Understanding Data Sovereignty & ArcGIS

Jeff Rummelsburg – Esri Privacy Engineer

Michael Young – Esri CISO - Products

2023 ESRI USER CONFERENCE

esri | THE SCIENCE OF WHERE®

Agenda

- Issue at Hand
- Data Sovereignty Basics
- Geospatial Infrastructure & Esri
- ArcGIS Implementation Patterns
- Resources & Compliance
- Conclusion
- Q & A

Data: The New Oil?

In an era where data is the new oil, understanding and respecting data sovereignty has become a crucial aspect of our digital lives.

The UK Trade Policy Observatory estimates that international e-commerce and digitally delivered services would is likely worth US$5.5 to US$6 trillion, or almost 25% of total world exports.

According to the International Data Corporation (IDC), the global datasphere will grow from 33 zettabytes (ZB) in 2018 to 175 ZB by 2025.

According to the International Association of Privacy Professionals (IAPP), as of 2020, more than 130 out of 194 countries have enacted legislation to secure the protection of data and privacy.

Issue at Hand

- Customers want to know where their data is stored, and which entities have access to it
- They want to ensure transparency about the location of their data and how Esri can provide in-country or regional offerings
- The above needs to be backed by robust data security and privacy protocols and standards

Open Geospatial Consortium

- Data Sovereignty was identified by Open GIS Consortium (OGC) as key impediment for global pandemic preparedness going forwards
- More specifically
  - Balancing individual patient privacy with public health needs
  - National sovereignty with transparency and trust in global institutions
  - Populations' health needs across dissenting political boundaries with differing perspectives

Data Sovereignty Basics

What is Data Sovereignty?

Data Sovereignty:

Data collected, processed, and stored subject to regulations of country's location

Data Localization:

The requirement for data to be stored physically within the borders of the specific country where it was generated.

Data Residency:

- When a business or government specifies data storage geographical location
- Ensures data stays in specified geographical location

Summary:

Data sovereignty makes sure information subject to country legal punishments and protections where physically stored.

Why does Data Sovereignty Matter?

- Exponential growth in data crossing boarders
- Data Laws and Regulations:
  - GDPR regulations
  - CCPA
  - Regional variances
- Data Localization requirements
- US Privacy Shield deprecation highlighted concerns with inadequacy of international data transfers
  - Led to new mechanisms needed to comply with EU data protection requirements when transferring personal data from the European Union to the United States
  - Note: EU Commission voted to adopt its adequacy decision for the EU-US Data Privacy Framework
- Security and data protection strategies of data
- Data identification and classification
- Cybersecurity Risks

Esri Meeting Data Sovereignty Demands

- GDPR Data Processing Agreement (DPA) commitments
  - Supplementary measures
  - EU Standard Contractual Clauses (SCC)
- Data Protection Strategies
  - Encryption
  - Data Retention
  - Monitoring Plan
  - Key Management
- Customer Enabled Technical Measures
  - Pseudonymization
- Data Location Options
  - EU and Asia Pacific regions
  - Store your data in your preferred region

More info in the ArcGIS Trust Center:
https://trust.arcgis.com/en/privacy/gdpr.htm

Esri Meeting Data Sovereignty Demands

Recent Esri DPA Updates

- Standard Contractual Clauses (SCC's) External references
  - Added SCC's obligations and addendums for the EU, UK, Brazil, and Swiss Privacy Law
  - Referenceable within our DPA
  - Obligations to implement appropriate security measures, restrictions on sub-processing, and obligations to assist data controllers in ensuring compliance with legal obligations.
- Added California Consumer Privacy Act (CPRA)
  - Data Minimization and Purpose Limitation
  - Consumer Rights
  - Security Measures
- Scoped to Online Services and Subscription and Maintenance

Geospatial Infrastructure & Esri

Integrated Geospatial Infrastructure

Connecting organizations across borders, jurisdictions, and sectors

Mobility

Green Infrastructure

Economy

Health

Disasters

Climate

Agriculture

Regional Planning

Biodiversity

SaaS

Beyond SDI

Citizen Science

Collaboration

Findable Accessible Interoperable Reusable

Open Data

Engagement

Web Services

DCAT-AP

FAIR

High-Value Datasets

OGC

APIs

Data spaces

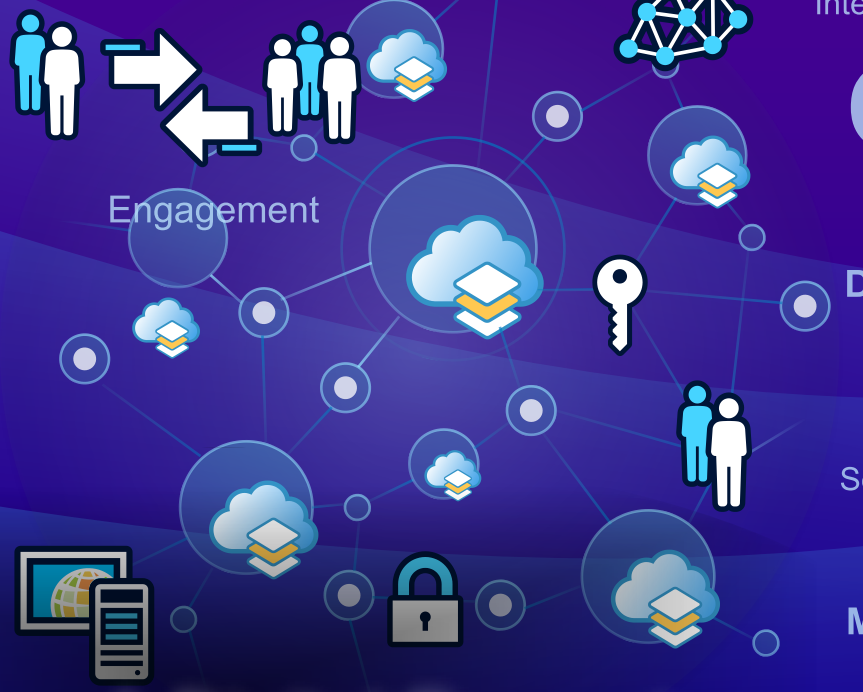
Secure

Privacy

Capacity Building

Metadata

INSPIRE



A Digital Ecosystem

GIS creating a sustainable future

Applications

Integration

AI/ML

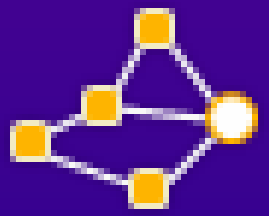
Analytics

Digital Twins

ArcGIS Online

Infrastructure

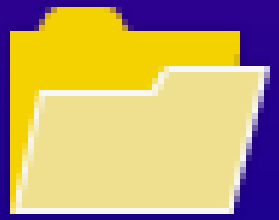
Website



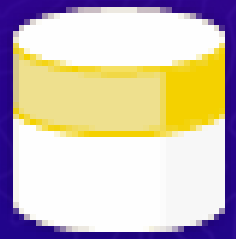
Services

Basemaps

Esri Managed Capabilities



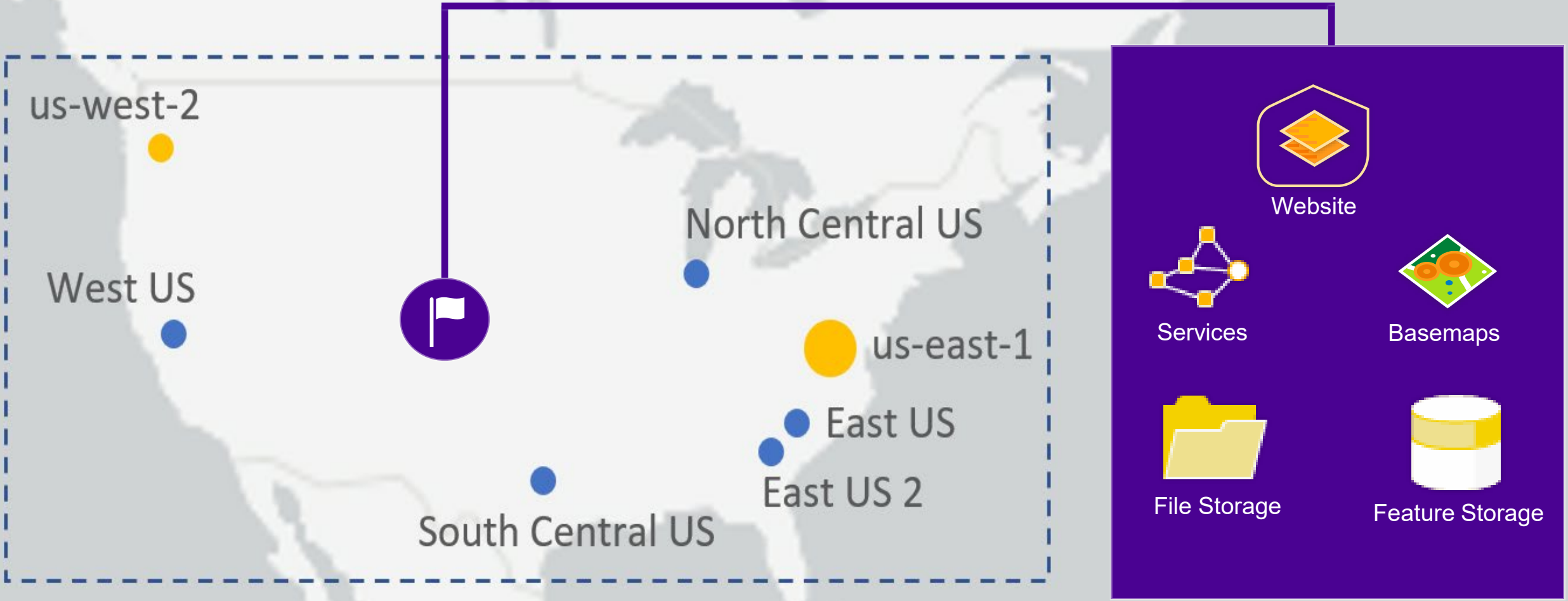
File Storage



Feature Storage

Customer Data

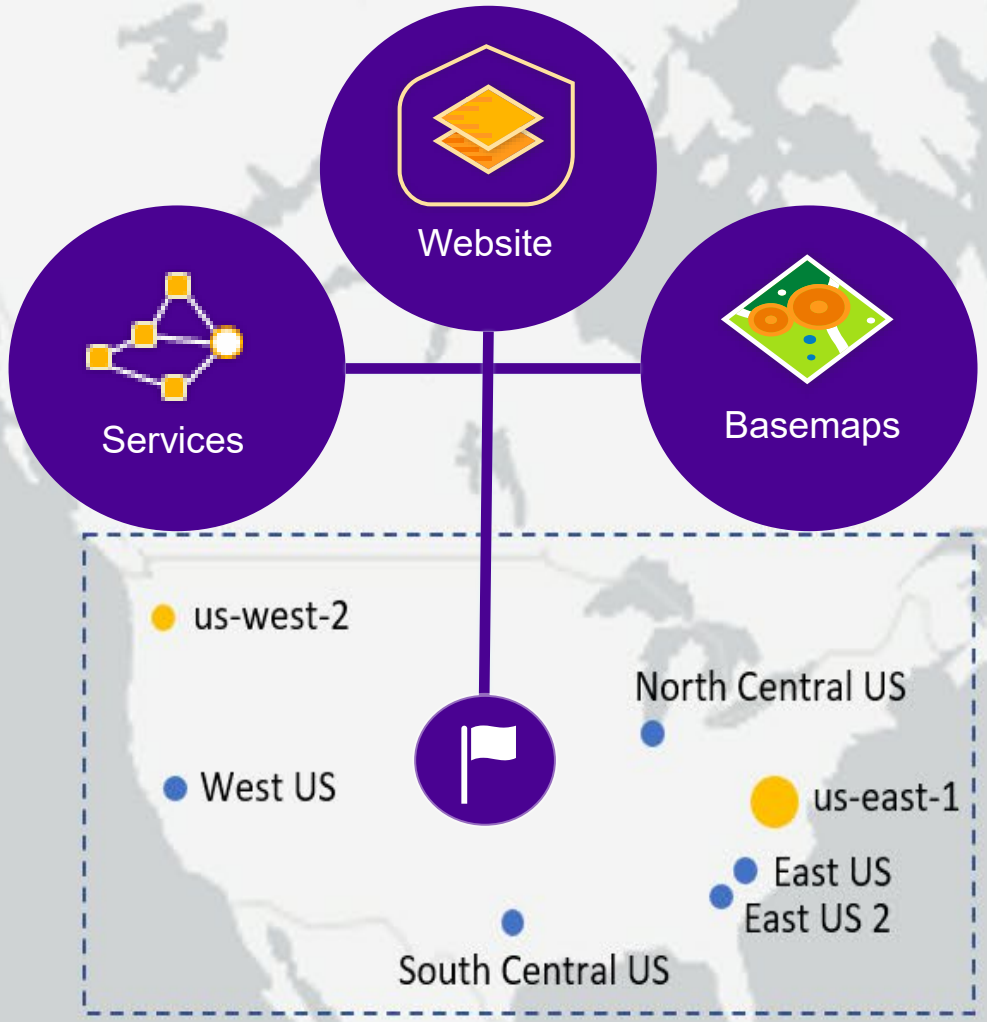
All components located on United States soil for US customers



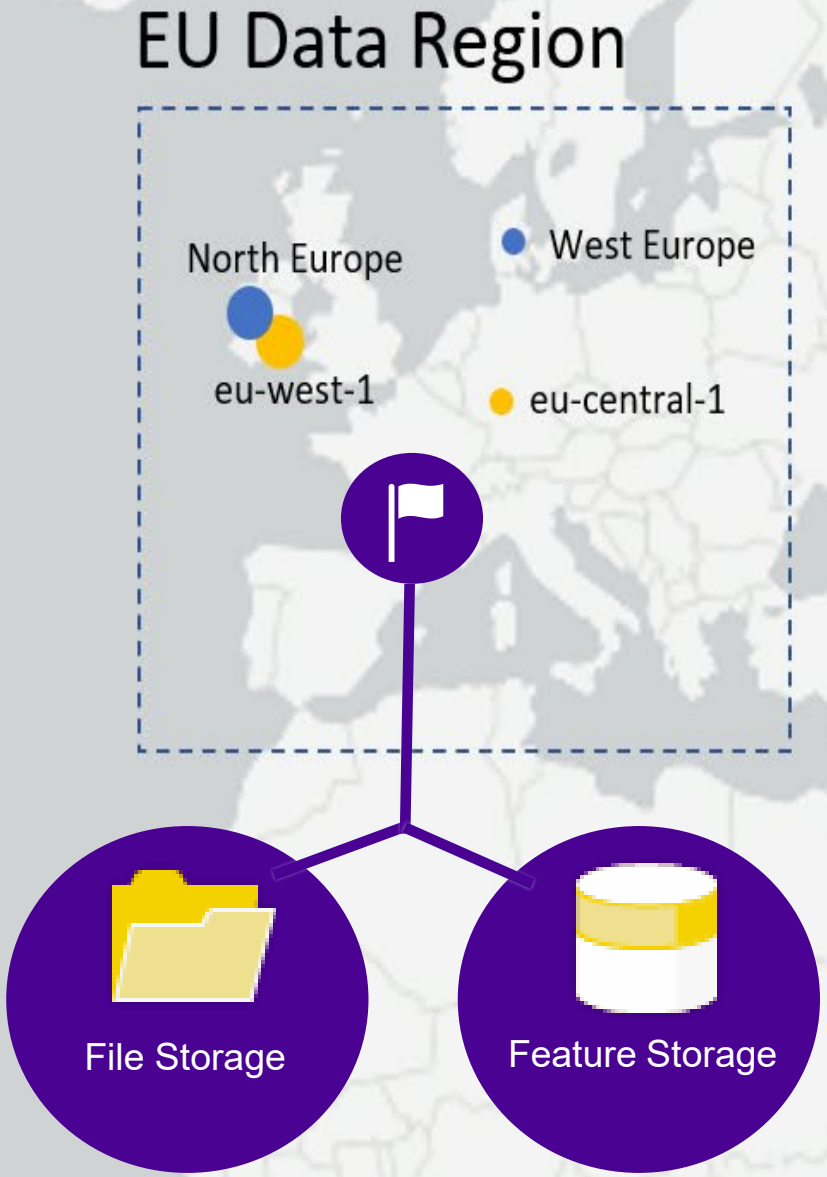
US Region

ArcGIS Online

Datacenters Utilized by US Customers



US Region

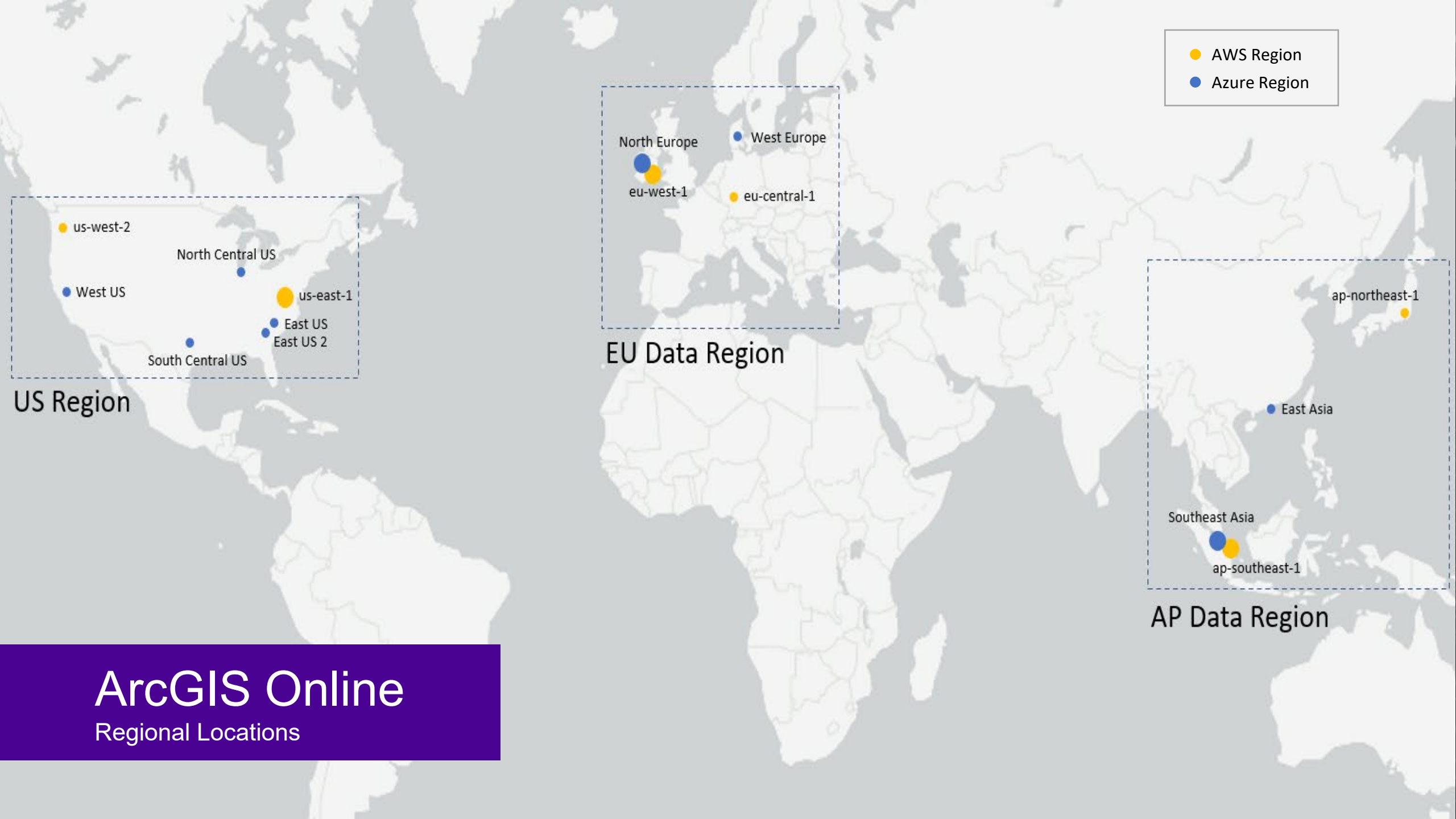


ArcGIS Online

Datacenters Utilized by EU Customers

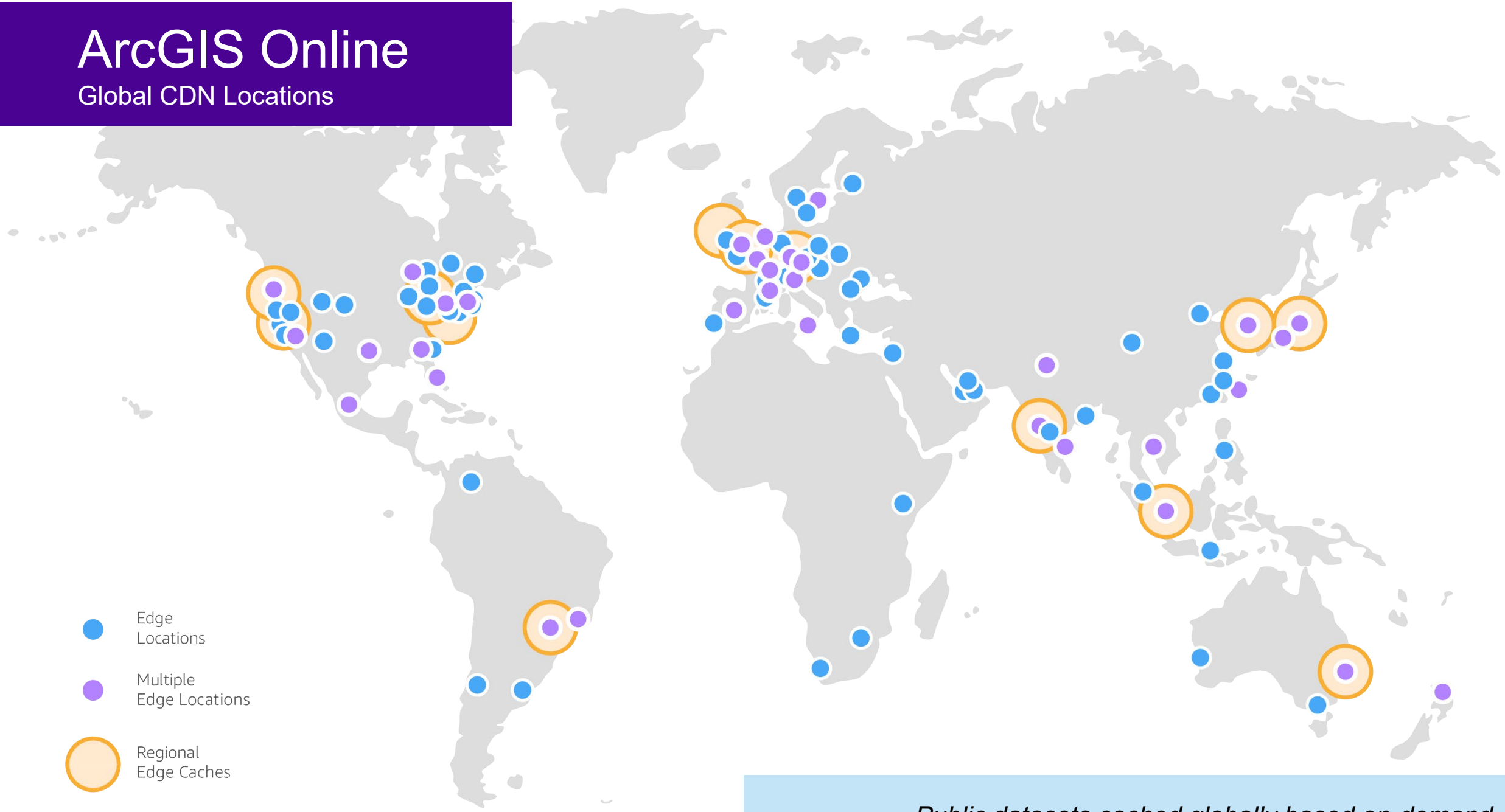
ArcGIS Online

Regional Locations



ArcGIS Online

Global CDN Locations



Public datasets cached globally based on-demand

ArcGIS Implementation Patterns

ArcGIS Implementation Patterns

Data & Metadata Specific Location Control

ArcGIS Enterprise

- Customer Hosted
- Hosting Provider

Data Specific Location Control

Hybrid

- All Data Registered
- Sensitive Data Registered

Data Regional Location Control

ArcGIS Online

- Regional Data Storage
- US-based Deployment

Decreasing Level of Data Sovereignty Paranoia

Customer Specific Location Control

ArcGIS Enterprise

- Counter to cloud first initiatives
- Increasingly less common
  - Scalability / infrastructure management costs
- For organizations with extreme/stringent data sovereignty demands
- ArcGIS Enterprise hosting provider options
  - Esri Distributors
  - Esri Business Partners
  - Esri Managed Cloud Services

Esri Only Hosts Metadata

Hybrid - Registered / Referenced

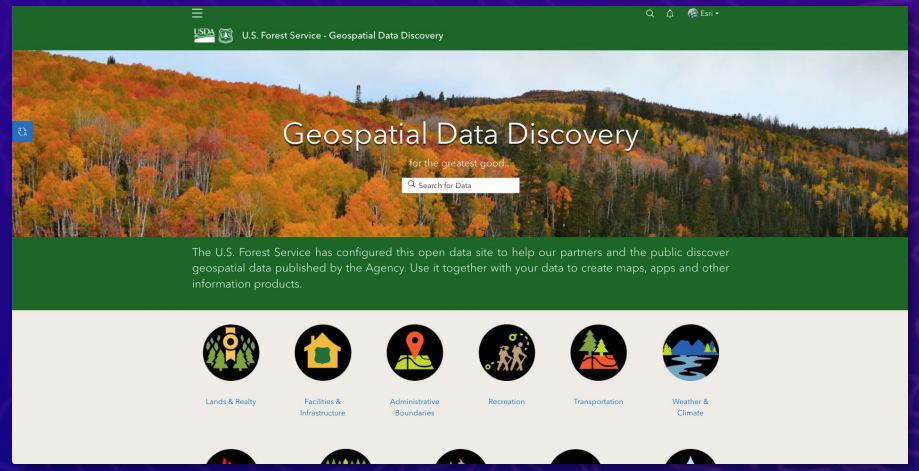
- ArcGIS Enterprise hosts ALL data in locations you approve
- ArcGIS Online/Hub used as user discovery interface
- Data sources from ArcGIS Enterprise are registered with ArcGIS Online to facilitate Open Data
- Your data is NOT stored within ArcGIS Online
  - Only service metadata stored

Data Specific Location Control

Hybrid

All Data Registered

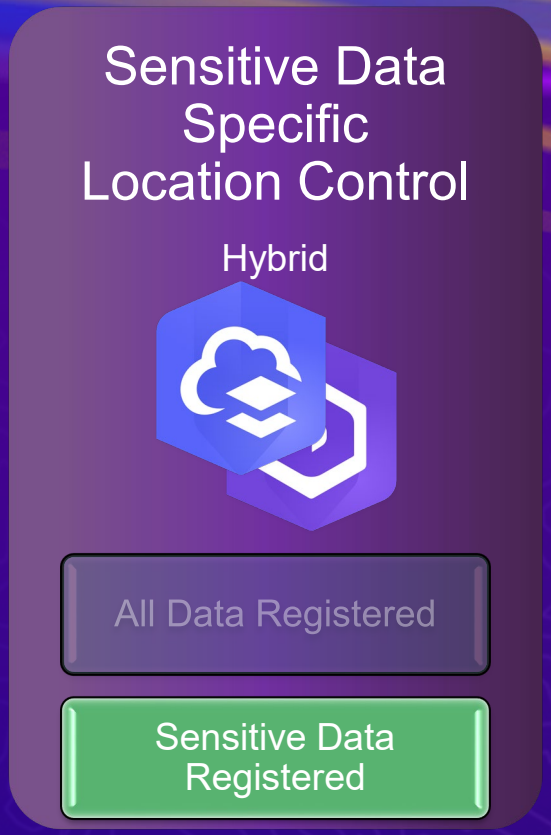
Sensitive Data Registered

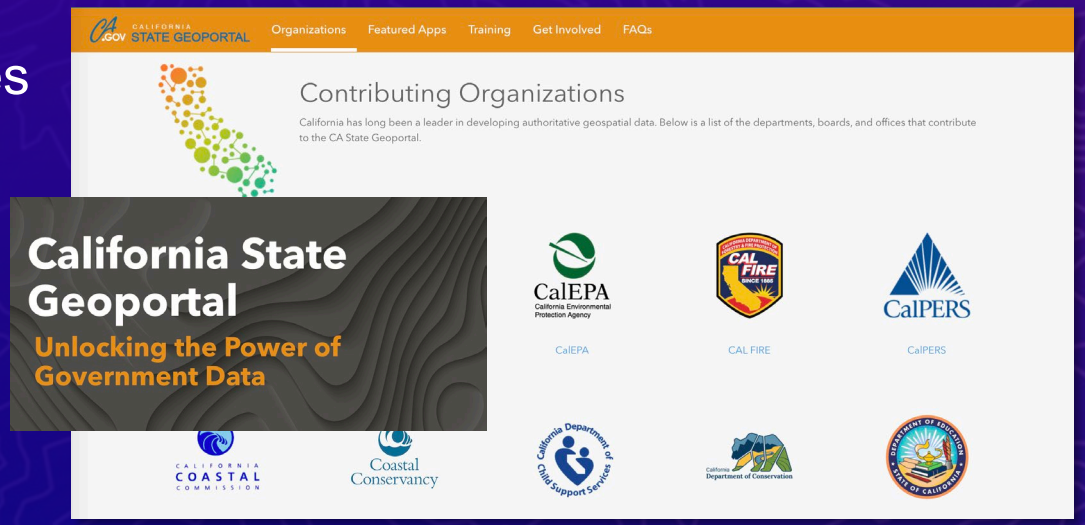


Esri Hosts Non-sensitive Data

Hybrid – Sensitive Data Limited to Enterprise

- Strikes balance
  - Host sensitive datasets within your Enterprise
  - Store other datasets within specific ArcGIS Online regions
- Most common deployment for SDI/Open Data demands
- Mitigation option in Esri's DPA Supplementary Measures





Hosted by Esri

ArcGIS Online

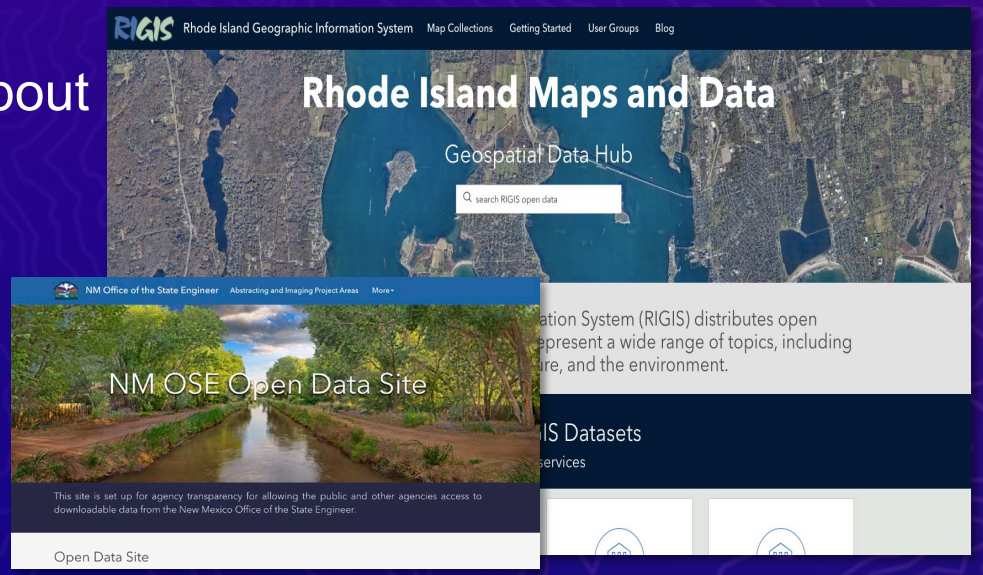
- Most cost-effective and typically strongest performance option
- Scalable and highest degree of discoverability
- Multiple data storage location options
  - EU / Asia PAC / US
- If you are a data manager with extraordinary concerns about
  - Public metadata stored in the US
  - Using global Content Distribution Network's (CDN)
- You may want to lean towards ArcGIS Enterprise
  - Otherwise, ArcGIS Online should be considered

Data
Regional
Location Control

ArcGIS Online

Regional Data Storage

US-based Deployment



Resources & Compliance

ArcGIS Trust Center

ArcGIS Trust Center

Overview | Security | Privacy | Compliance | Documents | Launch Security Advisor

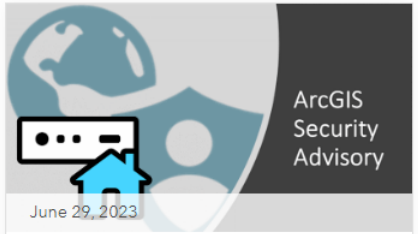
ArcGIS–Secure and Trustworthy

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

FedRAMP GDPR

Report a Security or Privacy Concern

Announcements



June 29, 2023

ArcGIS Insights Security Patches for ArcGIS Insights 2022.1 are now available

Esri has released ArcGIS Insights Security Patches for ArcGIS Insights 2022.1, resolving a high ...

June 23, 2023

Mid-2023 FedRAMP, CSA and ISO Update

Esri has expanded the security & privacy assurance of our products which opens new use case ...

May 22, 2023

ArcGIS and Apache Log4j Vulnerabilities

Esri's updated statement regarding Log4j vulnerabilities (Log4Shell) and ArcGIS ...

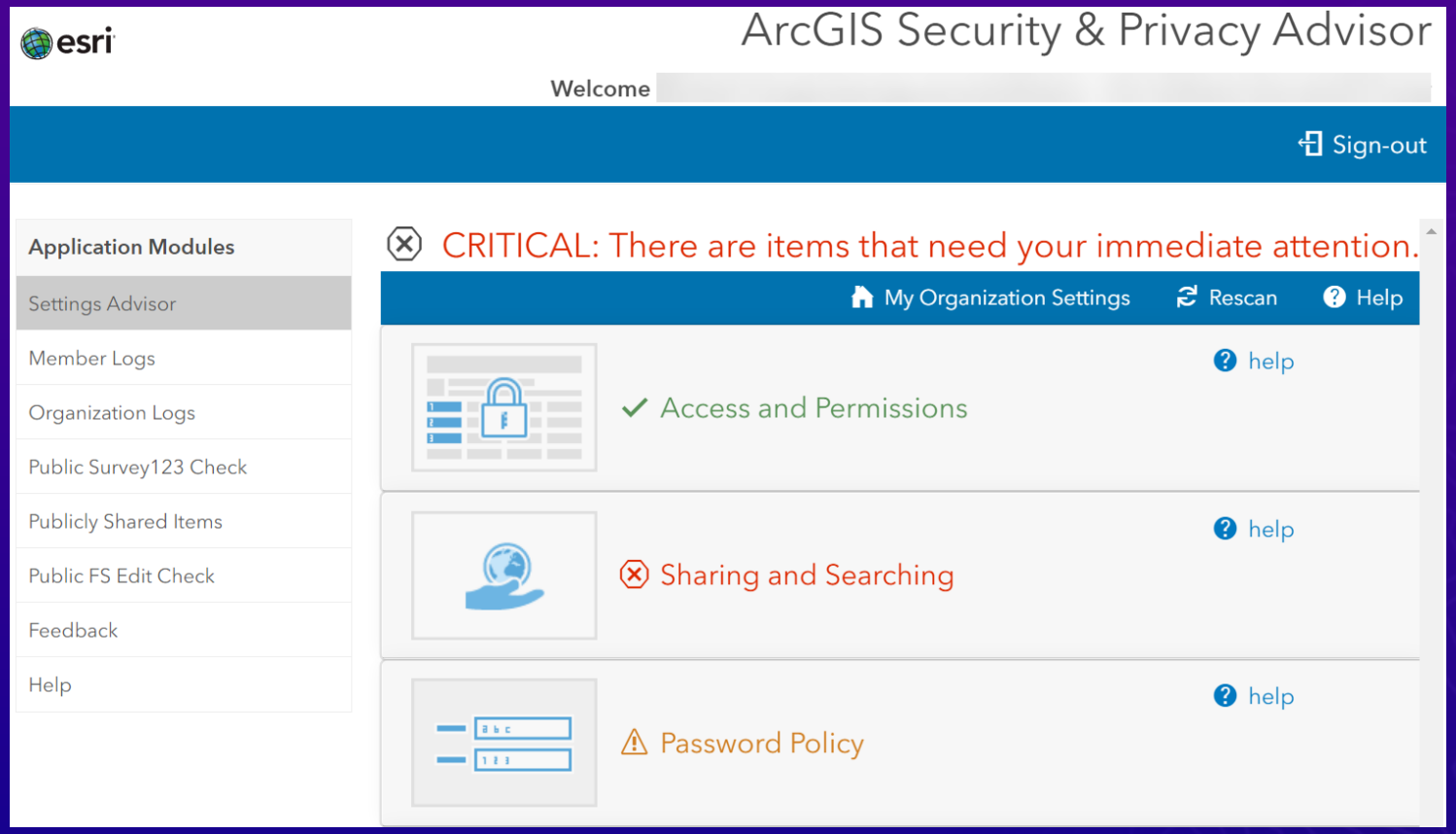
April 17, 2023

Portal for ArcGIS Security 2023 Update 1 Patch is now available

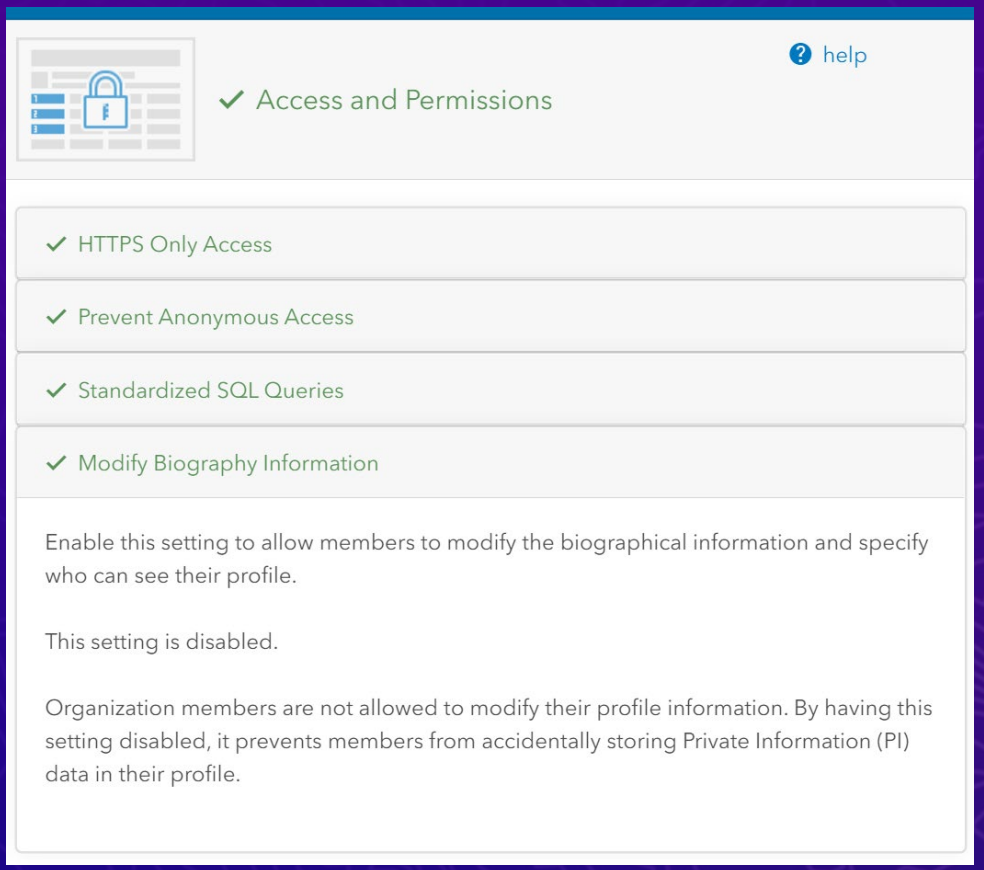
Esri has released the Portal for ArcGIS Security 2023 Update 1 Patch that resolves multiple ...

https://Trust.ArcGIS.com

ArcGIS Security & Privacy Advisor



Simple Red, Yellow, Green dashboard
Analyzes both ArcGIS Online AND ArcGIS Enterprise



Example of a privacy check to minimize PII

ArcGIS Location Sharing Privacy Technical Paper

An Esri
Software Security and Privacy
Technical Paper

January 2023

Version 3.2

ArcGIS® Location Sharing Privacy Best Practices

380 New York Street
Redlands, California 92373-8100 USA
909 793 2853
info@esri.com
esri.com

esri | THE SCIENCE OF WHERE™

2.6.2 ArcGIS QuickCapture

ArcGIS QuickCapture (see figure 5) is a mobile solution focused on a rapid data capture experience. Within ArcGIS Quick Capture location sharing can be enabled to provide the ability to record where users are and where they have been. Tracks and last known locations are uploaded from the QuickCapture mobile app to the Location Sharing service. QuickCapture records tracks whether or not there is a data connection and can provide mobile workers with control of when they are and are not tracked.

Figure 5—ArcGIS QuickCapture

2.6.3 ArcGIS Indoors

ArcGIS Indoors (see figure 6) supports indoor mapping with the ability to create and share indoor maps and location data. Indoors helps empower employees, occupants, and visitors to make the best use of buildings.

With Indoors, people can be provided a common picture of the environment within and around buildings. Indoor maps let users quickly find people, spaces, and events on-site. Operational data can be incorporated to help effectively maintain facilities, improve safety and security, and better allocate and manage resources.

Figure 2—ArcGIS Indoors Location Concept

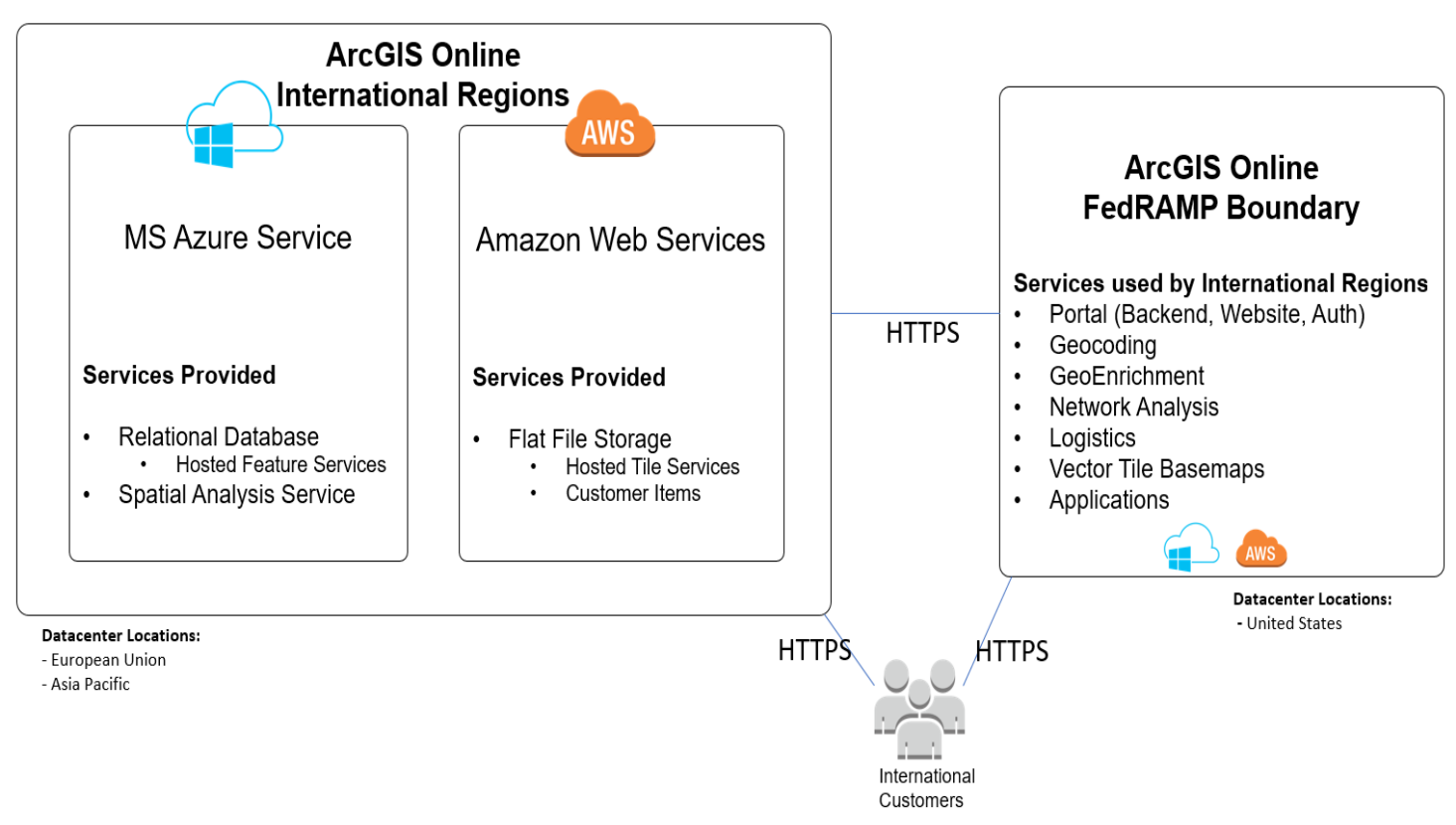
The overall Indoors solution includes the following components:

- An extension to ArcGIS Pro to curate and manage indoor data and author floor aware maps.
- A web application template, Indoors Viewer, for way finding and workspace reservation.
- A web application template, Indoors Space Planner, for space management.
- A native mobile (iOS and Android) application, Indoors Mobile, that supports way finding, workspace reservation, and location sharing

Topic	Recommended Option	ArcGIS Enterprise - 10.7.1 Base Deployment				ArcGIS Online				Criticality / Impact	
		Provided by Esri	Default	Configurable	Validation Tool	Provided by Esri	Default	Configurable	Validation Tool	Privacy	Security
HTTPS and Encryption											
	Stewide HTTPS TLS 1.2 Only	Yes	Yes	Yes	Scan.py	Yes	Yes	Yes	AGO SA	Danger	Danger
	Enforce HTTPS via HSTS	Yes	No	Yes		Yes[a]	Yes	No		Warning	Warning
	Configure Preferred Encryption Algorithms	Yes	Yes	Yes		Yes	Yes	No		Warning	Warning
	Website endpoint CA Certificates	No	No	Yes		Yes	Yes	No		Danger	Danger
	SAML IDP CA Certificates	No	No	Yes		No	No	Yes		Info	Info
	Enforce data storage encryption	No	No	Yes		Yes	Yes	No		Danger	Danger
	Remove self signed certs	Yes	No	Yes	Scan.py	Yes	Yes	No		Warning	Info
HTTP Header Config											
	X-Content-Type-Options: NOSNIFF	Yes	Yes	Yes		Yes	Yes	No		Warning	Warning
	X-XSS-Protection	Yes	Yes	No		No	No	No		Info	Info
	X-Frame-Options	Yes	Yes[b]	No		Yes	Yes	No		Warning	Warning
Interfaces											
	Disable Services Directory	Yes	No	Yes		No	No	No		Warning	Warning
	Disable Portal Directory	Yes	No	Yes	Scan.py	Yes	Yes	No		Warning	Warning
	Limit access to Admin Resources via Web Adaptor	Yes	No	Yes		No	No	No		Warning	Warning
	Understand Dynamic Workspace usage	Yes	Yes	Yes		No	No	No		Warning	Warning
	Secure System Services	Yes	Yes	Yes		Yes	Yes	No		Danger	Danger
Standardized Filtering											
	Enforce Standardized Queries	Yes	Yes	Yes		Yes	Yes	Yes	AGO SA	Danger	Danger
	Filter Web Content Enabled	Yes	Yes	Yes		Yes	Yes	No		Danger	Danger
Authentication and Authorization											
	Utilize Enterprise Logins via SAML instead of Built-in	No	No	Yes		No	No	Yes	AGO SA	Warning	Warning
	Block members joining org with social network credentials	No	No	No		Yes	No	Yes	AGO SA	Warning	Warning
	Define a password Complexity Policy	Yes	Yes	Yes		Yes	Yes	Yes	AGO SA	Warning	Danger
	Use Enterprise user store with account lockout policy	Yes	Yes	Yes		Yes	Yes	Yes		Warning	Warning
	Configure a shorter token Expiration Period	Yes	Yes	Yes		Yes	Yes	Yes		Warning	Warning
	Configure Multi-factor Authentication	No	No	Yes		Yes	No	Yes	AGO SA	Danger	Danger
	Disallow user account self-creation	Yes	Yes	Yes	Scan.py	Yes	Yes	Yes		Warning	Danger
	Define Custom Roles	Yes	No	Yes		Yes	No	Yes		Warning	Warning
	Disable Anonymous Access	Yes	No	Yes		Yes	No	Yes	AGO SA	Danger	Warning
	Configure role based access control	Yes	Yes	Yes		Yes	Yes	Yes		Danger	Danger
	Disallow token generation via GET	Yes	Yes	Yes	Scan.py	Yes	Yes	No		Danger	Danger
Web Tier Technologies											
	Use a WAF/Web Filter	No	No	Yes		Yes	Yes	No		Warning	Warning
	Utilize load balancer instead of Web Adaptor	No	No	Yes		Yes	Yes	No		Info	Warning
	Web Adaptor utilized for IWA only made organization	Yes	Yes	Yes		No	No	No		Info	Info
	Remove Technology identifiers and banners	Yes	Yes	No		Yes	Yes	No		Info	Info
	Use Data Loss Prevention (DLP)	No	No	Yes						Warning	Warning
	Define Allowed MIME types	No	No	Yes		No	No	No		Info	Warning
Data Ownership & Privacy											
	Prevent users from sharing publicly	Yes	Yes	Yes		Yes	Yes	Yes	AGO SA	Warning	Warning
	Disallow biography edits and visible profiles	Yes	Yes	Yes		Yes	Yes	Yes	AGO SA	Warning	Info
	Limit search to your organization only	Yes	Yes	Yes		Yes	No	Yes	AGO SA	Info	Info
	Remove social media links in item details/group pages	Yes	Yes	Yes		Yes	Yes	Yes	AGO SA	Warning	Info
	Do not allow members of other organizations to sign in	No	No	No		Yes	No	Yes		Warning	Warning
	Define specific allowed Portals for Access	Yes	No	Yes		Yes	No	Yes	AGO SA	Warning	Warning
	Validate Distributed Collaborations	Yes	No	Yes		Yes	No	Yes		Warning	Danger
	Disable Esri User Experience Improvement Program (EUEI)	No	No	No		Yes	No	Yes	AGO SA	Warning	Info
	Identify Authoritative Content	No	No	No		Yes	No	Yes		Warning	Info
	Configure Access Notice	Yes	No	Yes		Yes	No	Yes		Info	Warning
Server Trust Relationships											
	Define trusted servers	Yes	No	Yes		Yes	No	Yes	AGO SA	Warning	Warning
	Define allowed proxy hosts	Yes	No	Yes	Scan.py	Yes	No	No		Warning	Warning
	Define Cross Origin Policy	Yes	No	Yes		Yes	No	Yes	AGO SA	Warning	Warning
Sharing Best Practices											
	Create and document content review policy	No	No	Yes		No	No	Yes		Danger	Warning
	Create and document sharing review policy	No	No	Yes		No	No	Yes		Danger	Warning
	Validate need for editable layers	Yes	No	Yes		Yes	No	Yes		Danger	Warning

Compliance

- ArcGIS Online FedRAMP Boundary
  - Upgraded to FedRAMP Moderate for 2023
  - FedRAMP to ISO27k mapping in Trust Center
  - Cover US-based operations/systems
- ArcGIS Online Regions
  - Today
    - Security assurance of underlying providers
    - Microsoft Azure and Amazon Web Services
  - Mid-2024
    - ISO 27k EU Region compliance



Conclusion

Conclusion

- Esri Actions Taken
  - DPA supplementary measures and contractual clauses
  - Data protection strategies
  - EU & Asia Pacific region data storage

- Customer Deployment Options
  - Enterprise – Data & *Metadata* Specific Location Control
  - Hybrid – Data Specific Location Control
  - Online – Data *Regional* Location Control

- Guidance Available
  - ArcGIS Trust Center
  - ArcGIS Security & Privacy Advisor

esri®

THE SCIENCE OF WHERE®