Designing a Web GIS Security Strategy

Michael Young – CISO - Products

Randall Williams – Security Engineer - PSIRT Lead

Esri Software Security & Privacy Team

Agenda

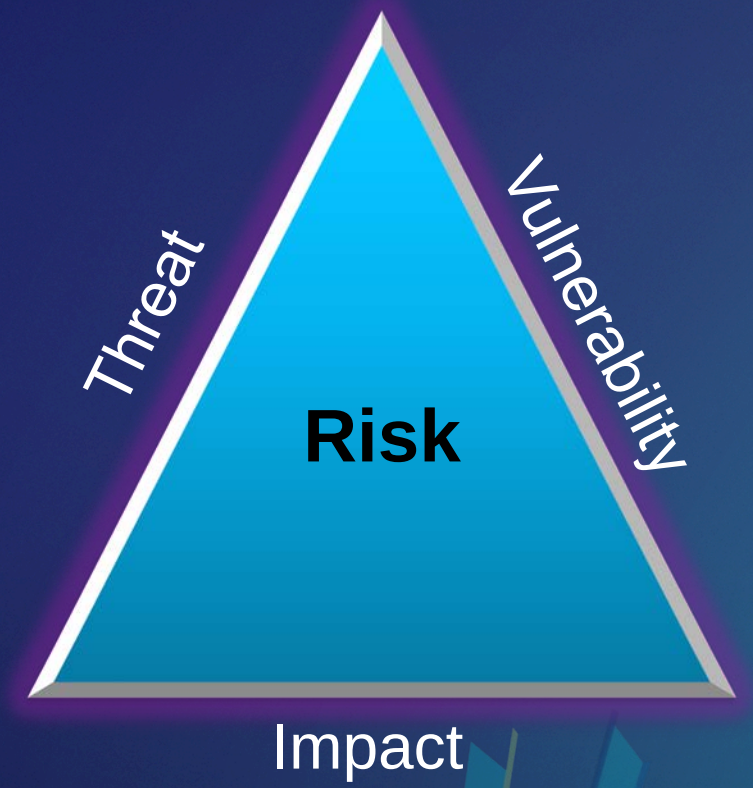
- Introduction
- Trends
- Strategy
- Mechanisms
- Web GIS
- Mobile
- Cloud
- Compliance

Introduction

What is a secure GIS?

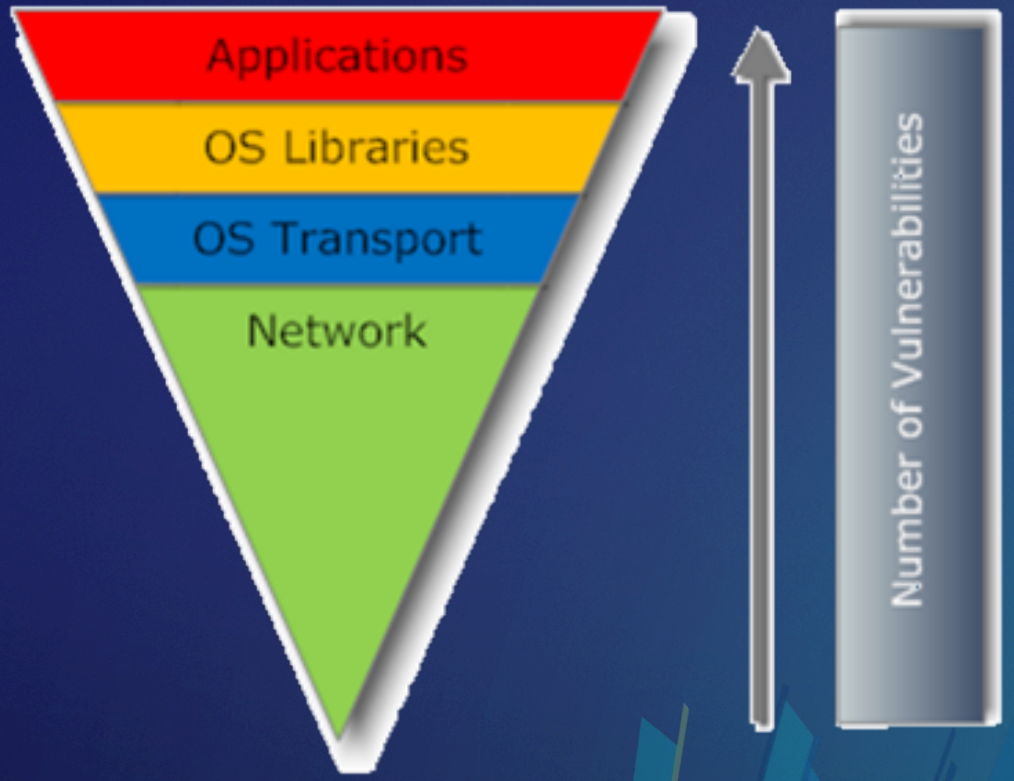
Introduction

What is “The” Answer?



Introduction

Where are the vulnerabilities?



*SANS Relative Vulnerabilities

Core component vulnerabilities were exposed in the past few years, application risks are still king

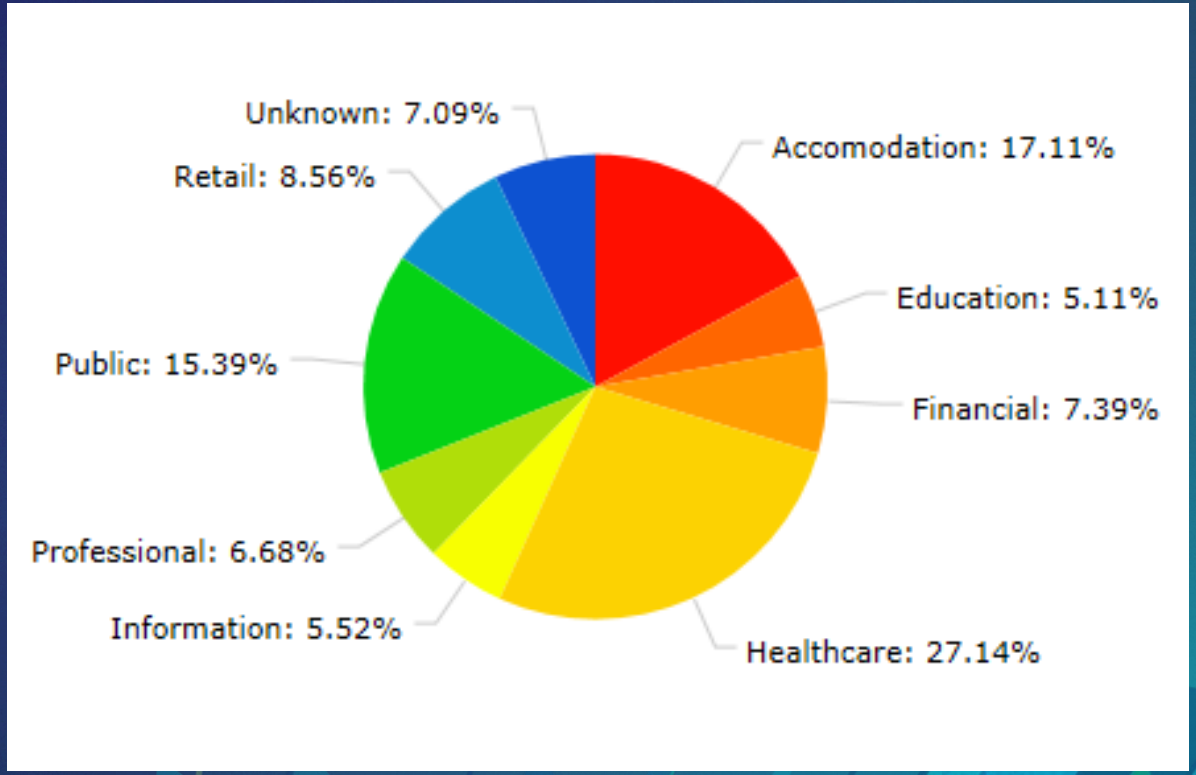
Trends & Real World Scenarios

Michael Young

Trends

Breaches: Is your industry a top target?

- **Top five breached industries**
  1. **Healthcare**
  2. **Accommodation**
  3. **Public**
  4. **Retail**
  5. **Finance**



*Verizon 2018 DBIR

Trends

Cloud adoption continues to expand

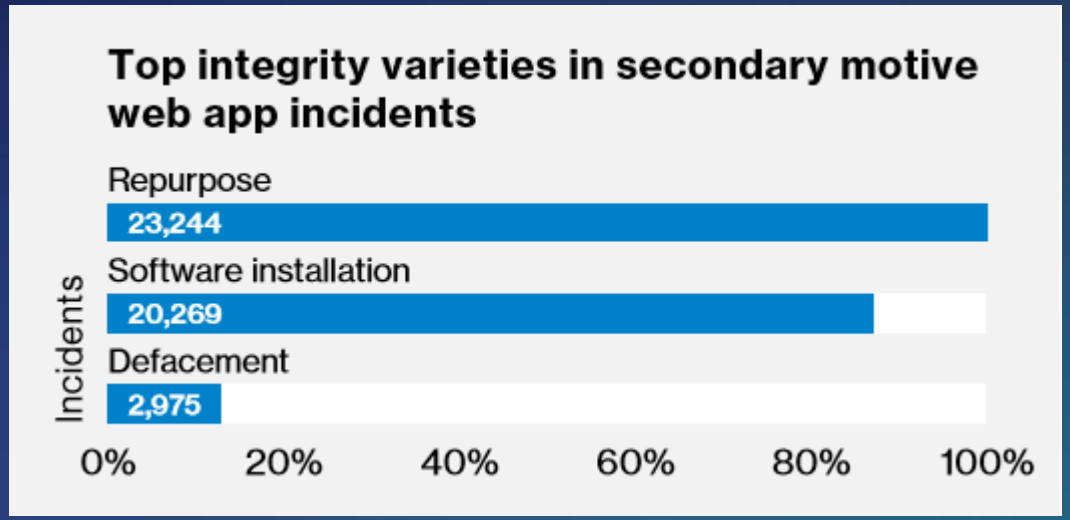
- **Frequently, cloud providers can and do provide robust security**
- **Largest downfall of cloud security continues to be customer configuration of the services**
  - **Gartner predicts by 2020, 95% of cloud security incidents will be the customer's fault**
  - **Demonstrated by repeated exposures of Amazon S3 cloud repositories**
  - **Repeated exposure of publicly editable mapping services**
- **Importance of administration maintenance & security processes can't be emphasized enough**
  - **Do your admin receive adequate training on the services?**
  - **Do you know about tools available to ensure alignment with best practices?**

How well are you controlling the publication process to external facing services?

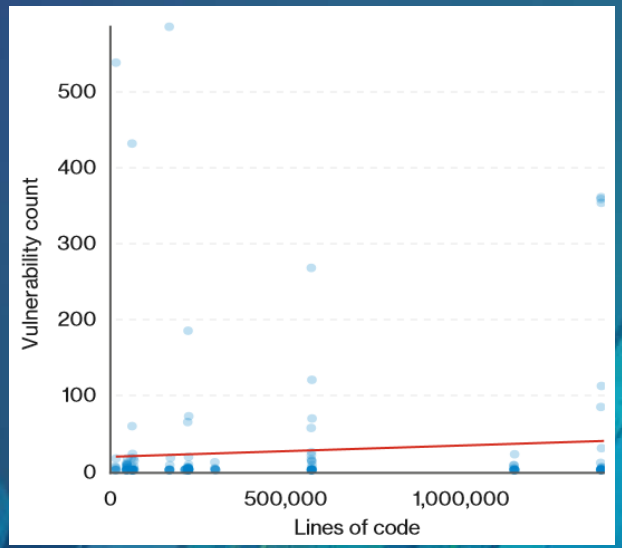
Trends

Importance of Web Application Security Remains High

- Even if not sensitive data on a web server, it is still a desirable target for criminals



- Small web apps typically have the same number of instances of a given type of vulnerability as large ones



*Verizon 2018 DBIR

Scenarios

Imagine Being Notified About a Hacktivist Group Threating To Attack Your Organization

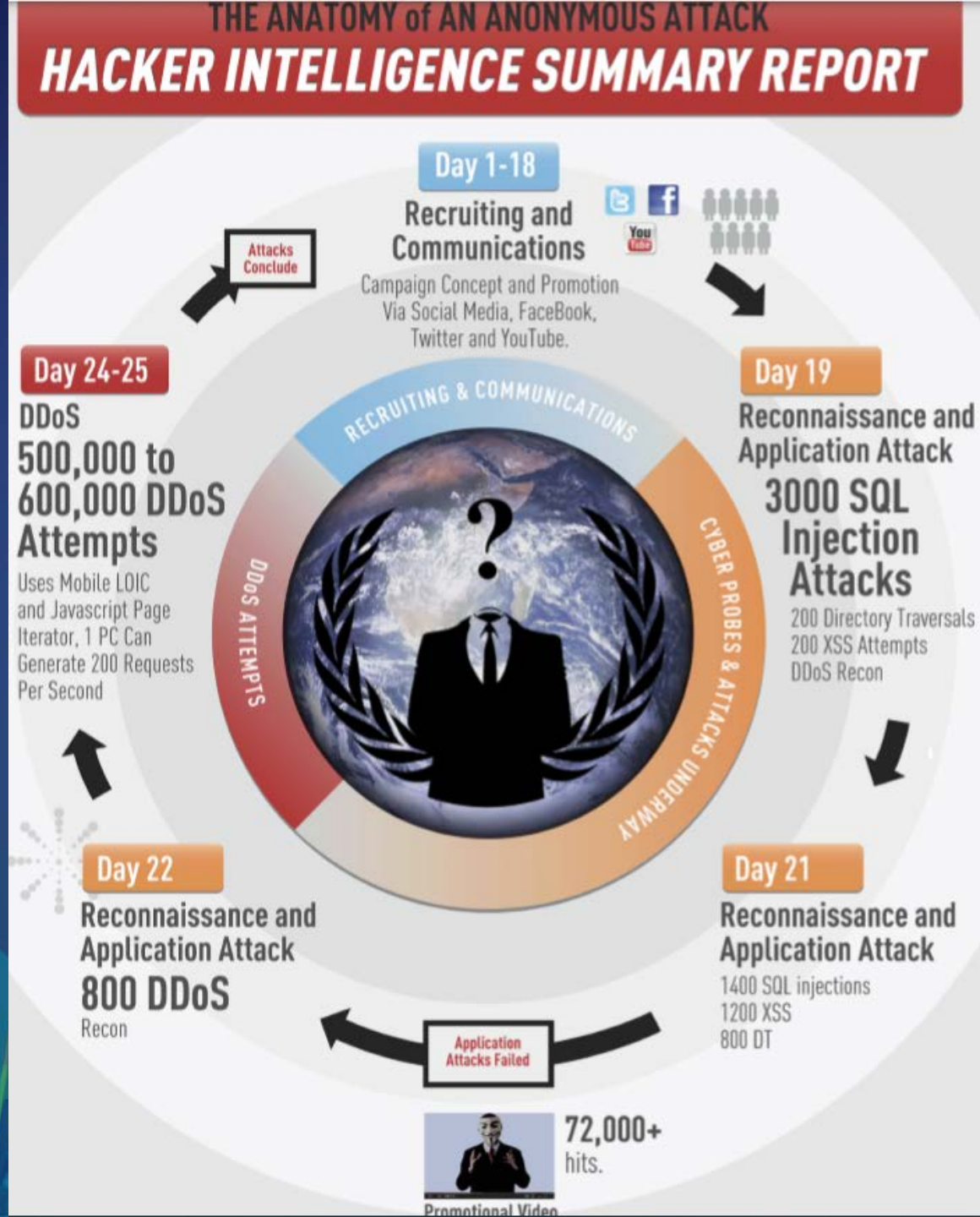
- Your organization has received an email from the FBI explaining that a well known hacktivist group has threatened to attack your organizations IT systems in the next several weeks
- Press has obtained your organization's internal announcement and shared with public
- You don't think your Internet-facing geospatial repositories contain information that could be damaging to your organization or others if released, but you are not positive
- You use multiple ArcGIS Online organizations as well as ArcGIS Enterprise on-premises
- What would you do as the Geospatial IT Manager?
  - Nothing – Assume everything is good enough?
  - Shutdown the GIS systems and disable your AGO Orgs?
  - Something else?

Scenarios

Dealing with a hacktivism threat

1. Get expert help as possible
    1. Work with your incident response team
    2. Contact vendor response teams

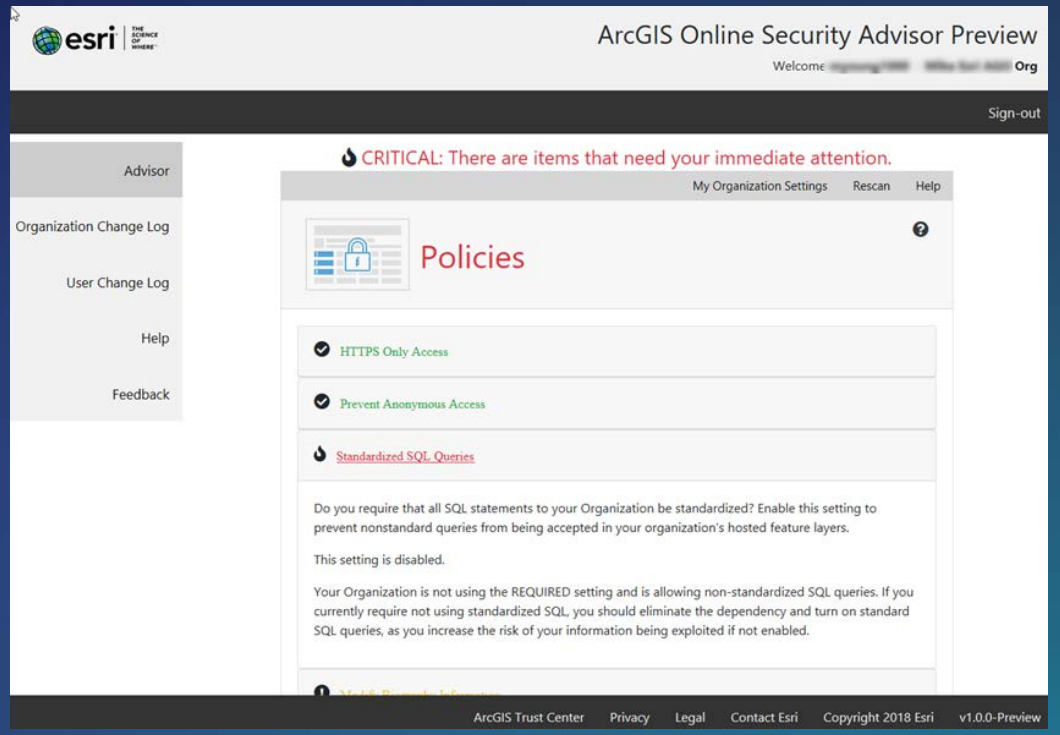
2. Understand your attackers mode of operation as well as what they would be most likely be interested in exploiting within your organization
    1. Recruitment
    2. Data exfiltration attempts
    3. DDoS attempts



Scenarios

Dealing with a hacktivism threat

- Ensure application layer is security hardened
- Apply patches for OS and GIS
  - Check Trust Center for latest security patches
- There are tools that check for GIS security best practices
  - Python admin scripts included with both Portal & Server
- What about ArcGIS Online?
  - Yes – NEW AGO Security Advisor
  - More on this to come



How likely is this to happen? Ask the customer it's happening to right now…

Scenarios

Imagine it's December 2018

- **You are the GIS administrator and you have a queue of emails awaiting for you**
- **Some emails complain about users with the desktop version of Operations Dashboard failing to run**
- **Other user say they are having problems connecting their desktops to ArcGIS Online**

What security change could result in this scenario?

Scenarios

Imagine it's December 2018 – TLS 1.0 & 1.1 were disabled for ArcGIS Online

- **ArcGIS Online transport security roadmap established**
- ***Will disrupt a number of customer's operations*** **if not tested/validated ahead of transition**
- **TLS 1.0 & 1.1 will be disabled (In alignment with PCI & FedRAMP standards)**
  - **Check out our TLS guide to understand compatibility with product versions (Trust Center)**

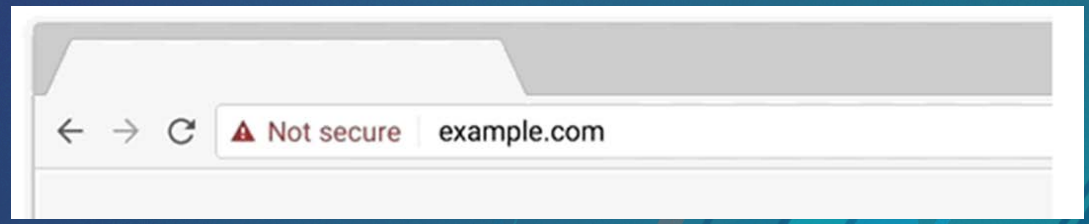
Don't be surprised by SaaS configuration changes – Stay in the loop of proposed changes and test accordingly!

Scenarios

Imagine it's September 2019

- As the primary ArcGIS Online administrator, you are swamped with calls from your users wondering why their maps are failing to display – causing widespread disruption of your geospatial services

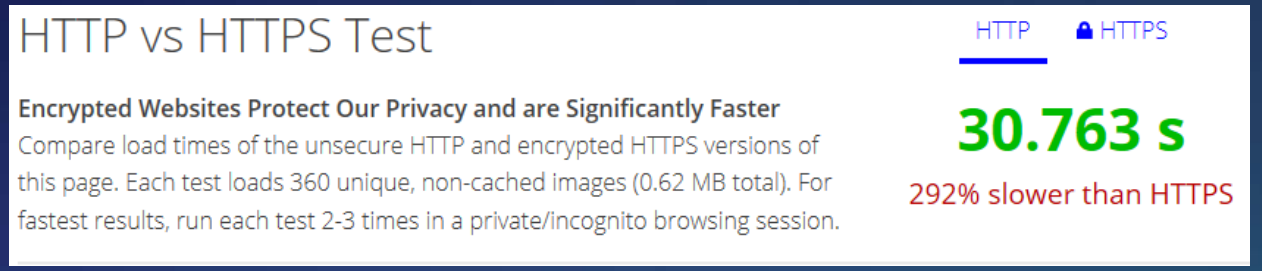
- Users have been complaining about Insecure messages from their browsers when visiting your site for months



Something changed, but what?

Scenarios

ArcGIS Online Allows Only HTTPS



- In September 2019, ArcGIS Online will only allow organizations to use HTTPS
- In October 2018, browsers like Chrome will flag sites with HTTP as insecure
  - Nobody will want to consume your maps/apps if you don't start correcting this immediately
- Ensure your systems can used HTTPS
- Performance and cost are non-issues in 2018
  - Free certificates are available if necessary
    - Let's Encrypt provides free HTTPS certificates
    - Amazon is offering free security certificates to AWS customers
  - Most browsers only support faster HTTP/2 with HTTPS
    - This means sites utilizing HTTPS can significantly outperform HTTP sites
    - See for yourself @ http://www.httpvshttps.com/
- Ensure the external services your organization and maps/apps use HTTPS

The sooner you eliminate HTTP from your systems and the services you consume the better

Scenarios

Disaster communications modified

- **Scenario**
  - Organization utilizes cloud based services for disseminating disaster communications
  - Required easy updates from home and at work
  - Drove allowing the public access to modify service information

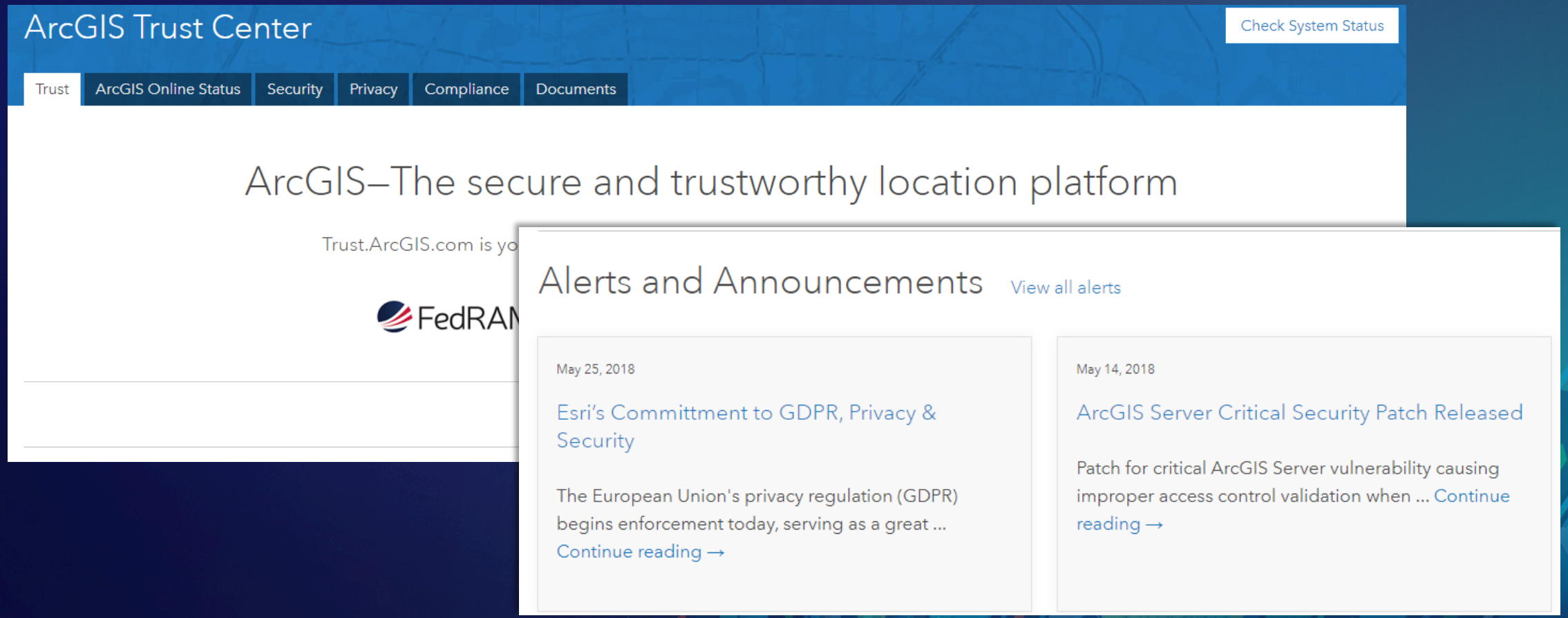
- **Lesson learned**
  - Enforce strong governance processes for web publication
  - Don’t allow anonymous users to modify web service content
  - Minimize or eliminate “temporary” modification rights of anonymous users
  - If web services are exposed to the internet, just providing security at the application level does not prevent direct access to web services

Lack of strong governance leads to unexpected consequences

Scenarios

QUIZ – When was the last ArcGIS Security patch released?

- **Hint – The Trust.ArcGIS.com site will always have this answer handy…**



99.9% of vulnerabilities are exploited more than a year after being released

Trends

Strategic Shifts in Security Priorities for 2018 and Beyond

- HTTP is about to die
  - Migrate away from any HTTP dependences
- Stronger Privacy regulation driving security demands (GDPR / New State of CA law)
- Enormous user password dumps now commonplace
  - Use 2-factor auth / enterprise password management solutions
- Mobile security threats increasing quickly
  - Become familiar with vendor mobile app recommendations
- Utilization of named users provides more granular tracking of geospatial information
  - Become familiar with your application logging capabilities
- Customer configuration primary source of cloud breaches
  - Drives importance of admin training & tools/automation for discovery of configuration issues

Strategy

Michael Young

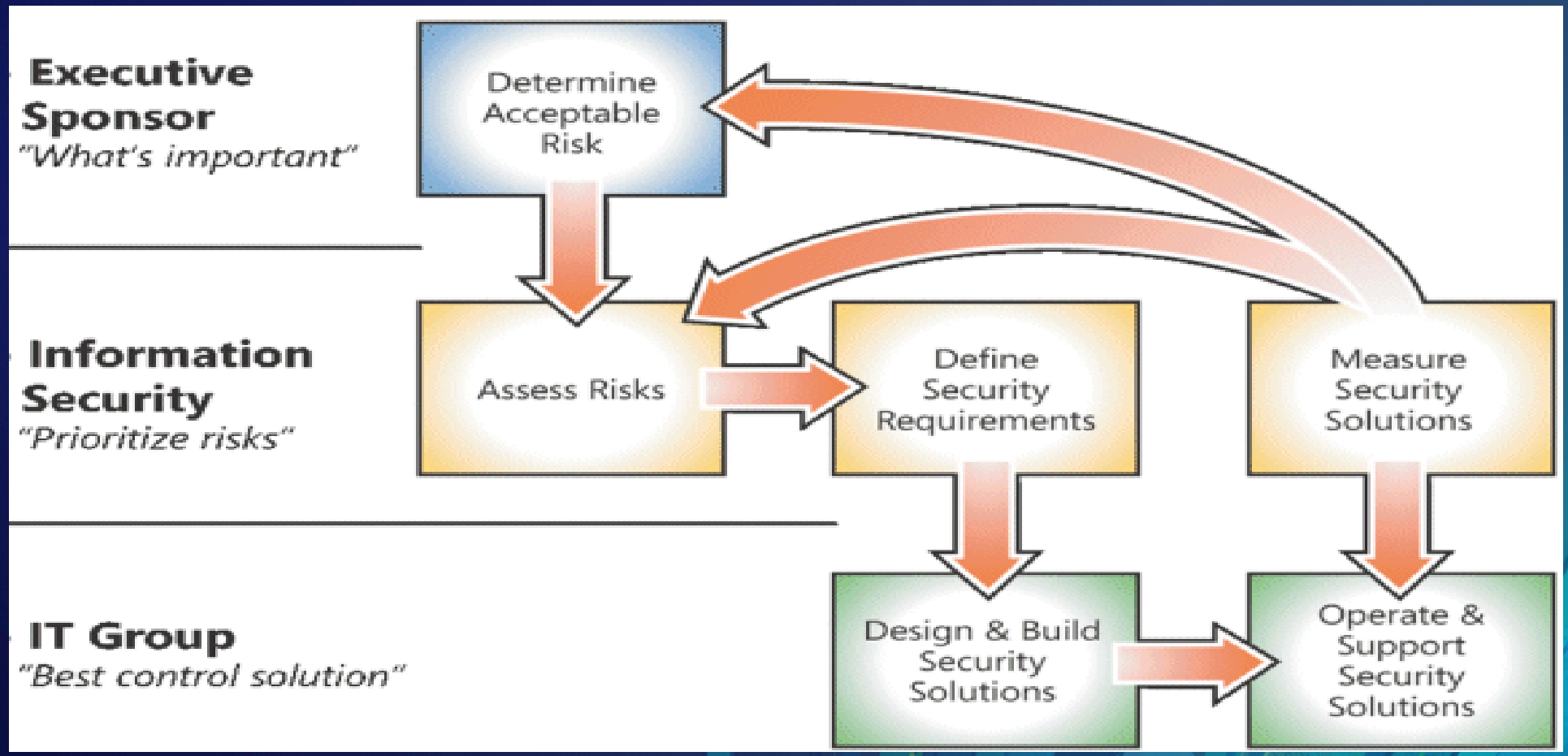
Strategy

A better answer

- Identify your security needs
  - Assess your environment
    - Datasets, systems, users
    - Data categorization and sensitivity
    - Understand your industry attacker motivation
- Understand security options
  - Trust.arcgis.com
  - Enterprise-wide security mechanisms
  - Application specific options
- Implement security as a business enabler
  - Improve appropriate availability of information
  - Safeguards to prevent attackers, not employees

Strategy

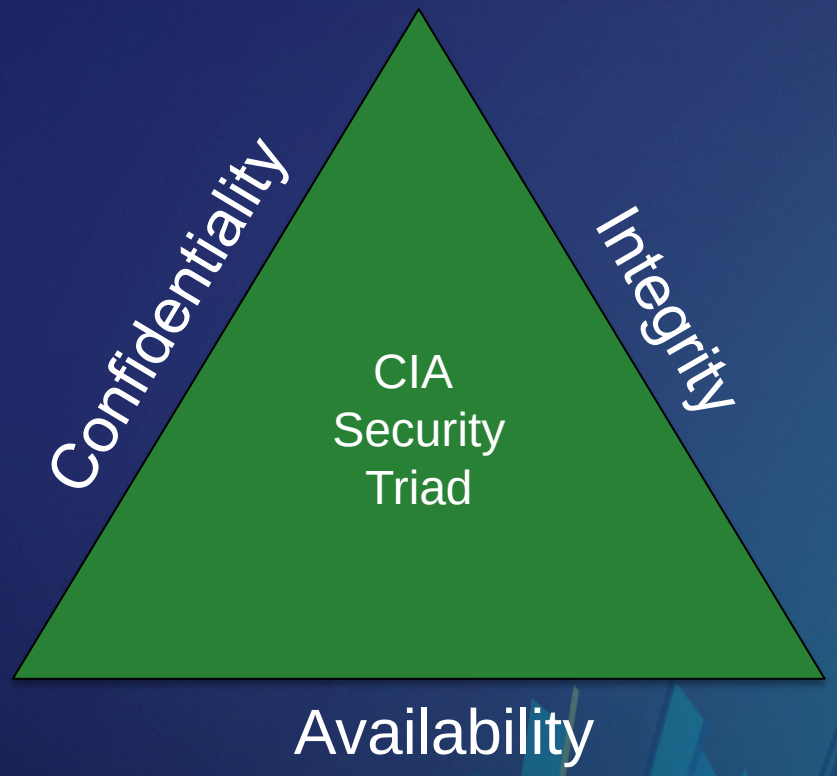
Enterprise GIS Security Strategy



Security Risk Management Process Diagram - Microsoft

Strategy

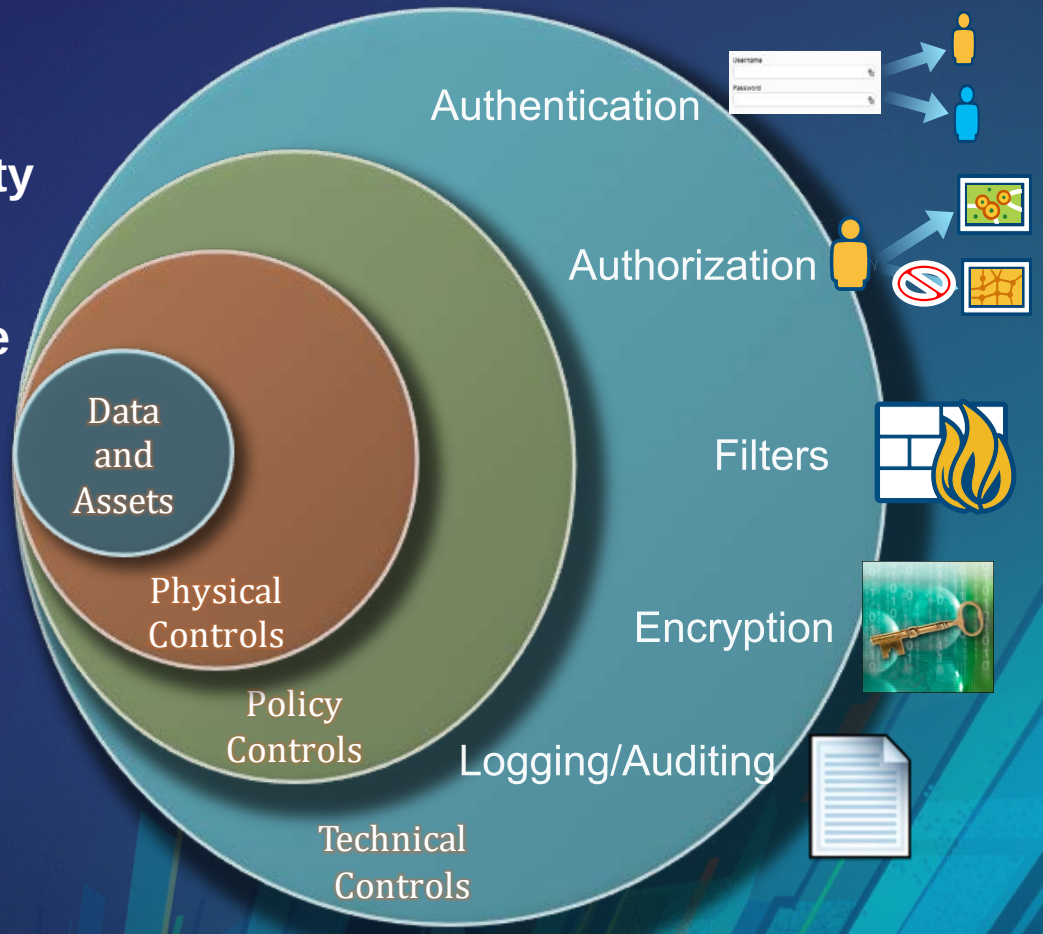
Security Principles



Strategy

Defense in Depth

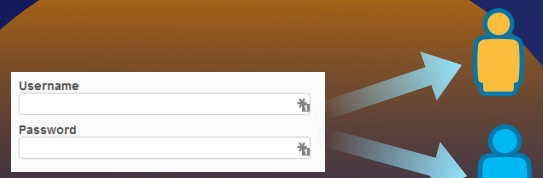
- More layers does NOT guarantee more security
- Understand how layers/technologies integrate
- Simplify
- Balance People, Technology, and Operations
- Holistic approach to security



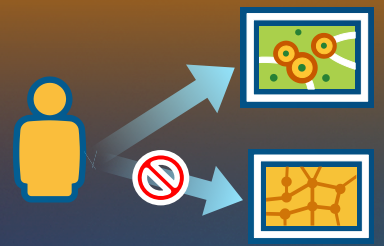
Mechanisms

Randall Williams

Mechanisms



Authentication



Authorization

Filters

Encryption

Logging/Auditing

Mechanisms - Authentication and Authorization

ArcGIS Token Based Authentication

ArcGIS Token-based Authentication

ArcGIS Online Options

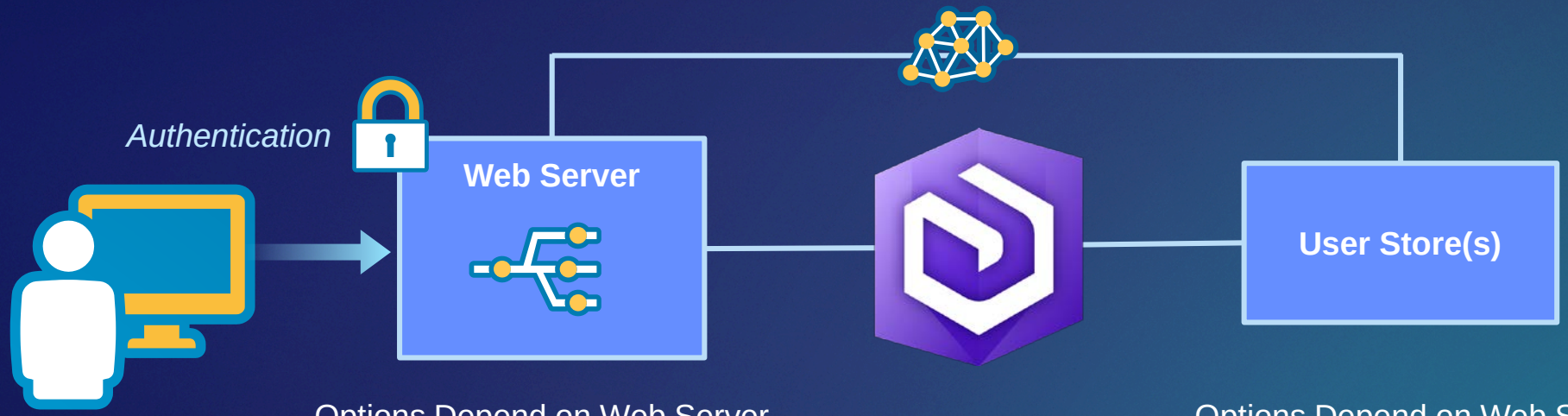
- Built-in User Store

ArcGIS Enterprise Options

- Built-in User Store
- Active Directory
- LDAP

Mechanisms - Authentication and Authorization

Web-Tier Authentication



Options Depend on Web Server…

- Integrated Windows Authentication (IWA)
- Client-Certificate Authentication (PKI)
- HTTP Digest Authentication

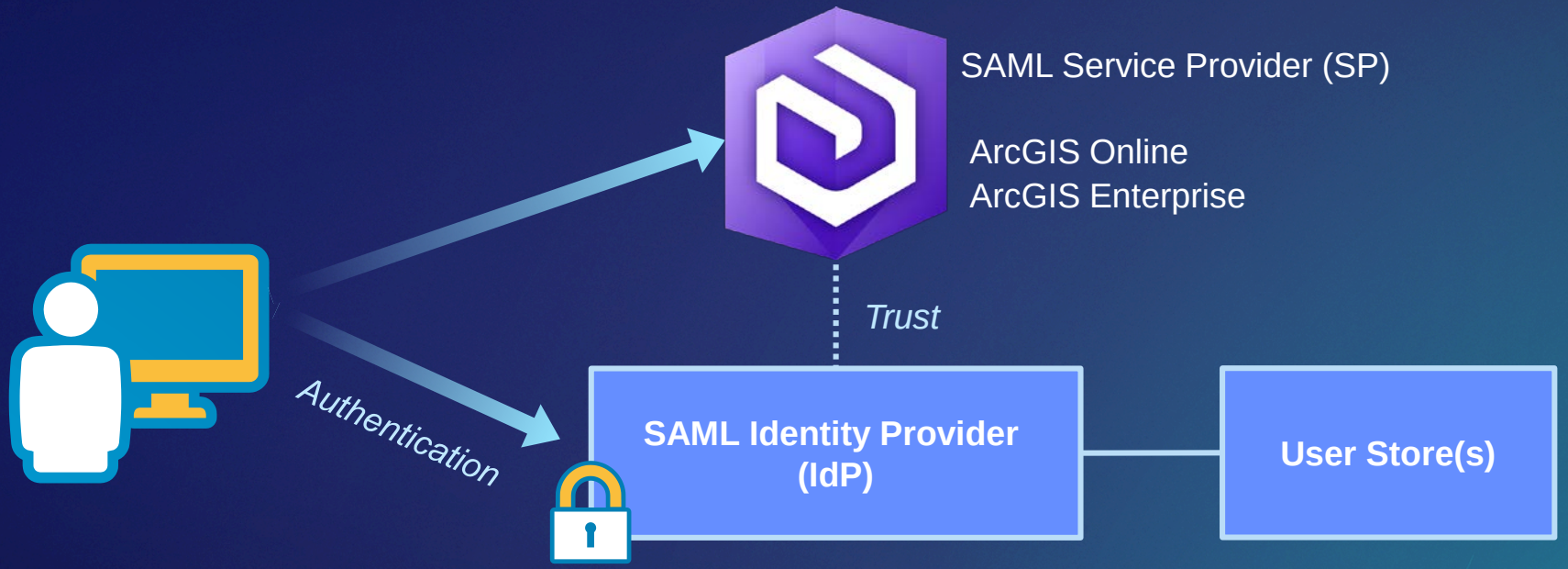
Options Depend on Web Server…

- Active Directory
- LDAP

Only supported using ArcGIS Enterprise…

Mechanisms - Authentication and Authorization

SAML Authentication



Many Options …

- Single or multi-factor authentication
- Client-specific authentication

Many Options …

- Enterprise user store(s)
- One user store or many
- Internal and external users
- …

Provides flexibility and security capabilities depending on IdP…

Mechanisms – Firewalls and Filters

Filters – 3rd Party Options

- Firewalls
  - Host-based
  - Network-based
- Reverse Proxy
- Web Application Firewall
  - Open Source option ModSecurity
- Anti-Virus Software
- Intrusion Detection / Prevention Systems
- Limit applications able to directly access geodatabase

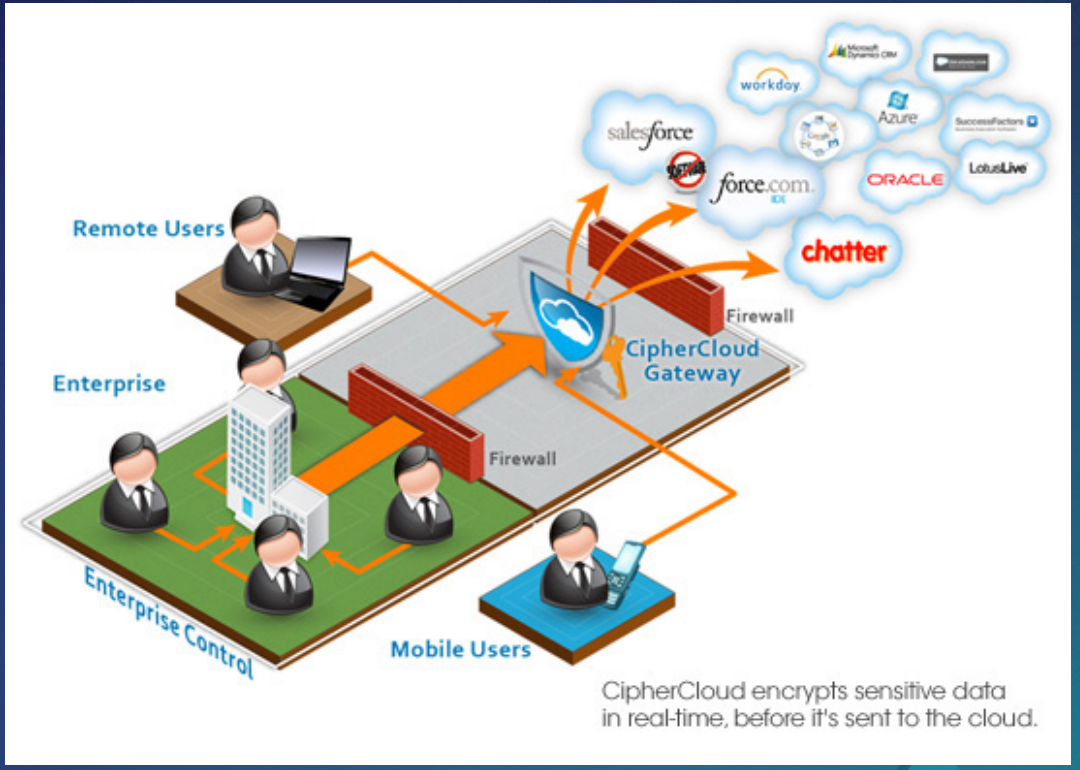
Mechanisms

Encryption – 3rd Party Options

- Network
  - IPSec (VPN, Internal Systems)
  - SSL/TLS (Internal and External System)
  - Cloud Encryption Gateways
    - Only encrypted datasets sent to cloud

- File Based
  - Operating System – BitLocker
  - GeoSpatially enabled PDF's combined with Certificates
  - Hardware (Disk)

- RDBMS
  - Transparent Data Encryption



Mechanisms

Logging and Auditing

- **Logging** involves recording events of interest from a system
- **Auditing** is the practice of inspecting those logs to ensure system is functioning desirably or to answer a specific question about a particular transaction that occurred.

Ensure logging across the system: Applications, Operating System and Network

Esri Apps & Capabilities

- Geodatabase history
- ArcGIS Workflow Manager
- ArcGIS Enterprise logging
- ArcGIS System Monitor

3rd Party Options

- Web Server & Database
- OS
- Network
- SIEM (for consolidation)

Web GIS

Randall Williams

Web GIS

ArcGIS Online or Portal?

ArcGIS Online

- SaaS
  - Releases often
  - Upgraded automatically *(by Esri)*
  - Esri controls SLA
- Functionality *(smart mapping, collaboration…)*
- Enterprise Integration
  - Web SSO via SAML
  - Native MFA
- FedRAMP Low Tailored Low Certified 6/27/2018

ArcGIS Enterprise

- Software
  - ArcGIS Server, Portal, Datastore
  - Releases twice per year
  - Upgraded manually *(by organization)*
  - Organization controls SLA
- Functionality *(smart mapping, collaboration…)*
- Enterprise Integration
  - Web SSO via SAML
  - Web-tier Authentication via Web Adaptor
  - Enterprise Groups
  - ArcGIS Server Integration…

Web GIS

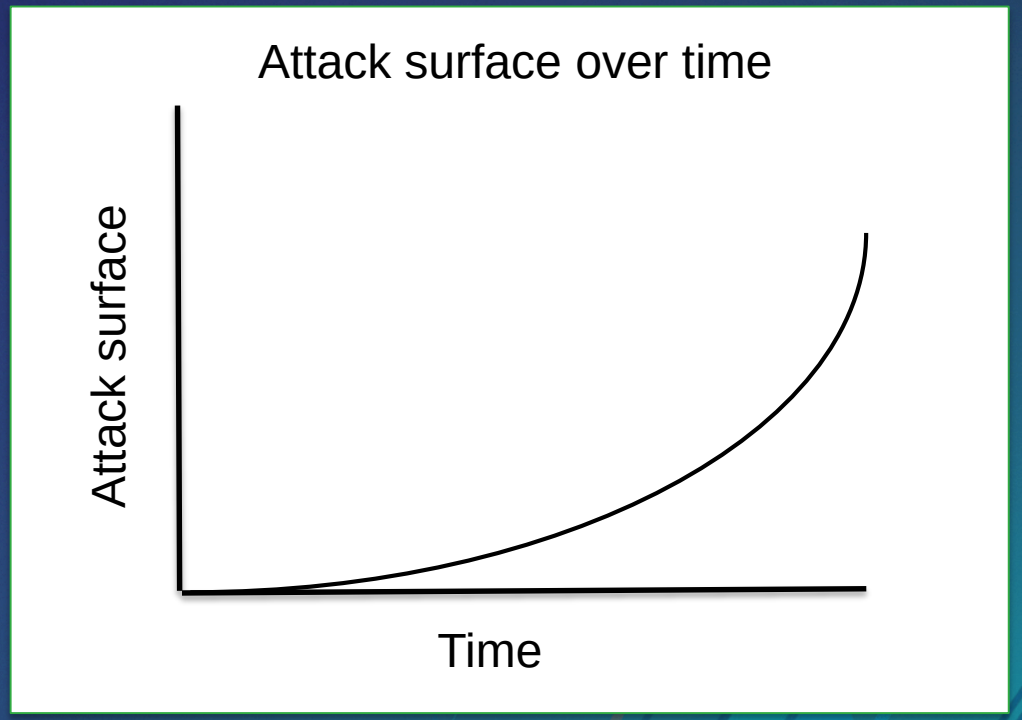
Architecture Options and Security Considerations

- What are the confidentiality and integrity needs of your GIS?
  - Drives extent to which cloud is used
  - Drives potential authentication options used
  - Drives encryption requirements
- What are the availability requirements of your GIS?
  - Redundancy across web tiers, GIS tier, and database tier
- Authentication requirements
  - Leverage centralized authentication (AD/LDAP)
  - For an on premise portal that can be Web-tier authentication or using Enterprise Logins

ArcGIS Enterprise

Implementation Guidance

- Don’t expose Server Manager, Server Admin, or Portal Admin interfaces to public
- Disable Services and Sharing Directories
- Disable Service Query Operations (as feasible)
- Limit utilization of commercial databases under website
  - File GeoDatabase can be a useful intermediary
- Require authentication to web services
- Require HTTPS
  - Or at least make it available!
- Restrict cross-domain requests
- Restrict Portal Proxy capability
  - Implement a whitelist of trusted domains



ArcGIS Enterprise

Recent Enhancements

10.5/10.5.1

- New Membership levels
- Default viewer role that can be assigned
- Portal to Portal collaboration
  - Share content across groups
- Moved option to unfederate ArcGIS Server sites to PortalAdmin
- New privileges for custom roles
- Two new edit privilege levels
  - Edit and Edit with full control
- Security fixes and enhancements

10.6/10.6.1

- Distributed collaboration
  - Share content among different Portals and ArcGIS Online
- Editor tracking for Hosted Feature Services
- Ownership-based access control for Feature Services records
- TLS 1.0 disabled OOTB for new installs
- HSTS support
- Logging and monitoring improvements
- Updated JSON content type
- Security fixes and enhancements

Mobile

Randall Williams

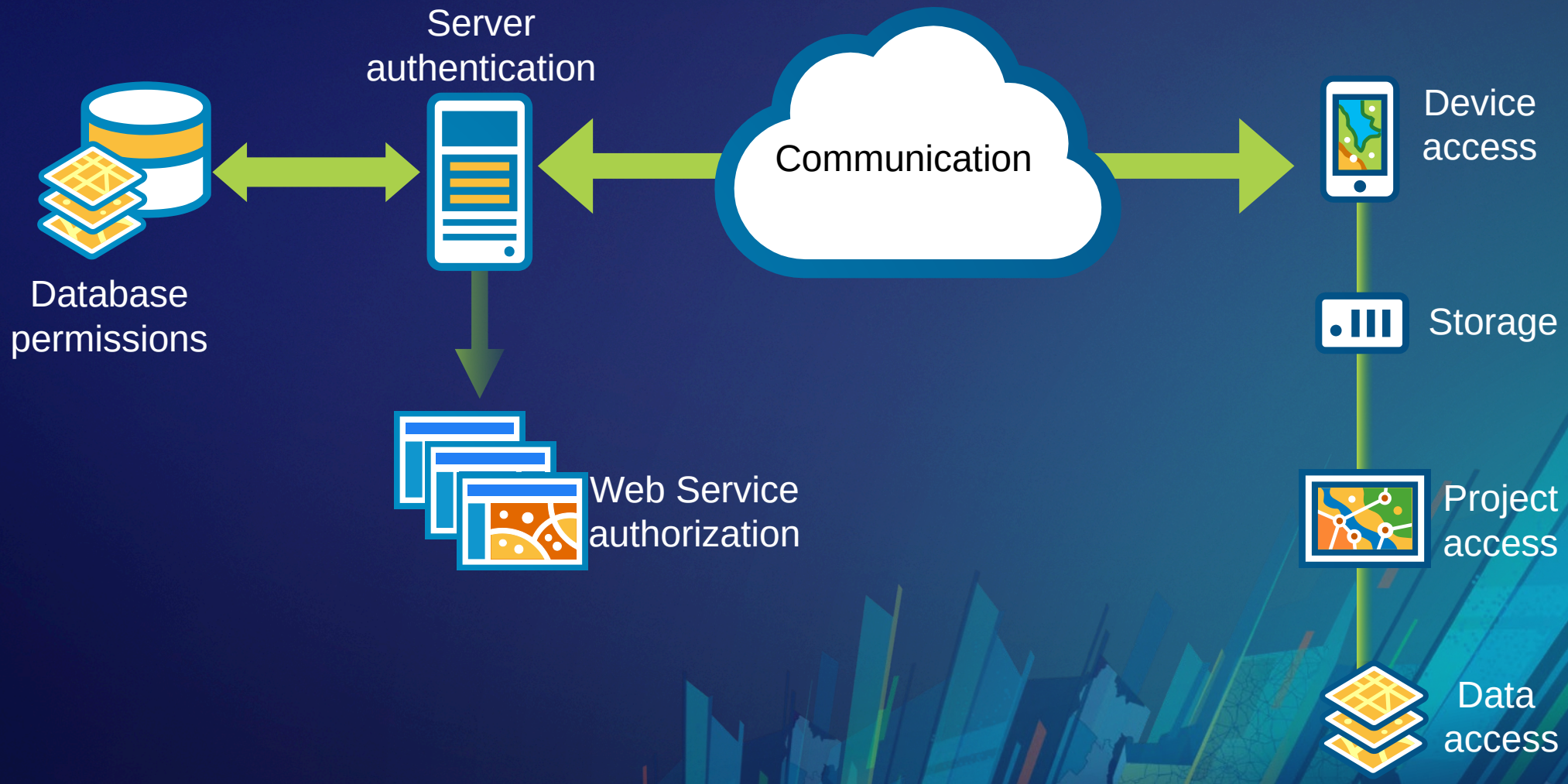
Mobile

What are the mobile concerns? *OWASP Top Ten Mobile: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

M1 - Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.
M2 - Insecure Data Storage	This new category is a combination of M2 + M4 from Mobile Top Ten 2014. This covers insecure data storage and unintended data leakage.
M3 - Insecure Communication	This covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.
M4 - Insecure Authentication	This category captures notions of authenticating the end user or bad session management. This can include: • Failing to identify the user at all when that should be required • Failure to maintain the user's identity when it is required • Weaknesses in session management
M5 - Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.
M6 - Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.
M7 - Client Code Quality	This was the "Security Decisions Via Untrusted Inputs", one of our lesser-used categories. This would be the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.
M8 - Code Tampering	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.
M9 - Reverse Engineering	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.
M10 - Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.

Mobile

Security Touch Points



Mobile

Challenges

- Users are beyond corporate firewall
  - To VPN or not to VPN?
- Authentication/Authorization challenges
- Disconnected editing
  - Local copies of data stored on device
- Management of mobile devices
  - Enterprise Mobility Management is the answer!
    - Mobile Device Management
    - Mobile Application Management
    - Security Gateways
    - Examples: MobileIron, MaaS360, Airwatch, and many more…

Mobile

Implementation Guidance

- Encrypt data-in-transit (HTTPS) via TLS
- Encrypt data-at-rest
- Segmentation
  - Use ArcGIS Online, Cloud, or DMZ systems to disseminate public-level data
- Perform Authentication/Authorization
- Use an Enterprise Mobility Management (EMM) solution
  - Secure e-mail
  - Enforce encryption
  - App distribution
  - Remote wipe
  - Control 3rd party apps & jailbreak detection
  - Distribute Certificates

Mobile

Need More Granularity?

White Paper: ArcGIS Secure Mobile Implementation Patterns

- Replacing redundant inefficient field processes
- Reducing costs and overhead
- Improving collection speed, accuracy, and currency of data
- Modernizing workflows and replacing paper-based workflows
- Helping management make timely and informed decisions

There are two additional mobile apps in the ArcGIS Platform that do not support field data collection workflows, but support other business use cases, (see Figure 5). These apps are mentioned in this document for completeness and are available for both iOS and Android devices. They will follow the same mobile implementation patterns described in later sections of this document. The apps are:

- **ArcGIS Business Analyst**[14]: Enables demographic and socio-economic data in the field
- **AppStudio Player for ArcGIS**: Displays custom apps built with *AppStudio for ArcGIS*[15]

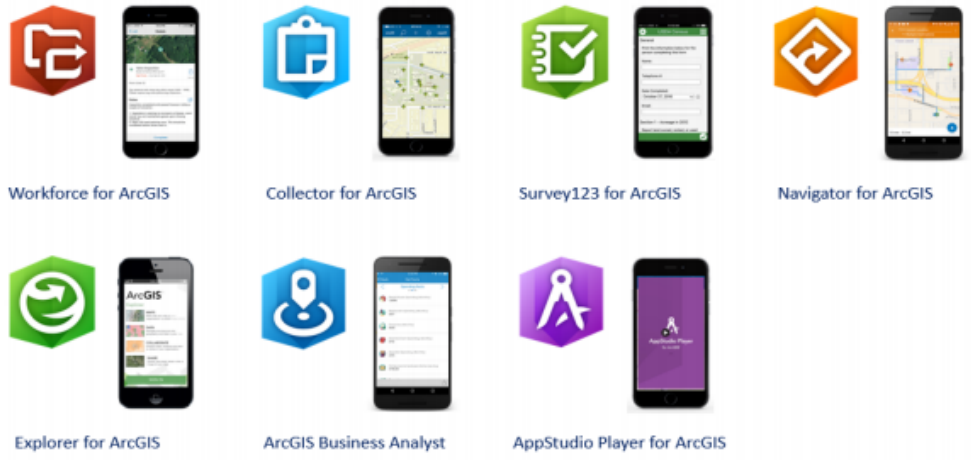


Figure 5: ArcGIS Mobile Apps

All these apps are designed to work with the ArcGIS Platform and support all Web GIS deployment

Cloud

Randall Williams

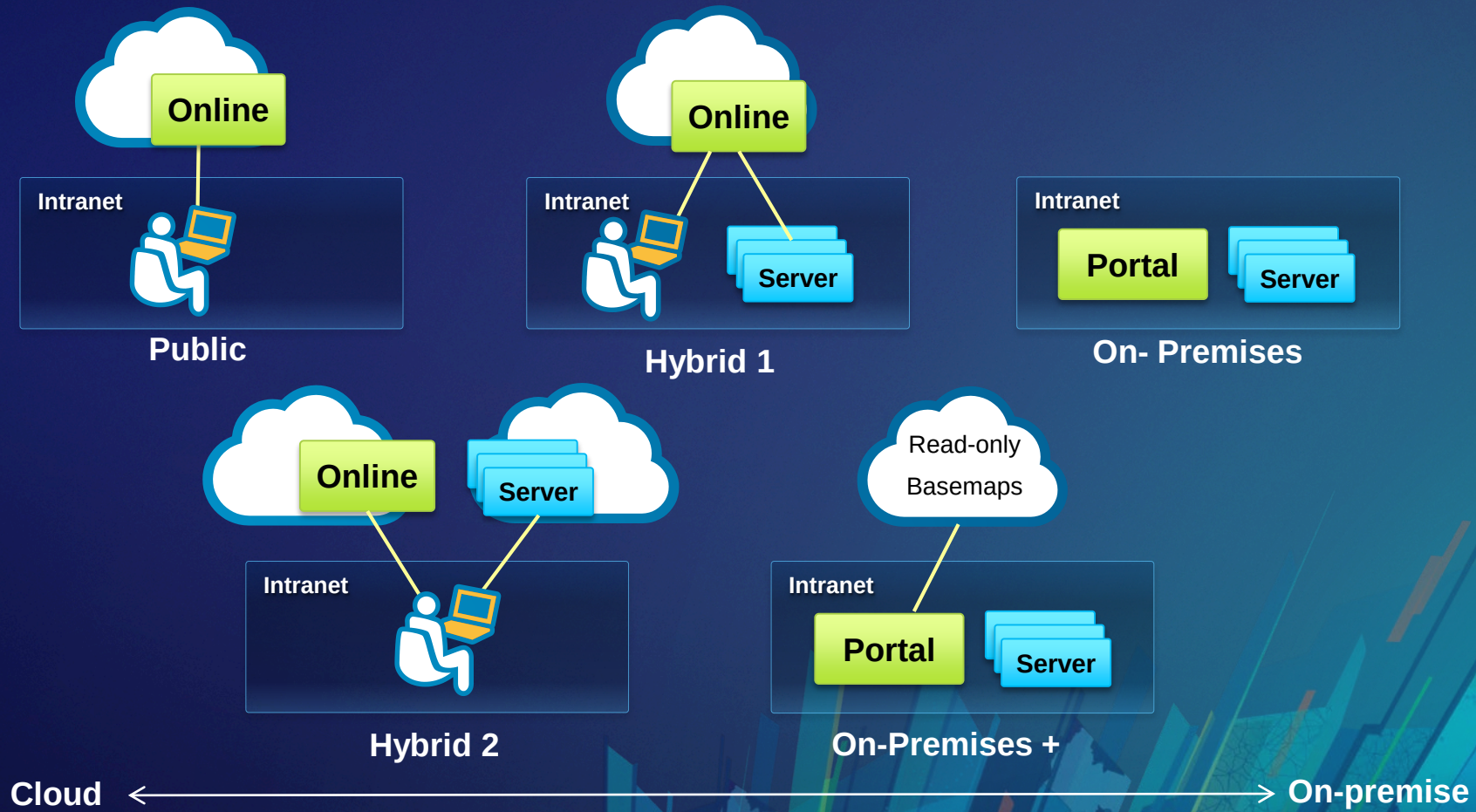
Cloud

Service Models

- **Non-Cloud: On Premises**
  - Traditional systems infrastructure deployment
  - ArcGIS Enterprise
- **IaaS: Infrastructure as a Service**
  - ArcGIS Enterprise
  - Some Citrix / Desktop
- **SaaS: Software as a Service**
  - ArcGIS Online
  - Business Analyst Online

Cloud

Deployment Models



ArcGIS Enterprise in the Cloud

IaaS Use Case – Amazon Web Services

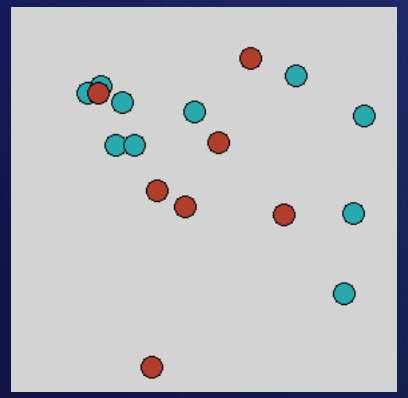
- 8 Security Areas to Address
  - Virtual Private Cloud (VPC)
  - Identity & Access Management (IAM)
  - Administrator gateway instance(s) (Bastion)
  - Reduce attack surface (Hardening)
  - Security Information Event Management (SIEM)
  - Patch management (SCCM)
  - Centralized authentication/authorization
  - Web application firewall (WAF)

Cloud

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**

On-Premises Operational Layer Service

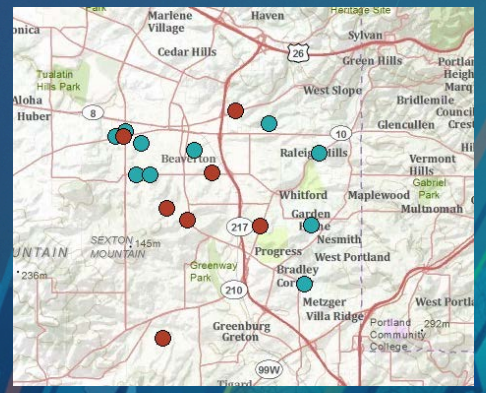


https://YourServer.com/arcgis/rest...

Cloud Basemap Service ArcGIS Online

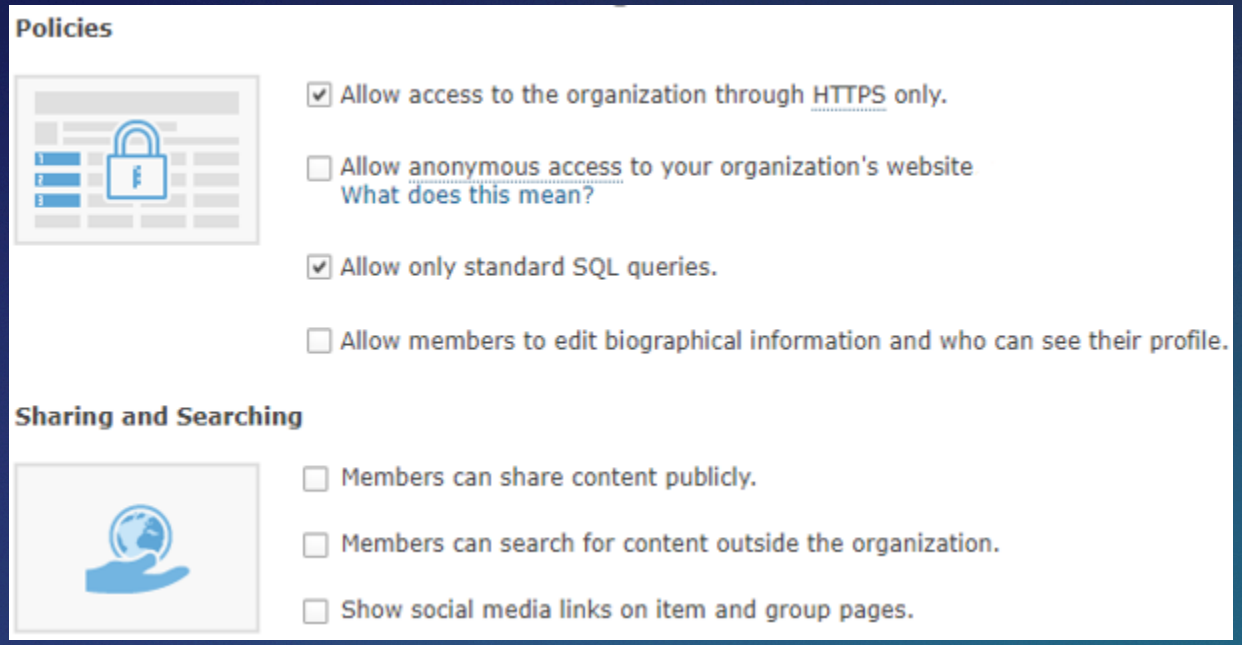
http://services.arcgisonline.com...

Browser Combines Layers



Cloud

ArcGIS Online – Implementation Guidance



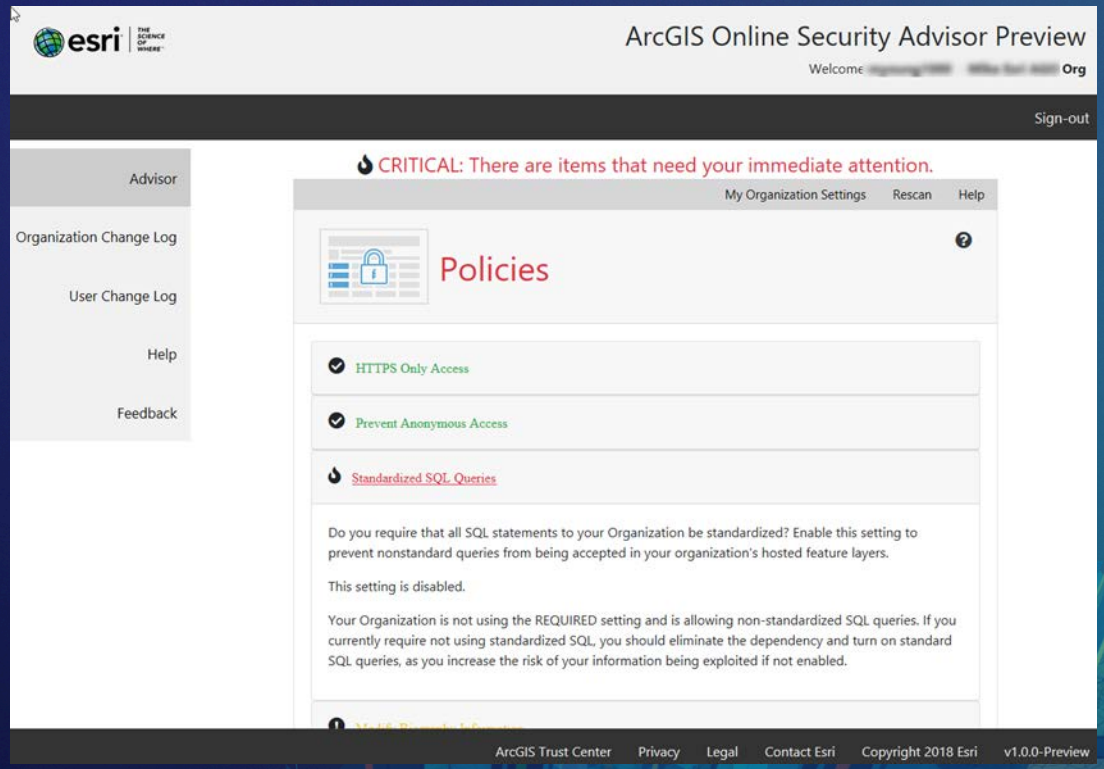
- Require HTTPS
- Do not allow anonymous access
- Allow only standard SQL queries
- Restrict members from sharing outside of organization (as feasible)
- Use enterprise logins with SAML 2.0 with existing Identity Provider (IdP)
  - If unable, use a strong password policy (configurable) in ArcGIS Online
  - Enable multi-factor authentication for users
- Always use multi-factor authentication for admin accounts
- Use a least-privilege model for roles and permissions
  - Custom roles

Cloud

ArcGIS Online – Implementation Guidance

How can you validate your configuration options?

New tool: ArcGIS Online Security Advisor - https://arcg.is/ago-advisor



Compliance

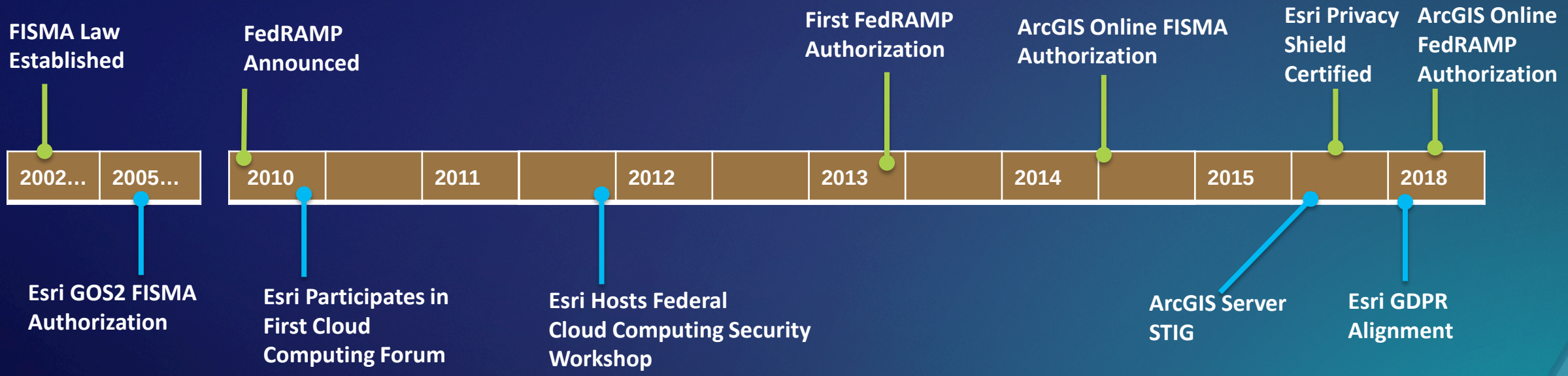
Michael Young

Compliance

- Milestones
- Cloud Infrastructure Providers
- Products and Services
- Privacy Assurance / GDPR
- Security Assurance / FedRAMP

Compliance

Milestones



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

Compliance

Cloud Infrastructure Providers

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

Cloud Infrastructure Security Compliance

Compliance

Products & Services

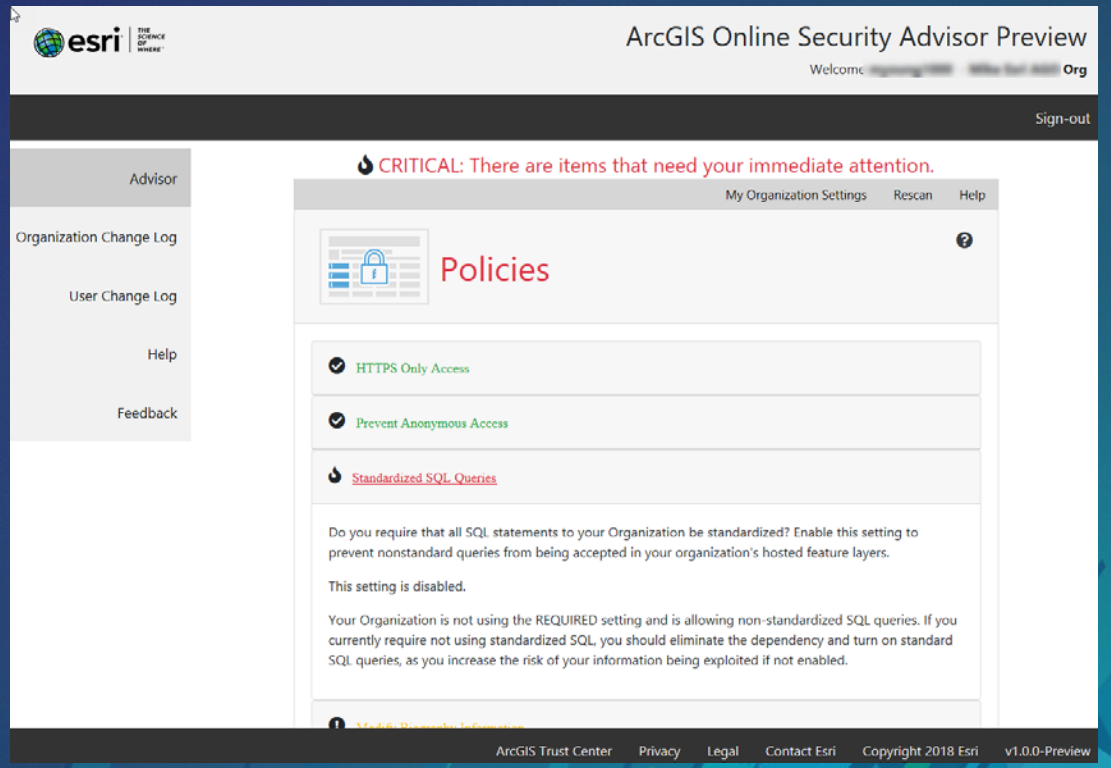
- **Service Based Initiatives**
  - EMCS Advanced Plus (Single-tenant) – FedRAMP Moderate
  - ArcGIS Online (Multi-tenant) – FedRAMP Tailored Low - *NEW!*

- **Product Based Initiatives**
  - ArcGIS Server
    - DISA STIG – Completed in 2016
    - ArcGIS Server 10.3 (More STIGs to follow)
    - Last update was released in 2018
    - Confirmed compatibility through all current product versions
  - ArcGIS Desktop (10.1 and above) and ArcGIS Pro (1.4.1 and above)
    - USGCB Self-Certified

Compliance

Products & Services

- **Security validation tools**
  - **ArcGIS Server – Python script located in Admin tools directory**
  - **Portal for ArcGIS – Python script located in Security tools directory**
  - **NEW - ArcGIS Online Security Advisor**
    - **Checklist validates your org settings/usage against secure best practice recommendations**



Compliance

Privacy Assurance

- **EU-U.S. Privacy Shield self-certified**
  - General Esri Privacy Statement
  - Products & Services Privacy Statement Supplement

- **TRUSTe provides privacy certification and dispute resolution**

- **General Data Protection Regulation (GDPR)** ***NEW***

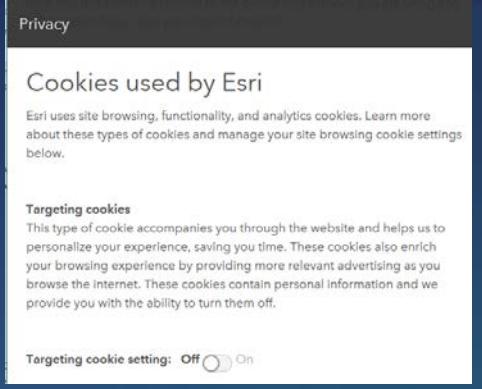
Compliance

GDPR / Privacy

Esri supports GDPR and continues to advance our privacy & security practices

Compliance

GDPR - Privacy Impact Assessment (PIA)



- Esri has been performing PIA's since the early 2000's for Online services
  - ArcGIS GDPR/Privacy Best Practices whitepaper to be released soon to help guide customers
  - We welcome assisting customers with their PIA's as necessary

- Supplementary privacy statement created specifically for our Products & Services
  - Privacy Collection & storage of privacy information is minimized in our products
  - Online Telemetry service (EUEI) disabled by default for organizations outside the US

- Company-wide privacy improvements
  - Tracking cookies can now be disabled centrally across Esri.com & ArcGIS.com
  - When Esri is Controller of customer PI, requests handled through Privacy@esri.com

Compliance

GDPR - Protect By Design

- Esri established a formal Security Development Lifecyle in 2017
- Addresses governance structure (CISO – Products, CISO – Corporate)
- Guidelines practices based on BSIMM, OWASP, CWE/SANS
- Most rigorous security measures starting with ArcGIS Enterprise & Online
- Static, Dynamic, and Component Analysis + 3rd party testing
- Product Security Incident Response Team (PSIRT) established
- FedRAMP Tailored Low Authorization drives continuous monitoring
- Customer datasets written/updated after March 10th, 2018 are encrypted at rest
  - Pre-existing datasets to be encrypted by end of 2018

Compliance

FedRAMP

- ArcGIS Online received an Agency FedRAMP Tailored Low authorization-to-operate (ATO) on June 28, 2018
- Authorization known as a Low-Impact Software as a Service (Li-SaaS)
- Value to US Government Agencies
  - FedRAMP standardizes way US government agencies perform security authorizations for cloud products and services, shifting the authorization process from years/months to weeks/days
- Value to Global Organizations
  - Recognized by many organizations around the globe as a gold standard for security
  - Mapping of ISO 27001 & 15408 controls is readily available via the Trust Center

Compliance

FedRAMP Alignment

- A Customer Responsibility Matrix (CRM) details recommended Organization settings to align with FedRAMP guidelines (summarized below)
  - Enable the HTTPS Only Security Policy
  - Enable Allow only Standard SQL Queries
  - Disable Security Policy allowing members to edit biographical information
  - Enable SAML v2.0 Enterprise Logins
  - Disable Social logins (w/exception for Google business accounts)
  - Add relevant domains for Allow Origins
  - Enable using Esri vector basemaps under Settings/Map/Basemap Gallery

Compliance

Summary

Summary

Michael Young

Summary

- Security demands are rapidly evolving
  - Prioritize efforts accord to your industry and needs
  - Don’t just add components, simplified Defense In Depth approach
  - Don’t get caught off-guard by security changes (Read the TLS Guide)

- Esri continues to advance their privacy and security
  - New FedRAMP Tailored Low authorization and GDPR alignment

- Secure Best Practice Guidance is Available
  - Check out the Trust.ArcGIS.com Site!
  - Mobile security whitepaper available now and GDPR paper coming soon
  - New security validation tools available use them now!

  - Feel free to contact us:
    - SoftwareSecurity@esri.com

esri
THE
SCIENCE
OF
WHERE