ArcGIS Online: A Security, Privacy, and Compliance Overview

Andrea Rosso – Lead Architect

Michael Young – CISO - Products
ArcGIS Online – A Multi-Tenant System
Agenda

• Online Platform Security
• Deployment Architecture
• Infrastructure and Compliance
Platform Security
Andrea Rosso
Portal Information Model

Groups

Portal

Items

Users
Items

<table>
<thead>
<tr>
<th>Title</th>
<th>Type</th>
<th>Modified</th>
<th>Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire Surveys</td>
<td>Feature Layer</td>
<td>Jul 17, 2015</td>
<td>Not Shared</td>
</tr>
<tr>
<td>Restaurant Finder</td>
<td>Web Map</td>
<td>Jul 16, 2015</td>
<td>Not Shared</td>
</tr>
<tr>
<td>Store Closures</td>
<td>CSV</td>
<td>Jul 17, 2015</td>
<td>Not Shared</td>
</tr>
<tr>
<td>USA Congressional Districts</td>
<td>Layer Package</td>
<td>Jul 16, 2015</td>
<td>Not Shared</td>
</tr>
<tr>
<td>Wildfires</td>
<td>Web Map</td>
<td>Jul 16, 2015</td>
<td>Not Shared</td>
</tr>
<tr>
<td>Yellowstone</td>
<td>Map Document</td>
<td>Jul 16, 2015</td>
<td>Not Shared</td>
</tr>
</tbody>
</table>

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

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

• 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

- **Custom Roles**
  - Templates
  - Fine Grained Privileges

- **Use Cases**
  - Restrict Access
  - Restrict Credits
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
- Use cases
  - Access
  - Collections
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
Feature Service Editing

- **Users who always can edit**
  - Owner
  - Admins
  - Members of Groups w/ Update

- **Enable Editing**
  - Options
    - Add, update and delete features
    - Update feature attributes only
    - Add features only
  - Anyone who can access the service

- Custom Roles can have Edit or Edit with full control privileges
Admin Organization Controls

• Sharing to Public
• Use all SSL/TLS
• Anonymous Access
• Standardized Queries
• Trusted Servers
• Purchasers
• Admin Contacts
• Disable Bio
Administrator Controls on Users

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

ArcGIS Online

Esri Access

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

Third Party Applications

Login
Authentication Options

**Enterprise Logins**

**Password**

- Sign in to UC 2015
- Username
- Password
- Keep me signed in
- SIGN IN
- Forgot password?  Forgot username?

**Multi-Factor**

- Sign in to UC 2015
- Use your authentication app to generate a six-digit code in order to complete the sign in process.
- Enter the code your app provided:
- Ten digit code
- VERIFY
- Having trouble signing in with your code?

**Password Policies**

- 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 [ ] 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
- UPDATE PASSWORD POLICY  CANCEL

**Enterprise Logins**

- Set Identity Provider
- Specify the properties to establish your organization's Enterprise Identity Provider:
  - Name:
  - Your users will be able to join:
    - Automatically
    - Upon Invitation from an administrator
  - Metadata for the Enterprise Identity Provider will be supplied using:
    - A URL
    - A File
    - Parameters specified here
- URL: [http://yoursite.net/identity](http://yoursite.net/identity)
- Other advanced settings:
- SET IDENTITY PROVIDER  CANCEL
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
Password Policies

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

• Status Reports
  - Credits
  - Content
  - Members
  - Groups
Deployment Architecture
Michael Young
Deployment Architecture

Options

ArcGIS Online

Managed Services

Cloud Images

On Premises
Deployment Architecture

Responsibility

**On-premises**

- ArcGIS Server
- OS/DB/Network
- Security Infrastructure
- Virtual / Physical Servers

**Cloud Images**

- ArcGIS Server
- OS/DB/Network
- No Security Infrastructure by default
- Cloud Infrastructure (IaaS)

**Managed Services** *FedRAMP Moderate*

- ArcGIS Server
- OS/DB/Network
- Security Infrastructure
- Cloud Infrastructure (IaaS)

**ArcGIS Online** *FISMA Low*

- ArcGIS Online
- OS/DB/Network
- Security Infrastructure
- Cloud Infrastructure (IaaS)

Customer Responsibility  
Esri Responsibility  
CSP Responsibility
Deployment Architecture
Hybrid Growth

By 2018, at least 40% of enterprises will have evolved toward a hybrid data center model...

...with one or more strategic partners for the purposes of supporting digital business services.

*Select the Right IT Service Continuity Targets for Recovery, Availability and Budget Allocation, Published 8 June 2015, Analysts: John P. Morency, Carl Claunch, Gartner #G00274506.

Hybrid IT blends legacy protection with the fast provisioning and future-proof scalability of the cloud, helping you battle the barrage of web-based business activity.
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

Anonymous Access

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

**Deployment Architecture**
**User Scenario – ArcGIS Online + Cloud Images**

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

**ArcGIS Online**
- Rapid Deployment (SaaS)
- Low TCO
- Data: Low Impact
Deployment Architecture
User Scenario – ArcGIS Online + On-Premises

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

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

- Internal Data
- Disconnected
- Integrated Security

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**

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
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
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.

**Deployment Architecture**

**User Scenario – ArcGIS Online + Managed Services**

- Rapid Deployment (SaaS)
- External Data
- SAML (Enterprise Logins)
- Moderate Data
  - 24x7 SOC
  - 4 services levels

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

Esri Managed Cloud Services

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

**Application Architecture**

- **Web Application Firewall (WAF)**
- **ArcGIS for Portal**
- **ArcGIS Server**
- **Relational Database**
- **File Servers**
- **Intrusion Detection (IDS / SIEM)**
- **Centralized Management**
- **Bastion Gateway (MFA)**
- **Authentication/Authorization**
- **Cloud Infrastructure**
  - Hypervisor, TCP/IP, Network ACLs, Routing, Storage, Hardware

**Customer Infrastructure**
- **Public-Facing Gateway**
- **Security Service Gateway**
- **Esri Admin Gateway**

**Security Ops Center (SOC)**

**End Users**

**Esri Administrators**

**Legend**
- **Customer**
- **Application**
- **Cloud Provider**
- **Security**
Deployment Architecture

Common ArcGIS Online Questions

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
Infrastructure & Compliance
Esri Security Compliance

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

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

• ISO 27001
  - Esri’s Corporate Security Charter

• Privacy Assurance
  - US EU/Swiss SafeHarbor self-certified
  - TRUSTed cloud certified
Cloud Infrastructure Provider Compliance

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

Cloud Infrastructure Security Compliance
Product, Services, and Solution Compliance

• Product Based Initiatives
  - ArcGIS Server - DISA STIG
  - ArcGIS Desktop – USGCB

• Service Based Initiatives
  - ArcGIS Online – FISMA Low
  - Esri Managed Cloud Services – FedRAMP Moderate

• Solution Based Guidance
  - CJIS- Law enforcement - Started
  - HIPAA – Healthcare - Future
Privacy & Compliance
Summary Across ArcGIS Online

Privacy
- TRUSTe
- U.S. - EU SAFEHARBOR
- EU-U.S. Privacy Shield
  Under Review

Compliance
- FISMA Authorization & Accreditation
- FedRAMP

Answers
- CSA Cloud Security Alliance
  ArcGIS Online | EMCS
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

Upcoming ArcGIS Online FedRAMP Agency Authorization
  - Cross-cloud provider authorization Azure/AWS
Want to Learn More?
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

Find the session you want to review

Scroll down to the bottom of the session

Answer survey questions and submit