Minimizing Sensitive Data Leaks

Jeff Rummelsburg

Randall Williams

Esri Software Security & Privacy

2023 ESRI USER CONFERENCE

esri THE SCIENCE OF WHERE®

Pop Quiz

Q: What is the most common security issue reported by users of ArcGIS Online?

a. Denial of Service

b. [✓ Information Leaks/Spills]

c. “Misinformation Propagation”

d. Hacked Accounts

Q: How do ArcGIS Online information leaks and spills occur?

a. Organization configuration

b. Item configuration

c. Account sharing practices

d. Lack of governance

[✓ e. All of the above]

What do we do about this?

Let’s discuss:

- Esri Privacy Initiatives & ArcGIS Online
- Configuration options and best practices
- Tools to help Monitor
- Processes and Pipelines

Esri Privacy Initiatives & ArcGIS Online

Building a Culture of Privacy

Privacy at its core: Our privacy efforts focus on internal governance systems that integrate privacy and data usage standards throughout Esri's operations.

- Privacy Committee: A multi-departmental committee, meeting monthly to uphold our privacy commitments.
- Integration: Privacy is embedded as an essential feature in our processes and development.
- Accountability & Trust: Shared responsibility of protecting privacy and transparency about data handling practices.
- Privacy Resources: Internal site and guidance documentation on privacy best practices.

Privacy Education: We advocate that privacy is a collective responsibility and promote ongoing education through comprehensive training and awareness campaigns.

- Privacy Training and Awareness
- Privacy week
- Roadshows

Esri's Product Privacy Priorities

- **Designing for privacy**: We design our products with privacy in mind from the start.
  - Privacy by Design (PbD)
  - Secure privacy experience
  - Age-Appropriate Privacy
- **Building privacy into our processes:** We have processes in place to ensure that privacy is considered throughout the development and operation of our products.
- **Safeguards & controls:** We've established both procedural and technical measures to mitigate privacy risks, ensuring compliance with all regulatory requirements related to data privacy.
- **Incident Management:** Our Incident Management program oversees the processes for identifying, assessing, mitigating, and remedying privacy incidents.
- **Privacy Principles:** Our processes guide the development of new or modified products, services, or practices according to our internal privacy expectations.
  - Purpose Limitation
  - Data Minimization & Retention
  - Data Access & Management
  - Fairness & Accountability

Esri's Privacy Initiatives in ArcGIS Online

- **Accountability & Transparency:** We offer customers a robust Data Processing Addendum (DPA) with privacy commitments, including data transfer mechanisms and provisions for compliance with data protection laws.
- **Security:** ArcGIS Online offers a variety of privacy features to ensure the security and confidentiality of user data including encryption, coding best practices, access control, and deployment models.
- **Resources & Guidance:** Extensive customer privacy guidance documents that covers high-level architecture guidance, down to individual configuration settings.
- **Privacy Rights:** Facilitate compliance with data protection regulations through features for data access, export, deletion, and updates. This includes support for processing restrictions, consent, data portability, and the right to be forgotten.
- **Privacy Compliance:** Adherence to GDPR, CCPA, and other international data privacy laws
- **Ownership Retention:** Customers maintain full ownership of their content. This means that the data you upload to ArcGIS Online remains yours.

Future of Privacy & Esri’s Commitment

- **New laws & regulations:** By the end of 2024, it is predicted that 75% of the world's population will have their personal data covered under modern privacy regulations.
- **Technological Advancements**: The development of privacy software and tools will play a significant role in the future of privacy.
- **AI Review:** As AI expands, our Responsible AI efforts are driven by our mission to ensure the positive impact of AI for people and society.
- **Data Localization**: There is increasing attention to data sovereignty issues worldwide.
- **Prioritize transparency and communication**: Clearly communicate with customers about data collection, usage, and protection measures to ensure trust.

Esri commitment to privacy: Protecting user data and privacy is vital to our business and vision. We continuously enhance our privacy program and products to meet evolving expectations and technological advancements.

Configuration Options & Best Practices

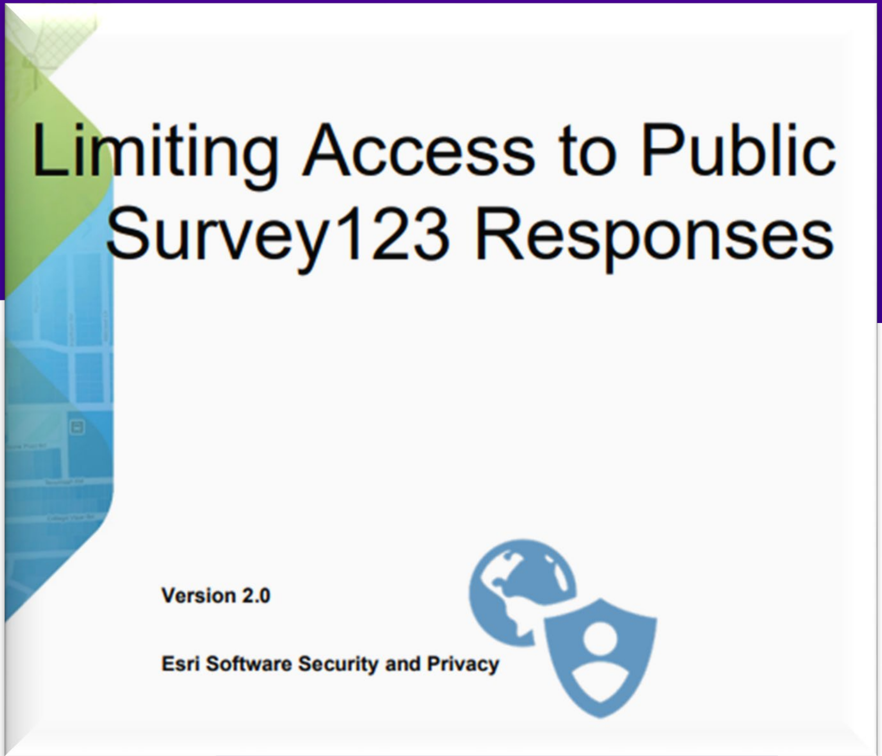
Tons of materials in ArcGIS Trust Center

An Esri
Software Security and Privacy
Technical Paper

January 2023

Version 3.2

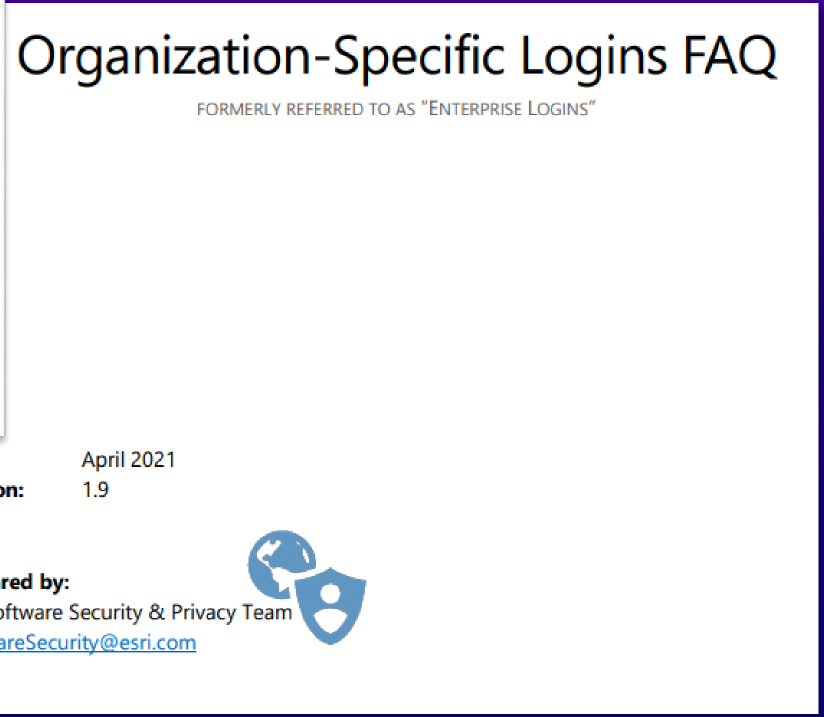
ArcGIS® Location Sharing Privacy Best Practices



Limiting Access to Public Survey123 Responses

Version 2.0

Esri Software Security and Privacy



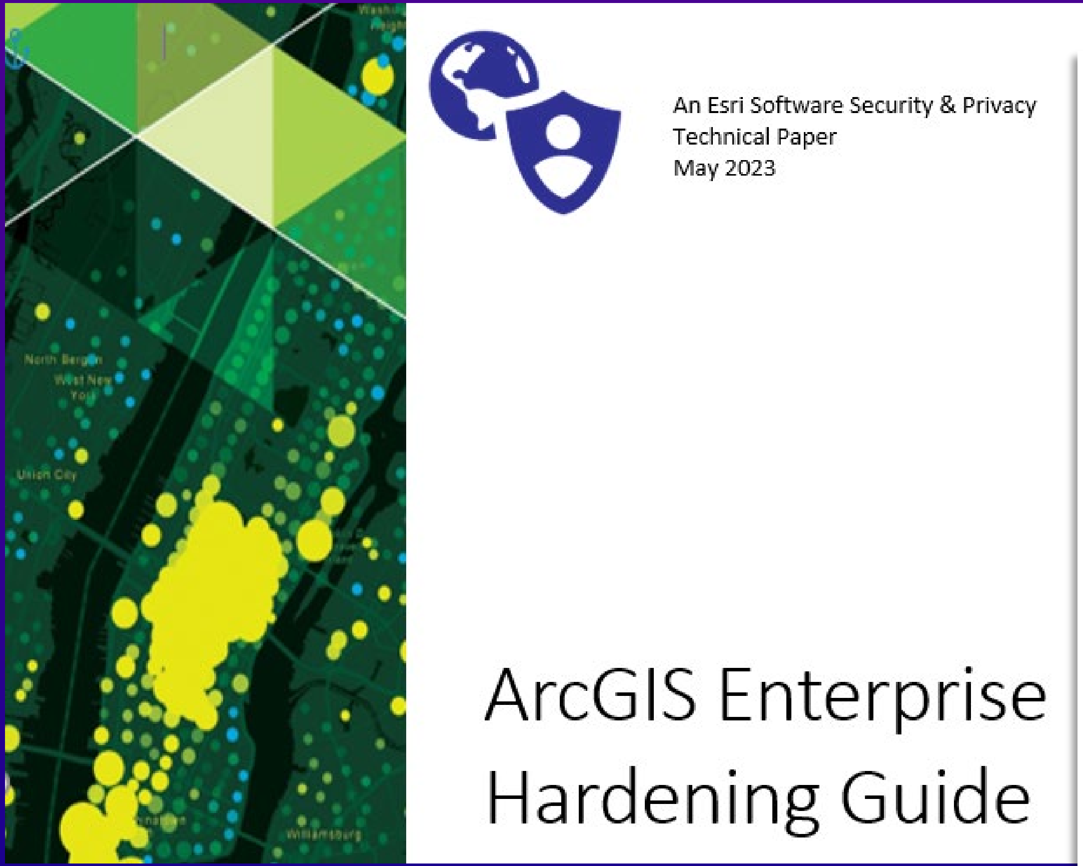
Organization-Specific Logins FAQ

FORMERLY REFERRED TO AS "ENTERPRISE LOGINS"

Date: April 2021
Version: 1.9

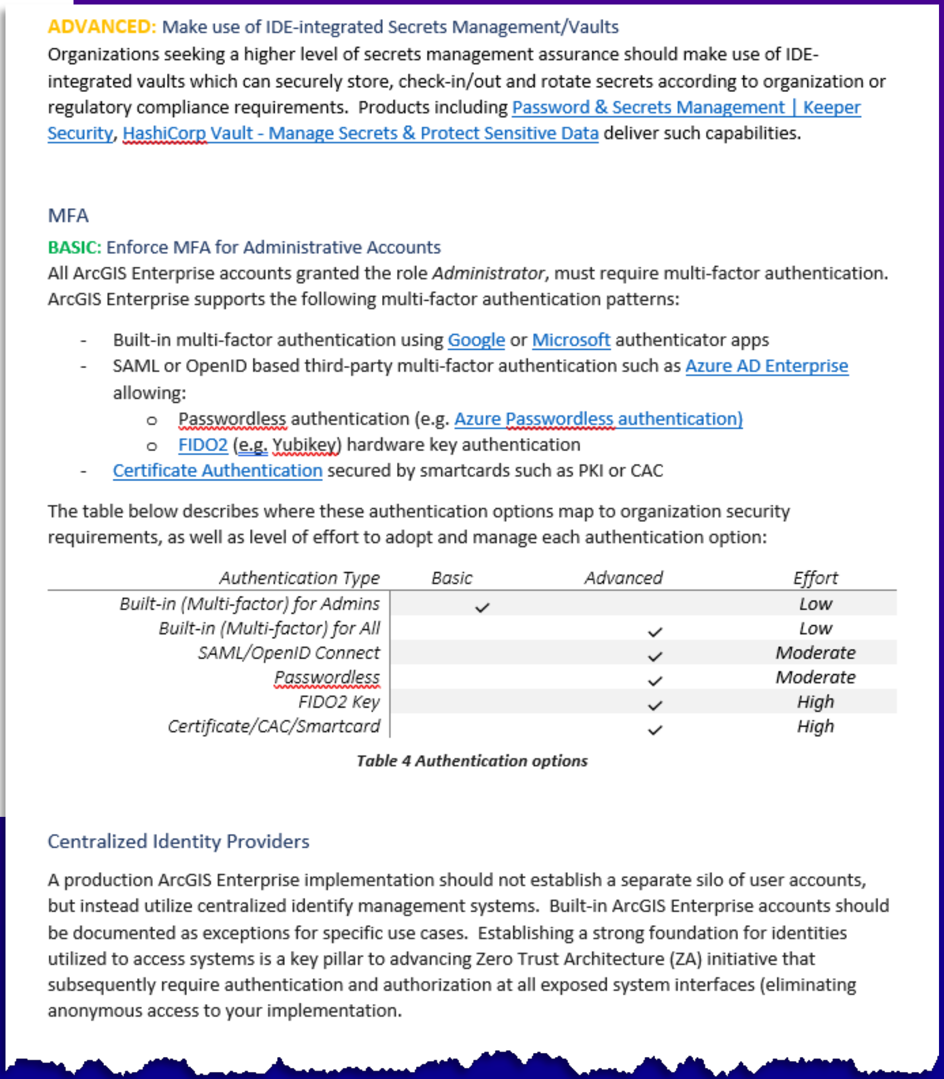
Prepared by:
Esri Software Security & Privacy Team
SoftwareSecurity@esri.com

Teaser: ArcGIS Enterprise Hardening Guide



An Esri Software Security & Privacy
Technical Paper
May 2023

ArcGIS Enterprise Hardening Guide



ADVANCED: Make use of IDE-integrated Secrets Management/Vaults

Organizations seeking a higher level of secrets management assurance should make use of IDE-integrated vaults which can securely store, check-in/out and rotate secrets according to organization or regulatory compliance requirements. Products including Password & Secrets Management | Keeper Security, HashiCorp Vault - Manage Secrets & Protect Sensitive Data deliver such capabilities.

MFA

BASIC: Enforce MFA for Administrative Accounts

All ArcGIS Enterprise accounts granted the role *Administrator*, must require multi-factor authentication. ArcGIS Enterprise supports the following multi-factor authentication patterns:

- Built-in multi-factor authentication using Google or Microsoft authenticator apps
- SAML or OpenID based third-party multi-factor authentication such as Azure AD Enterprise allowing:
  - Passwordless authentication (e.g. Azure Passwordless authentication)
  - FIDO2 (e.g. Yubikey) hardware key authentication
- Certificate Authentication secured by smartcards such as PKI or CAC

The table below describes where these authentication options map to organization security requirements, as well as level of effort to adopt and manage each authentication option:

Authentication Type	*Basic*	*Advanced*	*Effort*
Built-in (Multi-factor) for Admins	✓		*Low*
Built-in (Multi-factor) for All		✓	*Low*
SAML/OpenID Connect		✓	*Moderate*
Passwordless		✓	*Moderate*
FIDO2 Key		✓	*High*
Certificate/CAC/Smartcard		✓	*High*

Table 4 Authentication options

Centralized Identity Providers

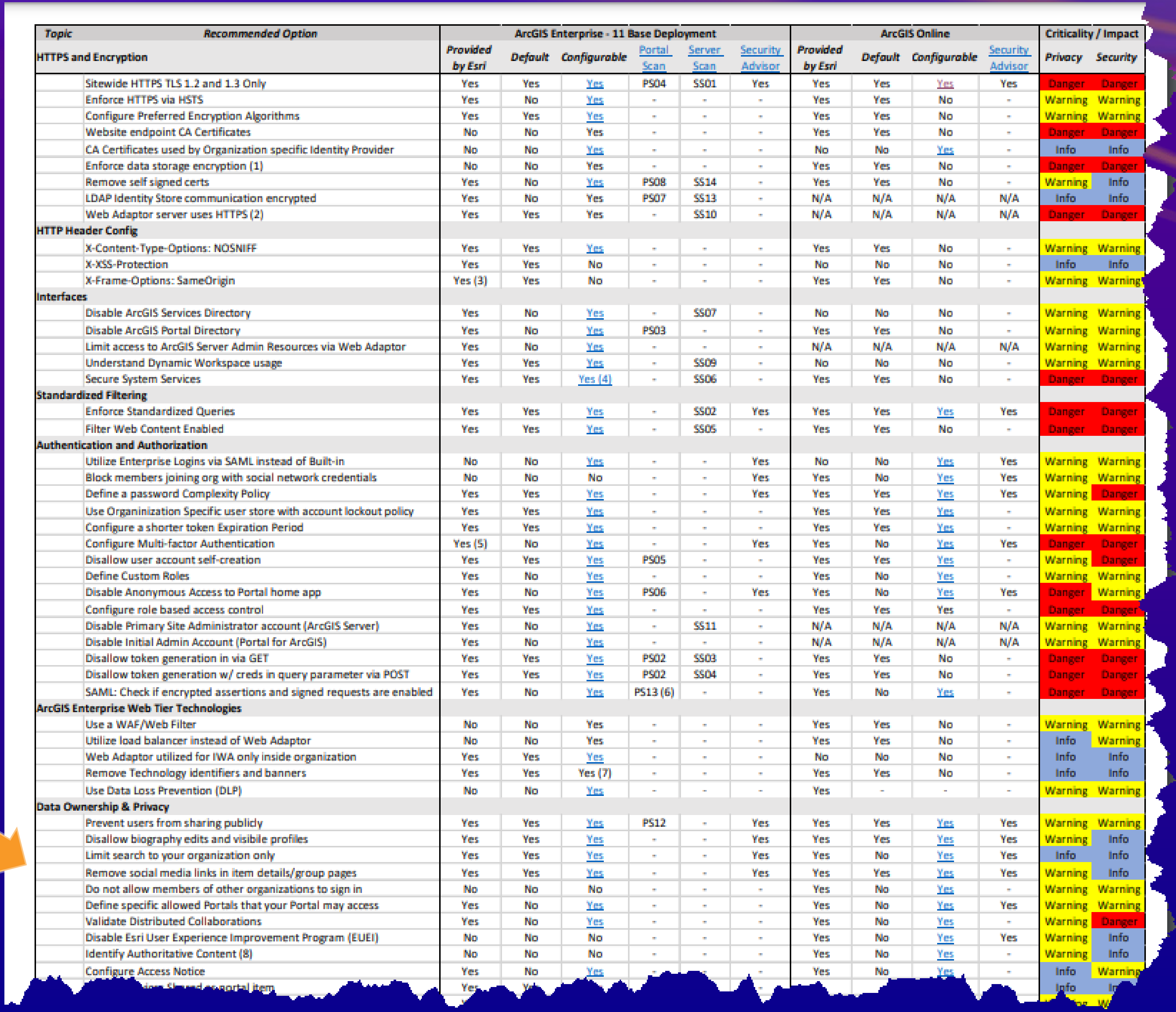
A production ArcGIS Enterprise implementation should not establish a separate silo of user accounts, but instead utilize centralized identify management systems. Built-in ArcGIS Enterprise accounts should be documented as exceptions for specific use cases. Establishing a strong foundation for identities utilized to access systems is a key pillar to advancing Zero Trust Architecture (ZA) initiative that subsequently require authentication and authorization at all exposed system interfaces (eliminating anonymous access to your implementation.

Cheat Sheet!

https://TRUST.arcgis.com

Online & Enterprise

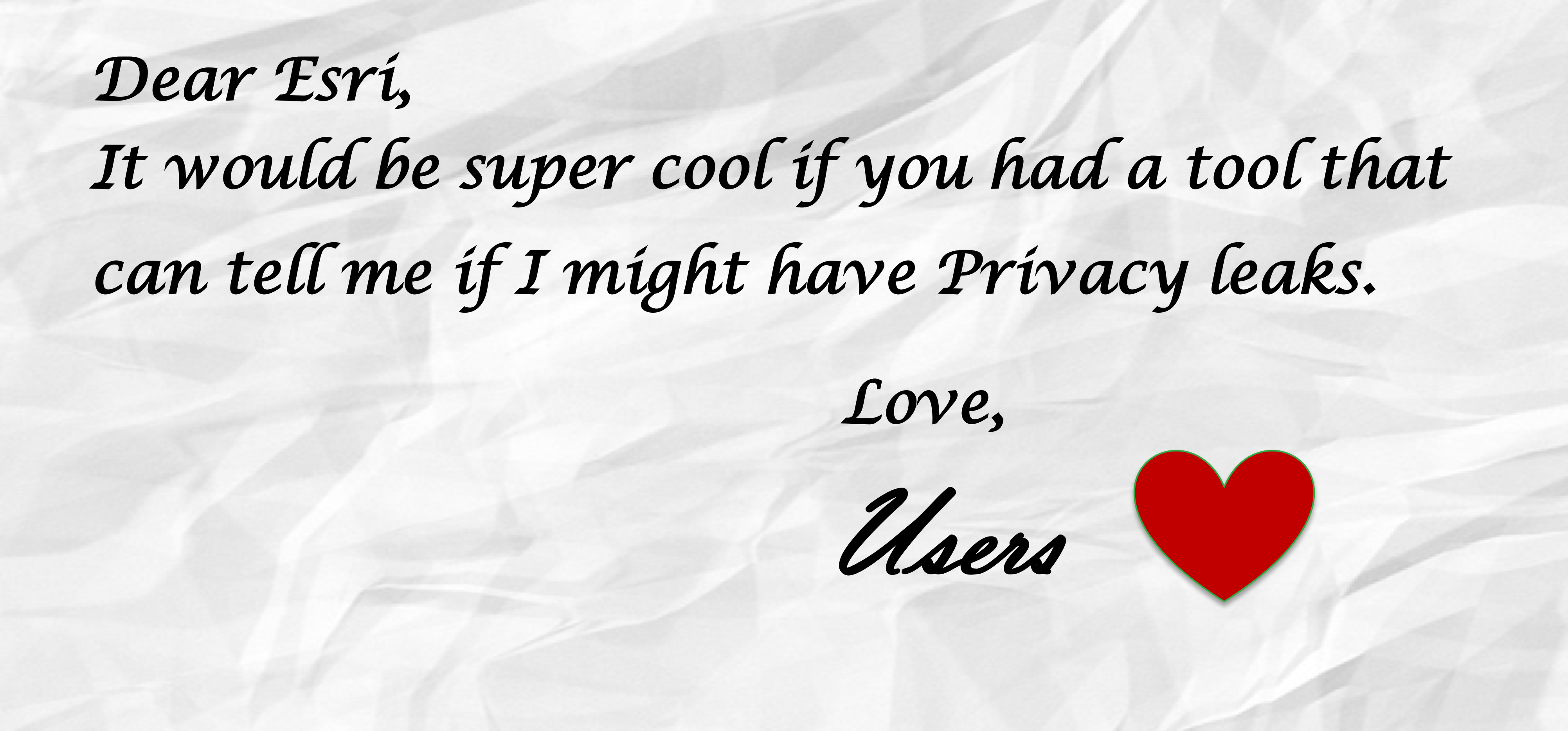
Privacy Guidance Included



Topic	Recommended Option	ArcGIS Enterprise - 11 Base Deployment						ArcGIS Online				Criticality / Impact	
HTTPS and Encryption		Provided by Esri	Default	Configurable	Portal Scan	Server Scan	Security Advisor	Provided by Esri	Default	Configurable	Security Advisor	Privacy	Security
	Sitewide HTTPS TLS 1.2 and 1.3 Only	Yes	Yes	Yes	PS04	SS01	Yes	Yes	Yes	Yes	Yes	Danger	Danger
	Enforce HTTPS via HSTS	Yes	No	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
	Configure Preferred Encryption Algorithms	Yes	Yes	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
	Website endpoint CA Certificates	No	No	Yes	-	-	-	Yes	Yes	No	-	Danger	Danger
	CA Certificates used by Organization specific Identity Provider	No	No	Yes	-	-	-	No	No	Yes	-	Info	Info
	Enforce data storage encryption (1)	No	No	Yes	-	-	-	Yes	Yes	No	-	Danger	Danger
	Remove self signed certs	Yes	No	Yes	PS08	SS14	-	Yes	Yes	No	-	Warning	Info
	LDAP Identity Store communication encrypted	Yes	No	Yes	PS07	SS13	-	N/A	N/A	N/A	N/A	Info	Info
	Web Adaptor server uses HTTPS (2)	Yes	Yes	Yes	-	SS10	-	N/A	N/A	N/A	N/A	Danger	Danger
HTTP Header Config													
	X-Content-Type-Options: NOSNIFF	Yes	Yes	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
	X-XSS-Protection	Yes	Yes	No	-	-	-	No	No	No	-	Info	Info
	X-Frame-Options: SameOrigin	Yes (3)	Yes	No	-	-	-	Yes	Yes	No	-	Warning	Warning
Interfaces													
	Disable ArcGIS Services Directory	Yes	No	Yes	-	SS07	-	No	No	No	-	Warning	Warning
	Disable ArcGIS Portal Directory	Yes	No	Yes	PS03	-	-	Yes	Yes	No	-	Warning	Warning
	Limit access to ArcGIS Server Admin Resources via Web Adaptor	Yes	No	Yes	-	-	-	N/A	N/A	N/A	N/A	Warning	Warning
	Understand Dynamic Workspace usage	Yes	Yes	Yes	-	SS09	-	No	No	No	-	Warning	Warning
	Secure System Services	Yes	Yes	Yes (4)	-	SS06	-	Yes	Yes	No	-	Danger	Danger
Standardized Filtering													
	Enforce Standardized Queries	Yes	Yes	Yes	-	SS02	Yes	Yes	Yes	Yes	Yes	Danger	Danger
	Filter Web Content Enabled	Yes	Yes	Yes	-	SS05	-	Yes	Yes	No	-	Danger	Danger
Authentication and Authorization													
	Utilize Enterprise Logins via SAML instead of Built-in	No	No	Yes	-	-	Yes	No	No	Yes	Yes	Warning	Warning
	Block members joining org with social network credentials	No	No	No	-	-	Yes	Yes	No	Yes	Yes	Warning	Warning
	Define a password Complexity Policy	Yes	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Warning	Danger
	Use Organinization Specific user store with account lockout policy	Yes	Yes	Yes	-	-	-	Yes	Yes	Yes	-	Warning	Warning
	Configure a shorter token Expiration Period	Yes	Yes	Yes	-	-	-	Yes	Yes	Yes	-	Warning	Warning
	Configure Multi-factor Authentication	Yes (5)	No	Yes	-	-	Yes	Yes	No	Yes	Yes	Danger	Danger
	Disallow user account self-creation	Yes	Yes	Yes	PS05	-	-	Yes	Yes	Yes	-	Warning	Danger
	Define Custom Roles	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Warning	Warning
	Disable Anonymous Access to Portal home app	Yes	No	Yes	PS06	-	Yes	Yes	No	Yes	Yes	Danger	Warning
	Configure role based access control	Yes	Yes	Yes	-	-	-	Yes	Yes	Yes	-	Danger	Danger
	Disable Primary Site Administrator account (ArcGIS Server)	Yes	No	Yes	-	SS11	-	N/A	N/A	N/A	N/A	Warning	Warning
	Disable Initial Admin Account (Portal for ArcGIS)	Yes	No	Yes	-	-	-	N/A	N/A	N/A	N/A	Warning	Warning
	Disallow token generation in via GET	Yes	Yes	Yes	PS02	SS03	-	Yes	Yes	No	-	Danger	Danger
	Disallow token generation w/ creds in query parameter via POST	Yes	Yes	Yes	PS02	SS04	-	Yes	Yes	No	-	Danger	Danger
	SAML: Check if encrypted assertions and signed requests are enabled	Yes	No	Yes	PS13 (6)	-	-	Yes	No	Yes	-	Danger	Danger
ArcGIS Enterprise Web Tier Technologies													
	Use a WAF/Web Filter	No	No	Yes	-	-	-	Yes	Yes	No	-	Warning	Warning
	Utilize load balancer instead of Web Adaptor	No	No	Yes	-	-	-	Yes	Yes	No	-	Info	Warning
	Web Adaptor utilized for IWA only inside organization	Yes	Yes	Yes	-	-	-	No	No	No	-	Info	Info
	Remove Technology identifiers and banners	Yes	Yes	Yes (7)	-	-	-	Yes	Yes	No	-	Info	Info
	Use Data Loss Prevention (DLP)	No	No	Yes	-	-	-	Yes	-	-	-	Warning	Warning
Data Ownership & Privacy													
	Prevent users from sharing publicly	Yes	Yes	Yes	PS12	-	Yes	Yes	Yes	Yes	Yes	Warning	Warning
	Disallow biography edits and visibile profiles	Yes	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Warning	Info
	Limit search to your organization only	Yes	Yes	Yes	-	-	Yes	Yes	No	Yes	Yes	Info	Info
	Remove social media links in item details/group pages	Yes	Yes	Yes	-	-	Yes	Yes	Yes	Yes	Yes	Warning	Info
	Do not allow members of other organizations to sign in	No	No	No	-	-	-	Yes	No	Yes	-	Warning	Warning
	Define specific allowed Portals that your Portal may access	Yes	No	Yes	-	-	-	Yes	No	Yes	Yes	Warning	Warning
	Validate Distributed Collaborations	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Warning	Danger
	Disable Esri User Experience Improvement Program (EUEI)	No	No	No	-	-	-	Yes	No	Yes	Yes	Warning	Info
	Identify Authoritative Content (8)	No	No	No	-	-	-	Yes	No	Yes	-	Warning	Info
	Configure Access Notice	Yes	No	Yes	-	-	-	Yes	No	Yes	-	Info	Warning
	[illegible] Shared as portal item	Yes	[illegible]				-					Info	[illegible]

Monitor and Validate

Monitor and Validate



Dear Esri,

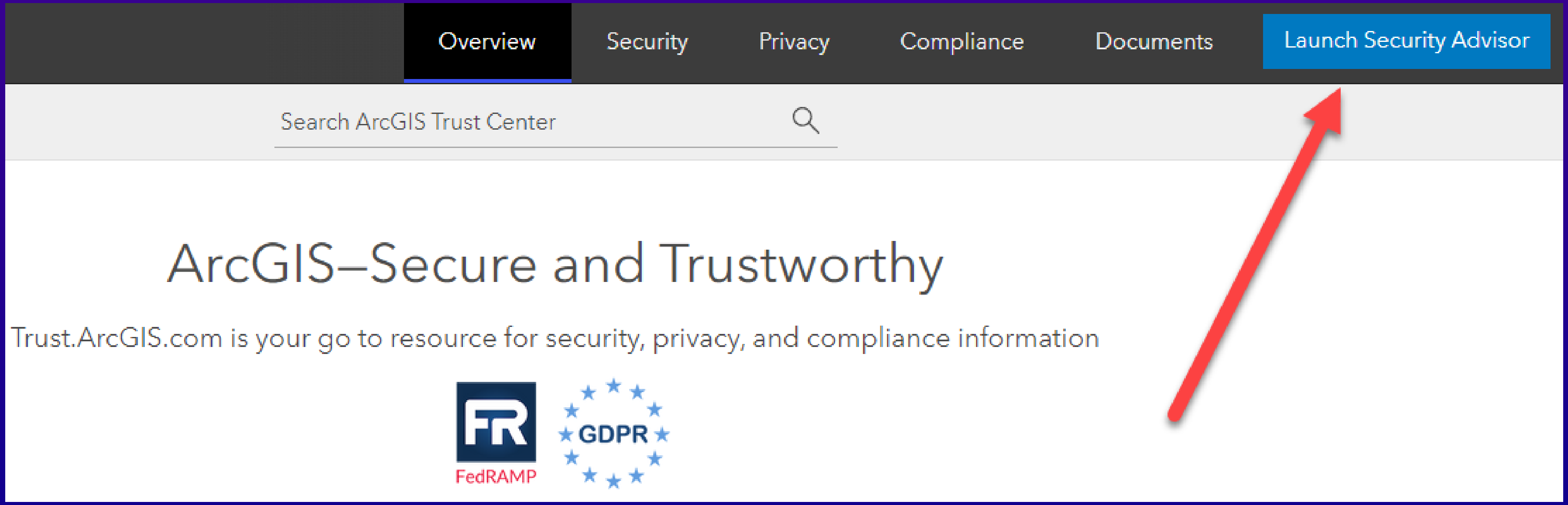
It would be super cool if you had a tool that can tell me if I might have Privacy leaks.

Love,

Users ❤

ArcGIS Security and Privacy Advisor!

- Link from ArcGIS Trust Center
- Supports ArcGIS Online and ArcGIS Enterprise
- Proactively discover potential security and privacy issues
- Prevent configuration drift

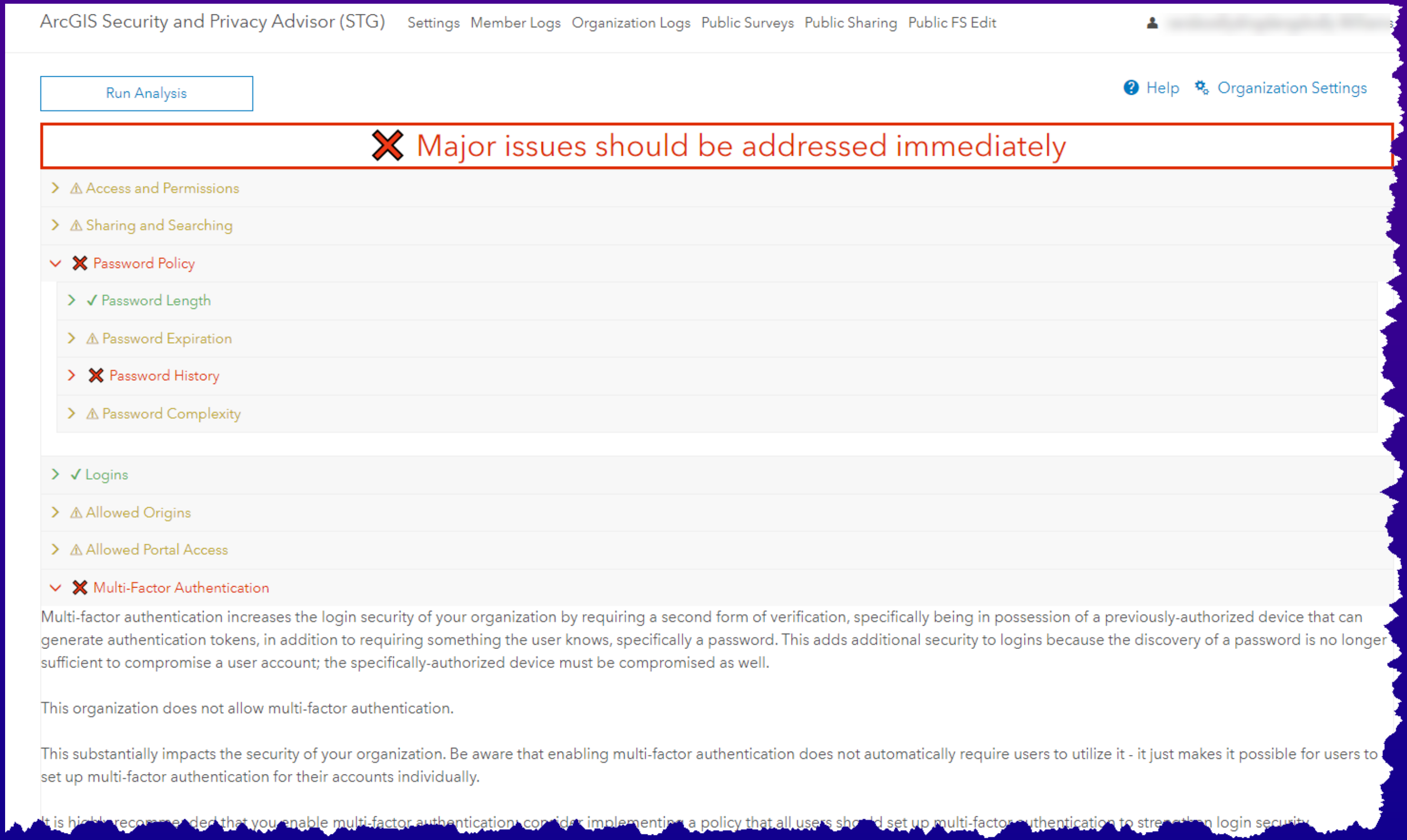


ArcGIS–Secure and Trustworthy

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

ArcGIS Security and Privacy Advisor!

- Validate:
  - Settings
  - Survey Result Visibility
  - Public Items
  - Public Edit capabilities



ArcGIS Security and Privacy Advisor (STG) Settings Member Logs Organization Logs Public Surveys Public Sharing Public FS Edit [redacted]

Run Analysis

Help Organization Settings

❌ Major issues should be addressed immediately

- ⚠ Access and Permissions
- ⚠ Sharing and Searching
- ❌ Password Policy
  - ✓ Password Length
  - ⚠ Password Expiration
  - ❌ Password History
  - ⚠ Password Complexity
- ✓ Logins
- ⚠ Allowed Origins
- ⚠ Allowed Portal Access
- ❌ Multi-Factor Authentication

Multi-factor authentication increases the login security of your organization by requiring a second form of verification, specifically being in possession of a previously-authorized device that can generate authentication tokens, in addition to requiring something the user knows, specifically a password. This adds additional security to logins because the discovery of a password is no longer sufficient to compromise a user account; the specifically-authorized device must be compromised as well.

This organization does not allow multi-factor authentication.

This substantially impacts the security of your organization. Be aware that enabling multi-factor authentication does not automatically require users to utilize it - it just makes it possible for users to set up multi-factor authentication for their accounts individually.

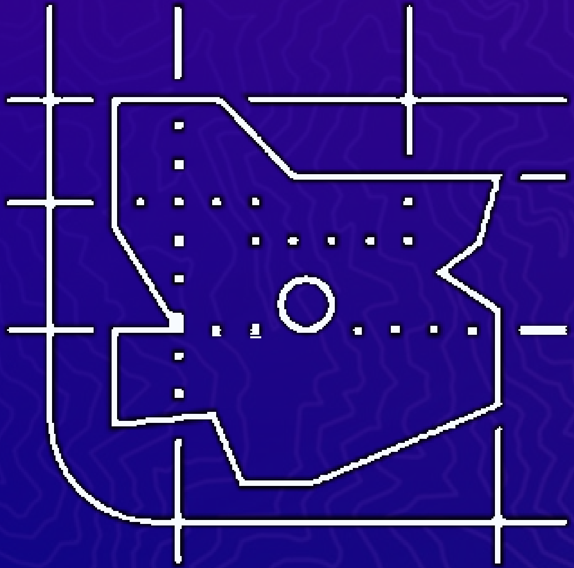
It is highly recommended that you enable multi-factor authentication, consider implementing a policy that all users should set up multi-factor authentication to strengthen login security.

Processes & Pipelines To Govern Information Delivery

Real Risks the Wild

Privacy Leaks: School Bus Stop Geocoding/Routing

#1 Reported Privacy issue to Esri PSIRT – STUDENT PII/PHI



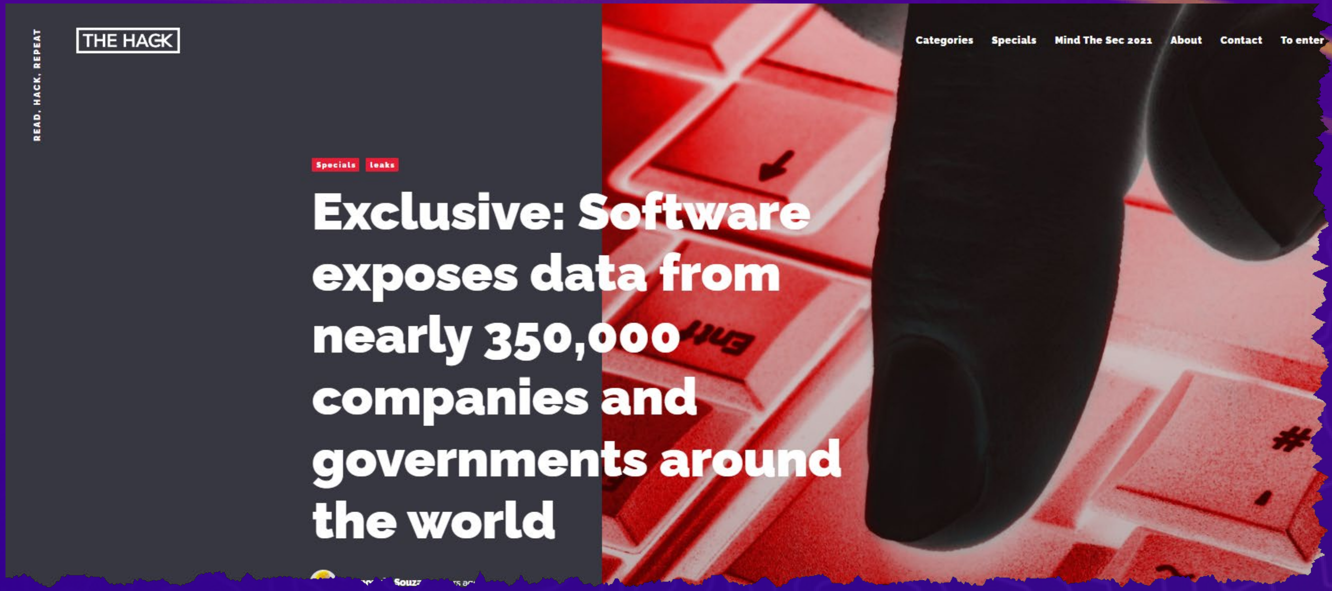
Real Risks the Wild

Privacy Leaks: Public Survey Results…

…Misconfigured Surveys?

Proprietary Data Sets: Public Sharing…

…Contractors?



Exclusive: Software exposes data from nearly 350,000 companies and governments around the world

Souza

Product Improvements Implemented!
Technical Documents Written!

WHAT'S MISSING…?

Customer Responsibilities

Processes

- Establish a content Publication Review Board
  - Review content before publication
  - Regularly review content after
  - Disable the ability for users to share publicly
- Classify your datasets and secure them appropriately
  - Leverage groups to bucket datasets
- Use custom roles to granularly define permissions
  - Don’t use ADMIN as daily driver

PROCESSES

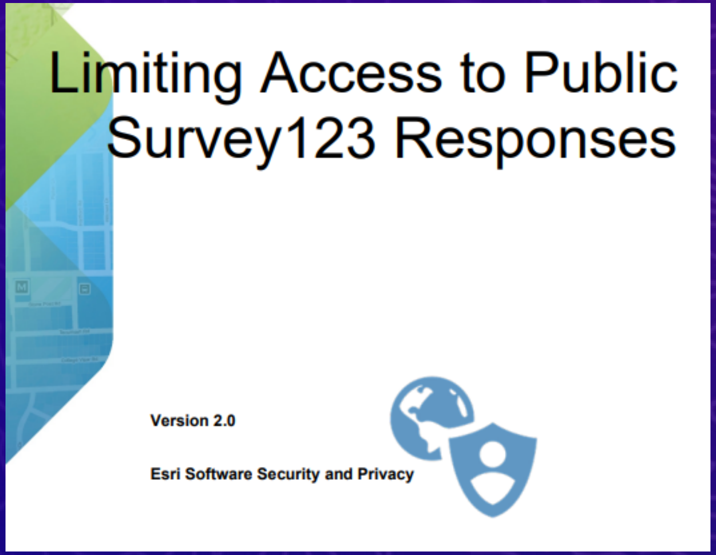
Customer Responsibilities

Processes

- **REVIEW ALL CONTENT PRIOR TO SHARING TO “EVERYONE”**
- Enable and use Multi Factor Authentication
- Leverage Hosted Feature Service Views
- Filter sensitive content
- Delete sensitive columns before publishing (as feasible)
  - POP UP FILTERING is NOT ENOUGH!
    - (Client-Side filtering does NOT prevent direct queries to web service)

PROCESSES

Technical Papers in ArcGIS Trust Center



Limiting Access to Public Survey123 Responses

Version 2.0

Esri Software Security and Privacy

esri®

THE
SCIENCE
OF
WHERE®