



ArcGIS Online: A Security, Privacy & Compliance Overview

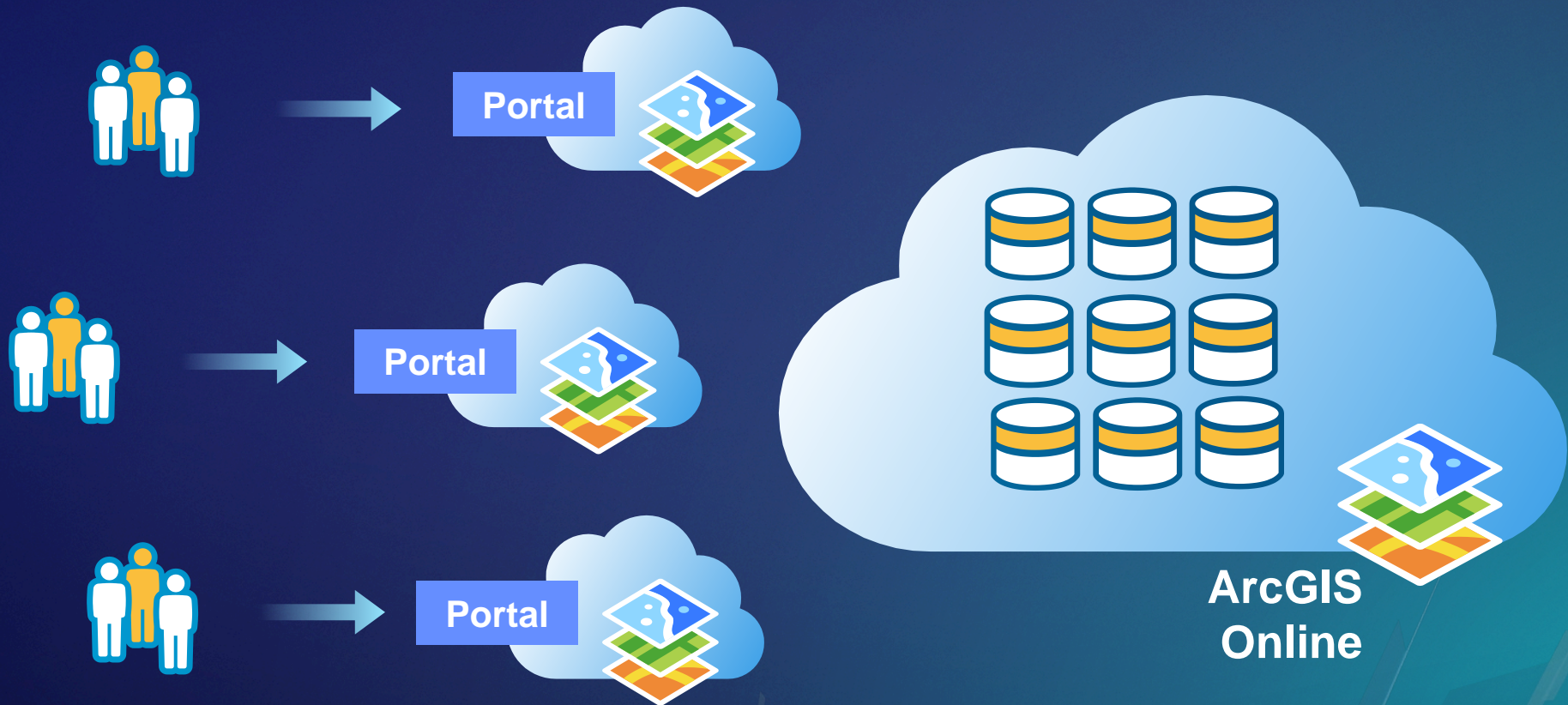
Andrea Rosso – Lead Architect

Michael Young – CISO Products

An abstract 3D architectural graphic on the right side of the slide. It features various geometric shapes in shades of blue, teal, orange, and red, some with topographic contour lines. The shapes are layered and angled, creating a sense of depth and perspective.

**GIS
INSPIRING
WHAT'S
NEXT**

ArcGIS Online – A Multi-Tenant System



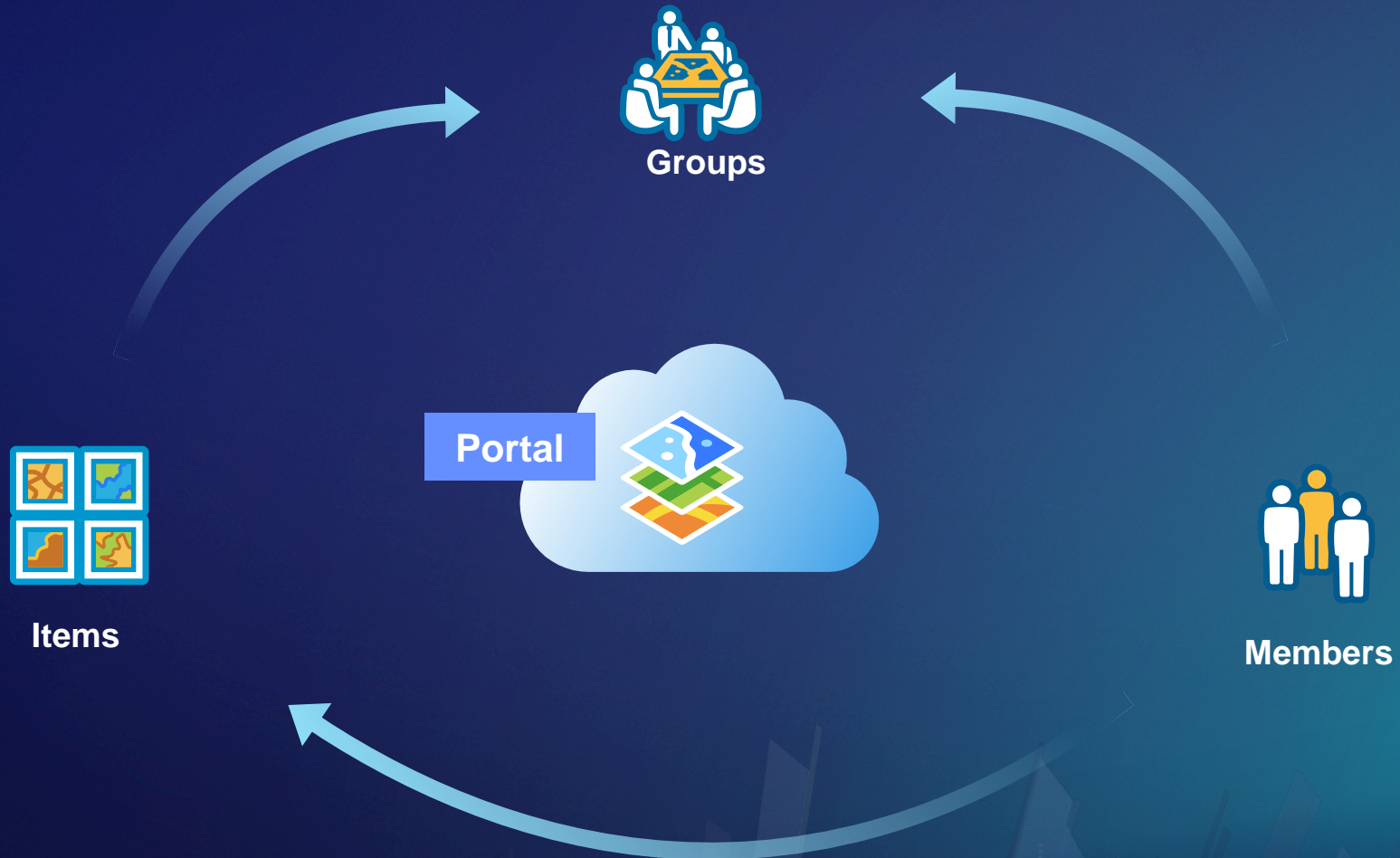
Agenda

- **Platform Security**
- **Deployment Architecture**
- **Compliance (FedRAMP/GDPR & more)**
- **New Security Advisor Tool**

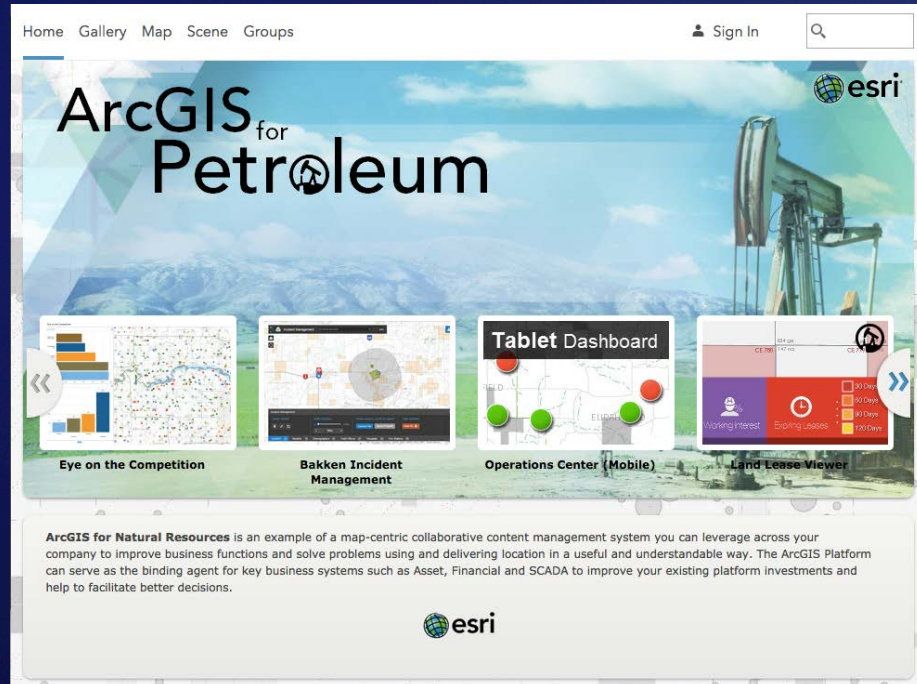
Platform Security

Andrea Rosso

Portal Information Model













Portal



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

Items

1 - 5 of 5 in uc2018sec Sort by: Date Modified ▾ ↓

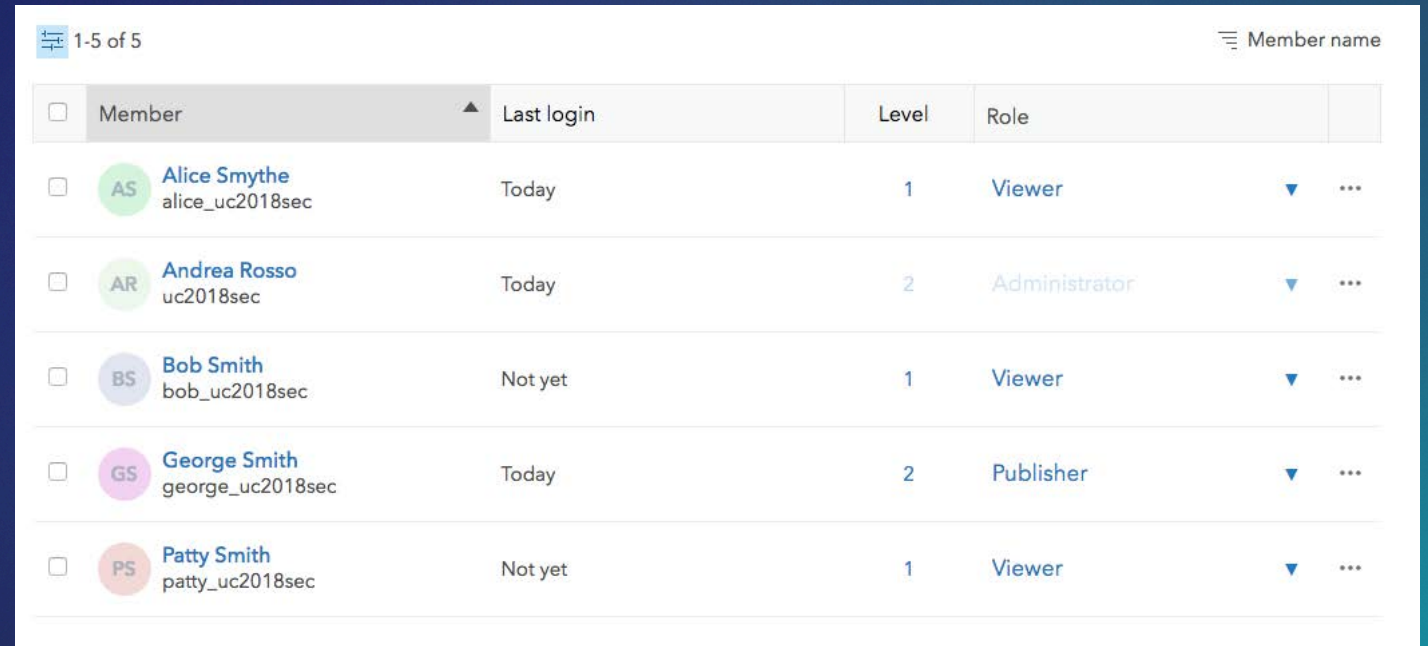
<input type="checkbox"/>	Title			Modified
<input type="checkbox"/>	 Store Closures	CSV	 ★ ...	Jul 6, 2018
<input type="checkbox"/>	 Buildings	Web Scene	 ★ ...	Jul 6, 2018
<input type="checkbox"/>	 Hazards	Feature Layer (hosted)	 ★ ...	Jul 6, 2018
<input type="checkbox"/>	 Schools	Shapefile	 ★ ...	Jul 6, 2018
<input type="checkbox"/>	 USA Zip Codes	Layer Package	 ★ ...	Jul 6, 2018

- **Typed**
 - Web Map
 - Services
 - Data
 - ...

- **Private by default**
- **Can Share to**
 - Groups
 - Organization
 - Everyone/Public






Members (Users)

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



1-5 of 5

Member name

<input type="checkbox"/>	Member	Last login	Level	Role	
<input type="checkbox"/>	 Alice Smythe alice_uc2018sec	Today	1	Viewer	▼ ...
<input type="checkbox"/>	 Andrea Rosso uc2018sec	Today	2	Administrator	▼ ...
<input type="checkbox"/>	 Bob Smith bob_uc2018sec	Not yet	1	Viewer	▼ ...
<input type="checkbox"/>	 George Smith george_uc2018sec	Today	2	Publisher	▼ ...
<input type="checkbox"/>	 Patty Smith patty_uc2018sec	Not yet	1	Viewer	▼ ...

Roles

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

Roles

Role Name:

Description:

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

Minimum Level: 1 2

General Privileges

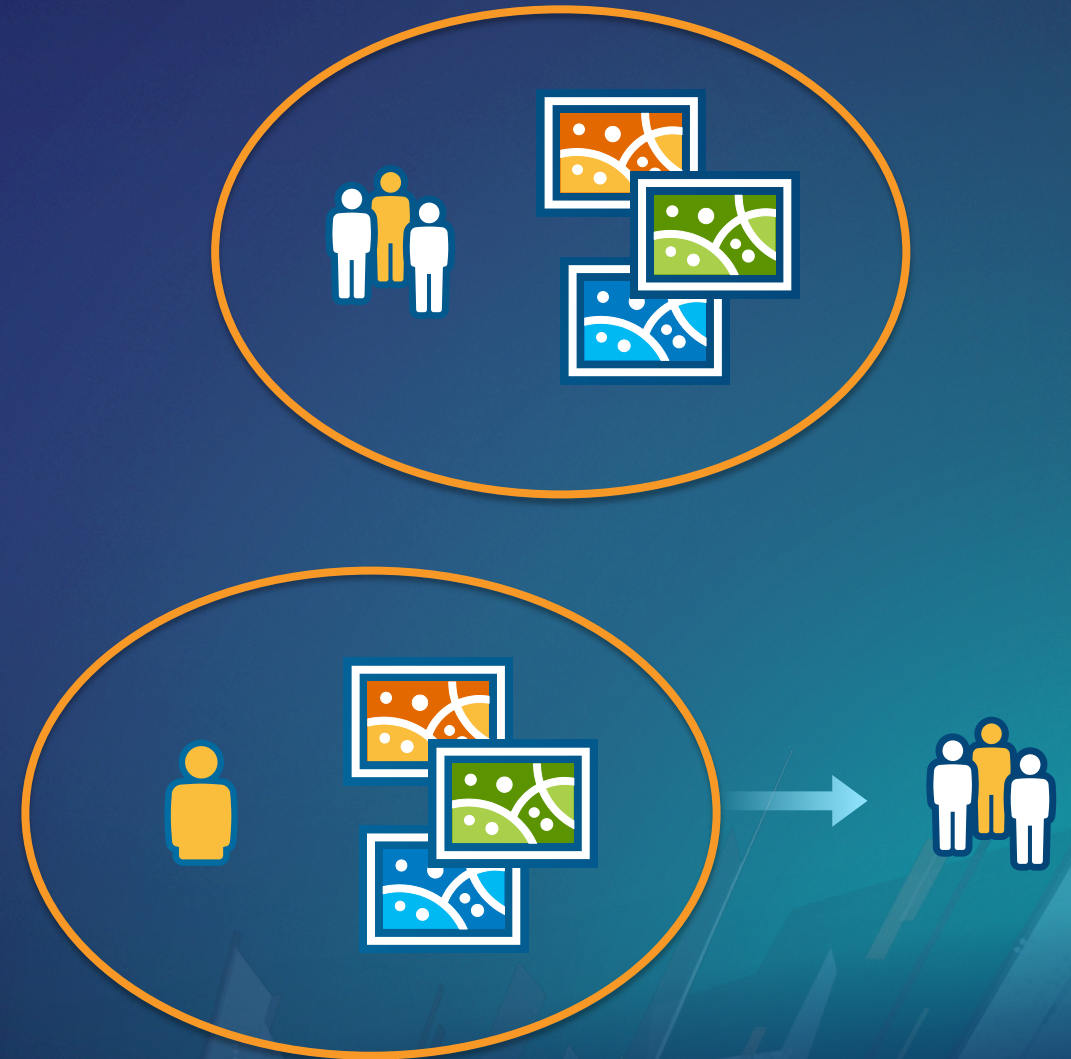
<input checked="" type="checkbox"/> Members [-]	<input type="checkbox"/> Groups [-]	<input type="checkbox"/> Content [-]
<input checked="" type="checkbox"/> View	<input type="checkbox"/> Create, update, and delete	<input type="checkbox"/> Create, update, and delete
	<input checked="" type="checkbox"/> Join organizational groups	<input type="checkbox"/> Publish hosted feature layers
	<input type="checkbox"/> Join external groups	<input type="checkbox"/> Publish hosted tile layers
	<input checked="" type="checkbox"/> View groups shared with organization	<input type="checkbox"/> Publish hosted scene layers
<input type="checkbox"/> Sharing [-]	<input type="checkbox"/> Premium Content [-]	<input type="checkbox"/> Features [-]
<input type="checkbox"/> Share with groups	<input type="checkbox"/> Geocoding	<input checked="" type="checkbox"/> Edit
<input type="checkbox"/> Share with organization	<input type="checkbox"/> Network Analysis	<input type="checkbox"/> Edit with full control
<input type="checkbox"/> Share with public	<input type="checkbox"/> Spatial Analysis	
<input type="checkbox"/> Make groups visible to organization	<input type="checkbox"/> GeoEnrichment	
<input type="checkbox"/> Make groups visible to public	<input type="checkbox"/> Demographics	
	<input type="checkbox"/> Elevation Analysis	

Administrative Privileges

<input type="checkbox"/> Members [-]	<input type="checkbox"/> Groups [-]	<input type="checkbox"/> Content [-]
<input type="checkbox"/> View all	<input type="checkbox"/> View all	<input type="checkbox"/> View all
<input type="checkbox"/> Update	<input type="checkbox"/> Update	<input type="checkbox"/> Update
<input type="checkbox"/> Delete	<input type="checkbox"/> Delete	<input type="checkbox"/> Delete
<input type="checkbox"/> Invite	<input type="checkbox"/> Reassign ownership	<input type="checkbox"/> Reassign ownership
<input type="checkbox"/> Disable	<input type="checkbox"/> Assign members	<input type="checkbox"/> Manage categories
<input type="checkbox"/> Change roles	<input type="checkbox"/> Link to enterprise group	
<input type="checkbox"/> Manage licenses	<input type="checkbox"/> Create with update capabilities	

Groups

- Contain Items and Members
- Members 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 Members must be in Org
 - Capability cannot be toggled
- **Use Cases**
 - Shift Operators
 - Collaborative Editing

Who can view this group?

- Only group members
- People in the organization (Client Team testing organization)
- 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
- Members of an enterprise group
- Anyone

Who can contribute content to the group?

- Group members
- Only group owner and managers

What items in the group can its members update? [?](#)

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

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

Feature Layer (hosted)

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
- Add and update features
- Add features
- Update features
- Update attributes only

• 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?

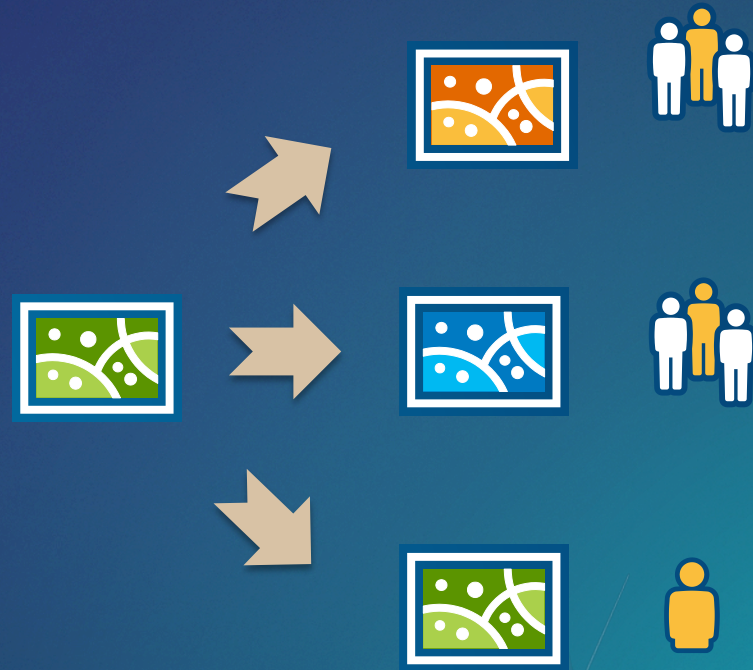
- You
- Administrators
- Data curators with the appropriate privileges

Export Data

- Allow others to export to different formats.

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 esri

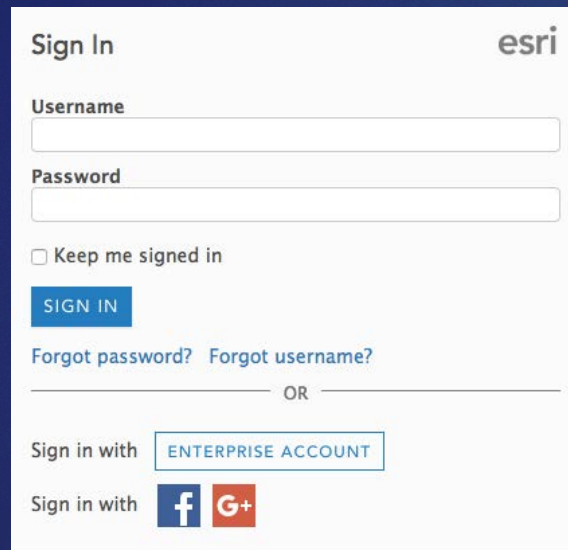
Username

Password

Keep me signed in

[Forgot password?](#) [Forgot username?](#)

ArcGIS Account



Sign In esri

Username



Password

Keep me signed in

[Forgot password?](#) [Forgot username?](#)

OR

Sign in with

Sign in with  

Social Account



Sign in to ArcGIS for Petroleum esri


OR

Enterprise Account

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
- Members 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
Andrea Rosso (uc2018sec)
George Smith (george_uc2018sec)

Click a name to remove.

Designated Administrators
Andrea Rosso (uc2018sec)
George Smith (george_uc2018sec)

Password Policies

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

Password Policy ✕

Set the password policy for members in your organization with ArcGIS accounts. Member passwords may not match their username and must follow these rules:

Is at least characters long

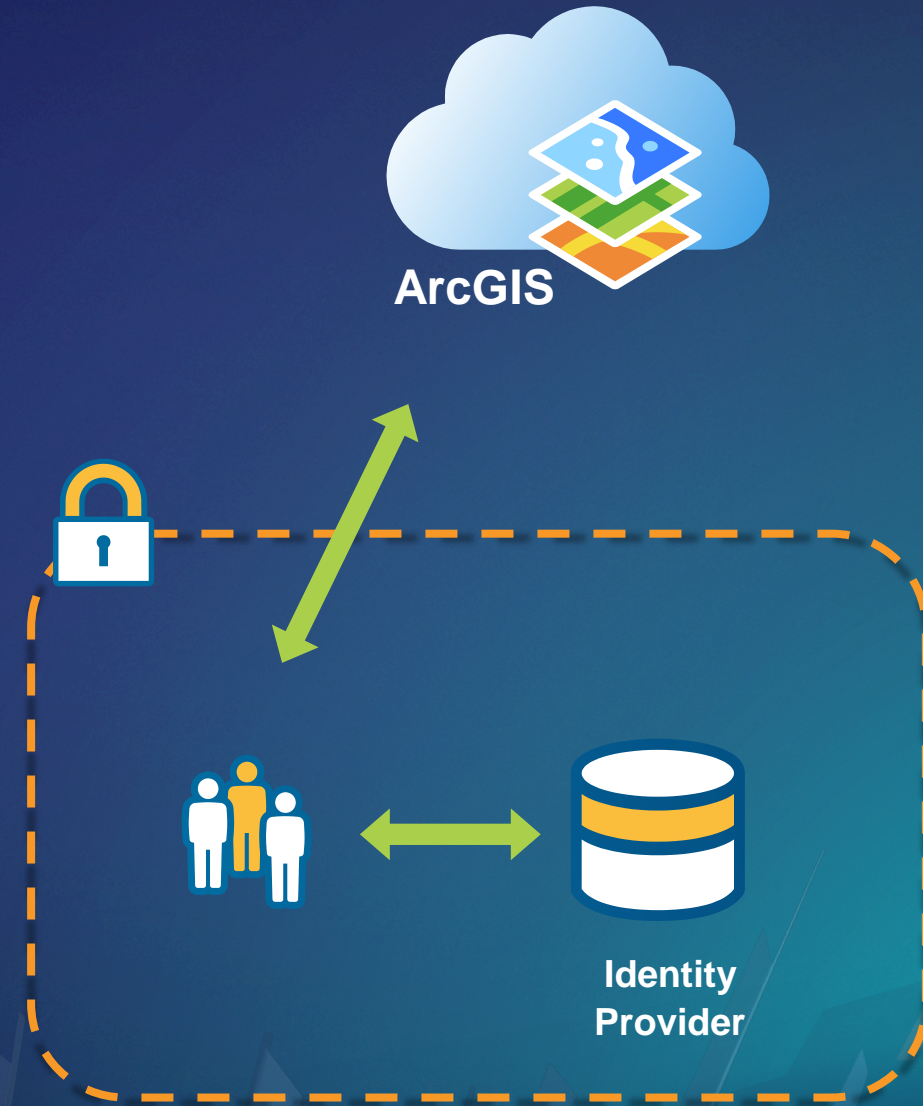
- Contains at least one letter (A-Za-z)
- Contains at least one upper case letter (A-Z)
- Contains at least one lower case letter (a-z)
- Contains at least one number (0-9)
- Contains at least one special (non-alphanumeric) character

Password will expire after days

Members may not reuse their last passwords

Enterprise Identities

- Use your own identity provider
 - SAML 2.0
 - ADFS
 - NetIQ Access Manager
 - Shibboleth
 -
- Can add members:
 - Automatically upon login
 - With an Invitation
- Can use ArcGIS Online identities with Enterprise Identities
- Enterprise groups are now supported
- One SAML IDP or SAML Federation



Application Trust Boundaries




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, uc2018sec.maps.arcgis.com.
[What does this mean?](#)
- Allow only standard SQL queries.
- Allow members to edit biographical information and who can see their profile.

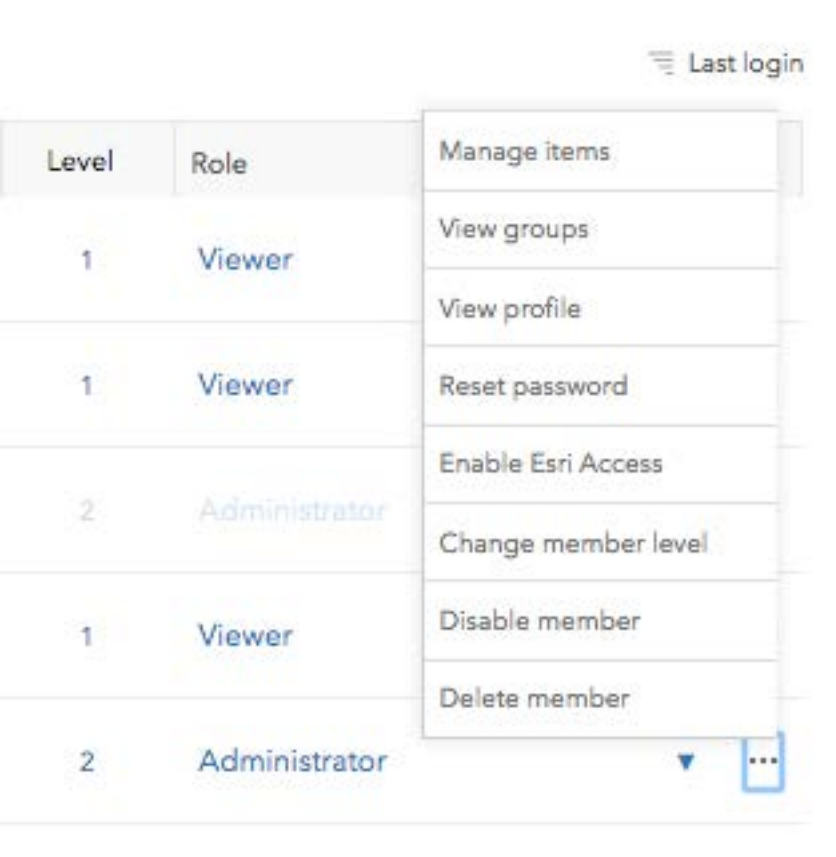
Sharing and Searching



- Members can share content publicly.
- Members can search for content outside the organization.
- Show social media links on item and group pages.

Administrator Controls on Members

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

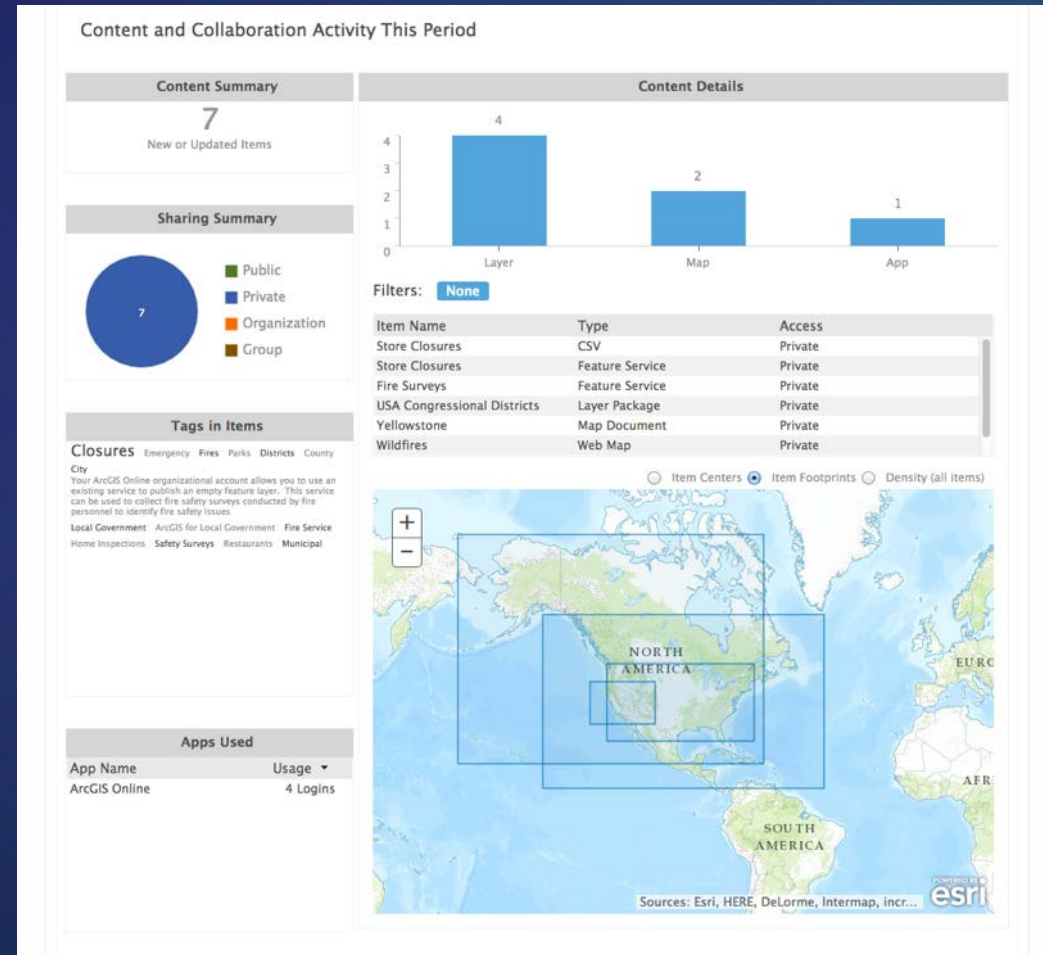


The screenshot shows a user management interface with a table of members and a context menu. The table has columns for Level and Role. The context menu is open over the last row, which is an Administrator (Level 2). The menu items are: Manage items, View groups, View profile, Reset password, Enable Esri Access, Change member level, Disable member, and Delete member. There is also a 'Last login' label in the top right corner of the table area.

Level	Role	
1	Viewer	
1	Viewer	
2	Administrator	
1	Viewer	
2	Administrator	▼ ...

Keeping Track of Usage

- Status Reports
 - Credits
 - Content
 - Members
 - Groups



Recommendations

- **HTTPS Only**
 - **Standardized Queries Only**
 - **Setup Admin Contacts**
 - **MFA or your own IDP**
 - **Don't make Editabled Feature Layers Public and Use Views**
 - **Setup Custom Roles and restrict full Admins**
- **Private Orgs**
 - **Disable Public Sharing**
 - **Disable Anonymous Org Access**

Deployment Architecture

Michael Young

Deployment Architecture

Options



ArcGIS
Online



Managed
Services



Cloud
Images

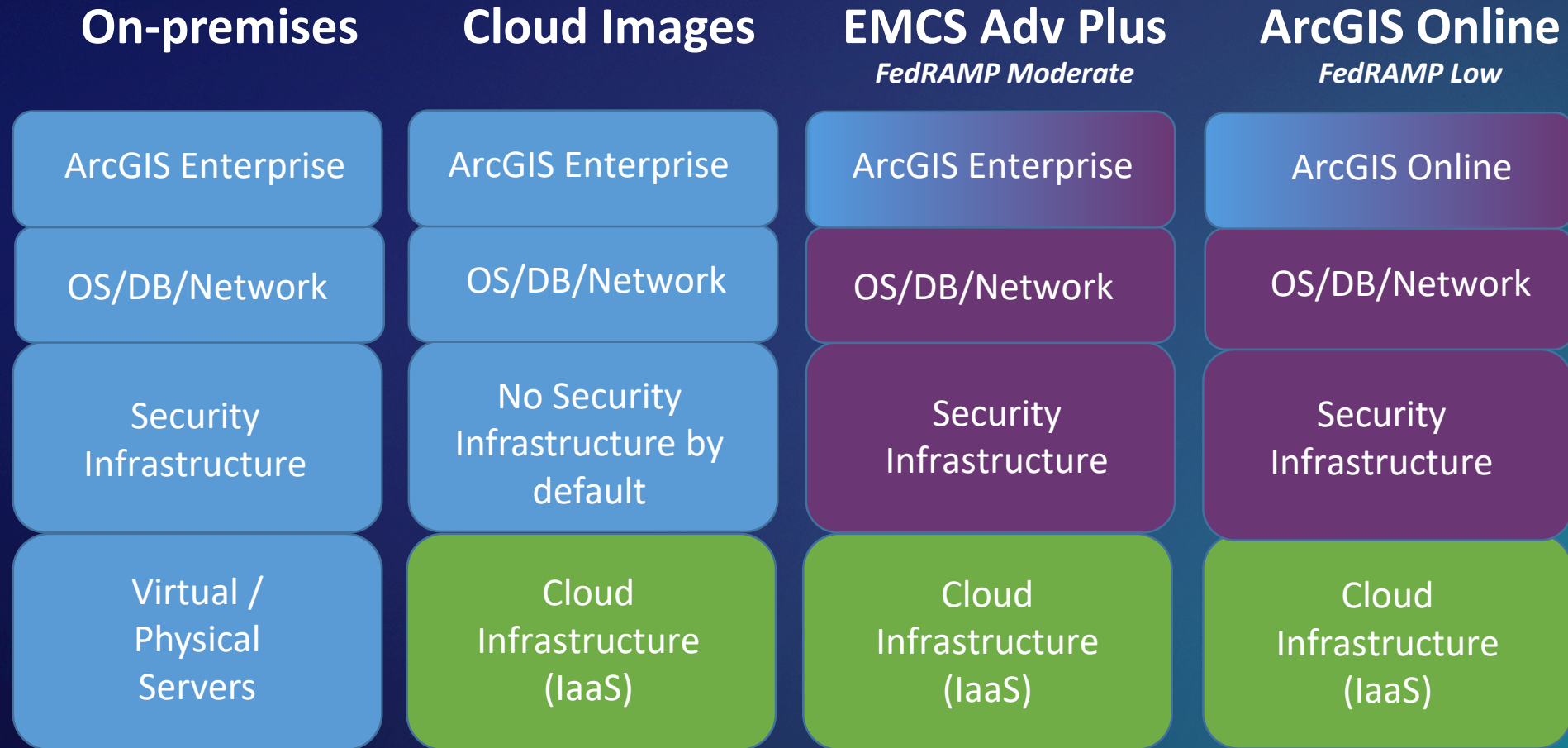


On
Premises



Deployment Architecture

Responsibility



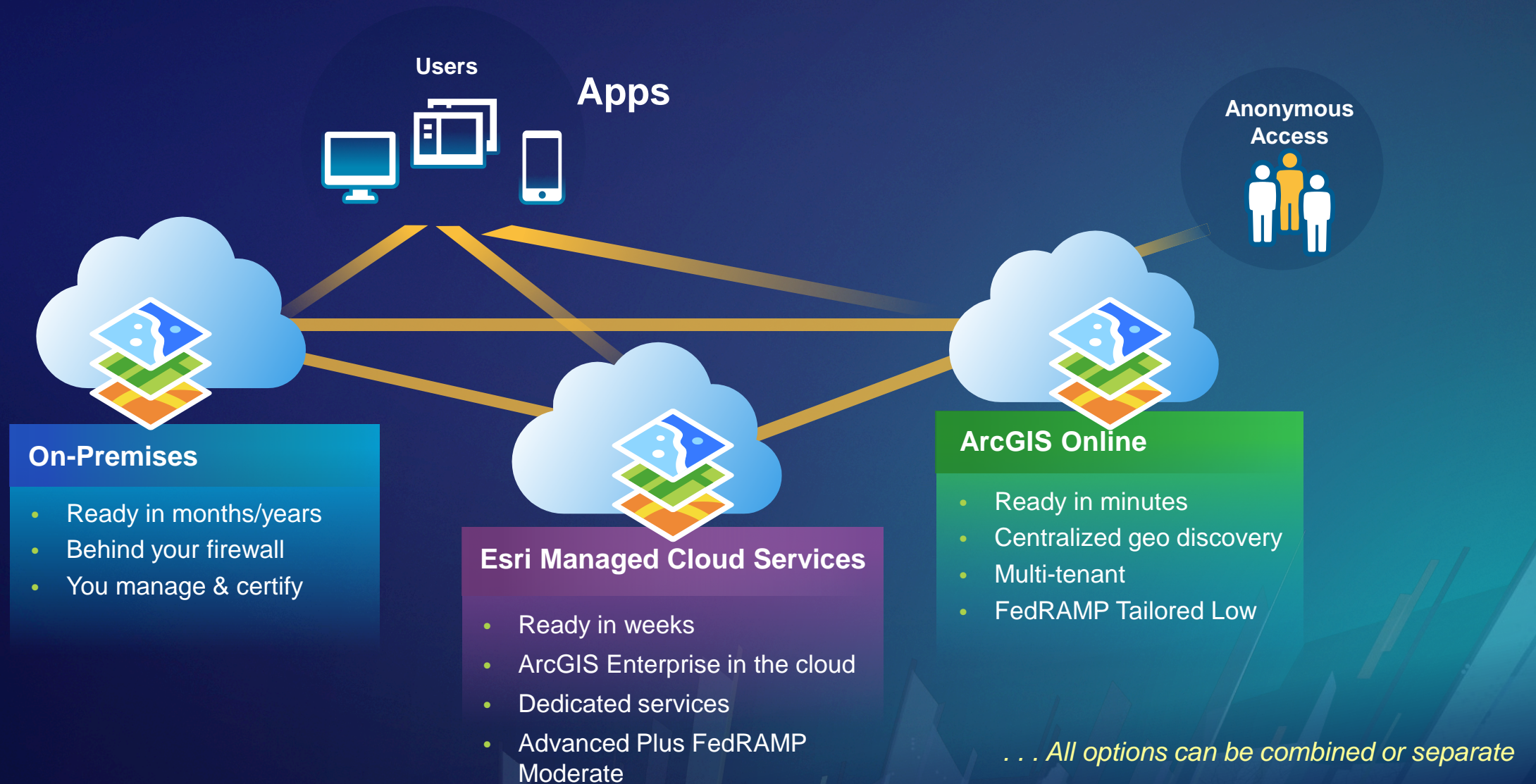
Customer Responsibility 

Esri Responsibility 

CSP Responsibility 

Deployment Architecture

Hosting Options



Deployment Architecture

User Scenario – ArcGIS Online Alone

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



ArcGIS
Online

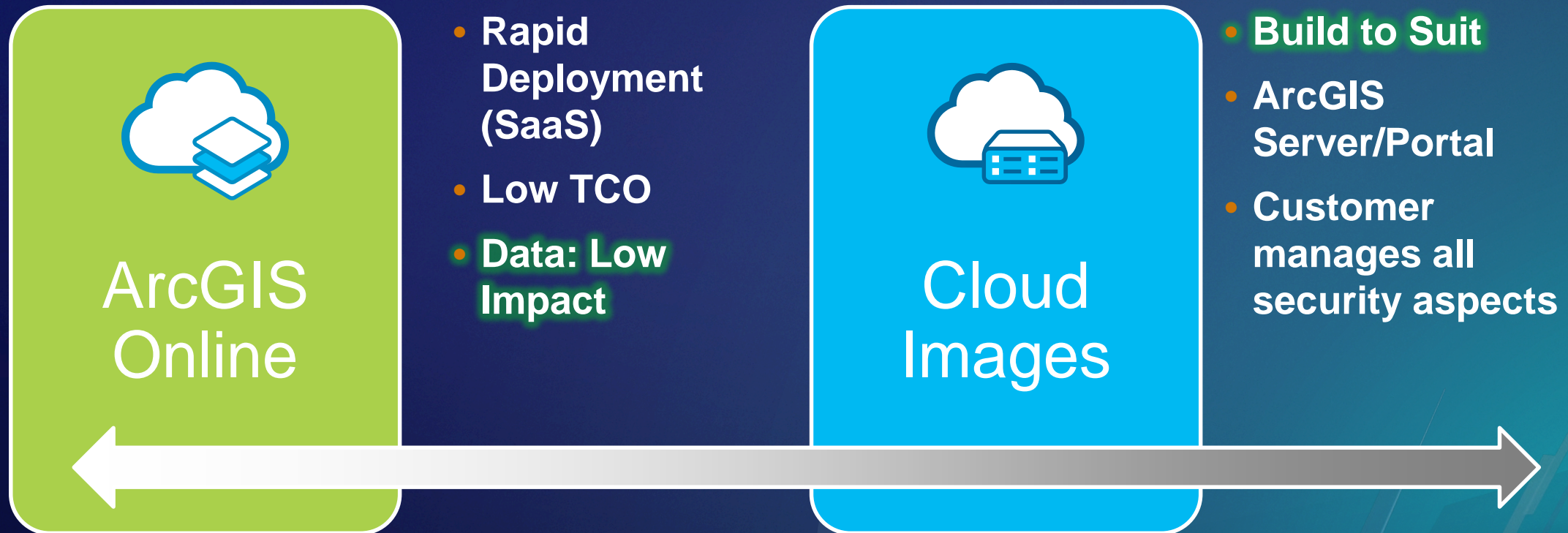
- Rapid Deployment (SaaS)
- Low TCO
- Utilize content / Basemaps
- **Data: Low Impact**



Deployment Architecture

User Scenario – ArcGIS Online + Cloud Images

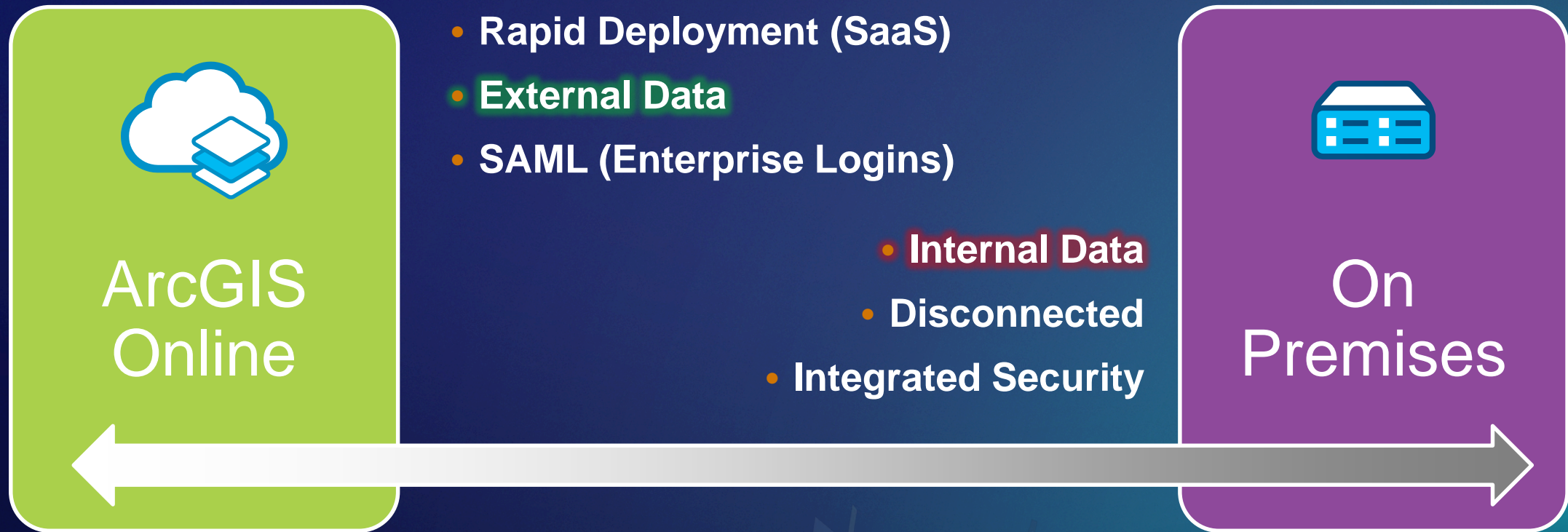
I need to pilot a solution that requires basemaps and some ArcGIS Server specific features.



Deployment Architecture

User Scenario – ArcGIS Online + On-Premises

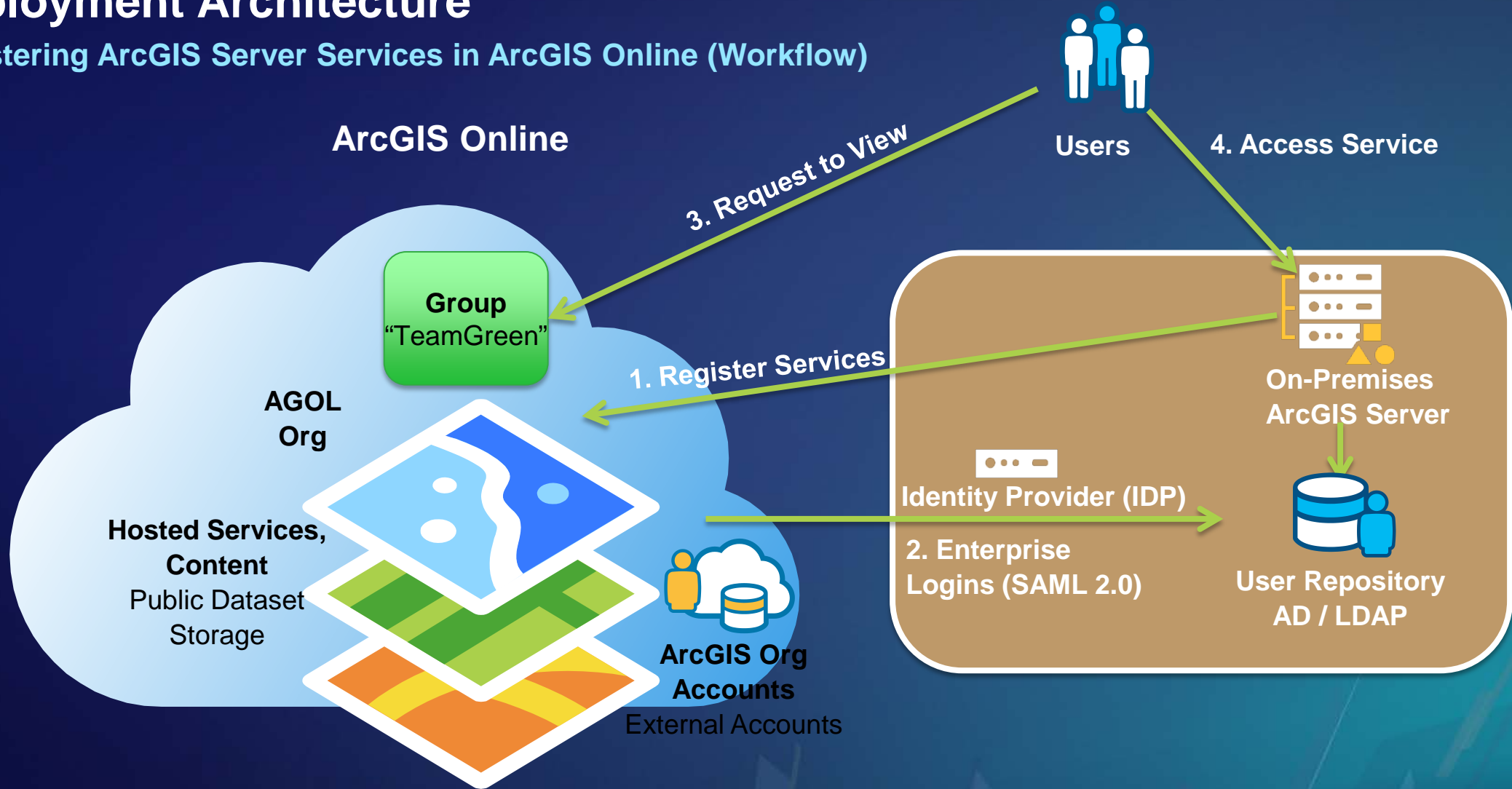
I want to share sensitive data internally, but provide subsets to external and public users.



Example: EPA's FISMA Authorized GeoPlatform

Deployment Architecture

Registering ArcGIS Server Services in ArcGIS Online (Workflow)



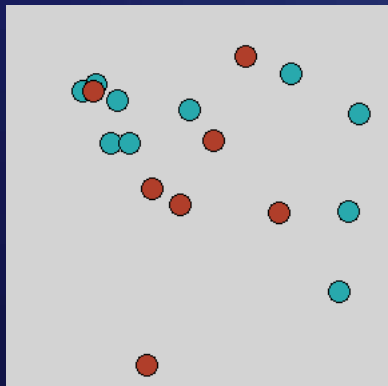
Segment sensitive data internally and public data in cloud

Deployment Architecture

Registering ArcGIS Server Services in ArcGIS Online

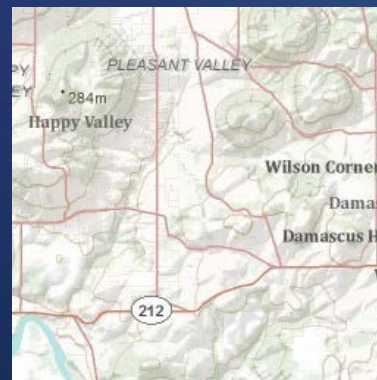
- Where are internal and cloud datasets combined?
 - At the browser
 - The browser makes separate requests for information to multiple sources and does a “mash-up”
 - Token security with TLS or even a VPN connection could be used between the device browser and on-premises system

On-Premises Operational
Layer Service



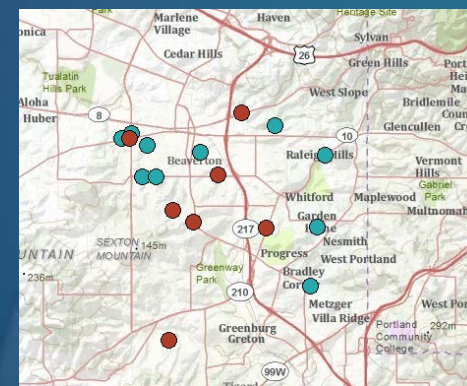
<https://YourServer.com/arcgis/rest...>

Cloud Basemap Service
ArcGIS Online



<https://services.arcgisonline.com...>

Browser Combines Layers



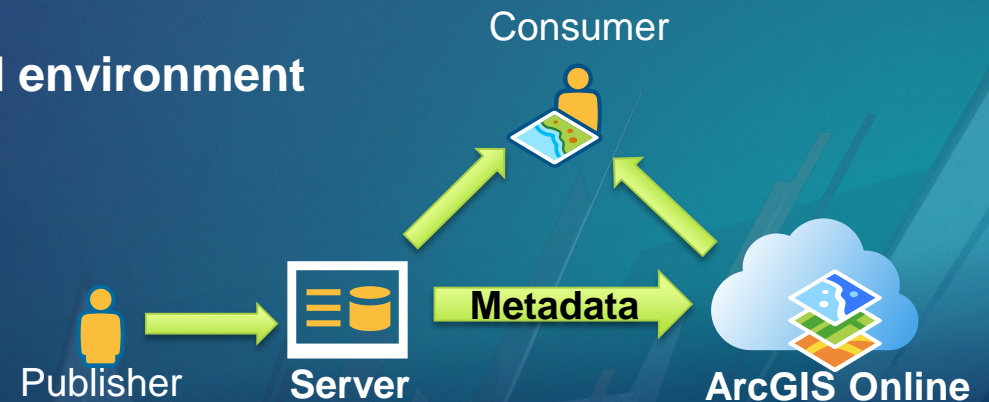
Deployment Architecture

ArcGIS Online FedRAMP Authorized Use Cases

- **Use Case 1 – Public Dissemination**
 - Publish tiles for fast, scalable visualizations
 - Share information with the public
 - Works well with new “Authoritative” content label



- **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

Significant Security Changes Coming



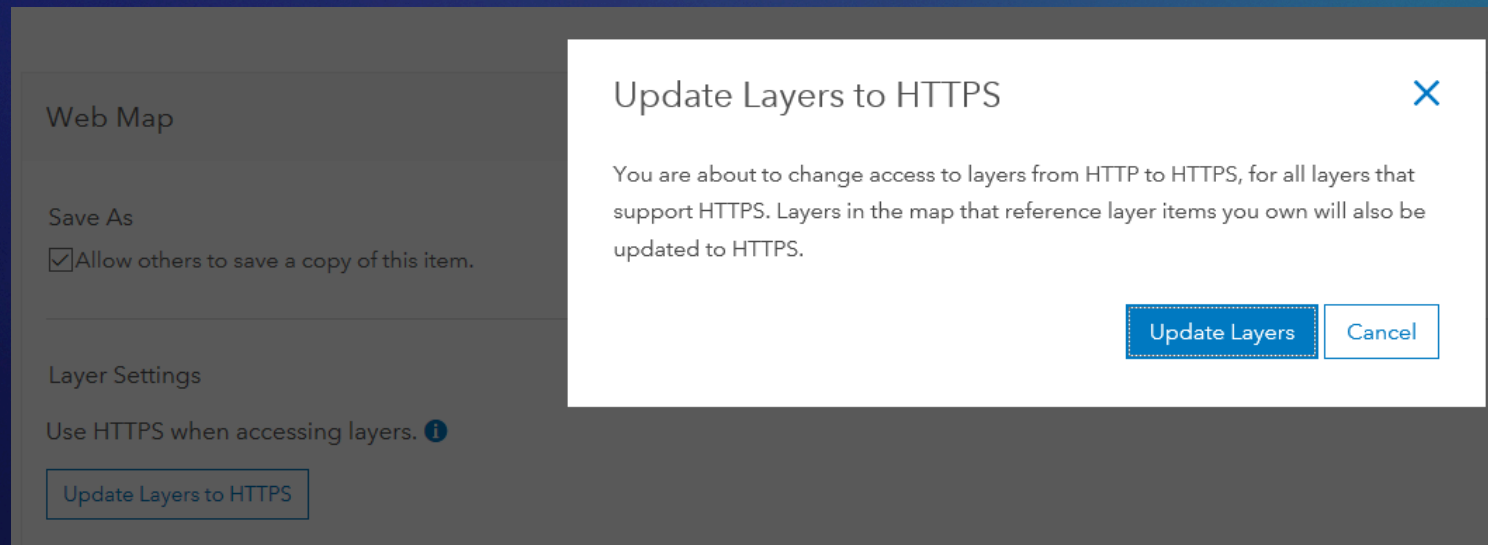
- **Transport security improvement roadmap established**
- ***Will disrupt a number of customer's operations if not tested/validated ahead of transition***
- **Broad announcement forthcoming**
- **First major change is disabling TLS 1.0 & 1.1 (In alignment with PCI & FedRAMP standards)**
 - **Planned for December 2018 release**
 - **Check out our TLS guide to understand compatibility with product versions (Trust Center)**

Deployment Architecture

Significant Security Changes Coming (con't)



- **Second major change is disabling HTTP for all Organizations**
 - Planned for September 2019 release
 - Eliminating HTTP allows utilizing HSTS across our domain, as opposed to just specific services as currently implemented
 - Maps/services/apps with HTTP calls will break and need to be fixed
 - We've been adding capabilities to make the transition easier
 - Update Map Layers to HTTPS



Compliance

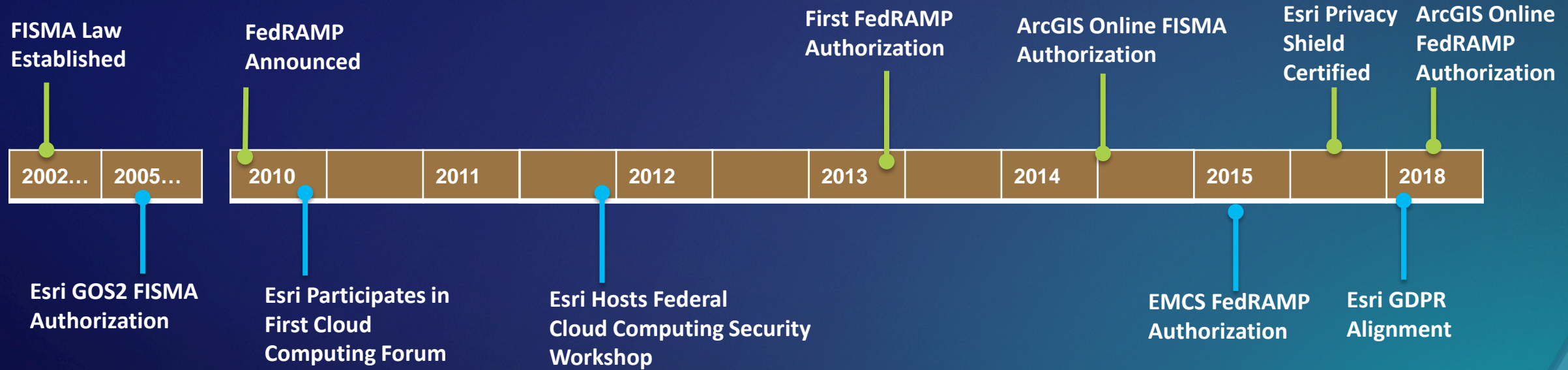


Compliance

- **Milestones**
- **Cloud Infrastructure Providers**
- **Products and Services**
- **Privacy Assurance / GDPR**
- **Security Assurance / FedRAMP**

Compliance

Milestones



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

Compliance

Cloud Infrastructure Providers

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

Cloud Infrastructure Security Compliance



Compliance

Products & Services

- **Product Based Initiatives**

- ArcGIS Server 10.3+ - DISA STIG
- ArcGIS Desktop 10.1+ - USGCB
- ArcGIS Pro 1.4.1+ - USGCB

- **Service Based Initiatives**

- EMCS Advanced Plus (Single-tenant) – FedRAMP Moderate
- ArcGIS Online (Multi-tenant) – FedRAMP Tailored Low - **NEW!**

Compliance

Privacy Assurance

- EU-U.S. Privacy Shield self-certified
 - General Esri Privacy Statement
 - Products & Services Privacy Statement Supplement



- TRUSTe provides privacy certification and dispute resolution



- General Data Protection Regulation (GDPR) ***NEW**



Compliance

GDPR / Privacy



Esri supports GDPR and continues to advance our privacy & security practices

Compliance

GDPR - Personal Data within Online Services

- **Who owns the data**
 - The customer
- **Who is responsible for categorizing datasets?**
 - The customer
- **Are there any restrictions for processing personal dataset types?**
 - Esri recommends customers not store Sensitive Personal Data unless encrypted or pseudonymized before posting for storage – Such as with a security gateway
- **What laws govern my data?**
 - Government entities – Applicable laws of customer's jurisdiction
 - Non-government entities – US federal law & State of California law
- **Where is my data?**
 - Online service data is stored within the United States and “adequate data privacy safeguards are in place” assured through our Privacy Shield compliance

Compliance

GDPR - Privacy Impact Assessment (PIA)

- **Esri has been performing PIA's since the early 2000's for Online services**
 - **ArcGIS GDPR/Privacy Best Practices whitepaper to be released soon to help guide customers**
 - **We welcome assisting customers with their PIA's as necessary**
- **Supplementary privacy statement created specifically for our Products & Services**
 - **Privacy Collection & storage of privacy information is minimized in our products**
 - **Online Telemetry service (EUEI) disabled by default for organizations outside the US**
- **Company-wide privacy improvements**
 - **Tracking cookies can now be disabled centrally across Esri.com & ArcGIS.com**
 - **When Esri is Controller of customer PI, requests handled through Privacy@esri.com**

Privacy

Cookies used by Esri

Esri uses site browsing, functionality, and analytics cookies. Learn more about these types of cookies and manage your site browsing cookie settings below.

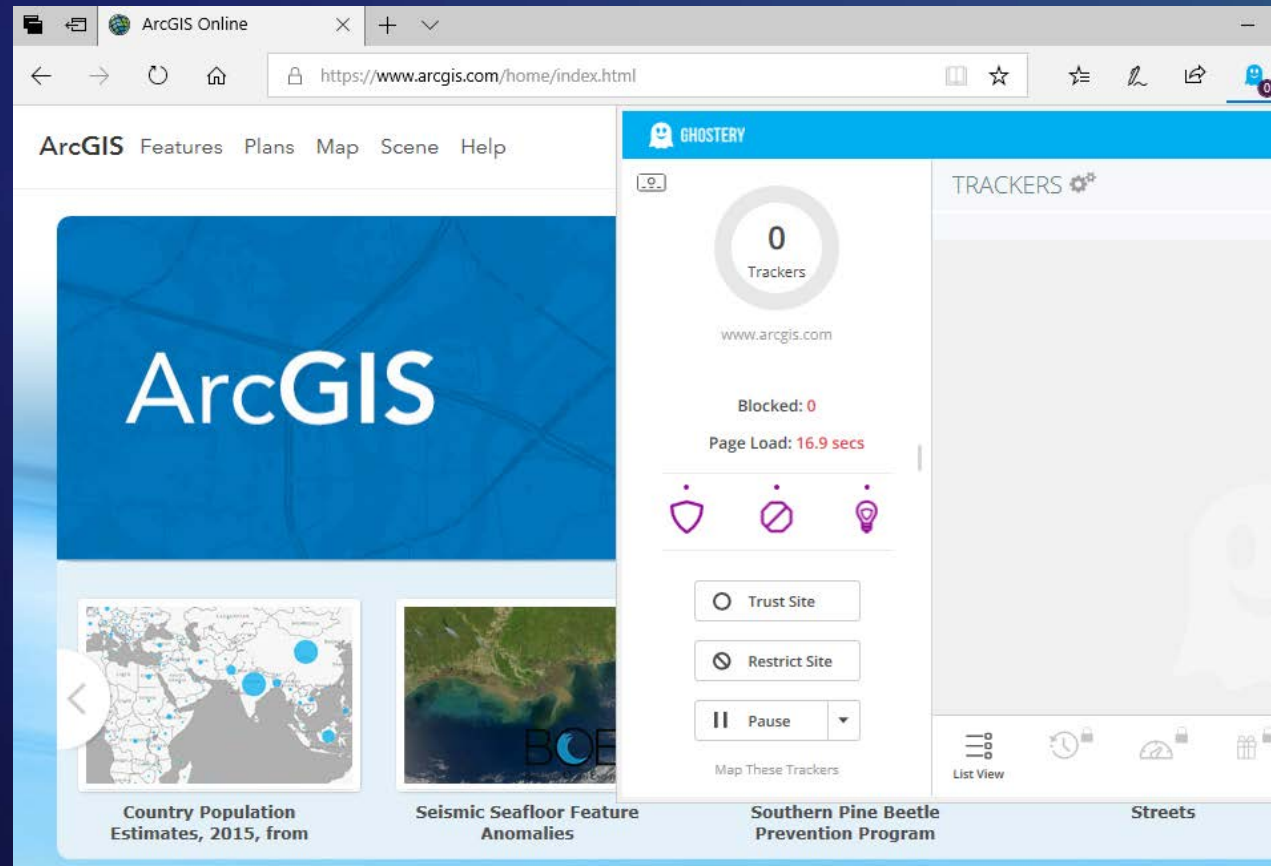
Targeting cookies
This type of cookie accompanies you through the website and helps us to personalize your experience, saving you time. These cookies also enrich your browsing experience by providing more relevant advertising as you browse the internet. These cookies contain personal information and we provide you with the ability to turn them off.

Targeting cookie setting: Off On

Compliance

GDPR - Cookies

- Marketing focused tracking cookies are not used across paid-for ArcGIS Online services no matter what the centralized cookie setting is



The screenshot shows the ArcGIS Online homepage in a web browser. The URL is <https://www.arcgis.com/home/index.html>. The page features the ArcGIS logo and navigation links for Features, Plans, Map, Scene, and Help. Below the logo are several map thumbnails, including 'Country Population Estimates, 2015, from', 'Seismic Seafloor Feature Anomalies', 'Southern Pine Beetle Prevention Program', and 'Streets'. A Ghostery cookie tracker overlay is visible on the right side of the page. The overlay shows 0 Trackers, 0 Blocked, and a Page Load of 16.9 secs. It includes icons for a shield, a crossed-out shield, and a lightbulb, and buttons for 'Trust Site', 'Restrict Site', and 'Pause'. The 'Trust Site' button is selected.

Compliance

GDPR - Protect By Design

- **Esri established a formal Security Development Lifecycle in 2017**
- **Addresses governance structure (CISO – Products, CISO – Corporate)**
- **Guidelines practices based on BSIMM, OWASP, CWE/SANS**
- **Most rigorous security measures starting with ArcGIS Enterprise & Online**
- **Static, Dynamic, and Component Analysis + 3rd party testing**
- **Product Security Incident Response Team (PSIRT) established**
- **FedRAMP Tailored Low Authorization drives continuous monitoring**
- **Customer datasets written/updated after March 10th, 2018 are encrypted at rest**
 - **Pre-existing datasets to be encrypted by end of 2018**

Compliance

GDPR - Data Breach Notification

- **Esri notifies customers within 72hrs of confirming their data has been breached**
- **Customers may report concerns directly to our PSIRT team through our Trust Center**
- **Support for Restriction of Processing for legal holds or otherwise**
 - **Online records can be identified, exported, and deleted by the customer**
 - **Customer org admin can disable user access or call our support team to temporarily disable org**

The screenshot shows the ArcGIS Trust Center interface. At the top, there is a navigation bar with the title 'ArcGIS Trust Center' and a 'Check System Status' button. Below the navigation bar, there are tabs for 'Trust', 'ArcGIS Online Status', 'Security', 'Privacy', 'Compliance', and 'Documents'. The main content area is titled 'Report a Security Concern'. It includes a paragraph of instructions: 'Please fill out the form on the right with all applicable information including sufficient details of your specific concern. Your contact details will be used to follow up on the information you provided. Please select the applicable subject from the subject drop-down menu.' Below this text is a bulleted list of options: 'Vulnerability - report a vulnerability found in our site or application.', 'Suspicious E-mail from Esri - If you believe you were targeted by a possible phishing attack from an Esri e-mail address, or have received other suspicious e-mail correspondence from Esri.', 'Privacy Issue - If you have a privacy concern related to our application or organization.', and 'Other - for all other security, privacy or compliance related concerns.' To the right of the text is a form with input fields for 'Name', 'Email Address' (with the example 'johnsmith@esri.com'), 'Phone Number', and 'Organization (optional)'.

Compliance

GDPR - Consent

- **Contracts**

- **Data Processing Addendum (DPA) pre-signed by Esri, ready for customers to sign and available within the Trust Center documents**

- **Forms**

- **Forms asking for private information now require consent / awareness of privacy statement**

- **Cookies**

- **Pages with marketing related tracking have cookie consent banners**

This Data Processing Addendum ("Addendum") is effective on the first date that Customer provides to Esri EU Personal Data (as defined below) subject to the GDPR (as defined below) or May 25, 2018, whichever is later, and forms part of the Master Agreement or other written or electronic agreement ("Agreement") by and between the organization signing or accepting below ("Customer") and Environmental Systems Research Institute, Inc. ("Esri"), and sets forth the terms and conditions relating to the privacy, confidentiality, and security of EU Personal Data associated with Online Services and Maintenance to be rendered by Esri to Customer pursuant to the Agreement. All terms defined or used in the Agreement shall have the same meaning in this Addendum unless otherwise specified.

Whereas Customer may provide Esri, a company located in the United States, with access to personally identifiable information about individuals located in the European Union to act as a Processor in connection with Online Services and Maintenance performed by Esri for or on behalf of Customer pursuant to the Agreement, and

Whereas Customer requires that Esri preserve and maintain the privacy and security of such EU Personal Data as a Processor according to the terms of this Addendum;

Now therefore, in consideration of the mutual covenants and agreements in this Addendum and the Agreement and for other good and valuable consideration, the sufficiency of which is hereby acknowledged, Customer and Esri agree as follows:

SECTION I—DEFINITIONS

- A. "Controller" means any person or organization that, alone or jointly with others, determines the purposes and means of the Processing of EU Personal Data.
- B. "EU Personal Data" means personally identifiable information about individuals located in the European Union and may include, but not limited to, the following: (i) categories of data subjects: prospects, customers, business partners, and vendors and (ii) types of personal data: name, title, position, and email address and location.

Compliance

FedRAMP

- **ArcGIS Online received an Agency FedRAMP Tailored Low authorization-to-operate (ATO) on June 28, 2018**
- **Authorization known as a Low-Impact Software as a Service (Li-SaaS)**
- **Value to US Government Agencies**
 - **FedRAMP standardizes way US government agencies perform security authorizations for cloud products and services, shifting the authorization process from years/months to weeks/days**
- **Value to Global Organizations**
 - **Recognized by many organizations around the globe as a gold standard for security**
 - **Mapping of ISO 27001 & 15408 controls is readily available via the Trust Center**

Compliance

FedRAMP Alignment

- **A Customer Responsibility Matrix (CRM) details recommended Organization settings to align with FedRAMP guidelines (summarized below)**
 - **Enable the HTTPS Only Security Policy**
 - **Enable Allow only Standard SQL Queries**
 - **Disable Security Policy allowing members to edit biographical information**
 - **Enable SAML v2.0 Enterprise Logins**
 - **Disable Social logins (w/exception for Google business accounts)**
 - **Add relevant domains for Allow Origins**
 - **Enable using Esri vector basemaps under Settings/Map/Basemap Gallery**

If only there were a way to easily validate the status of these recommendations for your org...

Compliance

Summary Across ArcGIS Online



New Security Advisor Tool

Michael Young

Compliance

New AGO Advisor Tool

- Validates your org settings/usage against secure best practices
- Provides organization & user level audit log visualization
- Tool now available as Preview
 - <https://arcg.is/ago-advisor>
- Value immediately proven
 - Already used by customer to quickly check 8 orgs and prepare for Anonymous Hacktivist Threat

The screenshot shows the ArcGIS Online Security Advisor Preview interface. At the top, the Esri logo and "THE SCIENCE OF WHERE" tagline are visible. The page title is "ArcGIS Online Security Advisor Preview" with a "Welcome" message and "Org" label. A "Sign-out" link is in the top right. A navigation menu on the left includes "Advisor", "Organization Change Log", "User Change Log", "Help", and "Feedback". The main content area displays a "CRITICAL: There are items that need your immediate attention." warning. Below this, the "Policies" section is shown, featuring a lock icon and a list of settings: "HTTPS Only Access" (checked), "Prevent Anonymous Access" (checked), and "Standardized SQL Queries" (unchecked). A detailed message explains that the "Standardized SQL Queries" setting is disabled and provides instructions on how to enable it to prevent nonstandard queries.

The screenshot shows the ArcGIS Online Security Advisor Preview interface with the "User Change Log" section selected. The page title is "ArcGIS Online Security Advisor Preview" with a "Welcome" message and "Org" label. A "Sign-out" link is in the top right. The navigation menu on the left includes "Advisor", "Organization Change Log", "User Change Log", "Help", and "Feedback". The main content area displays a table of user change logs for the organization "myyoung1000". The table has columns for "Actor", "Action", "Affected User", "Affected Resource", "Time Stamp", and "Actor's Source IP Address".

Actor	Action	Affected User	Affected Resource	Time Stamp	Actor's Source IP Address
myyoung1000	enablemfa	myyoung1000	/sharing/oauth2/enableMfa	Thu Feb 08 2018 17:50:08 GMT-0800 (Pacific Standard Time)	198.102.62.250
myyoung1000	disablemfa	myyoung1000	/sharing/rest/community/users/myyoung1000/disableMfa	Thu Aug 18 2016 14:56:05 GMT-0700 (Pacific Daylight Time)	198.102.62.250
myyoung1000	enablemfa	myyoung1000	/sharing/oauth2/enableMfa	Mon Jun 20 2016 22:12:39 GMT-0700 (Pacific Daylight Time)	198.102.62.250
myyoung1000	disablemfa	myyoung1000	/sharing/rest/community/users/myyoung1000/disableMfa	Mon Jun 20 2016 22:12:08 GMT-0700 (Pacific Daylight Time)	198.102.62.250
myyoung1000	enablemfa	myyoung1000	/sharing/oauth2/enableMfa	Mon Jun 20 2016 21:56:54 GMT-0700 (Pacific Daylight Time)	198.102.62.250
myyoung1000	disablemfa	myyoung1000	/sharing/rest/community/users/myyoung1000/disableMfa	Mon Jun 20 2016 21:54:25 GMT-0700 (Pacific Daylight Time)	198.102.62.250
myyoung1000	update	myyoung1000	/sharing/oauth2/resetPassword	Sat May 07 2016 10:54:37 GMT-0700 (Pacific Daylight Time)	198.102.62.250
myyoung1000	enablemfa	myyoung1000	/sharing/oauth2/enableMfa	Sat May 07 2016 10:53:23 GMT-0700 (Pacific Daylight Time)	198.102.62.250

Compliance

New AGO Advisor Tool

- **Considering enhancements based on user input**
 - **Discovery of embedded HTTP links within Services/Apps**
 - To help ease HTTPS transition
 - **Summarize all publicly editable services**
 - This is the most common way organizations accidentally leak data
 - **More extensive audit log display configuration**
 - **Support multiple Advisor scanning policies**
 - GDPR, FedRAMP, General best practices, custom
 - **Validate Portal for ArcGIS deployments**
 - **Report generation / export capability**
- **The Software Security & Privacy team welcomes your ideas**
 - SoftwareSecurity@Esri.com



Summary

- **New FedRAMP Tailored Low authorization and GDPR alignment ensure ArcGIS Online security & privacy capabilities continue to advance**
- **Significant security advancements are coming that could directly affect your operations**
 - Read the TLS Guide now – Much more info to come
- **Extensive security, privacy, compliance, and status info available**
 - Trust Center - [Trust.ArcGIS.com](https://trust.arcgis.com)
 - In-depth Cloud Security Alliance (CSA) answers readily available
 - New security best practice validation tool

Want to Learn More?

[> Overview](#)[> Cloud](#)[Product capabilities](#)[Implementation guidance](#)[Esri Managed Cloud Services](#)[> Enterprise](#)[> Desktop](#)[> Mobile](#)

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
- For more information, see [Configure security settings](#) in the ArcGIS Online Help.

In this topic

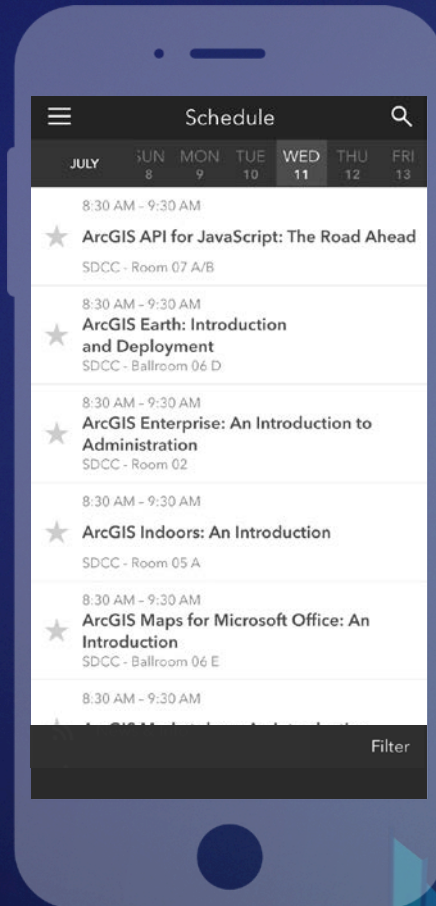
[Report a Security Concern](#)[Application security settings](#)[Authentication](#)[Authorization](#)[Encryption](#)[Logging and Auditing](#)[Related content](#)

Please Take Our Survey on the App

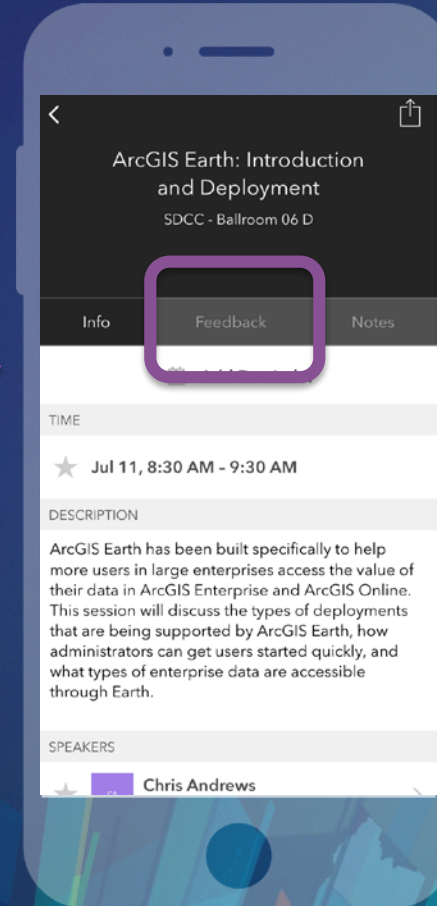
Download the Esri Events app and find your event



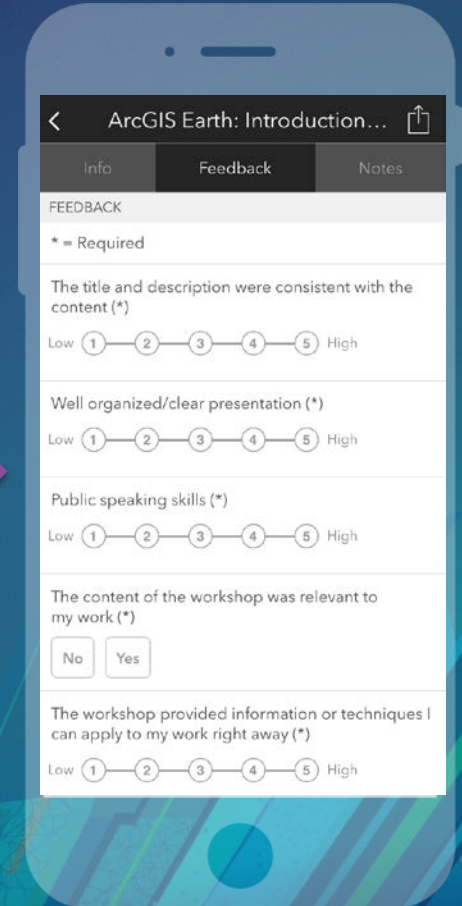
Select the session you attended



Scroll down to find the feedback section



Complete answers and select "Submit"



Session name: ArcGIS Online : An Introduction to Security, Privacy, and Compliance



esri

**THE
SCIENCE
OF
WHERE**