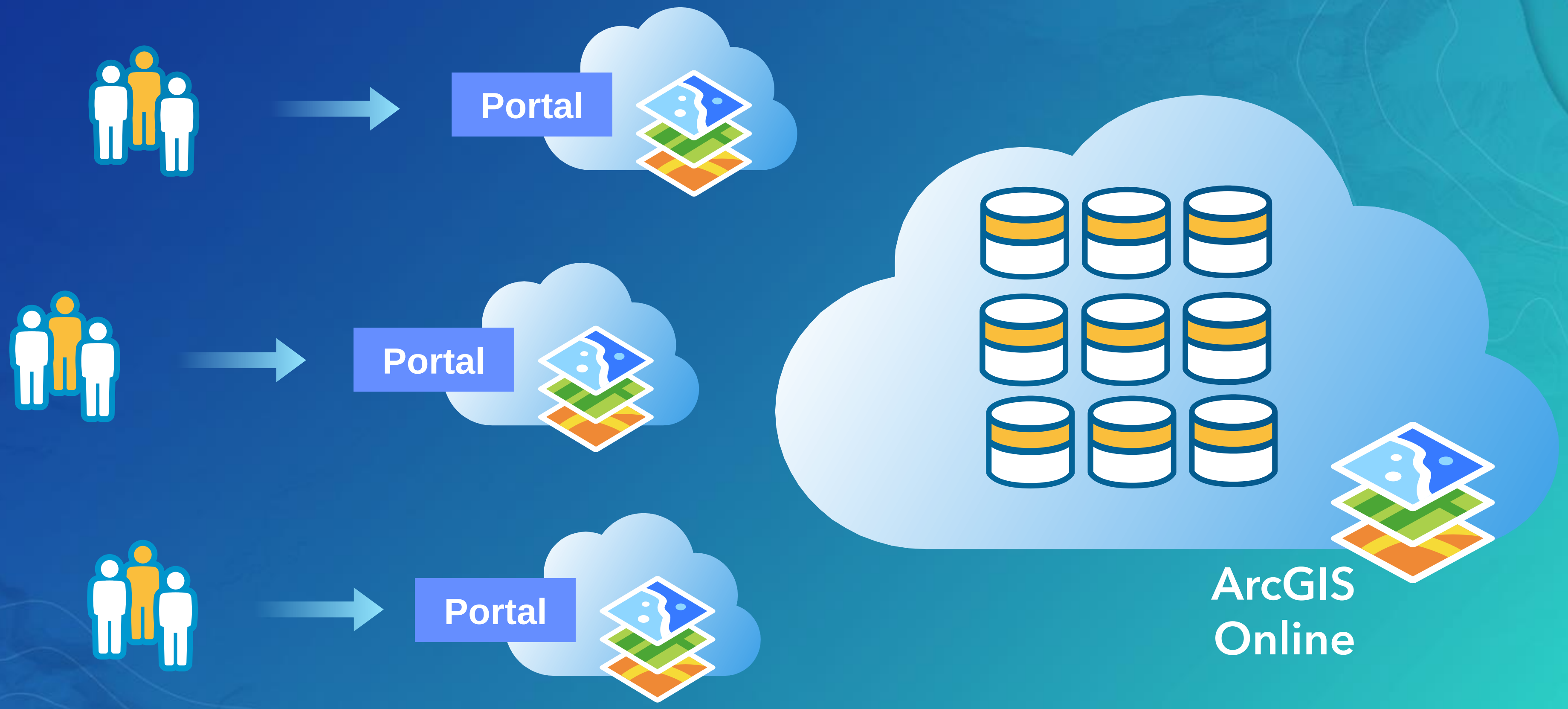
ArcGIS Online: A Security, Privacy & Compliance Overview

Andrea Rosso – Lead Architect

Michael Young – CISO Products

ArcGIS Online – A Multi-Tenant System



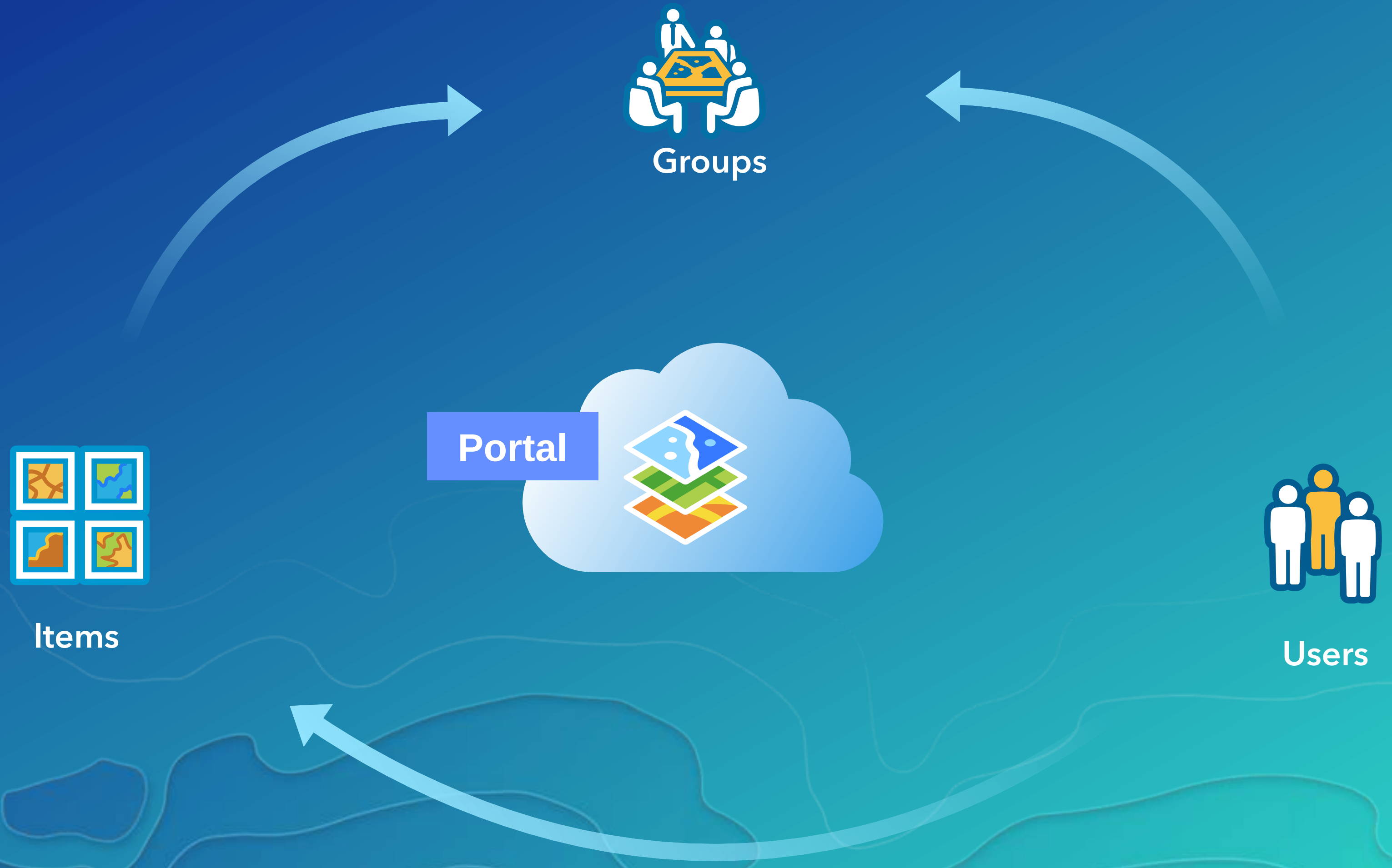
Agenda

- **Platform Security**
- **Deployment Architecture**
- **Compliance**

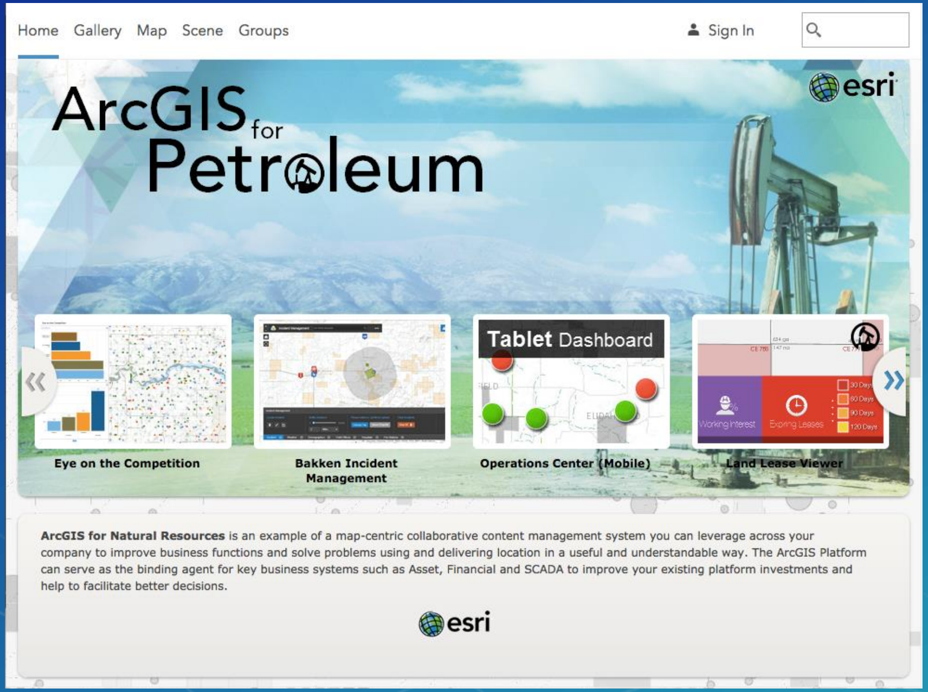
Platform Security

Andrea Rosso

Portal Information Model



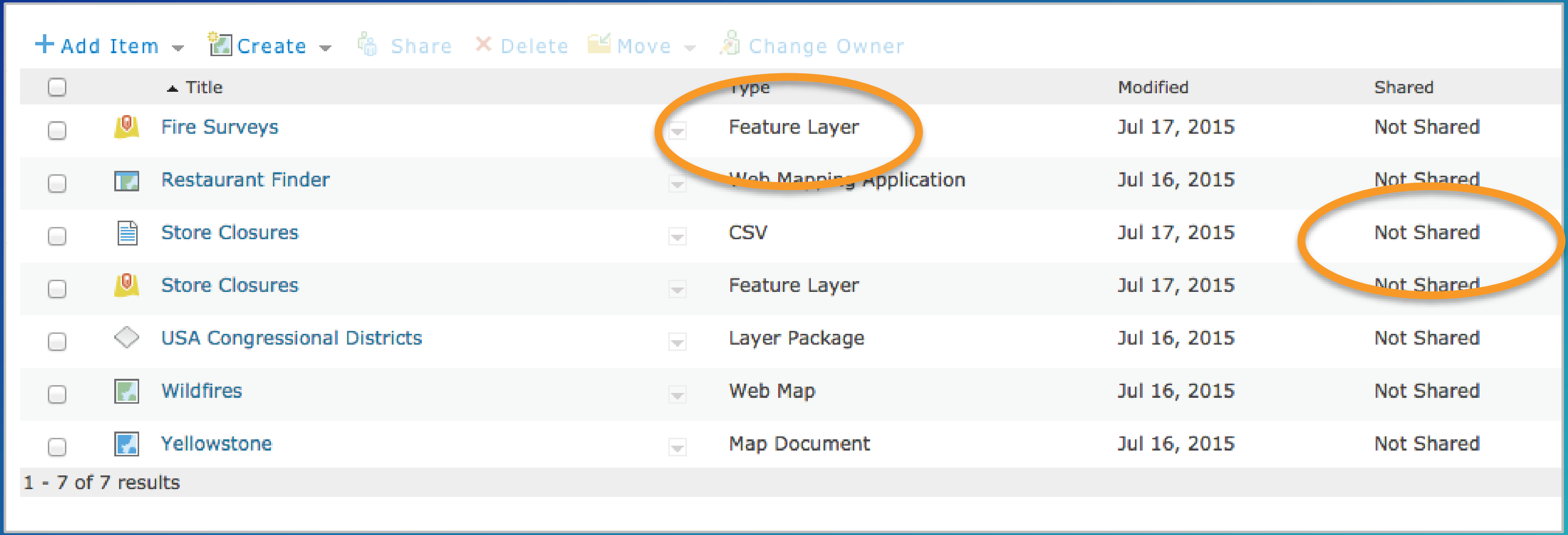
Portal



ArcGIS for Natural Resources is an example of a map-centric collaborative content management system you can leverage across your company to improve business functions and solve problems using and delivering location in a useful and understandable way. The ArcGIS Platform can serve as the binding agent for key business systems such as Asset, Financial and SCADA to improve your existing platform investments and help to facilitate better decisions.

- Your Organization
- Custom Url (yoururl.maps.arcgis.com)
- Public or Private

Items



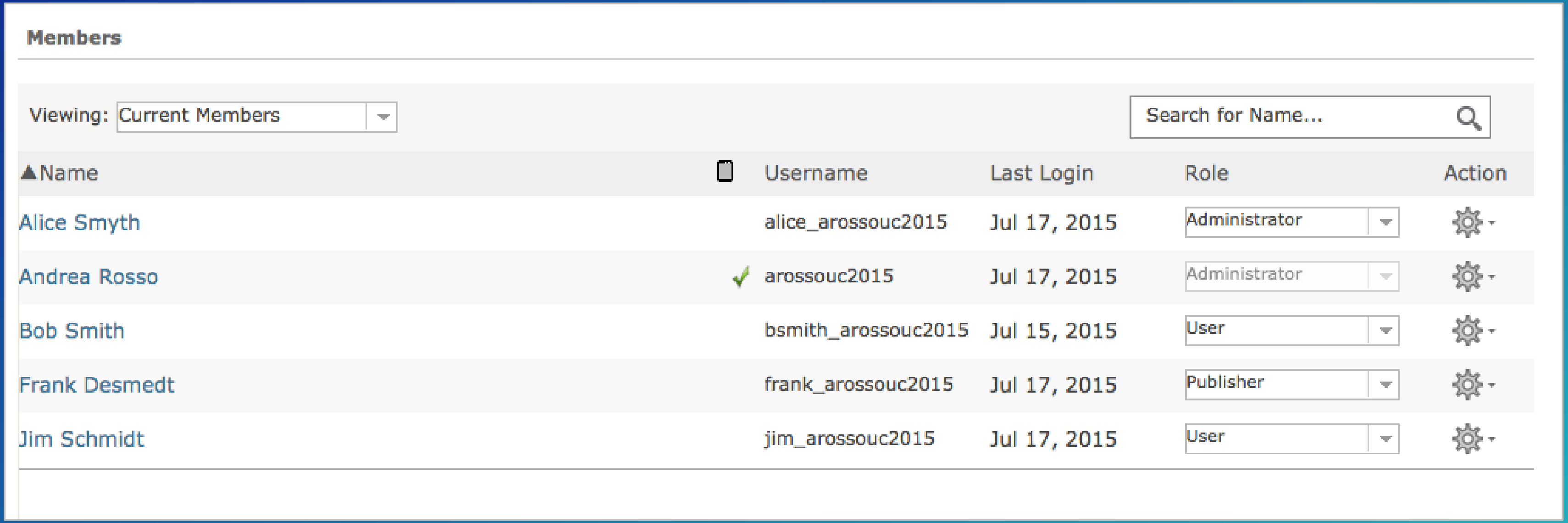
□	Title	Type	Modified	Shared
□	Fire Surveys	Feature Layer	Jul 17, 2015	Not Shared
□	Restaurant Finder	Web Mapping Application	Jul 16, 2015	Not Shared
□	Store Closures	CSV	Jul 17, 2015	Not Shared
□	Store Closures	Feature Layer	Jul 17, 2015	Not Shared
□	USA Congressional Districts	Layer Package	Jul 16, 2015	Not Shared
□	Wildfires	Web Map	Jul 16, 2015	Not Shared
□	Yellowstone	Map Document	Jul 16, 2015	Not Shared

1 - 7 of 7 results

- Typed
  - Web Map
  - Services
  - Data
  - …

- <u>Private</u> by default
- Can Share to
  - Groups
  - Organization
  - Everyone/Public

Users



Members

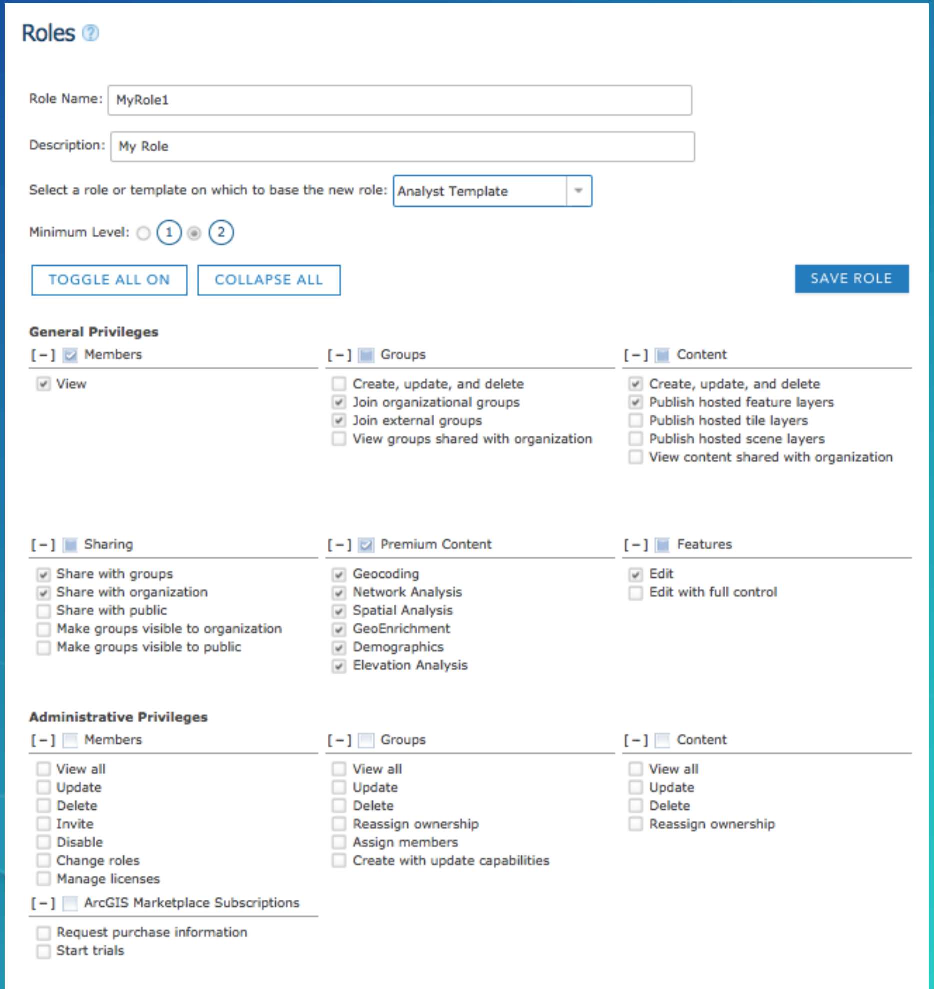
Viewing: Current Members

▲Name	▯	Username	Last Login	Role	Action
Alice Smyth		alice_arossouc2015	Jul 17, 2015	Administrator	⚙
Andrea Rosso	✓	arossouc2015	Jul 17, 2015	Administrator	⚙
Bob Smith		bsmith_arossouc2015	Jul 15, 2015	User	⚙
Frank Desmedt		frank_arossouc2015	Jul 17, 2015	Publisher	⚙
Jim Schmidt		jim_arossouc2015	Jul 17, 2015	User	⚙

- Users own items and groups
- Discoverable
  - No one
  - Organization
  - Everyone
- Users have a profile
- Users have a Role

User Roles

- Built-in Roles
  - Administrator
  - Publisher
  - User
  - Viewer
- Custom Roles
  - Templates
  - Fine Grained Privileges



Roles

Role Name: MyRole1

Description: My Role

Select a role or template on which to base the new role: Analyst Template

Minimum Level: ○ 1 ● 2

General Privileges

[–] ☑ Members
- ☑ View

[–] ▣ Groups
- □ Create, update, and delete
- ☑ Join organizational groups
- ☑ Join external groups
- □ View groups shared with organization

[–] ▣ Content
- ☑ Create, update, and delete
- ☑ Publish hosted feature layers
- □ Publish hosted tile layers
- □ Publish hosted scene layers
- □ View content shared with organization

[–] ▣ Sharing
- ☑ Share with groups
- ☑ Share with organization
- □ Share with public
- □ Make groups visible to organization
- □ Make groups visible to public

[–] ☑ Premium Content
- ☑ Geocoding
- ☑ Network Analysis
- ☑ Spatial Analysis
- ☑ GeoEnrichment
- ☑ Demographics
- ☑ Elevation Analysis

[–] ▣ Features
- ☑ Edit
- □ Edit with full control

Administrative Privileges

[–] □ Members
- □ View all
- □ Update
- □ Delete
- □ Invite
- □ Disable
- □ Change roles
- □ Manage licenses

[–] □ ArcGIS Marketplace Subscriptions
- □ Request purchase information
- □ Start trials

[–] □ Groups
- □ View all
- □ Update
- □ Delete
- □ Reassign ownership
- □ Assign members
- □ Create with update capabilities

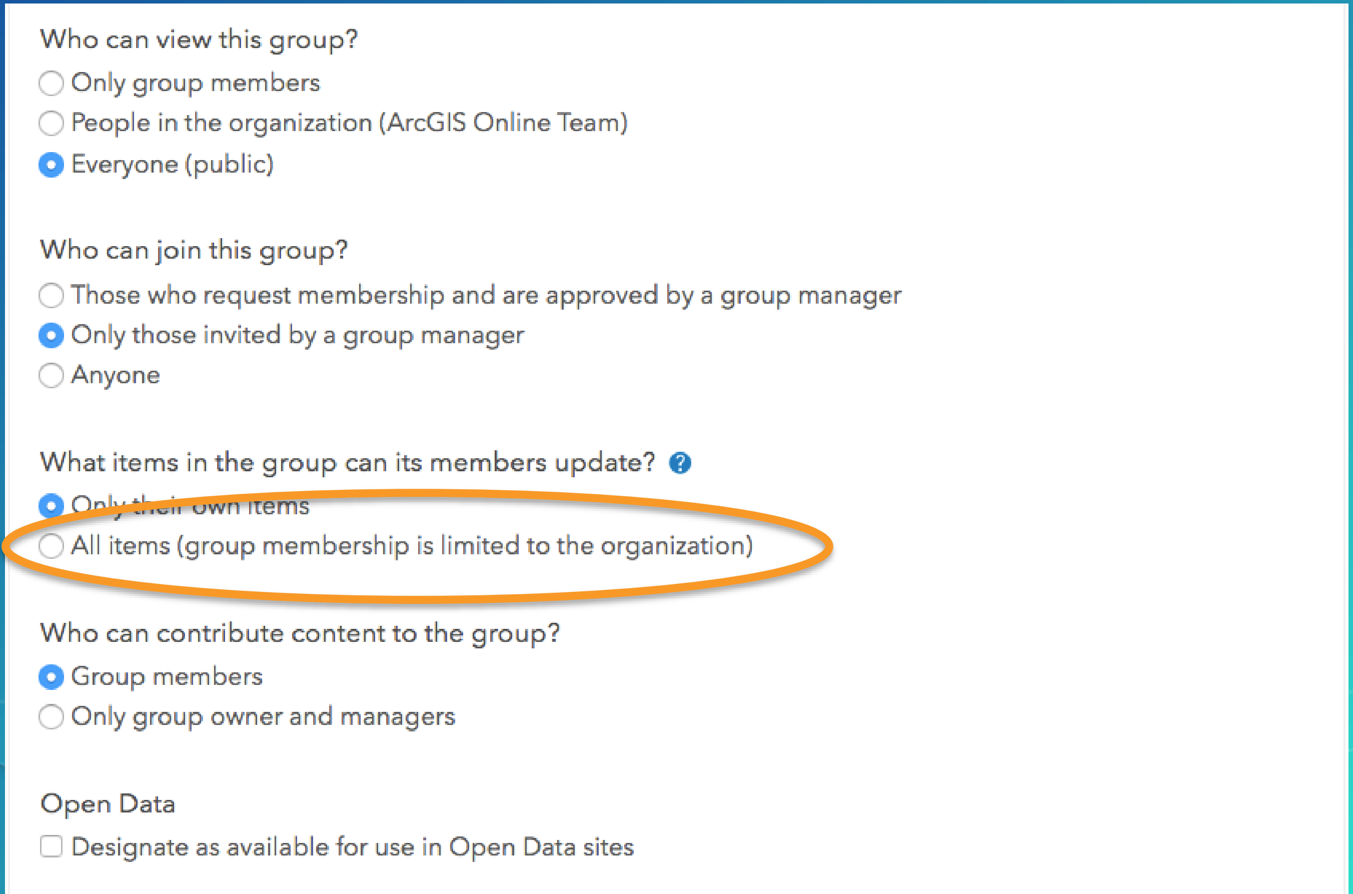
[–] □ Content
- □ View all
- □ Update
- □ Delete
- □ Reassign ownership

Groups

- Contain Items and Users
- Users have access to items in group
- Group owners can share items to their own groups
- Groups can be visible to:
  - No one (private)
  - Organization
  - Everyone
- Items do not inherit visibility

Groups with Update Capability

- Specialized Groups
  - All members can update included items
- Restrictions
  - Can only be created by Admins
  - Items and Users must be within Org
  - Capability cannot be toggled
- Use Cases
  - Shift Operators
  - Collaborative Editing



Who can view this group?

○ Only group members
○ People in the organization (ArcGIS Online Team)
● Everyone (public)

Who can join this group?

○ Those who request membership and are approved by a group manager
● Only those invited by a group manager
○ Anyone

What items in the group can its members update? ?

● Only their own items
○ All items (group membership is limited to the organization)

Who can contribute content to the group?

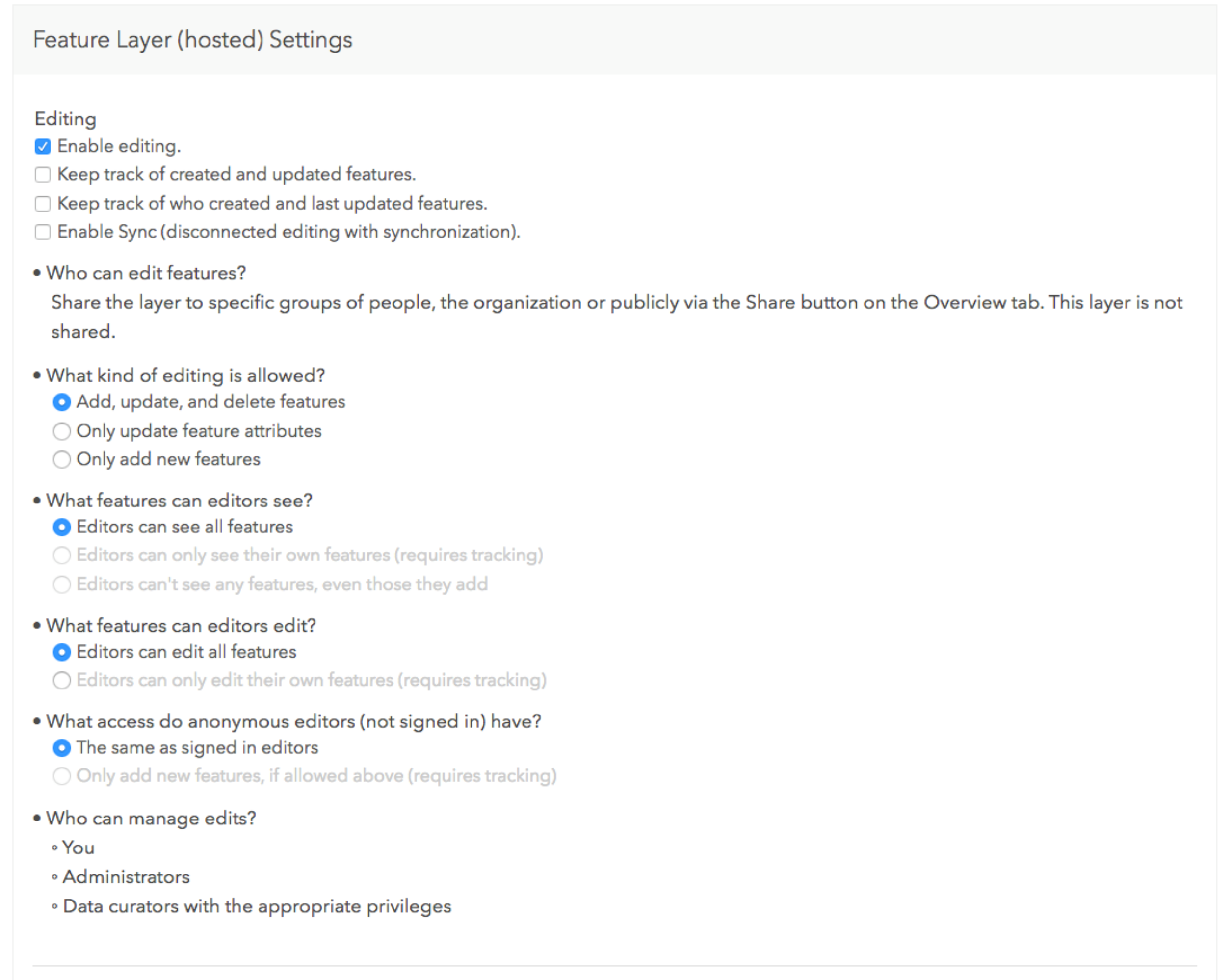
● Group members
○ Only group owner and managers

Open Data

□ Designate as available for use in Open Data sites

Feature Layer Editing

- Users who always can edit
  - Owner
  - Admins
  - Members of Groups w/ Update
- Enable Editing
  - Anyone who can access the service
  - Options
    - Add, update and delete features
    - Only update feature attributes
    - Only add new features
- Custom Roles can have Edit or Edit with full control privileges



Feature Layer (hosted) Settings

Editing

☑ Enable editing.

□ Keep track of created and updated features.

□ Keep track of who created and last updated features.

□ Enable Sync (disconnected editing with synchronization).

- Who can edit features?

  Share the layer to specific groups of people, the organization or publicly via the Share button on the Overview tab. This layer is not shared.

- What kind of editing is allowed?

  ● Add, update, and delete features

  ○ Only update feature attributes

  ○ Only add new features

- What features can editors see?

  ● Editors can see all features

  ○ Editors can only see their own features (requires tracking)

  ○ Editors can't see any features, even those they add

- What features can editors edit?

  ● Editors can edit all features

  ○ Editors can only edit their own features (requires tracking)

- What access do anonymous editors (not signed in) have?

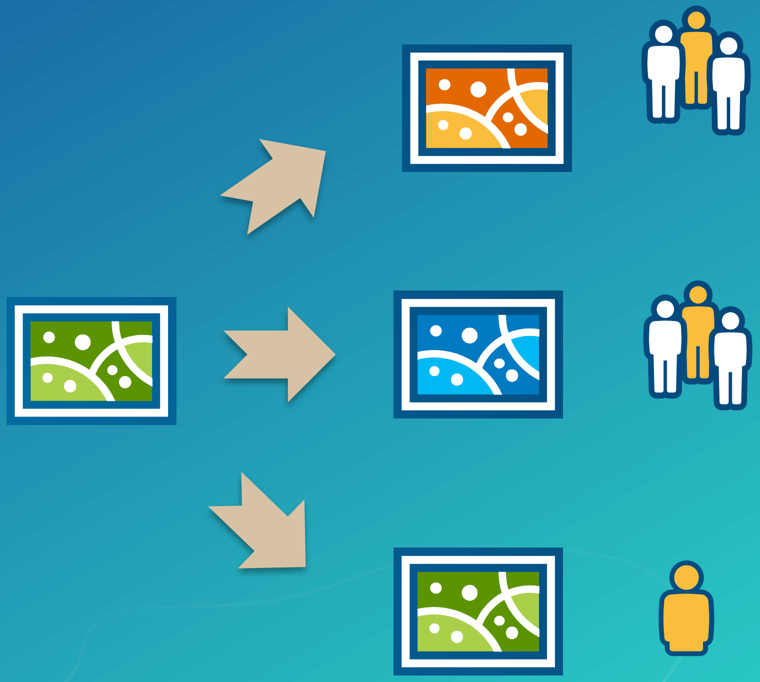
  ● The same as signed in editors

  ○ Only add new features, if allowed above (requires tracking)

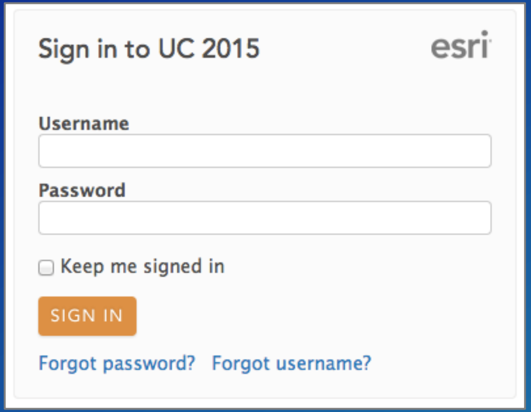
- Who can manage edits?
  - You
  - Administrators
  - Data curators with the appropriate privileges

Hosted Feature Layer Views

- A Feature Layer based on another Feature Layer
- Can have different settings:
  - Sharing
  - Editing
  - Export
  - Filters
  - Metadata
  - Time settings
- Can only be created by owner of base layer
- “Allow only standard SQL queries” should be true



Authentication Options



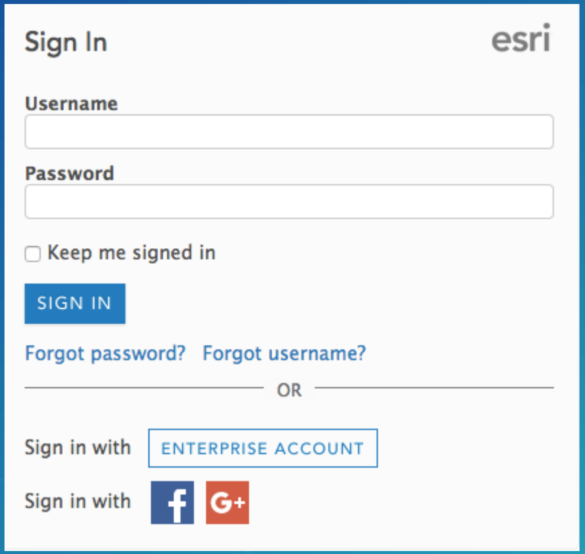
Sign in to UC 2015

Username

Password

□ Keep me signed in

ArcGIS Account



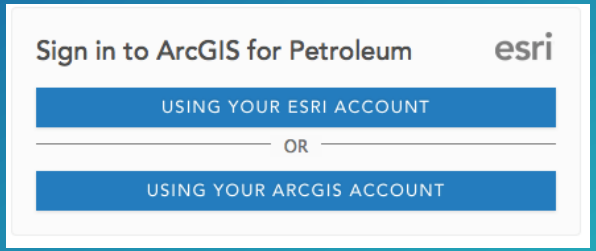
Sign In

Username

Password

□ Keep me signed in

Social Account

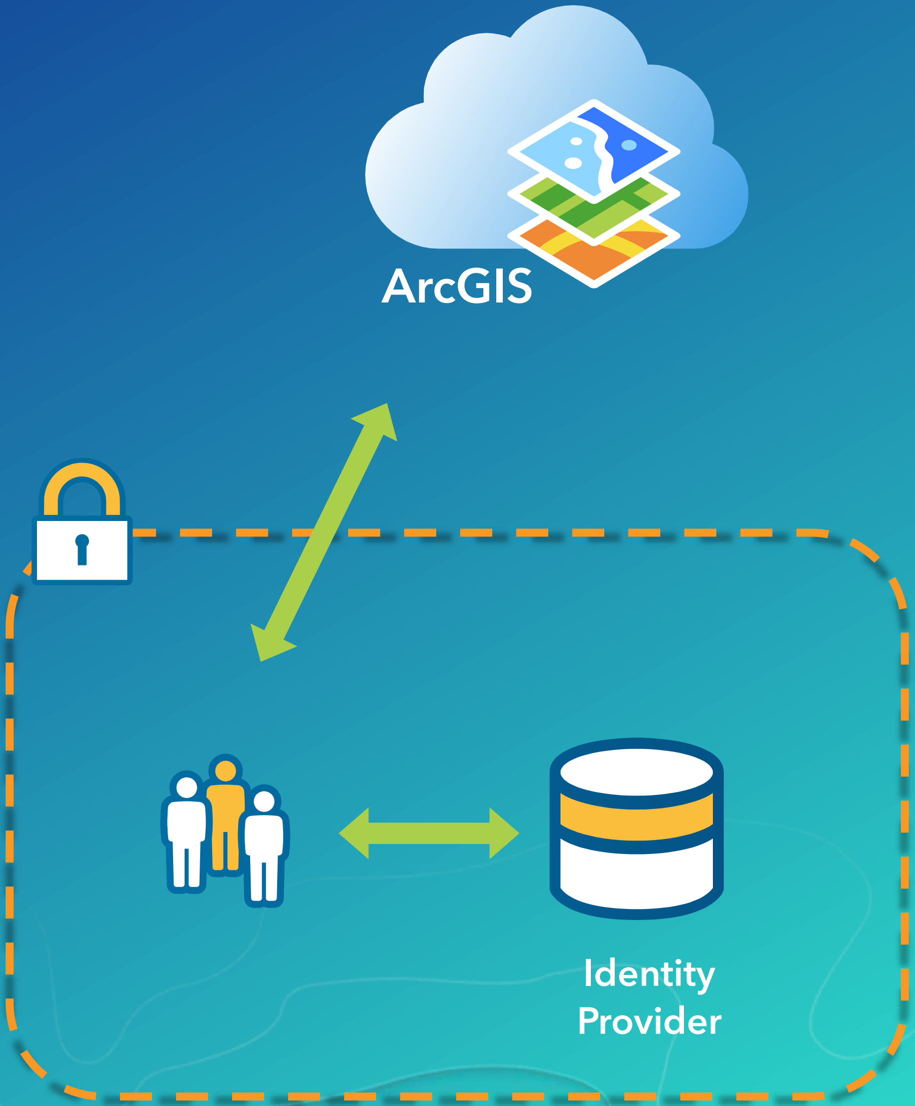


Sign in to ArcGIS for Petroleum

Enterprise Account

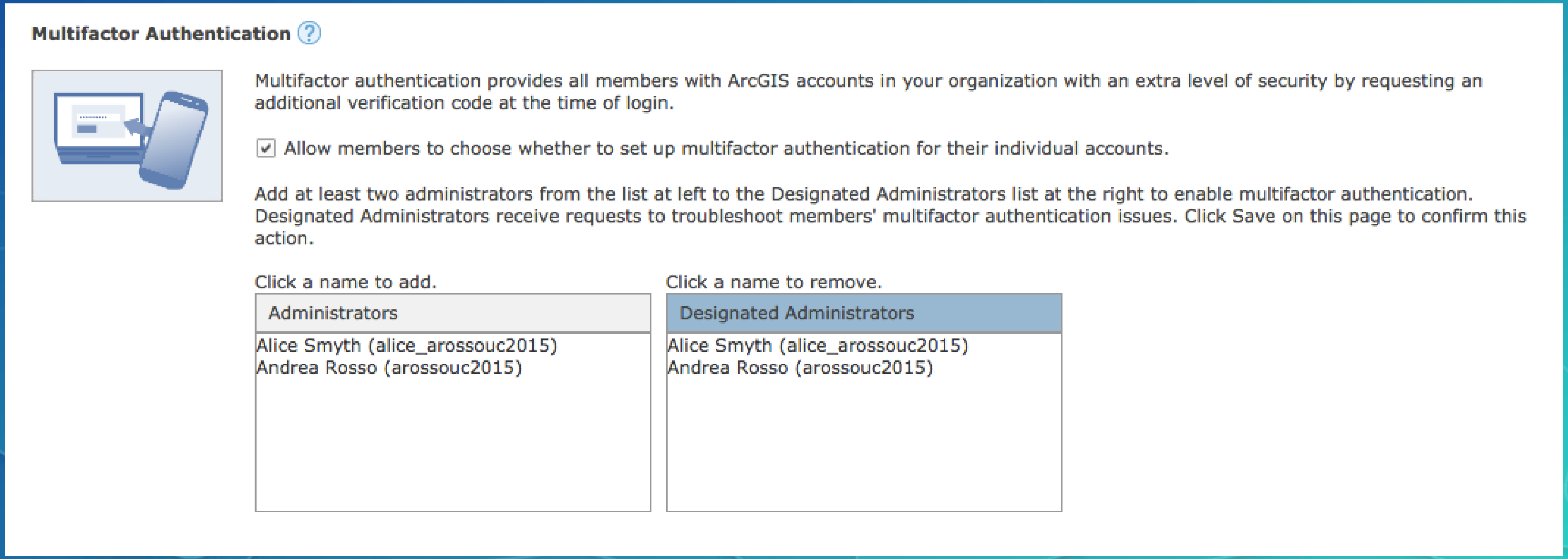
Enterprise Identities

- Use your own identity provider
  - SAML 2.0
    - ADFS
    - NetIQ Access Manager
    - Shibboleth
    - ....
- Can add users:
  - Automatically upon login
  - With an Invitation
- Can use ArcGIS Online identities with Enterprise Identities



Multi-Factor Authentication

- Additional security with second factor at login
- Support for Google Authenticator or MS Authenticator
- Admin needs to enable for Organization
- Must have 2 admins
- Users setup their own Multi-factor



Multifactor Authentication ?

Multifactor authentication provides all members with ArcGIS accounts in your organization with an extra level of security by requesting an additional verification code at the time of login.

☑ Allow members to choose whether to set up multifactor authentication for their individual accounts.

Add at least two administrators from the list at left to the Designated Administrators list at the right to enable multifactor authentication. Designated Administrators receive requests to troubleshoot members' multifactor authentication issues. Click Save on this page to confirm this action.

Click a name to add.

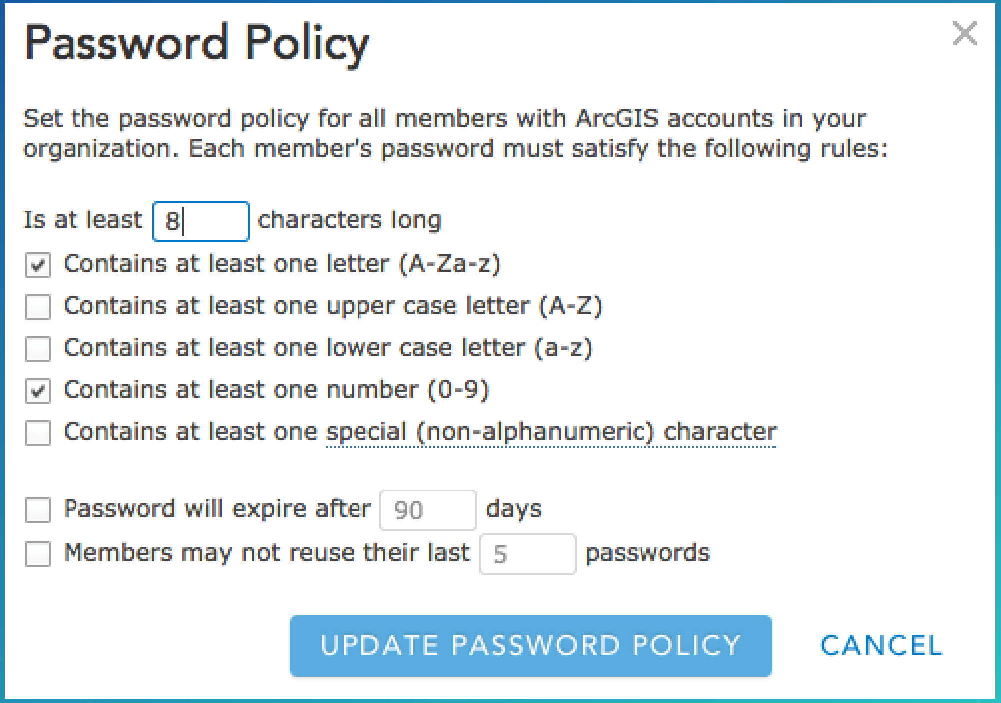
Administrators
Alice Smyth (alice_arossouc2015)
Andrea Rosso (arossouc2015)

Click a name to remove.

Designated Administrators
Alice Smyth (alice_arossouc2015)
Andrea Rosso (arossouc2015)

Password Polices

- Default Password Policy
  - 8 characters with at least 1 number
- Can Customize
  - Complexity
  - History
  - Expiration



Password Policy

Set the password policy for all members with ArcGIS accounts in your organization. Each member's password must satisfy the following rules:

Is at least 8 characters long

☑ Contains at least one letter (A-Za-z)

☐ Contains at least one upper case letter (A-Z)

☐ Contains at least one lower case letter (a-z)

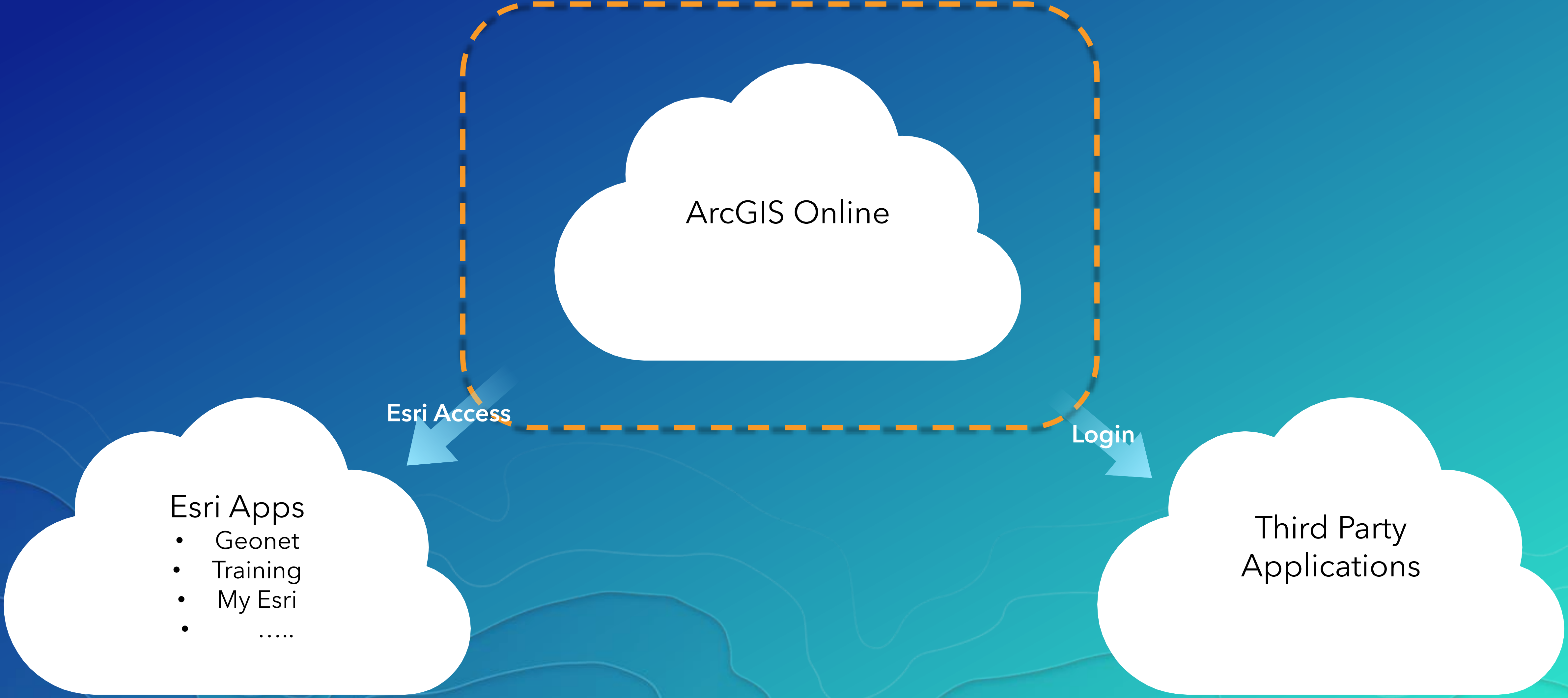
☑ Contains at least one number (0-9)

☐ Contains at least one special (non-alphanumeric) character

☐ Password will expire after 90 days

☐ Members may not reuse their last 5 passwords

Trust Boundaries



ArcGIS Online

Esri Access

Login

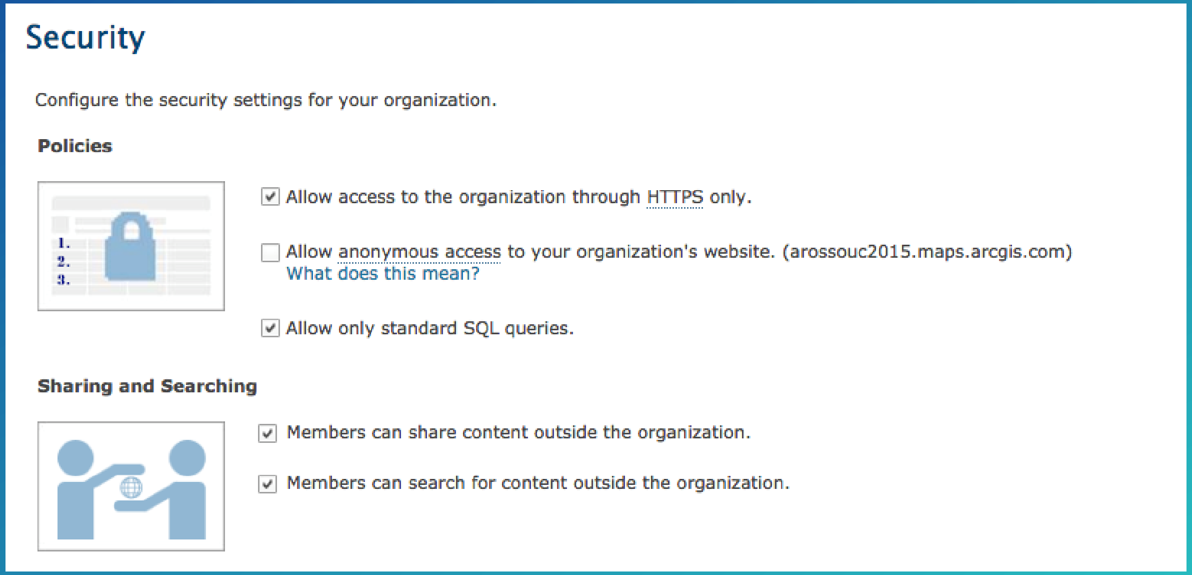
Esri Apps

- Geonet
- Training
- My Esri
- .....

Third Party Applications

Admin Organization Controls

- Use only HTTPS (HSTS)
- Disable Sharing to Everyone
- Purchasers
- Admin Contacts
- Disable Bio



Security

Configure the security settings for your organization.

Policies

☑ Allow access to the organization through HTTPS only.

□ Allow anonymous access to your organization's website. (arossouc2015.maps.arcgis.com)
What does this mean?

☑ Allow only standard SQL queries.

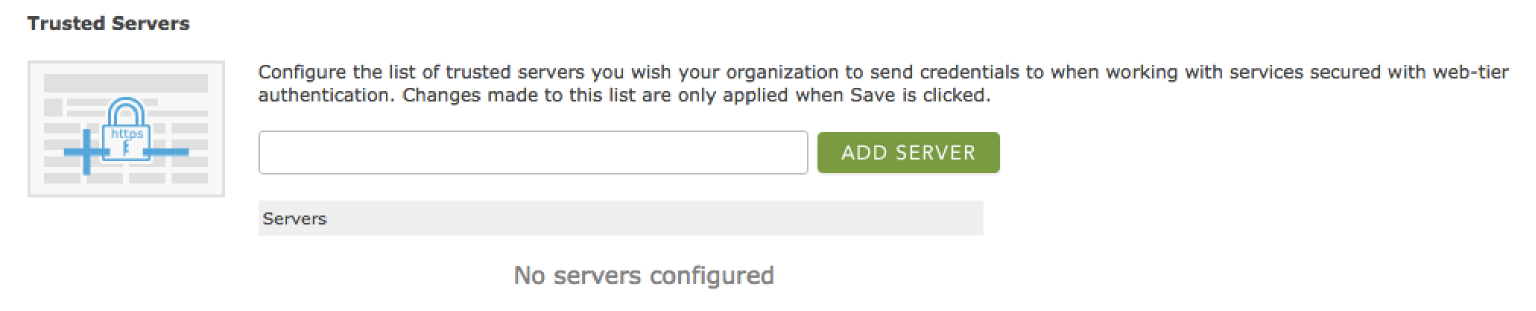
Sharing and Searching

☑ Members can share content outside the organization.

☑ Members can search for content outside the organization.

Admin Organization Controls

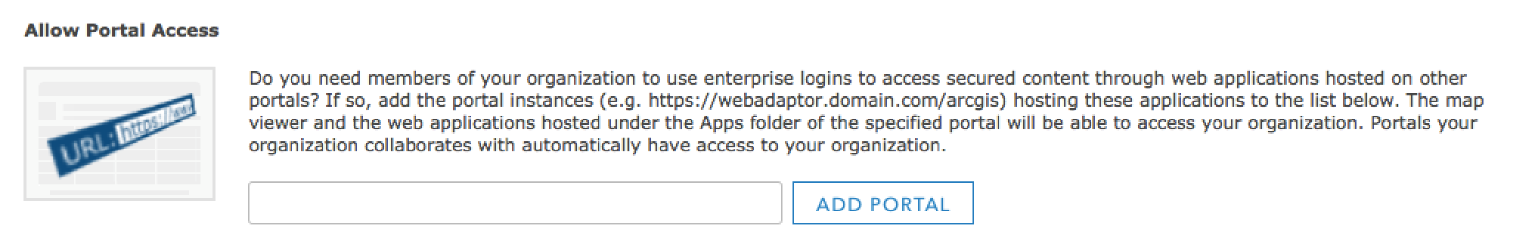
- Trusted Servers
- Allow Portal Access
- Allow Origins



Trusted Servers

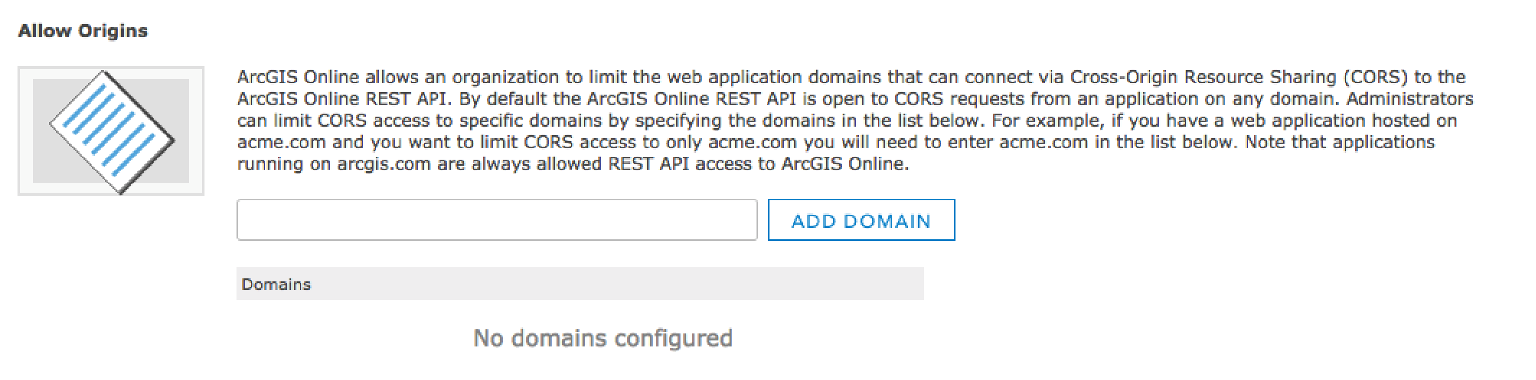
Configure the list of trusted servers you wish your organization to send credentials to when working with services secured with web-tier authentication. Changes made to this list are only applied when Save is clicked.

No servers configured



Allow Portal Access

Do you need members of your organization to use enterprise logins to access secured content through web applications hosted on other portals? If so, add the portal instances (e.g. https://webadaptor.domain.com/arcgis) hosting these applications to the list below. The map viewer and the web applications hosted under the Apps folder of the specified portal will be able to access your organization. Portals your organization collaborates with automatically have access to your organization.



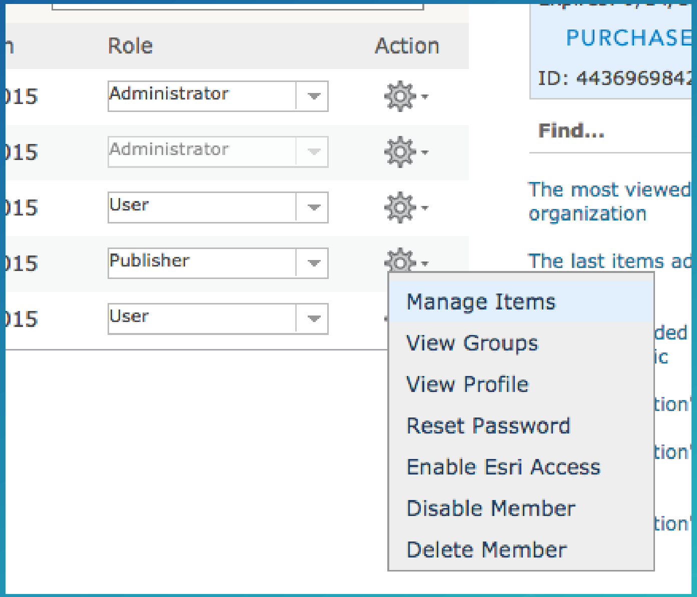
Allow Origins

ArcGIS Online allows an organization to limit the web application domains that can connect via Cross-Origin Resource Sharing (CORS) to the ArcGIS Online REST API. By default the ArcGIS Online REST API is open to CORS requests from an application on any domain. Administrators can limit CORS access to specific domains by specifying the domains in the list below. For example, if you have a web application hosted on acme.com and you want to limit CORS access to only acme.com you will need to enter acme.com in the list below. Note that applications running on arcgis.com are always allowed REST API access to ArcGIS Online.

No domains configured

Administrator Controls on Users

- Admins can
  - Manage Items, Groups, Profile
  - Disable Users
  - Delete Users
  - Reset User's Password
  - Change Role
  - Enable Esri Access

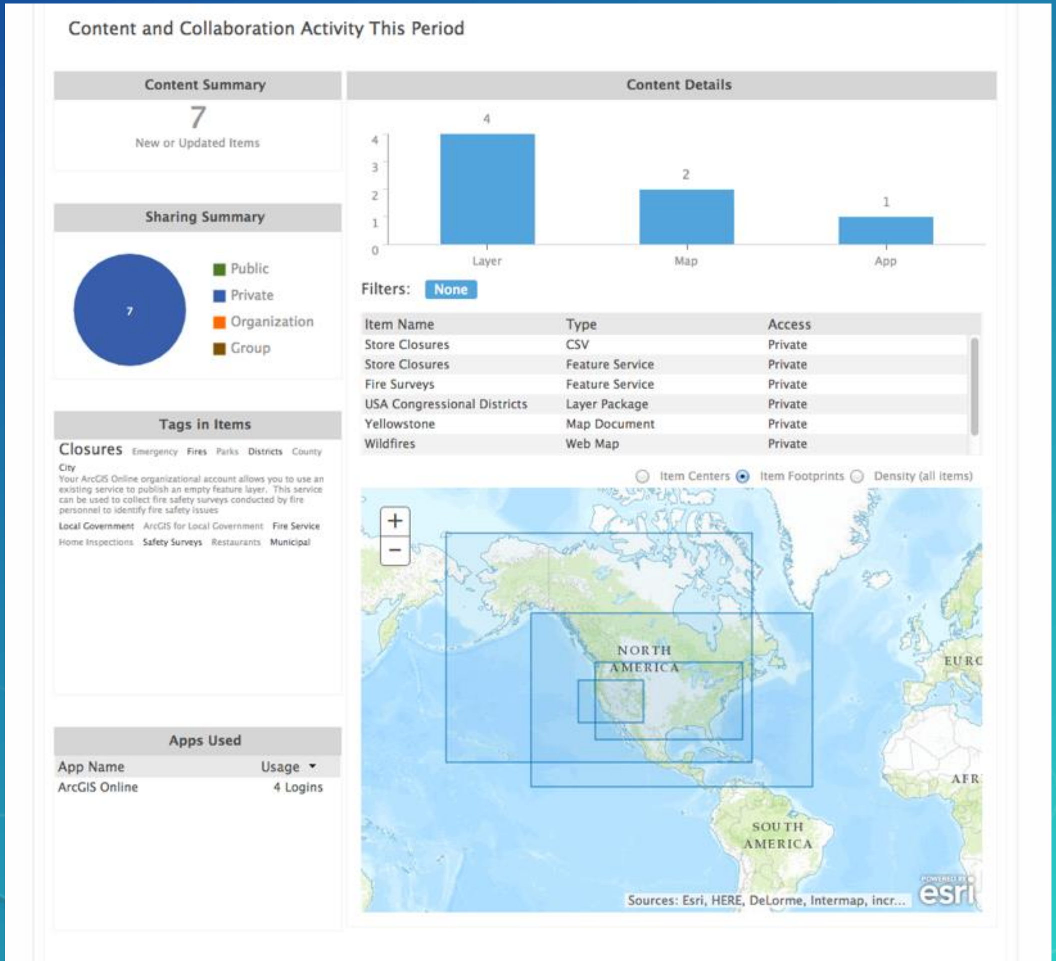


n	Role	Action
)15	Administrator	
)15	Administrator	
)15	User	
)15	Publisher	
)15	User	

ID: 4436969842

Keeping Track of Usage

- **Status Reports**
  - Credits
  - Content
  - Members
  - Groups



Content and Collaboration Activity This Period

Content Summary

7

New or Updated Items

Sharing Summary

🟩 Public

🟦 Private

🟧 Organization

🟫 Group

Tags in Items

Closures Emergency Fires Parks Districts County City

Your ArcGIS Online organizational account allows you to use an existing service to publish an empty feature layer. This service can be used to collect fire safety surveys conducted by fire personnel to identify fire safety issues

Local Government ArcGIS for Local Government Fire Service Home Inspections Safety Surveys Restaurants Municipal

Apps Used

App Name	Usage ▾
ArcGIS Online	4 Logins

Content Details

Filters: None

Item Name	Type	Access
Store Closures	CSV	Private
Store Closures	Feature Service	Private
Fire Surveys	Feature Service	Private
USA Congressional Districts	Layer Package	Private
Yellowstone	Map Document	Private
Wildfires	Web Map	Private

○ Item Centers ● Item Footprints ○ Density (all items)

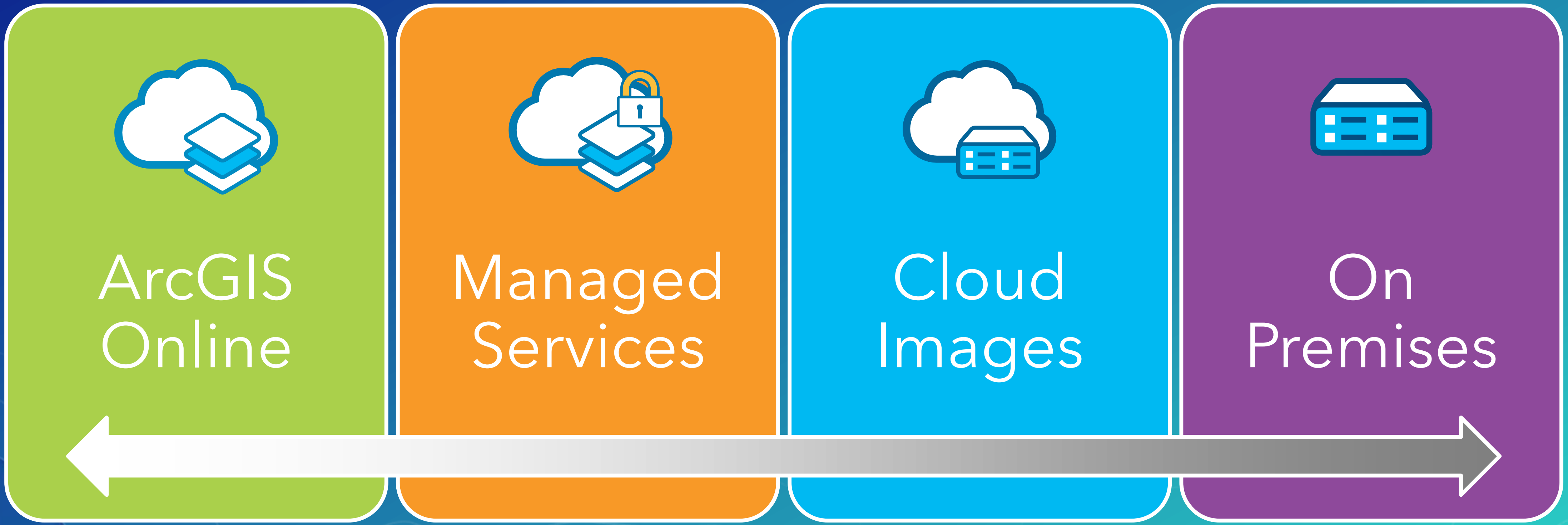
Sources: Esri, HERE, DeLorme, Intermap, incr...

Deployment Architecture

Michael Young

Deployment Architecture

Options



ArcGIS Online

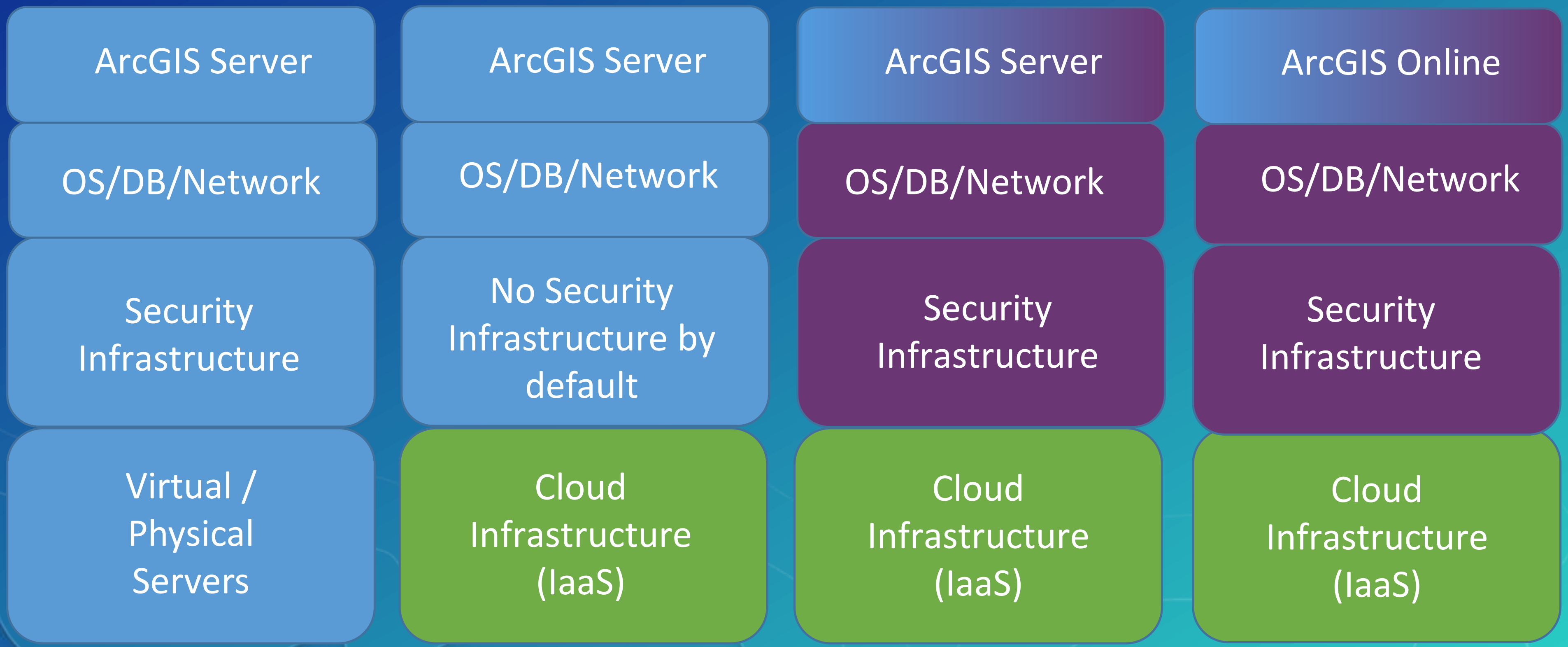
Managed Services

Cloud Images

On Premises

Deployment Architecture

Responsibility

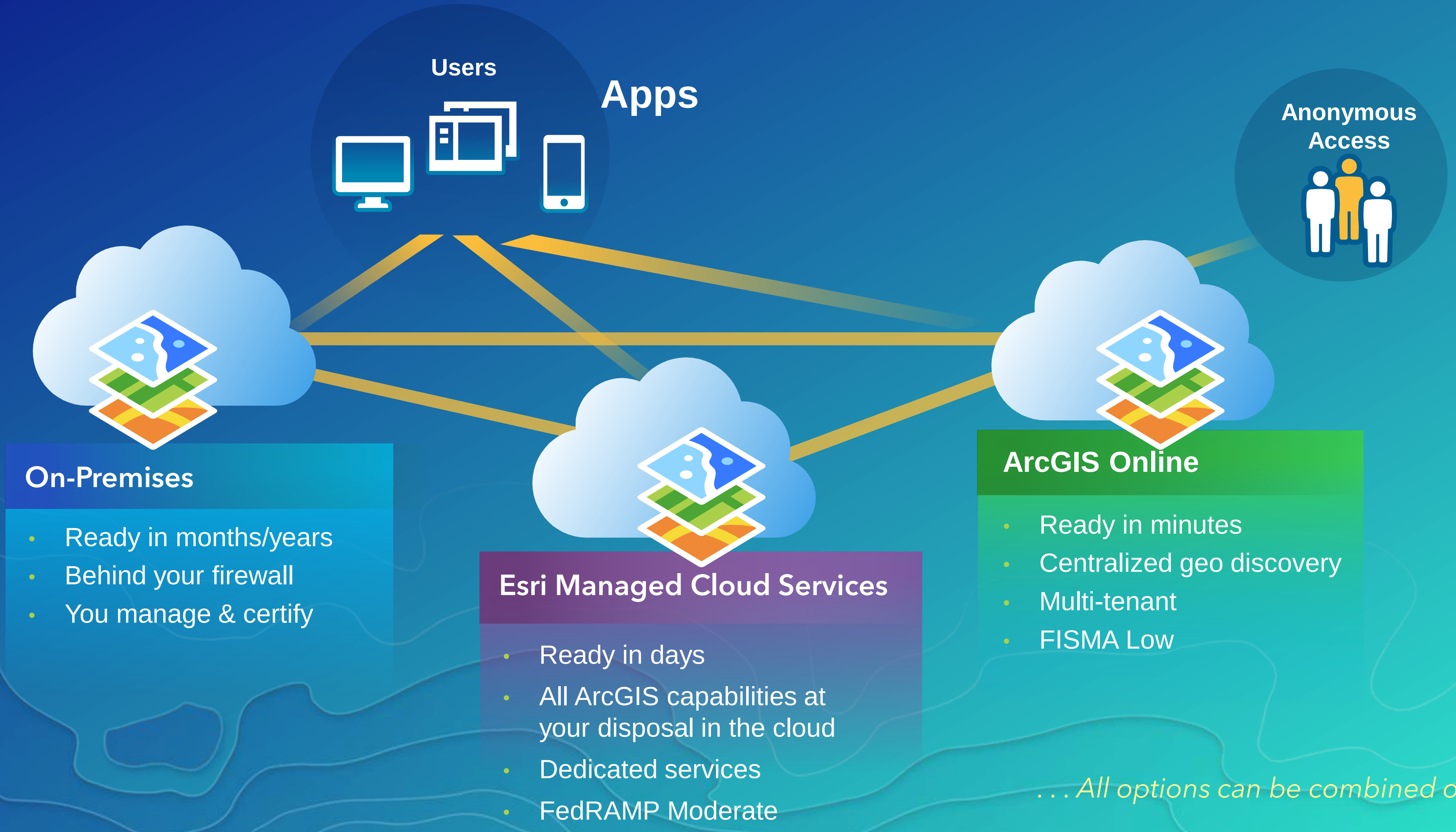


On-premises	Cloud Images	Managed Services *FedRAMP Moderate*	ArcGIS Online *FISMA Low*
🟦 ArcGIS Server	🟦 ArcGIS Server	🟦🟪 ArcGIS Server	🟦🟪 ArcGIS Online
🟦 OS/DB/Network	🟦 OS/DB/Network	🟪 OS/DB/Network	🟪 OS/DB/Network
🟦 Security Infrastructure	🟦 No Security Infrastructure by default	🟪 Security Infrastructure	🟪 Security Infrastructure
🟦 Virtual / Physical Servers	🟩 Cloud Infrastructure (IaaS)	🟩 Cloud Infrastructure (IaaS)	🟩 Cloud Infrastructure (IaaS)

Customer Responsibility 🟦 **Esri Responsibility** 🟪 **CSP Responsibility** 🟩

Deployment Architecture

Hosting Options



On-Premises

- Ready in months/years
- Behind your firewall
- You manage & certify

Esri Managed Cloud Services

- Ready in days
- All ArcGIS capabilities at your disposal in the cloud
- Dedicated services
- FedRAMP Moderate

ArcGIS Online

- Ready in minutes
- Centralized geo discovery
- Multi-tenant
- FISMA Low

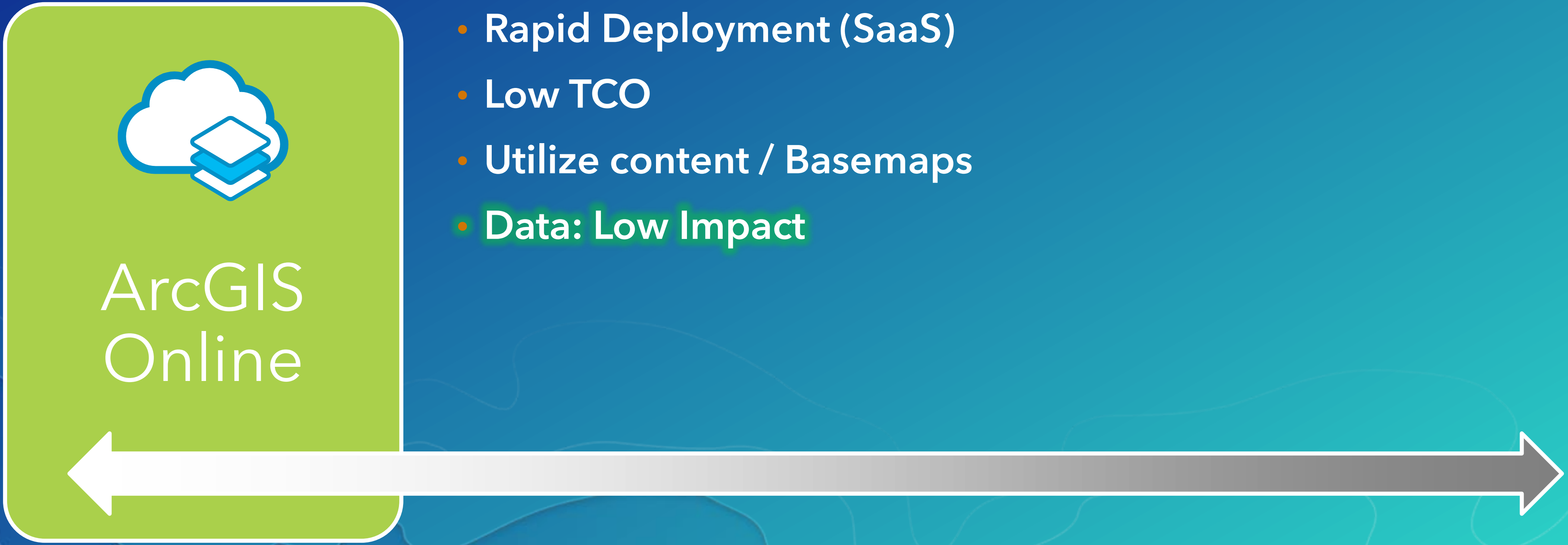
. . . All options can be combined or separate

Deployment Architecture

User Scenario – ArcGIS Online Alone

I want to share and process operational data with field workers.

- Rapid Deployment (SaaS)
- Low TCO
- Utilize content / Basemaps
- Data: Low Impact

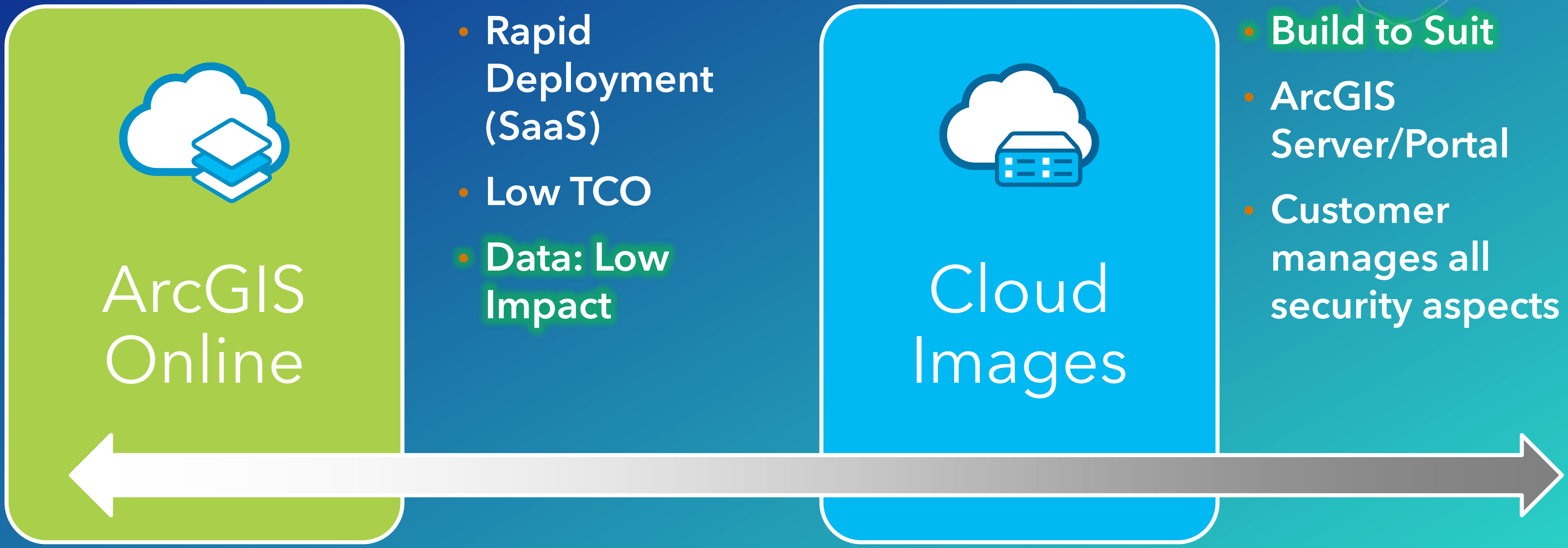


ArcGIS Online

Deployment Architecture

User Scenario – ArcGIS Online + Cloud Images

I need to pilot a solution that requires basemaps and some ArcGIS server specific features.



ArcGIS Online

- Rapid Deployment (SaaS)
- Low TCO
- Data: Low Impact

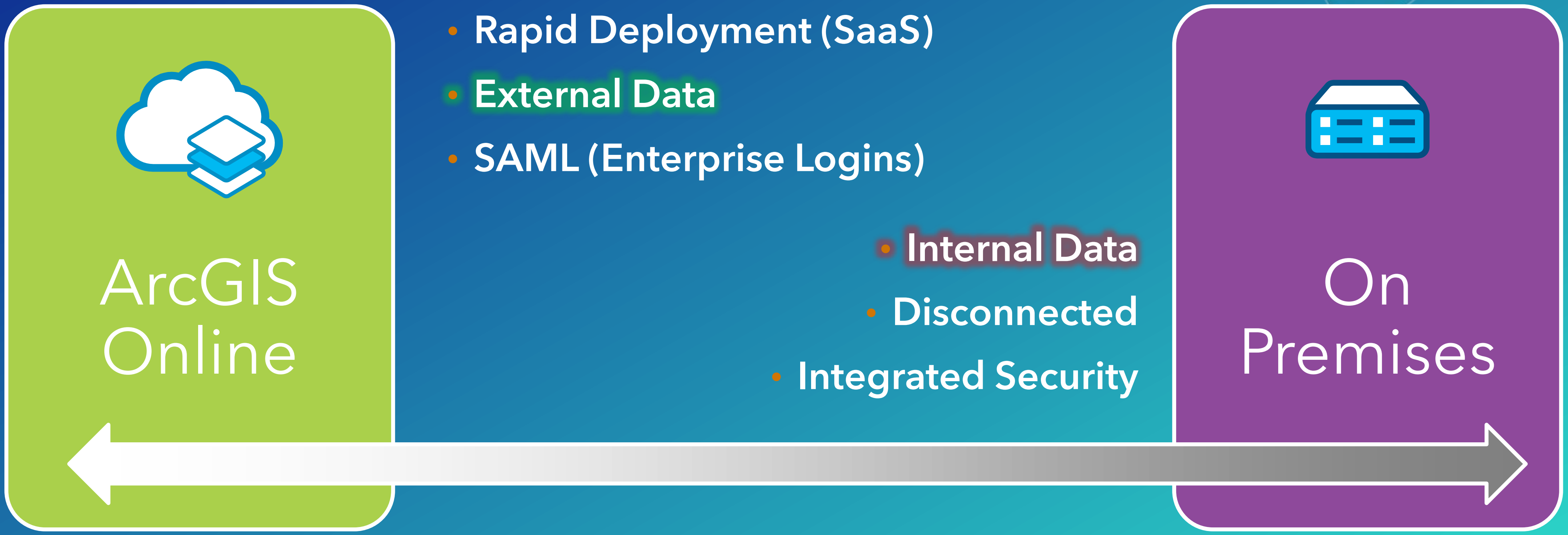
Cloud Images

- Build to Suit
- ArcGIS Server/Portal
- Customer manages all security aspects

Deployment Architecture

User Scenario – ArcGIS Online + On-Premises

I want to share sensitive data internally but provide subsets to external and public users.



ArcGIS Online

- Rapid Deployment (SaaS)
- External Data
- SAML (Enterprise Logins)

- Internal Data
- Disconnected
- Integrated Security

On Premises

***Example**: EPA's FISMA Authorized GeoPlatform*

Deployment Architecture

Registering ArcGIS Server Services in ArcGIS Online

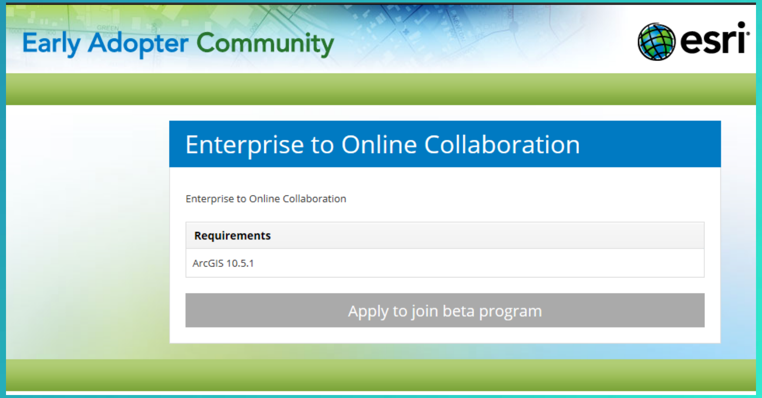
- **Common for large enterprises**
  - **Primary reason**
    - **Data Segmentation / Prevent storing sensitive data in the cloud**

- **What is stored in ArcGIS Online? – Service Metadata**
  - **Username & password -** Default, not saved
  - **Initial extent -** Adjust to a less specific area
  - **Name & tags -** Address with organization naming convention
  - **IP Address -** Utilize DNS names within URL's
  - **Thumbnail image –** Replace with any image as appropriate

Deployment Architecture

User Scenario – ArcGIS Online + On-Premises w/Collaboration

- Starting with 10.5.1 Collaboration was enhanced to connect ArcGIS Online with ArcGIS Enterprise
- Allows for a greater flow of data and maps between the two systems
- Search and discover data and maps through a single home system, no matter how it is physically spread out and maintained across different departments within your organization
- Currently provided as part of the early adopter program
- http://doc.arcgis.com/en/arcgis-online/administer/create-a-collaboration.htm



Early Adopter Community

esri

Enterprise to Online Collaboration

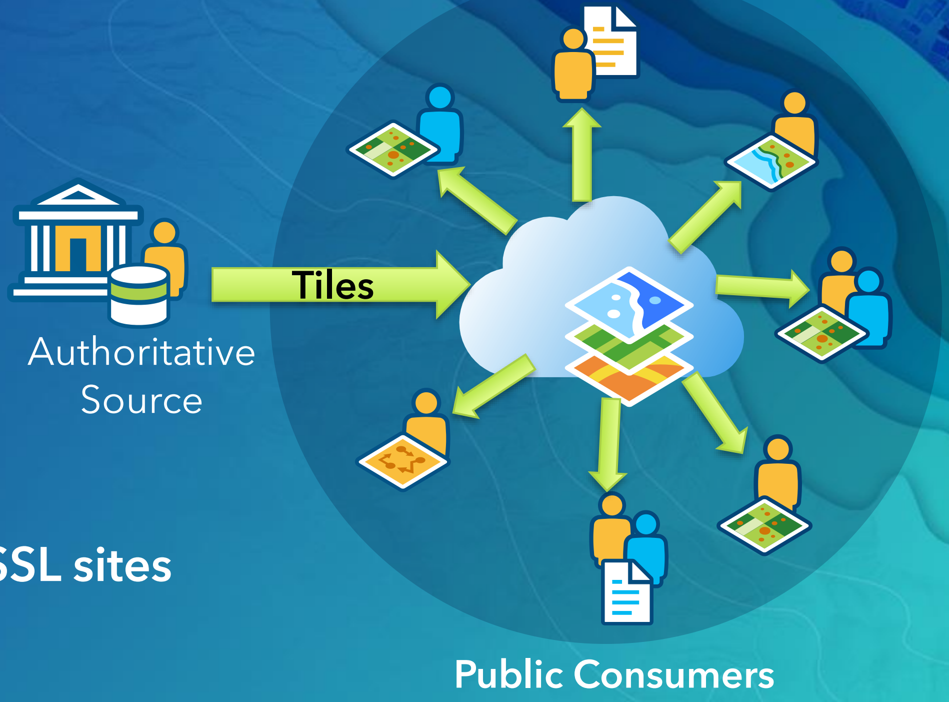
Enterprise to Online Collaboration

Requirements
ArcGIS 10.5.1

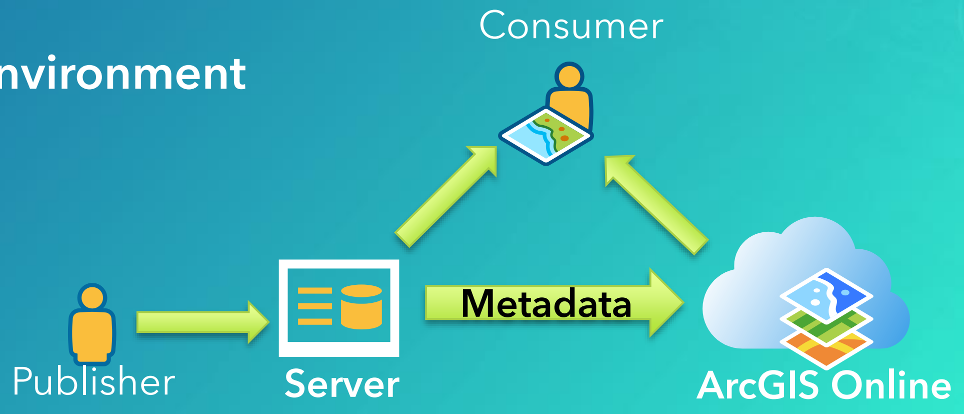
Deployment Architecture

ArcGIS Online FISMA Authorized Use Cases

- Use Case 1 – Public Dissemination
  - Publish tiles for fast, scalable visualizations
  - Share information with the public
  - Can be used for mashing up services with external non-SSL sites



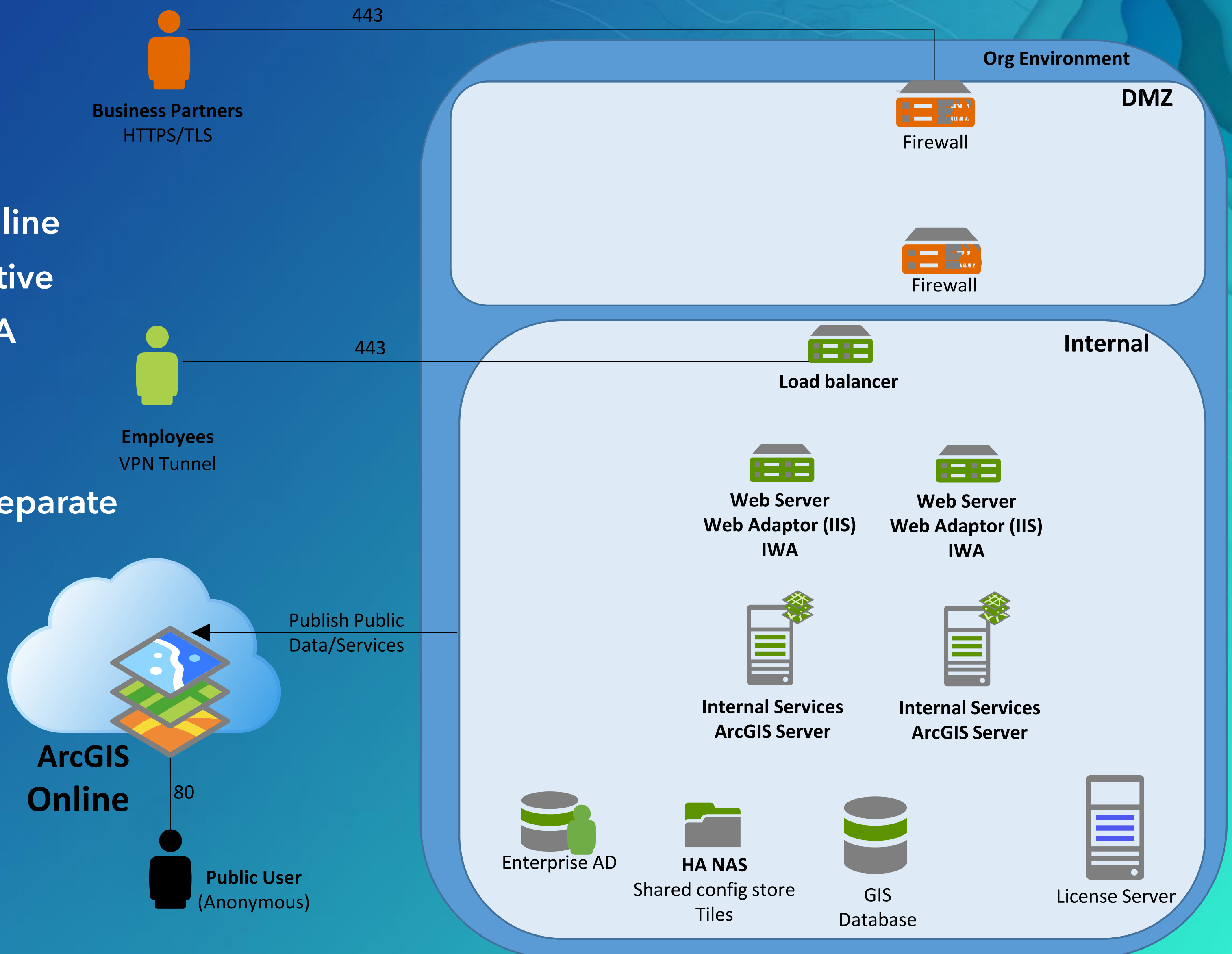
- Use Case 2 – Share operational data within or between businesses
  - Register ArcGIS Server Services in ArcGIS Online
  - Sensitive data stored on premises or other authorized environment
  - ArcGIS Online operates as a discovery portal
  - Utilize Enterprise Logins



Deployment Architecture

Using ArcGIS Online for Public Dissemination

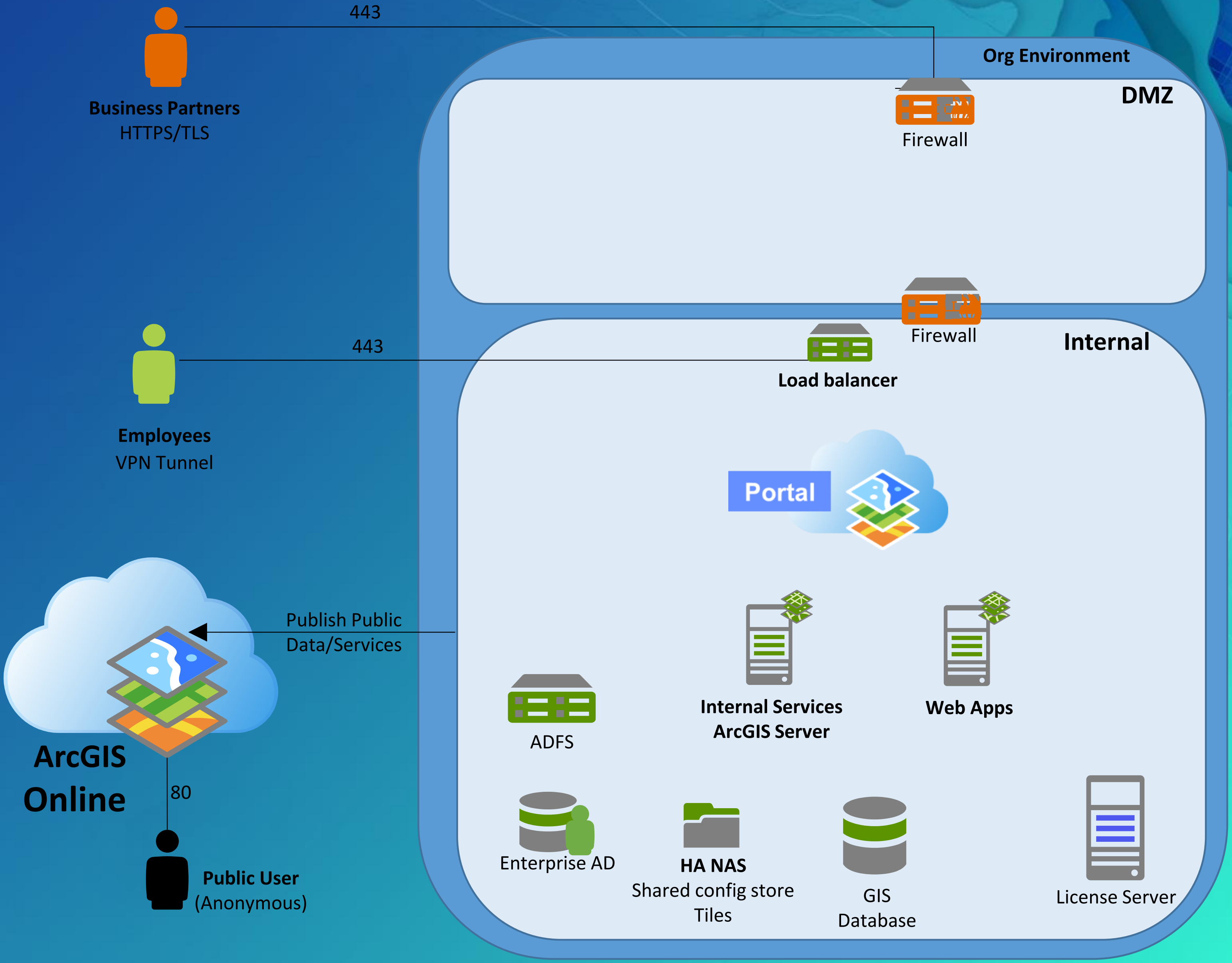
- Pros
  - Variable user loads handled by ArcGIS Online
  - Public information Segmented from Sensitive
  - Internal users have SSO experience w/IWA
- Cons
  - Internal users access ArcGIS Online with separate logins
  - Partners do not have an SSO experience
  - External publishing workflow is needed



Deployment Architecture

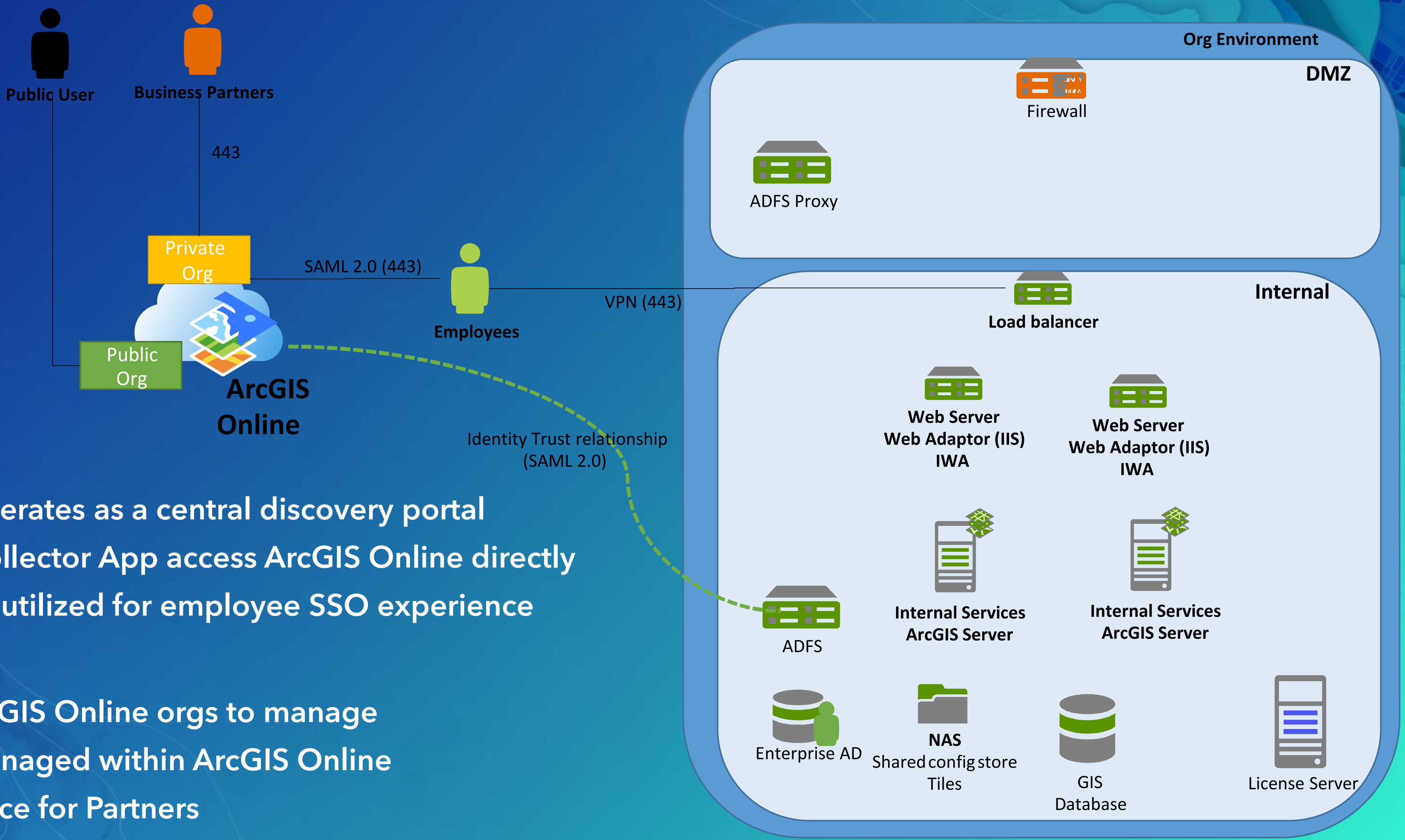
Using Both ArcGIS Online & Portal On-Premises

- Pros
  - Same scalability and segmentation benefits for public services
  - Portal & Server Federation provide employee SSO
- Cons
  - Overhead of internal Portal management / hardware
  - Separate workflows for Portal and ArcGIS Online
    - New ArcGIS Online / Portal collaboration capabilities in 10.5.1 can offset this con



Deployment Architecture

Using Multiple ArcGIS Online Orgs for Segmentation (Private/Public)

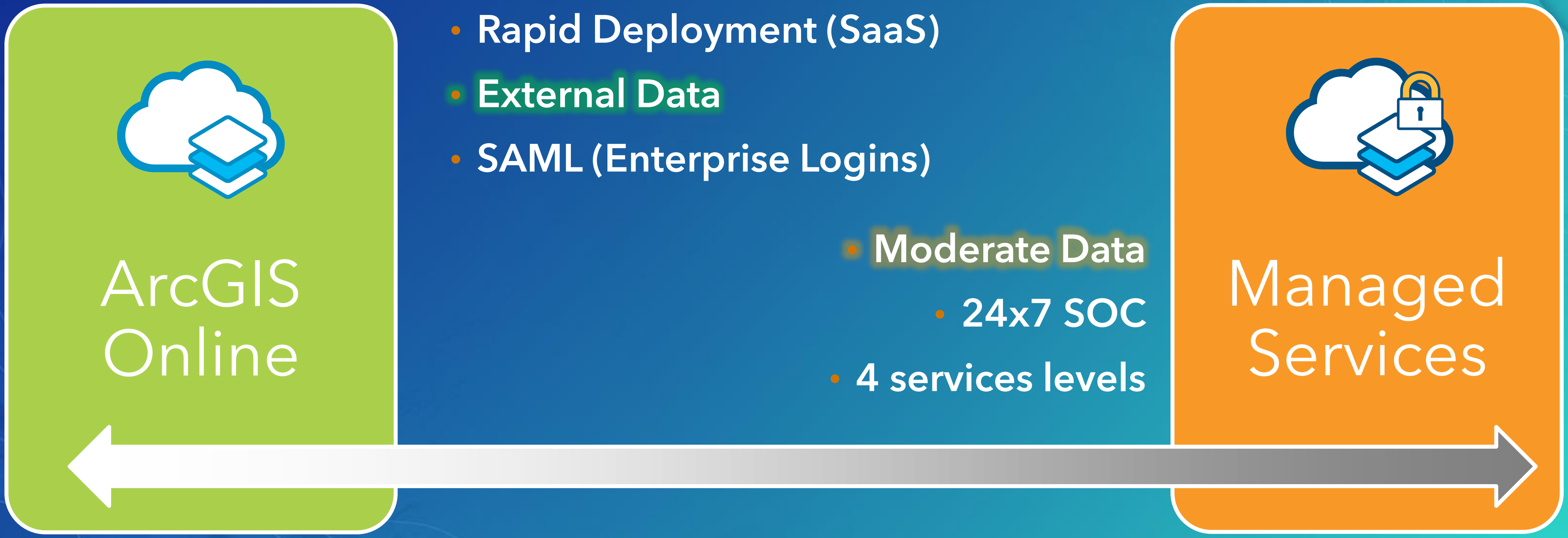


- Pros
  - ArcGIS Online operates as a central discovery portal
  - Mobile users / Collector App access ArcGIS Online directly
  - Enterprise logins utilized for employee SSO experience
- Cons
  - Two separate ArcGIS Online orgs to manage
  - Partner logins managed within ArcGIS Online
  - No SSO experience for Partners

Deployment Architecture

User Scenario – ArcGIS Online + Managed Services

I want to share sensitive internal data, but provide subsets to external and public users. I also don’t want to have to manage servers/infrastructure.



ArcGIS Online

- Rapid Deployment (SaaS)
- External Data
- SAML (Enterprise Logins)

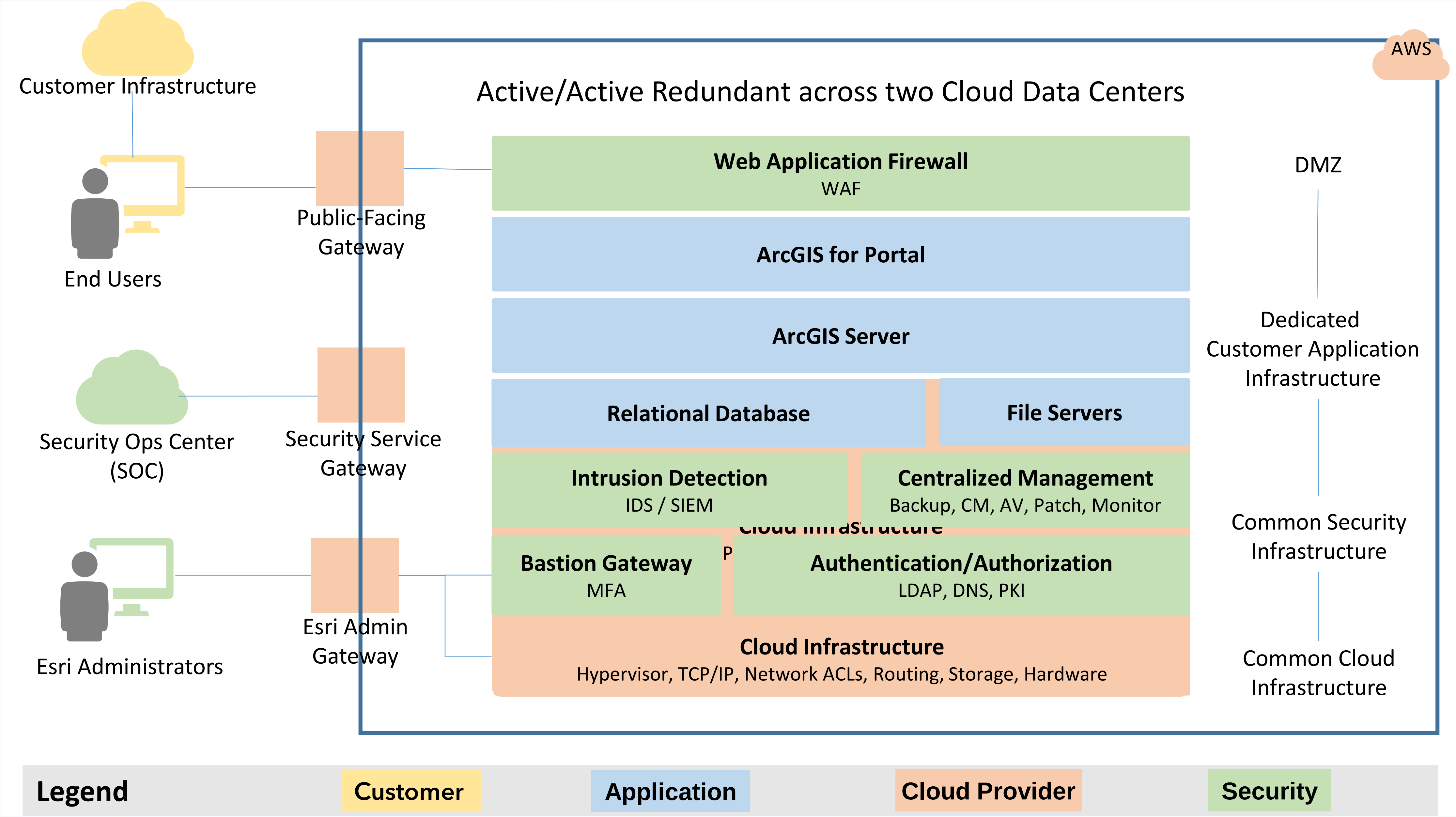
- Moderate Data
- 24x7 SOC
- 4 services levels

Managed Services

Example: *US Census utilizes Managed Services Adv Plus offering for Public information*

Deployment Architecture

Esri Managed Cloud Services



Customer Infrastructure

End Users

Public-Facing Gateway

Security Ops Center (SOC)

Security Service Gateway

Esri Administrators

Esri Admin Gateway

AWS

Active/Active Redundant across two Cloud Data Centers

Web Application Firewall
WAF

ArcGIS for Portal

ArcGIS Server

Relational Database

File Servers

Intrusion Detection
IDS / SIEM

Centralized Management
Backup, CM, AV, Patch, Monitor

Bastion Gateway
MFA

Authentication/Authorization
LDAP, DNS, PKI

Cloud Infrastructure
Hypervisor, TCP/IP, Network ACLs, Routing, Storage, Hardware

DMZ

Dedicated Customer Application Infrastructure

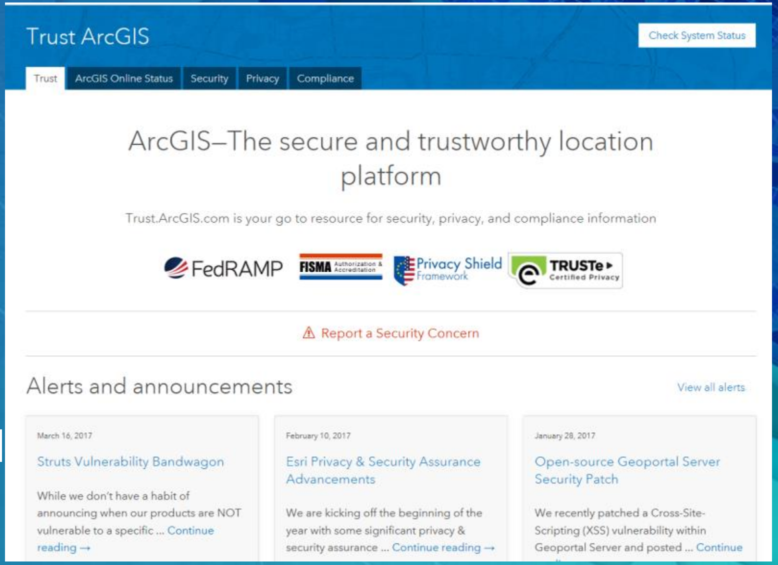
Common Security Infrastructure

Common Cloud Infrastructure

Legend **Customer** **Application** **Cloud Provider** **Security**

Deployment Architecture

Common ArcGIS Online Questions



ArcGIS–The secure and trustworthy location platform

Trust.ArcGIS.com is your go to resource for security, privacy, and compliance information

Alerts and announcements

March 16, 2017
Struts Vulnerability Bandwagon
While we don't have a habit of announcing when our products are NOT vulnerable to a specific ... Continue reading →

February 10, 2017
Esri Privacy & Security Assurance Advancements
We are kicking off the beginning of the year with some significant privacy & security assurance ... Continue reading →

January 28, 2017
Open-source Geoportal Server Security Patch
We recently patched a Cross-Site-Scripting (XSS) vulnerability within Geoportal Server and posted ... Continue

1. **Where is my data?**
   - All ArcGIS Online customer data resides within US Data centers on US soil

2. **Is my information encrypted?**
   - Organization administrator can force TLS encryption for all communications
   - ArcGIS Online does not encrypt customer data at rest

3. **Is my data locked into ArcGIS Online?**
   - No, customer can download data back to their organization via shapefiles, CSVs, or original publication package

4. **How do I know if ArcGIS Online was affected by the latest major Internet vulnerability?**
   - Trust.ArcGIS.com announcements
   - Answers to all of the above questions and more available

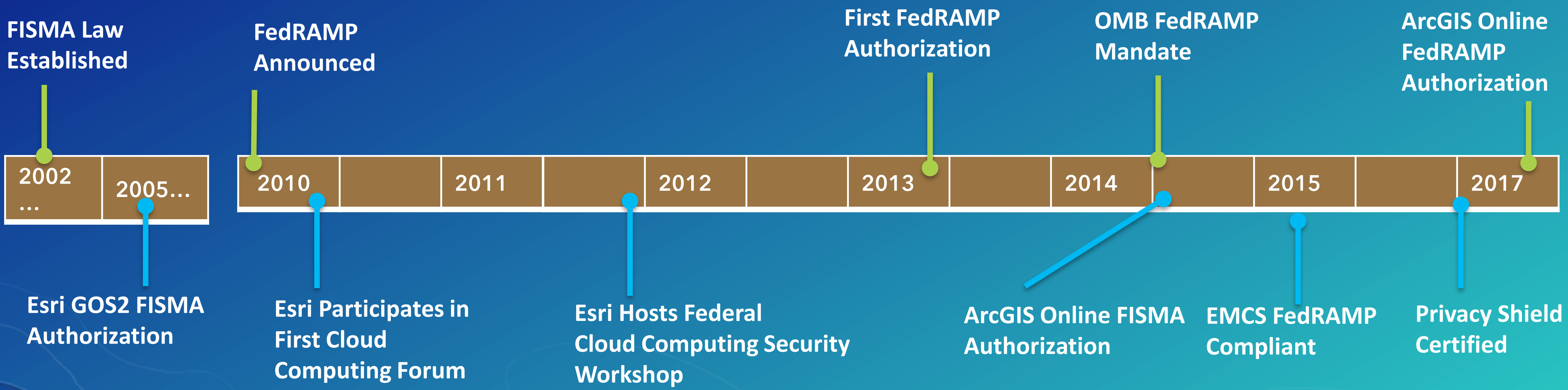
Compliance

Compliance

- Milestones
- Esri Corporate
- Cloud Infrastructure Providers
- Products and Services
- Solution Guidance

Compliance

Milestones



FISMA Law Established

FedRAMP Announced

First FedRAMP Authorization

OMB FedRAMP Mandate

ArcGIS Online FedRAMP Authorization

Esri GOS2 FISMA Authorization

Esri Participates in First Cloud Computing Forum

Esri Hosts Federal Cloud Computing Security Workshop

ArcGIS Online FISMA Authorization

EMCS FedRAMP Compliant

Privacy Shield Certified

Esri has actively participated in hosting and advancing secure compliant solutions for over a decade

Compliance

Corporate

- ISO 27001
  - Esri's Corporate Security Charter
- Privacy Assurance
  - EU-U.S. Privacy Shield self-certified
    - General Esri Privacy Statement
    - Products & Services Privacy Statement Supplement
  - TRUSTed cloud certified
  - General Data Protection Regulation (GDPR)
    - Active alignment project in place for May 2018 deadline

Privacy Shield

TRUSTe
Certified Privacy

Compliance

Cloud Infrastructure Providers

- ArcGIS Online Utilizes World-Class Cloud Infrastructure Providers
  - Microsoft Azure
  - Amazon Web Services

Cloud Infrastructure Security Compliance

Executive Office of the President of the United States
GSA
CIO COUNCIL
FedRAMP
Department of Defense United States of America
NIST
U.S. Department of Homeland Security

Compliance

Product, Service, Solution

- Product Based Initiatives
  - ArcGIS Server 10.3+ - DISA STIG
  - ArcGIS Desktop 9.3+ - USGCB
  - ArcGIS Pro 1.4.1+ - USGCB
- Service Based Initiatives
  - ArcGIS Online (Multi-tenant) – FISMA Low
  - EMCS Advanced Plus (Single-tenant) – FedRAMP Moderate
- Solution Based Guidance
  - CJIS- Law enforcement - Started
  - HIPAA – Healthcare - Future

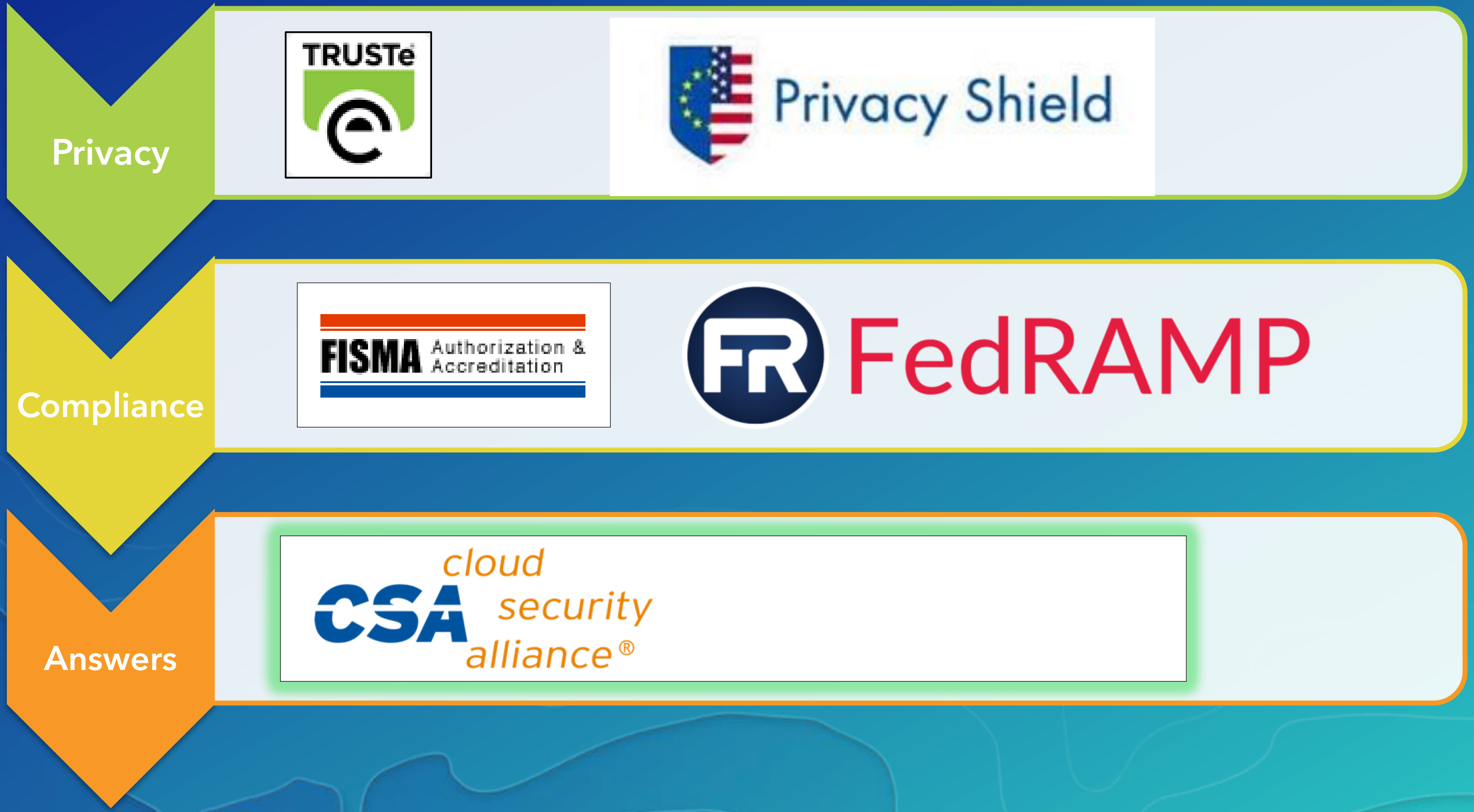
Compliance

FedRAMP

- New FedRAMP Tailored Low Authorization Program being released August 2017
- Program targeted for SaaS offerings hosted on FedRAMP authorized cloud infrastructure providers
  - Great fit for ArcGIS Online
  - Advancements made during this authorization include
    - Incorporating cloud-specific security control guidance of FedRAMP beyond FISMA
    - Shifts from NIST 800-53 Rev 3 security controls to Rev 4 (current release)
    - Incorporate ArcGIS Online capabilities from both AWS and MS Azure such as Hosted Feature Services
  - Goal is to complete ArcGIS Online authorization before end of 2017
- Details on new Tailored Low program: https://tailored.fedramp.gov/policy/

Compliance

Summary Across ArcGIS Online



Privacy

Compliance

Answers

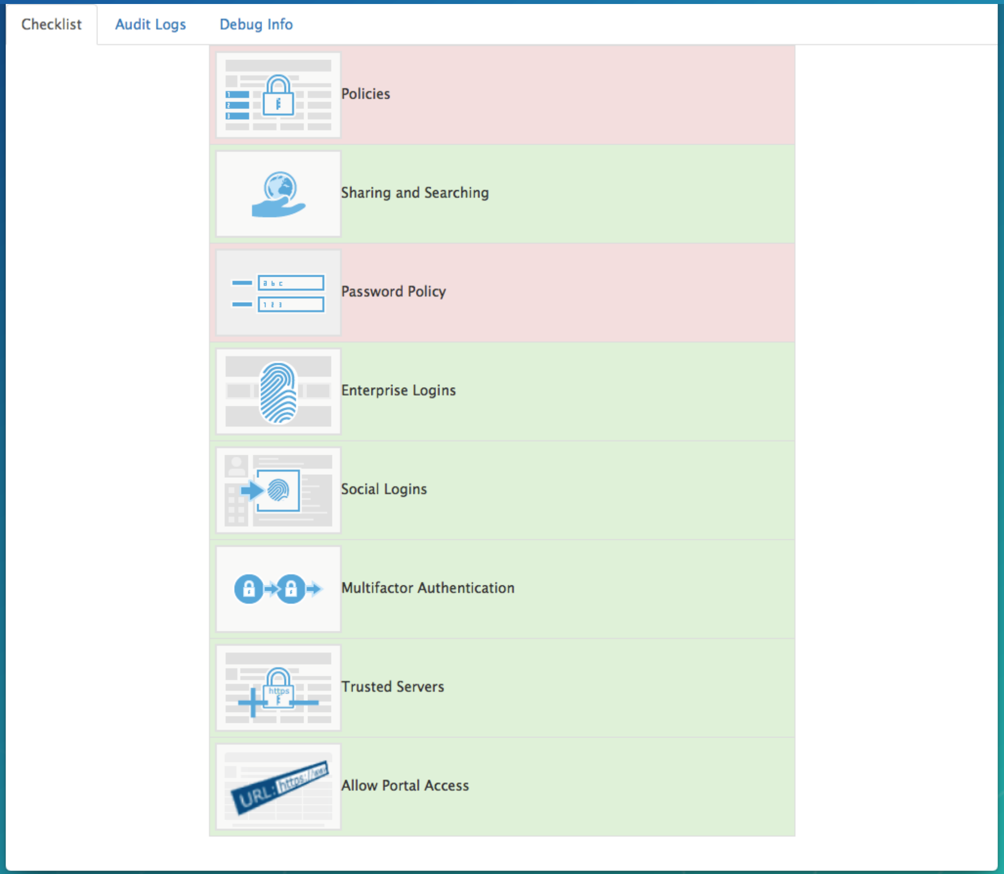
TRUSTe
Privacy Shield
FISMA Authorization & Accreditation
FR FedRAMP
CSA cloud security alliance®

Trust.ArcGIS.com

Compliance

Validation Tool

- Checklist validates your org settings/usage against secure best practice recommendations
- Audit log provides a summary of user actions
- Tool in beta form at this time and looking for feedback
- Interested? SecureSoftware@Esri.com



Policies

Sharing and Searching

Password Policy

Enterprise Logins

Social Logins

Multifactor Authentication

Trusted Servers

Allow Portal Access

Summary

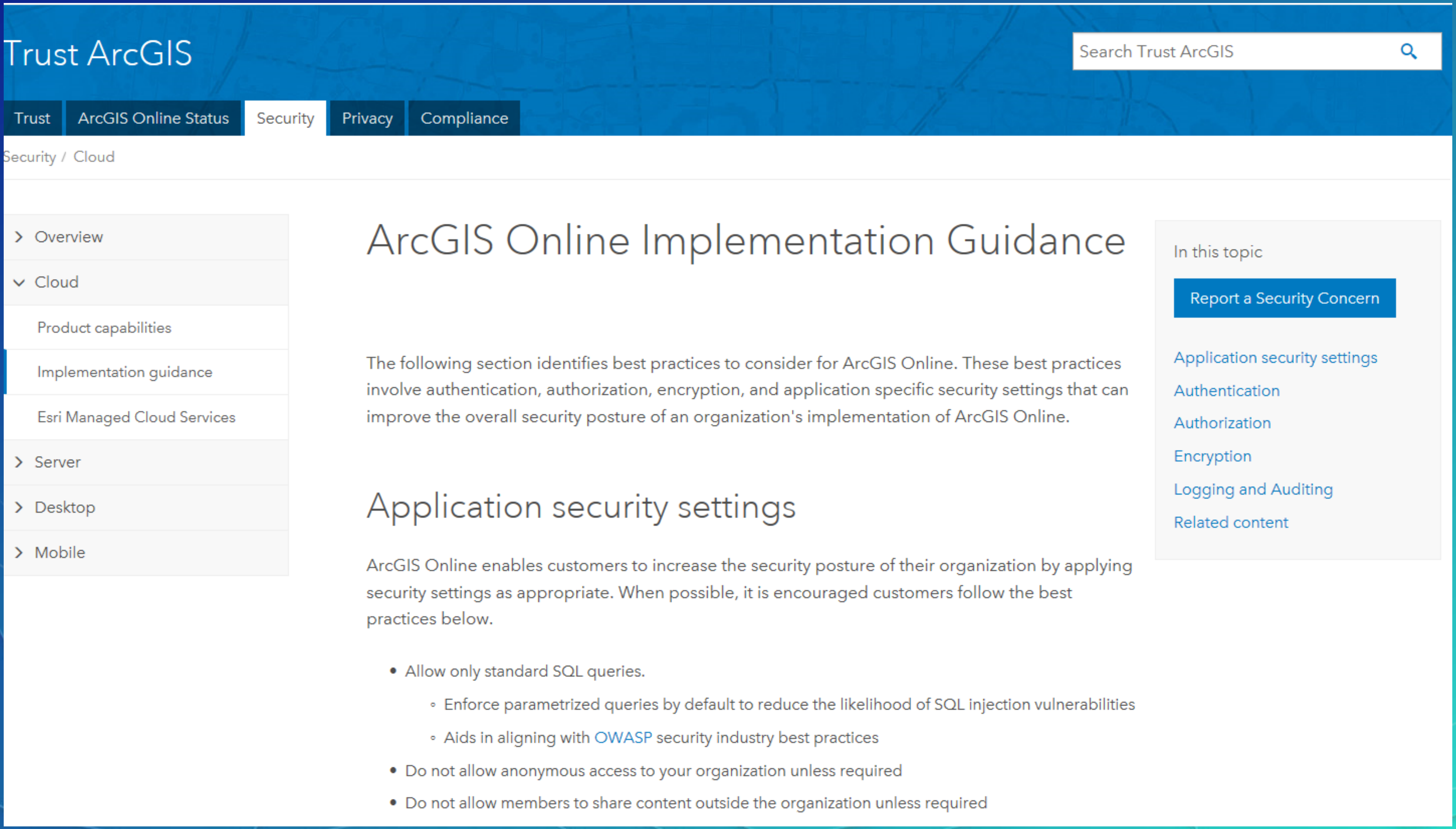
- ArcGIS Online security capabilities continue to advance

- Utilizes World-Class Cloud Infrastructure Providers

- Extensive security, privacy, compliance, and status info available
  - Trust.ArcGIS.com
  - In-depth Cloud Security Alliance (CSA) answers readily available
  - New security best practice validation tool

- Upcoming ArcGIS Online FedRAMP Tailored Agency Authorization
  - Cross-cloud provider authorization Azure/AWS

Want to Learn More?



ArcGIS Online Implementation Guidance

The following section identifies best practices to consider for ArcGIS Online. These best practices involve authentication, authorization, encryption, and application specific security settings that can improve the overall security posture of an organization's implementation of ArcGIS Online.

Application security settings

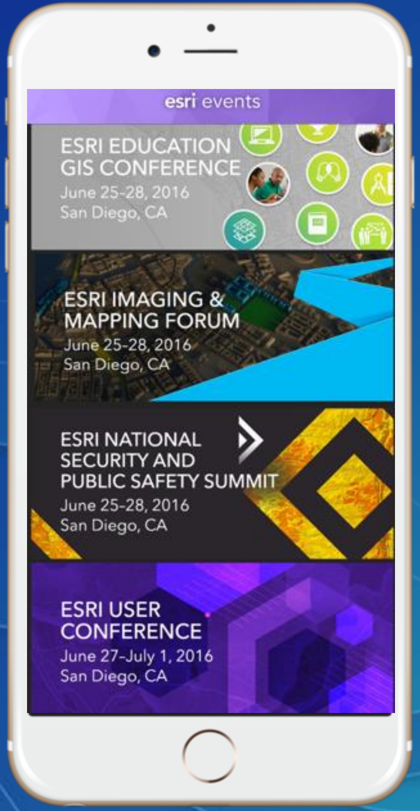
ArcGIS Online enables customers to increase the security posture of their organization by applying security settings as appropriate. When possible, it is encouraged customers follow the best practices below.

- Allow only standard SQL queries.
  - Enforce parametrized queries by default to reduce the likelihood of SQL injection vulnerabilities
  - Aids in aligning with OWASP security industry best practices
- Do not allow anonymous access to your organization unless required
- Do not allow members to share content outside the organization unless required

Please take our Survey

Your feedback allows us to help maintain high standards and to help presenters

Find your event in the Esri Events App



esri events

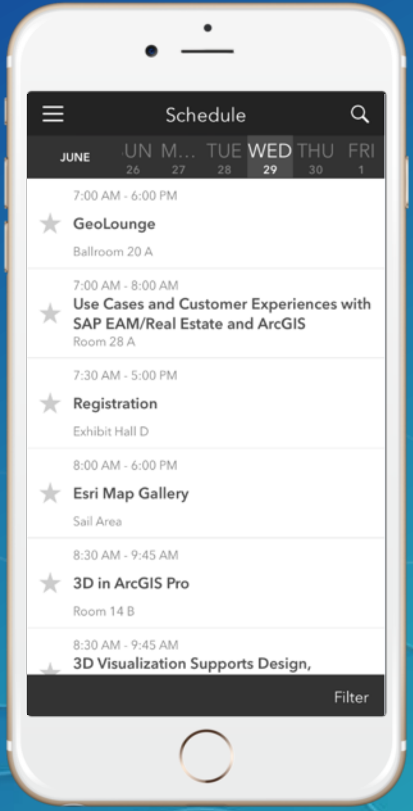
ESRI EDUCATION GIS CONFERENCE
June 25-28, 2016
San Diego, CA

ESRI IMAGING & MAPPING FORUM
June 25-28, 2016
San Diego, CA

ESRI NATIONAL SECURITY AND PUBLIC SAFETY SUMMIT
June 25-28, 2016
San Diego, CA

ESRI USER CONFERENCE
June 27-July 1, 2016
San Diego, CA

Find the session you want to review



Schedule

JUNE UN 26 M... 27 TUE 28 WED 29 THU 30 FRI 1

7:00 AM - 6:00 PM
GeoLounge
Ballroom 20 A

7:00 AM - 8:00 AM
Use Cases and Customer Experiences with SAP EAM/Real Estate and ArcGIS
Room 28 A

7:30 AM - 5:00 PM
Registration
Exhibit Hall D

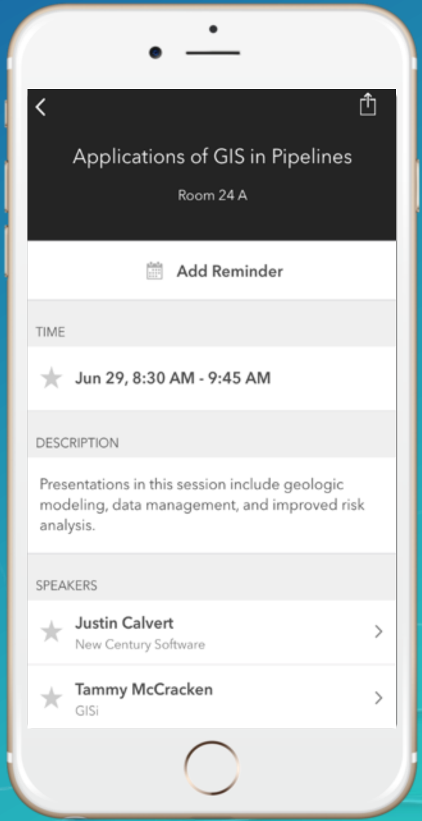
8:00 AM - 6:00 PM
Esri Map Gallery
Sail Area

8:30 AM - 9:45 AM
3D in ArcGIS Pro
Room 14 B

8:30 AM - 9:45 AM
3D Visualization Supports Design,

Filter

Scroll down to the bottom of the session



Applications of GIS in Pipelines
Room 24 A

Add Reminder

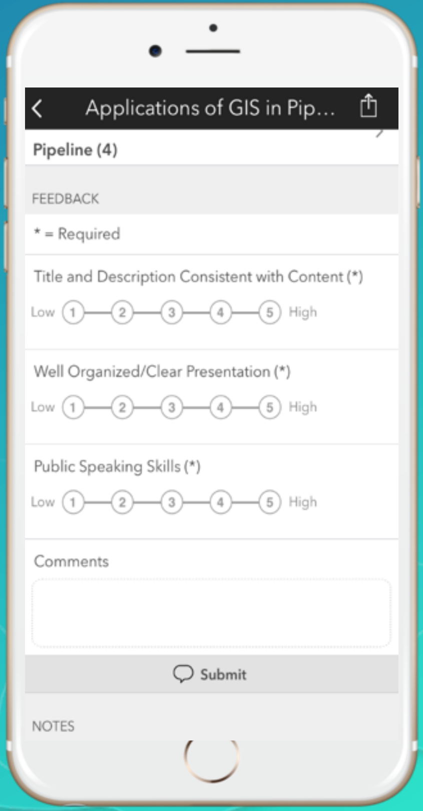
TIME
Jun 29, 8:30 AM - 9:45 AM

DESCRIPTION
Presentations in this session include geologic modeling, data management, and improved risk analysis.

SPEAKERS
Justin Calvert
New Century Software

Tammy McCracken
GISi

Answer survey questions and submit



Applications of GIS in Pip...

Pipeline (4)

FEEDBACK

* = Required

Title and Description Consistent with Content (*)
Low ① ② ③ ④ ⑤ High

Well Organized/Clear Presentation (*)
Low ① ② ③ ④ ⑤ High

Public Speaking Skills (*)
Low ① ② ③ ④ ⑤ High

Comments

Submit

NOTES

esri

THE
SCIENCE
OF
WHERE