



The ArcGIS Platform: Security Practices and Policy

Esri Software Security & Privacy Team

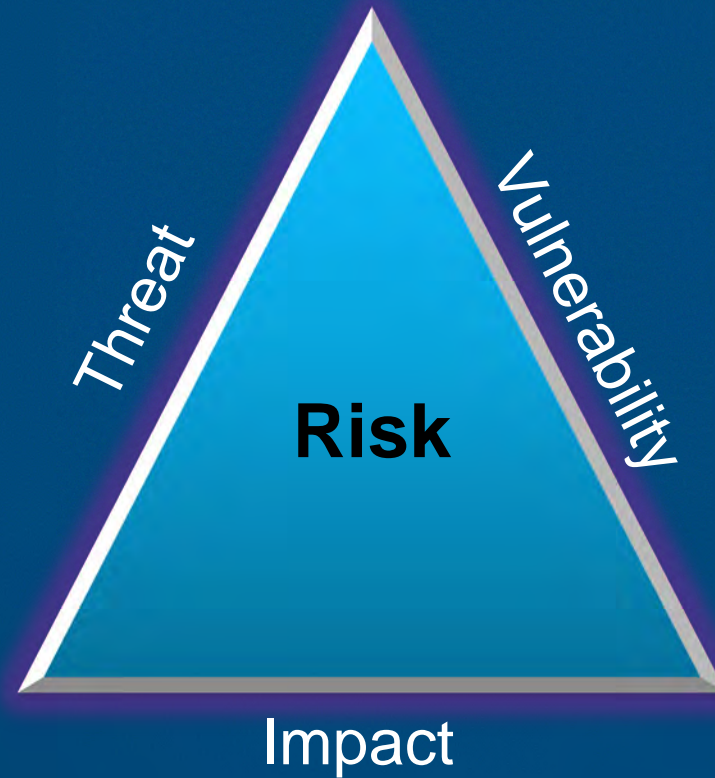


Agenda

- **Introduction**
- **Security Strategy**
 - **Product Based Security Initiatives**
 - **Solution Based Security Initiatives**
- **Deployment Strategy**
- **ArcGIS Server STIG**
- **Esri Managed Cloud Services (EMCS) Advanced Plus**
- **Summary**

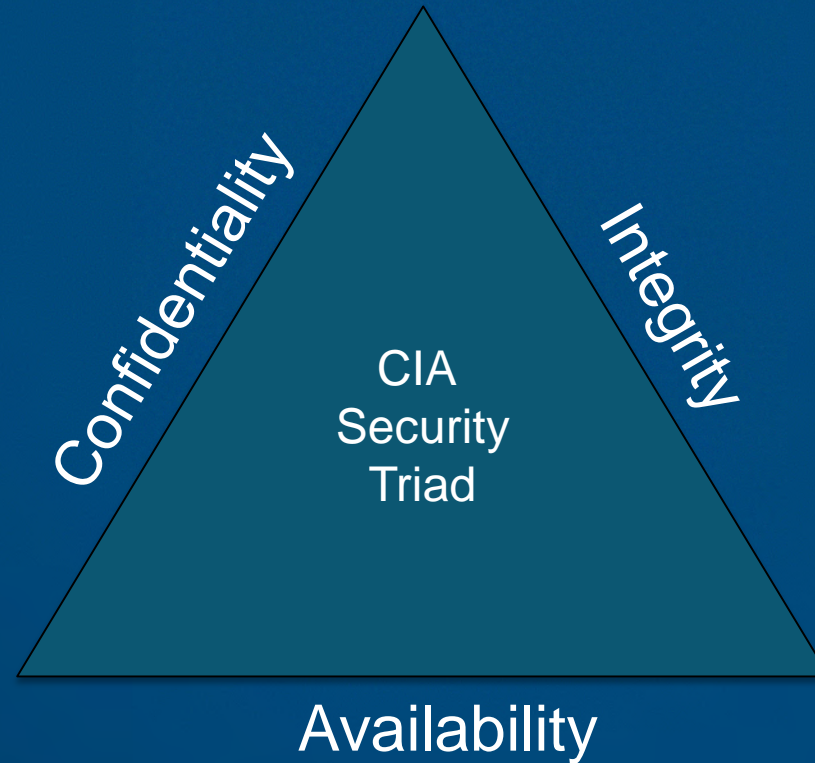
Introduction

It's all about reducing risk



Introduction

Security Principles – CIA Triad





1

Security Strategy



Security Strategy

Evolution of Esri Products & Services



Desktop
GIS

Server
GIS

Web GIS

Distributed
Web GIS



3rd Party Security



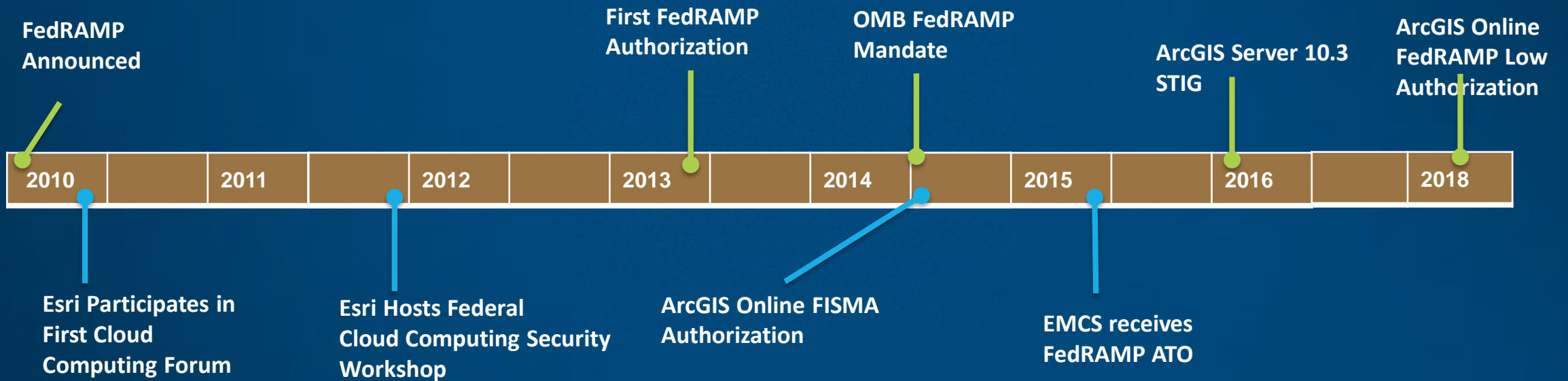
Embedded Security



Shared Responsibility Security

Security Strategy

Extensive security compliance history



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

Security Strategy

Authorization levels across products and services

- **Product Based Initiatives**

- ArcGIS Desktop
- ArcGIS Server
- ArcGIS Enterprise

- **Solution/Service Based Initiatives**

- ArcGIS Online
- Esri Managed Cloud Services Advanced Plus

Product Based Security Initiatives

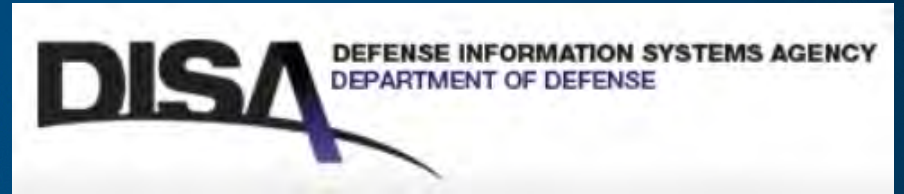
Desktop Clients

- **Esri performs self-certification of desktop products**
 - Ensures smooth product deployments on hardened systems
- **FDCC**
 - **Federal Desktop Core Configuration**
 - **Versions 9.3-10**
 - **Deprecated due to Windows XP focus**
- **USGCB**
 - **United States Government Configuration Baseline**
 - **ArcGIS Desktop Version 10.1+**
 - **ArcGIS Pro 1.4.1 +**



Product Based Security Initiatives

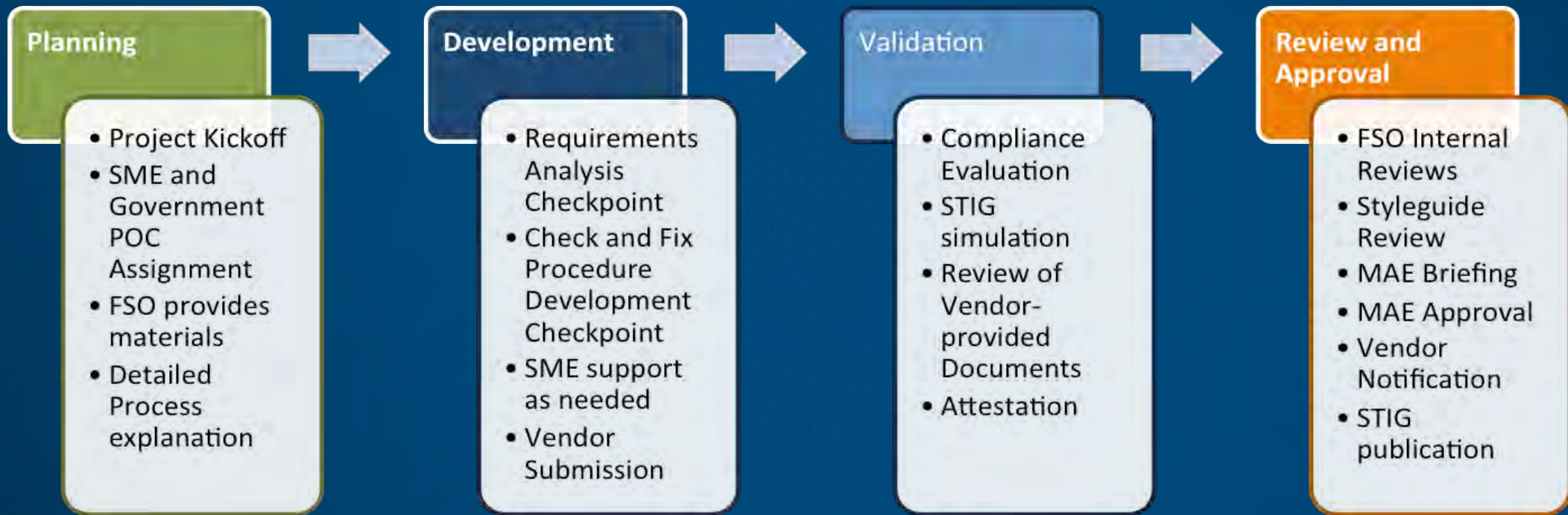
ArcGIS Server – DISA STIG



- **First Esri product Security Technical Implementation Guide (STIG)**
 - Sponsored by government to work with DISA
 - STIG is publically accessible
 - First STIG Windows 2008/2012R2 ArcGIS Server 10.3 (2016)
 - Other STIGs will be performed based on demand
- **STIG usage**
 - STIG input for providing a more general Server hardening guide
 - Enterprise component integration testing and best practices incorporation
 - Immediately implemented by multiple customers upon release in 2016

Product Based Security Initiatives

DISA STIG Creation Process



Product Based Security Initiatives

ArcGIS Server – Awareness of Relative Risk

- Security hardening best practices provide insights into relative risk of different services, and optional mitigation measures to reduce risk

Relative Service Risk

Service	Capability	Default when Enabled	Security Hardened
Map	Mapping	Yellow	Green
Map	Query	Yellow	Green
Feature	Read	Yellow	Green
Feature	Edit	Red	Yellow
Feature	Sync	Yellow	Green
Geocoding	Geocode	Yellow	Green
Geodata	Query	Yellow	Green
Geodata	Data Extraction	Red	Green
Geodata	Replica	Red	Yellow
Geoprocessing	Geoprocessing	Red	Yellow
Image	Imaging	Yellow	Green
Image	Edit	Red	Yellow
Image	Upload	Yellow	Green

Red = Higher Risk
 Yellow = Average Risk
 Green = Low Risk

Security Hardened Settings

- Map Services
 - Disable “Feature Access”
 - Disable “Mobile Data Access”
 - Disable “WFS”
 - Disable “Query”
 - Publish File Geodatabases
- Feature Services
 - Always Secure
 - Use Versioned Data
 - Disable “Sync”
 - Disable “Insert, Update, Delete”
- Geocoding Services
 - Publish File Geodatabases
- Geodata Services
 - Always Secure
 - Use Versioned Data
 - Grant ArcGIS Account Read-Only (RBDMS)
- Geoprocessing Service
 - Risk Varies by Script/Model Design
 - Limit Inputs
- Globe Service
 - Publish File Geodatabases
 - Disable “Query”
- Image Service
 - Disable “Edit”
 - Disable “Upload”

Providing new insights

Product Based Security Initiatives

Security validation and monitoring

- **ArcGIS Server and Portal security scan tool**
 - **Validates best practices**
 - **Server and Portal 10.4 +**
 - **Python script**

SS05	Critical	Filter web content enabled	Generates a list of feature services where the filter web content property is disabled. Disabling this property allows a user to enter any text into the input fields, which exposes the service to potential cross-site scripting (XSS) attacks. This property is enabled by default and unless unsupported HTML entities or attributes are required, it should not be disabled.
SS06	Critical	System folder permissions	Determines if non-default permissions are applied to the System folder in Server Manager. By default, only administrators and publishers should have access to the services in the System folder.
SS07	Important	REST services directory	Determines if the REST services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks.
SS08	Important	Cross-domain limitations	Determines if cross-domain requests are limited to specific domains. To reduce the possibility of an unknown application sending malicious commands to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust.

Solution Based Security Initiatives

ArcGIS Online

- **ArcGIS Online**
 - **FISMA Low ATO by USDA (2014)**
 - **FedRAMP Tailored Low by DOI (2018)**
- **Cloud Infrastructure Providers are ISO 27001 and FedRAMP Moderate compliant**
 - **Amazon Web Services**
 - **Microsoft Azure**

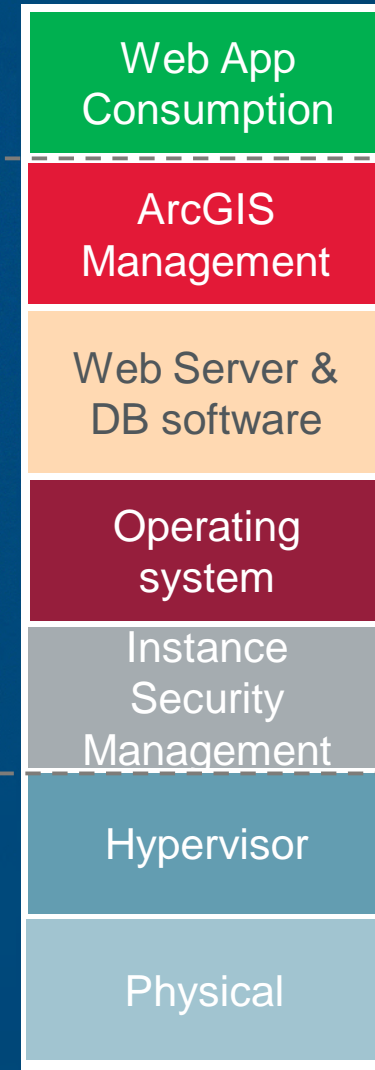


Solution Based Security Initiatives

ArcGIS Online Assurance Layers

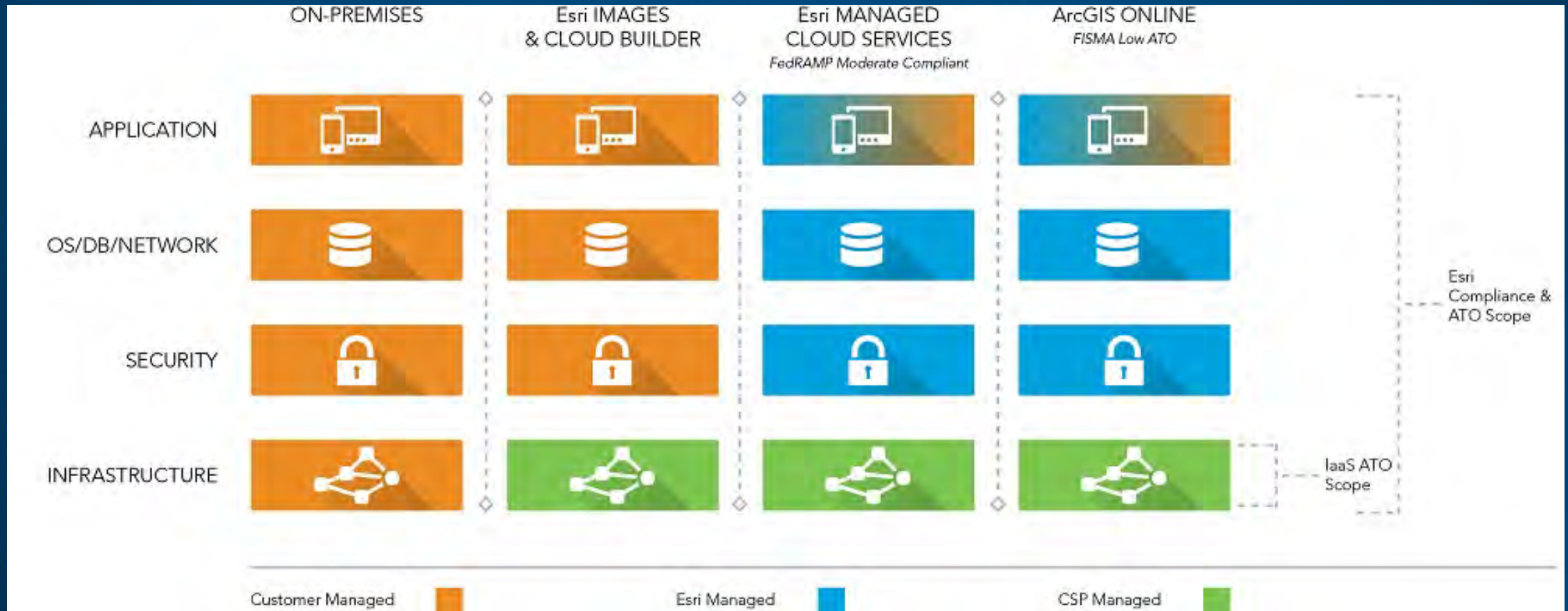
AGOL SaaS
FISMA Low
(USDA)

Cloud Provider
ISO 27001
SSAE16
FedRAMP Mod



Solution Based Security Initiatives

Cloud deployment model responsibility





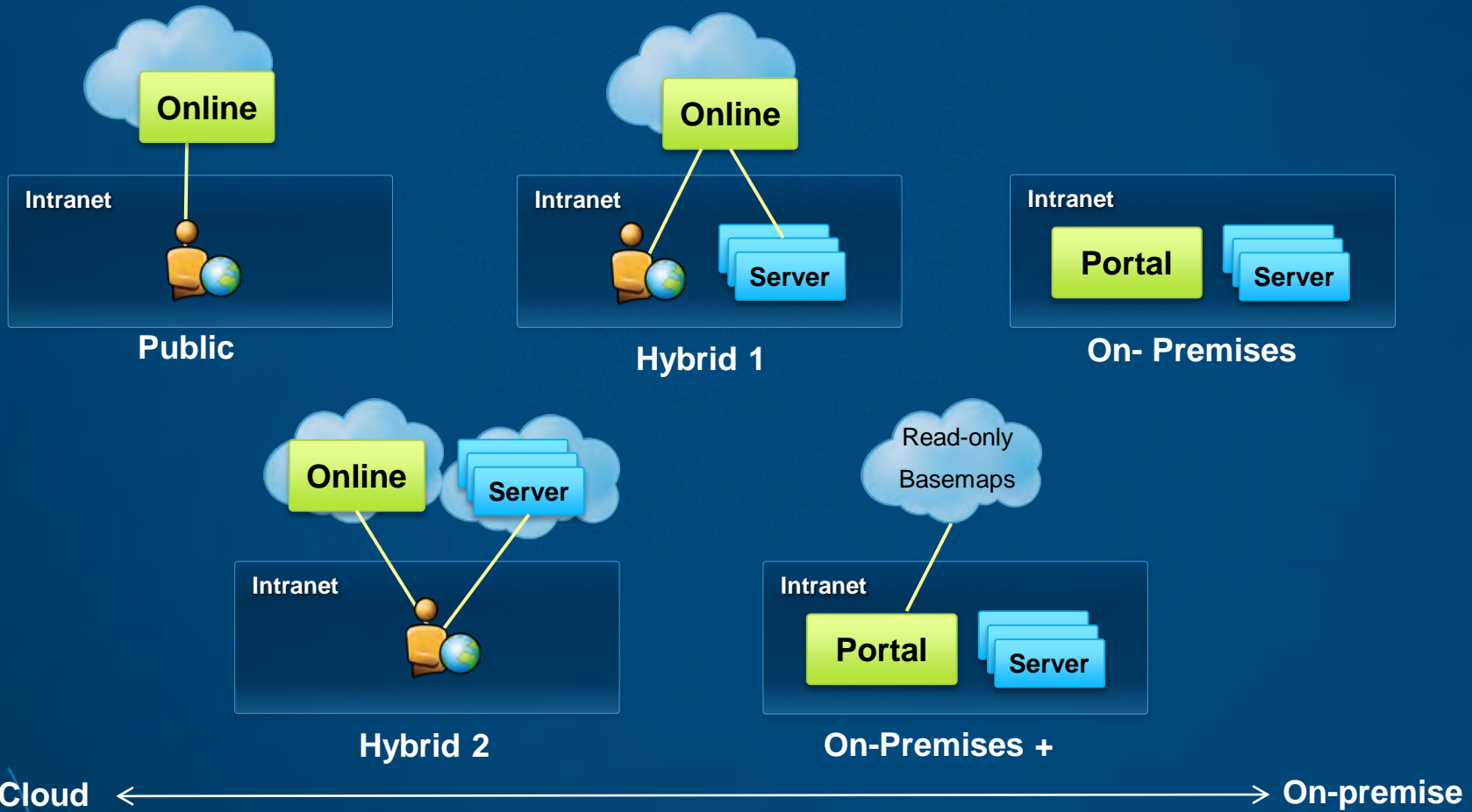
2

Deployment Strategy



Deployment Strategy

Deployment Models



Deployment Strategy

Real Permutations

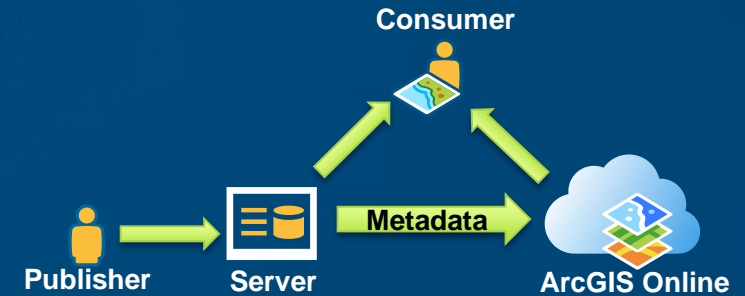
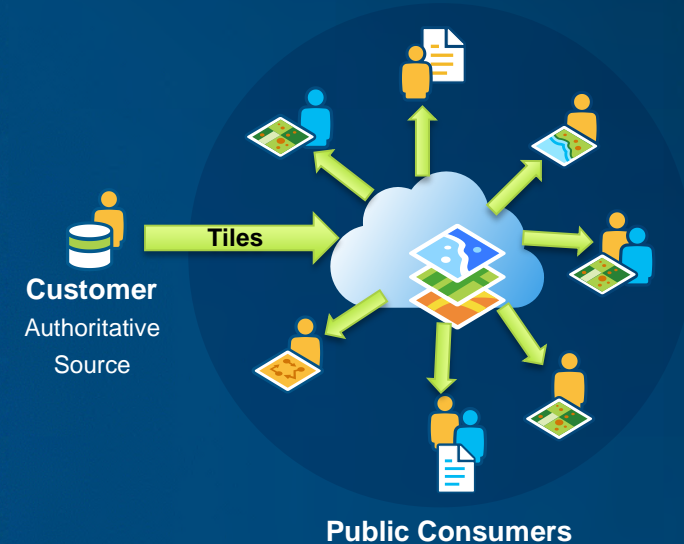


Deployment Strategy

ArcGIS Online Accreditation 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 sites

- **Use Case 2 – USG Internal Operations**
 - Hybrid deployment of ArcGIS Server and ArcGIS Online
 - Share operational data within or between organizations
 - Sensitive data maintained on customer premises or other accredited environment
 - ArcGIS Online operates as a discovery portal
 - Utilize Enterprise Logins

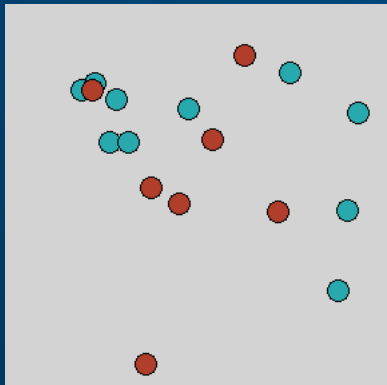


Deployment Strategy

Hybrid – How does it work?

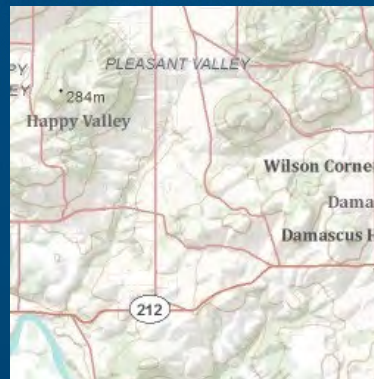
- Where are internal and cloud datasets combined?
 - At the browser
 - The browser makes separate requests for information to multiple sources and does a “mash-up”
 - Token security with HTTPS (TLS) or even a VPN connection could be used between the device browser and on-premises system

On-Premises Operational
Layer Service



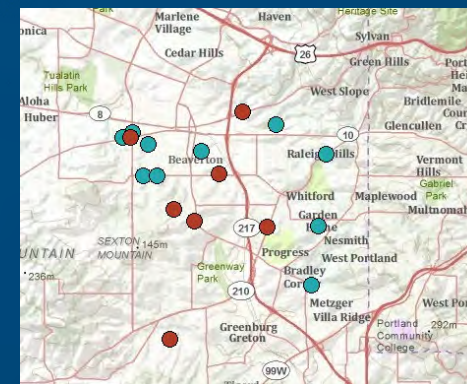
<https://YourServer.com/arcgis/rest...>

Cloud Basemap Service
ArcGIS Online



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

Browser Combines Layers



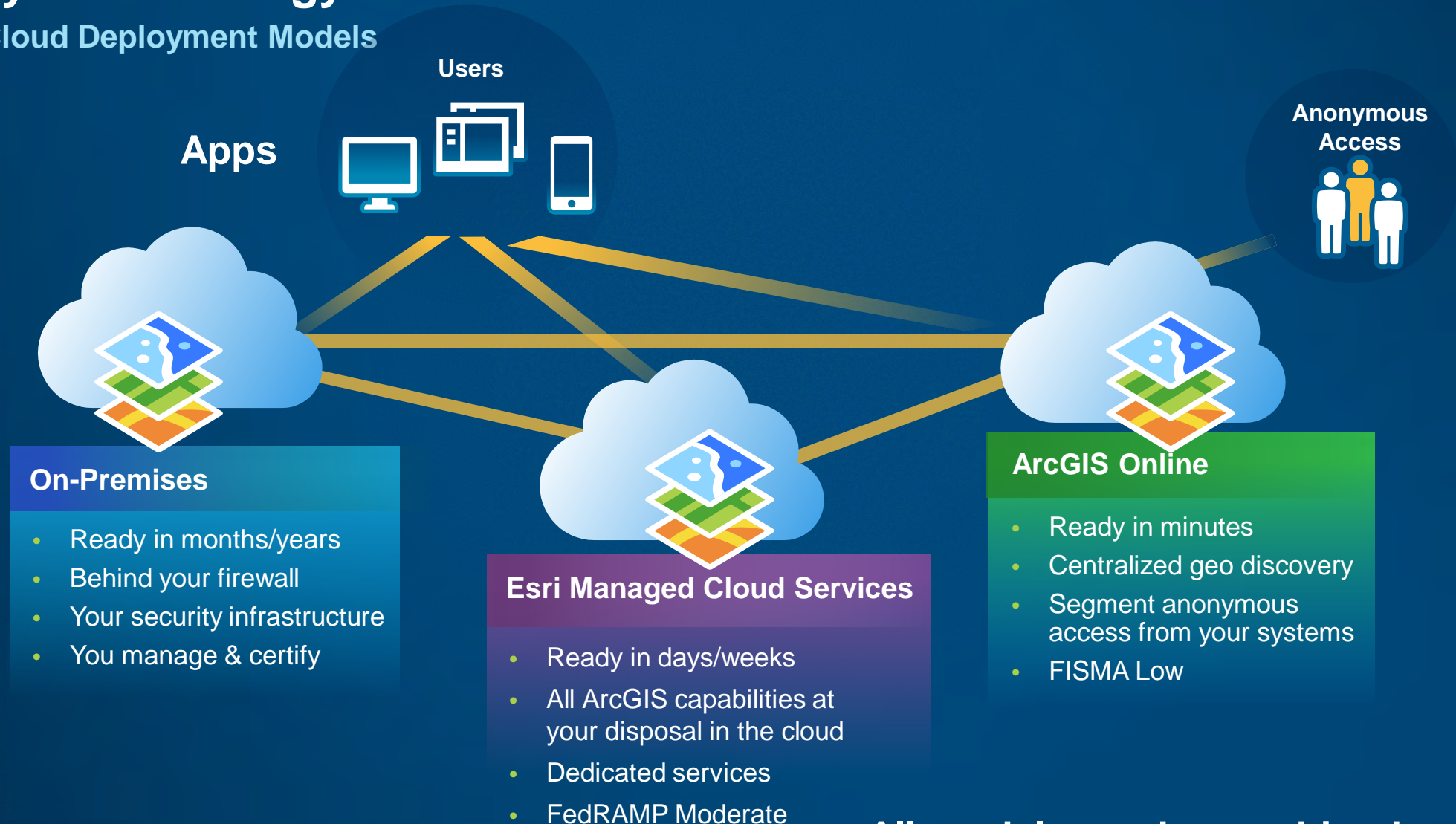
Deployment Strategy

Hybrid Deployments

- **Common for large enterprises**
- **Data Segmentation**
- **Meet more stringent security and compliance requirements such as CJIS by storing sensitive datasets on-premises**
- **ArcGIS Online or EMCS can operate as discovery portal in the cloud**

Deployment Strategy

Hybrid Cloud Deployment Models



On-Premises

- Ready in months/years
- Behind your firewall
- Your security infrastructure
- You manage & certify

Esri Managed Cloud Services

- Ready in days/weeks
- All ArcGIS capabilities at your disposal in the cloud
- Dedicated services
- FedRAMP Moderate

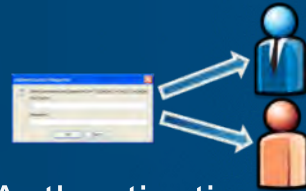
ArcGIS Online

- Ready in minutes
- Centralized geo discovery
- Segment anonymous access from your systems
- FISMA Low

... All models can be combined or separate

Deployment Strategy

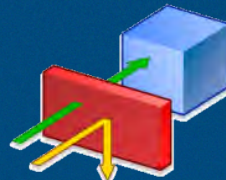
Key security areas to address



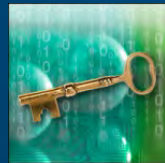
Authentication



Authorization



Filters



Encryption



Logging/Auditing

Deployment Strategy

Security Best Practices

- **Authentication – 2 Factor Authentication (2FA)**
 - ArcGIS Online: SAML 2.0 or built-in accounts
 - ArcGIS for Server: Web-tier Authentication
 - Portal for ArcGIS: Web-Authentication or SAML 2.0

- **Authorization – Principle of Least Privilege**
 - Role Based Access Control – Administrator, Publisher, and User
 - Custom Roles in Portal and ArcGIS Online
 - ArcGIS for Server – Service level authorization set by publisher/admin roles
 - ArcGIS Online and Portal – Item level authorization set by item owner
 - Can be extended by third party components
 - Database level: Row or Feature Class Level, SDE Views
 - Web Server level: URL filtering
 - Service level: Layer / Attribute level authorization

Deployment Strategy

Security Best Practices

- **Filters – Security Infrastructure**

- Web Application Firewall (WAF), Anti-virus, firewalls, reverse proxies, ...
- Intrusion Detection Systems (IDS)

- **Encryption**

- In-transit – supported across products
 - Use strong protocols (TLS) and ciphers
 - IPSec with corporate VPN
- At-rest
 - Database level: Transparent Data Encryption (TDE)
 - File based: Operation System Level (such as Bitlocker), Disk-level

- **Logging and Auditing**

- Logging should be done and reviewed across application, OS, database, firewall, and other layers
- Consolidate with a SIEM



3

STIG Highlights



STIG Implementation Approach

ArcGIS Server STIG

- + Windows 2012 R2 Member Server STIG
- + IIS 7.0 STIG *Concepts* (Applied to 8.x)
- + ArcGIS Server 10.3x STIG

Inherited Controls

ArcGIS Server STIG

- **Windows Server 2012 / 2012 R2 Member Server STIG**
 - Enforce DoD Approved Encryption Algorithms (FIPS 140-2)
 - Implement Organization Approved Certificates (PKI)
 - Integrate with Central Authentication (Active Directory/LDAP)
 - Multifactor Authentication (Smartcards)
- **IIS 7.0 STIG *Concepts* (Applied to IIS 8.5)**
 - Web Tier Authentication (HTTP/PKI)

AC (Access Control)

ArcGIS Server STIG

- Enforce DoD Approved Encryption Algorithms (FIPS 140-2)
- Implement Organization Approved Certificates (PKI)
- Integrate with Central Authentication (Active Directory/LDAP)

The image shows a screenshot of the ArcGIS Server Manager interface. On the left, the 'Connections' pane shows a tree view with 'AGS1' expanded to 'Sites' > 'Default Web Site' > 'arcgis'. The main window displays the 'Authentication' configuration page. A table lists various authentication methods, with 'Active Directory Client Certificate ...' selected and highlighted. Below this, the 'ArcGIS Server Manager' interface shows the 'Security' tab selected. The 'Configuration Settings' section is visible, with 'User Store' and 'Role Store' both set to 'Windows Domain', which is circled in red. Other settings include 'Authentication Tier' and 'Authentication Mode', both set to 'Web'.

Name	Status	Response Type
Active Directory Client Certificate ...	Enabled	HTTP 401 Challenge
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	
Forms Authentication	Disabled	
Windows Authentication	Disabled	

ArcGIS Server Manager Services Site Security

Settings Users Roles

ArcGIS Server Security

ArcGIS Server security determines who can administer the GIS server, who can publish to the GIS server, and who can use the service...

General ArcGIS Server security settings are displayed below. To change the accounts recognized by ArcGIS Server and set their permissions, use the Users and Roles links above. To set access rules for a service, use the Services > Manage Services page.

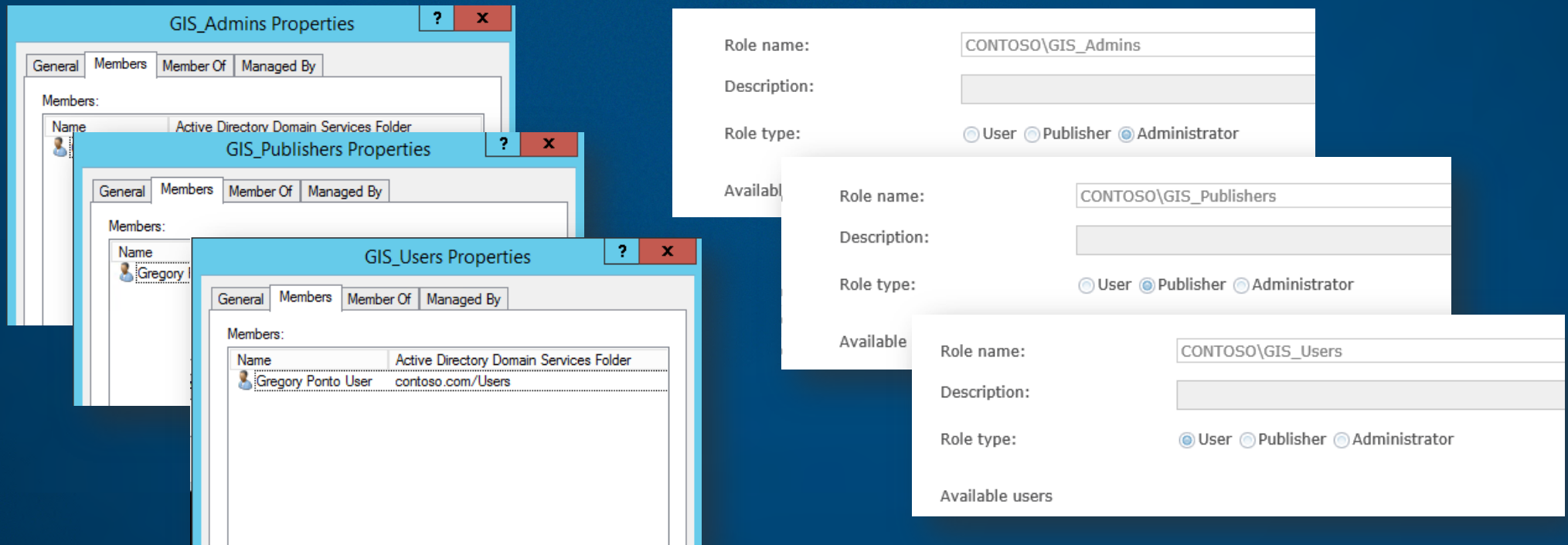
Configuration Settings

User Store:	Windows Domain
Role Store:	Windows Domain
Authentication Tier:	Web
Authentication Mode:	Web

AC (Access Control)

ArcGIS Server STIG

- Enforce DoD Approved Encryption Algorithms (FIPS 140-2)
- Implement Organization Approved Certificates (PKI)
- Integrate with Central Authentication (Active Directory/LDAP)



AU (Audit & Accountability)

ArcGIS Server STIG

- Configure VERBOSE Logging with ArcGIS Server

The screenshot shows the ArcGIS Server Log Settings dialog box and the Log Filter interface. The Log Settings dialog box is open, showing the Log level dropdown menu with 'Verbose' selected. The Log Filter interface shows the Log Filter dropdown set to 'Verbose', Age set to 'Last 24 Hours', Source set to 'All', and Machine set to 'All Machines'. The Log Filter interface also displays a table of log messages.

Log Settings

Specify the level of detail, age and location for creating log messages.

Log level: **Verbose**

Keep logs for at least: days

Log file path:

This location must be a local path and exist in the site.

Log Filter: **Verbose** Age: Last 24 Hours Source: All Machine: All Machines Query

Level	Time	Message	Source
FINE	Feb 8, 2016, 9:12:10 PM	useExisting=1	Server
INFO	Feb 8, 2016, 9:12:10 PM	Request user: Anonymous user. Service: hosted/California1/Featureserver	Rest
FINE	Feb 8, 2016, 9:12:10 PM	HTTP Referer: http://www.arcgis.com/home/webmap/viewer.html? useExisting=1	Server
FINE	Feb 8, 2016, 9:12:10 PM	HTTP Referer: http://www.arcgis.com/home/webmap/viewer.html? useExisting=1	Server
INFO	Feb 8, 2016, 9:12:10 PM	Request user: Anonymous user. Service: hosted/California1/Featureserver	Rest
INFO	Feb 8, 2016, 9:12:10 PM	Request user: Anonymous user. Service: hosted/California1/Featureserver	Rest
FINE	Feb 8, 2016, 9:12:10 PM	HTTP Referer: http://www.arcgis.com/home/webmap/viewer.html? useExisting=1	Server

CM (Configuration Management)

ArcGIS Server STIG

- Disable HTTP Listener
- Disable REST Services Directory

ArcGIS Server Administrator Directory

[Home](#) > [security](#) > [config](#) > [update](#)

Update Security Configuration

Warning
Changing Protocol will cause the web server to be restarted.

Security Configuration

Protocol: HTTPS Only

Virtual directories security enabled:

Authentication tier: WEB_ADAPTOR

https://ags1.contoso.com/arcgis/rest/services

ArcGIS REST Framework

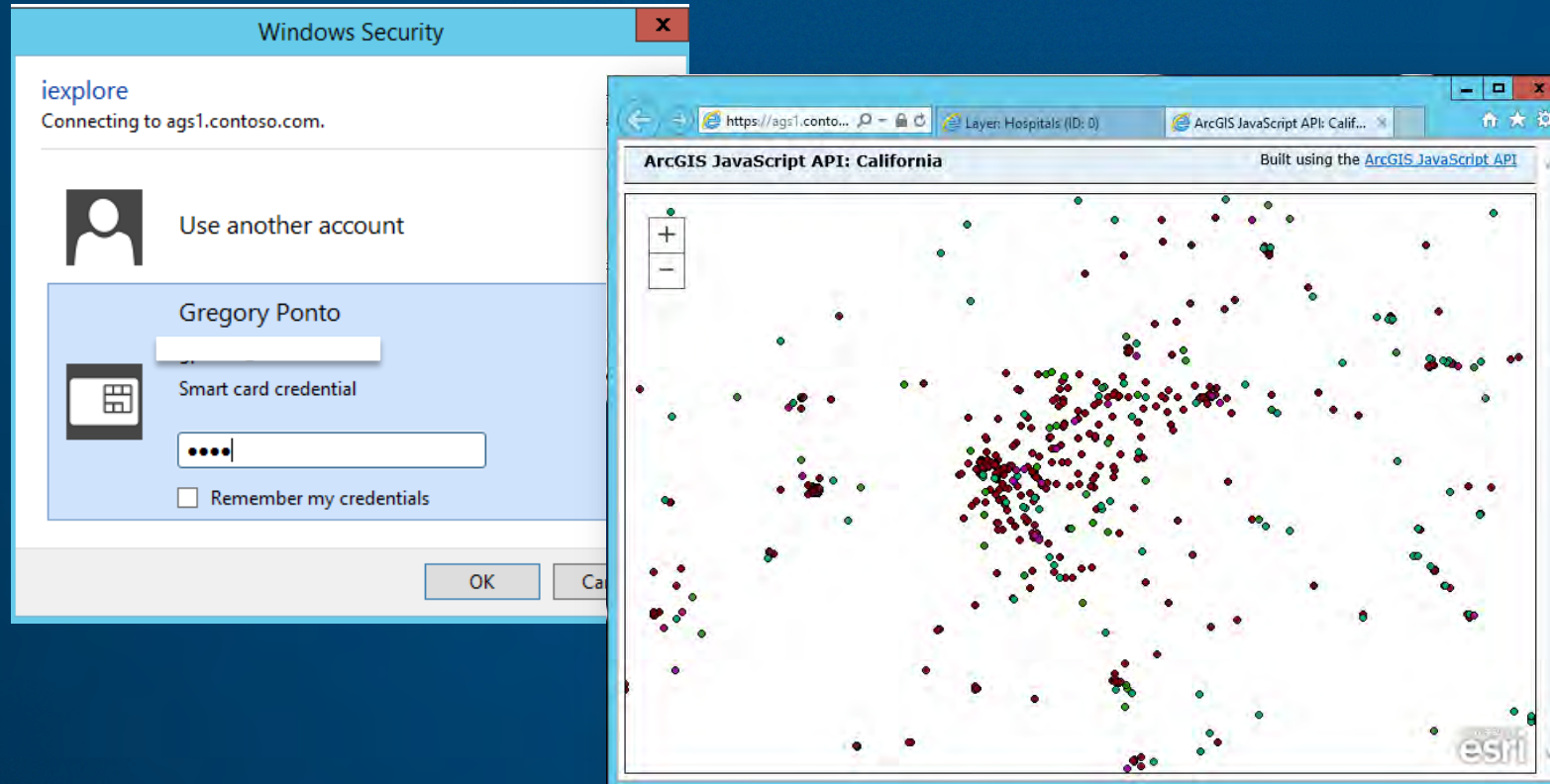
[Home](#)

Error: Services Directory has been disabled.
Code: 403

IA (Information Assurance)

ArcGIS Server STIG

- Require Certificate Authentication (MFA/Smartcards)
- Utilize Centralized Authorization (Active Directory Groups)



IA (Information Assurance)

ArcGIS Server STIG

- Require Certificate Authentication (MFA/Smartcards)
- Utilize Centralized Authorization (Active Directory Groups)
- Require Encrypted Web Access
- Disable Anonymous Web Access

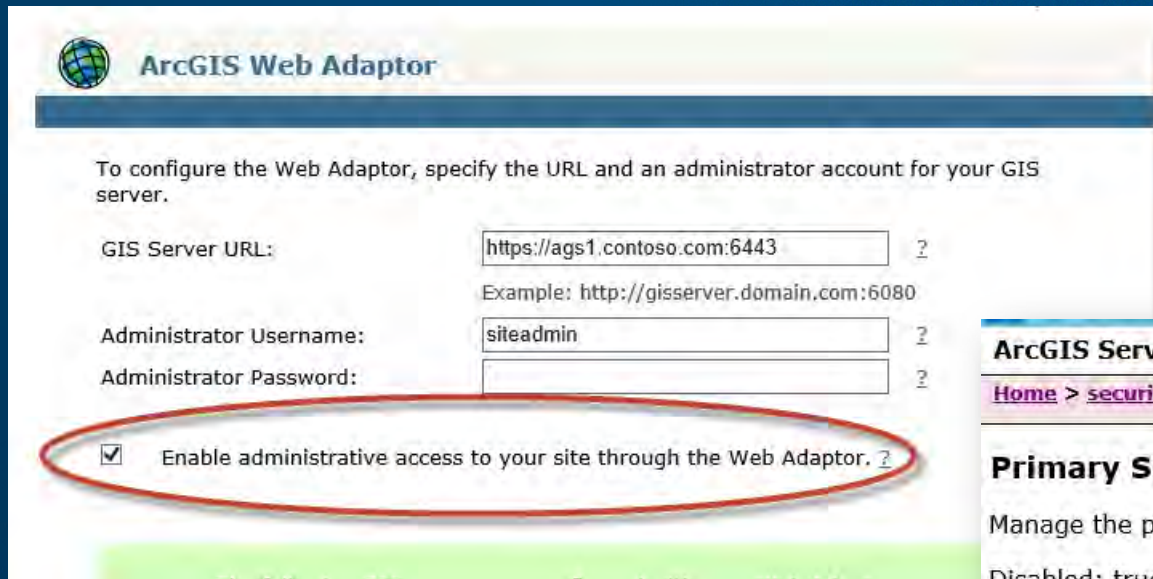
The image displays two screenshots from the ArcGIS Server Administration Console. The left screenshot shows the 'SSL Settings' page for the 'arcgis' site. The 'Require SSL' checkbox is checked and circled in red. The 'Client certificates' section has 'Require' selected. The right screenshot shows the 'Authentication' page for the 'arcgis' site. The 'Anonymous Authentication' row is circled in red, indicating it is disabled.

Name	Status	Response Type
Active Directory Client Certificate	Enabled	HTTP 401 Challenge
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

SC (System & Communication Protection)

ArcGIS Server STIG

- Disable “Primary Site Administrator”



ArcGIS Web Adaptor

To configure the Web Adaptor, specify the URL and an administrator account for your GIS server.

GIS Server URL: ?
Example: http://gisserver.domain.com:6080

Administrator Username: ?

Administrator Password: ?

Enable administrative access to your site through the Web Adaptor. ?



ArcGIS Server Administrator Directory Logged in: CONTOSO\gponto [Administrator]

[Home](#) > [security](#) > [psa](#) API F

Primary Site Administrator Account

Manage the primary site administrator account.

Disabled: true

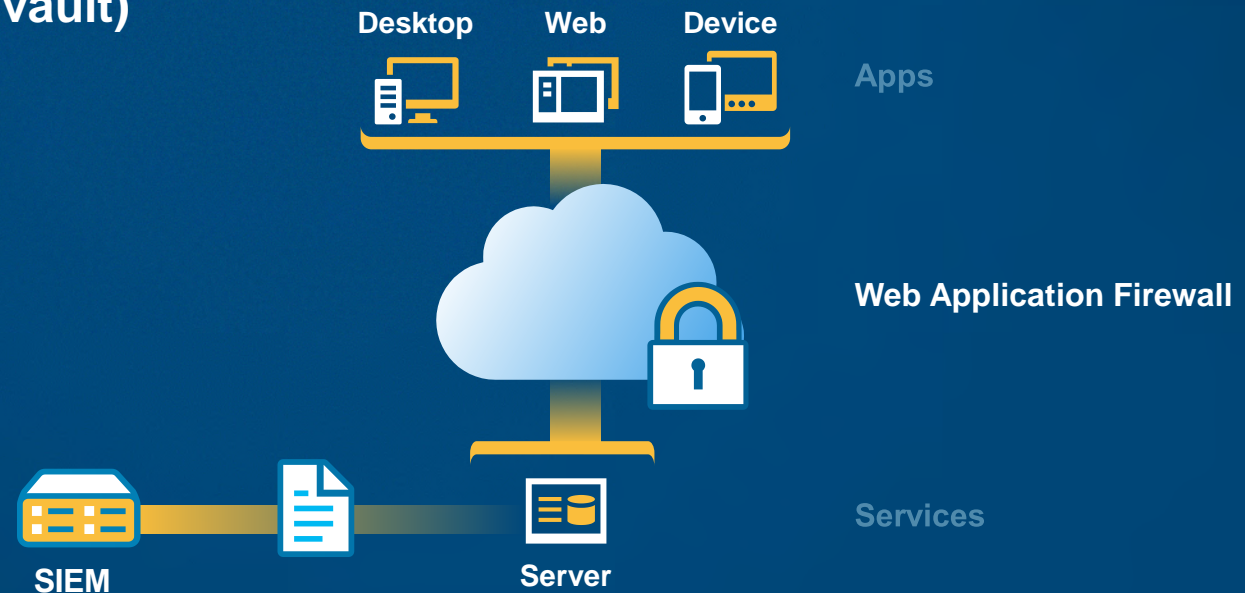
Supported Operations: [update](#) [enable](#) [disable](#)

Supported Interfaces: [REST](#)

Mitigating Controls

ArcGIS Server STIG

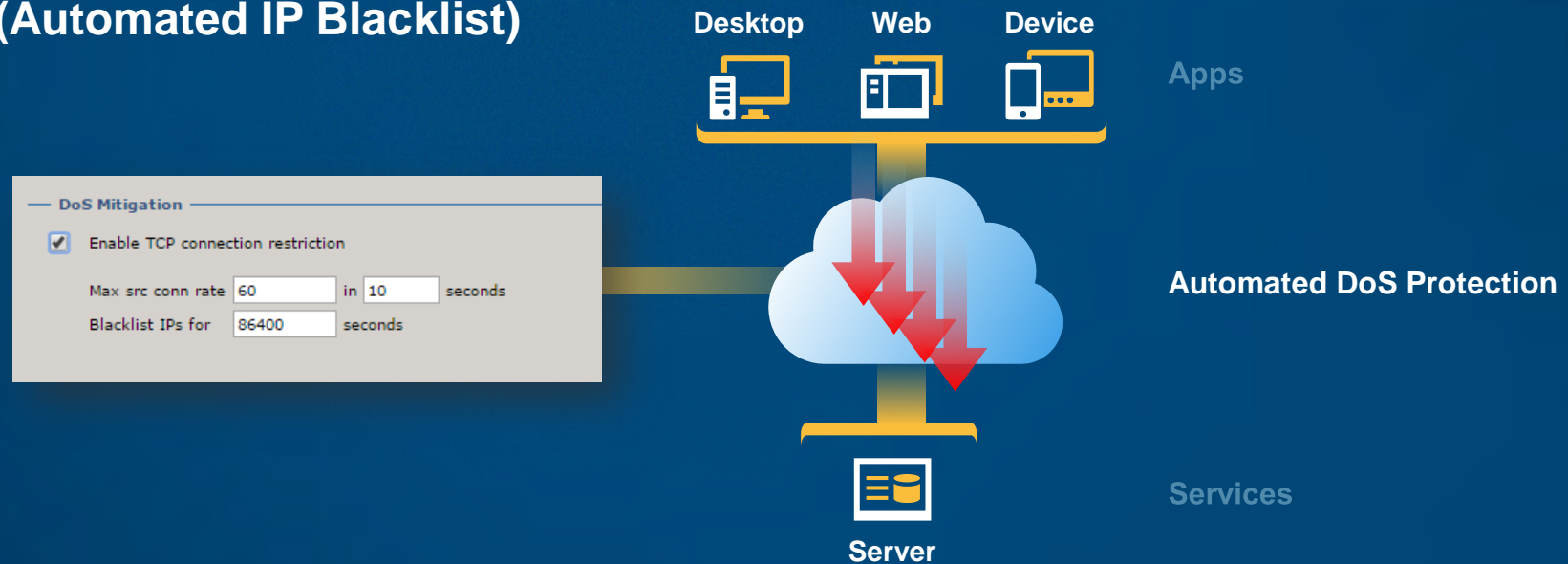
- **Access Control (AC): Endpoint Protection**
 - Web Application Firewalls (eg. Barracuda, Sonicwall)
- **Audit & Accountability (AU): Log Aggregation & Correlation**
 - 3rd Party SIEM (eg. Splunk, Alienvault)



Mitigating Controls

ArcGIS Server STIG

- **System & Communication Protection (SC): Mobile Code Execution**
 - Client Browser Management (“Trusted Sites”)
- **System & Communication Protection (SC): DoS Protection**
 - DoS Protection (Automated IP Blacklist)



Mitigating Controls

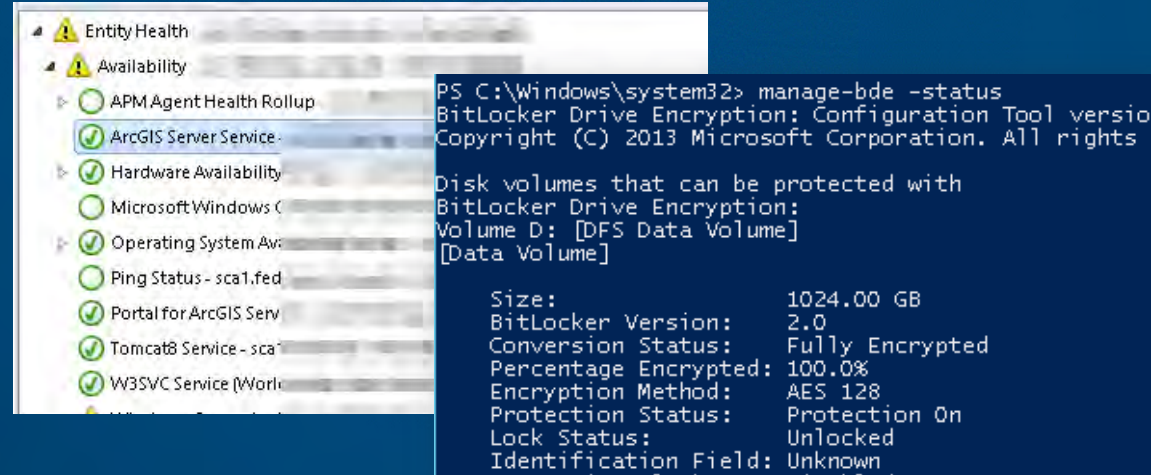
DoS/DDoS

Containment Strategy	Volumetric (Effectiveness)	Protocol (Effectiveness)	Application (Effectiveness)
Network firewalls, subnets, segmentation	High	High	Low
Scaling	Moderate	Moderate	Moderate
Report to your ISP	Varies	Varies	Low
Throttling	Moderate	Moderate	Low
Secure endpoints	Low	Low	High
Filtering (WAF)	Low	Low	Moderate-High

Mitigating Controls

ArcGIS Server STIG

- **System & Communication Protection (SC): Data Protection at Rest**
 - Whole Disk Encryption on Data Drives (Bitlocker, checkpoint, ...)
- **SI (System & Information Integrity): Automated Response to Anomalies**
 - System Center Operations Manager (SCOM, Solarwinds, ...)



Microsoft Bit Locker: <https://technet.microsoft.com/en-us/library/ff829849.aspx>

System Center Operations Manager: <https://technet.microsoft.com/en-us/library/hh509025.aspx>

Summary

ArcGIS Server STIG

- **Inherited Controls**
 - Windows 2012 / 2012 R2 STIG
 - IIS 7.x STIG Concepts
- **Configurable Controls (ArcGIS Server)**
 - Integrated Security (Active Directory & PKI)
 - Disable HTTP
 - Disable Services Directory
 - Enable Verbose Logging
 - Disable Primary Site Administrator
- **Mitigating Controls**
 - Whole Disk Encryption
 - Mobile Code Execution Management
 - Automated DoS Protection
 - Log Management (SIEM)
 - Automated Monitoring (SCOM)

Real World Deployments

Lessons Learned

- **Distributed File Services**
 - High Availability File Services
 - ArcGIS Server Config Store
 - ArcGIS Server Directories
 - File Data
- **Group Managed Service Accounts**
 - ArcGIS Server Service Account
 - Automated Password Management
- **Encryption at Rest (Easy Win)**
 - Whole Disk Encryption
 - Transparent Data Encryption
- **Web Application Firewalls**
 - High Effort / Maintenance
 - Automated Learning / Scoping



4

Esri Managed Cloud Services Advanced Plus

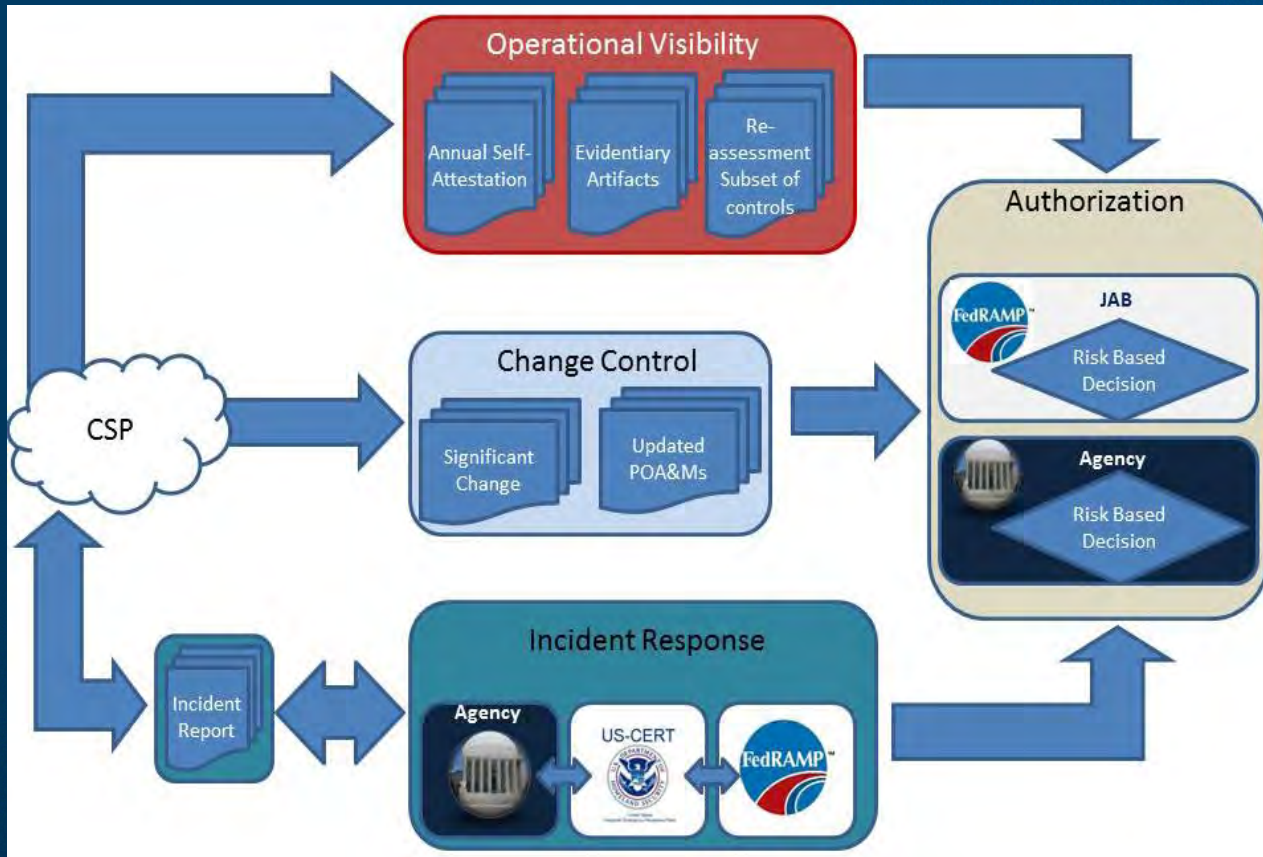
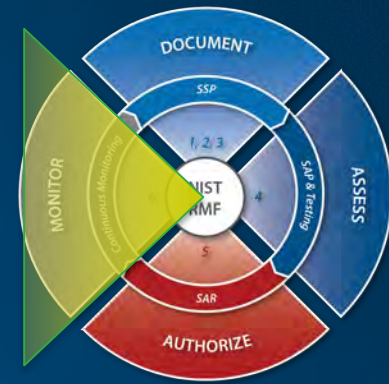


Esri Managed Cloud Services Advanced Plus

What is Esri Managed Cloud Services?

- **Cloud-based GIS infrastructure support, including:**
 - Enterprise system design
 - Infrastructure management
 - Software (Esri & 3rd Party) installation, updates, and patching
 - Application deployment
 - Database management
 - 24/7 support and monitoring
- **Advanced plus offering**
 - FedRAMP Moderate ATO by US Census Bureau
 - Security infrastructure & 24x7 SOC
 - Security controls and processes that align with FedRAMP moderate level
 - Initial offering based in AWS, looking at expanding into Azure based on demand

Esri Managed Cloud Services Advanced Plus Continuous Monitoring



FedRAMP Reporting Workflow

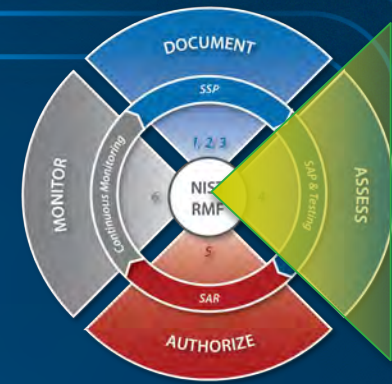


Monitoring Workflow

Ensures maintenance of acceptable risk posture

Esri Managed Cloud Services Advanced Plus

Rigorous Third Party Security Assessment



- **Must occur annually**
- **Third Party Assessment Organization (3PAO) accredited by FedRAMP**
- **Documentation**
 - A security review of all FedRAMP controls and implementation details
- **Technical Assessment**
 - System level scans
 - Web Interface scans
 - Database scans
 - Penetration testing

Great advisors and skilled assessors keep the effort focused

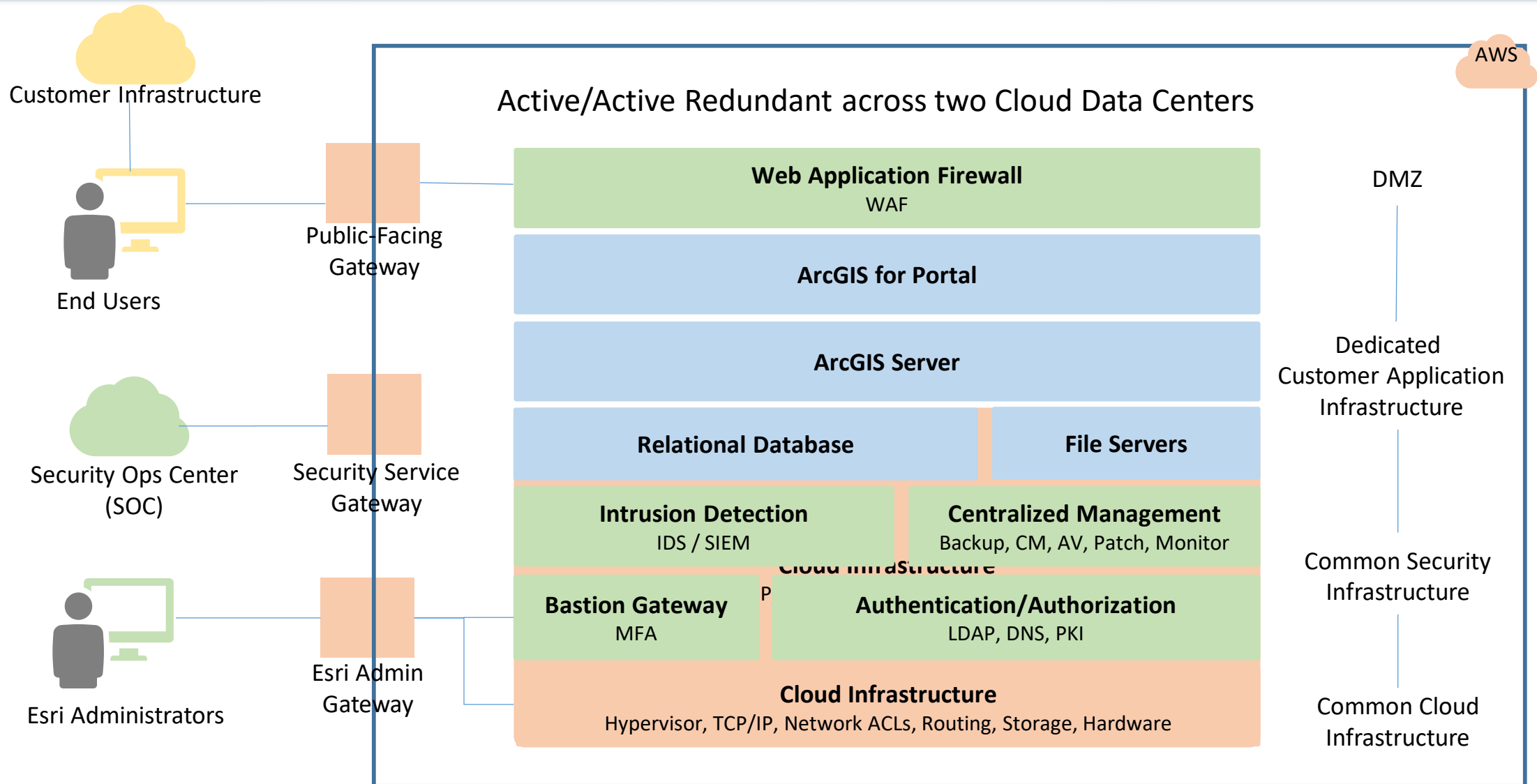
Esri Managed Cloud Services Advanced Plus

Design goals

- **Most government systems**
 - Require moderate security baseline controls
- **Most geospatial information sets**
 - Only require low baseline controls
 - ArcGIS Online FedRAMP Tailored Low is adequate for many customer use cases
- **EMCS FedRAMP Infrastructure Design Goals**
 - Consumable by the widest range of customers
 - Amazon East-West Regions – Not limited to GovCloud
 - Drive down customer expenses for secure, compliant geospatial services
 - Customer's can choose level of multi-tenancy vs dedicated services they are comfortable with
 - Meet and exceed current rigorous FedRAMP requirements for cloud services
 - First geospatial platform to be compliant with FedRAMP Rev 4 requirements

A balance of robust security and business requirements drove infrastructure choices

EMCS Security Infrastructure



Legend

Agency

Application

Cloud Provider

Security



5

Summary



Summary

Resources Available for Agency Review

- **Cloud infrastructure provider**
 - SSAE16 and ISO 27001
 - Report available from cloud providers under NDA
- **FedRAMP Repository**
 - ArcGIS Online Compliance Package (See FedRAMP.gov Marketplace)
 - Cloud Service Provider FedRAMP Moderate Packages
- **Esri**
 - Reports available from Esri under NDA
 - Cloud Security Alliance (CSA) Answers Publically Available
 - ArcGIS Online answers have been updated to newest version

Summary

Solution/Services Accreditation Roadmap

- **ArcGIS Online FedRAMP Tailored Low Authorization**
 - Agency authorization 2018

- **Esri Managed Cloud Services (EMCS) FedRAMP Moderate Authorization**
 - Agency Authorization 2015
 - Establishes validated secure clouds deployment patterns

- **Documentation and assessment materials enable FISMA or FedRAMP authorization**

Summary

- **Esri is working with security leaders to create standardized security hardened deployment guidance for our customers**
- **ArcGIS Online is FedRAMP Tailored Low authorized and we can work with you to support your Agency's authorization**
- **Esri Managed Cloud Services FedRAMP moderate compliant option ready for your agency to review and authorize**
- **Information readily available on [Trust.ArcGIS.com](https://trust.arcgis.com)**

We welcome your feedback concerning any authorization needs or gaps not addressed in this presentation

Summary

We are here for you

- **Esri's Software Security & Privacy Team**

- Led by Esri's Chief Product Security Officer consisting of Security Engineers and Architects
- Leads Security Certification efforts across the ArcGIS Platform
- Created and maintain Trust.ArcGIS.com as a one-stop shop for security and privacy
- Performs security validation / testing of products and deployments
- Utilizes all of the above as inputs for providing customer guidance such as this presentation

- **Contact our team at:**

SoftwareSecurity@Esri.com

The screenshot shows the ArcGIS Trust Center website. The navigation bar includes 'ArcGIS Trust Center', 'Overview', 'Security', 'Privacy', 'Compliance', 'Documents', and a 'Launch Security Advisor' button. A search bar is located below the navigation. The main content area features the heading 'ArcGIS—The secure and trustworthy location platform' and the subtext 'Trust.ArcGIS.com is your go to resource for security, privacy, and compliance information'. Below this are logos for FedRAMP, FISMA Authorization & Accreditation, Privacy Shield Framework, and TRUSTe Certified Privacy. A red button labeled 'Report a Security Concern' is visible. The 'Alerts and Announcements' section includes a 'View all alerts' link and a 'Subscribe to the Trust Esri RSS Feed' link. Three alert cards are shown: one dated July 5, 2019 about 'Prepare for Next Major ArcGIS Online Security Advancement Now', one dated July 2, 2019 about 'ArcGIS Workflow Manager Server Security Update Patch is available', and one dated May 24, 2019 about '2019 Update 1 ArcGIS Enterprise Security Patches Released'.

Questions?

Contact SoftwareSecurity@esri.com for Assistance/Guidance



esri

THE
SCIENCE
OF
WHERE

