ArcGIS Online – A multi-tenant system

Portal

User Data

Hosted Services

Tasks
Agenda

- Information Security
  - Online Platform Security
  - Deployment Scenarios
  - Infrastructure Security
Online Platform Security
Information Model

- Portal
- Groups
- Items
- Users
Items

- Typed
  - Web Map
  - Services
  - ...
- Private by default
- Shared to
  - Groups
  - Organization
  - Everyone/Public
Users

- Users own items and groups
- Only owners can update items
- Users have roles
  - Administrators
  - Publishers
  - Users
  - Custom
- Users have a profile
- Visible to
  - No one
  - Organization
  - Everyone
Groups

- Have users and items
- All users in a group have access to the items within that group
- Users share their items to groups they are members of
- Group owners can share items to their own groups
- Groups can be visible to:
  - No one (private)
  - Organization
  - Everyone
Security Options

• Force SSL
  - User credentials are always over SSL
  - ArcGIS Online will reject non-SSL requests

• Standardized Queries

• Enterprise Logins using SAML
Still concerned about information security?

- Portal for ArcGIS
- ArcGIS for Server
Deployment Scenarios
Deployment Scenarios

ArcGIS Platform

Capability

Portal
- SDKs
- online
- Maps
- Apps

GIS Services Infrastructure
- Data Tier
- GIS Servers

Content
- Geoenrichment
- Basemaps

SaaS
In the Cloud

ArcGIS Online for Organizations

Software
In your Infrastructure

Portal for ArcGIS

ArcGIS for Server

Data Appliance for ArcGIS
Deployment Scenarios

Basic Options

- **Intranet**
  - **Public**
  - **Hybrid 1**
  - **Hybrid 2**
  - **In Your Infrastructure**
  - **Cloud**
  - **On-premise**

- **Online**
  - **Server**

- **Portal**
  - **Read-only Basemaps**
  - **Server**

- **On-premise**
Deployment Scenarios
FISMA Low Accredited 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 – Business Operations
  - Hybrid deployment of ArcGIS Server and ArcGIS Online
  - Share operational data within or between organizations
  - Sensitive data maintained on your infrastructure or other accredited environment
  - ArcGIS Online operates as a discovery portal
  - Utilize Enterprise Logins
Deployment Scenarios

Hybrid

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

• **What is stored in AGOL? – 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 Scenarios
Hybrid – Data sources

• 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 SSL or even a VPN connection could be used between the device browser and on-premises system
Infrastructure Security
Infrastructure Security

Cloud Infrastructure

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

Cloud Infrastructure Security Compliance
Infrastructure Security

Compliance

• **Products & Services**
  - FISMA Low - ArcGIS Online
  - FedRAMP - Esri Managed Cloud Services (EMCS - Coming late 2014)

• **Solutions**
  - Validated guidance coming
  - CJIS- Law enforcement, HIPAA – Healthcare, STIGS - Defense

• **Corporate**
  - ISO 27k – Corporate Security Charter Basis
  - SSAE16 – Esri Datacenter Operations
  - Safe Harbor – Privacy assurance
Infrastructure Security

Layers of responsibility & assurance

Cloud Provider
ISO 27001
SSAE16
FedRAMP Mod

Customer

Esri

Web App Consumption

ArcGIS Management

Web Server & DB software

Operating system

Instance Security Management

Hypervisor

Physical

AGOL SaaS
FISMA Low (USDA)
SafeHarbor (TRUSTe)

Data from: Infrastructure Security
Infrastructure Security

Standards

• Enterprise Logins
  - SAML 2.0
  - Provides federated identity management
  - Integrate with your enterprise LDAP / AD
  - Online help and runbooks available for some vendor identity providers

• API’s to Manage users & app logins
  - Developers can utilize OAuth 2-based API’s
1. **Where is my data?**
   - All ArcGIS Online data and processing resides within US Data centers on US soil

2. **Is my information encrypted?**
   - Organization administrator can force SSL encryption for all communications
   - ArcGIS Online does not encrypt data at rest;
   - Sensitive items can be encrypted by 3rd party solutions or supplemented with a hybrid of EMCS

3. **Is my data locked into ArcGIS Online?**
   - Data publishers can extract and download data back to their organization via shapefiles, CSVs, or original publication package.
ArcGIS Online Security

Additional Resources

- **Trust ArcGIS Site - NEW**

- **ArcGIS For Professionals Site**
  - [http://pro.arcgis.com/enterprise-gis/](http://pro.arcgis.com/enterprise-gis/)

- **Professional Services**
  - ArcGIS Security Architecture 2-day Workshop
  - SecureSoftwareServices@esri.com

- **ArcGIS Online - Cloud Security Alliance (CSA)**
  - Standardized security answers