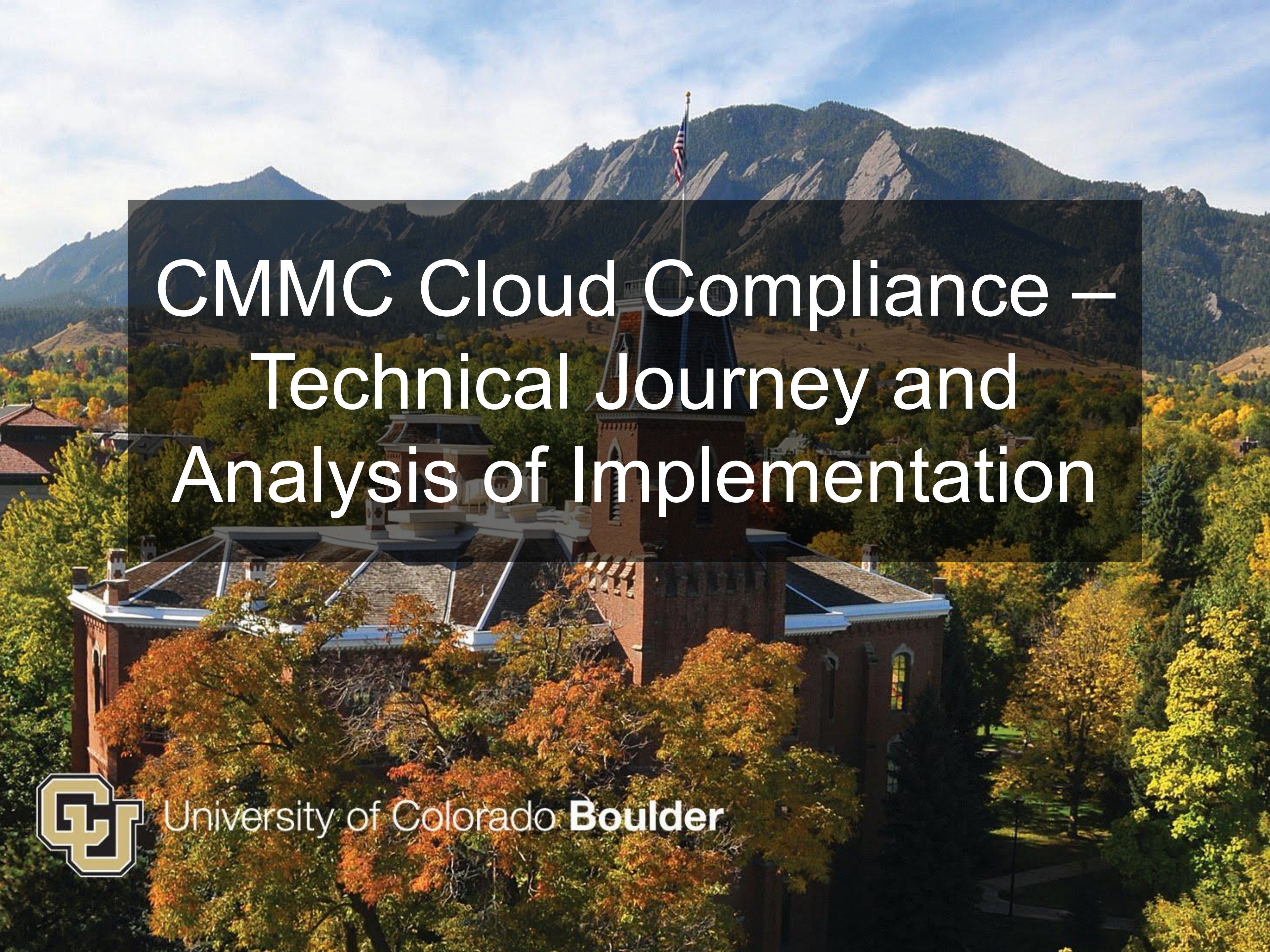


CMMC Cloud Compliance – Technical Journey and Analysis of Implementation

University of Colorado **Boulder**

Agenda

01 Who we are?

02 Initial Design Decisions

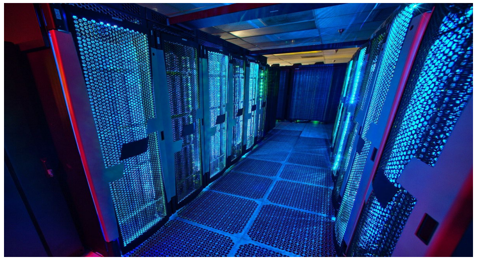
03 What Microsoft Got Right

04 Why Microsoft Why!?

05 How Hard Can It Be?

06 The Next Level

CU Research Computing



On-premise computing & storage

- High Performance Computing
- Large File Storage
- On-prem cloud (OpenStack)

Training & User Support

- Courses
- Office hours
- Help desk

Consulting

- On-prem focused
- Cloud focused
  (Ad hoc, emerging)

Cloud Enablement

- AWS
- Azure (emerging)
- GCP (future)

THE PRESERVE

Compliant Research Options

- The Preserve (Azure Gov - CMMC)
- Other TBD

CU Research Computing

Small sub team in Research Computing

2 Cloud Engineers
1 User Support / Cloud Analyst
1 Security Operations Engineer
1 Program Manager

Other Supporting Team Members

Cloud Security Architect
O365 Administrator
Compliance analyst

Initial Design Decisions

Initial Design Decisions

Azure Virtual Desktop (AVD)

Needed a place for users to work from without necessarily having to bring work devices into scope

FSLogix

Recommended way of handling profiles in AVD's supported by Microsoft and readily available in marketplace

Azure Active Directory (AAD)

Identity and group management along with multi-factor authentication (MFA)

Privileged Access Management (PIM)

Monitor and log role-based access, implement approval process, enables least privileged and just in time role-based access

Azure Active Directory Domain Services

Requirement for FSLogix to map Azure Files

Network Access

Azure Security Benchmark Foundation Blueprint, necessary Azure Firewall rules, and VPN gateways

What Microsoft Got Right

Features We Love

- Separated IAM Environment for Gov
- Azure Active Directory
- Direct Integration of O365 GCC High – BIG win!
- Isolation Levels
- Already at DoD Impact Level 4 or 5 without extra configuration
- Marketplace helps streamline solutions
- AVD connection brokers – Reverse Connect
- FSLogix profiles simplifies roaming profiles across AVD’s
- Azure Private Endpoints
- Azure Web Application Firewall
- Azure Sentinel overall

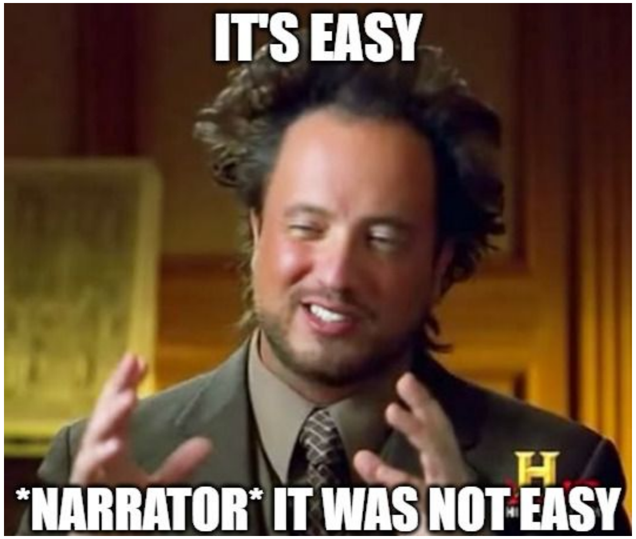
Why Microsoft Why!?

Features We Miss

- Azure DevOps
- Azure Storage Blob malware scanning
- Azure VM sizing restrictions
- AVD Autoscaling
- AAD Kerberos
- PIM groups (preview in commercial)
- Missing Defender features
- Missing Sentinel features
- Missing Sentinel Connectors
- Mix of gov and public endpoints that need to be allowed
- Readily Available DNS Logs
- Microsoft Gov Cloud Endpoints hard to discover
- Marketplace does not guarantee fully vetted or FedRAMPed software to meet compliance
- No recommendation exemption rules

How Hard Can It Be?

- Development Tools
- Ticketing System
- Data Ingress



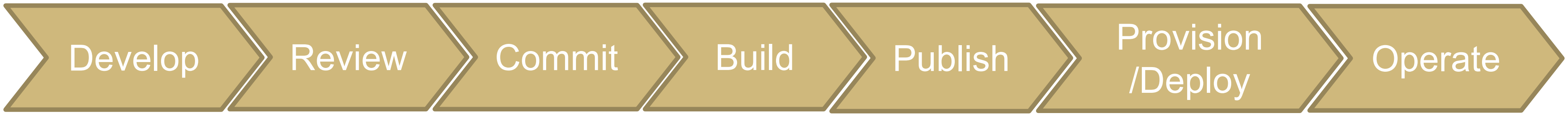
Development Tools

Create containers to import tools in a single instance rather than disparate sources

Build and maintain isolated DevOps tools artifact repository

Import and custom coded tools from noncompliant environment

Development Tools – Current State



HashiCorp Terraform

Visual Studio Code

PowerShell

Dev tools, libraries

[redacted]

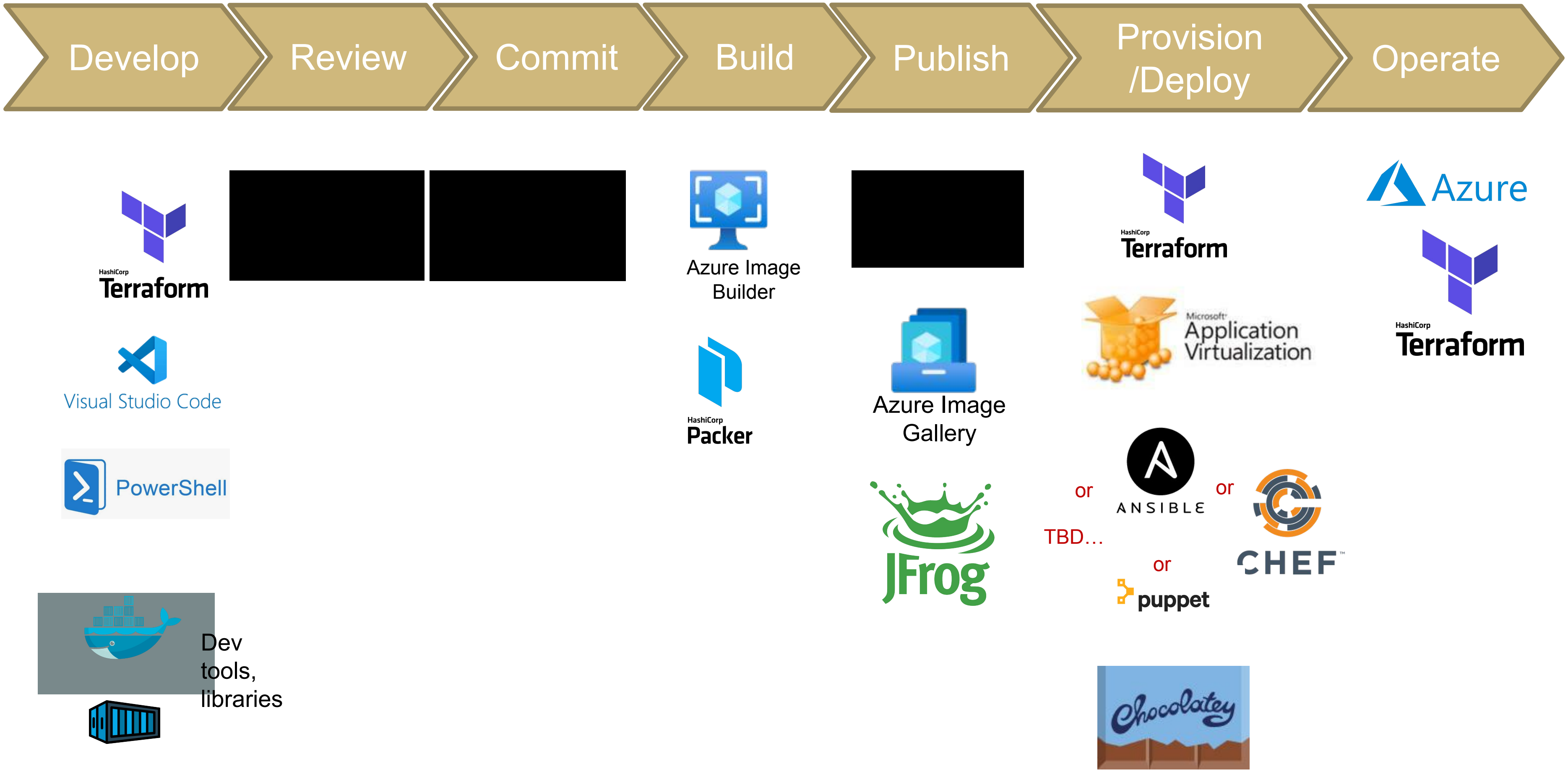
[redacted]

[redacted]

HashiCorp Terraform

Azure

Development Tools – Future State



Develop → Review → Commit → Build → Publish → Provision /Deploy → Operate

Develop
- HashiCorp Terraform
- Visual Studio Code
- PowerShell
- Dev tools, libraries

Review

[redacted]

Commit

[redacted]

Build
- Azure Image Builder
- HashiCorp Packer

Publish

[redacted]

- Azure Image Gallery
- JFrog

Provision /Deploy
- HashiCorp Terraform
- Microsoft Application Virtualization
- TBD… or ANSIBLE or CHEF or puppet
- Chocolatey

Operate
- Azure
- HashiCorp Terraform

Ticketing System

Compliance Guidlines

- System information must be treated as highly sensitive
- Need to find solution for user emails to help with specific systems
- Technical teams need to be able to share system information for change implementations

Purchase FedRAMPed Solutions

- MS Dynamics
- Service Now

Vet Other Potential Solutions

- Low cost or open-source solutions
- Must pass vetting process
- Requires more hands-on maintenance than SaaS FedRAMP solutions

Data Ingress

Compliance

- Isolate data as much as possible
- Conditional access by location and user RBAC
- Ability to control data workflows
- Ease of use

Security Issues

- Lots of edge cases
- How to restrict users access without it being overbearing
- Scanning files on ingress for malicious content
- Tracking devices and login locations
- Remote deletion for field devices
- Data Loss Prevention rules
- Legal holds

The Next Level

- Standardization and improvement of change control processes
- Reduce necessity of multiple golden images or eliminate all golden images.
- Improve Infrastructure as Code and deployment automation/consistency
- Simplify development and researcher cycles
- High Performance Computing
- Azure Container Registry
- Invest in ongoing security and compliance training

Q&A