NIST MULTI-CLOUD SECURITY PUBLIC WORKING GROUP (MCSPWG)

Meeting #1

January 31, 2022, 3PM ET

National Institute of Standards and Technology
U.S. Department of Commerce

Agenda

1. Welcome
2. Introduction (5-10 mins)
   a. Co-Chairs
   b. Members
3. MCSPWG (10 mins)
   a. PWG Goal and structure
   b. Charter
   c. Deliverables
4. Proposed Research Directions (3 x 10 min)
   a. Assessment and authorization (e.g. SP 800-37)
   b. ZTA principles (e.g. SP 800-207)
   c. Information Exchange principles (e.g. SP 800-47)
5. Open floor discussion & work planning
   a. Teams
   b. Team leaders
   c. Team members
6. Meeting adjourn
7. Next meeting: February 14, 2022, 3PM ET

MCSPWG CO-CHAIRS

NED GOREN

IT Specialist

NIST

CHRIS HUGHES

Co-Founder and CISO

Aquia Inc.

JOSEPH ALLEN

Enterprise Cloud Architect

Adept Consulting

ANNIE SOKOL

IT Specialist

NIST

https://csrc.nist.gov/projects/mcspwg
https://csrc.nist.gov/Projects/mcspwg/leadership

MCSPWG Charter

The purpose of the Multi-Cloud Security Public Working Group (MCSPWG) is to provide a **forum** in which participants from the public, including private industry, the public sector, academia, and civil society discuss the security and privacy risks and research guidance and best practices of implementing and using multi-cloud services.

The NIST MCSPWG is a subsidiary of the NIST Cloud Security Public Working Group and will focus the research on particular cloud computing architectures referred to as multi-cloud solutions, that connect services from more than one cloud service providers. The work will aim to:

- identify the **challenges** of implementing secure multi-cloud systems and
- develop **guidance and best practice** for mitigating the identified challenges.

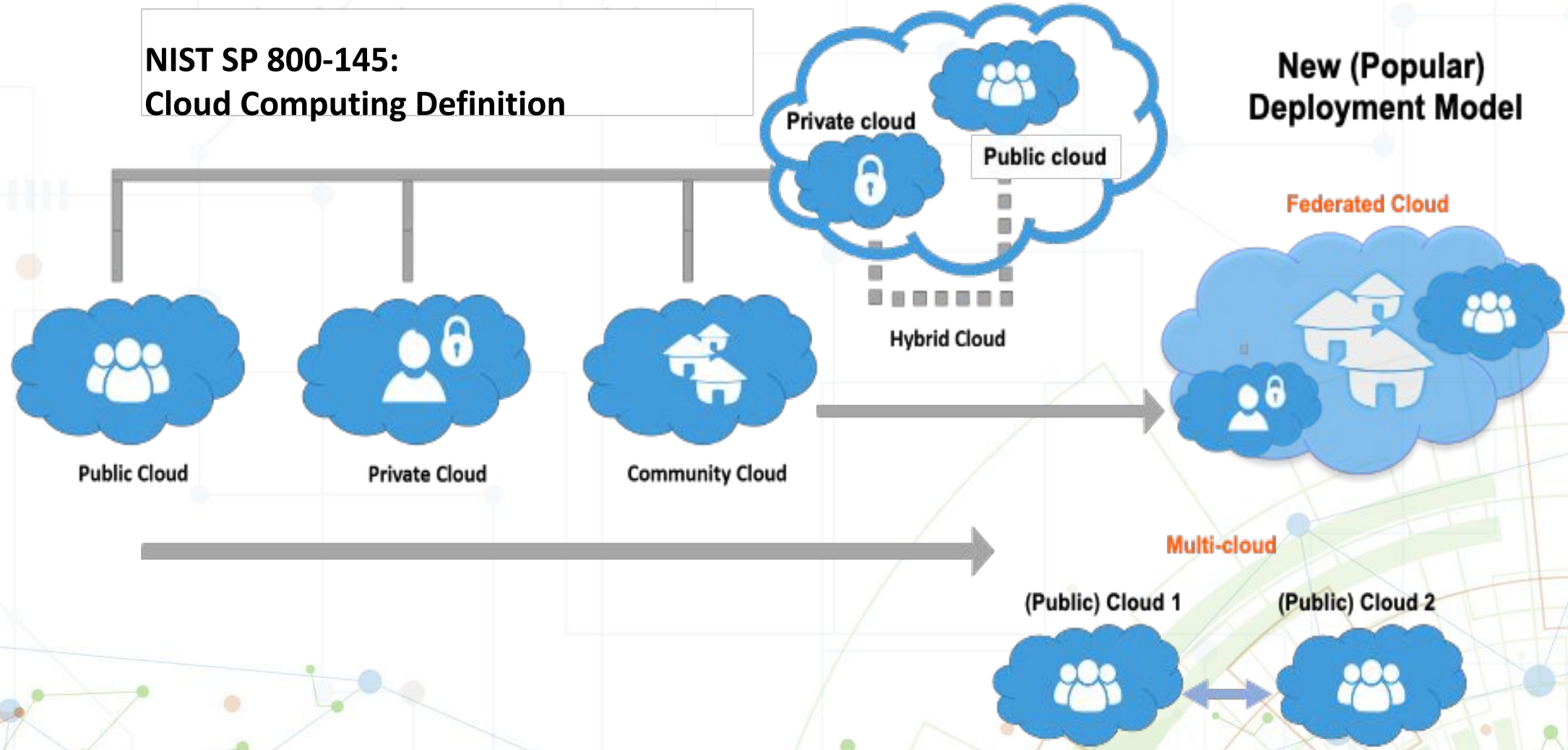
MCSPWG Structure, Charter & Deliverables

- MCSPWG is led by Co-Chairs
- Project Team Lead(s) to lead on identified topics and report to the PWG.
- MCSPWG will not be providing any formal recommendations to the federal government.
- All participants are to subscribe to the mailing list (see overview https://csrc.nist.gov/projects/mcspwg) to receive MCSPWG official communication.
- MCSPWG meets every two weeks on Monday at 3PM ET for an hour.
- MCSPWG Co-Chairs are to provide meeting agendas and minutes (see MCSPWG Charter https://csrc.nist.gov/Projects/mcspwg/mcspw-charter)

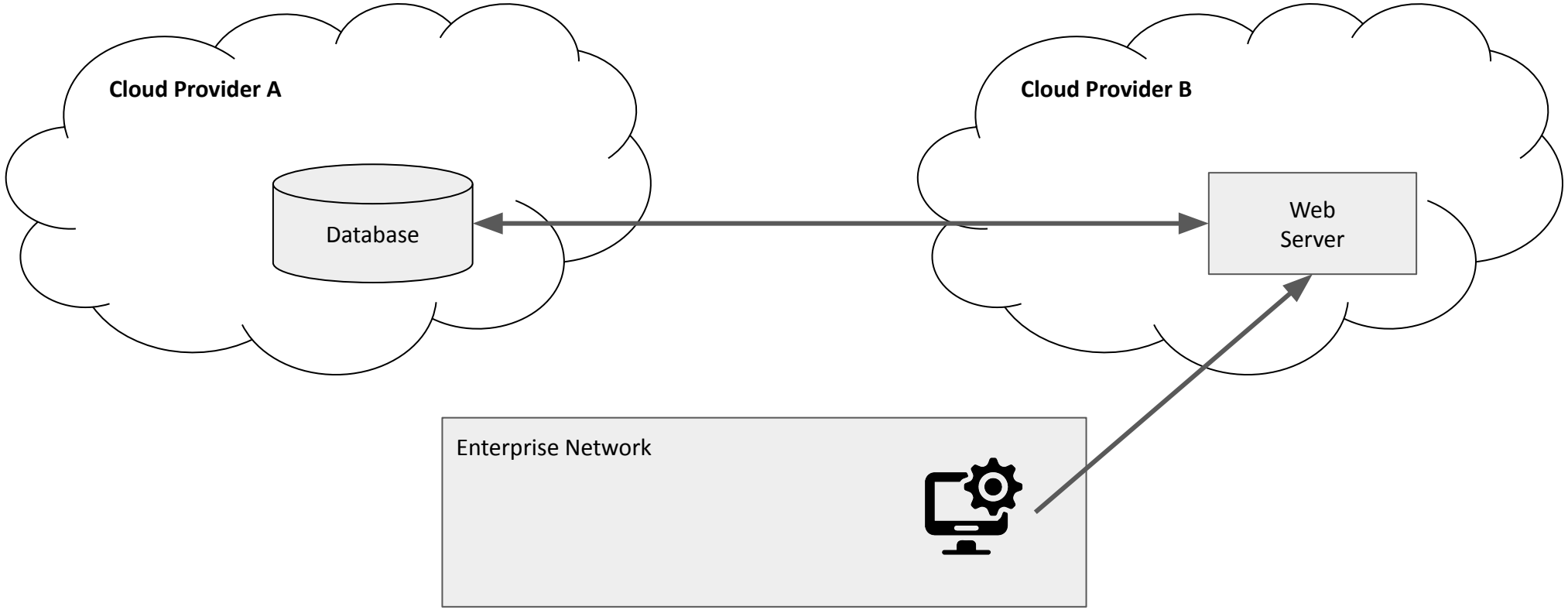
Proposed Research Directions

Discussion of initial use cases and focus areas

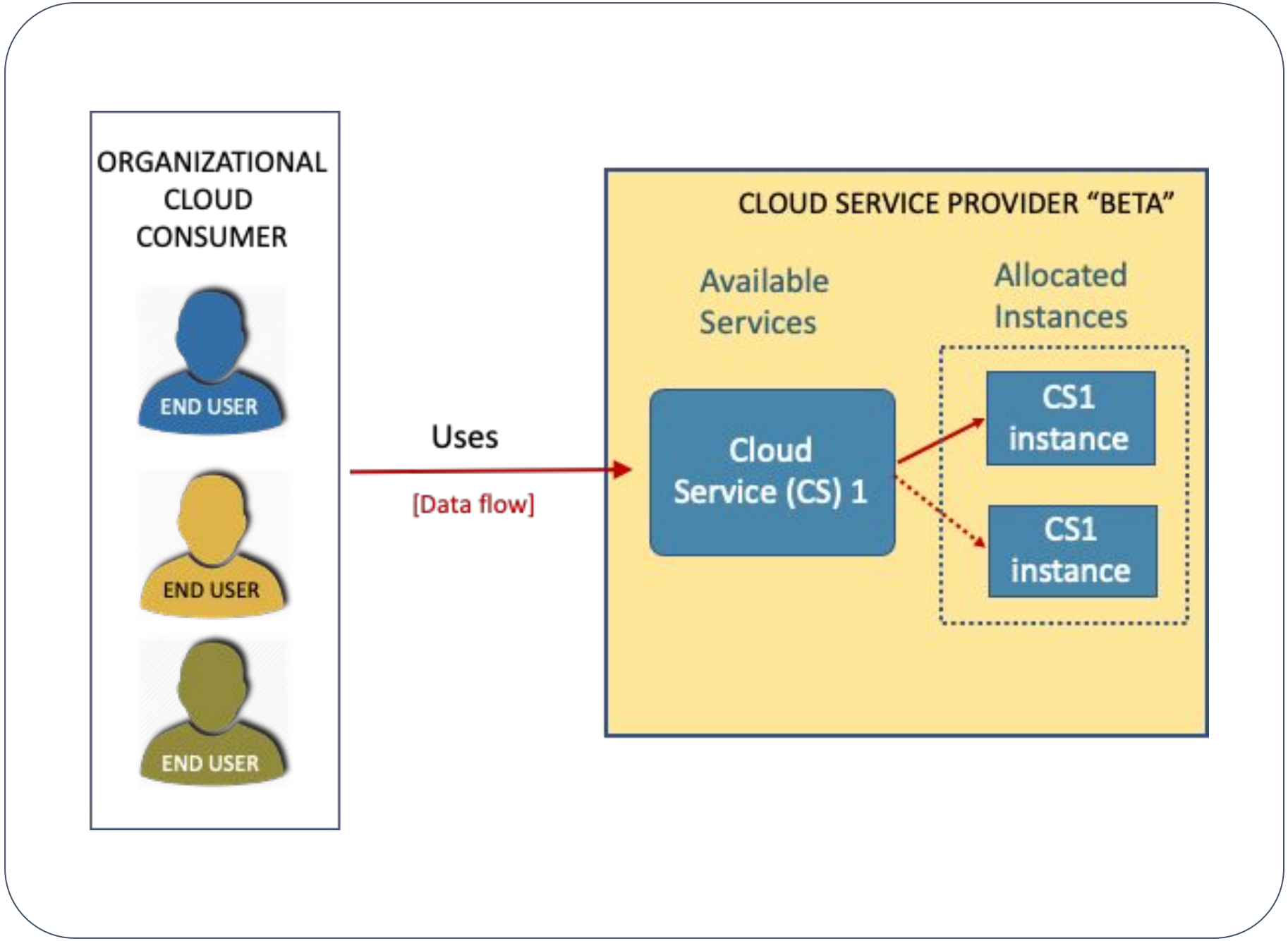
NIST SP 800-145:
Cloud Computing Definition



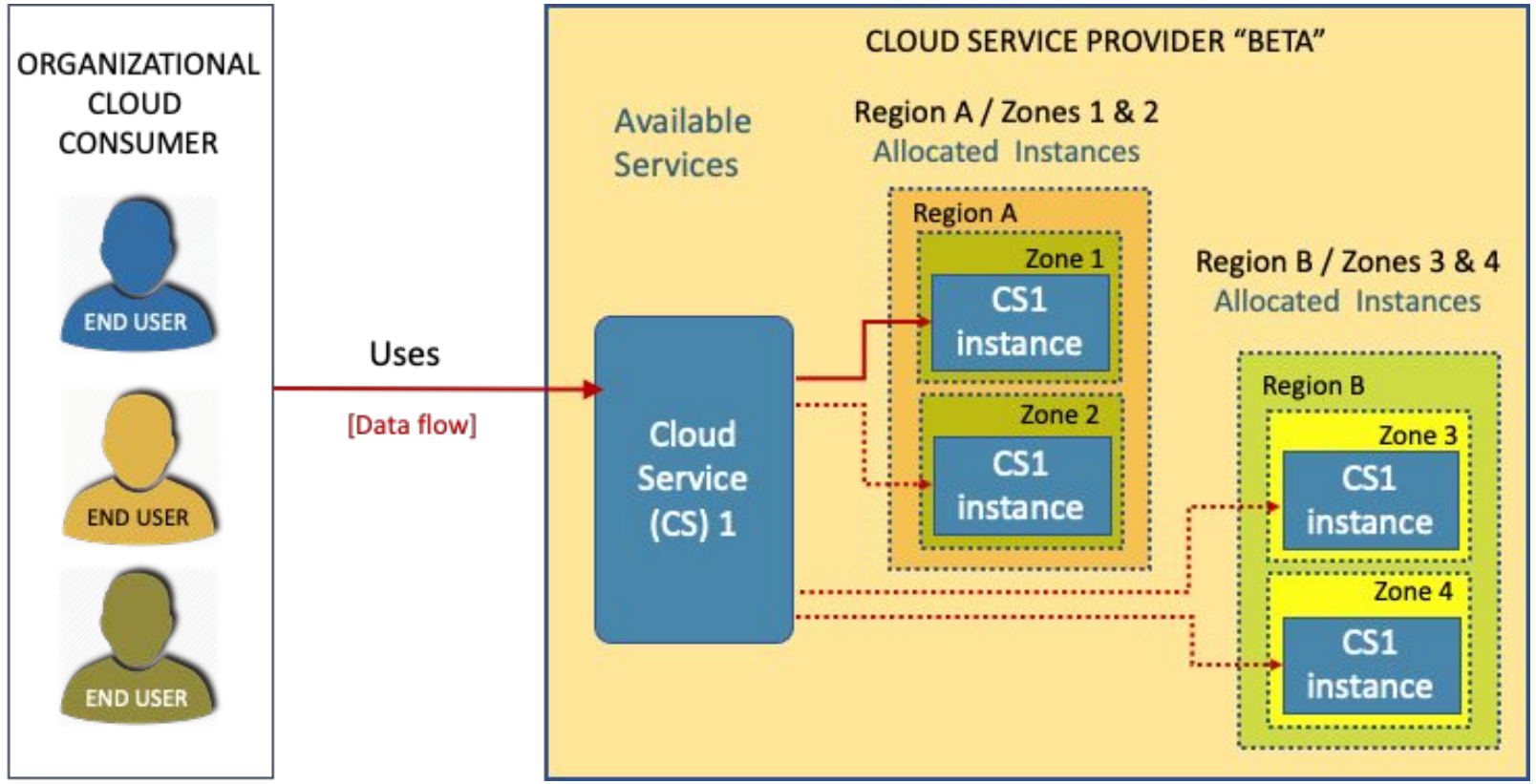
Multi-cloud/Cloud-to-Cloud Enterprise



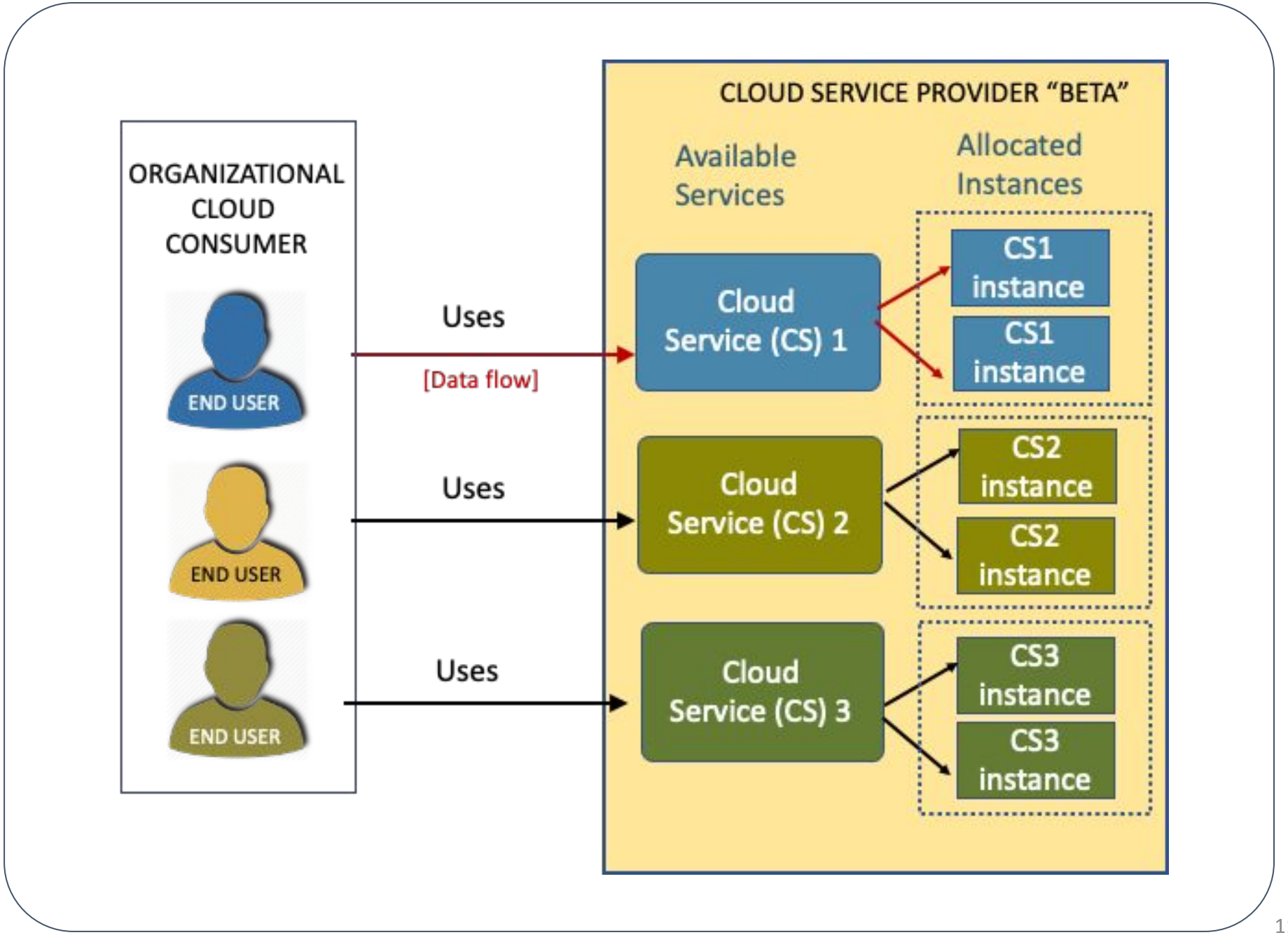
Public or Private Model



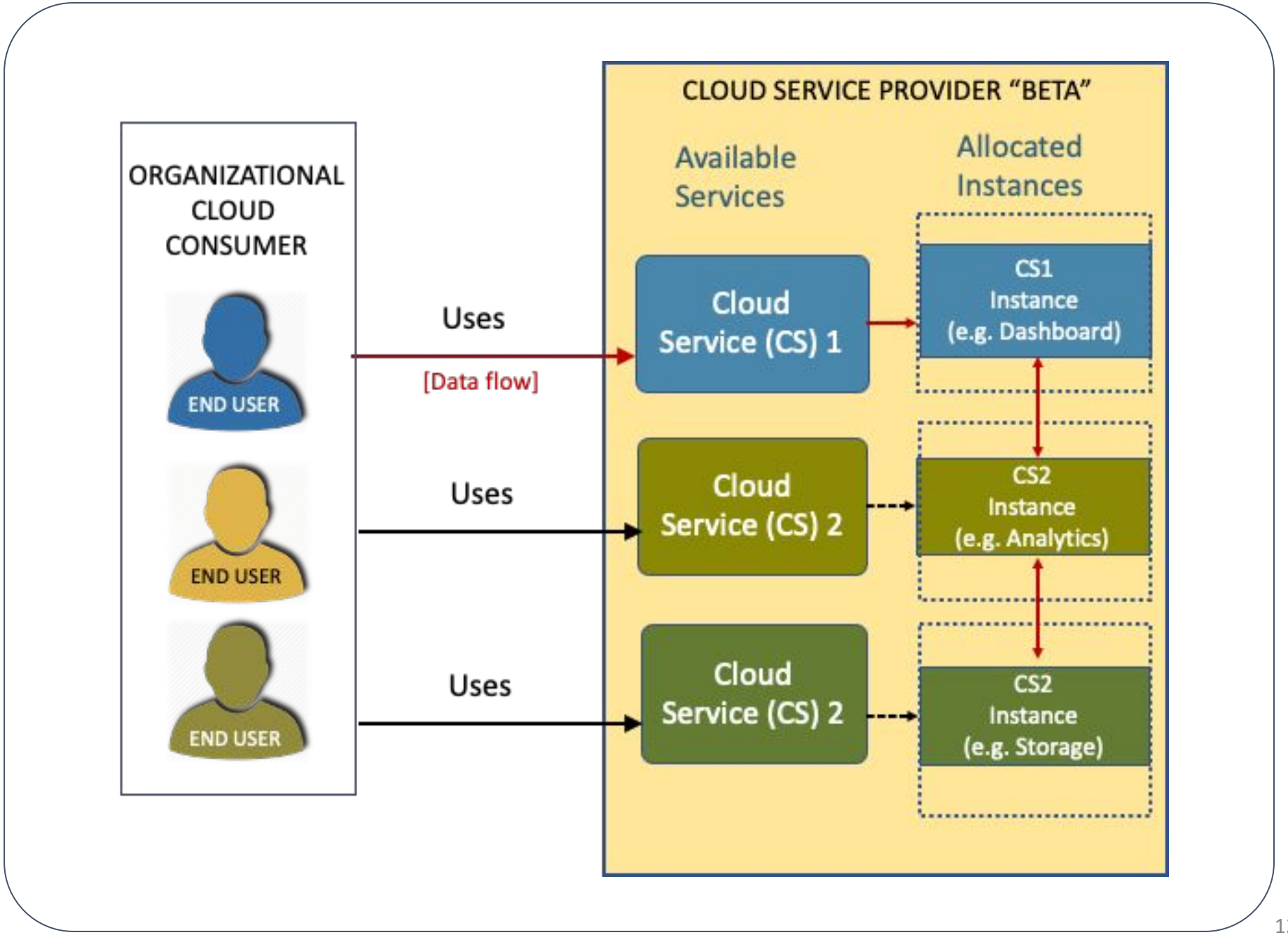
Public or Private Model



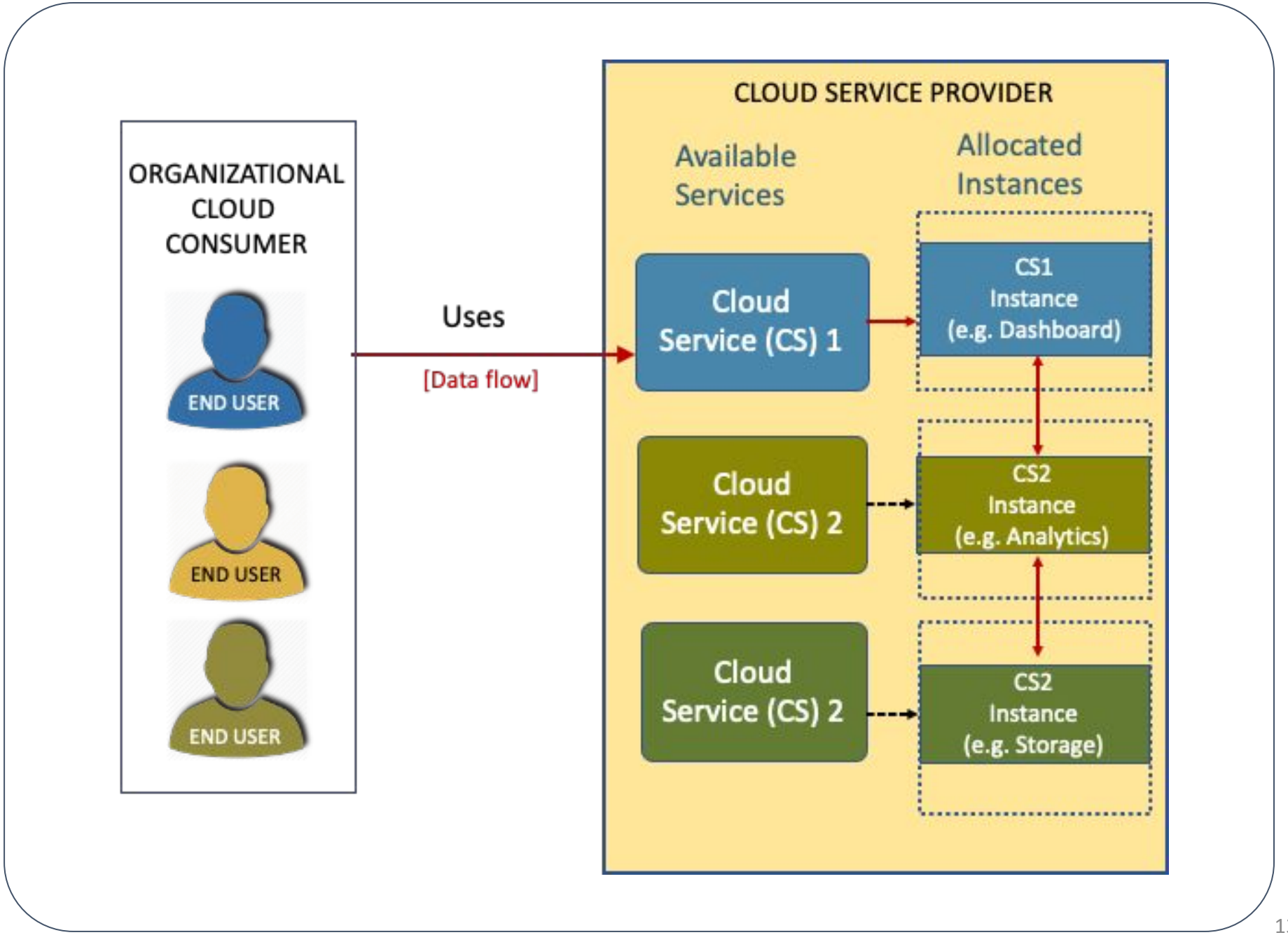
Public or Private Model



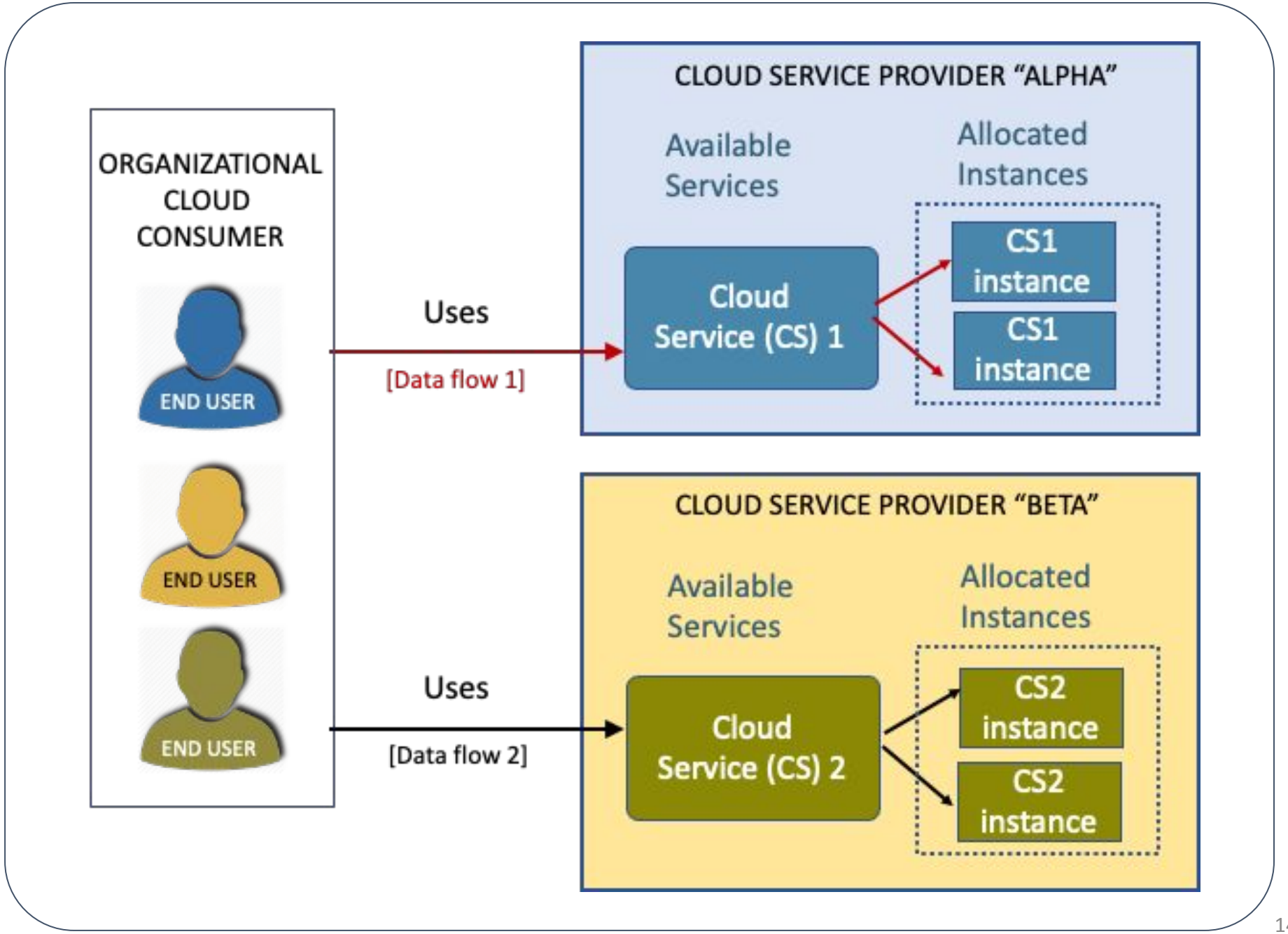
Public or Private Model



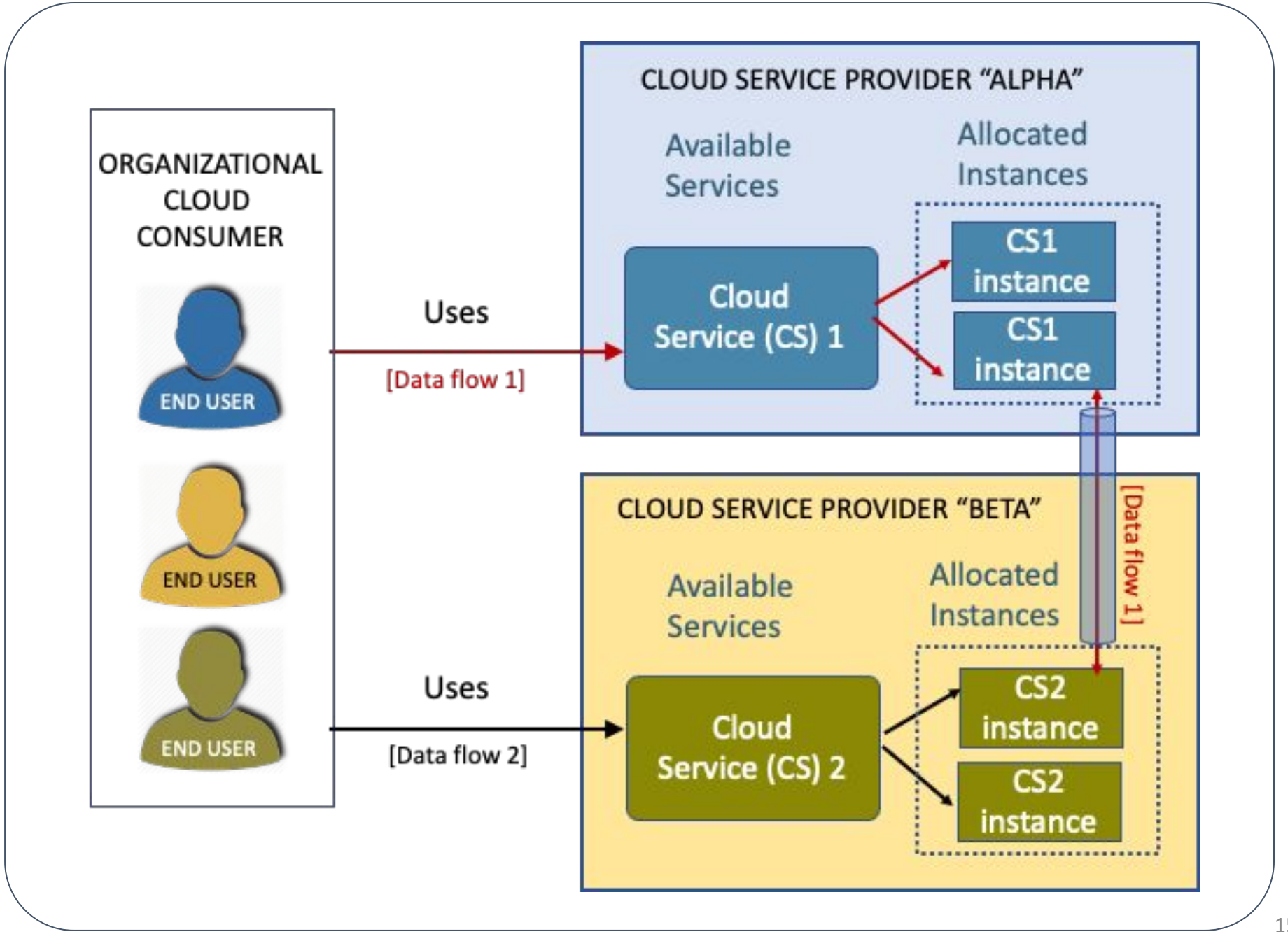
Public or Private Model



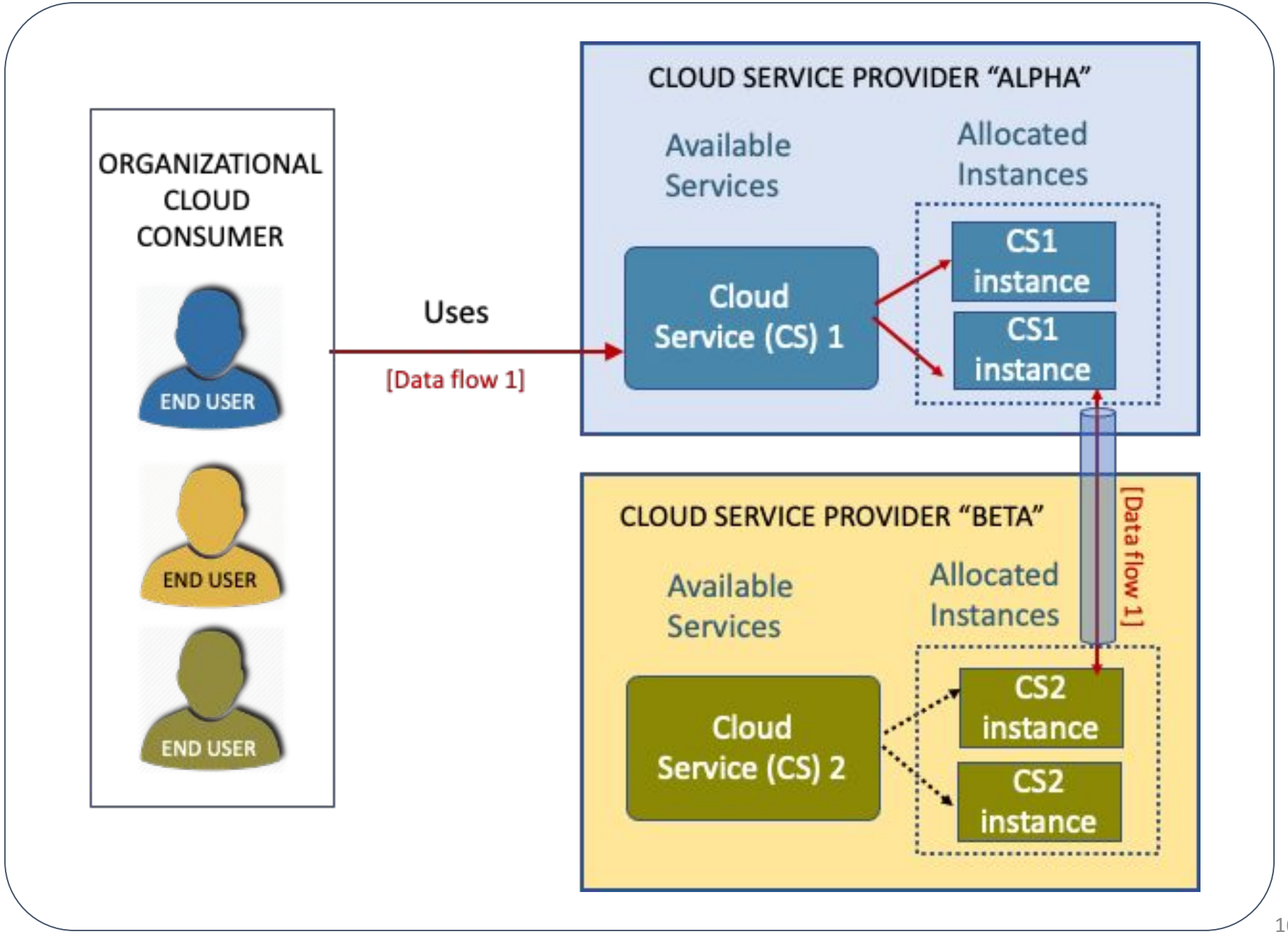
Public or Private Model



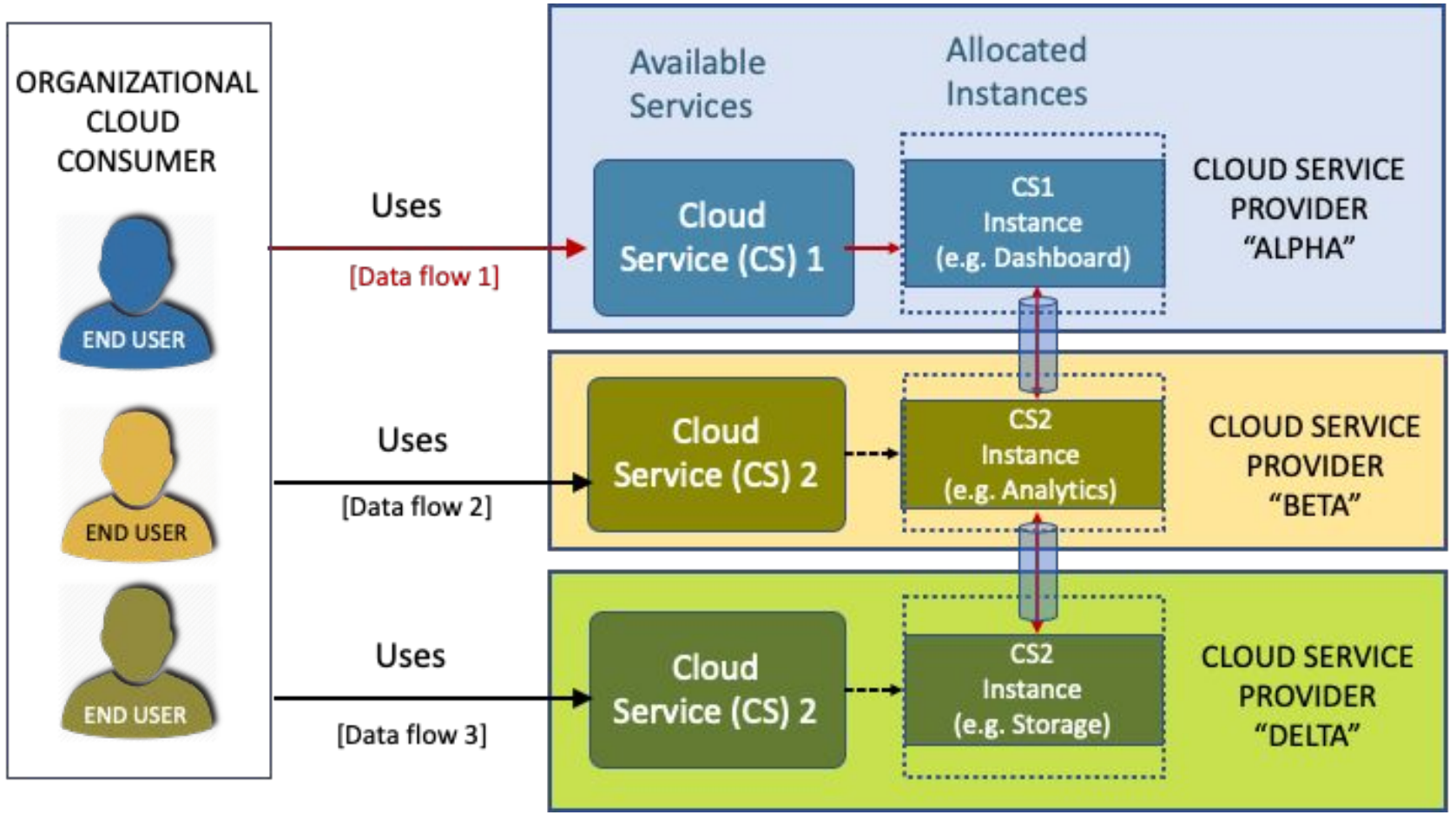
Multi-cloud Model



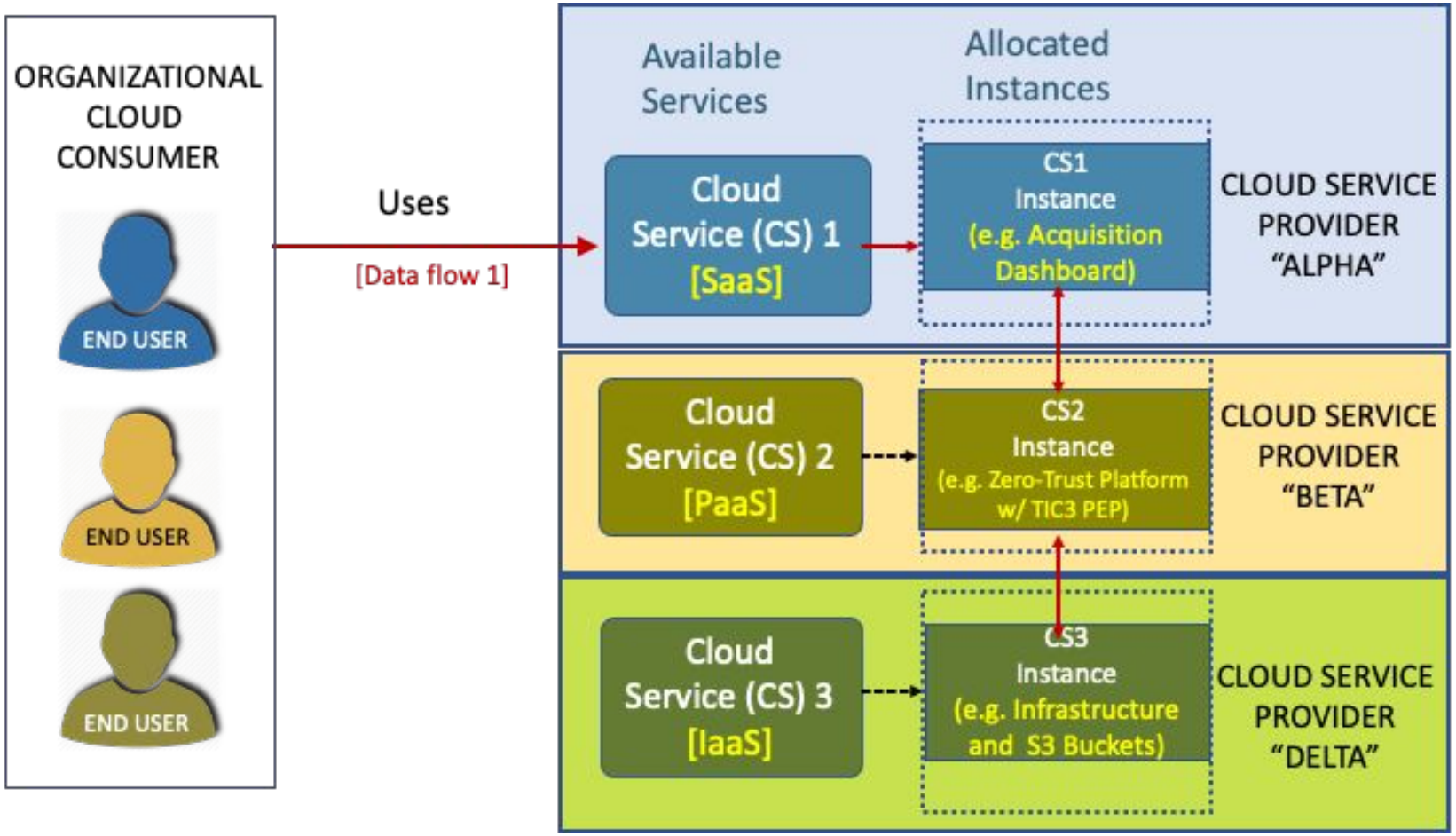
Multi-cloud Model



Multi-cloud Model



NOT Multi-cloud Model



logically stacked layers, inherited controls

Zero Trust Architecture

> Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated. Zero trust architecture is an end-to-end approach to enterprise resource and data security that encompasses identity (person and nonperson entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure.
>
> —NIST 800-207 *Zero Trust Architecture*

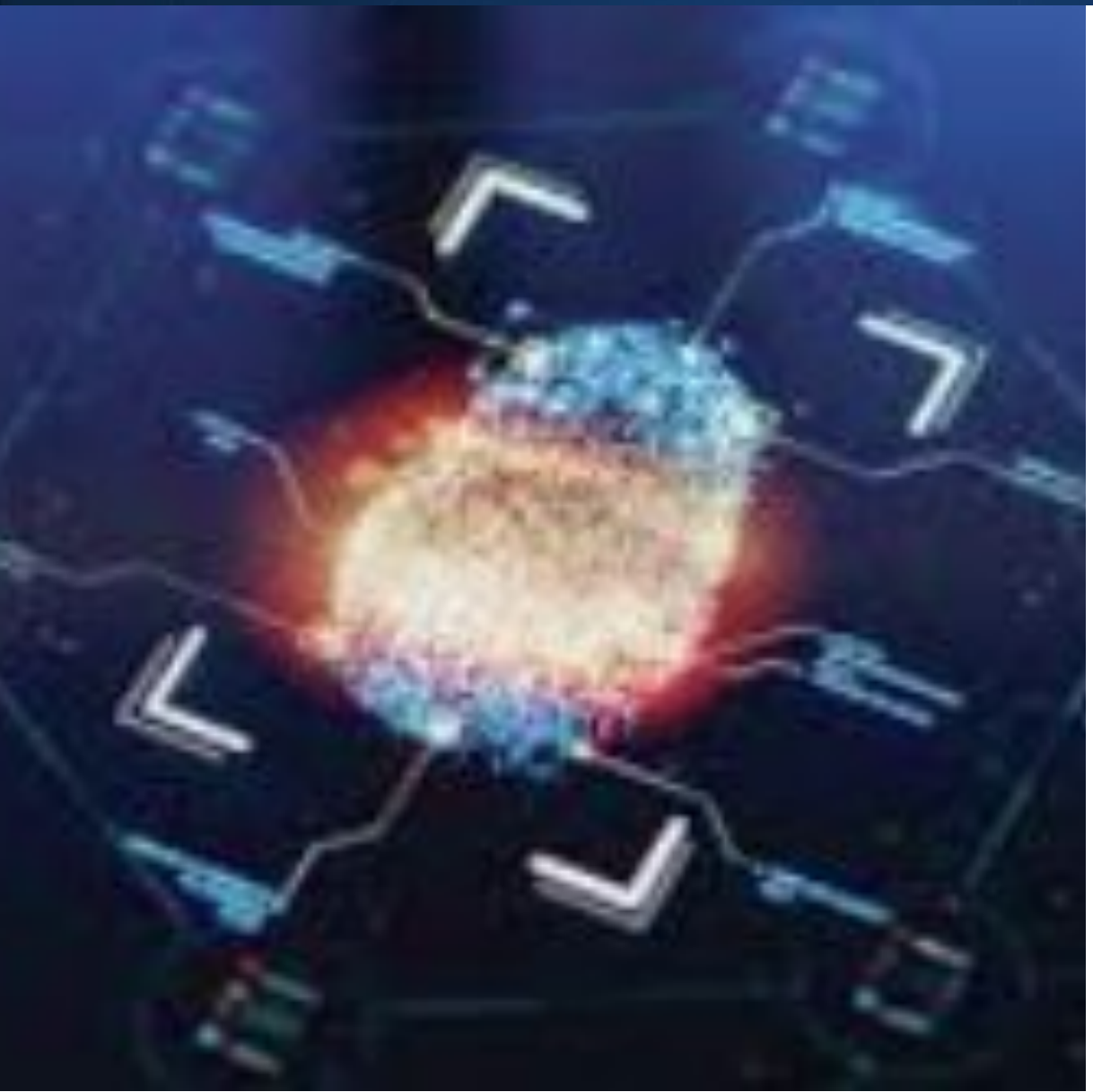
ZTA Introduction

- **History**
  - Concept was present before the phrase “zero trust” was coined
  - Affects FISMA, RMF, FICAM, TIC, CDM and more
- **Overview**
  - Based on zero trust principles
  - Designed to prevent data breaches
  - Limits internal lateral movement
  - Assumes a hybrid zero trust/perimeter-based mode
  - Encourages continued investment in IT modernization
  - Balances existing cybersecurity policies and guidance
    - Identity and access management
    - Continuous monitoring
    - Best practices
  - Uses a managed risk approach

ZTA Basics

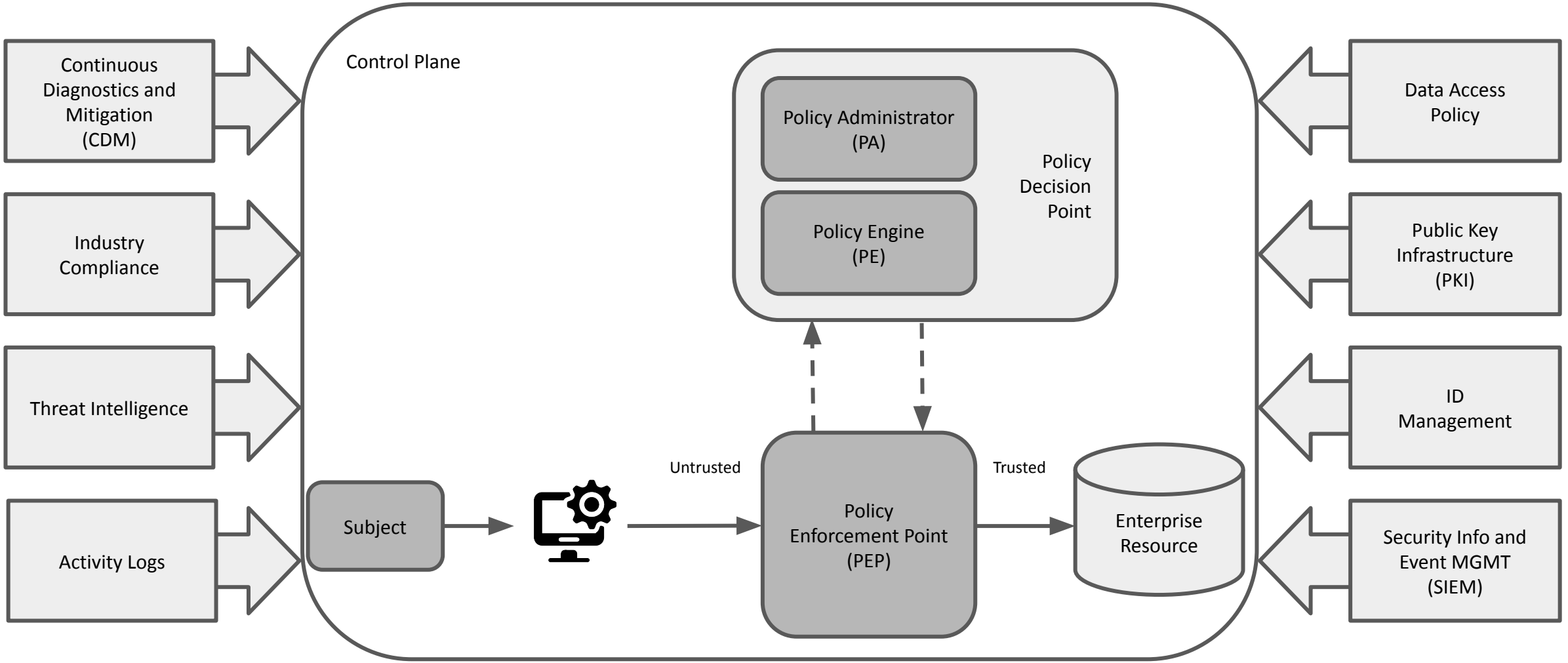
- **Tents of Zero Trust**
  - All data sources and computing services are considered resources
  - All communication is secured regardless of network location
  - Access to individual enterprise resources is granted on a per-session basis
  - Access to resources is determined by dynamic policy
  - The enterprise monitors and measures the integrity and security posture of all owned and associated asset
  - All resource authentication and authorization are dynamic and strictly enforced before access is allowed
  - The enterprise collects information and uses it to improve its security posture

ZTA Basics



- **A Zero Trust View of a Network**
  - No resource is inherently trusted
  - The entire enterprise private network is not considered an implicit trust zone
  - Devices on the network may not be owned or configurable by the enterprise
  - Not all enterprise resources are on enterprise-owned infrastructure
  - Remote enterprise subjects and assets cannot fully trust their local network connection
  - Assets and workflows should have consistent security

Core Zero Trust Logical Components



Logical Components of ZTA

- **Variations of Zero Trust Architecture**
  - Enhanced Identity Governance
  - Micro-Segmentation
  - Network Infrastructure and Software Defined Parameters
- **Deployed Variations of the Abstract Architecture**
  - Device Agent/Gateway-Based Deployment
  - Enclave-Based Deployment
  - Resource Portal-Based Deployment
  - Device Application Sandboxing
- **Trust Algorithm**
  - Trust Algorithm Variations
  - Network/Environment Components
  - Network Requirements to Support ZTA

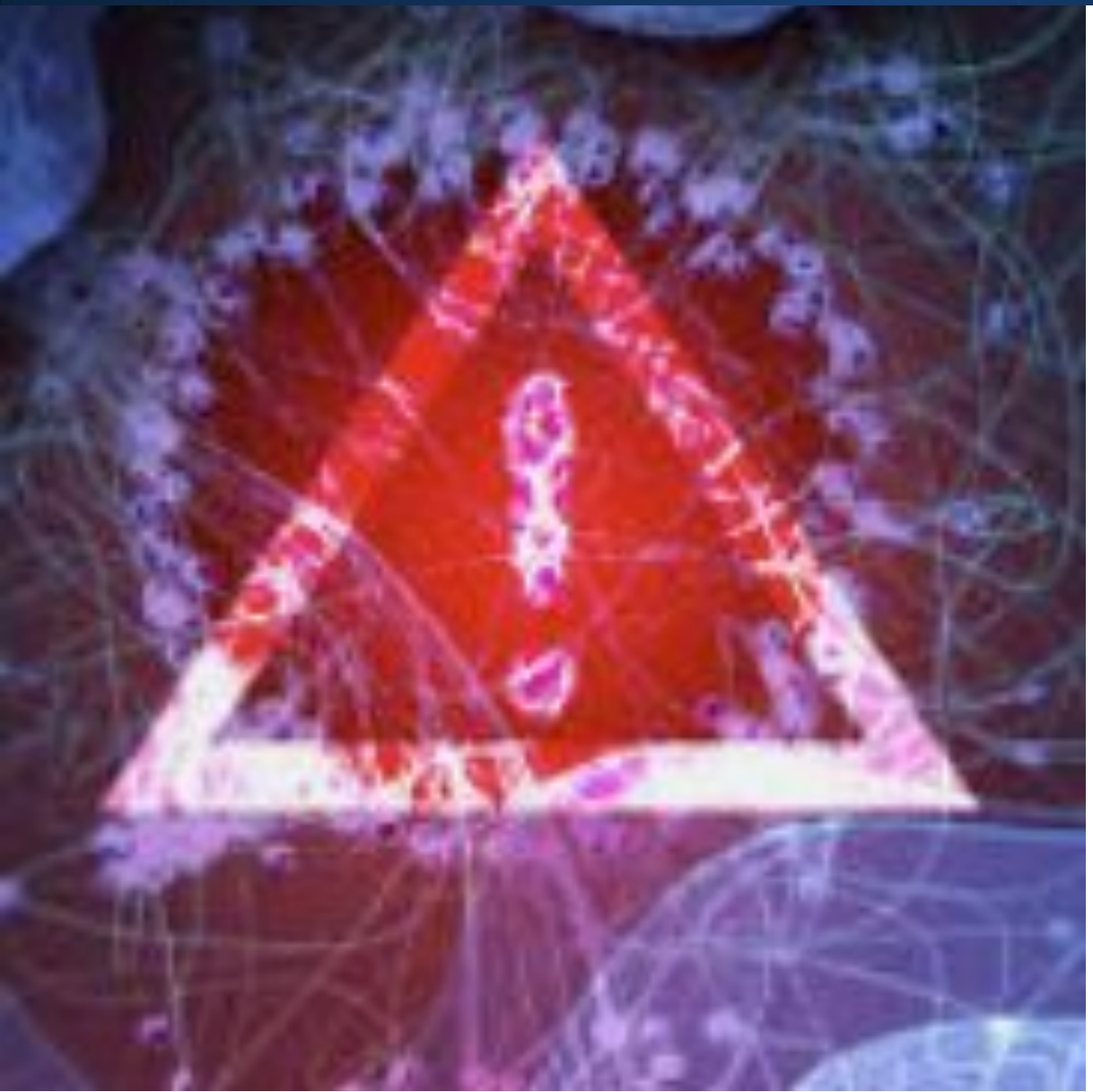
Deployment Scenarios/Use Cases

- Enterprise with Satellite Facilities
- Multi-cloud/Cloud-to-Cloud Enterprise*
- Enterprise with Contracted Services and/or Nonemployee Access
- Collaboration Across Enterprise Boundaries
- Enterprise with Public- or Customer-Facing Services

Multi-cloud/Cloud-to-Cloud Enterprise

- Relying on the enterprise perimeter for security becomes a liability
- There should be no difference between:
  - Enterprise-owned and -operated network infrastructure
  - Service provider-owned and -operated infrastructure
- Place policy enforcement points (PEP) at the access points of each application/service and data source
- Policy engine (PE) and Policy administrator (PA) may be services located in either cloud or even on a third cloud provider

Threats Associated with ZTA



- Subversion of ZTA Decision Process
- Denial-of-Service or Network Disruption
- Stolen Credentials/Insider Threat
- Visibility on the Network
- Storage of System and Network Information
- Reliance on Proprietary Data Formats or Solutions
- Overuse of Non-person Entities (NPE)/artificial intelligence in ZTA Administration

Possible Interactions with Federal Guidance

- ZTA and NIST Risk Management Framework
- Zero Trust and NIST Privacy Framework
- ZTA and Federal Identity, Credential, and Access Management Architecture
- ZTA and Trusted Internet Connections 3.0
- ZTA and EINSTEIN (NCPS – National Cybersecurity Protection System)
- ZTA and DHS Continuous Diagnostics and Mitigations (CDM) Program
- ZTA, Cloud Smart, and the Federal Data Strategy

Migrating to a ZTA

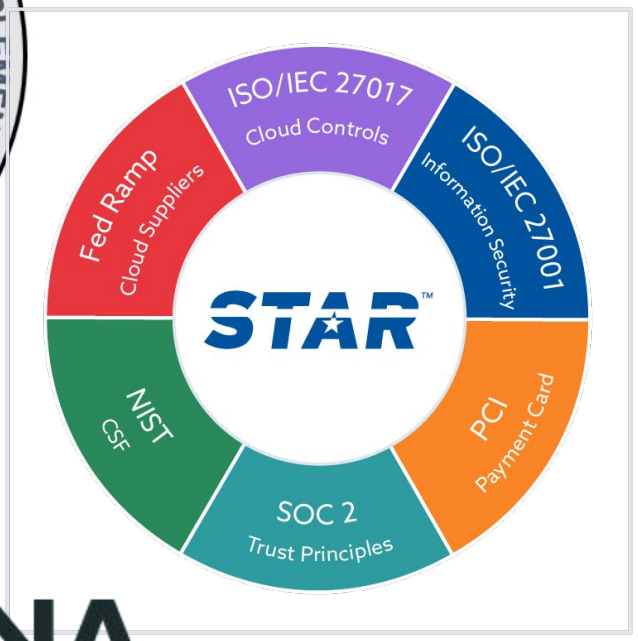
- Pure Zero Trust Architecture
- Hybrid ZTA and Perimeter-Based Architecture
- Steps to Introducing ZTA to a Perimeter-Based Architected Network
  - Identify Actors on the Enterprise
  - Identify Assets Owned by the Enterprise
  - Identify Key Processes and Evaluate Risks Associated with Executing Process
  - Formulating Policies for the ZTA Candidate
  - Identifying Candidate Solutions
  - Initial Deployment and Monitoring
  - Expanding the ZTA

Multi-cloud Information Exchange*

- Conducting risk assessments of the exchange communication channel.
- Will interconnections increase the risk of loss of confidentiality, integrity, and availability of exchange information?
- Are there specific software and hardware requirements?
- Are roles and responsibilities defined?
- Is a 3rd party providing the communication channel?
- Is the 3rd party providing the exchange services by implementing the exchange communication channel only or additional services are delivered?
- Applicable laws, regulations, and policies.

*** Based on NIST SP 800-47 Revision 1**

Multi-Cloud Ecosystem - Challenges for All



MEDINA

- Challenges for all customers (regardless the vertical market):
  - Complexities exist due to system authorizations in different Cloud Service Provider (CSP) hosting environments
  - Inventory/SBOM in multi-cloud
  - Dataflow analysis, & weaknesses/vulnerability management
  - Authorizing Official's (AO) risk tolerances across multi-cloud
  - Incident response

https://medina-project.eu/european-certification-multi-cloud-backends-iot-solutions

Multi-Cloud Ecosystem - Challenges for Federal

- Additional challenges for USG customers:
  - System Authorization Boundaries in multi-cloud
  - Differing DoD Security Requirement Guide (SRG) Impact Levels (IL)'s in multi-cloud systems
  - ATO Documentation across CSPs
  - Compliance Automation in a Multi-Cloud Deployment
  - Continuous monitoring
    - Logs aggregation
    - Events correlation
    - Weaknesses & vulnerabilities management (the MC solution is as vulnerable as the less secure CSP)

Authorization Decisions in Multi-Cloud

- Complexities exist due to system authorizations in different Cloud Service Provider (CSP) hosting environments
- System Authorization Boundaries in Multi-Cloud
  - Additive ATOs? How about the connection?
  - Arching ATO?
- Inventory/SBOM in multi-cloud
- Security requirements (regulatory frameworks /Impact Levels (IL)) in multi-cloud systems
  - Differing by design
    - Data protection?
  - Same by design but different interpretations of requirements and implementation of controls
    - Same assessment procedures
    - Assurance level

5. Open discussion and work planning

a. Teams
b. Team leaders
c. Team members

Resources

Next Meeting:
Feb 14, 2022

MCSPWG Site:
csrc.nist.gov/projects/mcspwg

Mailing list:
mcspwg@list.nist.gov