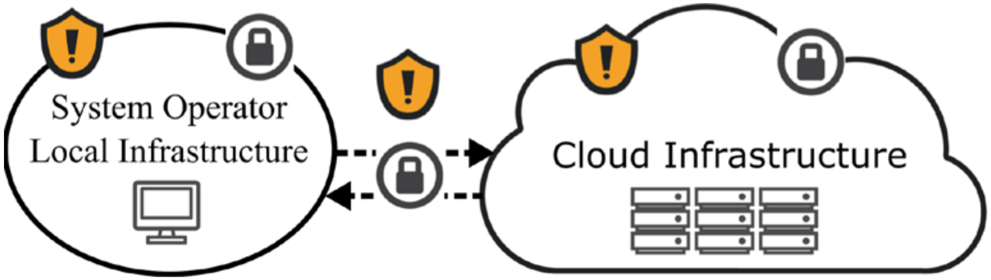
Time Criticality

- Power system applications require timeliness assurance
- Data must be time-consistent, requiring high-speed data synchronization

A Resilient and Trustworthy Cloud and Outsourcing Security Framework for Power Grid Applications

Objective

1. Design a comprehensive cloud-based framework for power grid applications
2. Model/quantify the security and time criticality requirements of grid applications
3. Deploy grid applications with different time criticality requirements in cloud
4. Model/quantify different types of cyberattacks against grid applications
5. Deploy security enhancements to cloud-based power grid applications.
6. Recommend cybersecurity improvements
7. Demonstrate best practices in cybersecurity for cloud-based grid applications



Performer:	**Argonne National Laboratory**
Partners:	**University at Buffalo, Illinois institute of Technology**

Project Schedule

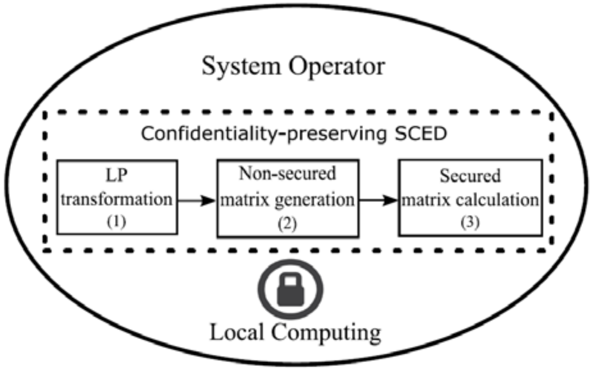
Started August 2016

Framework and white paper (Q2 2017)

Progress to Date

Major Accomplishments to-date

- Industry Advisory Board consisting of a diverse group of individuals applying cloud computing:
  - Xiaochuan Luo, ISO-NE
  - Alex Rudkevich, Newton Energy Group
  - Jianzhong Tong, PJM
  - Tobias Whitney, NERC

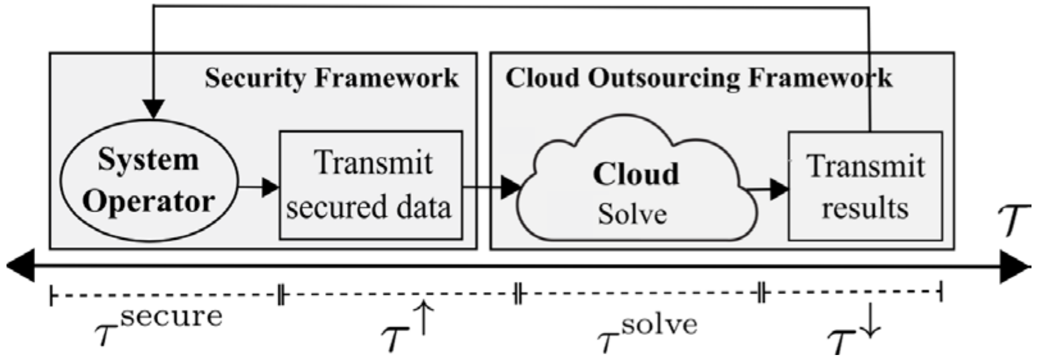


- Two papers under preparation
  - Security and Cloud Outsourcing Framework for Security-Constrained Economic Dispatch
  - Fast Encryption Scheme for Cloud-based SCUC Problem Outsourcing System

- Framework report and white paper being developed

Preliminary Technical Approach

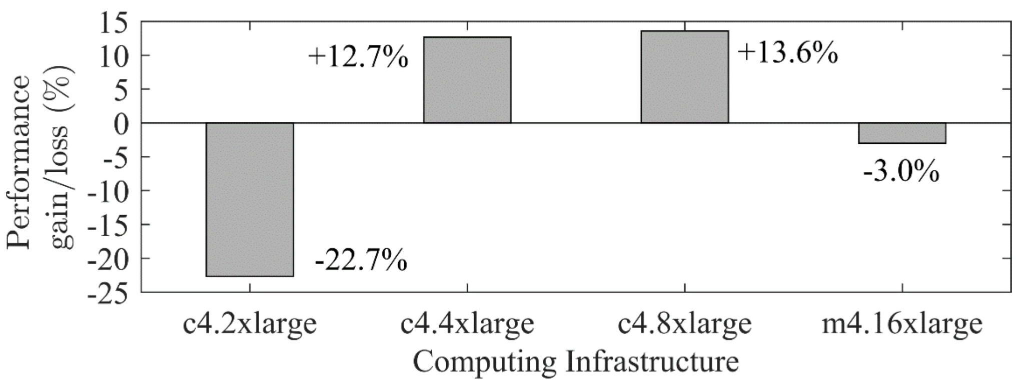
- Grid data must be kept confidential while in transmission and storage on the cloud
  - Various techniques (e.g., encryption, cryptography) will be explored
  - Mathematical models (SCED, SCUC) can be reconstructed to consider confidentiality
  - Leverage existing works in fields of Communications, Operational Research, among others
- Development of Confidentiality-Preserving SCED and SCUC models
  - Must conform to market rules, e.g., $\tau^{\text{solve}} + \tau^{\downarrow} \leq$ 5-min if market operates under 5-min



Security and Outsourcing Flow Chart

Results: Security-Constrained Economic Dispatch (SCED) on the Cloud

- In recent work, a confidentiality-preserving SCED was developed and simulated on
  - Argonne National Laboratory's (ANL) Blues HPC cluster
  - Four (4) Amazon EC2 instances
    - C4.2xlarge → less compute-optimized than ANL blues
    - C4.4xlarge and c4.8xlarge → more compute-optimized than ANL blues
    - M4.16xlarge → more memory-optimized than ANL blues
- A comparison of the **computational performance gain** against ANL Blues was performed



Conclusions

- Cloud Computing is a paradigm-shifting technology for the Power System
- Our project attempts to identify the benefits, challenges, and applicability to specific grid applications
- A comprehensive Cloud Security and Outsourcing Framework must:
  - Ensure infrastructure security, data confidentiality, and time criticality
  - Be economical against in-house infrastructures
  - Provide computational performance gains that justify the paradigm shift
  - Conform to market operating rules in practice today

Questions?

THANK YOU!

Jianhui Wang
Energy Systems Division
ARGONNE NATIONAL LABORATORY
9700 South Cass Avenue, Bldg. 362
Argonne, IL 60439
Tel: +1 630-252-1474
jianhui.wang@ANL.gov

NARUC Staff Subcommittee Meeting
Cloud Offerings Architecture

Joe Joyce, Cloud Solution Architect
Microsoft Corporation

Hyper-scale cloud

200+ cloud services,
100+ datacenters,
$15B+ infrastructure investment

1+ billion customers,
20+ million businesses,
90+ countries worldwide

500+ million
users in Azure Active Directory
Microsoft Azure

3.5 million
active users
Microsoft Dynamics CRM Online

50+ billion
minutes of connections handled each month
skype

7+ billion
worldwide queries each month[3]
bing

1.2+ billion
worldwide users
Office 365

48+ million
members in 57 countries
XBOX

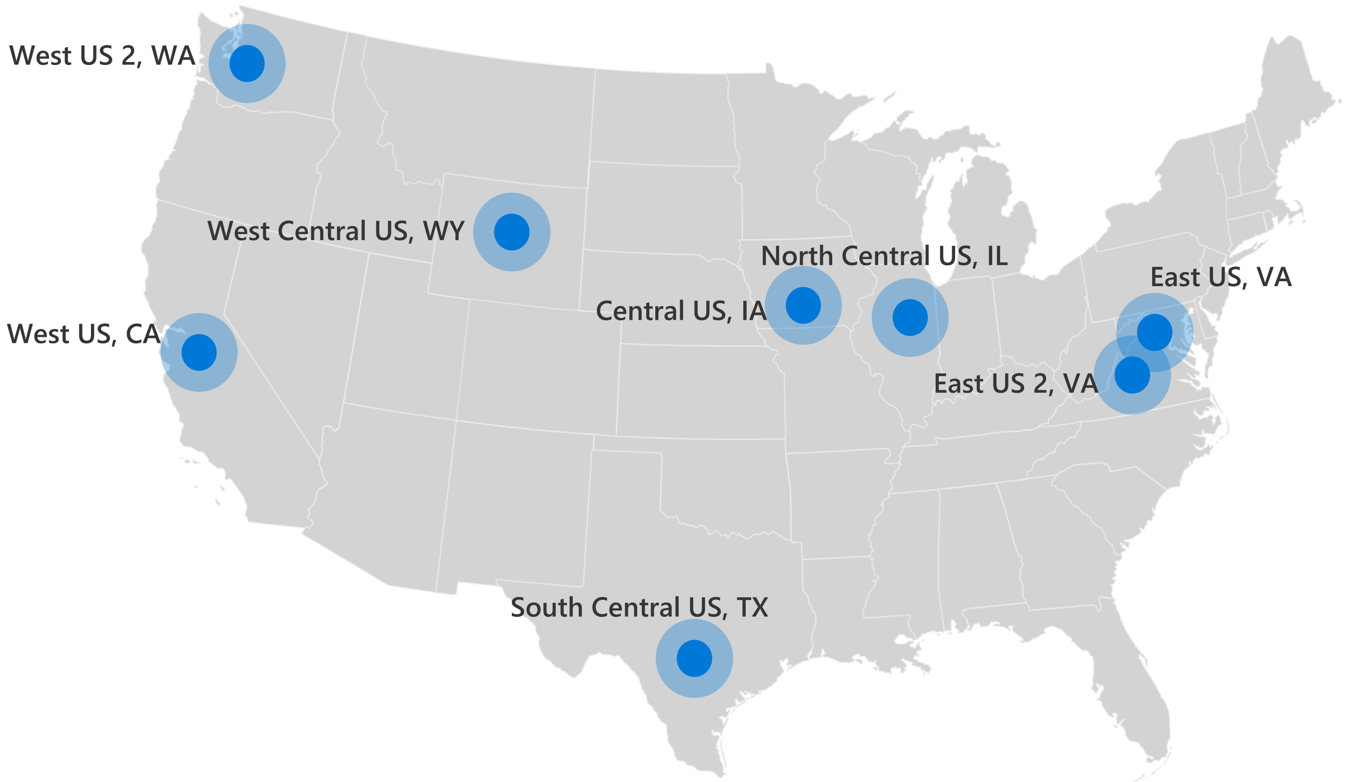
450+ million
unique users each month
msn

38

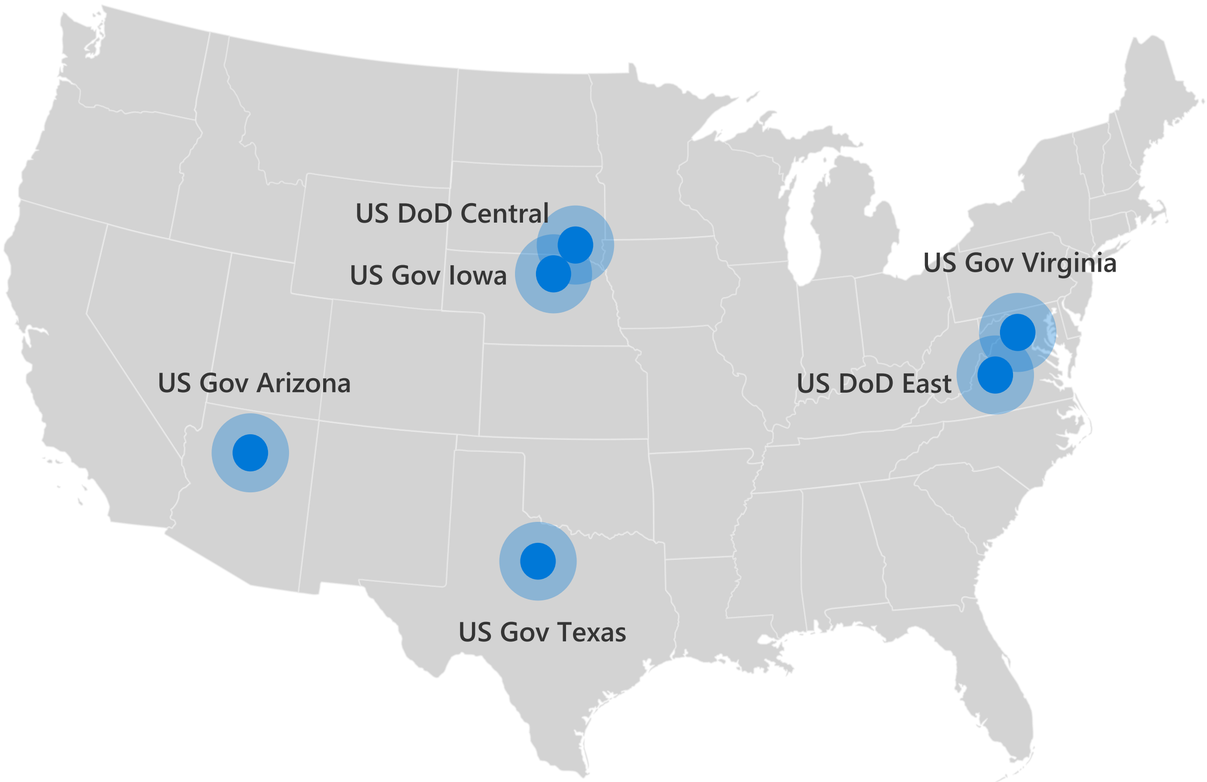
Azure regions

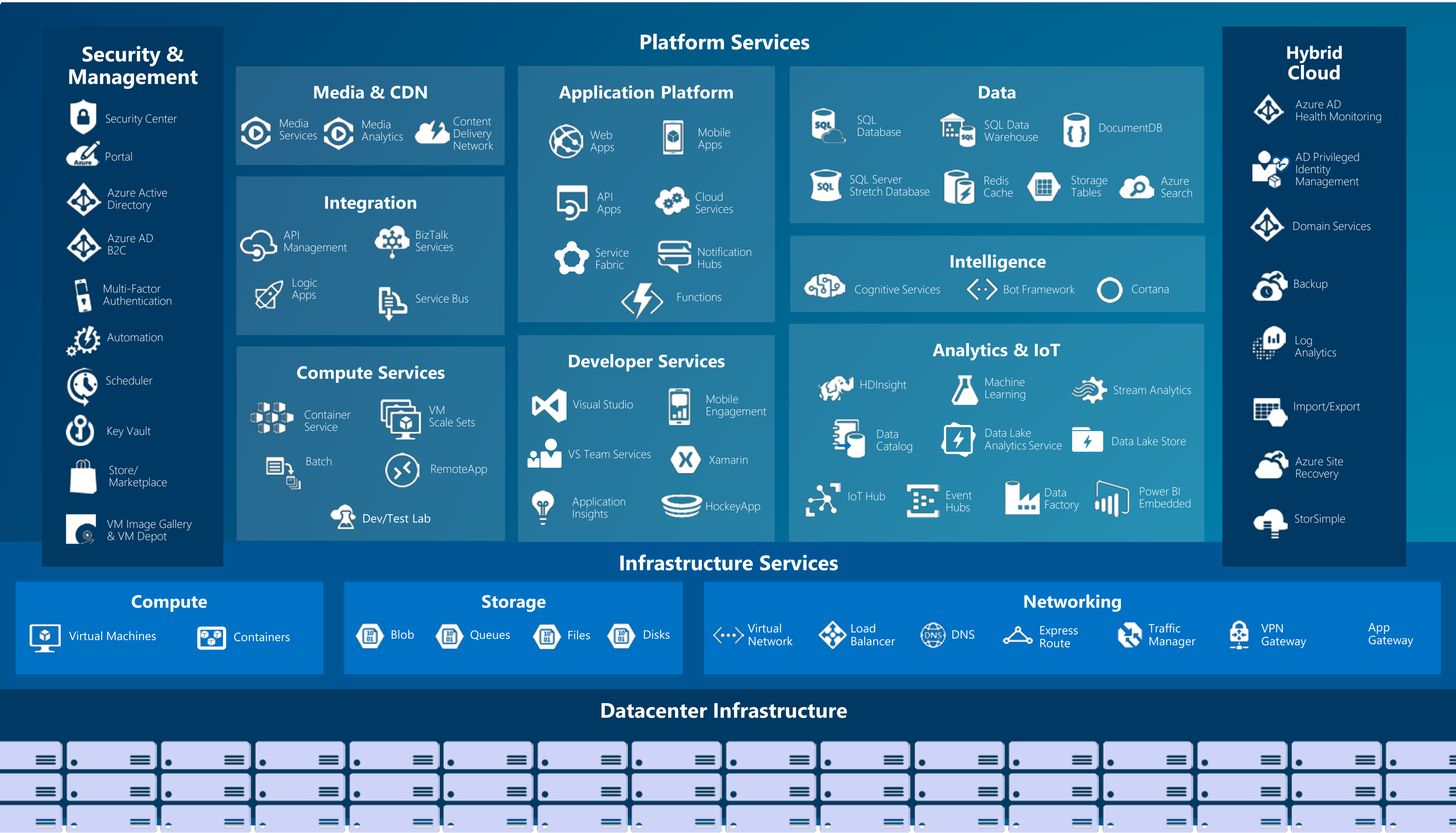
https://azure.microsoft.com/en-us/regions/

Azure Public cloud US locations

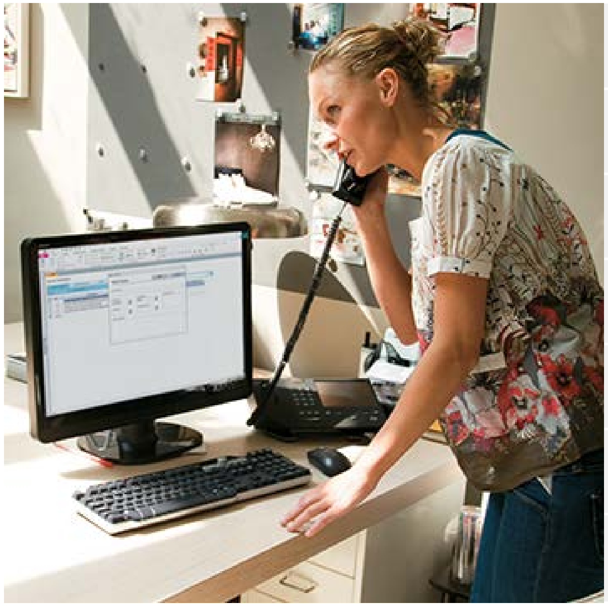


Azure Government locations



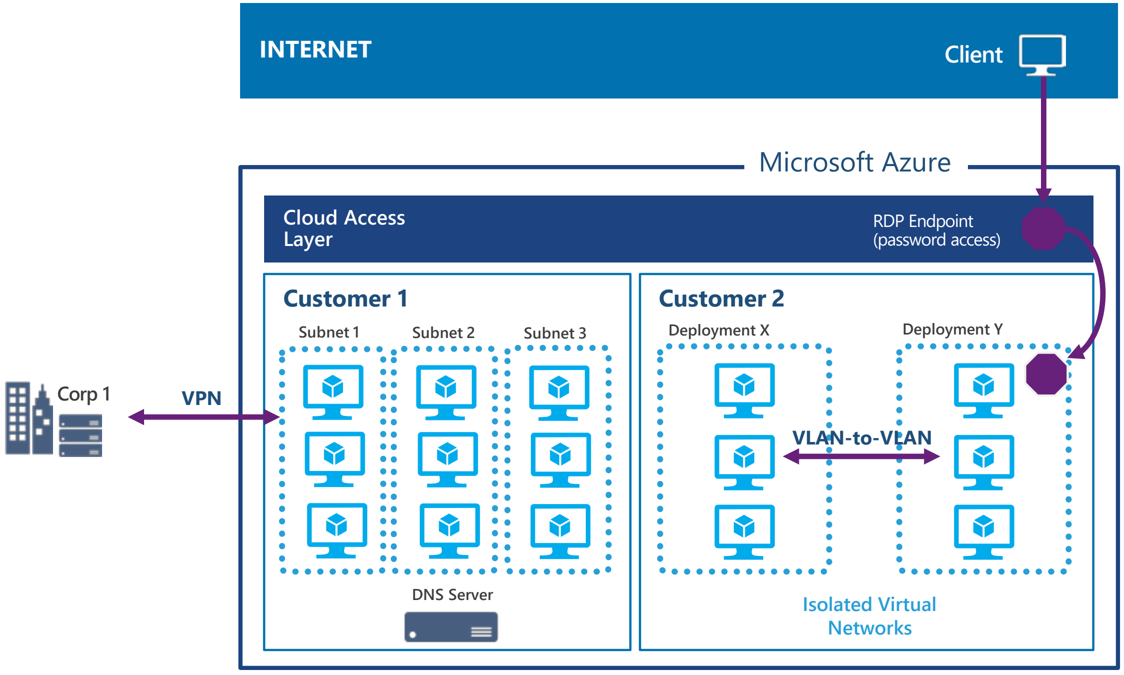

Security & Management
Security Center
Portal
Azure Active Directory
Azure AD B2C
Multi-Factor Authentication
Automation
Scheduler
Key Vault
Store/ Marketplace
VM Image Gallery & VM Depot
Platform Services
Media & CDN
Media Services
Media Analytics
Content Delivery Network
Integration
API Management
BizTalk Services
Logic Apps
Service Bus
Compute Services
Container Service
VM Scale Sets
Batch
RemoteApp
Dev/Test Lab
Application Platform
Web Apps
Mobile Apps
API Apps
Cloud Services
Service Fabric
Notification Hubs
Functions
Developer Services
Visual Studio
Mobile Engagement
VS Team Services
Xamarin
Application Insights
HockeyApp
Data
SQL Database
SQL Data Warehouse
DocumentDB
SQL Server Stretch Database
Redis Cache
Storage Tables
Azure Search
Intelligence
Cognitive Services
Bot Framework
Cortana
Analytics & IoT
HDInsight
Machine Learning
Stream Analytics
Data Catalog
Data Lake Analytics Service
Data Lake Store
IoT Hub
Event Hubs
Data Factory
Power BI Embedded
Hybrid Cloud
Azure AD Health Monitoring
AD Privileged Identity Management
Domain Services
Backup
Log Analytics
Import/Export
Azure Site Recovery
StorSimple
Infrastructure Services
Compute
Virtual Machines
Containers
Storage
Blob
Queues
Files
Disks
Networking
Virtual Network
Load Balancer
DNS
Express Route
Traffic Manager
VPN Gateway
App Gateway
Datacenter Infrastructure

Infrastructure protection



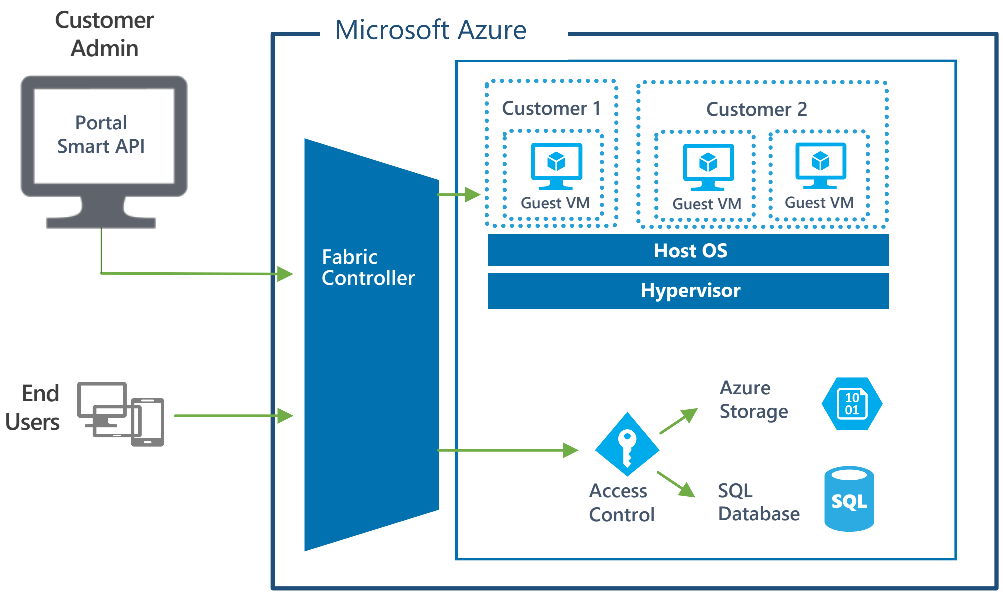
24 hour monitored physical security
System monitoring and logging
Patch management
Anti-Virus/Anti-Malware protection
Intrusion detection/DDoS
Penetration testing, vulnerability scanning
Security incidents and breach notification

Network isolation



- ✓ Provides logical isolation while enabling customer control
- ✓ Private IP addresses are isolated from other customers
- ✓ Firewalls limiting traffic to VMs
- ✓ Encrypted communications

Data segregation



- ✓ Storage is allocated sparsely
- ✓ Storage Access Key controls all access to storage account
- ✓ SQL Azure isolates separate account database
- ✓ Customer A cannot read active or deleted data belonging to Customer B

Data protection

Data segregation

Logical isolation segregates each customer's data from that of others.

At-rest data protection

Customers can implement a range of encryption options for virtual machines and storage.

In-transit data protection

Industry-standard protocols encrypt data in transit to/from outside components, as well as data in transit internally by default.

Encryption

Data encryption in storage or in transit can be deployed by the customer to align with best practices for ensuring confidentiality and integrity of data.

Data redundancy

Customers have multiple options for replicating data, including number of copies and number and location of replication datacenters.

Data destruction

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

Question (1): Utilities are embracing cloud technology (True or False)

Zpryme/Oracle Utilities Feb 2016 Study: *On Cloud Now: Cloud Technologies are Here for Utilities*
(surveyed 100 North American electric, water and gas utility executives)

"With 45% using the Cloud in some form today and another 52% planning to use the Cloud—nearly 97% of them told us they have become involved with Cloud technologies, or applications and computing resources delivered as services over a network connection instead of through in-house resources at a utility."

Ques. (2): State Regulators support utility use of cloud services (True or False)

Zpryme/Oracle Utilities Feb 2017 Study: *Clearing a Path to the Cloud: U.S. Regulator Perspectives on Cloud Technologies* (surveyed 76 U.S. regulatory staff and commissioners)

The cloud is an important technology trend. (83%)
The cloud will be critical to a utility's future success (67%)
We have a specific and comprehensive strategy for cloud in utilities. (33%)

"When asked what role they should play in determining whether utilities use on-premises or cloud technologies, **79% of respondents—or nearly 4 out of every 5—felt that regulators should play at least some role in determining whether or not utilities use cloud technologies."**

Question (3): NARUC supports utility use of Cloud services (True or False)

Resolution Encouraging State Utility Commissions to Consider Improving the Regulatory Treatment of Cloud Computing Arrangements (2016 Annual Meeting)

To thrive in the future, utilities may need to modernize and transform their business operations. A key element of this may be access to state-of-the-art commercial cloud computing services, which is increasingly delivered via a “cloud-based” or “software-as-a-service” model; *and*

WHEREAS, The various functionalities provided by commercial cloud computing services may help utilities fully realize the economic, social, and environmental value of the smart gas and electric grid;…

RESOLVED, That NARUC encourages State regulators to consider whether cloud computing and on-premise solutions should receive similar regulatory accounting treatment, in that both would be eligible to earn a rate of return and would be paid for out of a utility’s capital budget.

NARUC

Winter Committee Meetings

Staff Subcommittees on Electricity & Electric Reliability