Practical Security

MAKING TOUGH DECISIONS IN A CLOUD-FIRST WORLD

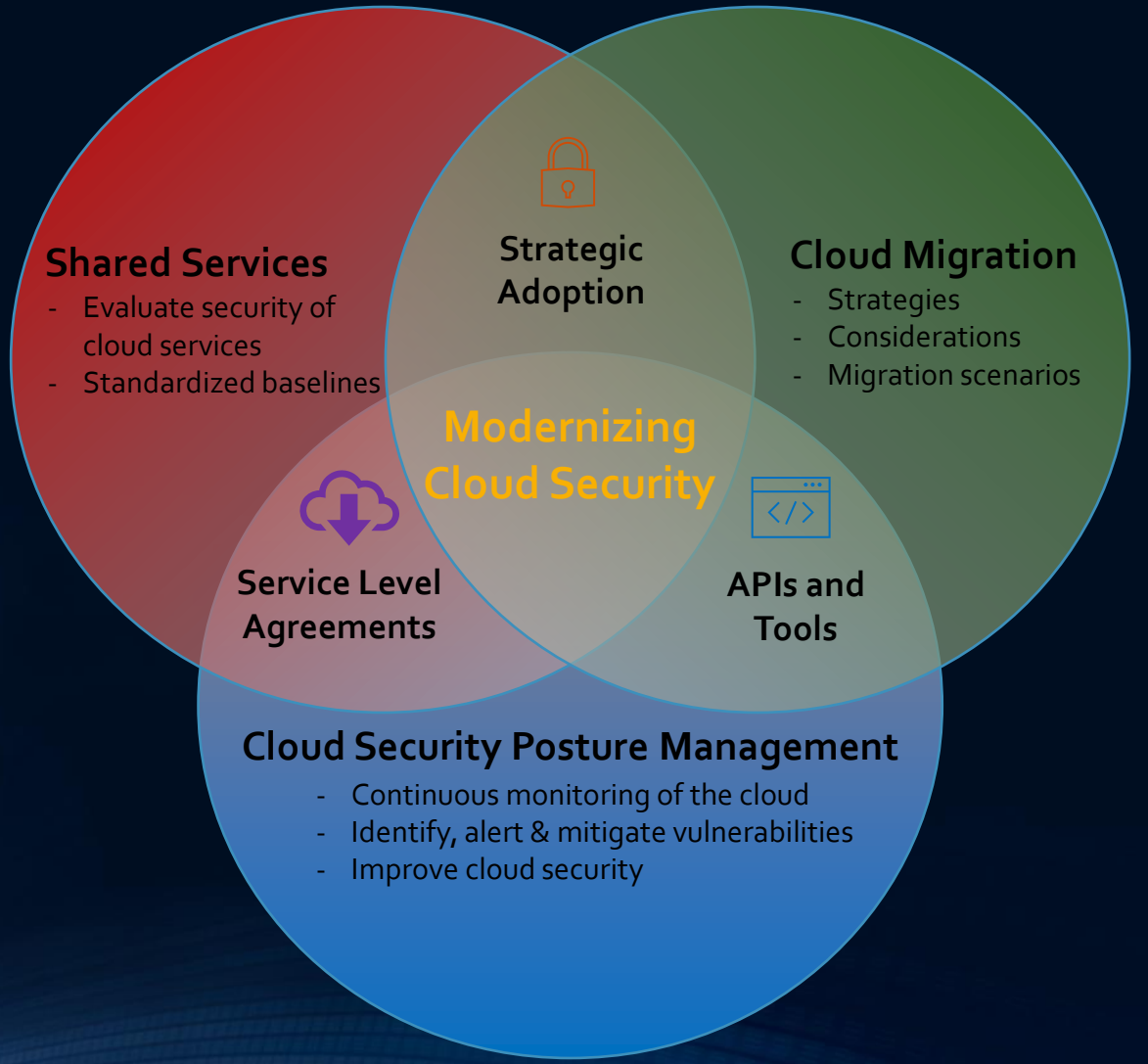
TROY ARWINE, MSIA | CEH | CISSP
SR. MANAGER, ENTERPRISE SECURITY ARCHITECTURE
NAVY FEDERAL CREDIT UNION (NFCU)

Agenda

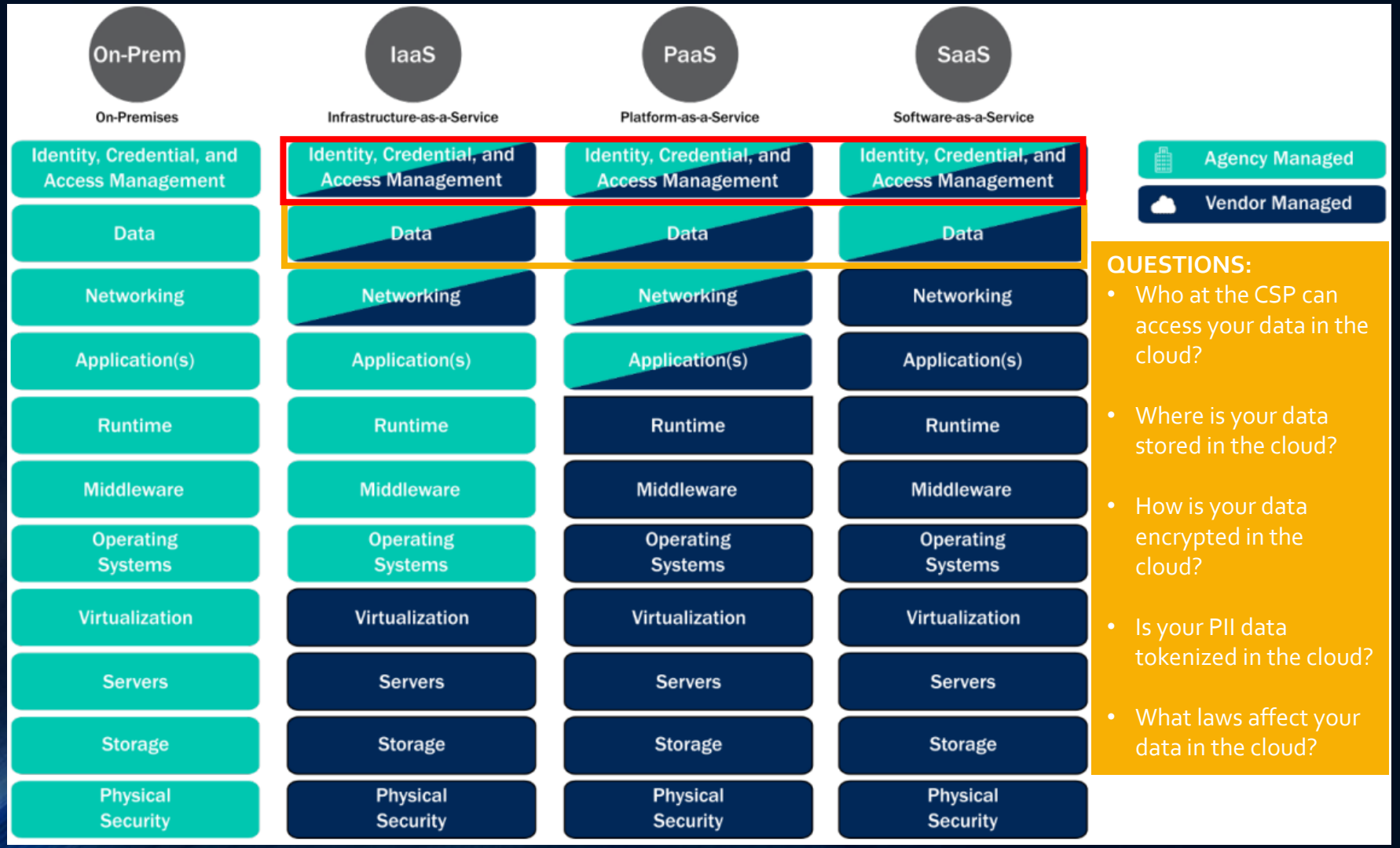
- Introduction
- Modernizing Cloud Security
- Responsibilities Matrix for Cloud Service
- Capabilities of Zero Trust
- Zero Trust Architecture & Cloud
- Driving multi-cloud security architecture
- Questions

Modernizing Cloud Security

Cloud Security Technical Reference Architecture (CISA.gov)



Responsibilities Matrix for Cloud Service
Cloud Security Technical Reference Architecture (CISA.gov)



QUESTIONS:

- Who at the CSP can access your data in the cloud?
- Where is your data stored in the cloud?
- How is your data encrypted in the cloud?
- Is your PII data tokenized in the cloud?
- What laws affect your data in the cloud?

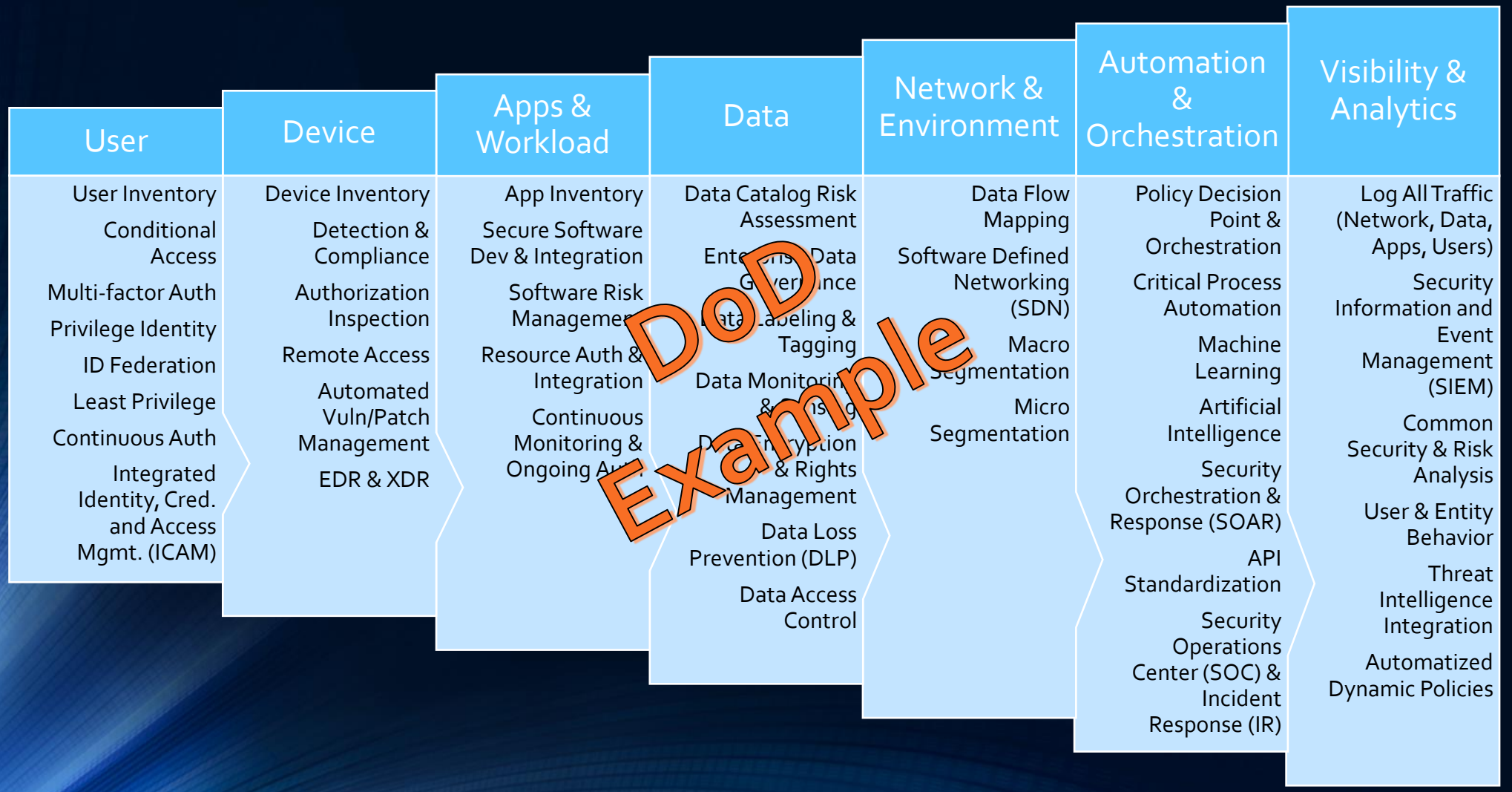
QUESTIONS:

- Who controls the identity stores?
- How are real people IDs authenticated (MFA, OTPs, secrets)?
- How are non-people IDs authenticated (APIs, B2B/B2C creds)?
- How are API identities authorized to access apps & data after strong authentication?

Fig 1. Responsibilities Matrix. Cybersecurity and Infrastructure Security Agency, United States Digital Service, and Federal Risk and Authorization Management Program (2022, June) . Responsibilities for Different Service Models [digital image]: https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf, p2.

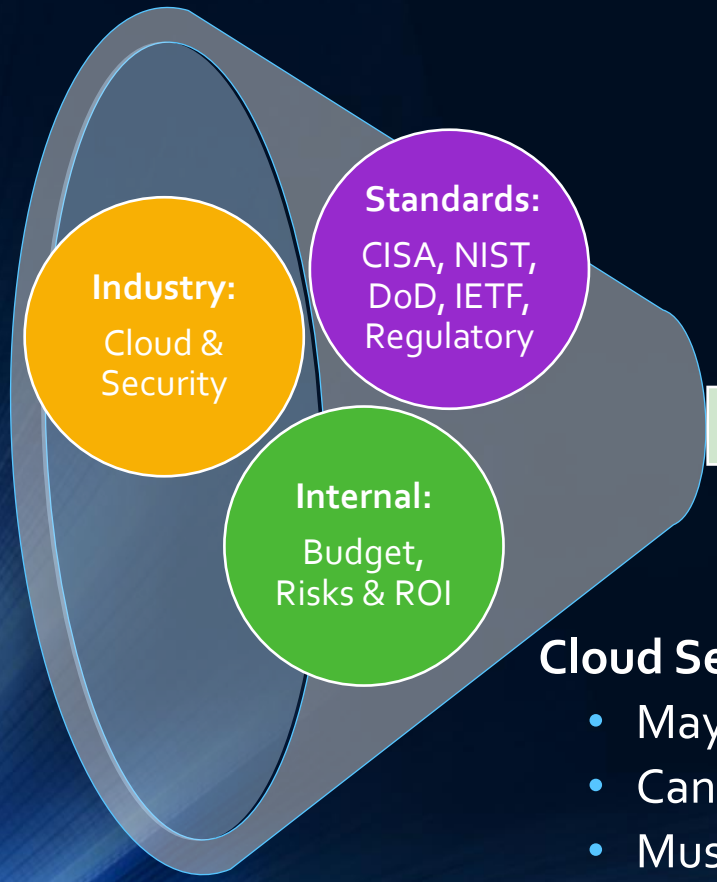
Capabilities of Zero Trust (defense.gov)

Define *your* ZT model for your journey to the Cloud



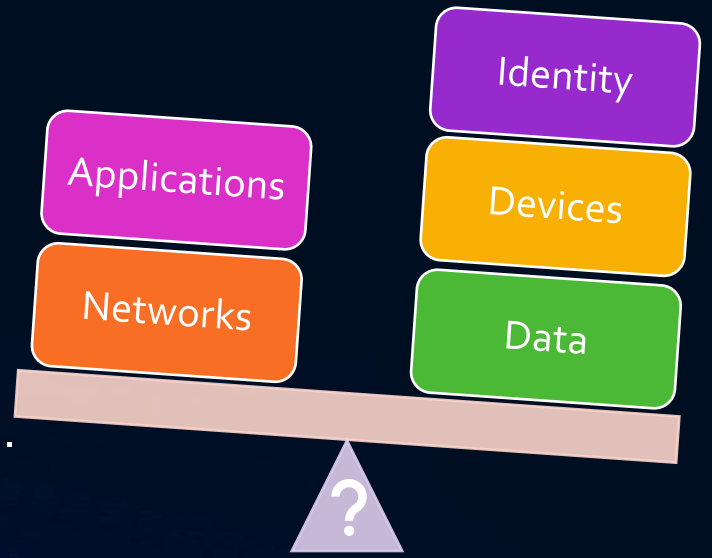
Zero Trust (ZT) Architecture & Cloud

One Size Does Not Fit All – What are *your* requirements?



Don't Assume

Zero Trust (ZT) Strategy



Cloud Service Providers (CSPs):

- May not be a secure as you think.
- Can prioritize roadmaps if required.
- Must be held accountable for ZT.
- CSPs adjust to your ZT standards.

Driving multi-cloud security architecture

Cloud is Not *Inherently Secure* by Default

- Don't let any cloud provider dictate their security standards regardless of CSPs reputation/size/market share or any awards (Forrester/Gartner)
- Require Cloud/SaaS providers to meet your security standards
- Require Cloud/SaaS providers to provide written attestation of their security compliance
- If provider cannot meet security requirements yet, ensure they commit to a date for delivery
- Follow-up & don't practice making exceptions to zero trust standards

Questions?