

Designing a Web GIS Security Strategy

Michael Young – CISO - Products

Matt Lorrain – Security Architect

Agenda

- **Introduction**
- **Trends**
- **Strategy**
- **Mechanisms**
- **Server**
- **Mobile**
- **Cloud**
- **Compliance**

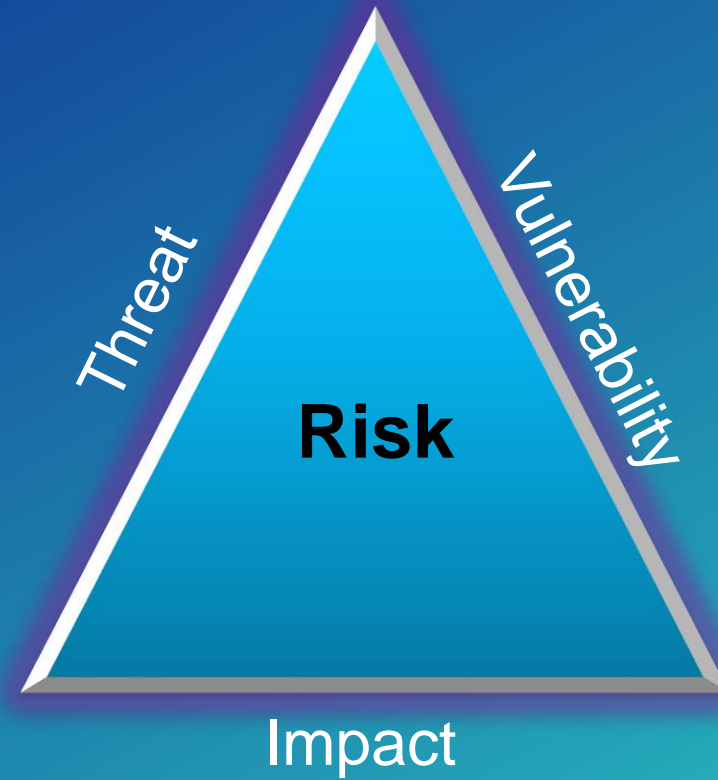
Introduction

What is a secure GIS?



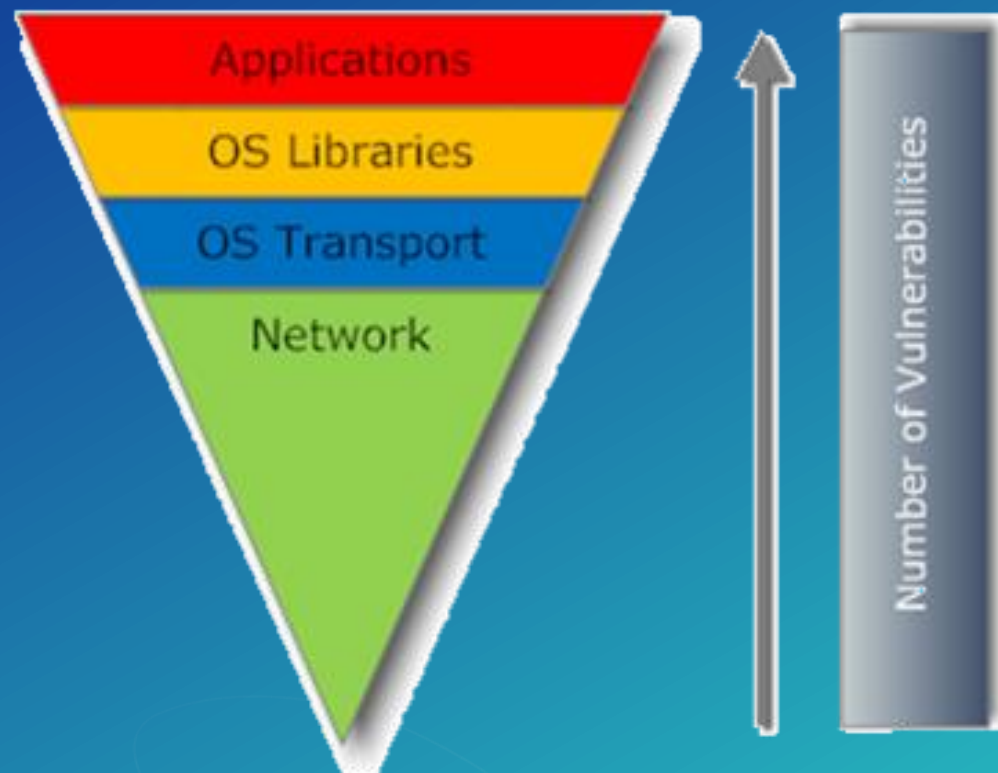
Introduction

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: Who and How?



Who's behind the breaches?

75%

perpetrated by outsiders.

25%

involved internal actors.

18%

conducted by state-affiliated actors.

3%

featured multiple parties.

2%

involved partners.

51%

involved organized criminal groups.



What tactics do they use?

62%

of breaches featured hacking.

51%

over half of breaches included malware.

81%

of hacking-related breaches leveraged either stolen and/or weak passwords.

43%

were social attacks.

14%

Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

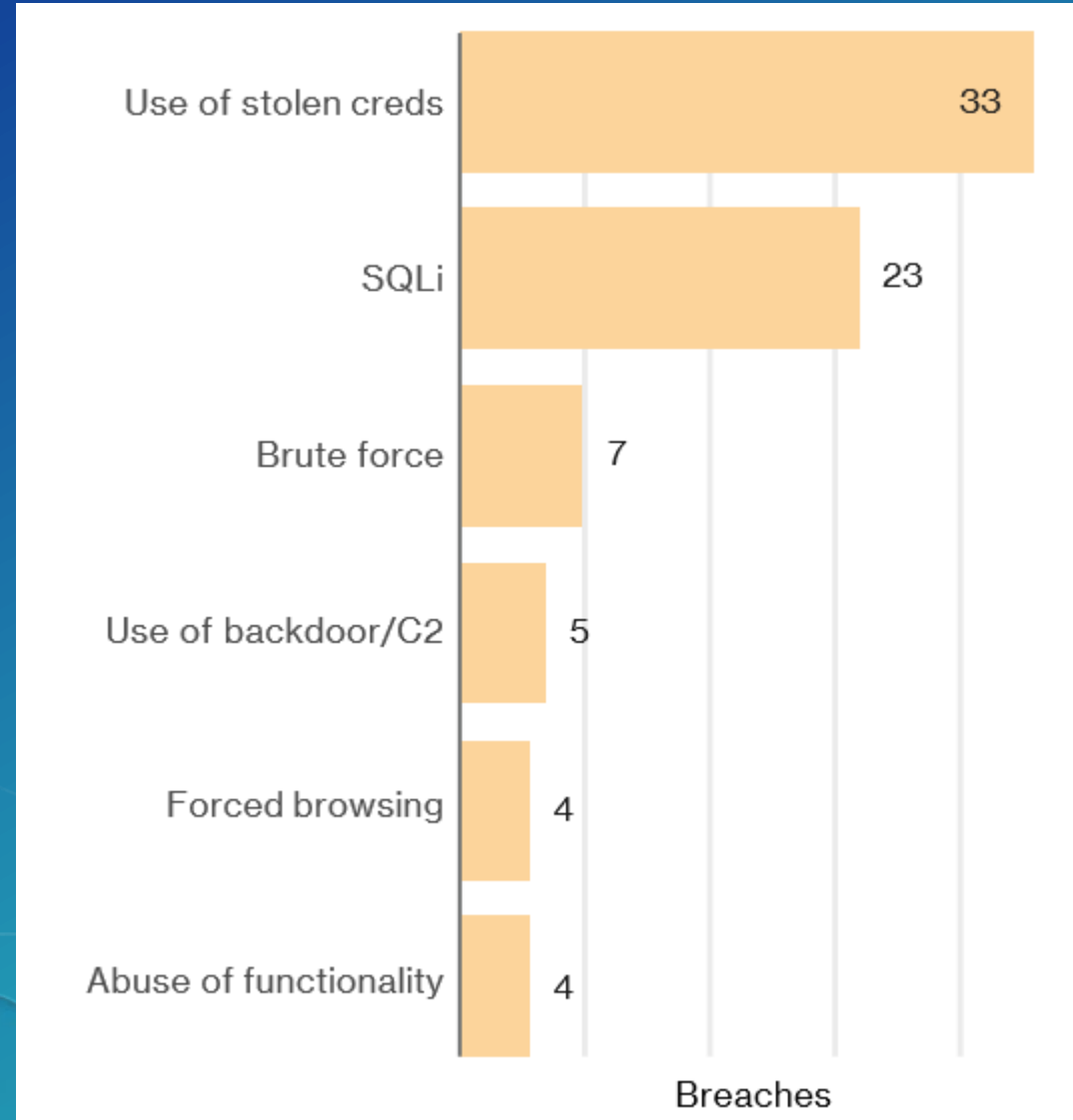
8%

Physical actions were present in 8% of breaches.

Trends

For Web Applications Attacks specifically....

- Password based authentication is **STILL** broken
 - Use 2-factor
- Validate inputs
 - Standardized queries
- Patching process
 - 3rd party components as well as OS



Trends

Trends by Industry

*Verizon 2017 DBIR

Pattern		Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail
	Denial of Service	4	228	445	3	508	10	617	180
	Privilege Misuse	5	7	48	125	23	13	7,417	9
	Lost and Stolen Assets	5	13	10	92	4	2	5,519	4
	Everything Else	8	106	20	40	32	213	88	8
	Point of Sale	182		3	4	1			9
	Miscellaneous Errors	2	24	14	114	13	3	2,246	16
	Web App Attacks	4	25	376	32	73	4	148	28
	Crimeware	5	32	30	54	63	261	5,102	14
	Payment Card Skimmers	6		53			1	1	57
	Cyber-Espionage		22	5	2	4	115	112	3

Incidents

	Accommodation	Education	Finance	Healthcare	Information	Manufacturing	Public	Retail
				1	2		1	
	5	5	26	104	13	8	58	6
	4	3	2	42	2	1	7	
	8	14	16	28	24	4	19	3
	180		3	3				8
	1	16	10	96	9	2	38	12
	3	11	364	15	61		13	24
		5	7	12	1	2	5	1
	5		44				1	39
		19	5	1	4	108	98	1

Breaches

Real-world security scenarios

Disaster communications modified

- **Scenario**

- Organization utilizes cloud based services for disseminating disaster communications
- Required easy updates from home and at work
- Drove allowing 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 service access

Lack of strong governance leads to unexpected consequences

Real-world security scenarios

Vulnerabilities makes organizations Wanna Cry...

Petya ransomware: Companies count the cost of massive cyber attack

Health and hygiene firm Reckitt Benckiser warns ransomware attack could cost it £100m in revenue.



By [Danny Palmer](#) | July 6, 2017 -- 11:59 GMT (12:59 BST) | Topic: Security

- **Scenario**

- Ransomware infected over 230,000 endpoints within 1 day of being released across 150 countries
- Propagated by exploiting Windows Server Message Block (SMB) protocol and Phishing
- Microsoft had released a security update months earlier that could prevent infection
- Ransomware variances continue to be released

- **Lessons learned**

- Patching processes vital for both OS and applications
- User security awareness training and rigorous publication processes
- Disable services if not utilized
- Paying ransom does not pay off (Petya victims unable to recover data after payment)

Real-World Security Scenarios

QUIZ – When was the last ArcGIS Security patch released?

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

The screenshot displays the Trust.ArcGIS.com website. The header includes the 'Trust ArcGIS' logo and a 'Check System Status' button. A navigation bar contains links for 'Trust', 'ArcGIS Online Status', 'Security', 'Privacy', and 'Compliance'. The main content area features the heading 'ArcGIS—The secure and trustworthy location platform' and the text 'Trust.ArcGIS.com is your go to re'. Below this, there are logos for 'FedRAMP' and 'FISMA'. A prominent article titled 'ArcGIS Server and Portal Security 2017 Patches Released' by Michael Young, dated January 17, 2017, is shown. The article includes an icon of a blue arrow pointing to an open padlock and the text: 'The first set of security patches for ArcGIS Server and Portal for ArcGIS in 2017 were just released. We recommend our customers apply these patches in a timely manner. To be clear, there are separate security patches for ArcGIS Server and ... Continue reading →'. At the bottom of the article snippet, it says 'Posted in Security | Tagged Patch, SSAMYMLGP, Update | 2 Comments'.

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

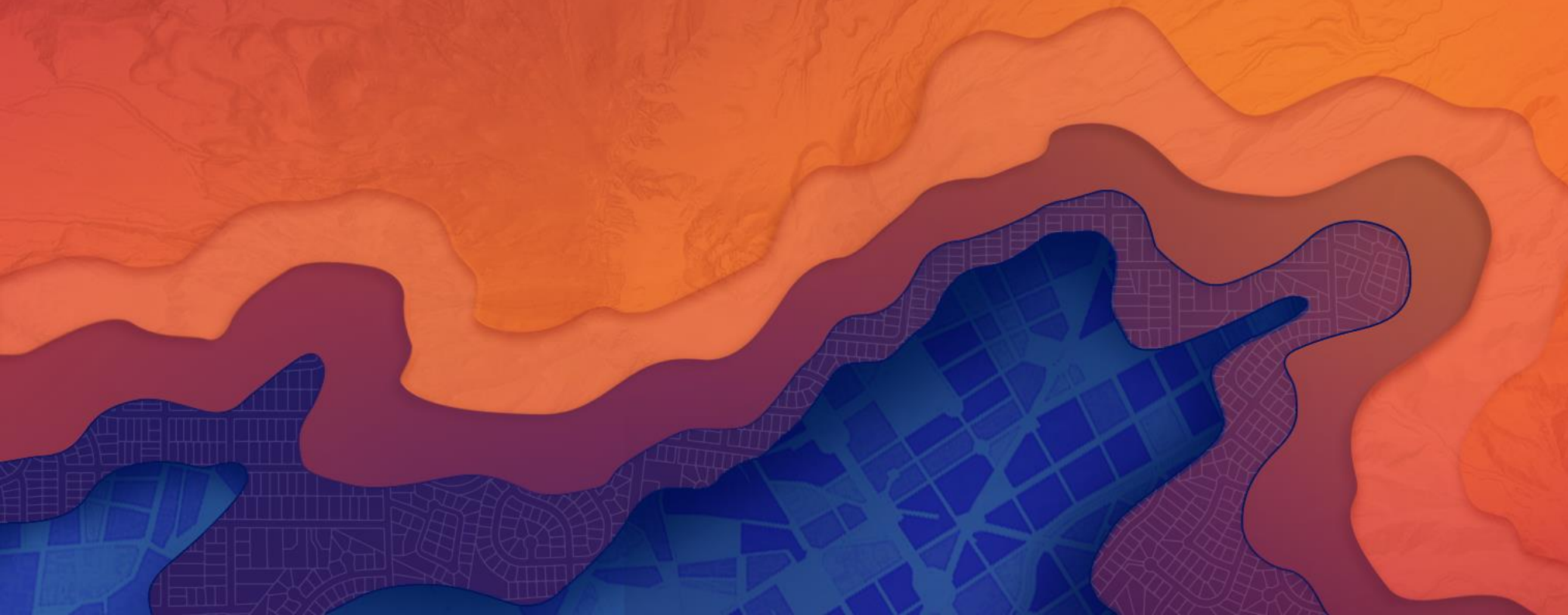
Trends

Strategic Shifts in Security Priorities for 2017 and Beyond

- Ransomware is rampant
 - Backup systems and patch systems/software in a timely manner
- Previously secretly managed hacking toolset dumps made widely available
- Enormous user password dumps now commonplace
 - Stronger mechanisms required such as 2-factor auth / Utilize enterprise password management solutions
- Guidance for password complexity / management changing – NIST 800-63B
- GDPR deadline in 2018 advancing privacy assurance and base security controls
- Cloud Access Security Broker (CASB) usage expanding for encryption management
- Smart cities threatened by IoT issues
- Mobile security threats increasing quickly (4% infected with malware)
- Cyberespionage continues to increase along with political hacking and propagating disinformation
- Machine learning becoming more critical for simplifying security view across enterprise
- Social media increasing used to provide more precise/convincing phishing e-mails
- Utilization of named users provides more granular tracking of geospatial information

Strategy

Michael Young



Strategy

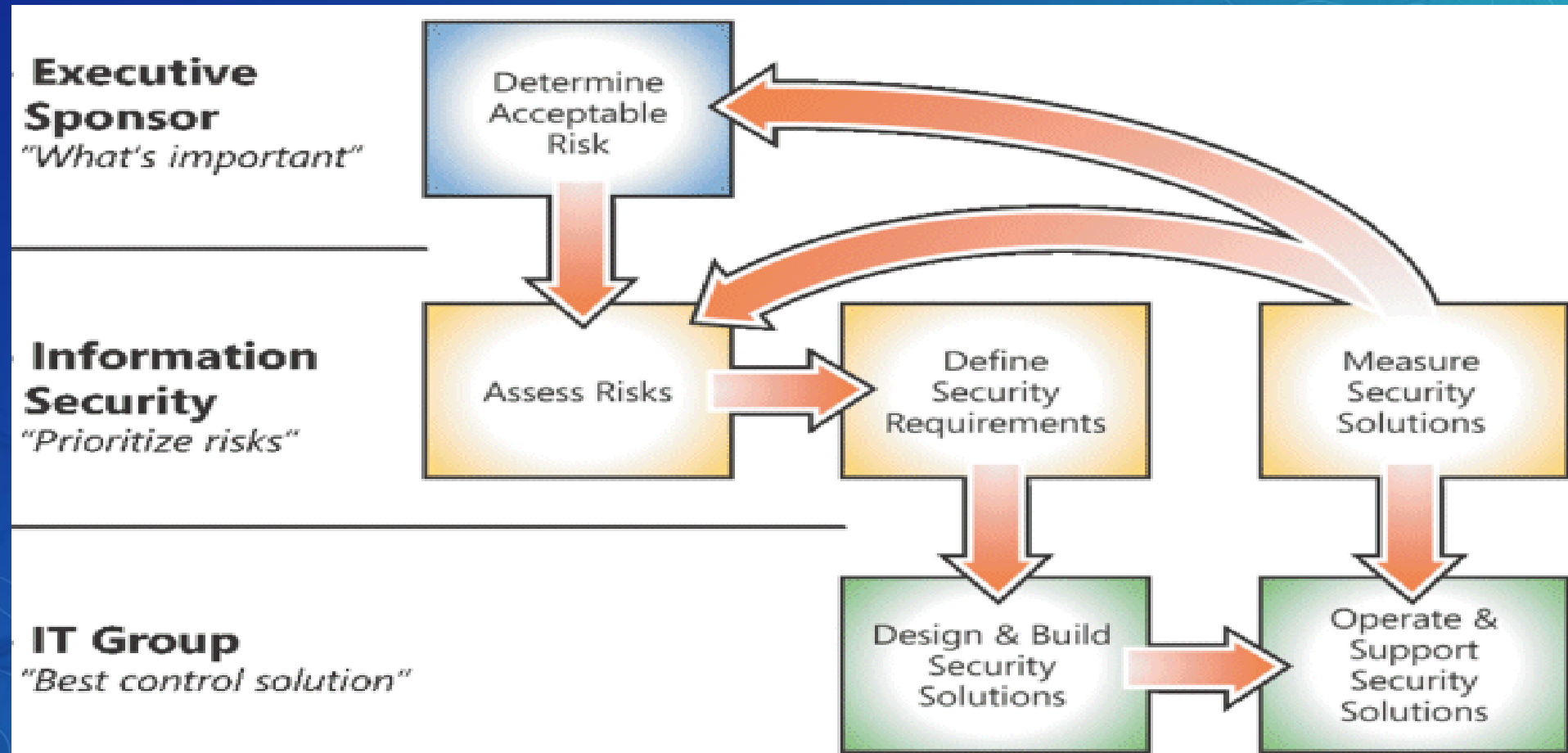
A better answer

- **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

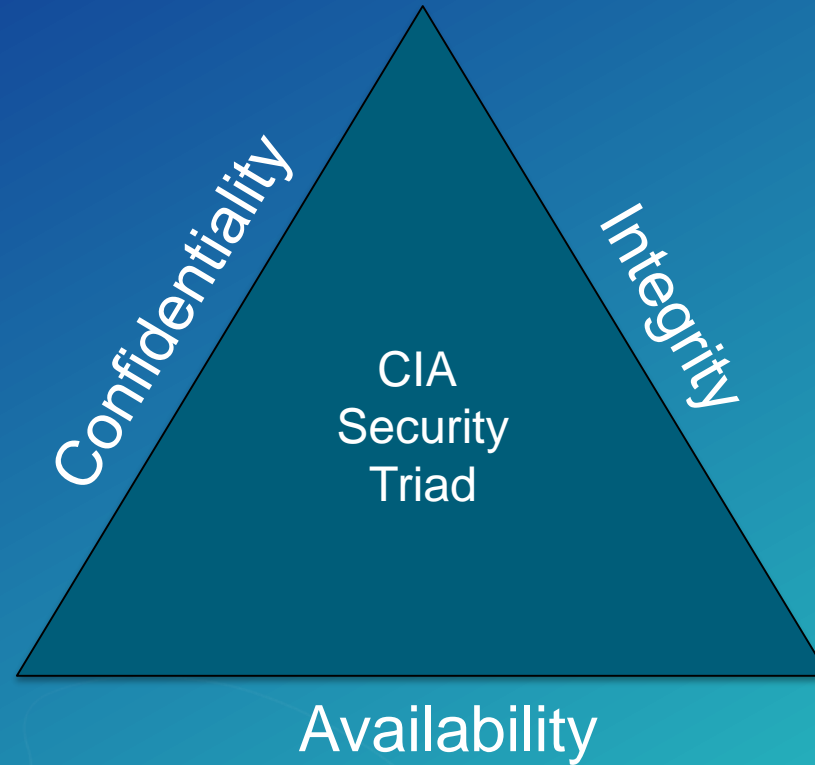
Enterprise GIS Security Strategy



Security Risk Management Process Diagram - Microsoft

Strategy

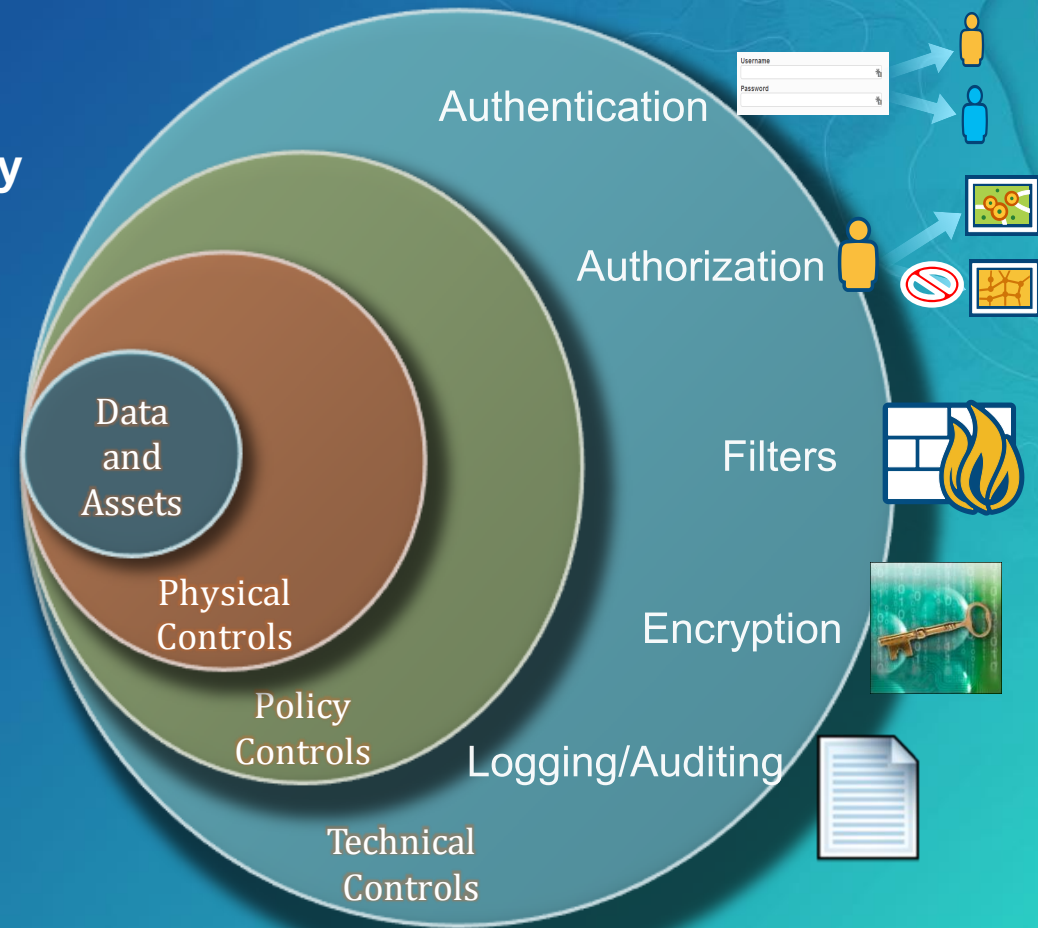
Security Principles



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

Matt Lorrain



Mechanisms



Authentication



Authorization



Filters



Encryption



Logging/Auditing

Mechanisms

Users & Authentication



Authentication

- ArcGIS Token-Based Authentication
- Web-Tier Authentication
- SAML Authentication (Portal/ArcGIS Online)



User Store

- ArcGIS “Built-In” User Store
- Enterprise User Stores



Mechanisms

ArcGIS Token Based Authentication



ArcGIS Token-based Authentication

ArcGIS Online Options

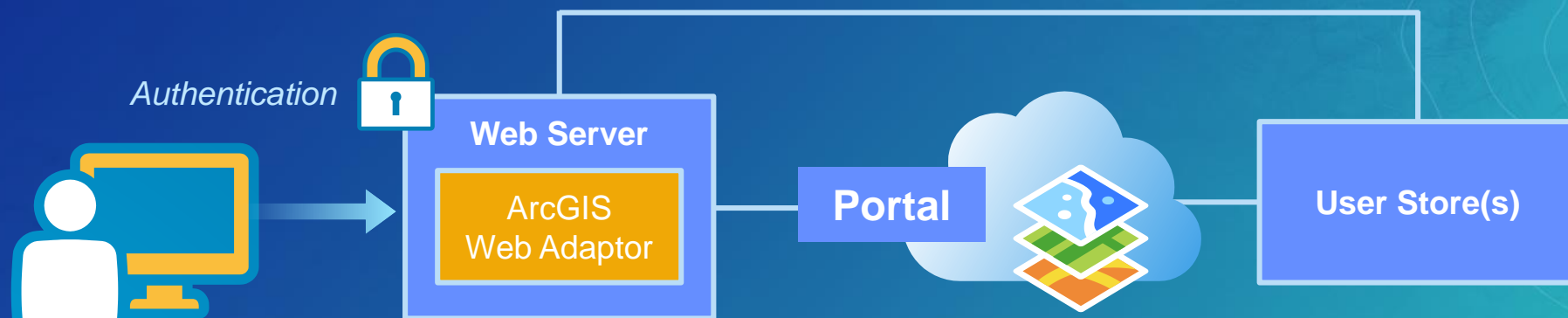
- Built-in User Store

ArcGIS Enterprise Options

- Built-in User Store
- Active Directory
- LDAP

Mechanisms

Web-Tier Authentication



Options Depend on Web Server...

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

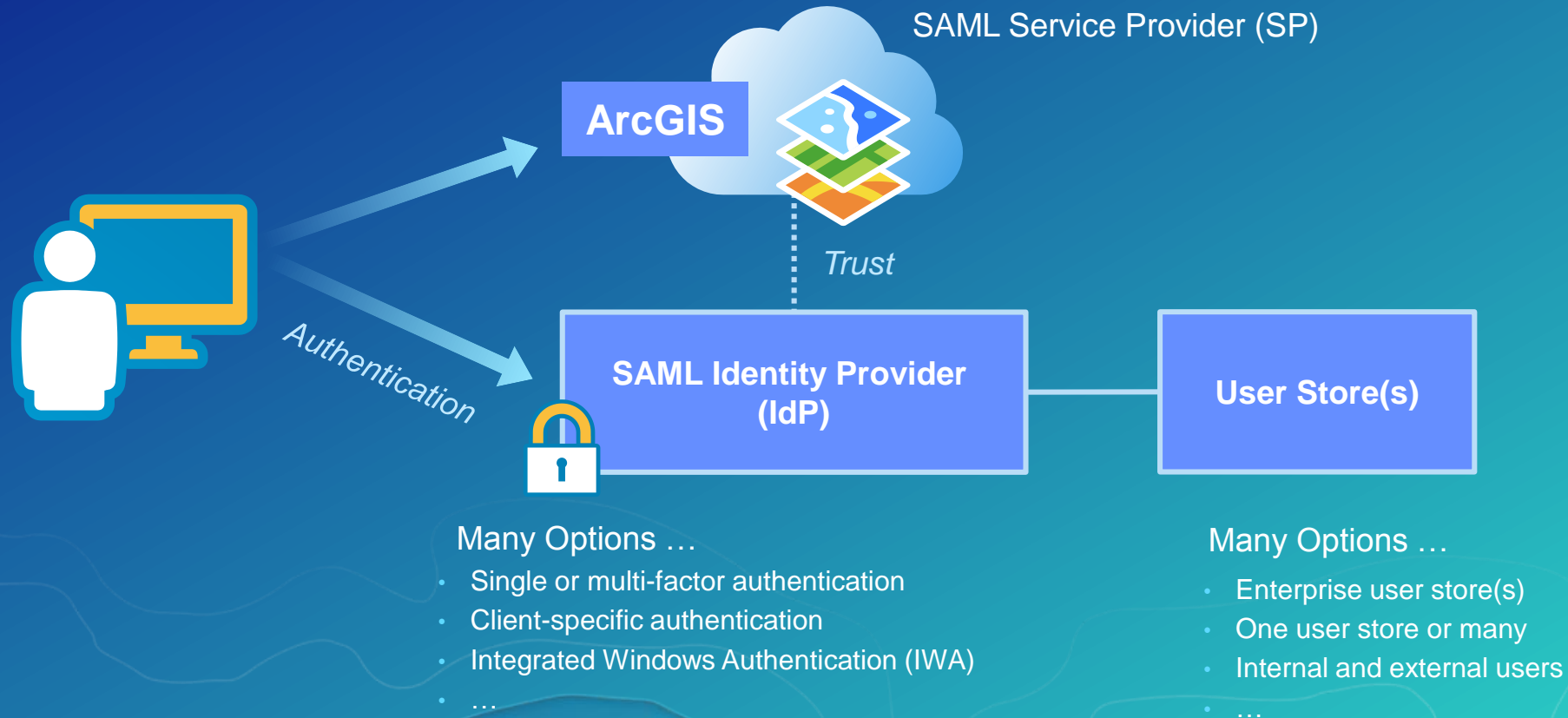
Options Depend on Web Server...

- Active Directory
- LDAP

Only supported using ArcGIS Enterprise...

Mechanisms

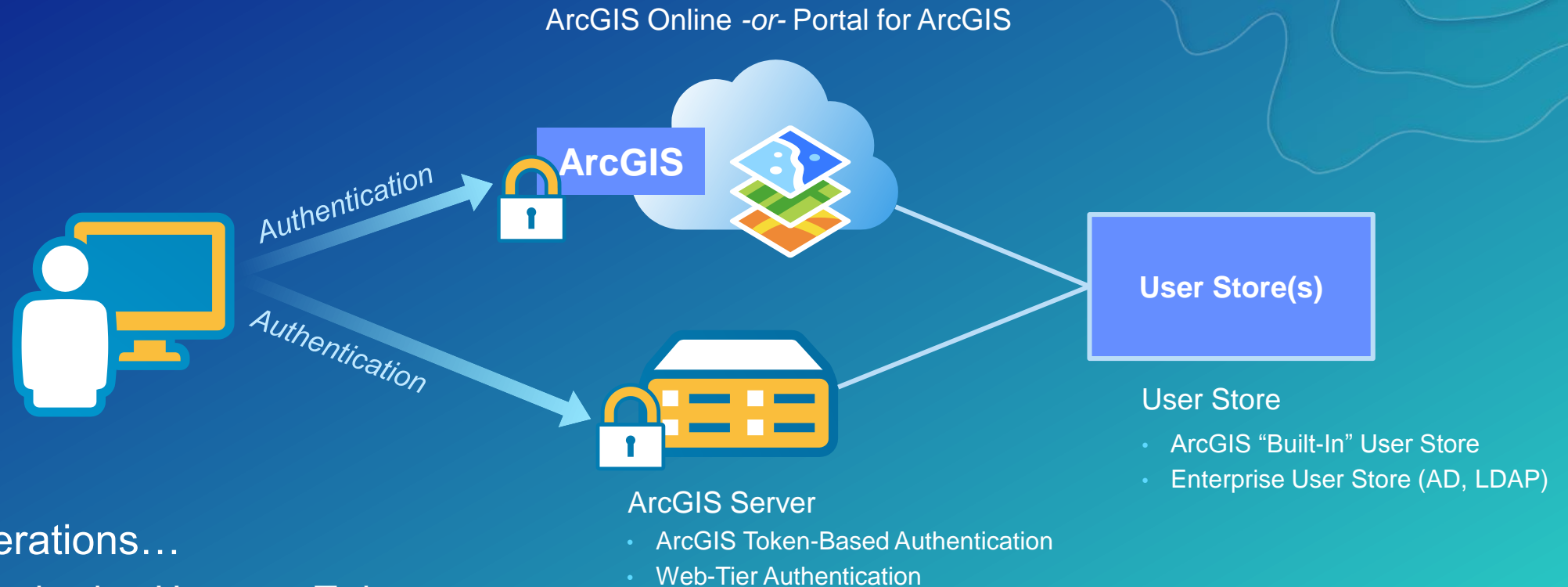
SAML Authentication



Provides flexibility and security capabilities depending on IdP...

Mechanisms

Authentication - What about ArcGIS Server?



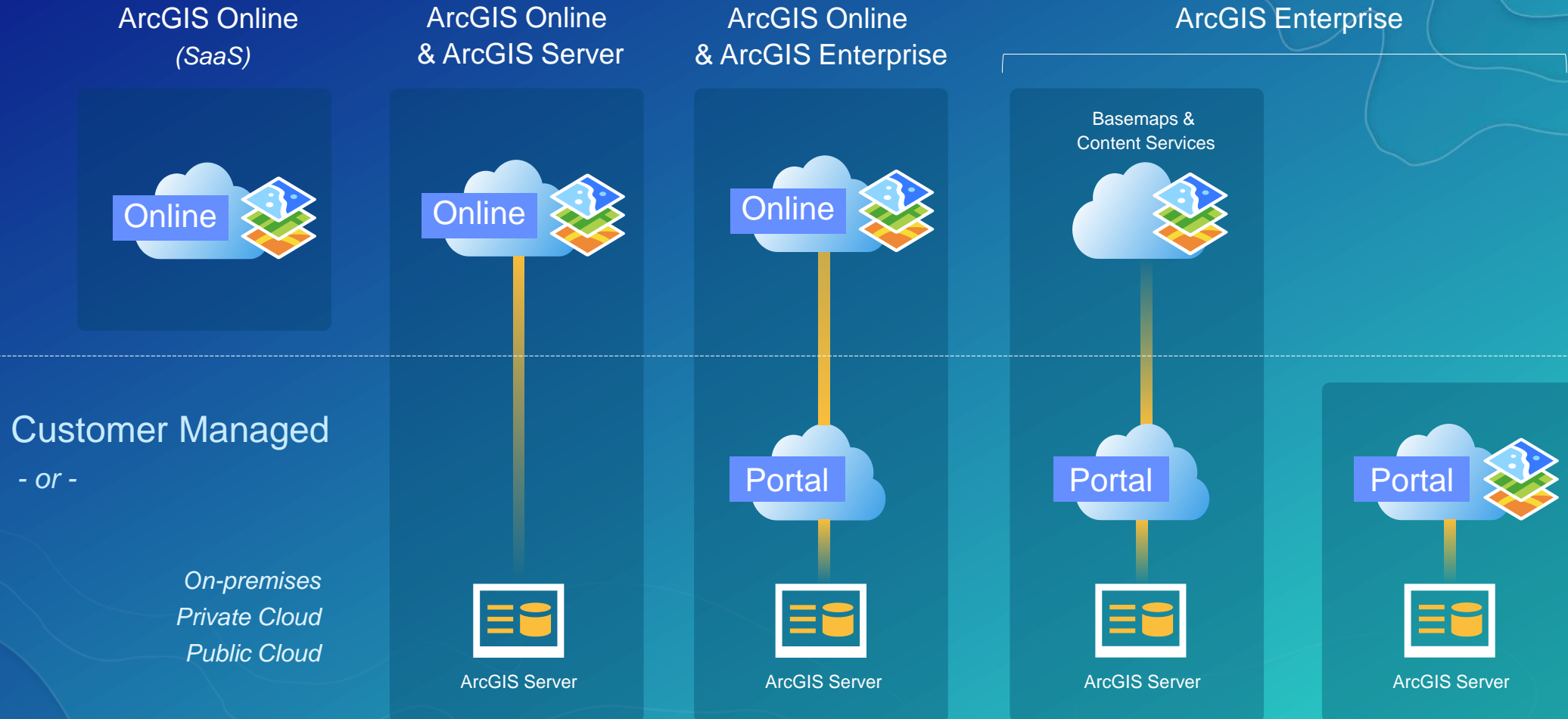
- Considerations...

- Authentication Happens Twice
- Cross-Origin Resource Sharing (CORS)
- ArcGIS “Trusted Servers”
- ArcGIS Server Federation

*This is a complex architecture topic with lots of nuance ...
... important for technical folks to understand*

Mechanisms

Authentication and Authorization – Which Option is best?



Mechanisms

Authorization – Role-Based Access Control

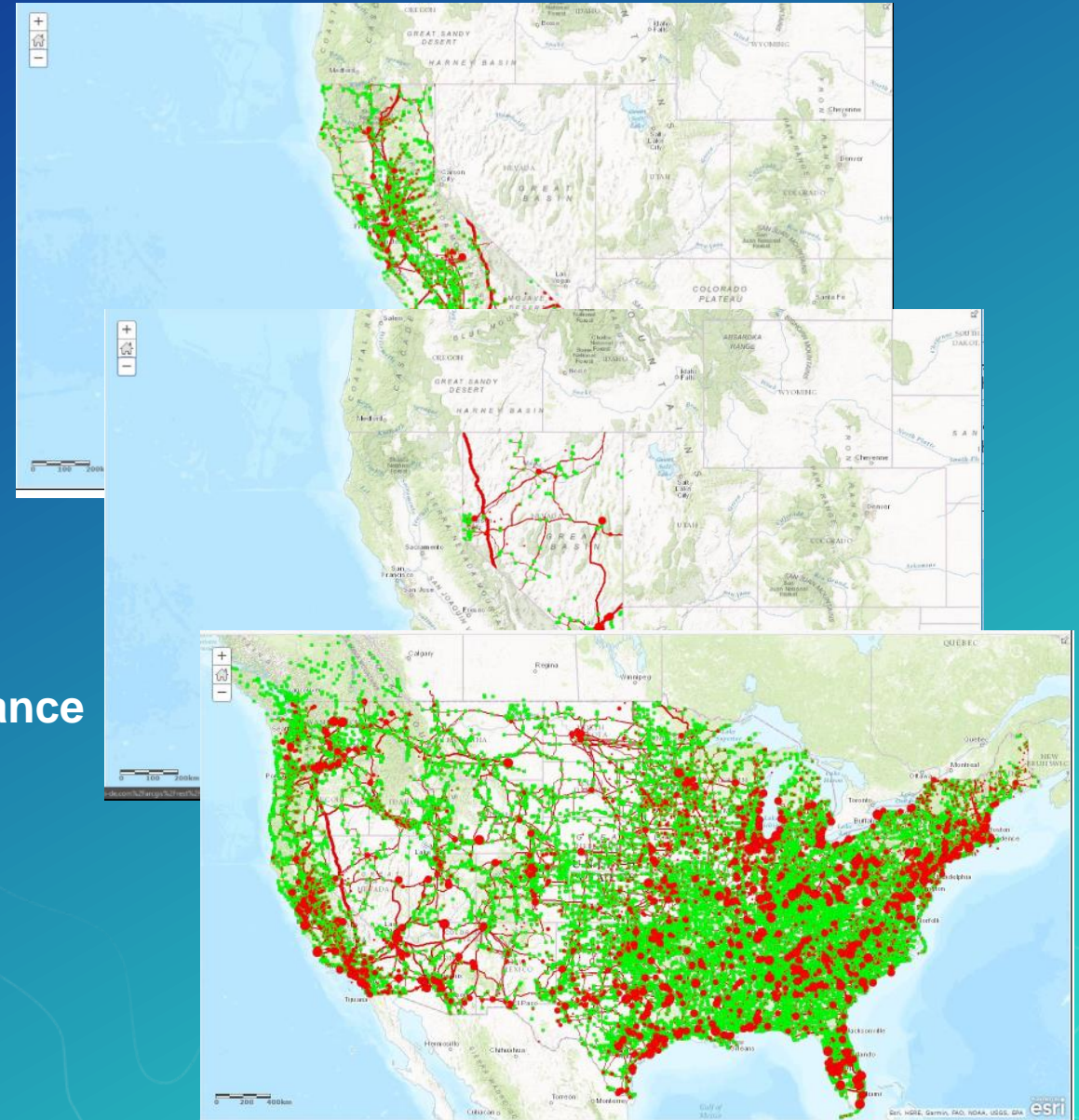
- **Out-of-box roles (level of permission)**
 - Administrators
 - Publishers
 - Users
 - Custom – Only for Portal for ArcGIS & ArcGIS Online
- **ArcGIS for Server – Web service authorization set by pub/admin**
 - Assign access with ArcGIS Manager
 - Service Level Authorization across web interfaces
 - Services grouped in folders utilizing inheritance
- **Portal for ArcGIS – Item authorization set by item owner**
 - Web Map – Layers secured independently
 - Packages & Data – Allow downloading
 - Application – Allows opening app



Mechanisms

Authorization – Extending with 3rd Party components

- Web services
 - Conterra's Security Manager (more granular)
 - Layer and attribute level security
- RDBMS
 - Row Level or Feature Class Level
 - Versioning with Row Level degrades performance
 - Alternative – SDE Views
- URL Based
 - Web Server filtering
 - Security application gateways and intercepts



Mechanisms

Filters – 3rd Party Options

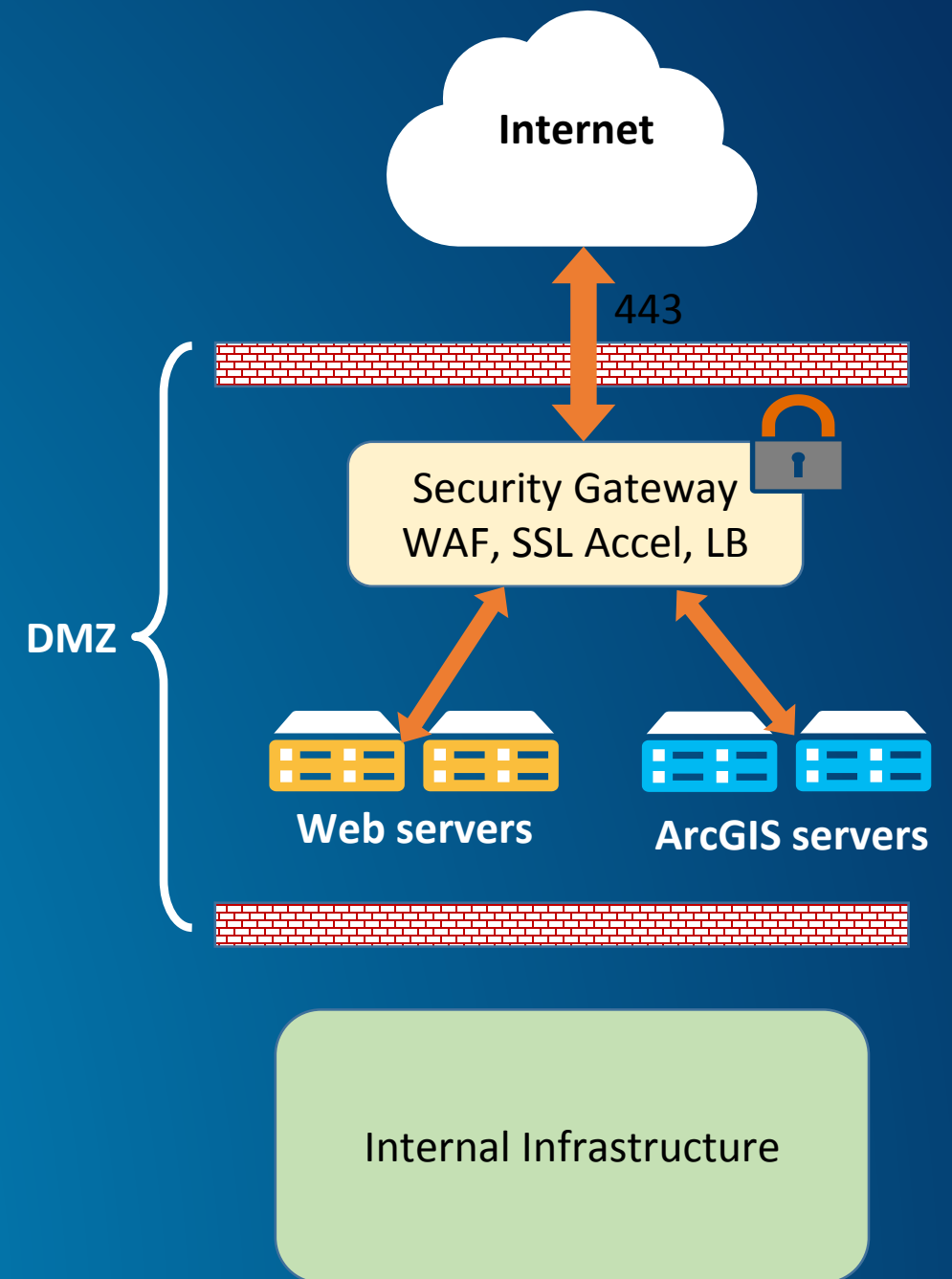
- **Firewalls**
 - Host-based
 - Network-based
- **Reverse Proxy**
- **Web Application Firewall**
 - Open Source option ModSecurity
- **Anti-Virus Software**
- **Intrusion Detection / Prevention Systems**
- **Limit applications able to access geodatabase**



Mechanisms

Filters - Web Application Firewall (WAF)

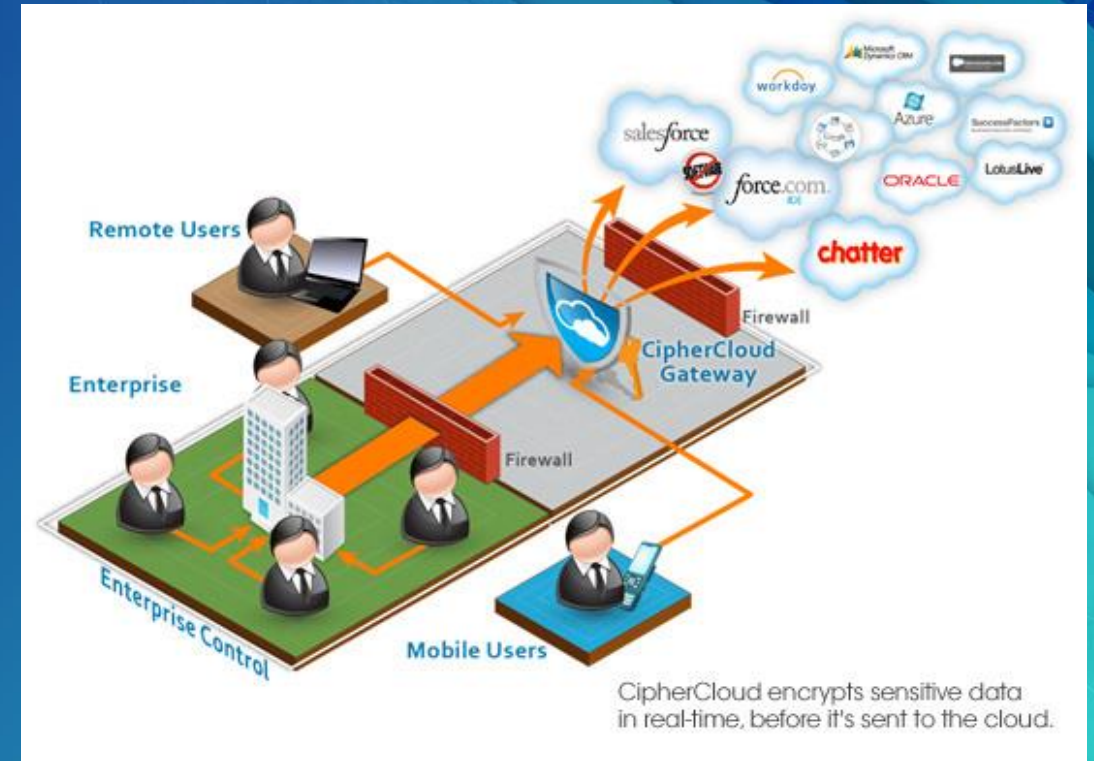
- Implemented in DMZ
- Protection from web-based attacks
- Monitors all incoming traffic at the application layer
- Protection for public facing applications
- Can be part of a security gateway
 - SSL Certificates
 - Load Balancer



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 Server logging
- System Monitor

3rd Party Options

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

Mechanisms

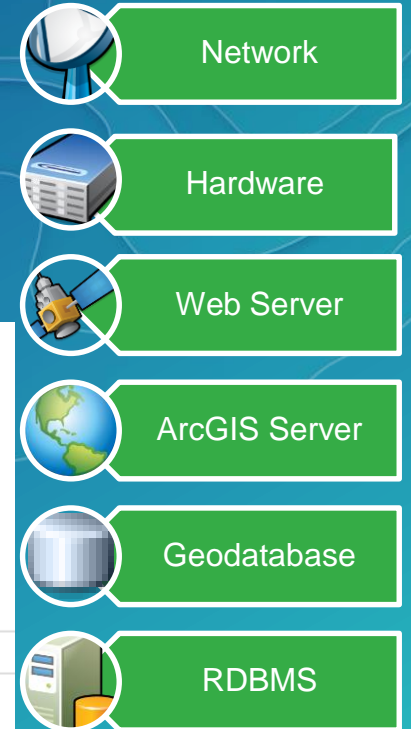
GIS monitoring with System Monitor

- **P**roactive
- **I**ntegrated
 - Dashboards across all tiers
- **E**nd-to-End
 - All tier monitoring
- **C**ontinuous
 - %Coverage provided
- **E**xtendable
 - Custom queries

Key Performance Indicators:

Hosts Process ArcGIS DB Http RDP

	% Coverage	% Uptime	% Alert
1	100.00	100.00	100.00
2	100.00	100.00	0.00
3	100.00	100.00	0.00
4	100.00	100.00	0.00
5	100.00	100.00	0.00
6	100.00	98.75	0.00



Web GIS

Matt Lorrain



Web GIS

ArcGIS Online or Portal?

ArcGIS Online

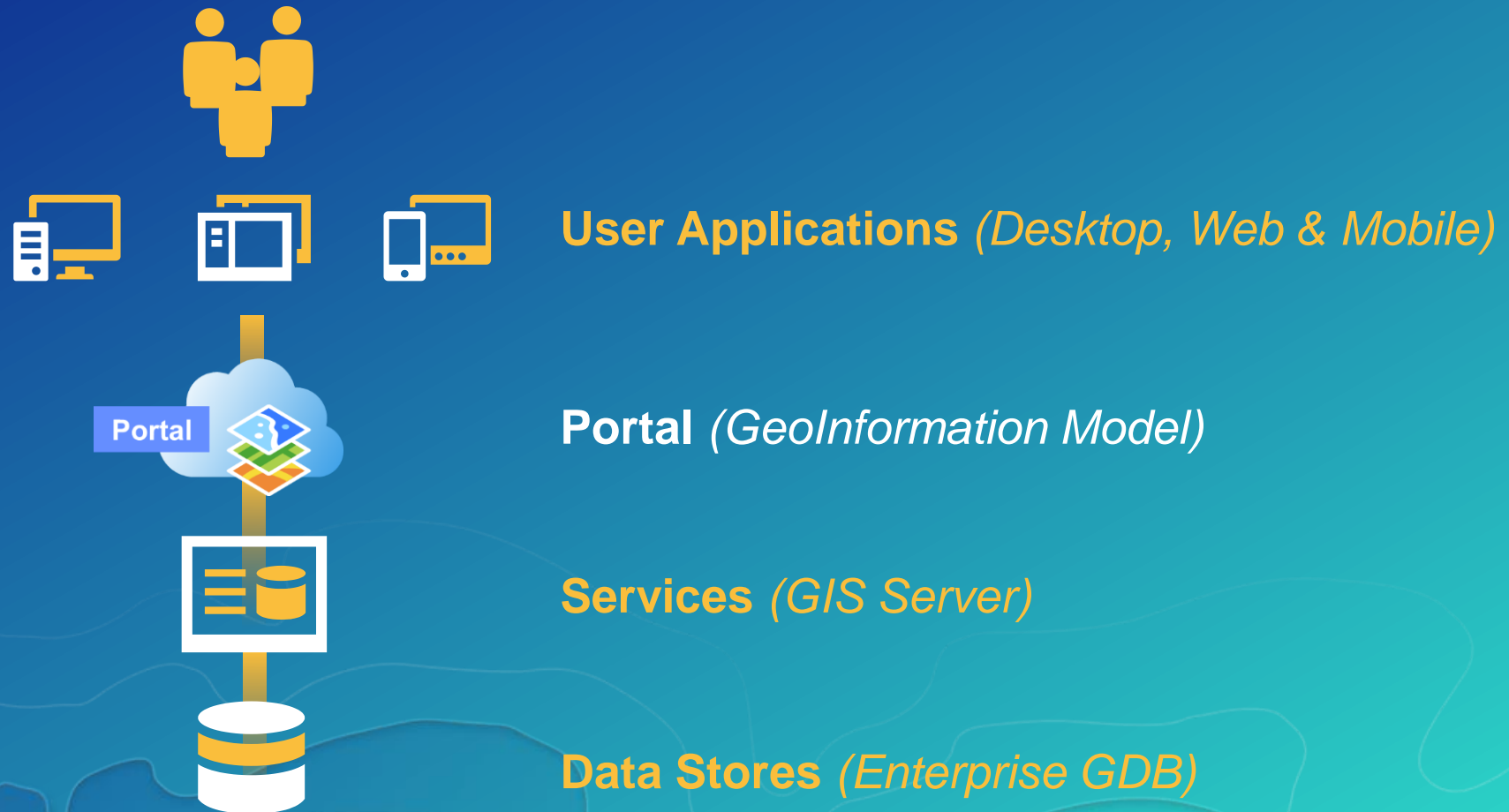
- SaaS
 - www.arcgis.com
 - Releases often
 - Upgraded automatically (*by Esri*)
 - Esri controls SLA
- Functionality (*smart mapping...*)
- Enterprise Integration
 - Web SSO via SAML

Portal for ArcGIS

- Software
 - Part of ArcGIS Server
 - Releases 1-2 times per year
 - Upgraded manually (*by organization*)
 - Organization controls SLA
- Functionality (*smart mapping...*)
- Enterprise Integration
 - Web SSO via SAML
 - Web-tier Authentication via Web Adaptor
 - Enterprise Groups
 - ArcGIS Server Integration...

Web GIS

Anatomy of a Web GIS

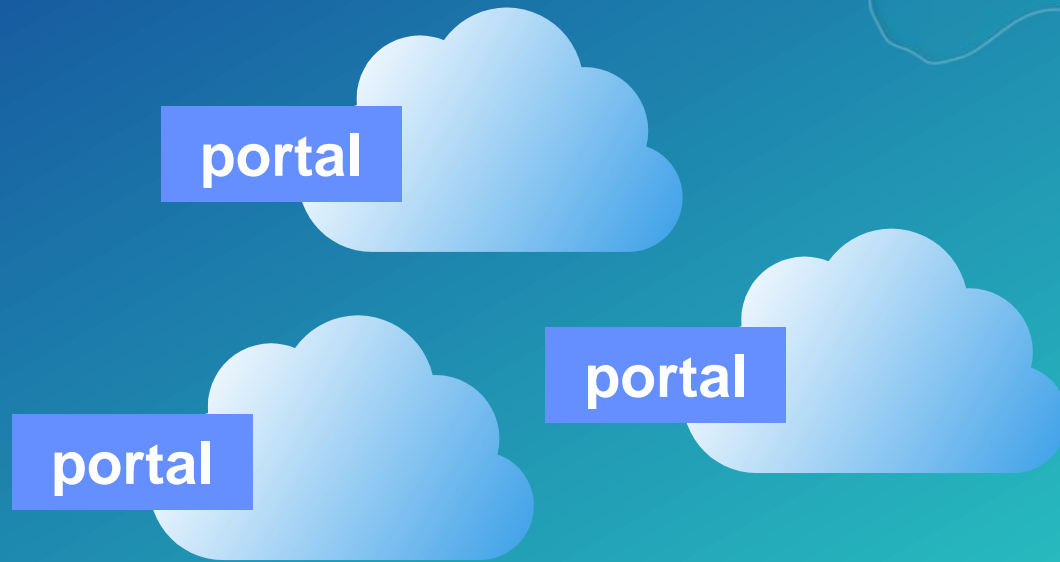


Web GIS

Multiple Portals



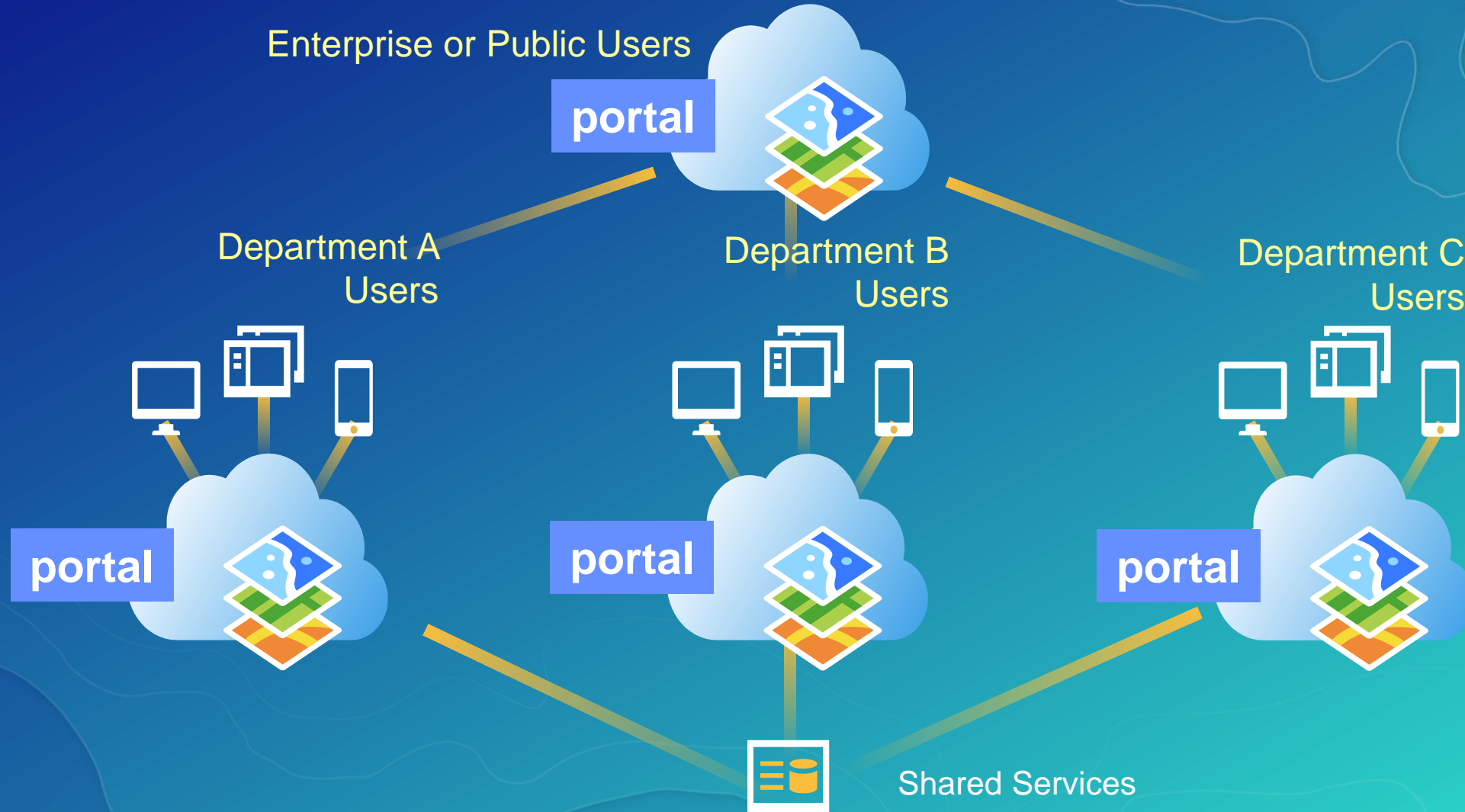
One Portal



Many Portals?

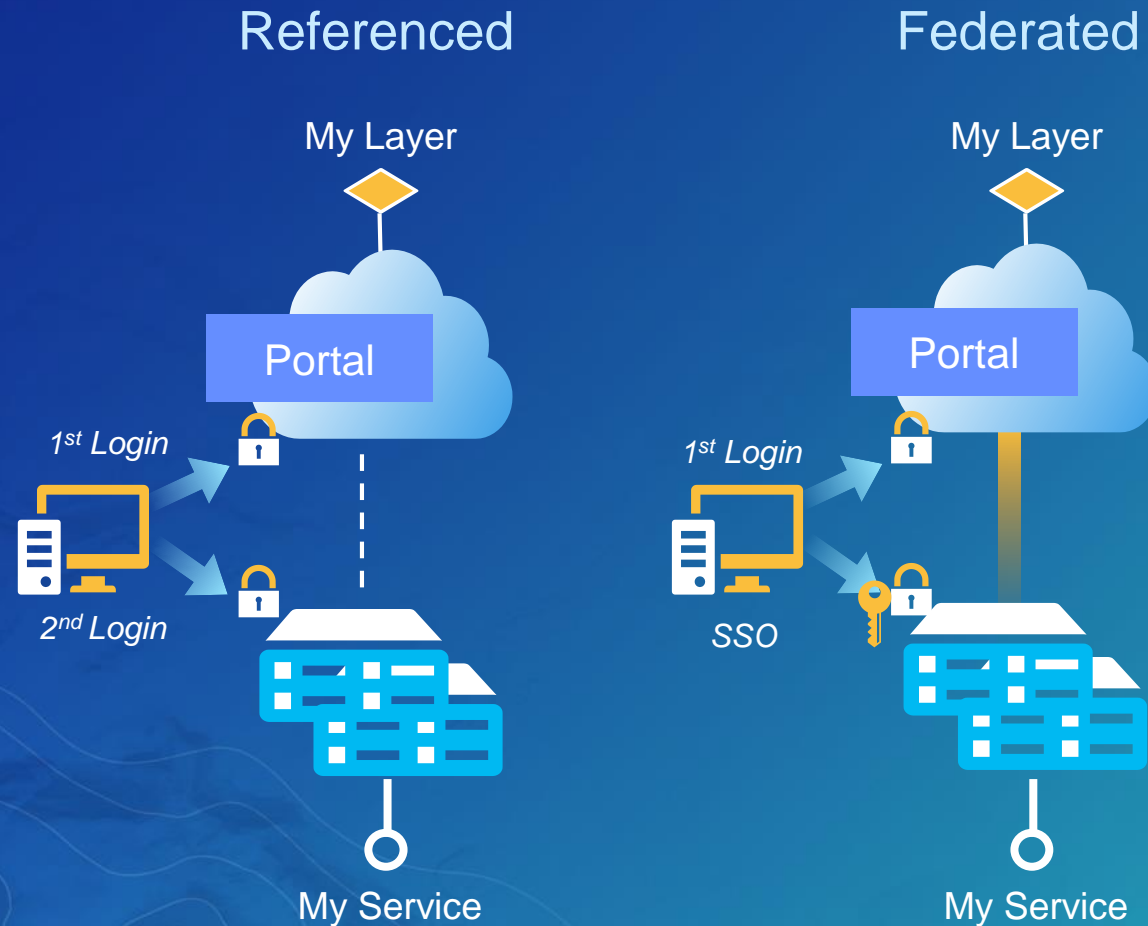
Web GIS

Multiple Portals



Web GIS

References vs. Federated



- Benefits

- Security

- Shared identity, SSO
 - Enables GIS Server w/ SAML
 - Portal groups for authorization
 - Shared roles w/ restricted publishing
 - Portal item management
 - More capabilities in future

- Considerations

- Highly distributed environments
 - Version consistency (upgrades)
 - HA and DR complexities

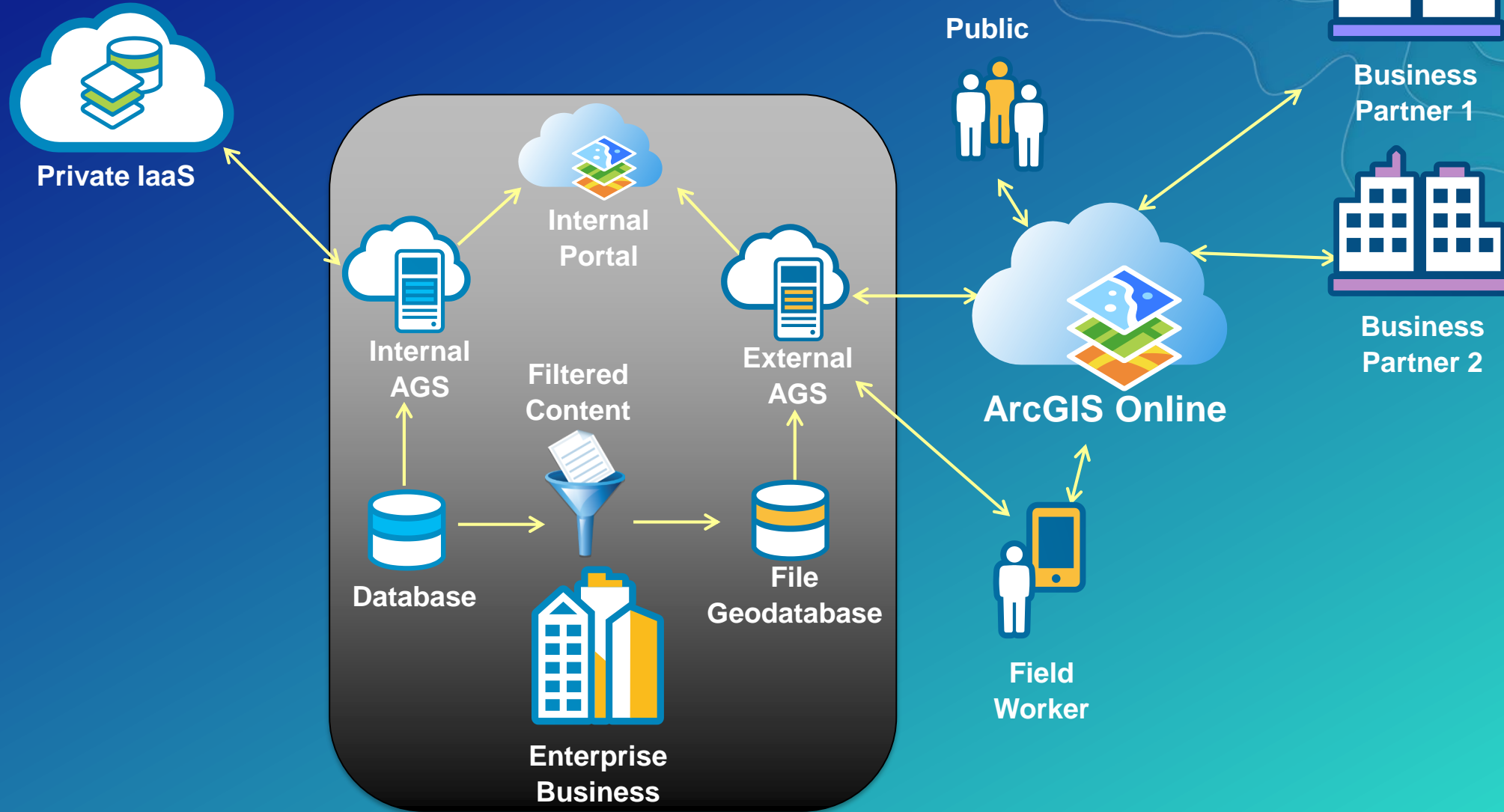
Web GIS

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

Enterprise deployment

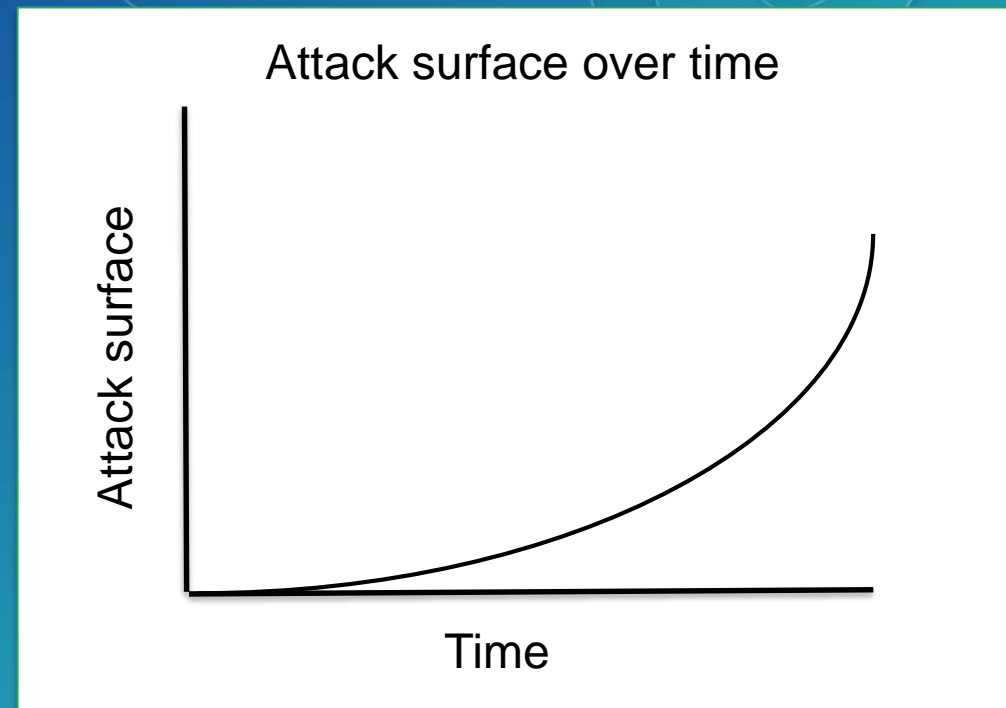
Real Permutations



ArcGIS Server

Implementation Guidance

- **Don't expose Server Manager or Admin interfaces to public**
- **Disable Services Directory**
- **Disable Service Query Operation (as feasible)**
- **Limit utilization of commercial databases under website**
 - File GeoDatabase can be a useful intermediary
- **Require authentication to services**
- **Use HTTPS**
 - Or at least make it available!
- **Restrict cross-domain requests**
 - Implement a whitelist of trusted domains for communications



ArcGIS Server

Recent Enhancements

10.4

- ArcGIS Server and Portal ArcGIS Server Best Practices security scanner
- Update passwords for registered and managed databases
 - To meet password policy requirements for cycling passwords
- ArcGIS Server Read-Only Mode
 - Disables publishing new services and blocks admin operations
- HTTP and HTTPS is enabled by default
- Enforce and choose cryptographic ciphers and algorithms

10.5

- New Membership levels
- Default viewer role that can be assigned
- Portal to Portal collaboration
 - Share content across groups
- Removed option to unfederate ArcGIS Server site from within Portal App
- Two new edit privilege levels
 - Edit and Edit with full control
- Security fixes and enhancements

ArcGIS Server

Recent Enhancements

- 10.5.1
- Custom roles provide more personalized and focused control of your access within the portal website. Beginning with ArcGIS Enterprise 10.5.1 update, the following new privileges are available when defining custom roles:
 - View content shared with portal
 - GeoAnalytics Feature Analysis
 - Raster Analysis

Mobile

Matt Lorrain



Mobile

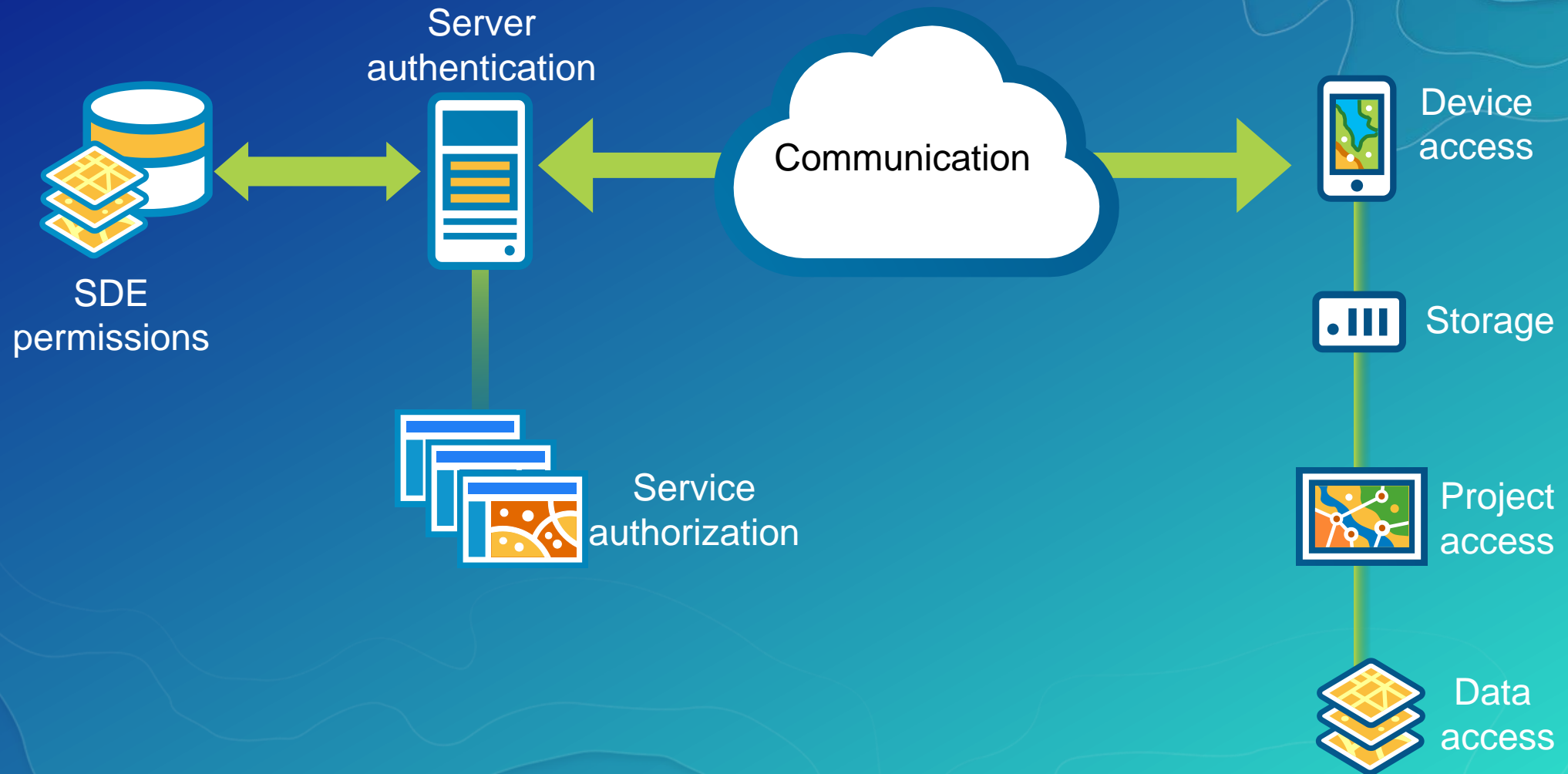
What are the mobile concerns?



*OWASP Top Ten Mobile: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks

Mobile

Security Touch Points



Mobile

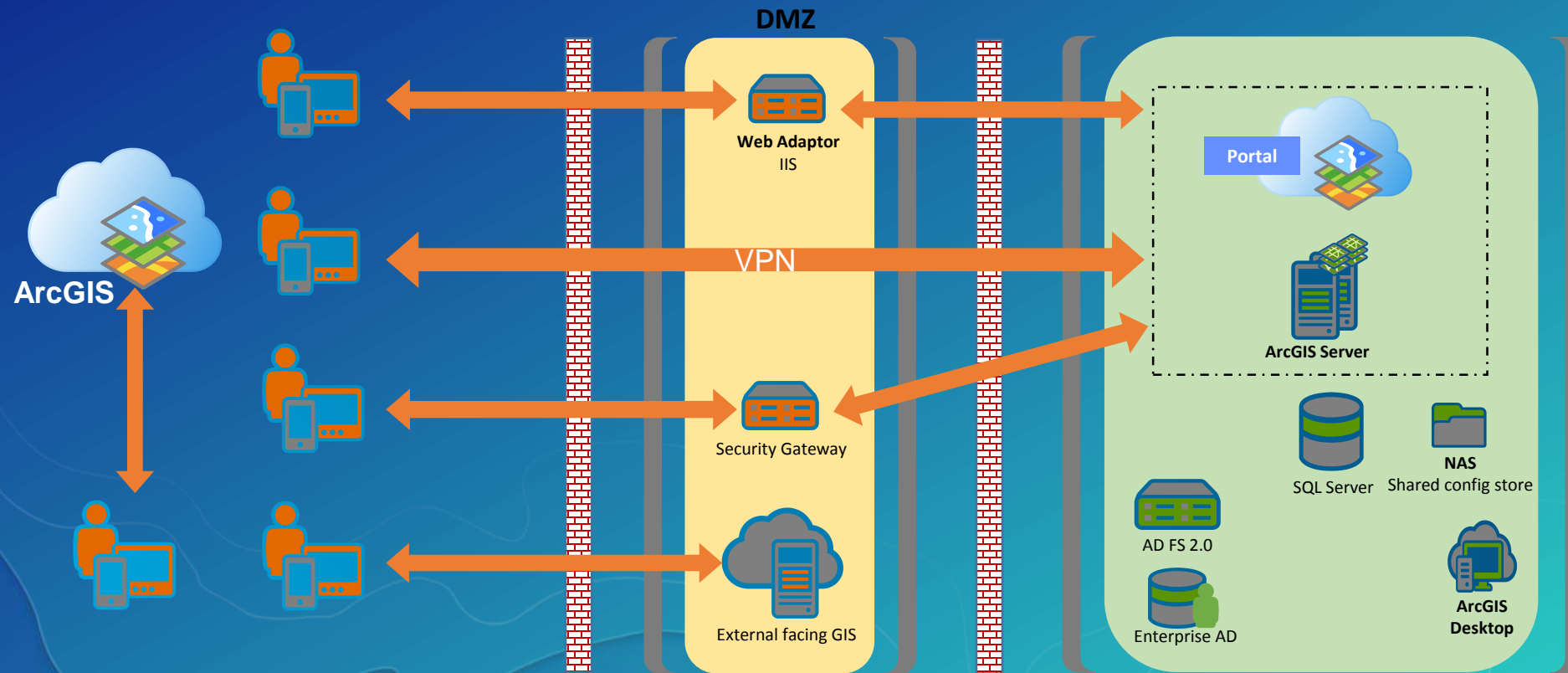
Challenges

- **Users are beyond corporate firewall**
 - To VPN or not to VPN?
- **Authentication/Authorization challenges**
- **Disconnected editing**
 - Local copies of data
- **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

Potential Access Patterns



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

Cloud

Matt Lorrain



Cloud

Service Models

- **Non-Cloud**

- Traditional systems infrastructure deployment
- Portal for ArcGIS & ArcGIS Server

- **IaaS**

- Portal for ArcGIS & ArcGIS Server
- Some Citrix / Desktop

- **SaaS**

- ArcGIS Online
- Business Analyst Online

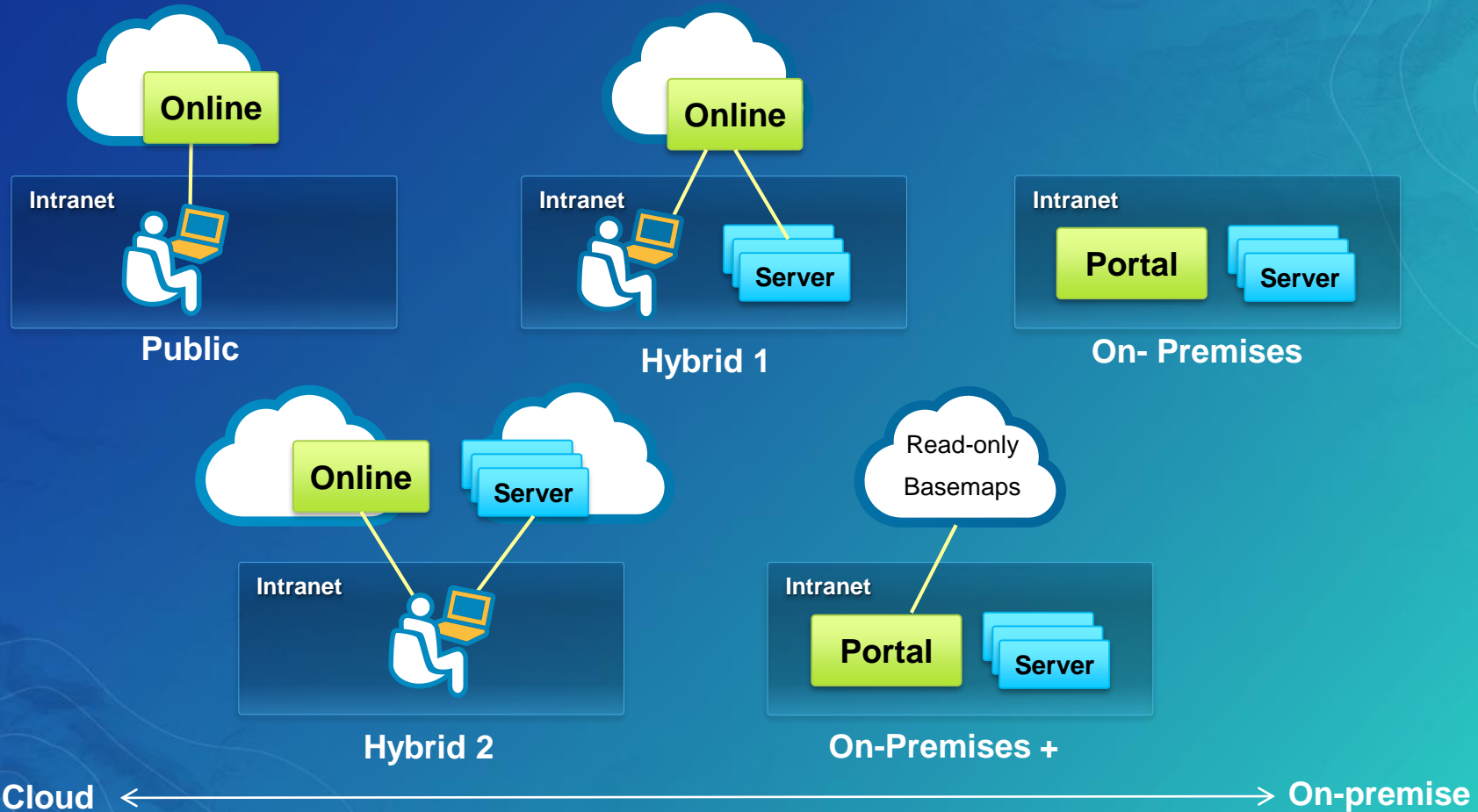
Customer Responsible
End to End

Decreasing Customer Responsibility

Customer Responsible
For Application Settings

Cloud

Deployment Models



Cloud

Management Models

- **Self-Managed**
 - Your responsibility for managing IaaS deployment security
 - Security measures discussed later
- **Provider Managed**
 - Esri Managed Services (Standard Offering)
 - Esri Managed Cloud Services (EMCS) Advanced Plus
 - FedRAMP Moderate environment

Cloud

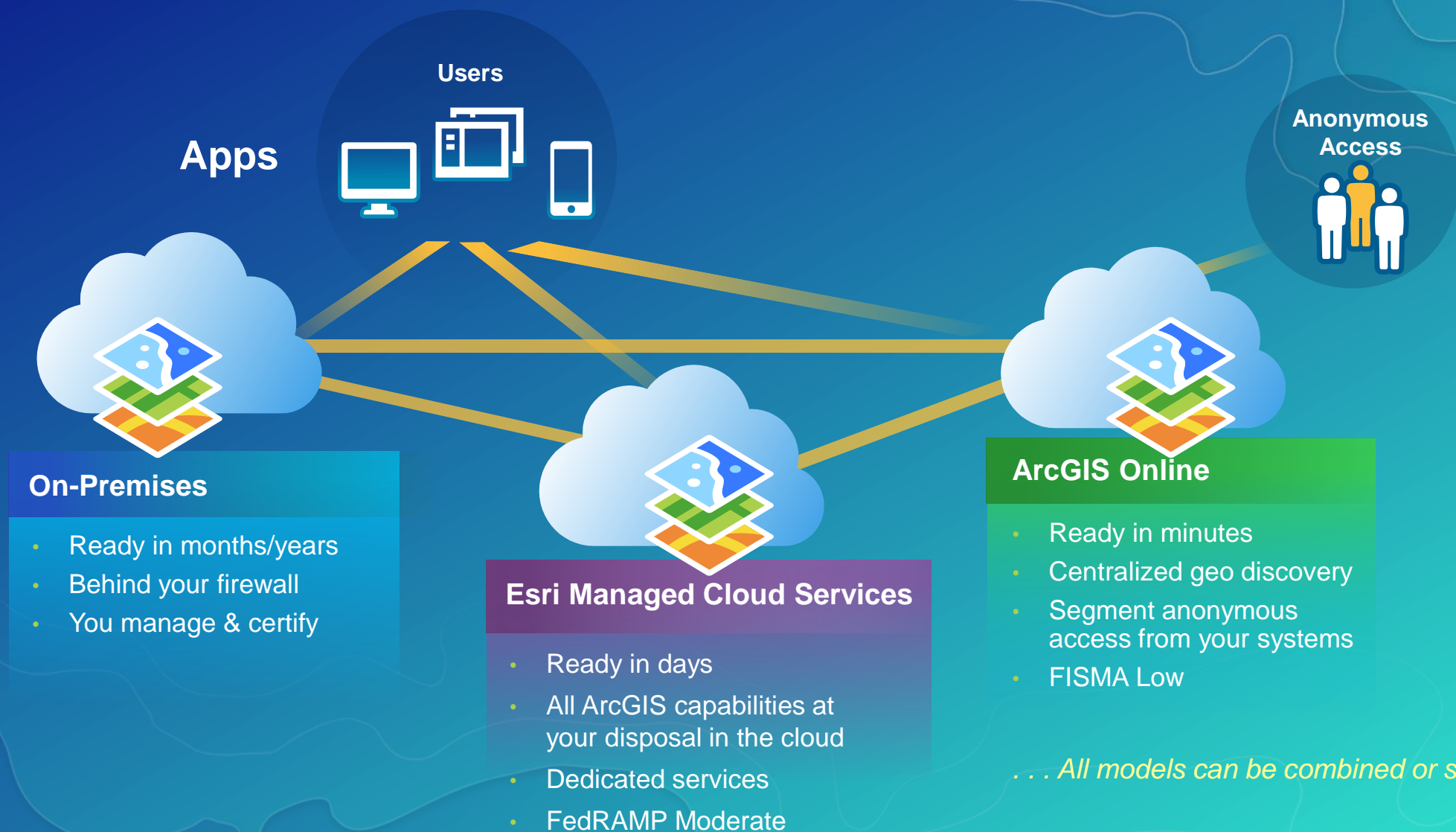
IaaS – Amazon Web Services

- **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)

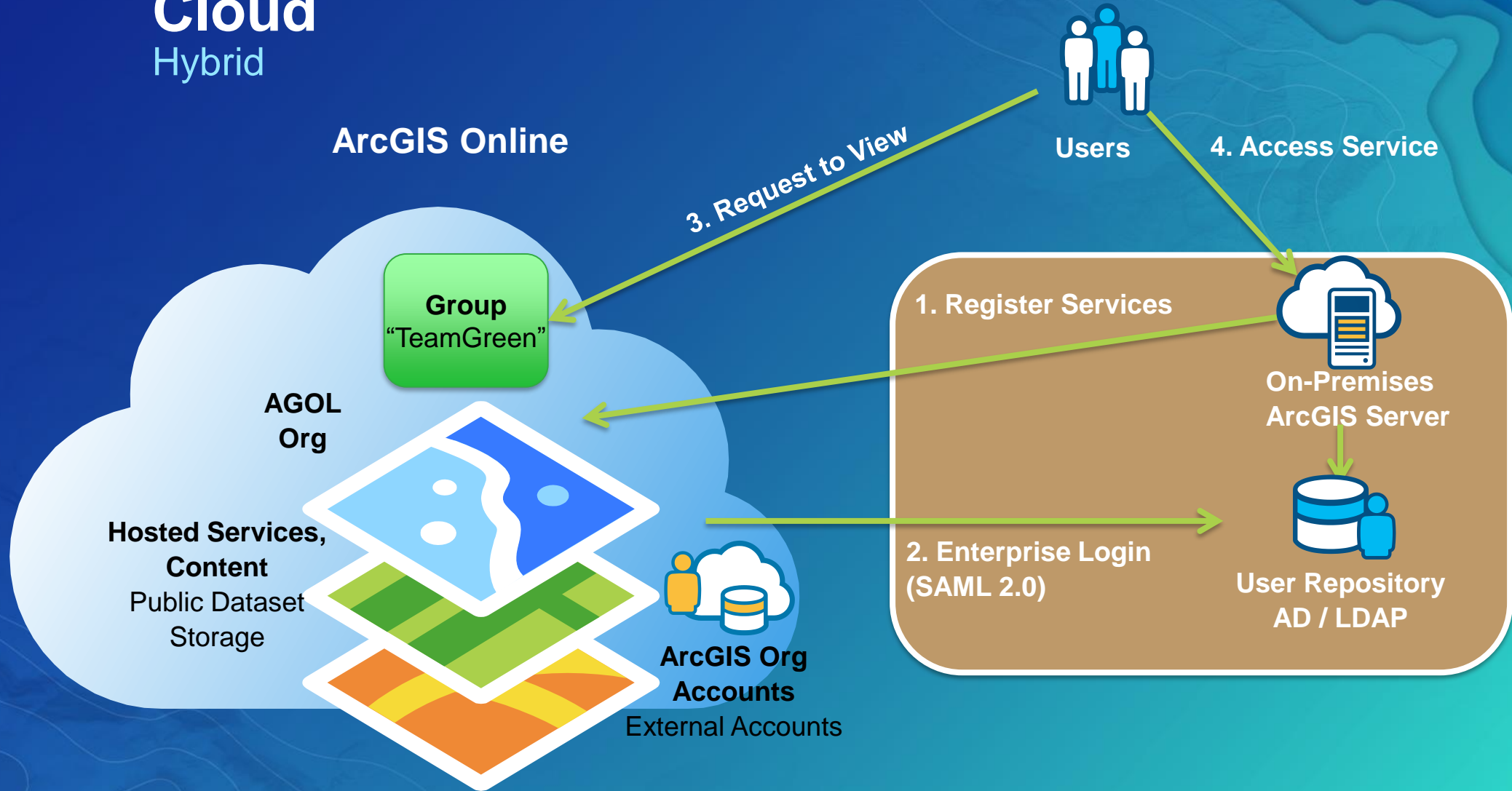


Cloud

Hybrid deployment combinations



Cloud Hybrid



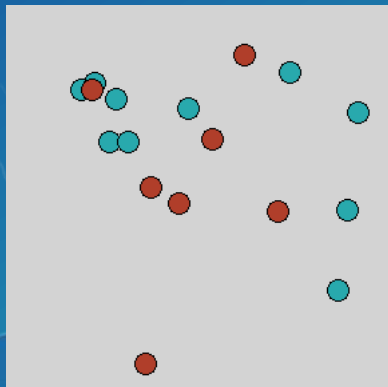
Segment sensitive data internally and public data in cloud

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**

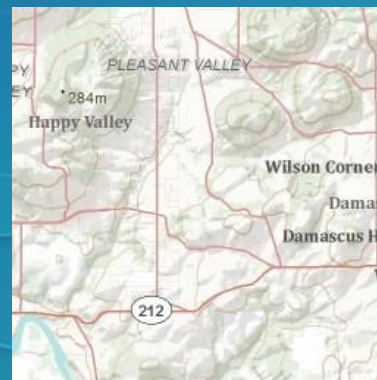
On-Premises Operational
Layer Service



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



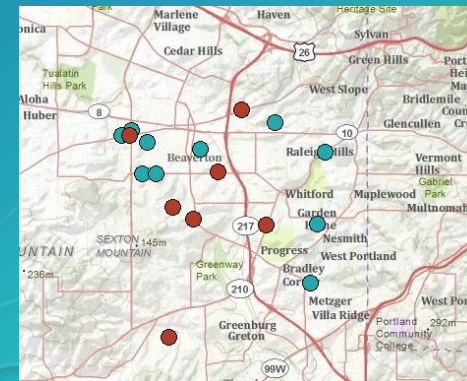
Cloud Basemap Service
ArcGIS Online



<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 for 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
- **Use multifactor for admin accounts**
- **Use a least-privilege model for roles and permissions**
 - Custom roles

Policies



- ☒ Allow access to the organization through HTTPS only.
- ☐ Allow anonymous access to your organization's website.
[What does this mean?](#)
- ☒ Allow only standard SQL queries.

Sharing and Searching



- ☐ Members can share content outside the organization.
- ☐ Members can search for content outside the organization.

Compliance

Michael Young



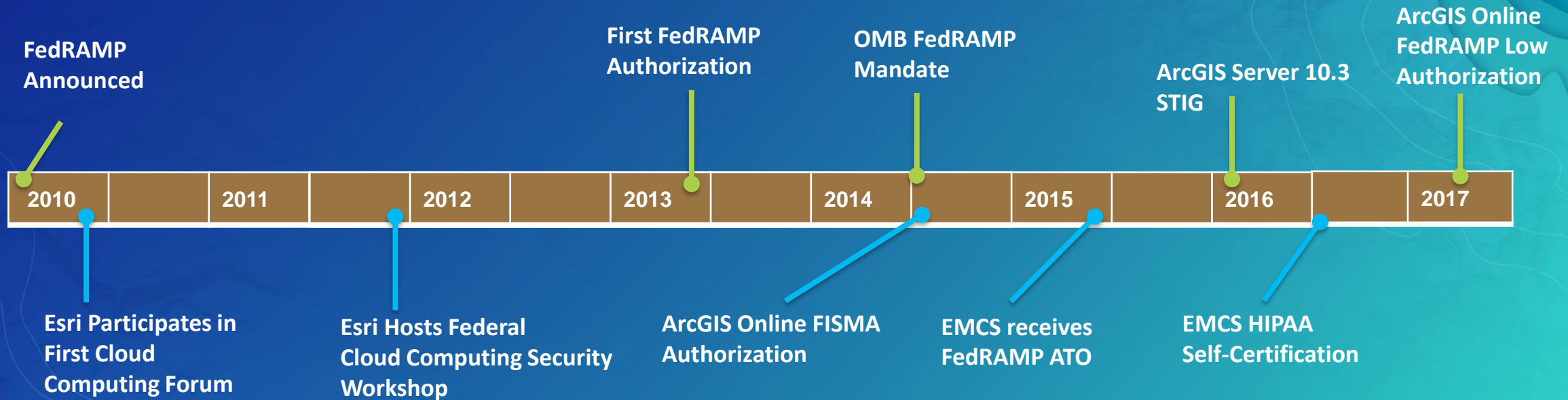
Compliance

ArcGIS Platform Security

- **Esri Corporate**
- **Cloud Infrastructure Providers**
- **Products and Services**
- **Solution Guidance**

Compliance

Extensive security compliance history



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

Compliance

Corporate

- **ISO 27001**
 - Esri's Corporate Security Charter
- **Privacy Assurance**
 - EU-U.S. Privacy Shield self-certified
 - General Esri Privacy Statement
 - Products & Services Privacy Statement Supplement
 - TRUSTed cloud certified
 - General Data Protection Regulation (GDPR)
 - Active alignment project in place for May 2018 deadline



Compliance

Cloud Infrastructure Providers

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

Cloud Infrastructure Security Compliance



Compliance

Products & Services

- **ArcGIS Online**
 - **FISMA Low Authority to Operate by USDA (Jan 2014)**
 - **New FedRAMP Tailored Low Authorization Program being released August 2017**
 - Targeted for SaaS offerings hosted on FedRAMP authorized cloud infrastructure providers
 - Advancements made during this authorization include
 - Incorporating cloud-specific security control guidance of FedRAMP beyond FISMA
 - Shifts from NIST 800-53 Rev 3 security controls to Rev 4 (current release)
 - Incorporate ArcGIS Online capabilities from both AWS and MS Azure such as Hosted Feature Services
 - **Goal is to complete ArcGIS Online FedRAMP authorization before end of 2017**



Compliance

Products and Services

- Esri Managed Cloud Services (EMCS) Advanced Plus
 - FedRAMP Moderate Authorized by US Census (September 2015)
 - HIPAA Self-certified (2016)
- ArcGIS Server
 - DISA STIG – Completed in 2016
 - ArcGIS Server 10.3 (More STIGs to follow)
- ArcGIS Desktop (10.1 and above) and ArcGIS Pro (1.4.1 and above)
 - USGCB Self-Certified

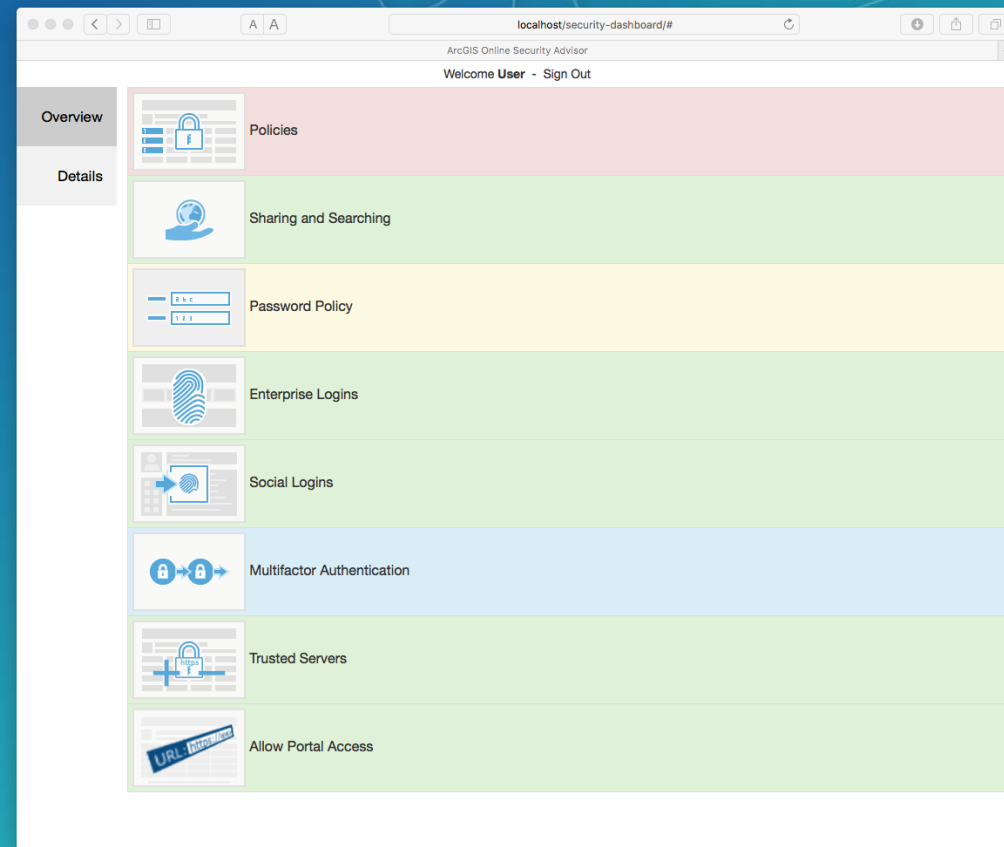


Compliance

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 - Beta security dashboard app**
 - Checklist validates your org settings/usage against secure best practice recommendations
 - Audit log provides a summary of user actions
 - Interested? SecureSoftware@Esri.com

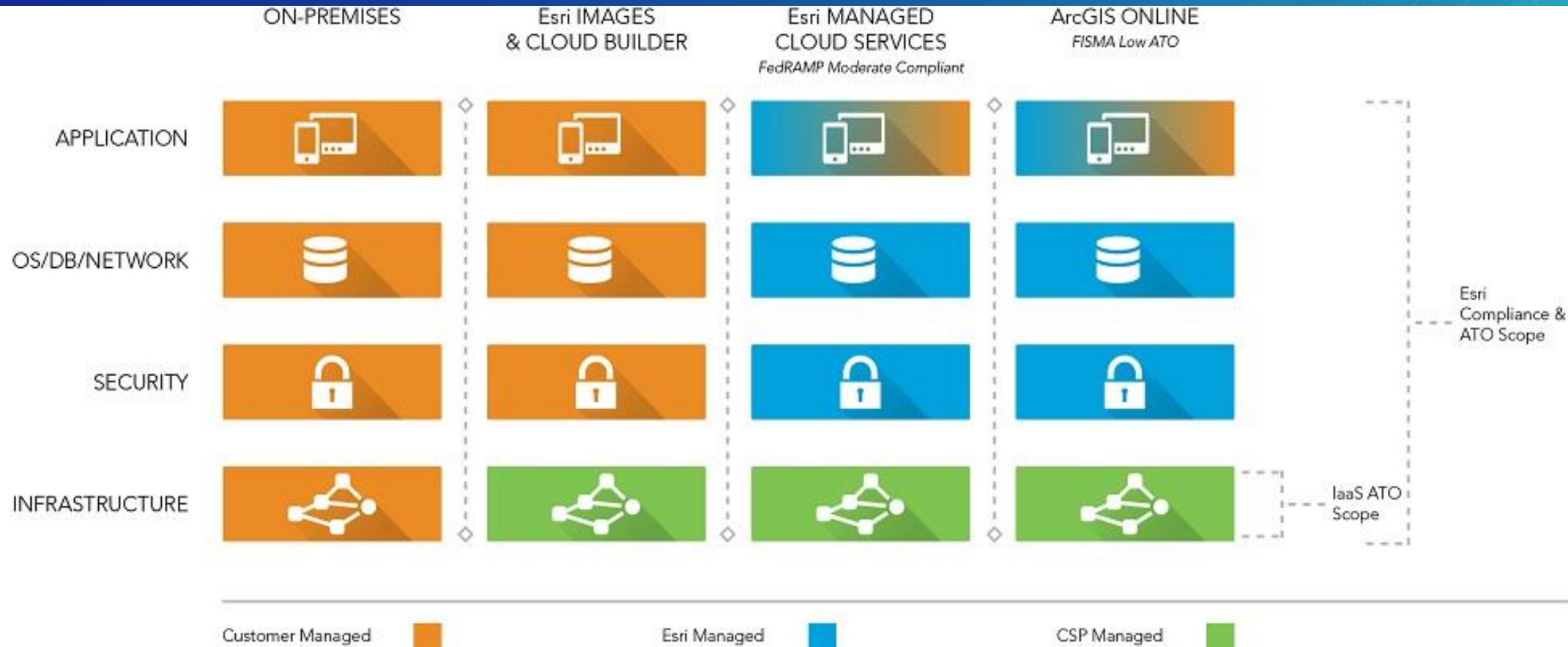


Solution Level

- [illegible]

Compliance

Deployment Model Responsibility



Summary

Michael Young



Summary

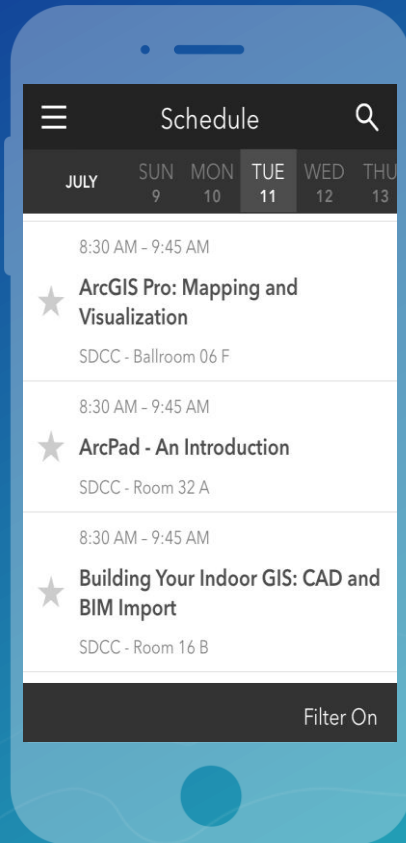
- **Security demands are rapidly evolving**
 - Prioritize efforts accord to your industry and needs
 - Don't just add components, simplified Defense In Depth approach
- **Secure Best Practice Guidance is Available**
 - Check out the [Trust.ArcGIS.com](https://trust.arcgis.com) Site!
 - New security validation tools coming out
 - Security Architecture Workshop
 - SecureSoftware@esri.com

Please Take Our Survey on the Esri Events App!

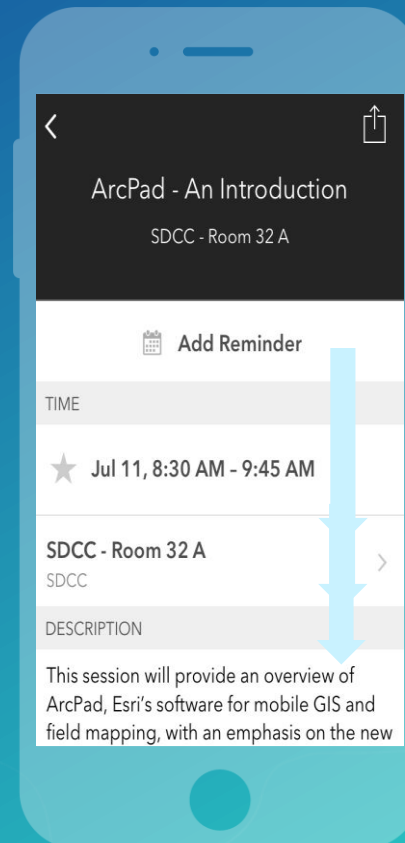
Download the Esri Events app and find your event



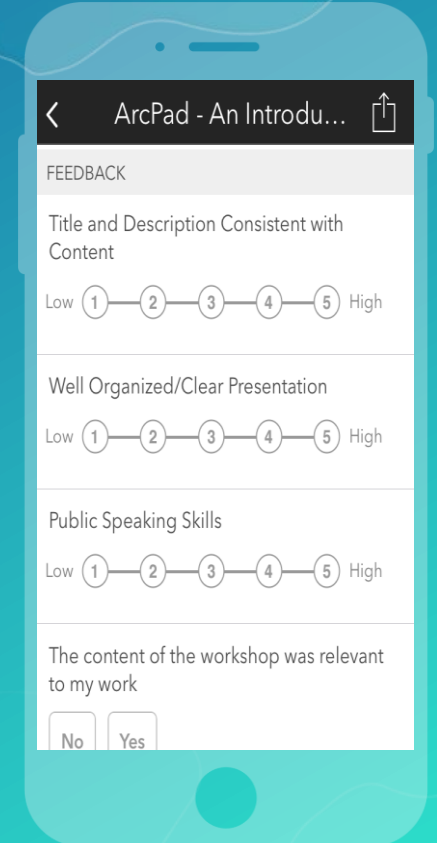
Select the session you attended



Scroll down to find the survey



Complete Answers and Select "Submit"





esri

THE
SCIENCE
OF
WHERE