

Understanding Data Sovereignty & ArcGIS

Jeff Rummelsburg – Esri Privacy Engineer

Michael Young – Esri CISO - Products





Agenda

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



Issue at Hand



Limited Control & Clarity:

Customers want to know where their data is stored, and which entities have access to it.



Data mobility

New laws may impose restrictions on the movement of data between countries.



Transparency and Options

Customers want to ensure transparency about the location of their data and how Esri can provide in-country or regional offerings



Security & Compliance Risks:

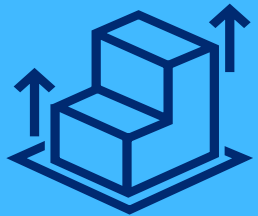
Concerns about data security in specific regions and uncertainty about meeting regulations.



Cost & Performance Impacts:

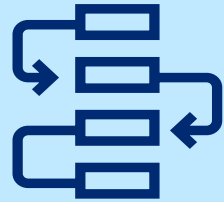
Potential operational costs and slower application performance due to data residency requirements.

By the Numbers



70%

**Growth of Data
Residency Laws**



125zB

**Global Data
Flows**



160k

**Data Breach
Notifications
Reported**



85%

**Enterprises are
Leveraging
Multi-cloud or
Hybrid
Environments**

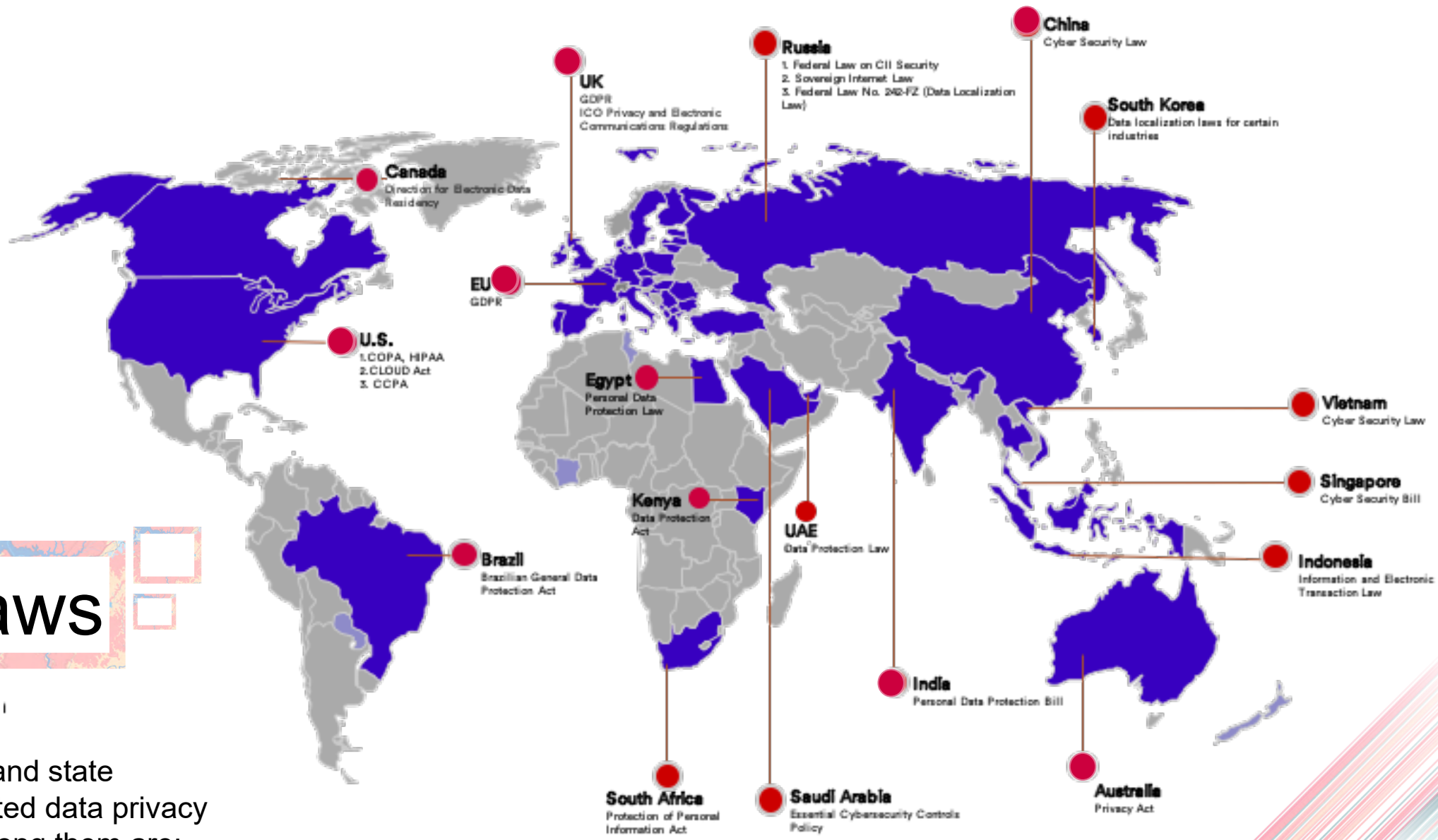


Data Sovereignty & Data Residency Basics



Whose Laws Apply?

More than 100 national and state governments have enacted data privacy and disclosure laws. Among them are:




Data Sovereignty



What is Data Sovereignty:

- Data sovereignty is the concept that data is used and kept per the laws and regulations of the country or jurisdiction in which it is situated.
- Examples of data sovereignty laws include:
 - Canadian Consumer Privacy Protection Act (CCPPA)
 - General Data Protection Regulation (GDPR)
 - Australian Privacy Principles (APP)

Importance of Data Sovereignty

- Data sovereignty is essential for businesses storing data in the cloud to observe the laws and regulations of the country or jurisdiction.
 - Implementing data protection measures is a key aspect of ensuring data sovereignty. This includes:
 - Encryption
 - Access controls
 - Monitoring
- 



Data Residency

What is Data Residency:

- Data residency refers to where data is stored. This could be a physical or virtual location.
 - Unlike data sovereignty, data residency is primarily concerned with the geographical location of the data itself.
 - Data residency involves the practice of data mapping, which helps customers understand:
 - What data they possess
 - Where it is located
 - The relevant data residency policies for each location

Importance of Data Residency

- Data residency is essential for adhering to data protection regulations, bolstering security, and providing access to data.
- 


Data Localization



What is Data Localization:

- Data Localization refers to the requirement that data generated within a country's borders must be stored and processed within that same country.
 - While data localization dictates where data must be stored, data residency simply indicates its current location.
 - Some countries want to maintain control over data generated by their citizens.

Importance of Data Localization

- The primary goal of data localization is to control data flow and safeguard it according to the local laws and standards.
 - By keeping data within a specific jurisdiction, some governments believe it's easier to secure and prevent unauthorized access.
- 

Coming Together

- Data sovereignty sets the overarching principles
- Data residency defines the location based on those principles
- Data localization enforces stricter control within a specific area

Together, they ensure that data is controlled, stored, and processed in compliance with local regulations and protecting it from unauthorized access.

The Why

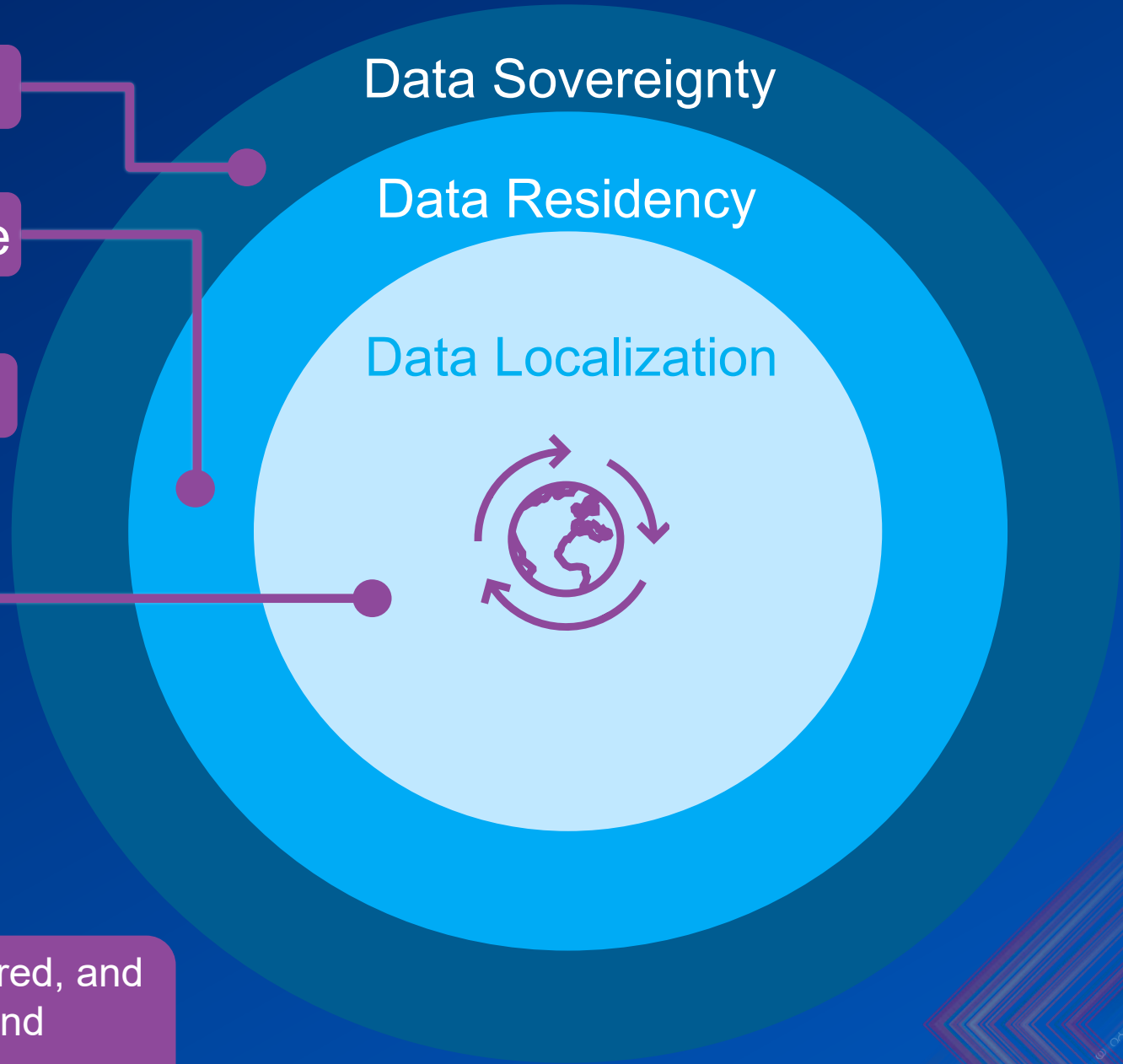
The Where

The How

Data Sovereignty

Data Residency

Data Localization



Why Does All This Matter?



Growing Importance of Data

- Exponential growth in data crossing borders



Rise of Global Data Flows

- Businesses operate internationally, collecting and processing data from users worldwide



Heightened Privacy Concerns

- Data breaches have raised public awareness about how personal information is collected and used.
- Data laws and regulations like GDPR, CCPA, and regional variances



Geopolitical Tensions

- Tensions between countries can lead to concerns about data security and government access



Impact on Businesses

- Organizations must comply with data residency and localization laws to avoid hefty fines and legal repercussions



Security Risks

- Knowing the data residency location helps identify who is responsible for data security in case of a breach.

Artificial Intelligence (AI) & Data Sovereignty

AI's Reliance on Data:

- The quality and quantity of data directly impact the effectiveness and accuracy of AI models
- Data sovereignty can influence the type and quality of data available for AI development.

Security Concerns with AI:

- AI systems can be vulnerable to manipulation or misuse
- Reduce the risk of unauthorized access by foreign actors with data localization

Algorithmic Bias:

- AI models trained on biased data can perpetuate those biases in their outputs
- Data sovereignty can provide some control over the data used for AI development

National AI Strategies:

- Many countries are developing national AI strategies that prioritize domestic AI development

Example:

- China has strict data residency laws and is heavily invested in domestic AI development.



Meeting Data Sovereignty & Data Residency Demands



Esri Meeting Data Sovereignty & Data Residency Demands

Offering Flexible Deployment Options

- EU and Asia Pacific regions
- Store your data in your preferred region

Transparency and Compliance

- ArcGIS Trust center information and documentation
- Product Supplement
- Compliance with relevant data privacy regulations (GDPR, CCPA)

Security Measures

- Encryption of data at rest and in transit, access controls, data retention, and regular security audits

Legal Framework

- DPAs and SCCs provide the legal foundation for data processing and transfers
- EU-US Data Privacy Framework (EU-US DPF) certification

Technical Controls

- Customer-enabled technical measures (Pseudonymization)
- ArcGIS Enterprise Hardening Guide

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

What Customers Can Do

Data Management

- Data mapping and classification of your data to understand the types of data
- Maintain clear records of data storage locations

Compliance with Industry-Specific Regulations

- Determine what risks exist to your data
- Research what laws and regulations apply and monitor regulatory changes

Ensure Appropriate Data Storage Locations

- Utilize Esri's regional data centers to store data within the required geographic boundaries
- When setting up services like ArcGIS Online, specify the preferred data storage location
- Engage with Esri's professional services for customized advice and solutions tailored to specific regulatory needs.

Implement Data Governance Policies

- Develop and enforce internal data governance policies that align with local regulations.
- Conduct regular audits to ensure ongoing compliance with data sovereignty and residency laws.

Security

- Implement strict access controls and authentication measures to safeguard data and ensure it is only accessible to authorized personnel.

Business Activities

- Evaluate the nature of your business activities and the types of data you handle
- Consider industry-specific regulations that may impose additional requirements on data handling practices

The background of the slide is a dark blue gradient. On the right side, there are two overlapping, semi-transparent maps of a city area, one above the other, with a vibrant, multi-colored border. The text 'Geospatial Infrastructure & Esri' is positioned on the left side. 'Geospatial Infrastructure' is in white, and '& Esri' is in a light blue color. There are some faint, overlapping square shapes in the background behind the text.

Geospatial Infrastructure & Esri

Integrated Geospatial Infrastructure

Connecting organizations across borders, jurisdictions, and sectors

Mobility

Green Infrastructure

Economy

Health

Disasters

Agriculture

Regional Planning

Biodiversity

Climate



A Digital Ecosystem

GIS creating a sustainable future

Applications

Integration

AI/ML

Analytics

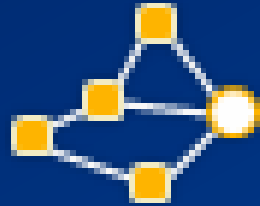
Digital Twins

ArcGIS Online

Infrastructure



Website



Services



Basemaps



File Storage

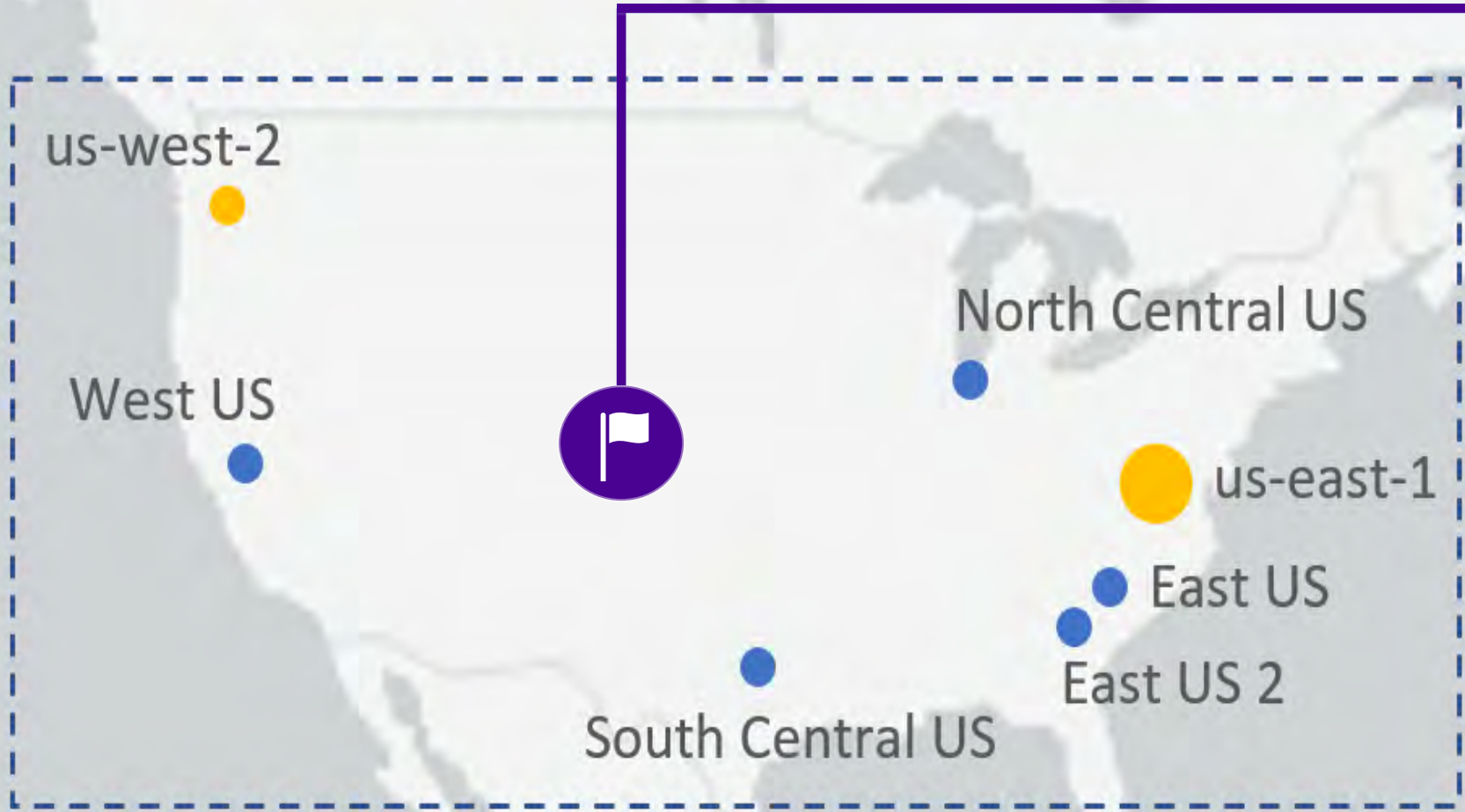


Feature Storage

Esri Managed
Capabilities

Customer Data

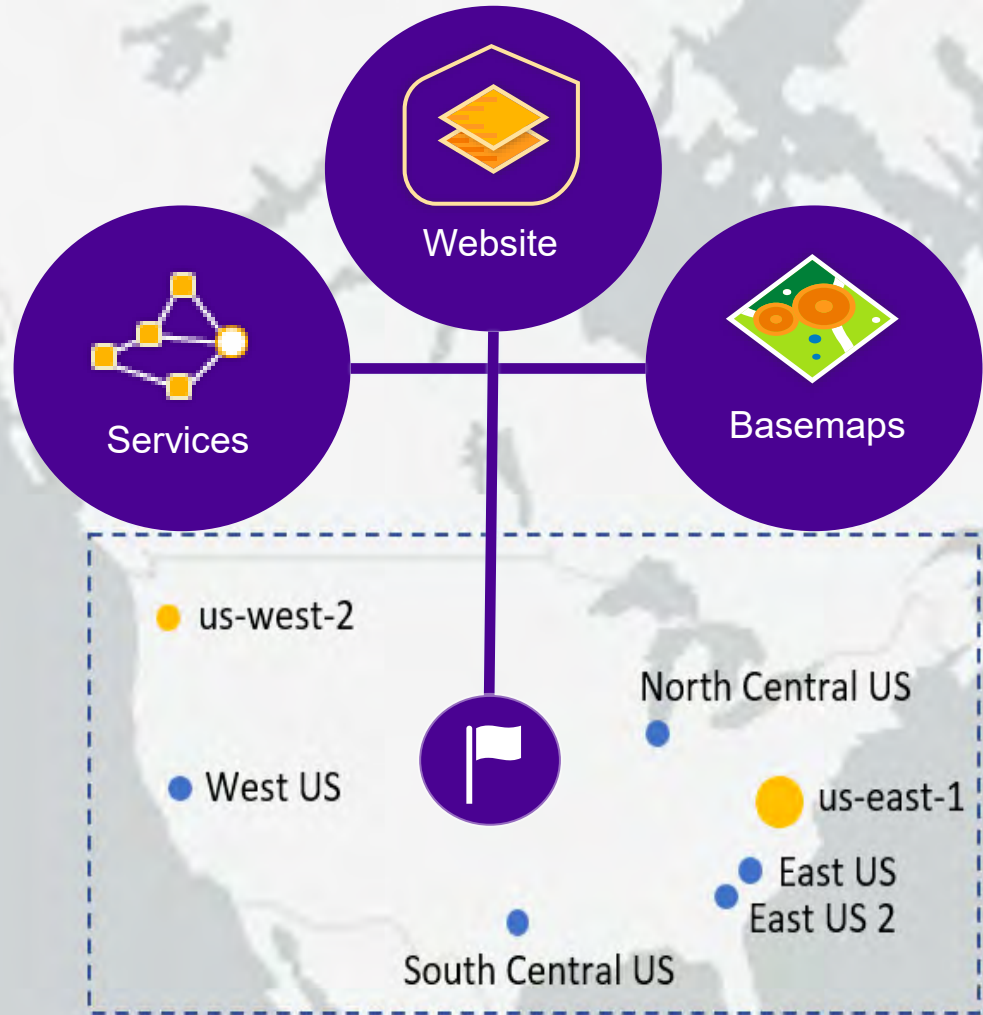
All components located on United States soil for US customers



US Region

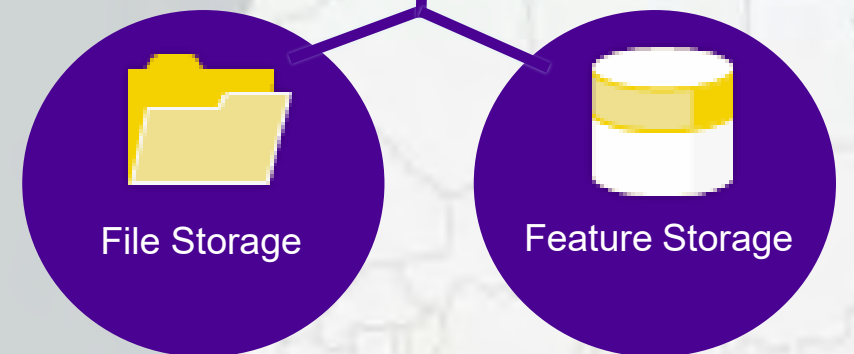
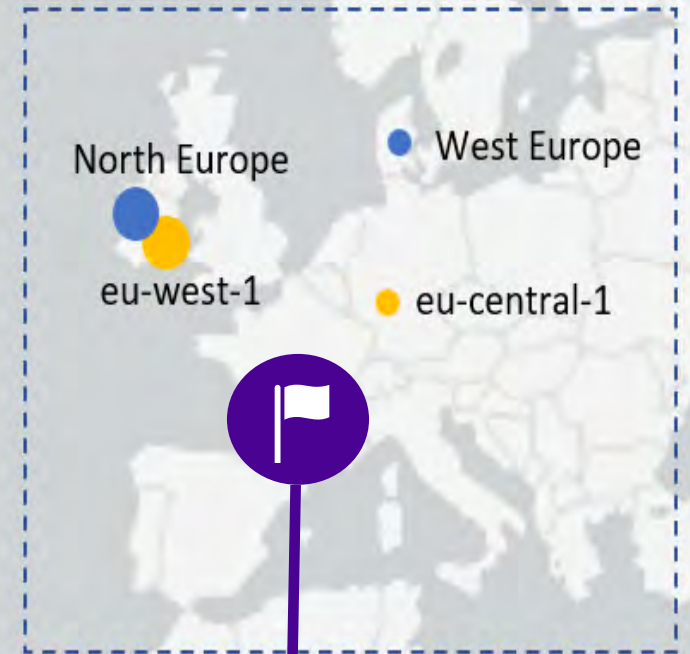
A purple rectangular box containing five icons representing ArcGIS Online services. The icons are arranged in a grid-like fashion. A line from the map on the left points to the top of this box.

- Website**: Represented by a hexagonal icon with three stacked yellow squares.
- Services**: Represented by a network diagram icon with four yellow nodes and connecting lines.
- Basemaps**: Represented by a diamond-shaped icon with a green background and orange circles.
- File Storage**: Represented by a yellow folder icon.
- Feature Storage**: Represented by a white cylindrical icon with a yellow band.



US Region

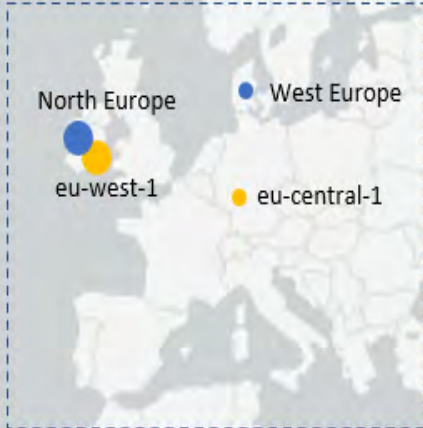
EU Data Region



ArcGIS Online

Datcenters Utilized by EU Customers

- AWS Region
- Azure Region



EU Data Region



AP Data Region



US Region

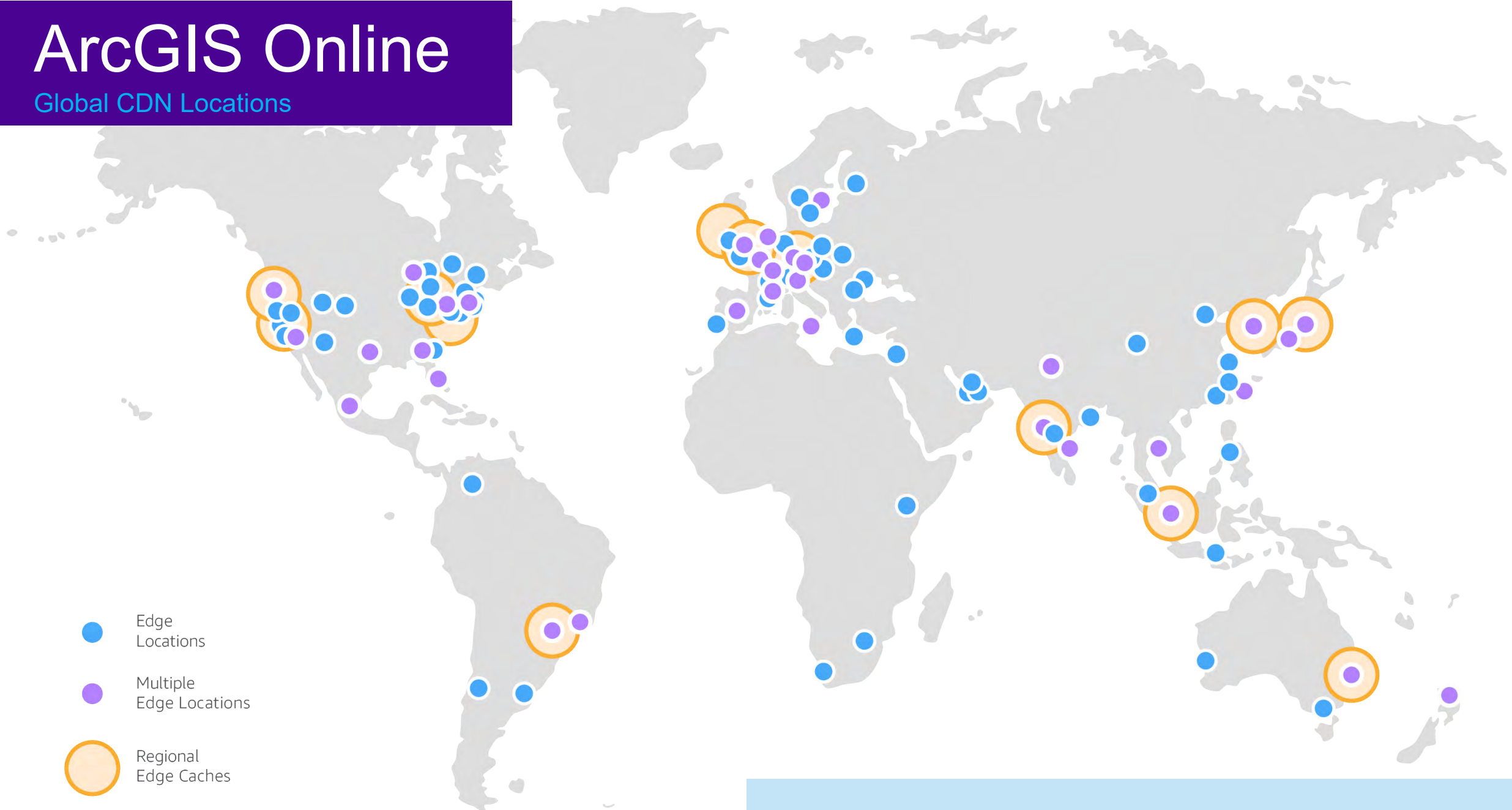
ArcGIS Online

Regional Locations

ArcGIS Online

Global CDN Locations

- Edge Locations
- Multiple Edge Locations
- Regional Edge Caches

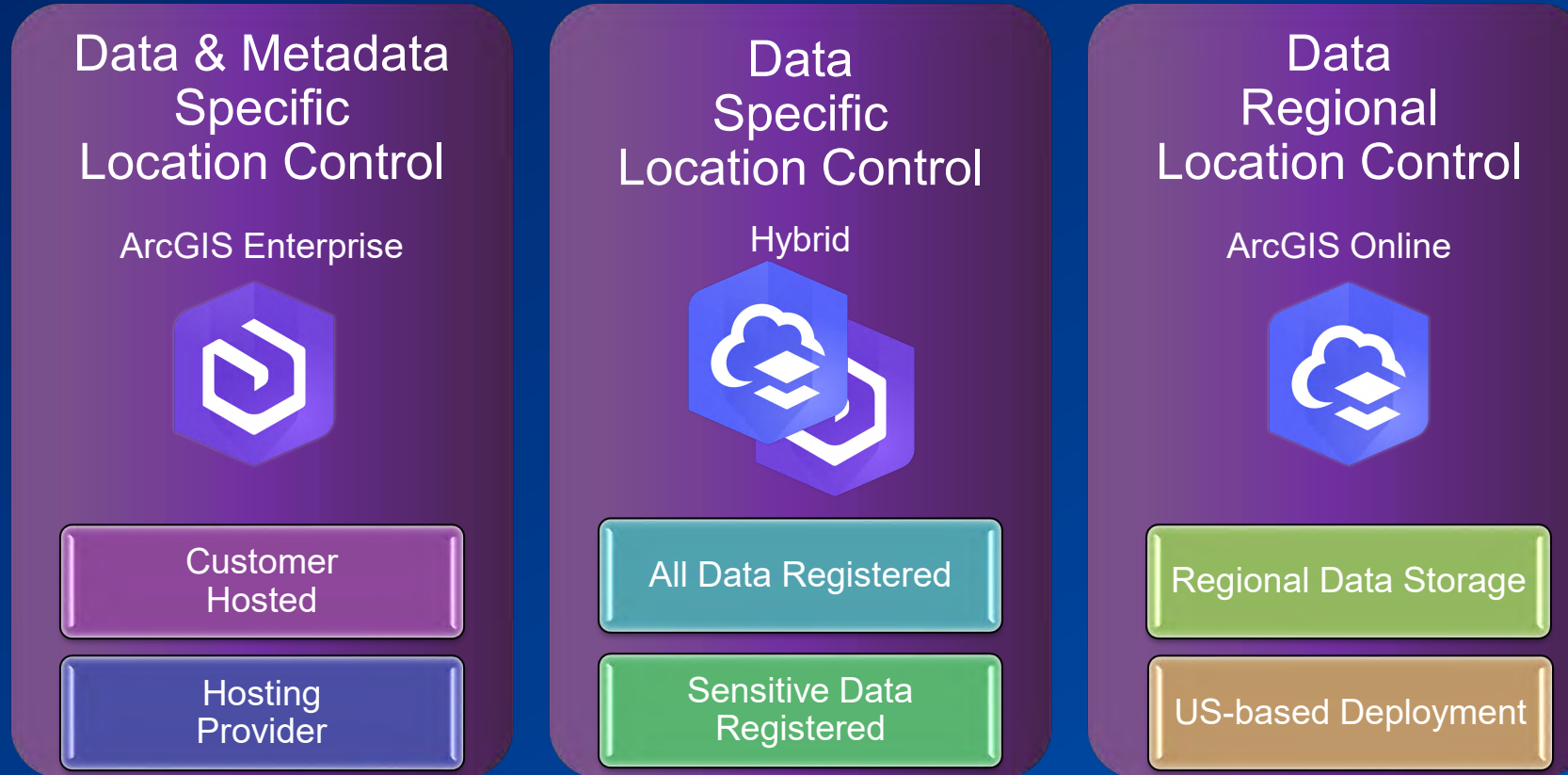


Public datasets cached globally based on-demand

ArcGIS Implementation Patterns



ArcGIS Implementation Patterns



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

Data & Metadata
Specific
Location Control

ArcGIS Enterprise



Customer
Hosted

Hosting
Provider

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

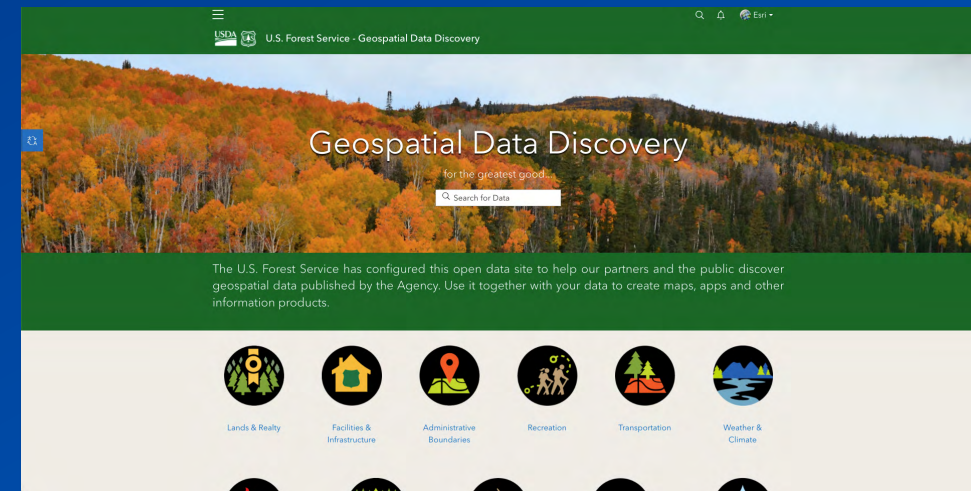
Data
Specific
Location Control

Hybrid



All Data Registered

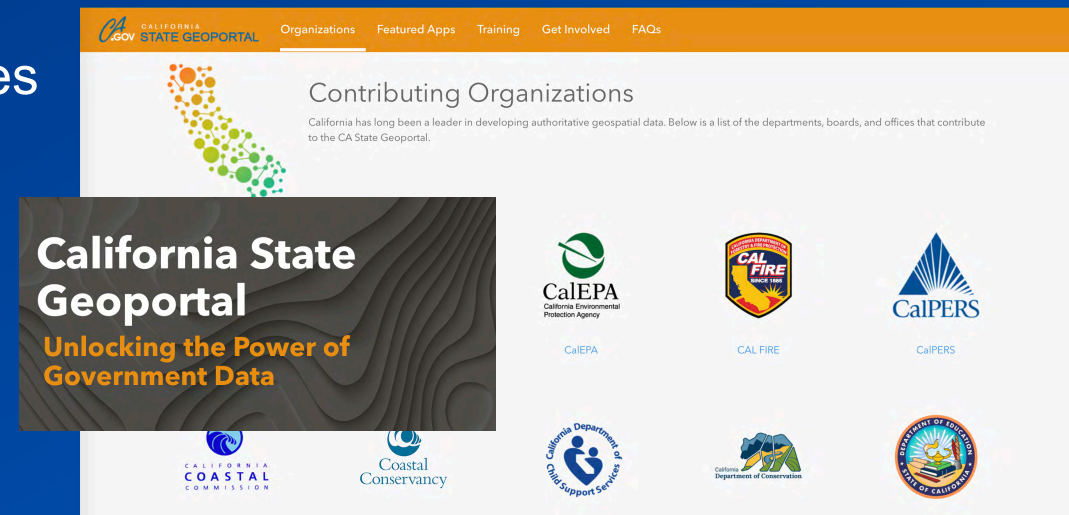
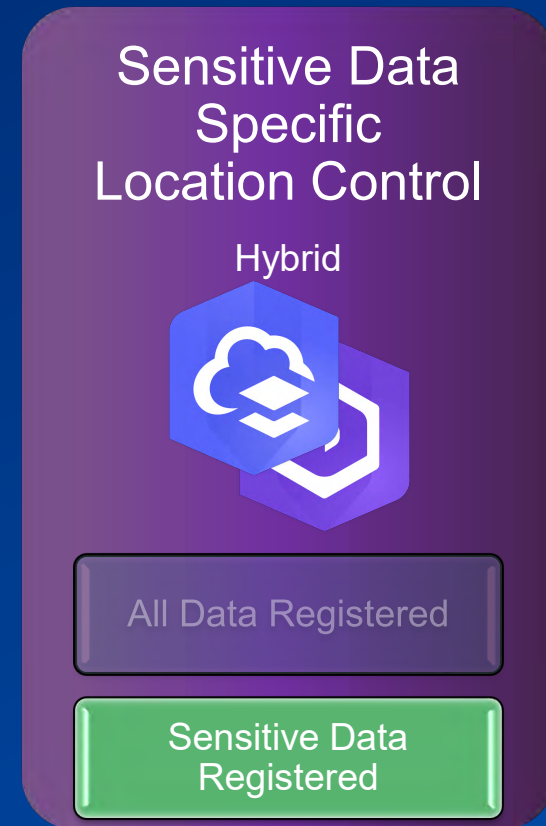
Sensitive Data
Registered



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

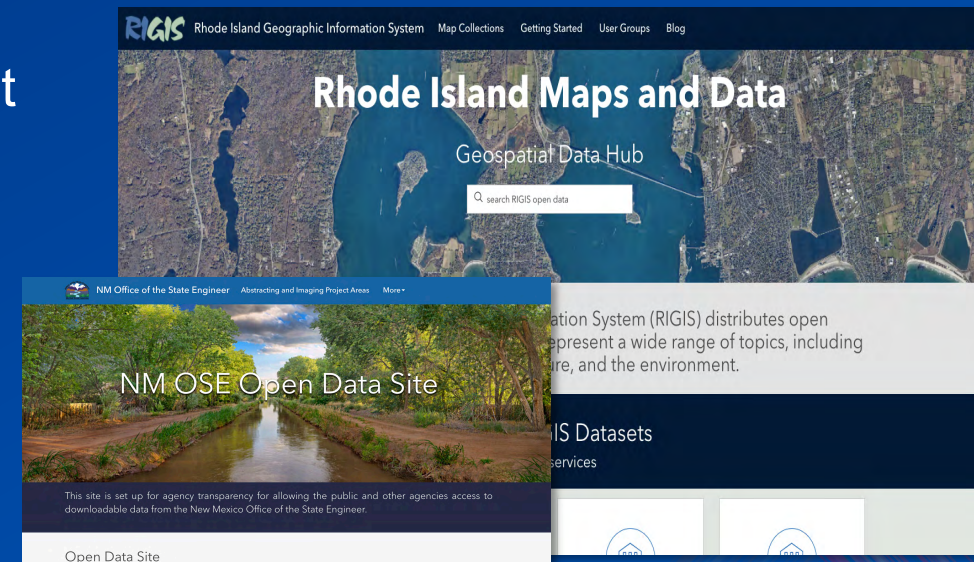
Data
Regional
Location Control

ArcGIS Online



Regional Data Storage

US-based Deployment





Resources & Compliance



ArcGIS Trust Center

<https://Trust.ArcGIS.com>

esri Products Industries Support & Services Stories About

ArcGIS Trust Center Overview Security Privacy Compliance Documents [Launch Security Advisor](#)

Search ArcGIS Trust Center

ArcGIS—Secure and Trustworthy

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

[Report a Security or Privacy Concern](#)

Announcements

- DATA PRIVACY FRAMEWORK PROGRAM**
January 18, 2024
New Hardening Guide, Privacy Certification & More
We kickoff 2024 with a new extensive
- ArcGIS Security Advisory**
December 14, 2023
Portal for ArcGIS Enterprise Sites 2023 Security Patch
An update regarding the ArcGIS Enterprise
- ArcGIS Security Advisory**
August 18, 2023
ArcGIS Server Map and Feature Service Security 2023 Update 1
- ArcGIS Security Advisory**
August 18, 2023
Action Required: ArcGIS Online SAML Customers
Customers that have configured the SAMI

ArcGIS Security & Privacy Adviser

esri ArcGIS Security & Privacy Adviser

Welcome Sign-out

Application Modules

- Settings Advisor
- Member Logs
- Organization Logs
- Public Survey123 Check
- Publicly Shared Items
- Public FS Edit Check
- Feedback
- Help

CRITICAL: There are items that need your immediate attention.

My Organization Settings Rescan Help

- ✓ Access and Permissions help
- ✗ Sharing and Searching help
- ⚠ Password Policy help

help

✓ Access and Permissions

- ✓ HTTPS Only Access
- ✓ Prevent Anonymous Access
- ✓ Standardized SQL Queries
- ✓ Modify Biography Information

Enable this setting to allow members to modify the biographical information and specify who can see their profile.

This setting is disabled.

Organization members are not allowed to modify their profile information. By having this setting disabled, it prevents members from accidentally storing Private Information (PI) data in their profile.

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

Example of a privacy check to minimize PII

Demo of latest beta available @ the Open Location Security & Privacy kiosk

ArcGIS Technical Papers



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



Topic	Recommended Option	ArcGIS Enterprise - 10.7.1 Base Deployment				ArcGIS Online		
		Provided by Esri	Default	Configurable	Validation Tool	Provided by Esri	Default	Configurable
HTTPS and Encryption								
	Stewards HTTPS T.5.1.2 Only	Yes	Yes	Yes	Scan.py	Yes	Yes	Yes
	Enforce HTTPS via HSTS	Yes	No	Yes		Yes*	Yes	No
	Configure Preferred Encryption Algorithms	Yes	Yes	Yes		Yes	Yes	No
	Website endpoint CA Certificates	No	No	Yes		Yes	Yes	No
	SAVIL DP CA Certificates	No	No	Yes		No	No	Yes
	Enforce data storage encryption	No	No	Yes		Yes	Yes	No
	Remove self signed certs	Yes	No	Yes	Scan.py	Yes	Yes	No
HTTP Header Config								
	X-Content-Type-Options: NOSNIFF	Yes	Yes	Yes		Yes	Yes	No
	X-XSS-Protection	Yes	Yes	No		No	No	No
	X-Frame-Options	Yes	Yes*	No		Yes	Yes	No
Interfaces								
	Disable Services Directory	Yes	No	Yes		No	No	No
	Disable Portal Directory	Yes	No	Yes	Scan.py	Yes	Yes	No
	Limit access to Admin Resources via Web Adaptor	Yes	No	Yes		No	No	No
	Understand Dynamic Workspace usage	Yes	Yes	Yes		No	No	No
	Secure System Services	Yes	Yes	Yes		Yes	Yes	No
Standardized Filtering								
	Enforce Standardized Queries	Yes	Yes	Yes		Yes	Yes	Yes
	Filter Web Content Disabled	Yes	Yes	Yes		Yes	Yes	No
Authentication and Authorization								
	Utilize Enterprise Login via SAML instead of Built-in	No	No	Yes		No	No	Yes
	Block members joining org with social network credentials	No	No	No		Yes	No	Yes
	Define a password Complexity Policy	Yes	Yes	Yes		Yes	Yes	Yes
	Use Enterprise user store with account lockout policy	Yes	Yes	Yes		Yes	Yes	Yes
	Configure a shorter token expiration period	Yes	Yes	Yes		Yes	Yes	Yes
	Configure Multi-factor Authentication	No	No	Yes		Yes	No	Yes
	Disallow user account self-creation	Yes	Yes	Yes	Scan.py	Yes	Yes	Yes
	Define Custom Roles	Yes	No	Yes		Yes	No	Yes
	Disable Anonymous Access	Yes	No	Yes		Yes	No	Yes
	Configure role based access control	Yes	Yes	Yes		Yes	Yes	Yes
	Disallow token generation via GET	Yes	Yes	Yes	Scan.py	Yes	Yes	No
Web Tier Technologies								
	Use a WAF/Web Filter	No	No	Yes		Yes	Yes	No
	Utilize load balancer instead of Web Adaptor	No	No	Yes		Yes	Yes	No
	Web Adaptor utilized for IWA only inside organization	Yes	Yes	Yes		No	No	No
	Remove Technology identifiers and banners	Yes	Yes	No		Yes	Yes	No
	Use Data Loss Prevention (DLP)	No	No	Yes		No	No	No
	Define Allowed MIME types	No	No	Yes		No	No	No
Data Ownership & Privacy								
	Prevent users from sharing publicly	Yes	Yes	Yes		Yes	Yes	Yes
	Disallow biography edits and visible profiles	Yes	Yes	Yes		Yes	Yes	Yes
	Limit search to your organization only	Yes	Yes	Yes		Yes	No	Yes
	Remove social media links in item details/group pages	Yes	Yes	Yes		Yes	Yes	Yes
	Do not allow members of other organizations to sign in	No	No	No		Yes	No	Yes
	Define specific allowed Portals for Access	Yes	No	Yes		Yes	No	Yes
	Validate Distributed Collaborations	Yes	No	Yes		Yes	No	Yes
	Disable End User Experience Improvement Program (UEIP)	No	No	No		Yes	No	Yes
	Identify Authoritative Content	No	No	No		Yes	No	Yes
	Configure Access Notice	Yes	No	Yes		Yes	No	Yes
Server Trust Relationships								
	Define trusted servers	Yes	No	Yes		Yes	No	Yes
	Define allowed proxy hosts	Yes	No	Yes	Scan.py	Yes	No	Yes
	Define Cross Origin Policy	Yes	No	Yes		Yes	No	Yes
Sharing Best Practices								
	Create and document content review policy	No	No	Yes		No	No	Yes
	Create and document sharing review policy	No	No	Yes		No	No	Yes
	Validate need for editable layers	Yes	No	Yes		Yes	No	Yes



AN ESRI
TECHNICAL PAPER

April 2024

ArcGIS Enterprise Hardening Guide

[Click here to download latest guide from the ArcGIS Trust Center](#)

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



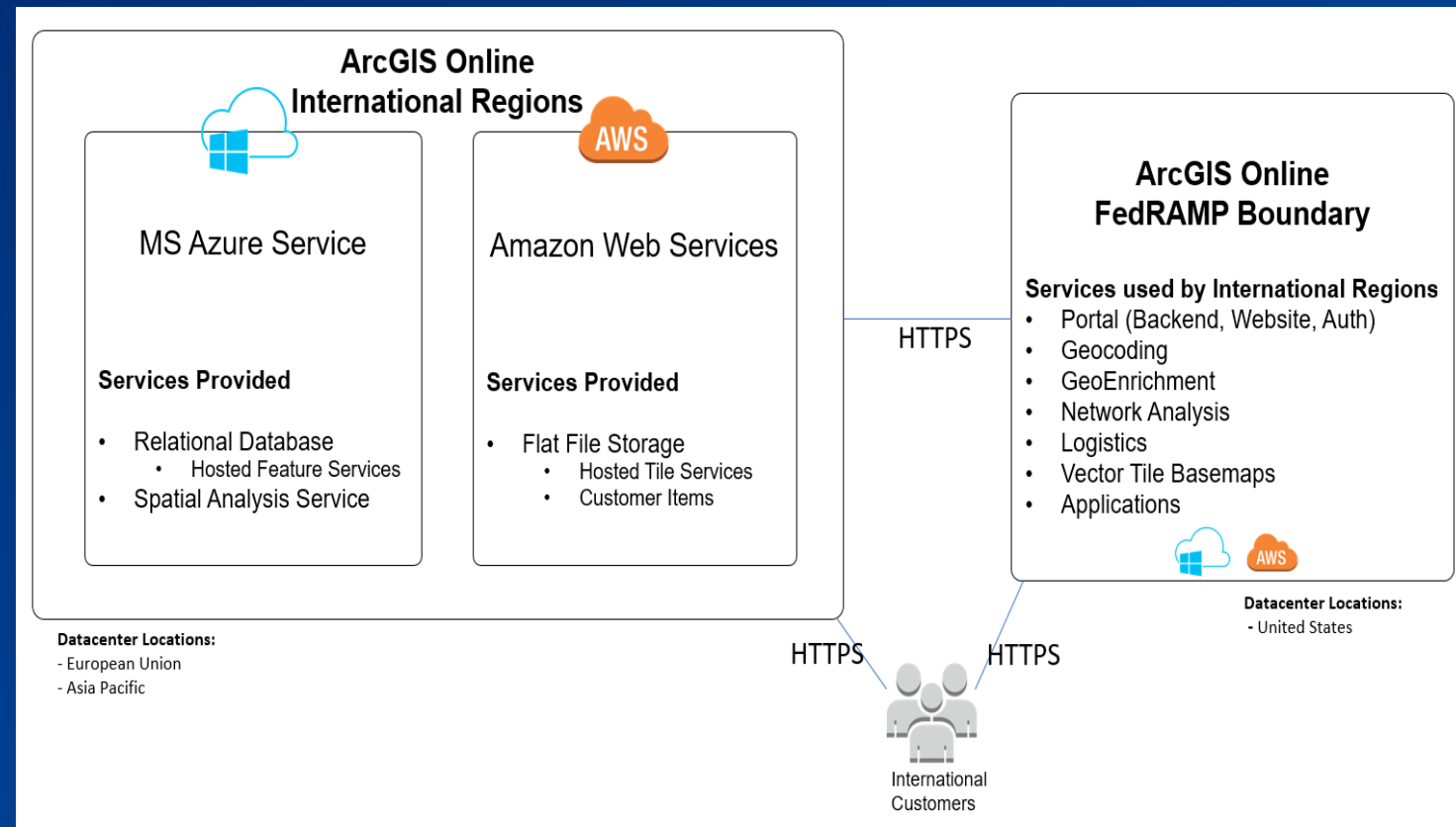
Compliance

- ArcGIS Online FedRAMP Boundary

- Running @ FedRAMP Moderate since 2023
- FedRAMP to ISO27k mapping in Trust Center
- Covers US-based operations/systems

- ArcGIS Online and ArcGIS Location Platform Regions

- Today
 - Security assurance of underlying providers
 - Microsoft Azure and Amazon Web Services
- Mid-2025
 - ISO 27k EU Region compliance
- Future Additional Regions





Conclusion





Conclusion

- Esri Actions Taken

- DPA supplementary measures and contractual clauses
- EU-US Data Privacy Framework Certification
- 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 Adviser
 - ArcGIS Enterprise Hardening Guide
- 



esri[®]

**THE
SCIENCE
OF
WHERE**[®]

Copyright © 2024 Esri. All rights reserved.