REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)* 11/05/2020	**2. REPORT TYPE** Technical Report	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE Cloud Computing Technical Exchange	**5a. CONTRACT NUMBER** W56KGU-18-D-0004
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Reavey, Michael	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) The MITRE Corporation 202 Burlington Road Bedford, MA 01730	**8. PERFORMING ORGANIZATION REPORT NUMBER** PRS-20-2788
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

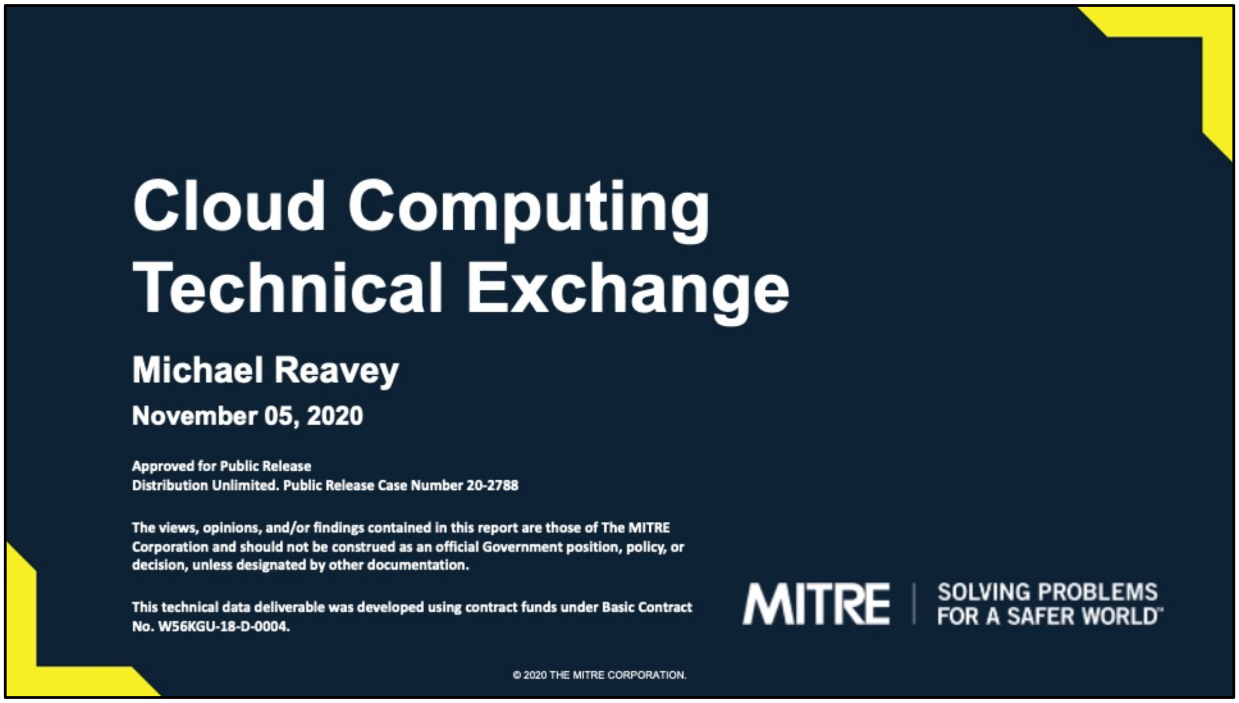
12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
1-Definition, 2-Policy and Strategy, 3-Adoption/Migration, 4-Security, 5-Economics, 6-Workforce Development, 7-Cloud DevSecOps, 8-References

15. SUBJECT TERMS
Computing Methodologies (General); Computer Security; Network Security cloud computing; adoption; ATT&CK; federal policy; migration; strategy;

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Susan Carpenito
				56	**19b. TELEPHONE NUMBER** *(Include area code)* 781-271-7646



Cloud Computing Technical Exchange

Michael Reavey

November 05, 2020

Approved for Public Release
Distribution Unlimited. Public Release Case Number 20-2788

The views, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-18-D-0004.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Outline

Definition

Policy and Strategy

Adoption/Migration

Security

Economics

Workforce Development

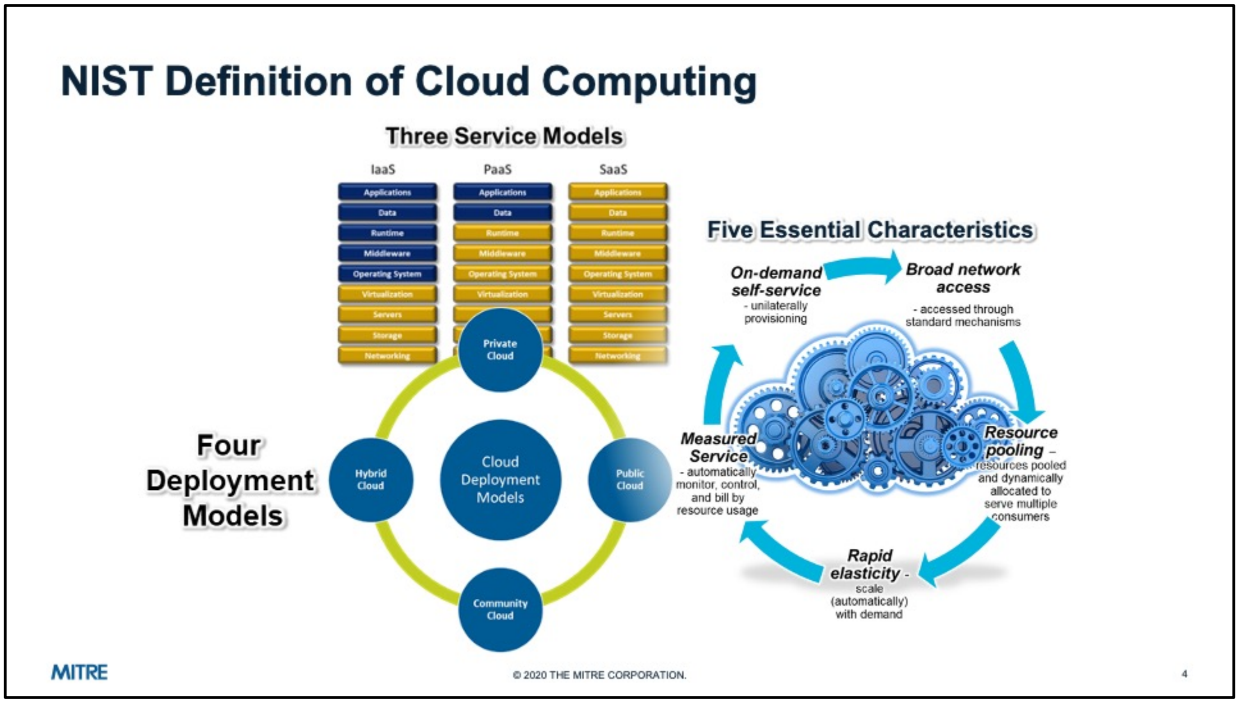
Cloud DevSecOps

References

Backup

Definition

MITRE



NIST Definition of Cloud Computing

Three Service Models

Four Deployment Models

Five Essential Characteristics

On-demand self-service - unilaterally provisioning

Broad network access - accessed through standard mechanisms

Resource pooling – resources pooled and dynamically allocated to serve multiple consumers

Rapid elasticity - scale (automatically) with demand

Measured Service - automatically monitor, control, and bill by resource usage

MITRE

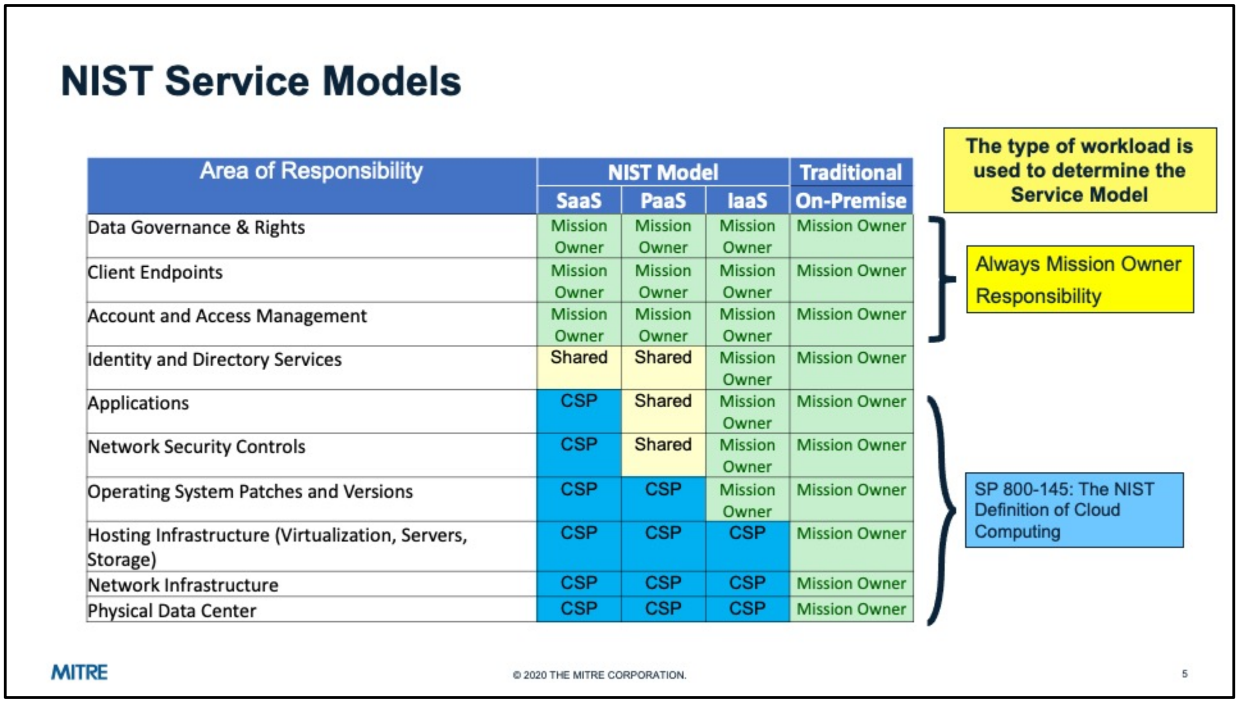
© 2020 THE MITRE CORPORATION.

4

Slide Source: MITRE

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. [1]

-Pay-per-Use – Pay only for the IT resources you use
-Resource Pooling - Shared, multi-tenant, location-independent
-On-demand - Self-service, real-time, automatic provisioning
-Network Accessible - Available over the Internet
-Elastic - Automatically scaled up and down as needed



NIST Service Models

Area of Responsibility	NIST Model			Traditional
	SaaS	PaaS	IaaS	On-Premise
Data Governance & Rights	Mission Owner	Mission Owner	Mission Owner	Mission Owner
Client Endpoints	Mission Owner	Mission Owner	Mission Owner	Mission Owner
Account and Access Management	Mission Owner	Mission Owner	Mission Owner	Mission Owner
Identity and Directory Services	Shared	Shared	Mission Owner	Mission Owner
Applications	CSP	Shared	Mission Owner	Mission Owner
Network Security Controls	CSP	Shared	Mission Owner	Mission Owner
Operating System Patches and Versions	CSP	CSP	Mission Owner	Mission Owner
Hosting Infrastructure (Virtualization, Servers, Storage)	CSP	CSP	CSP	Mission Owner
Network Infrastructure	CSP	CSP	CSP	Mission Owner
Physical Data Center	CSP	CSP	CSP	Mission Owner

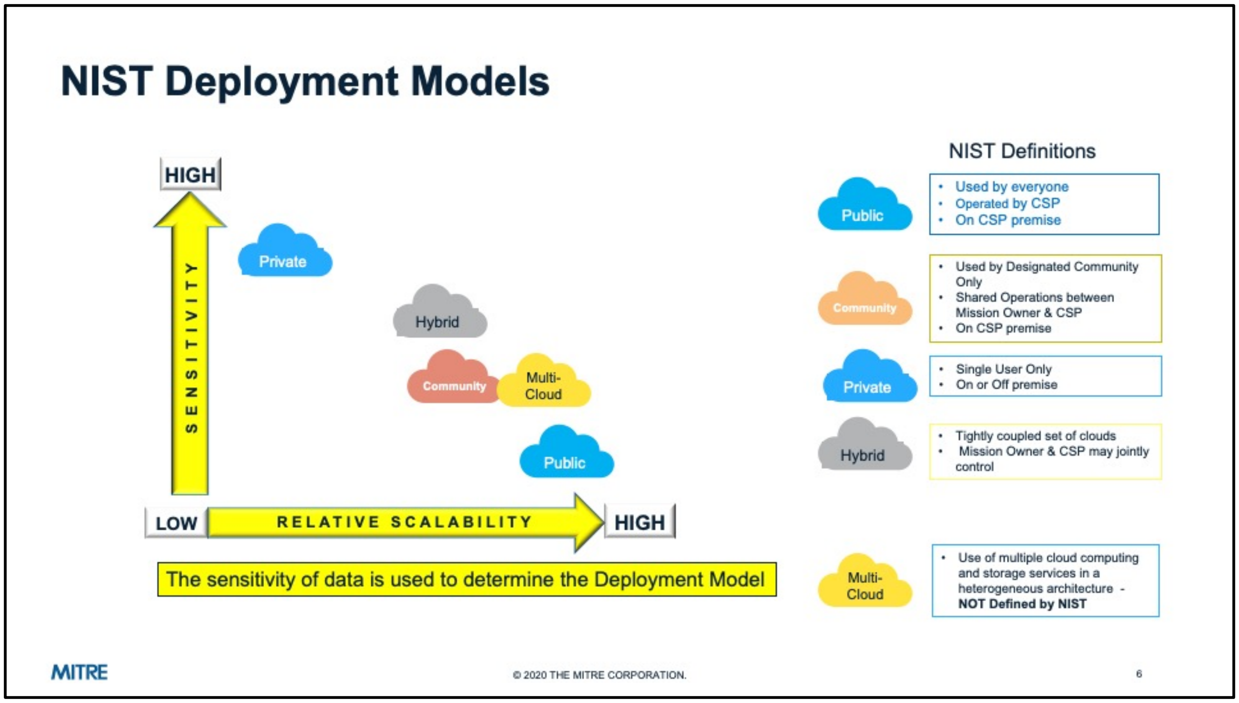
The type of workload is used to determine the Service Model

Always Mission Owner Responsibility

SP 800-145: The NIST Definition of Cloud Computing

MITRE

Slide Source: MITRE



NIST Deployment Models

The sensitivity of data is used to determine the Deployment Model

NIST Definitions

Public
- Used by everyone
- Operated by CSP
- On CSP premise

Community
- Used by Designated Community Only
- Shared Operations between Mission Owner & CSP
- On CSP premise

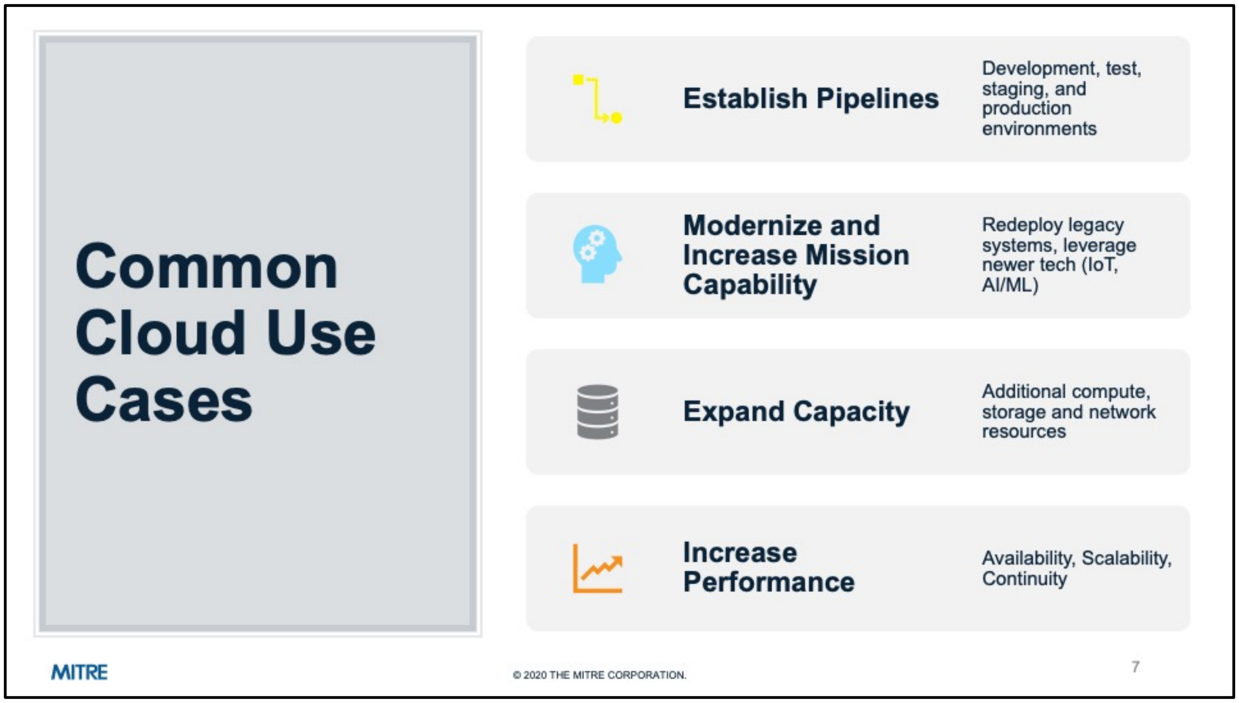
Private
- Single User Only
- On or Off premise

Hybrid
- Tightly coupled set of clouds
- Mission Owner & CSP may jointly control

Multi-Cloud
- Use of multiple cloud computing and storage services in a heterogeneous architecture - **NOT Defined by NIST**

MITRE

Slide Source: MITRE



Common Cloud Use Cases

Establish Pipelines
Development, test, staging, and production environments

Modernize and Increase Mission Capability
Redeploy legacy systems, leverage newer tech (IoT, AI/ML)

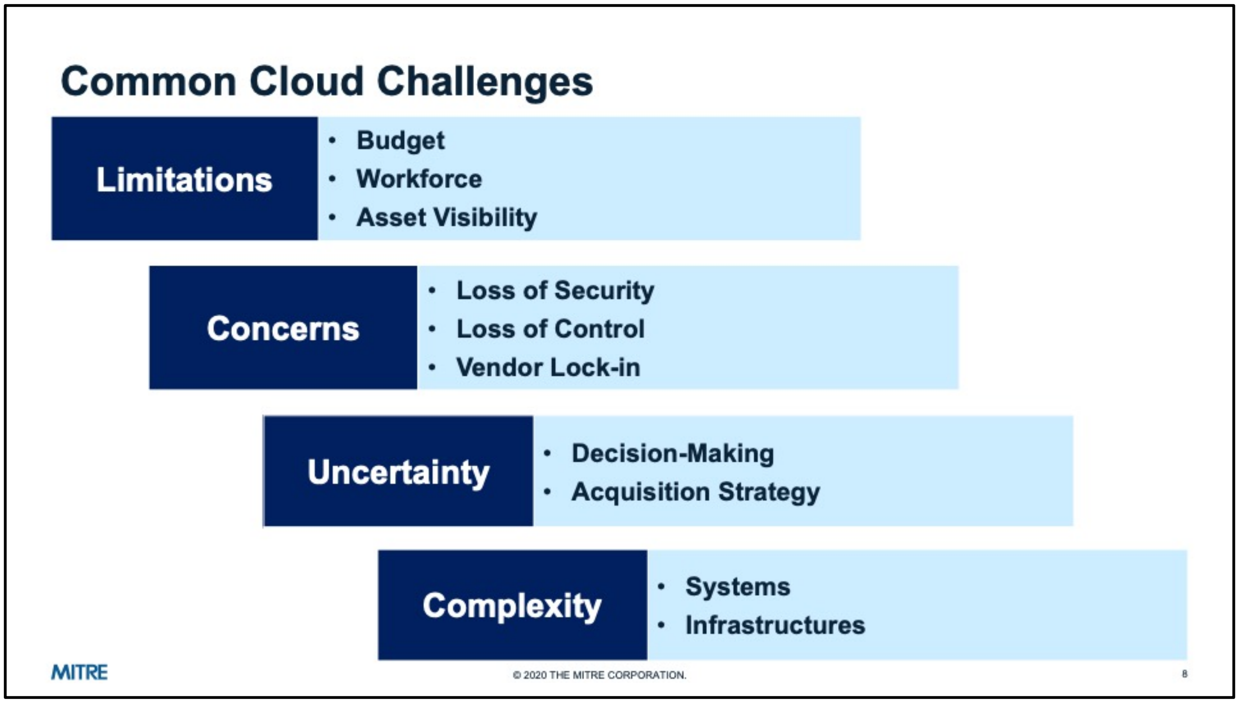
Expand Capacity
Additional compute, storage and network resources

Increase Performance
Availability, Scalability, Continuity

MITRE

7

Slide Source: MITRE



Common Cloud Challenges

Limitations
- Budget
- Workforce
- Asset Visibility

Concerns
- Loss of Security
- Loss of Control
- Vendor Lock-in

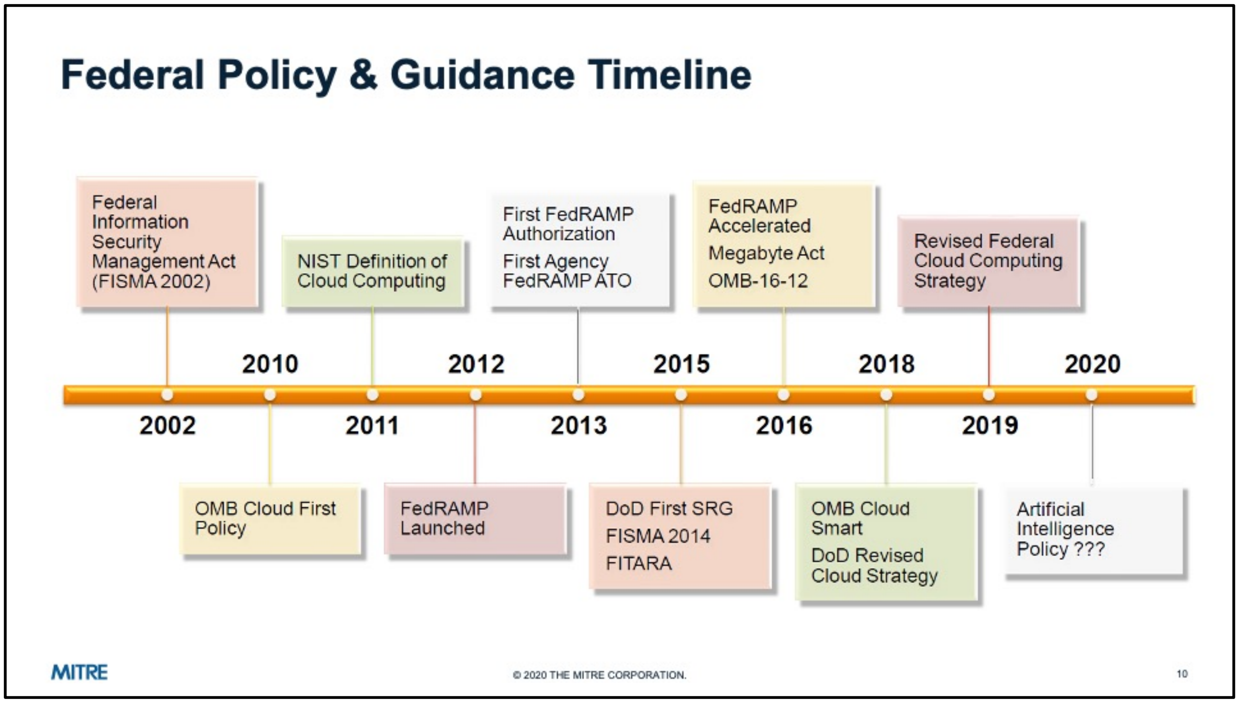
Uncertainty
- Decision-Making
- Acquisition Strategy

Complexity
- Systems
- Infrastructures

MITRE

Slide Source: MITRE

Policy and Strategy



Federal Policy & Guidance Timeline

2002

Federal Information Security Management Act (FISMA 2002)

2010

OMB Cloud First Policy

2011

NIST Definition of Cloud Computing

2012

FedRAMP Launched

2013

First FedRAMP Authorization

First Agency FedRAMP ATO

2015

DoD First SRG

FISMA 2014

FITARA

2016

FedRAMP Accelerated

Megabyte Act

OMB-16-12

2018

OMB Cloud Smart

DoD Revised Cloud Strategy

2019

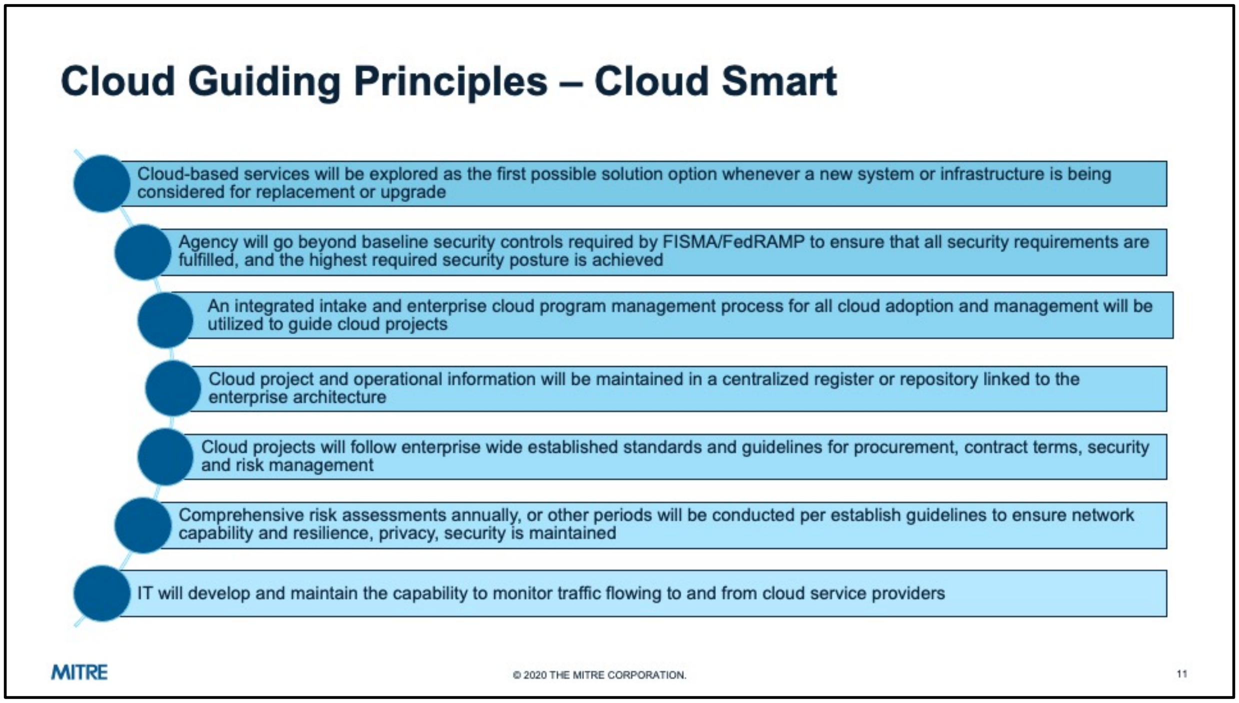
Revised Federal Cloud Computing Strategy

2020

Artificial Intelligence Policy ???

MITRE

Slide Source: MITRE



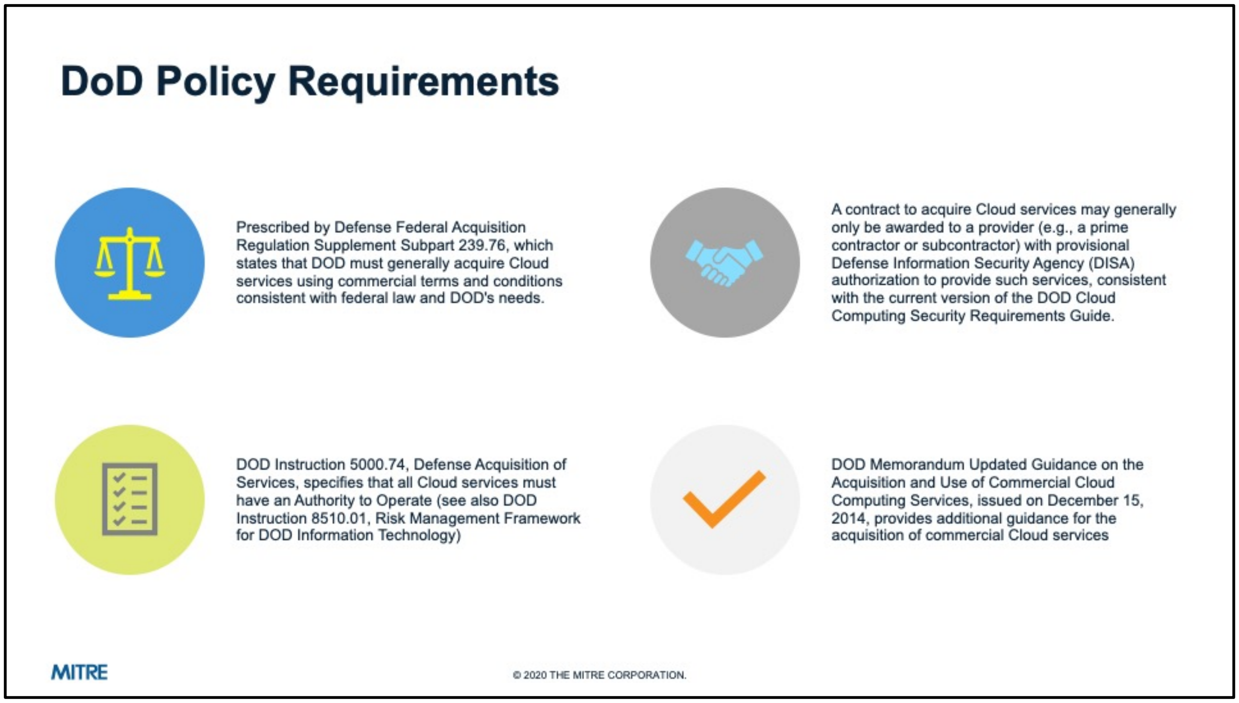
Cloud Guiding Principles – Cloud Smart

- Cloud-based services will be explored as the first possible solution option whenever a new system or infrastructure is being considered for replacement or upgrade
- Agency will go beyond baseline security controls required by FISMA/FedRAMP to ensure that all security requirements are fulfilled, and the highest required security posture is achieved
- An integrated intake and enterprise cloud program management process for all cloud adoption and management will be utilized to guide cloud projects
- Cloud project and operational information will be maintained in a centralized register or repository linked to the enterprise architecture
- Cloud projects will follow enterprise wide established standards and guidelines for procurement, contract terms, security and risk management
- Comprehensive risk assessments annually, or other periods will be conducted per establish guidelines to ensure network capability and resilience, privacy, security is maintained
- IT will develop and maintain the capability to monitor traffic flowing to and from cloud service providers

MITRE

Slide Source: MITRE

Cloud First (2011) evolved to Cloud Smart (2019)



DoD Policy Requirements

Prescribed by Defense Federal Acquisition Regulation Supplement Subpart 239.76, which states that DOD must generally acquire Cloud services using commercial terms and conditions consistent with federal law and DOD's needs.

A contract to acquire Cloud services may generally only be awarded to a provider (e.g., a prime contractor or subcontractor) with provisional Defense Information Security Agency (DISA) authorization to provide such services, consistent with the current version of the DOD Cloud Computing Security Requirements Guide.

DOD Instruction 5000.74, Defense Acquisition of Services, specifies that all Cloud services must have an Authority to Operate (see also DOD Instruction 8510.01, Risk Management Framework for DOD Information Technology)

DOD Memorandum Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, issued on December 15, 2014, provides additional guidance for the acquisition of commercial Cloud services

MITRE

Slide Source: MITRE

Source: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services (2014) [2]

DoD Cloud Acquisition Business Requirements:

Analyze Cloud Services using DoD Memorandum, "Use of Enterprise Information Technology Standard Business Case Analysis," October 23, 2014.

DISA provided cloud services must be considered as part of the BCA.

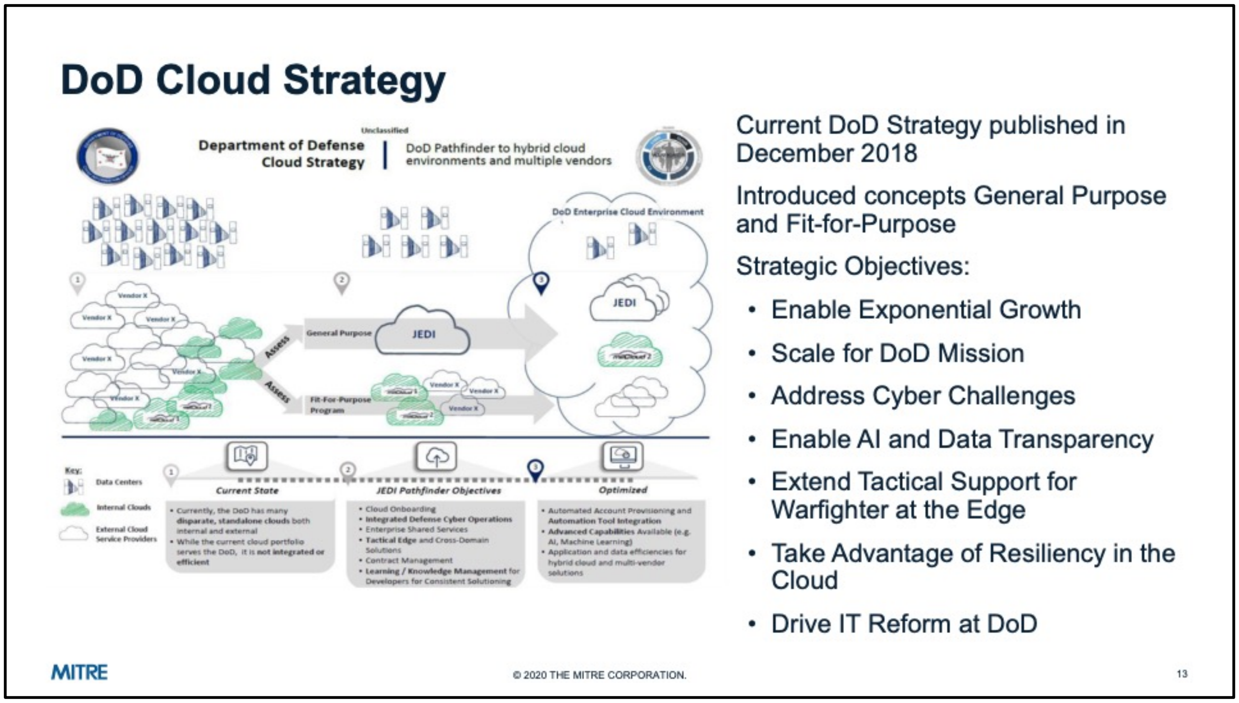
DoD Cloud Acquisition Security Requirements:

Publicly released, Unclassed DoD information may be hosted on FedRAMP approved cloud services.

For more sensitive data, cloud providers must consult the DoD Cloud Computing Security Requirements Guide (SRG) and receive a DoD Provisional Authorization (PA).

Commercial cloud services for Sensitive Data must be connected to customers through a Cloud Access Point provided by DISA or through a CAP provided by another DoD Components

Components are responsible for cyberspace defense of all information and missions hosted in commercial cloud services. Requires collaboration and information sharing among the component, DISA, and the CSP.



DoD Cloud Strategy

Current State

- Currently, the DoD has many **disparate, standalone clouds** both internal and external
- While the current cloud portfolio serves the DoD, it is **not integrated or efficient**

JEDI Pathfinder Objectives

- Cloud Onboarding
- **Integrated Defense Cyber Operations**
- Enterprise Shared Services
- **Tactical Edge** and Cross-Domain Solutions
- Contract Management
- **Learning / Knowledge Management** for Developers for Consistent Solutioning

Optimized

- Automated Account Provisioning and **Automation Tool Integration**
- **Advanced Capabilities** Available (e.g. AI, Machine Learning)
- Application and data efficiencies for hybrid cloud and multi-vendor solutions

Current DoD Strategy published in December 2018

Introduced concepts General Purpose and Fit-for-Purpose

Strategic Objectives:

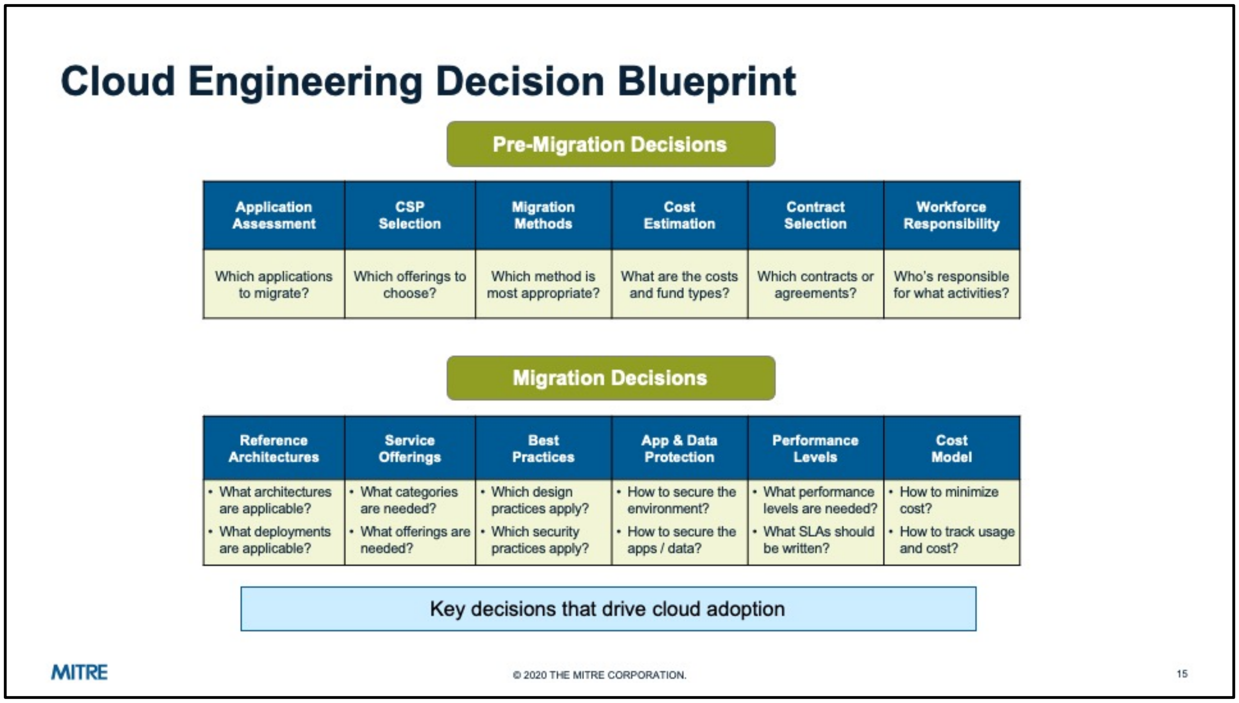
- Enable Exponential Growth
- Scale for DoD Mission
- Address Cyber Challenges
- Enable AI and Data Transparency
- Extend Tactical Support for Warfighter at the Edge
- Take Advantage of Resiliency in the Cloud
- Drive IT Reform at DoD

MITRE

Slide Source: DoD Cloud Strategy [3]

Note: Current status of protests with JEDI and DEOS are slowly getting resolved, however, effective implementation is still somewhat uncertain
Fit-for-Purpose – when General Purpose cloud can not support mission. Requires approval from the DoD CIO. Should be developed to support the enterprise

Adoption/Migration



Cloud Engineering Decision Blueprint

Pre-Migration Decisions

Application Assessment	CSP Selection	Migration Methods	Cost Estimation	Contract Selection	Workforce Responsibility
Which applications to migrate?	Which offerings to choose?	Which method is most appropriate?	What are the costs and fund types?	Which contracts or agreements?	Who's responsible for what activities?

Migration Decisions

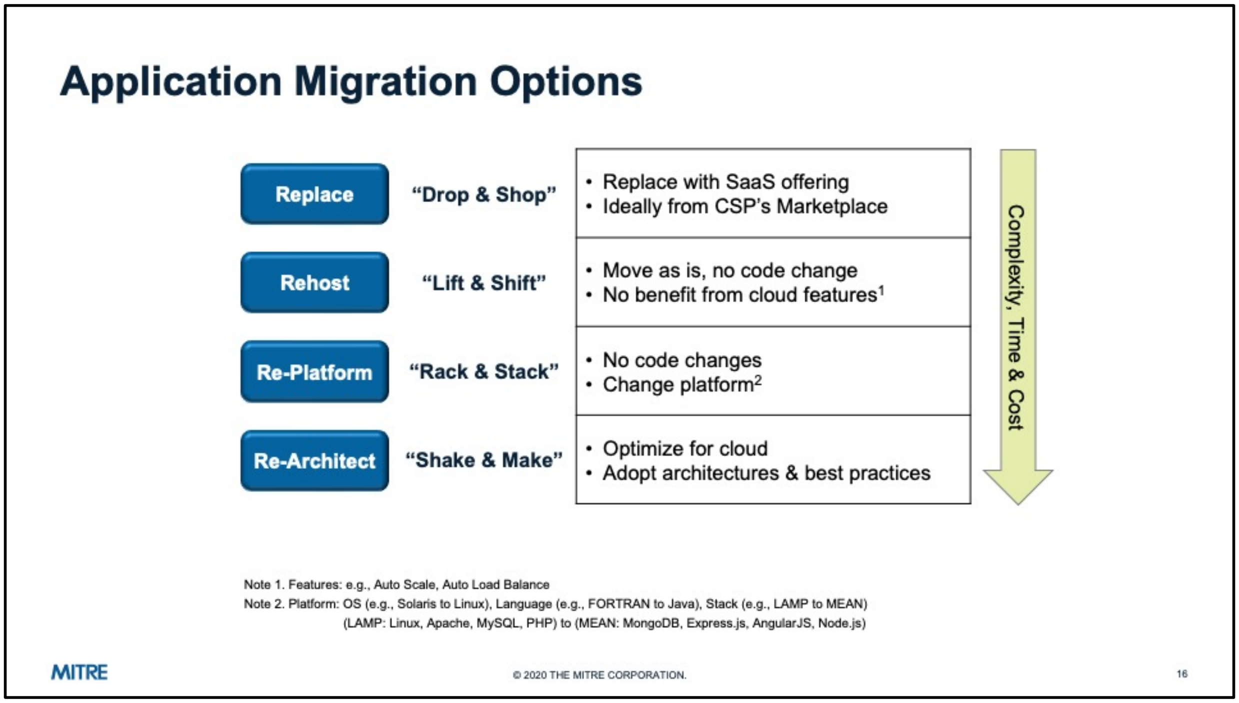
Reference Architectures	Service Offerings	Best Practices	App & Data Protection	Performance Levels	Cost Model
• What architectures are applicable? • What deployments are applicable?	• What categories are needed? • What offerings are needed?	• Which design practices apply? • Which security practices apply?	• How to secure the environment? • How to secure the apps / data?	• What performance levels are needed? • What SLAs should be written?	• How to minimize cost? • How to track usage and cost?

Key decisions that drive cloud adoption

MITRE

15

Slide Source: MITRE



Application Migration Options

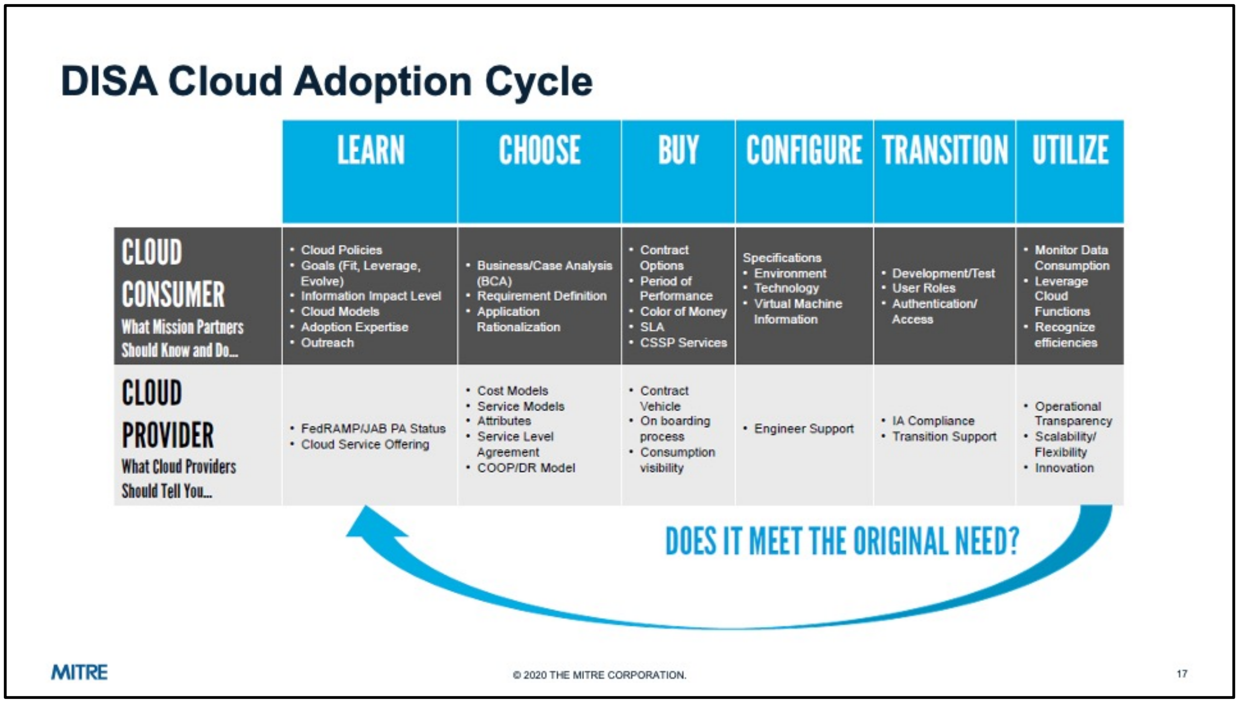
Replace	"Drop & Shop"	• Replace with SaaS offering • Ideally from CSP's Marketplace
Rehost	"Lift & Shift"	• Move as is, no code change • No benefit from cloud features[1]
Re-Platform	"Rack & Stack"	• No code changes • Change platform[2]
Re-Architect	"Shake & Make"	• Optimize for cloud • Adopt architectures & best practices

Note 1. Features: e.g., Auto Scale, Auto Load Balance

Note 2. Platform: OS (e.g., Solaris to Linux), Language (e.g., FORTRAN to Java), Stack (e.g., LAMP to MEAN)
(LAMP: Linux, Apache, MySQL, PHP) to (MEAN: MongoDB, Express.js, AngularJS, Node.js)

MITRE

Slide Source: MITRE



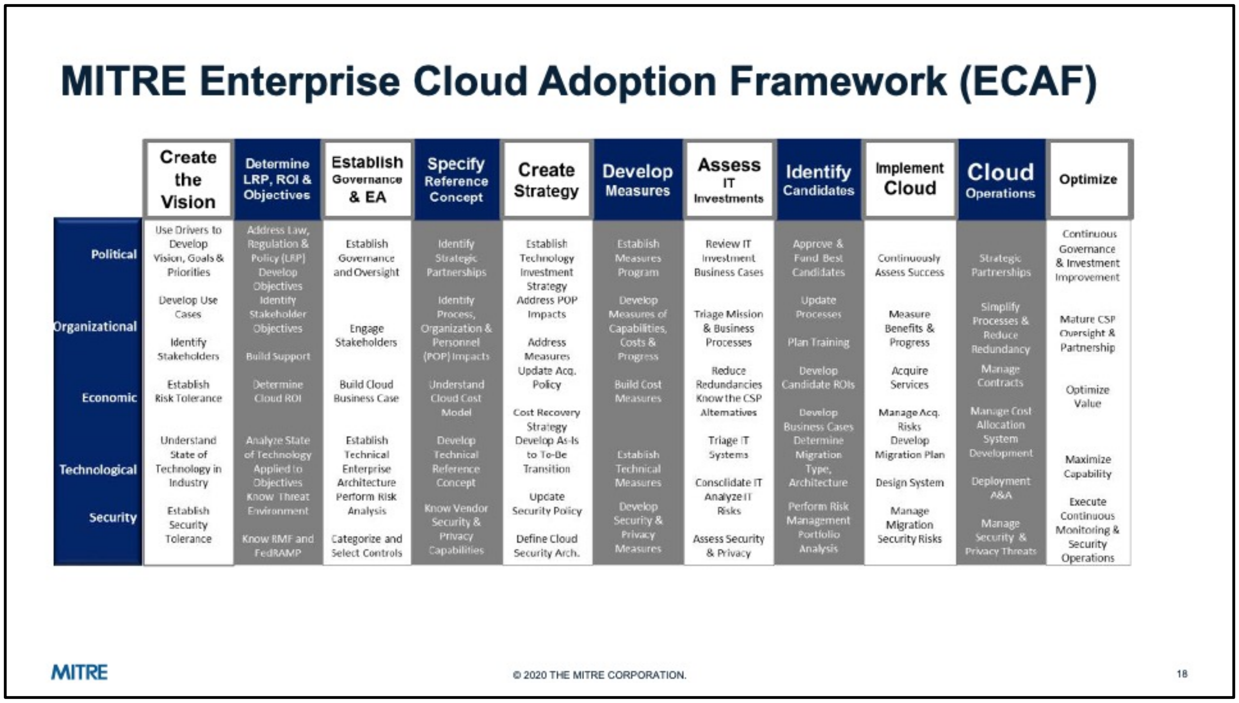
DISA Cloud Adoption Cycle

	LEARN	CHOOSE	BUY	CONFIGURE	TRANSITION	UTILIZE
CLOUD CONSUMER What Mission Partners Should Know and Do…	• Cloud Policies • Goals (Fit, Leverage, Evolve) • Information Impact Level • Cloud Models • Adoption Expertise • Outreach	• Business/Case Analysis (BCA) • Requirement Definition • Application Rationalization	• Contract Options • Period of Performance • Color of Money • SLA • CSSP Services	Specifications • Environment • Technology • Virtual Machine Information	• Development/Test • User Roles • Authentication/ Access	• Monitor Data Consumption • Leverage Cloud Functions • Recognize efficiencies
CLOUD PROVIDER What Cloud Providers Should Tell You…	• FedRAMP/JAB PA Status • Cloud Service Offering	• Cost Models • Service Models • Attributes • Service Level Agreement • COOP/DR Model	• Contract Vehicle • On boarding process • Consumption visibility	• Engineer Support	• IA Compliance • Transition Support	• Operational Transparency • Scalability/ Flexibility • Innovation

MITRE

17

Slide Source: DISA-Cloud-Playbook-v2.pdf [4]



MITRE Enterprise Cloud Adoption Framework (ECAF)

	Create the Vision	Determine LRP, ROI & Objectives	Establish Governance & EA	Specify Reference Concept	Create Strategy	Develop Measures	Assess IT Investments	Identify Candidates	Implement Cloud	Cloud Operations	Optimize
Political	Use Drivers to Develop Vision, Goals & Priorities	Address Law, Regulation & Policy (LRP) Develop Objectives	Establish Governance and Oversight	Identify Strategic Partnerships	Establish Technology Investment Strategy	Establish Measures Program	Review IT Investment Business Cases	Approve & Fund Best Candidates	Continuously Assess Success	Strategic Partnerships	Continuous Governance & Investment Improvement
Organizational	Develop Use Cases Identify Stakeholders	Identify Stakeholder Objectives Build Support	Engage Stakeholders	Identify Process, Organization & Personnel (POP) Impacts	Address POP Impacts Address Measures	Develop Measures of Capabilities, Costs & Progress	Triage Mission & Business Processes	Update Processes Plan Training	Measure Benefits & Progress	Simplify Processes & Reduce Redundancy	Mature CSP Oversight & Partnership
Economic	Establish Risk Tolerance	Determine Cloud ROI	Build Cloud Business Case	Understand Cloud Cost Model	Update Acq. Policy Cost Recovery Strategy	Build Cost Measures	Reduce Redundancies Know the CSP Alternatives	Develop Candidate ROIs Develop Business Cases	Acquire Services Manage Acq. Risks	Manage Contracts Manage Cost Allocation	Optimize Value
Technological	Understand State of Technology in Industry	Analyze State of Technology Applied to Objectives	Establish Technical Enterprise Architecture	Develop Technical Reference Concept	Develop As-Is to To-Be Transition	Establish Technical Measures	Triage IT Systems Consolidate IT	Determine Migration Type, Architecture	Develop Migration Plan Design System	System Development Deployment A&A	Maximize Capability
Security	Establish Security Tolerance	Know Threat Environment Know RMF and FedRAMP	Perform Risk Analysis Categorize and Select Controls	Know Vendor Security & Privacy Capabilities	Update Security Policy Define Cloud Security Arch.	Develop Security & Privacy Measures	Analyze IT Risks Assess Security & Privacy	Perform Risk Management Portfolio Analysis	Manage Migration Security Risks	Manage Security & Privacy Threats	Execute Continuous Monitoring & Security Operations

MITRE

18

Slide Source: MITRE

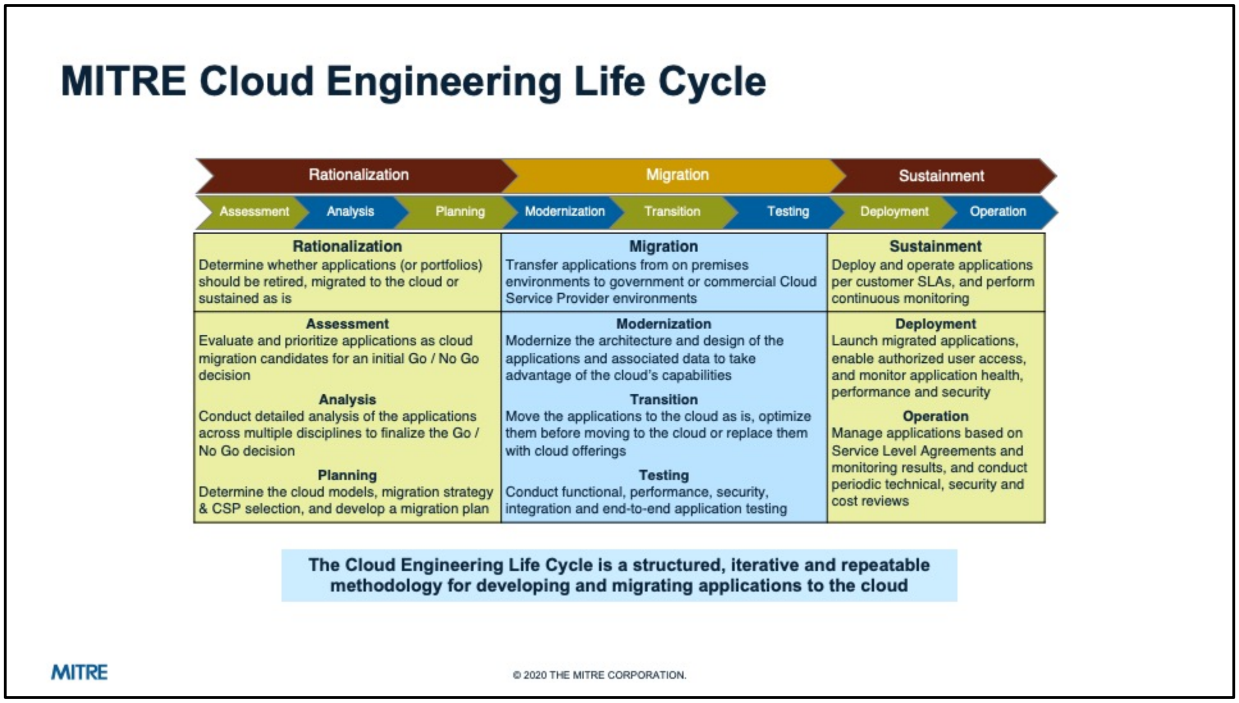
Creating Vision, Goals & Priorities is key to adoption success & should be done first
ECAF can be used as an assessment tool to determine areas of strengths & weaknesses
Identifies interactions & inter-dependence of activities to successfully adopt cloud
Flexible & iterative, activities may be revisited as necessary

Not a schedule, some activities may be quick, other may be projects

Not all areas of the framework may be necessary for every sponsor or situation

Some activities may already be cloud ready

Not performing an activity potentially increases risks



MITRE Cloud Engineering Life Cycle

Rationalization → Migration → Sustainment

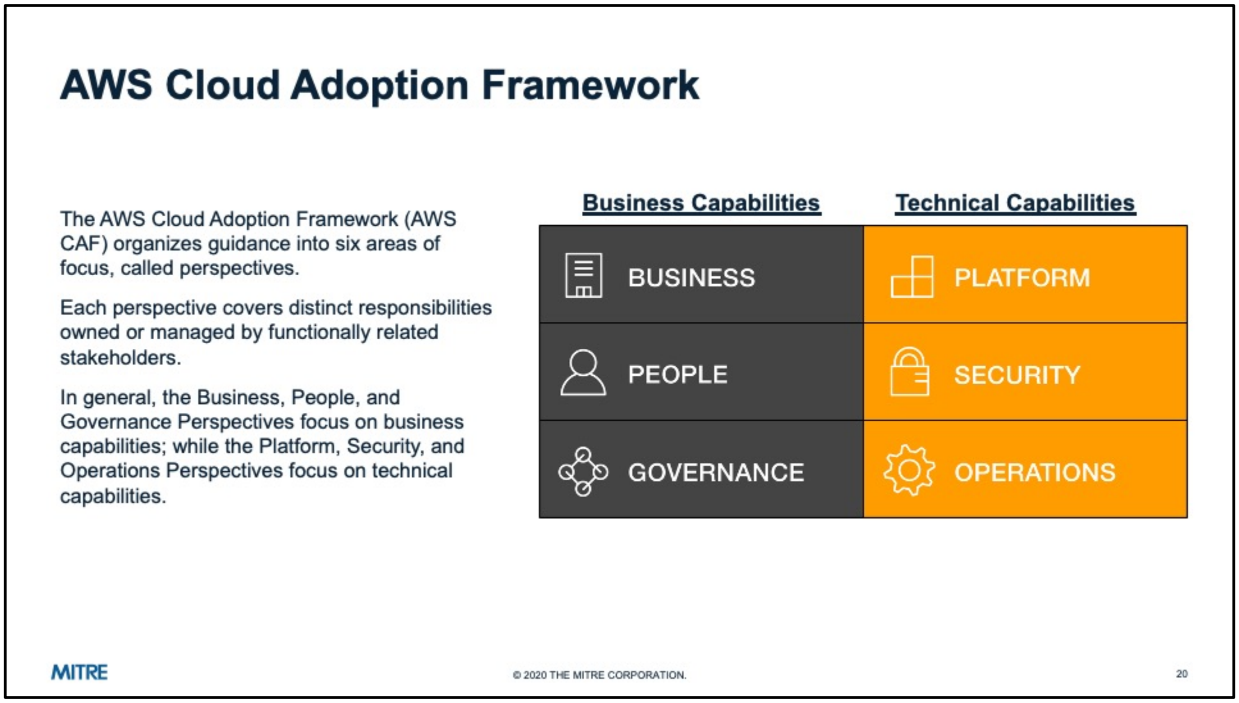
Assessment → Analysis → Planning → Modernization → Transition → Testing → Deployment → Operation

Rationalization Determine whether applications (or portfolios) should be retired, migrated to the cloud or sustained as is	**Migration** Transfer applications from on premises environments to government or commercial Cloud Service Provider environments	**Sustainment** Deploy and operate applications per customer SLAs, and perform continuous monitoring
Assessment Evaluate and prioritize applications as cloud migration candidates for an initial Go / No Go decision **Analysis** Conduct detailed analysis of the applications across multiple disciplines to finalize the Go / No Go decision **Planning** Determine the cloud models, migration strategy & CSP selection, and develop a migration plan	**Modernization** Modernize the architecture and design of the applications and associated data to take advantage of the cloud's capabilities **Transition** Move the applications to the cloud as is, optimize them before moving to the cloud or replace them with cloud offerings **Testing** Conduct functional, performance, security, integration and end-to-end application testing	**Deployment** Launch migrated applications, enable authorized user access, and monitor application health, performance and security **Operation** Manage applications based on Service Level Agreements and monitoring results, and conduct periodic technical, security and cost reviews

The Cloud Engineering Life Cycle is a structured, iterative and repeatable methodology for developing and migrating applications to the cloud

MITRE

Slide Source: MITRE



AWS Cloud Adoption Framework

The AWS Cloud Adoption Framework (AWS CAF) organizes guidance into six areas of focus, called perspectives.

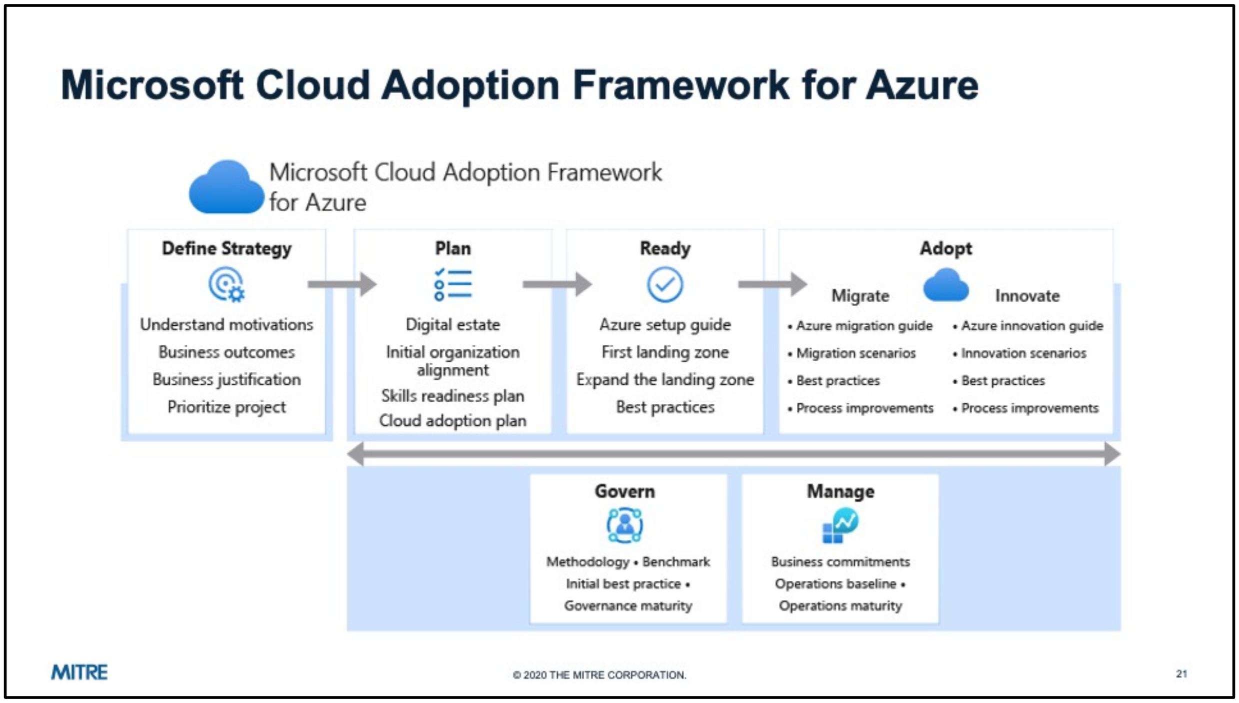
Each perspective covers distinct responsibilities owned or managed by functionally related stakeholders.

In general, the Business, People, and Governance Perspectives focus on business capabilities; while the Platform, Security, and Operations Perspectives focus on technical capabilities.

Business Capabilities	**Technical Capabilities**
BUSINESS	PLATFORM
PEOPLE	SECURITY
GOVERNANCE	OPERATIONS

MITRE

Slide Source:
https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf [5]



Microsoft Cloud Adoption Framework for Azure

Microsoft Cloud Adoption Framework for Azure

Define Strategy

Understand motivations
Business outcomes
Business justification
Prioritize project

Plan

Digital estate
Initial organization alignment
Skills readiness plan
Cloud adoption plan

Ready

Azure setup guide
First landing zone
Expand the landing zone
Best practices

Adopt

Migrate

- Azure migration guide
- Migration scenarios
- Best practices
- Process improvements

Innovate

- Azure innovation guide
- Innovation scenarios
- Best practices
- Process improvements

Govern

Methodology • Benchmark
Initial best practice •
Governance maturity

Manage

Business commitments
Operations baseline •
Operations maturity

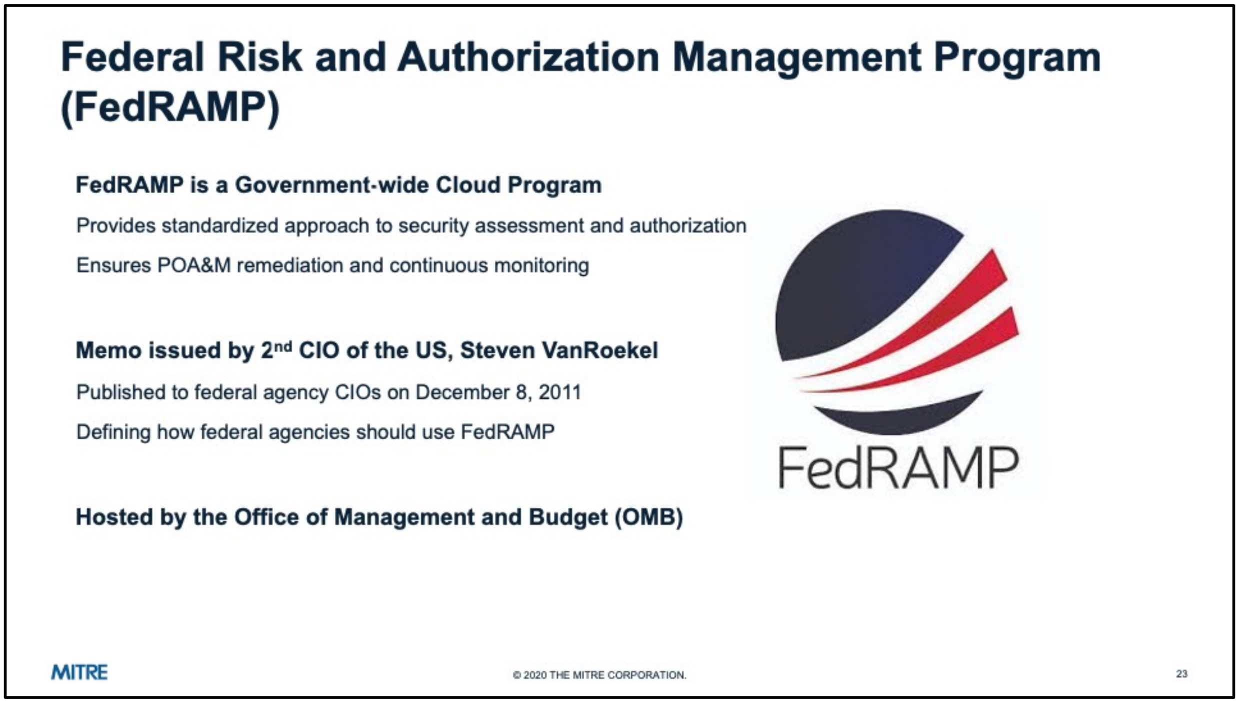
MITRE

© 2020 THE MITRE CORPORATION.

21

Slide Source: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview [6]

Security



Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a Government-wide Cloud Program

Provides standardized approach to security assessment and authorization

Ensures POA&M remediation and continuous monitoring

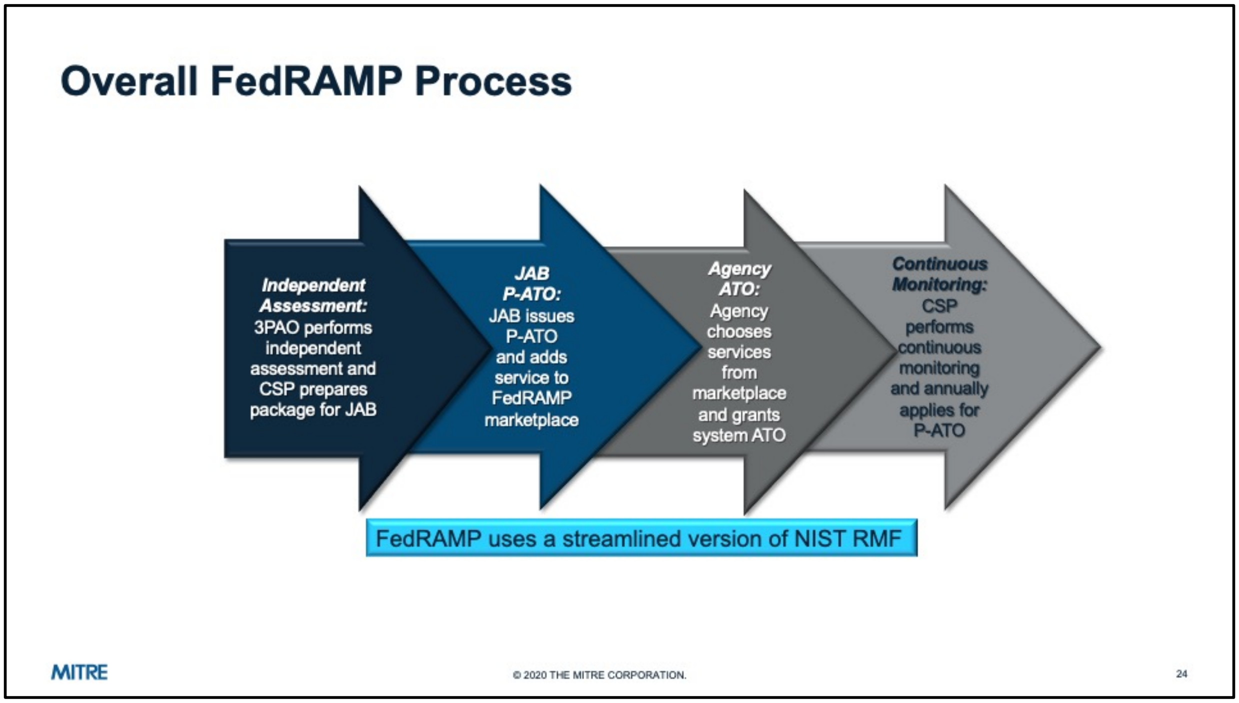
Memo issued by 2nd CIO of the US, Steven VanRoekel

Published to federal agency CIOs on December 8, 2011

Defining how federal agencies should use FedRAMP

Hosted by the Office of Management and Budget (OMB)

Slide Source: MITRE



Overall FedRAMP Process

Independent Assessment: 3PAO performs independent assessment and CSP prepares package for JAB

JAB P-ATO: JAB issues P-ATO and adds service to FedRAMP marketplace

Agency ATO: Agency chooses services from marketplace and grants system ATO

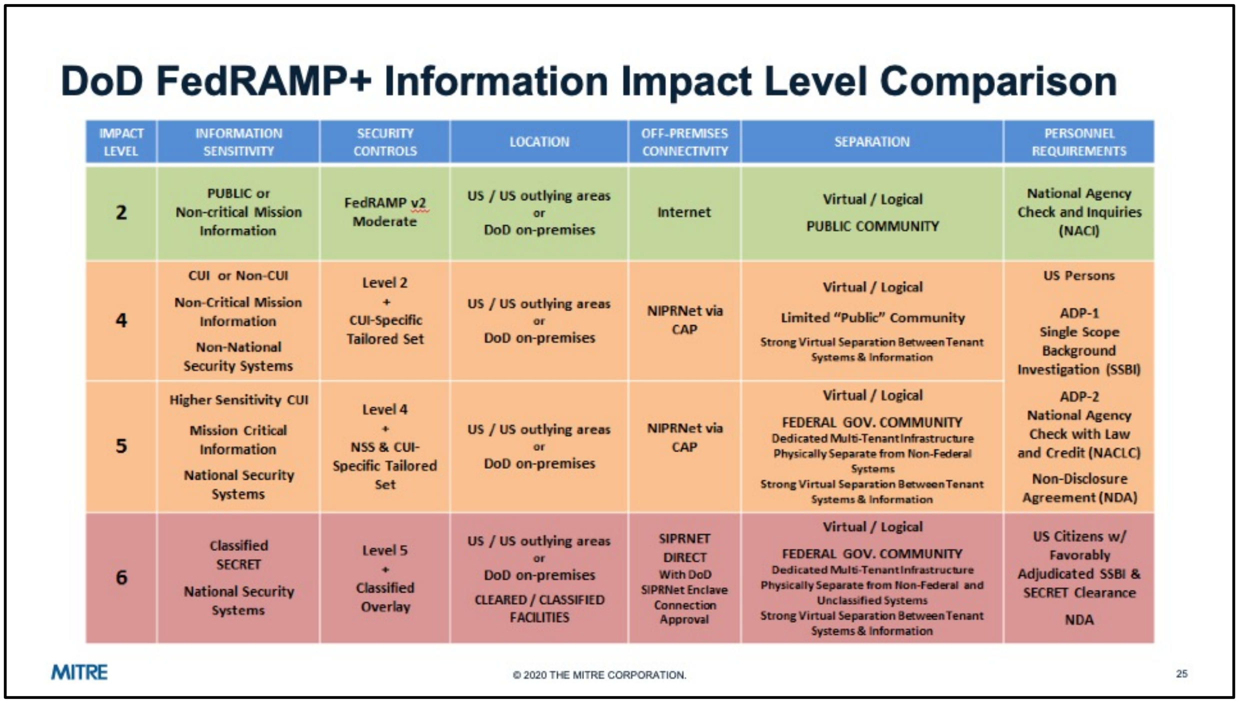
Continuous Monitoring: CSP performs continuous monitoring and annually applies for P-ATO

FedRAMP uses a streamlined version of NIST RMF

MITRE

Slide Source: MITRE

3PAO: Third-party assessment organization
P-ATO: Provisional Authority to Operate
JAB: (FedRAMP) Joint Assessment Board



DoD FedRAMP+ Information Impact Level Comparison

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI) ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

MITRE

25

Slide Source: DoD Cloud Computing Security Requirements Guide, Version 1, Release 3 [7]

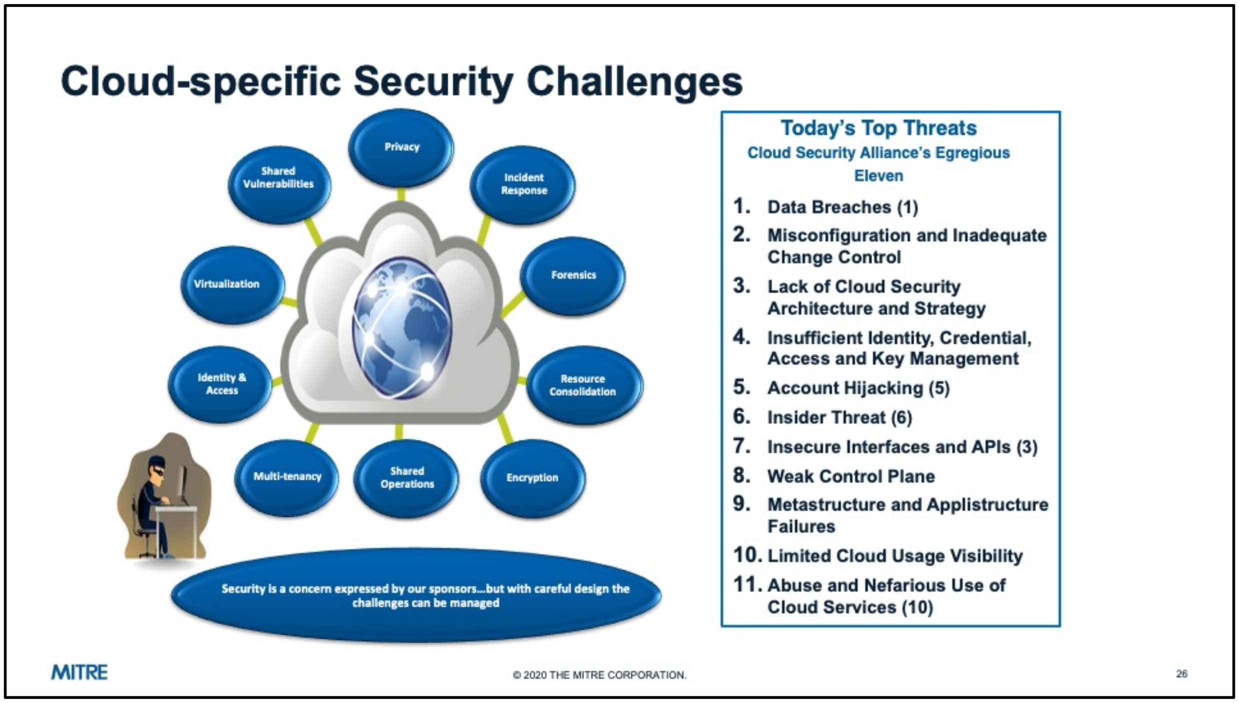
Accreditation Process:

1. FedRAMP - a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the Federal Government.
2. FedRAMP+ - the concept of leveraging the work done as part of the FedRAMP assessment and adding specific security controls and requirements necessary to meet and assure DoD's critical mission requirements.
3. DoD Provisional Authorization (PA) - an acknowledgement of risk based on an evaluation of the CSP's CSO and the potential for risk introduced to DoD networks.

Cloud security information impact levels are defined by the combination of:

1) the sensitivity or confidentiality level of information (e.g., public, private, classified, etc.) to be stored and processed in the CSP environment; and
2) the potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information.

IL2: Accommodates DoD information that has been approved for public release (Low confidentiality, Moderate Integrity)
IL4: Accommodates DoD Controlled Unclassified Information (CUI) (e.g., FOUO)
IL5: Accommodates DoD CUI and National Security Systems (NSS)
IL6: Accommodates DoD Classified Information up to SECRET



Cloud-specific Security Challenges

Privacy

Incident Response

Forensics

Resource Consolidation

Encryption

Shared Operations

Multi-tenancy

Identity & Access

Virtualization

Shared Vulnerabilities

Security is a concern expressed by our sponsors…but with careful design the challenges can be managed

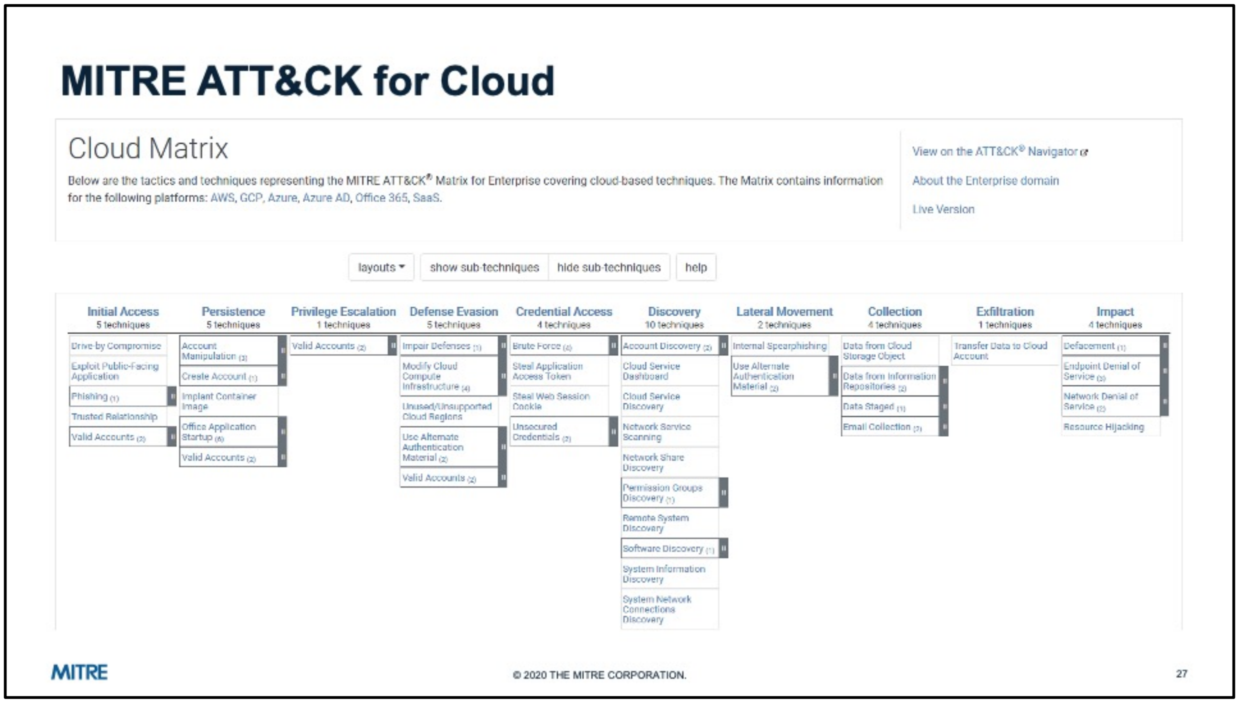
Today's Top Threats

Cloud Security Alliance's Egregious Eleven

1. Data Breaches (1)
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking (5)
6. Insider Threat (6)
7. Insecure Interfaces and APIs (3)
8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services (10)

MITRE

Slide Source: MITRE
Slide Source: [8]



MITRE ATT&CK for Cloud

Cloud Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the following platforms: AWS, GCP, Azure, Azure AD, Office 365, SaaS.

View on the ATT&CK® Navigator

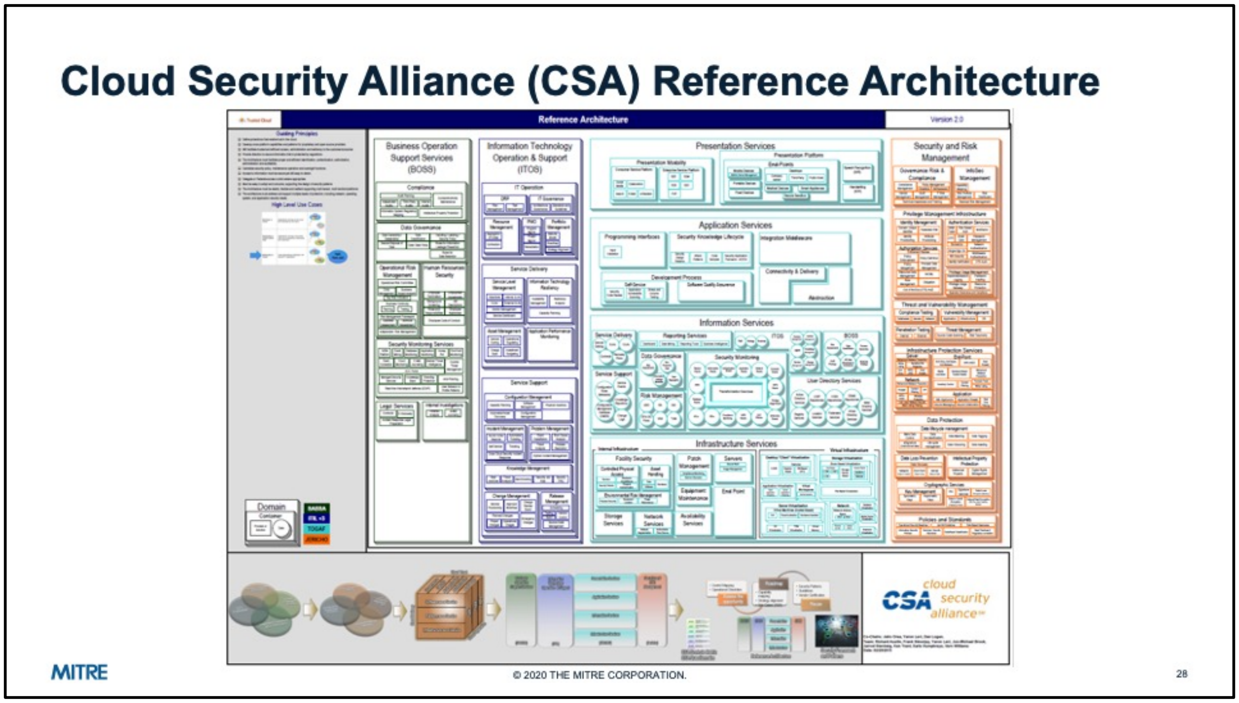
About the Enterprise domain

Live Version

Initial Access 5 techniques	Persistence 5 techniques	Privilege Escalation 1 techniques	Defense Evasion 5 techniques	Credential Access 4 techniques	Discovery 10 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 4 techniques
Drive-by Compromise	Account Manipulation (3)	Valid Accounts (2)	Impair Defenses (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Cloud Storage Object	Transfer Data to Cloud Account	Defacement (1)
Exploit Public-Facing Application	Create Account (1)		Modify Cloud Compute Infrastructure (4)	Steal Application Access Token	Cloud Service Dashboard	Use Alternate Authentication Material (2)	Data from Information Repositories (2)		Endpoint Denial of Service (3)
Phishing (1)	Implant Container Image		Unused/Unsupported Cloud Regions	Steal Web Session Cookie	Cloud Service Discovery		Data Staged (1)		Network Denial of Service (2)
Trusted Relationship	Office Application Startup (6)		Use Alternate Authentication Material (2)	Unsecured Credentials (2)	Network Service Scanning		Email Collection (2)		Resource Hijacking
Valid Accounts (2)	Valid Accounts (2)		Valid Accounts (2)		Network Share Discovery				
					Permission Groups Discovery (1)				
					Remote System Discovery				
					Software Discovery (1)				
					System Information Discovery				
					System Network Connections Discovery				

MITRE

Slide Source: https://attack.mitre.org/matrices/enterprise/cloud/ [9]



Cloud Security Alliance (CSA) Reference Architecture

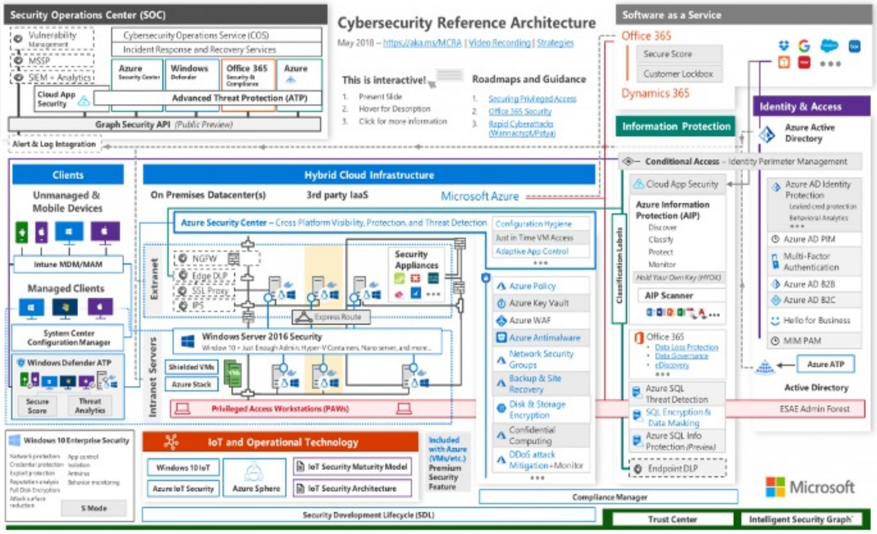
MITRE

© 2020 THE MITRE CORPORATION.

28

Slide Source: Enterprise Architecture v2.0 [10]

MS Azure Security Architecture



Security Operations Center (SOC)

Vulnerability Management

MSSP

SIEM + Analytics

Cybersecurity Operations Service (COS)

Incident Response and Recovery Services

Azure Security Center

Windows Defender

Office 365 Security & Compliance

Azure

Cloud App Security

Advanced Threat Protection (ATP)

Graph Security API *(Public Preview)*

Alert & Log Integration

Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365

Secure Score

Customer Lockbox

Dynamics 365

Information Protection

Identity & Access

Azure Active Directory

Conditional Access – Identity Perimeter Management

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Windows Defender ATP

Secure Score

Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s)

3rd party IaaS

Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Configuration Hygiene

Just in Time VM Access

Adaptive App Control

Extranet

NGFW

Edge DLP

SSL Proxy

IPS

Security Appliances

Express Route

Intranet Servers

Windows Server 2016 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more…

Shielded VMs

Azure Stack

Privileged Access Workstations (PAWs)

Azure Policy

Azure Key Vault

Azure WAF

Azure Antimalware

Network Security Groups

Backup & Site Recovery

Disk & Storage Encryption

Confidential Computing

DDoS attack Mitigation+Monitor

Classification Labels

Cloud App Security

Azure Information Protection (AIP)

Discover

Classify

Protect

Monitor

Hold Your Own Key (HYOK)

AIP Scanner

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection (Preview)

Endpoint DLP

Azure AD Identity Protection

Leaked cred protection

Behavioral Analytics

Azure AD PIM

Multi-Factor Authentication

Azure AD B2B

Azure AD B2C

Hello for Business

MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Windows 10 Enterprise Security

Network protection

Credential protection

Exploit protection

Reputation analysis

Full Disk Encryption

Attack surface reduction

App control

Isolation

Antivirus

Behavior monitoring

S Mode

IoT and Operational Technology

Windows 10 IoT

Azure IoT Security

Azure Sphere

IoT Security Maturity Model

IoT Security Architecture

Included with Azure (VMs/etc.)

Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center

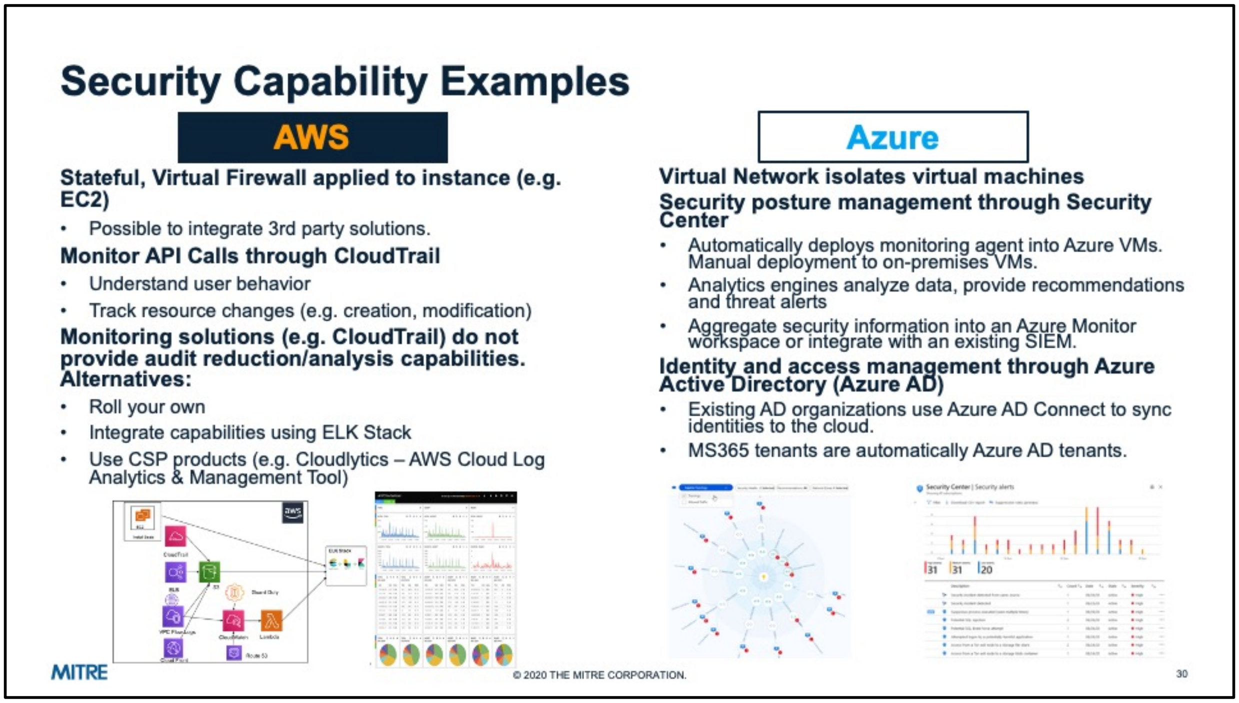
Intelligent Security Graph

Microsoft

MITRE

© 2020 THE MITRE CORPORATION.

Slide Source: https://www.microsoft.com/security/blog/2018/06/06/cybersecurity-reference-architecture-security-for-a-hybrid-enterprise/ [11]



Security Capability Examples

AWS

Stateful, Virtual Firewall applied to instance (e.g. EC2)

- Possible to integrate 3rd party solutions.

Monitor API Calls through CloudTrail

- Understand user behavior
- Track resource changes (e.g. creation, modification)

Monitoring solutions (e.g. CloudTrail) do not provide audit reduction/analysis capabilities. Alternatives:

- Roll your own
- Integrate capabilities using ELK Stack
- Use CSP products (e.g. Cloudlytics – AWS Cloud Log Analytics & Management Tool)

Azure

Virtual Network isolates virtual machines

Security posture management through Security Center

- Automatically deploys monitoring agent into Azure VMs. Manual deployment to on-premises VMs.
- Analytics engines analyze data, provide recommendations and threat alerts
- Aggregate security information into an Azure Monitor workspace or integrate with an existing SIEM.

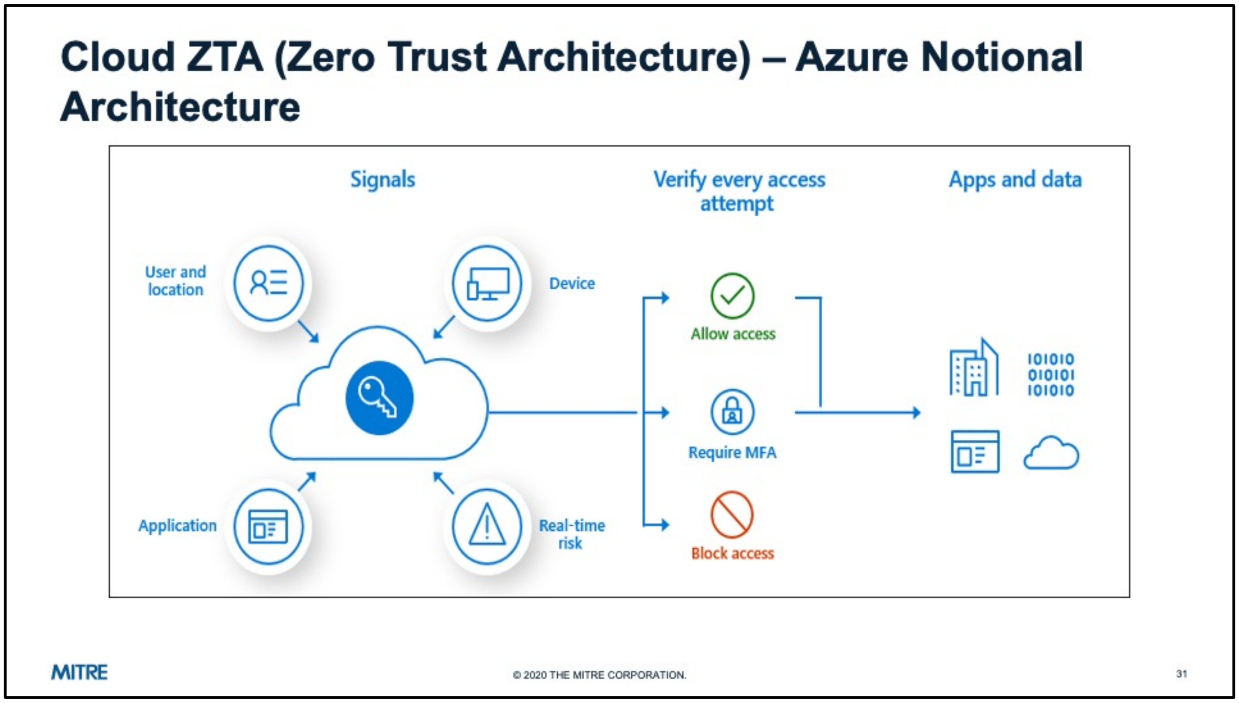
Identity and access management through Azure Active Directory (Azure AD)

- Existing AD organizations use Azure AD Connect to sync identities to the cloud.
- MS365 tenants are automatically Azure AD tenants.

MITRE

30

Slide Source: MITRE
Slide Source: https://azure.microsoft.com/en-us/services/security-center/ [12]
Slide Source: https://docs.microsoft.com/en-us/azure/security-center/security-center-intro [13]
Slide Source: https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad [14]



Cloud ZTA (Zero Trust Architecture) – Azure Notional Architecture

Signals

User and location

Device

Application

Real-time risk

Verify every access attempt

Allow access

Require MFA

Block access

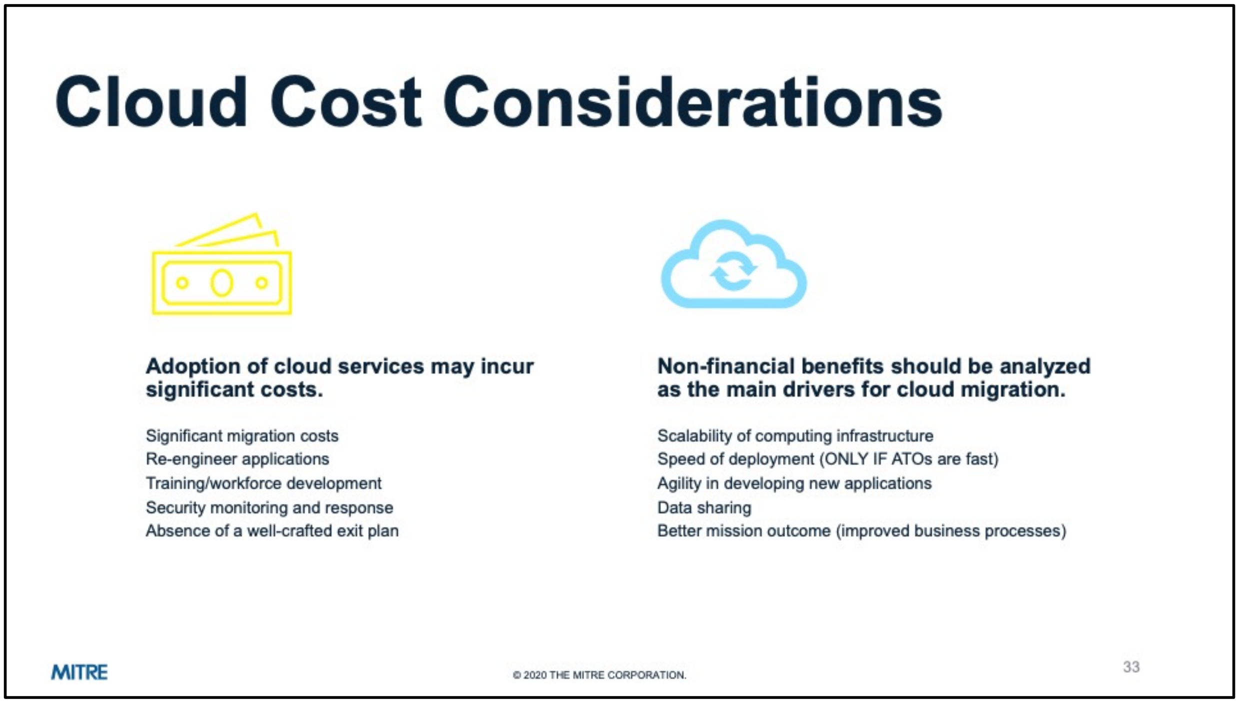
Apps and data

MITRE

31

Slide Source: https://devblogs.microsoft.com/azuregov/implementing-zero-trust-with-microsoft-azure-identity-and-access-management-1-of-6/ [15]

Economics



Cloud Cost Considerations

Adoption of cloud services may incur significant costs.

Significant migration costs
Re-engineer applications
Training/workforce development
Security monitoring and response
Absence of a well-crafted exit plan

Non-financial benefits should be analyzed as the main drivers for cloud migration.

Scalability of computing infrastructure
Speed of deployment (ONLY IF ATOs are fast)
Agility in developing new applications
Data sharing
Better mission outcome (improved business processes)

MITRE

33

Slide Source: MITRE

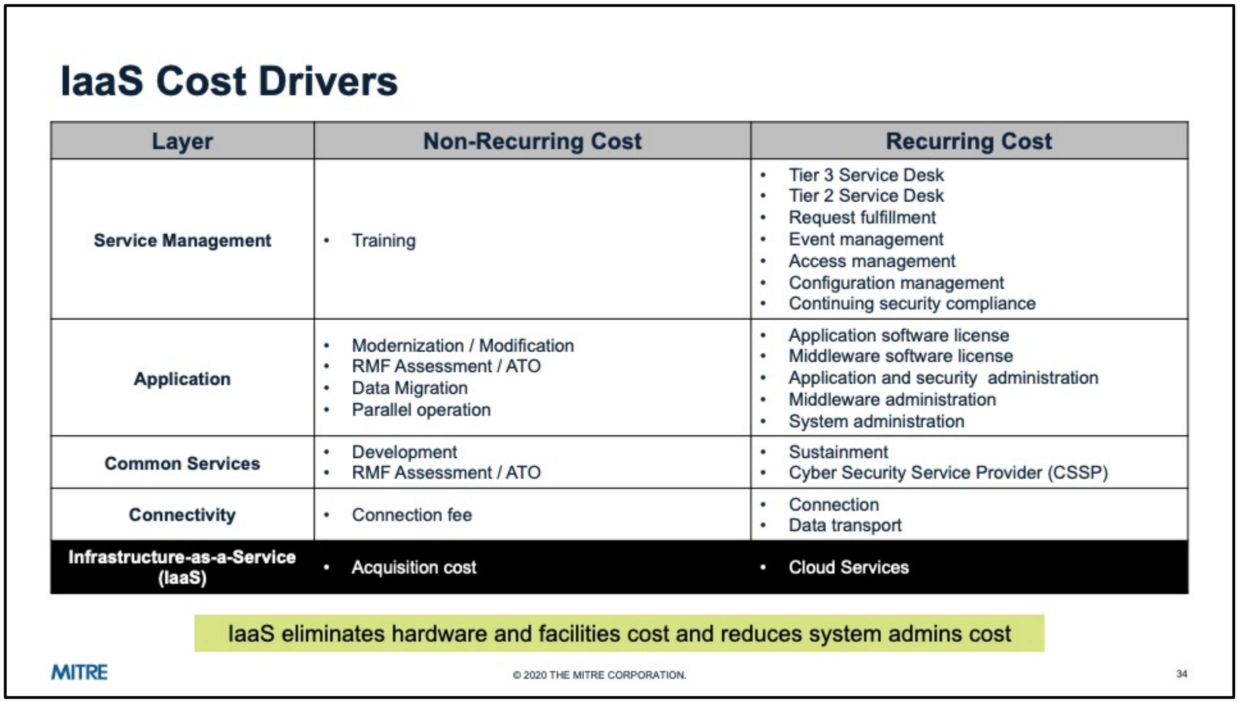
Katy Warren comment:

Hosting costs can be enormous if performed incorrectly or based on incorrect assumptions and data, well performed right-sizing is actually rare and difficult; real savings usually occurs when tech refreshes requires purchasing less computers
Use of FFP contracting tends to lead to more expensive cloud costs (i.e., contracting types influence costs)
Significant costs include:

- **training everyone on cloud**
- **business process changes**
- **changes in contractor and CSP contract management practices**
- **migration project costs**
- **poor acquisitions**
- **poor technical architecture**
- **security failures**

Benefits include

better mission outcome (improved business processes)
continued tech sustainability and evolution
rapid deployments ONLY IF security can perform ATOs quickly



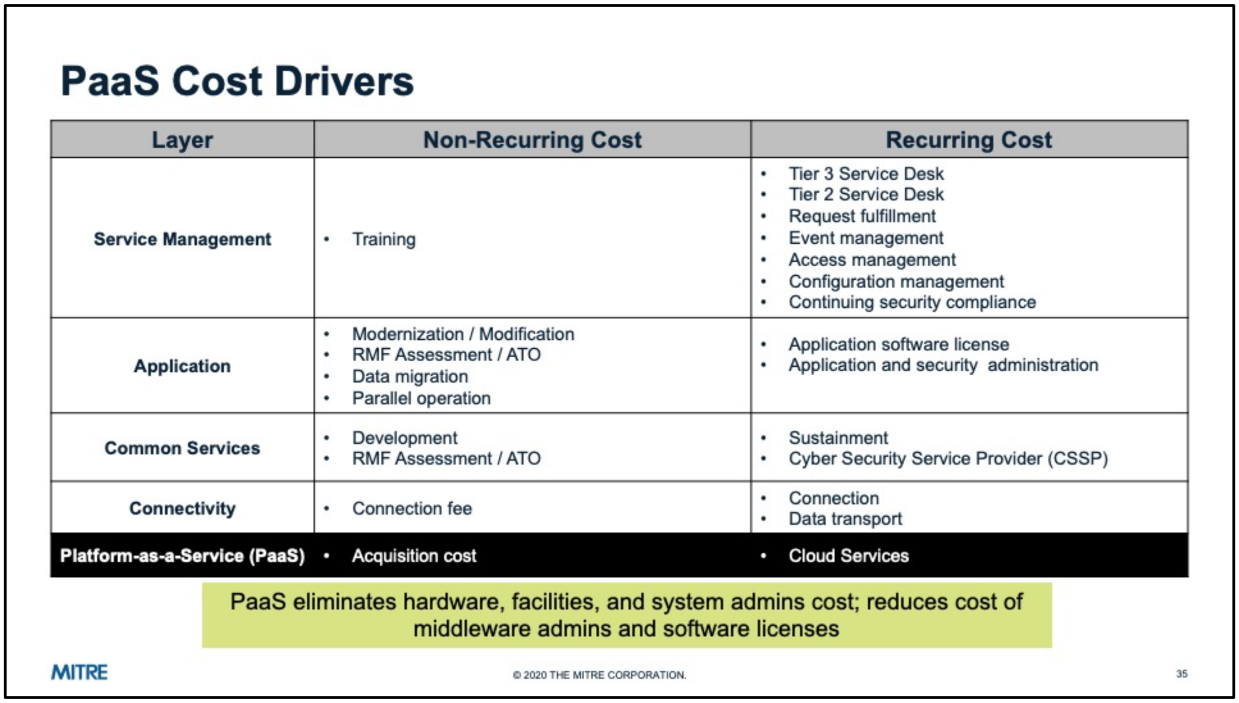
IaaS Cost Drivers

Layer	Non-Recurring Cost	Recurring Cost
Service Management	• Training	• Tier 3 Service Desk • Tier 2 Service Desk • Request fulfillment • Event management • Access management • Configuration management • Continuing security compliance
Application	• Modernization / Modification • RMF Assessment / ATO • Data Migration • Parallel operation	• Application software license • Middleware software license • Application and security administration • Middleware administration • System administration
Common Services	• Development • RMF Assessment / ATO	• Sustainment • Cyber Security Service Provider (CSSP)
Connectivity	• Connection fee	• Connection • Data transport
Infrastructure-as-a-Service (IaaS)	• Acquisition cost	• Cloud Services

IaaS eliminates hardware and facilities cost and reduces system admins cost

MITRE

Slide Source: MITRE



PaaS Cost Drivers

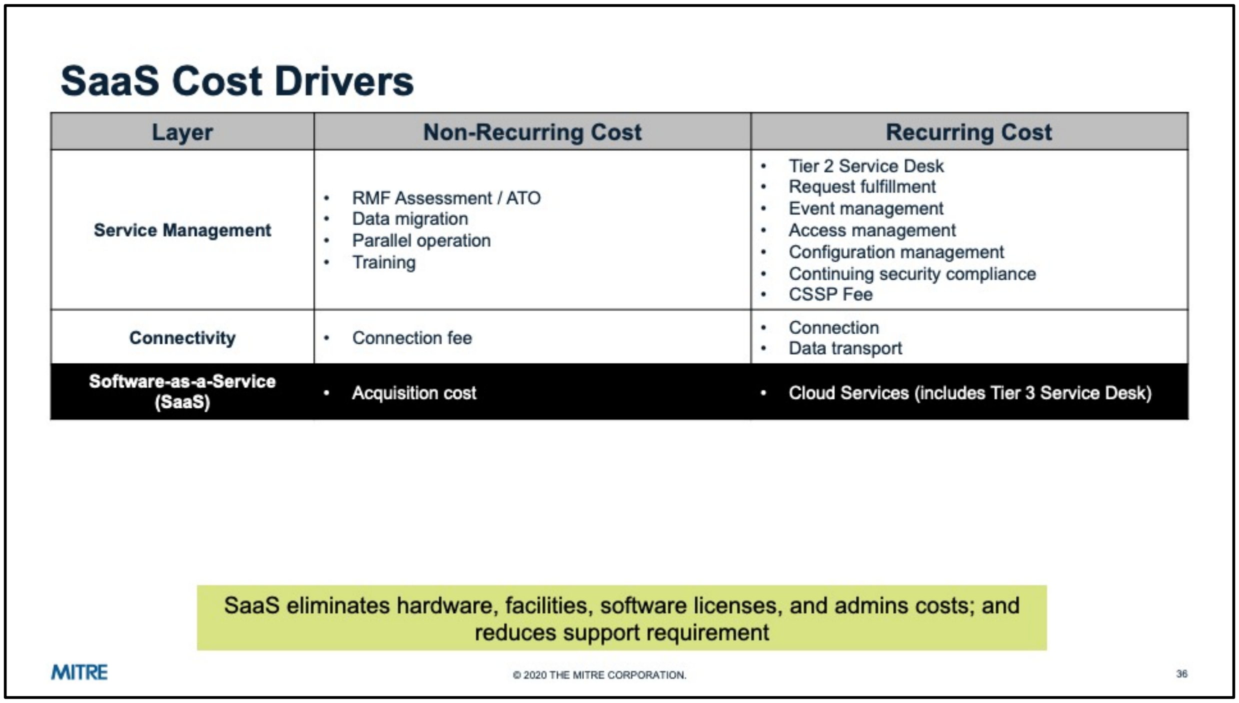
Layer	Non-Recurring Cost	Recurring Cost
Service Management	• Training	• Tier 3 Service Desk • Tier 2 Service Desk • Request fulfillment • Event management • Access management • Configuration management • Continuing security compliance
Application	• Modernization / Modification • RMF Assessment / ATO • Data migration • Parallel operation	• Application software license • Application and security administration
Common Services	• Development • RMF Assessment / ATO	• Sustainment • Cyber Security Service Provider (CSSP)
Connectivity	• Connection fee	• Connection • Data transport
Platform-as-a-Service (PaaS)	• Acquisition cost	• Cloud Services

PaaS eliminates hardware, facilities, and system admins cost; reduces cost of middleware admins and software licenses

MITRE

35

Slide Source: MITRE



SaaS Cost Drivers

Layer	Non-Recurring Cost	Recurring Cost
Service Management	• RMF Assessment / ATO • Data migration • Parallel operation • Training	• Tier 2 Service Desk • Request fulfillment • Event management • Access management • Configuration management • Continuing security compliance • CSSP Fee
Connectivity	• Connection fee	• Connection • Data transport
Software-as-a-Service (SaaS)	• Acquisition cost	• Cloud Services (includes Tier 3 Service Desk)

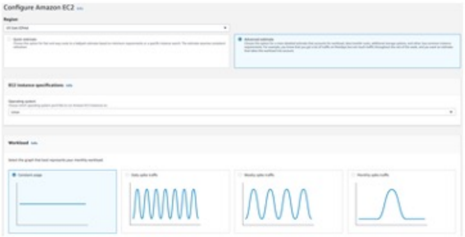
SaaS eliminates hardware, facilities, software licenses, and admins costs; and reduces support requirement

MITRE

Slide Source: MITRE

Cost Calculators – Hosting

AWS


Configure Amazon EC2

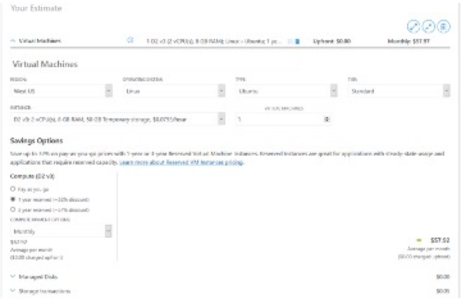
Region

EC2 instance specifications

Operating system

Workload

Azure


Your Estimate

Virtual Machines Upfront: $0.00 Monthly: $57.57

Virtual Machines

REGION	OPERATING SYSTEM	TYPE	TIER
West US	Linux	Ubuntu	Standard

Savings Options

Compute (D2 v3)

○ Pay as you go
● 1 year reserved
○ 3 year reserved

Monthly

$57.52 Average per month

Managed Disks $0.00

Storage transactions $0.00

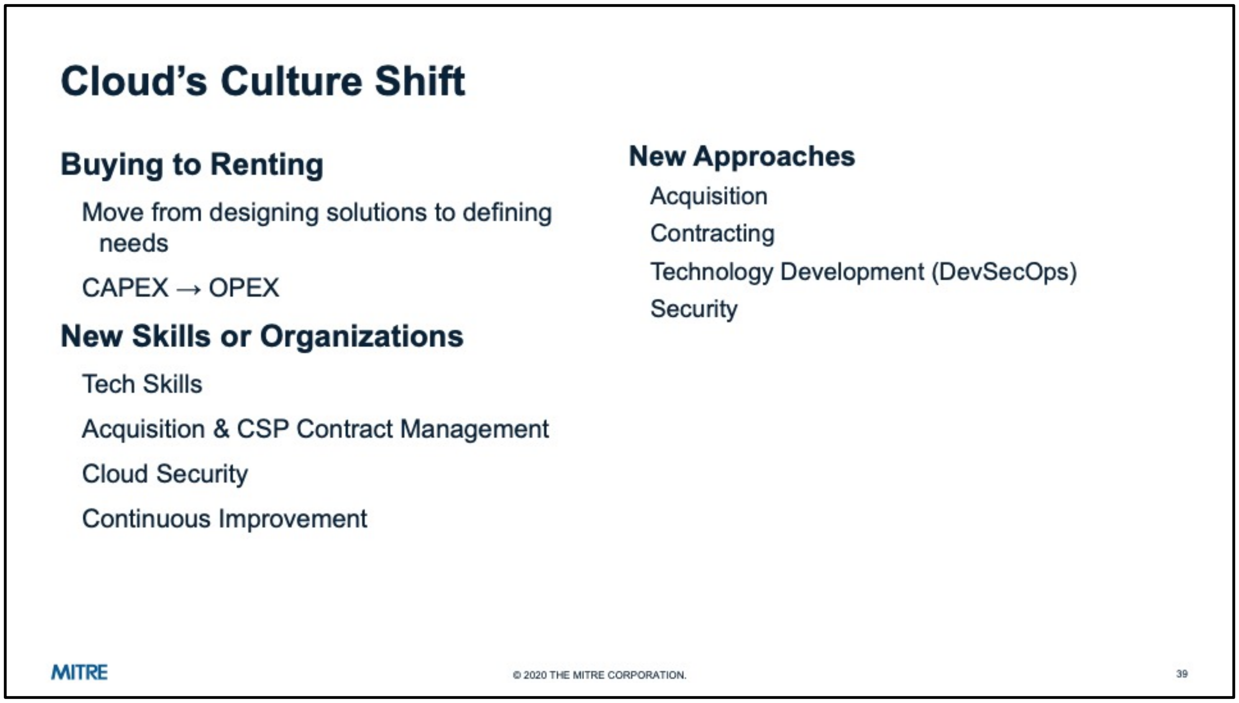
CAUTION: Tools are only as good as the user's knowledge and the data available

MITRE

Slide Source: AWS: https://calculator.aws/#/addService [16]
Slide Source: Azure: https://azure.microsoft.com/en-us/pricing/calculator/ [17]

Workforce Development

MITRE



Cloud's Culture Shift

Buying to Renting

- Move from designing solutions to defining needs
- CAPEX → OPEX

New Skills or Organizations

- Tech Skills
- Acquisition & CSP Contract Management
- Cloud Security
- Continuous Improvement

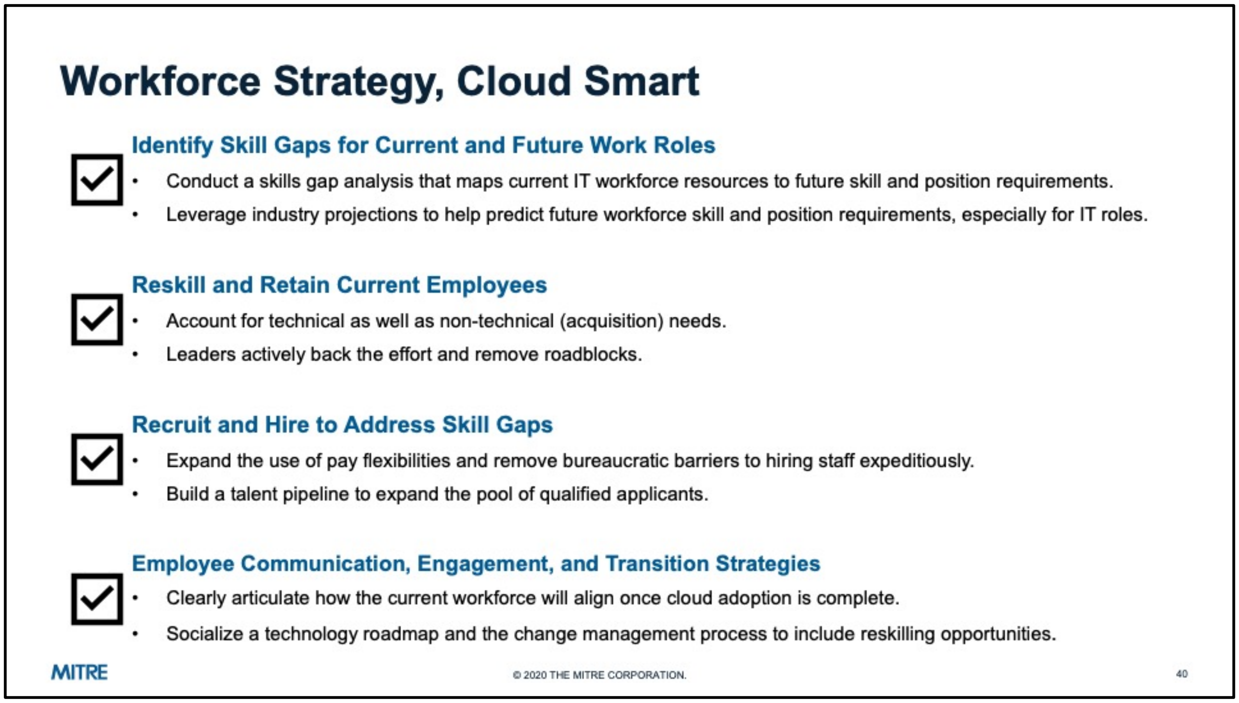
New Approaches

- Acquisition
- Contracting
- Technology Development (DevSecOps)
- Security

MITRE

39

Slide Source: MITRE



Workforce Strategy, Cloud Smart

☑ **Identify Skill Gaps for Current and Future Work Roles**

- Conduct a skills gap analysis that maps current IT workforce resources to future skill and position requirements.
- Leverage industry projections to help predict future workforce skill and position requirements, especially for IT roles.

☑ **Reskill and Retain Current Employees**

- Account for technical as well as non-technical (acquisition) needs.
- Leaders actively back the effort and remove roadblocks.

☑ **Recruit and Hire to Address Skill Gaps**

- Expand the use of pay flexibilities and remove bureaucratic barriers to hiring staff expeditiously.
- Build a talent pipeline to expand the pool of qualified applicants.

☑ **Employee Communication, Engagement, and Transition Strategies**

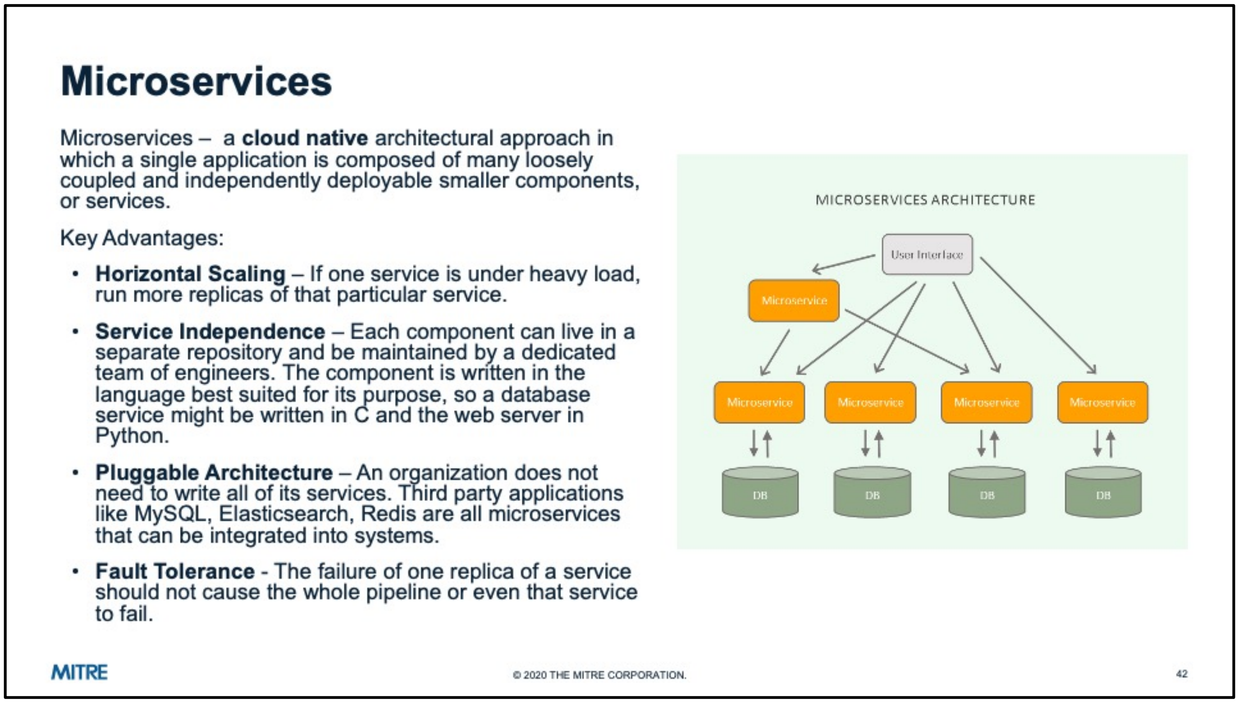
- Clearly articulate how the current workforce will align once cloud adoption is complete.
- Socialize a technology roadmap and the change management process to include reskilling opportunities.

MITRE

40

Slide Source: https://cloud.cio.gov/strategy/ [18]

Cloud DevSecOps



Microservices

Microservices – a **cloud native** architectural approach in which a single application is composed of many loosely coupled and independently deployable smaller components, or services.

Key Advantages:

- **Horizontal Scaling** – If one service is under heavy load, run more replicas of that particular service.
- **Service Independence** – Each component can live in a separate repository and be maintained by a dedicated team of engineers. The component is written in the language best suited for its purpose, so a database service might be written in C and the web server in Python.
- **Pluggable Architecture** – An organization does not need to write all of its services. Third party applications like MySQL, Elasticsearch, Redis are all microservices that can be integrated into systems.
- **Fault Tolerance** - The failure of one replica of a service should not cause the whole pipeline or even that service to fail.

MITRE

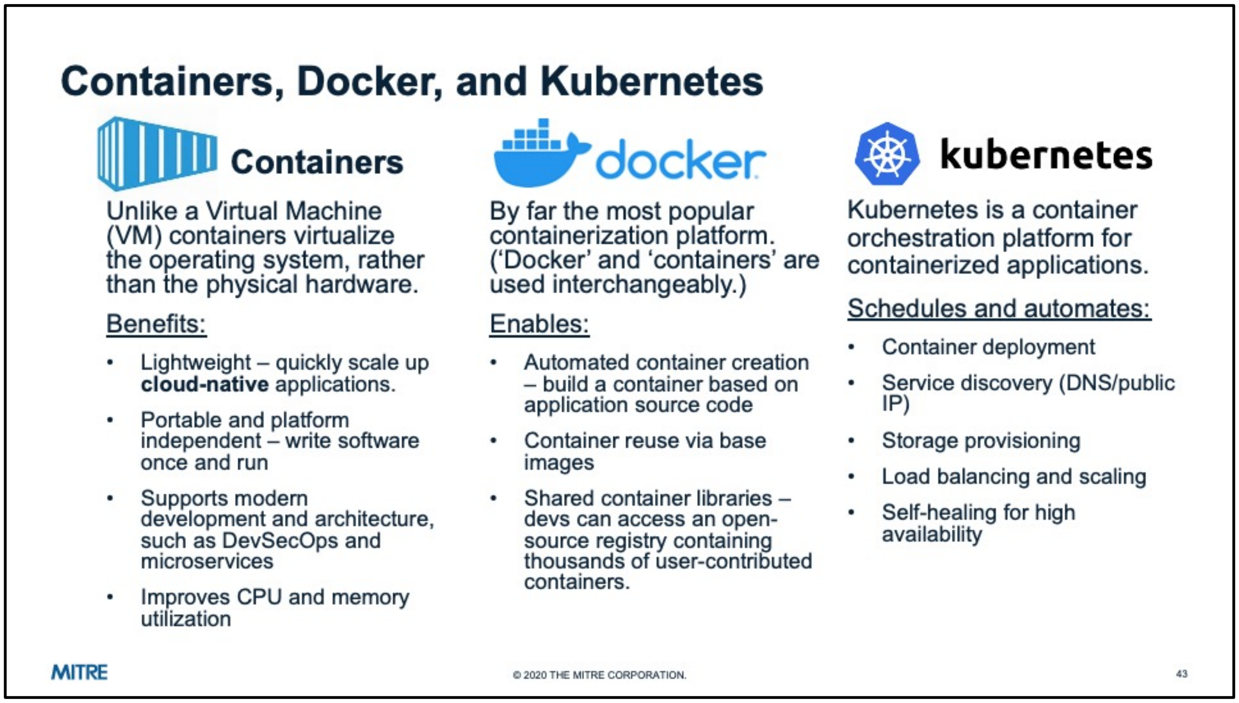
© 2020 THE MITRE CORPORATION.

42

Slide Source: https://www.ibm.com/cloud/learn/microservices [19]
Slide Source: https://hackernoon.com/how-microservices-saved-the-internet-30cd4b9c6230 [20]

Microservices Image: https://hackernoon.com/how-microservices-saved-the-internet-30cd4b9c6230

Microservices are not necessarily exclusively relevant to cloud computing but there are a few important reasons why they so frequently go together—reasons that go beyond microservices being a popular architectural style for new applications and the cloud being a popular hosting destination for new applications.



Containers, Docker, and Kubernetes

Containers

Unlike a Virtual Machine (VM) containers virtualize the operating system, rather than the physical hardware.

Benefits:

- Lightweight – quickly scale up **cloud-native** applications.
- Portable and platform independent – write software once and run
- Supports modern development and architecture, such as DevSecOps and microservices
- Improves CPU and memory utilization

docker

By far the most popular containerization platform. (‘Docker’ and ‘containers’ are used interchangeably.)

Enables:

- Automated container creation – build a container based on application source code
- Container reuse via base images
- Shared container libraries – devs can access an open-source registry containing thousands of user-contributed containers.

kubernetes

Kubernetes is a container orchestration platform for containerized applications.

Schedules and automates:

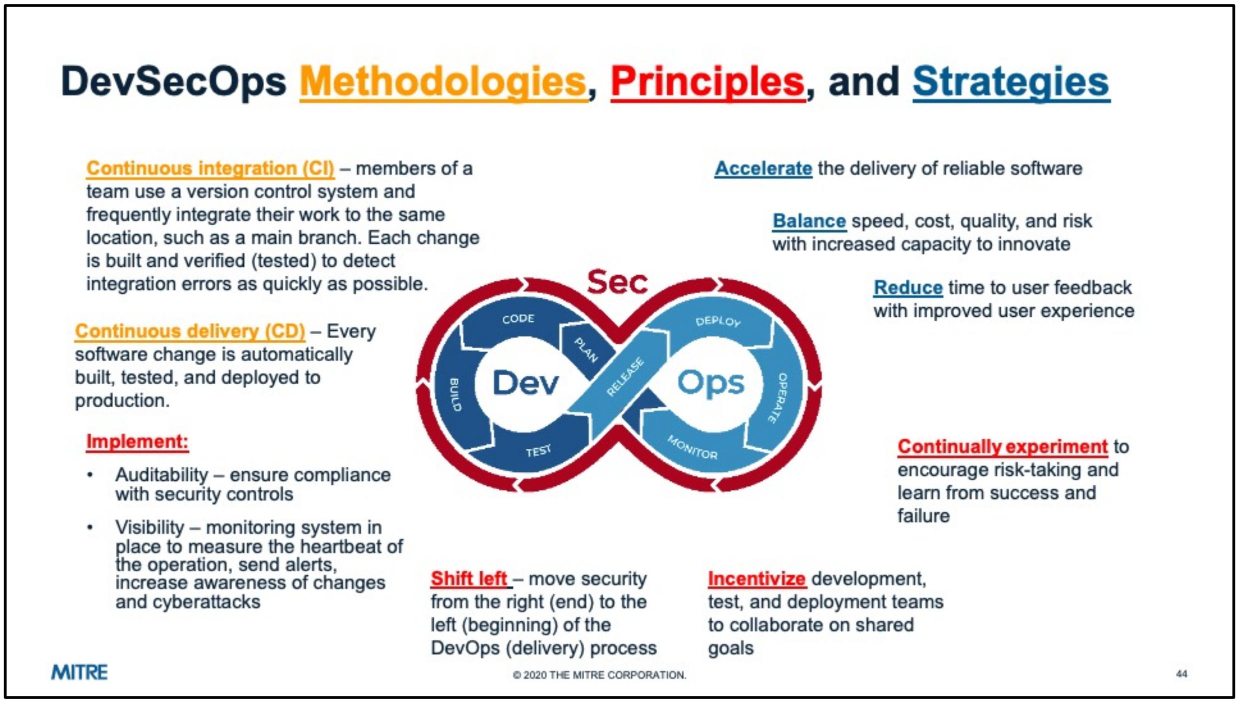
- Container deployment
- Service discovery (DNS/public IP)
- Storage provisioning
- Load balancing and scaling
- Self-healing for high availability

MITRE

43

Slide Source: https://www.ibm.com/cloud/learn/microservices [19]

Container image: https://archive.turbonomic.com/wp-content/uploads/2014/04/ContainerIconBlue-min.jpg
Docker image: https://www.docker.com/company/newsroom/media-resources
Kubernetes image: https://blogs.vmware.com/cloudnative/files/2017/12/1024px-Kubernetes_logo.svg_-1024x181.png



DevSecOps Methodologies, Principles, and Strategies

Continuous integration (CI) – members of a team use a version control system and frequently integrate their work to the same location, such as a main branch. Each change is built and verified (tested) to detect integration errors as quickly as possible.

Continuous delivery (CD) – Every software change is automatically built, tested, and deployed to production.

Implement:

- Auditability – ensure compliance with security controls
- Visibility – monitoring system in place to measure the heartbeat of the operation, send alerts, increase awareness of changes and cyberattacks

Shift left – move security from the right (end) to the left (beginning) of the DevOps (delivery) process

Incentivize development, test, and deployment teams to collaborate on shared goals

Accelerate the delivery of reliable software

Balance speed, cost, quality, and risk with increased capacity to innovate

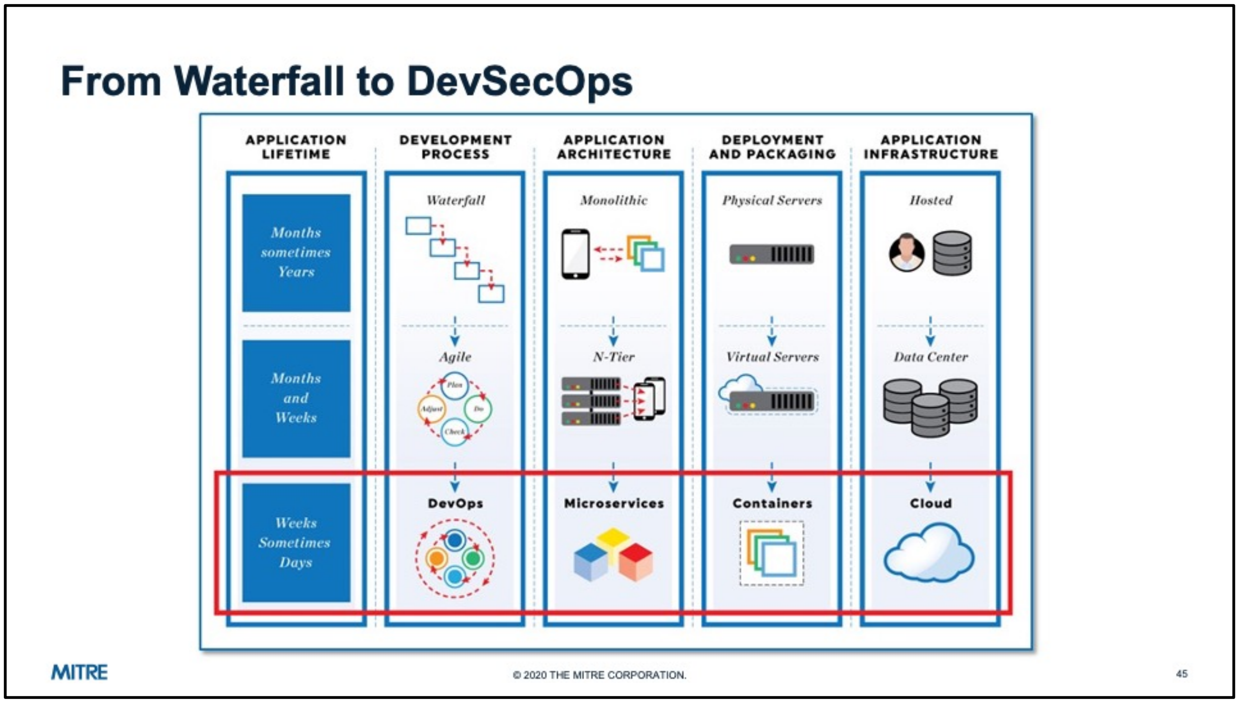
Reduce time to user feedback with improved user experience

Continually experiment to encourage risk-taking and learn from success and failure

MITRE

Slide Source: https://docs.aws.amazon.com/codepipeline/latest/userguide/concepts-continuous-delivery-integration.html [21]
Slide Source: https://www.ibm.com/cloud/learn/devops-a-complete-guide [22]
Slide Source: https://www.ibm.com/cloud/learn/devsecops [23]

DevSecOps image: https://sasg.arizona.edu/sites/default/files/devsecops_diagram.png

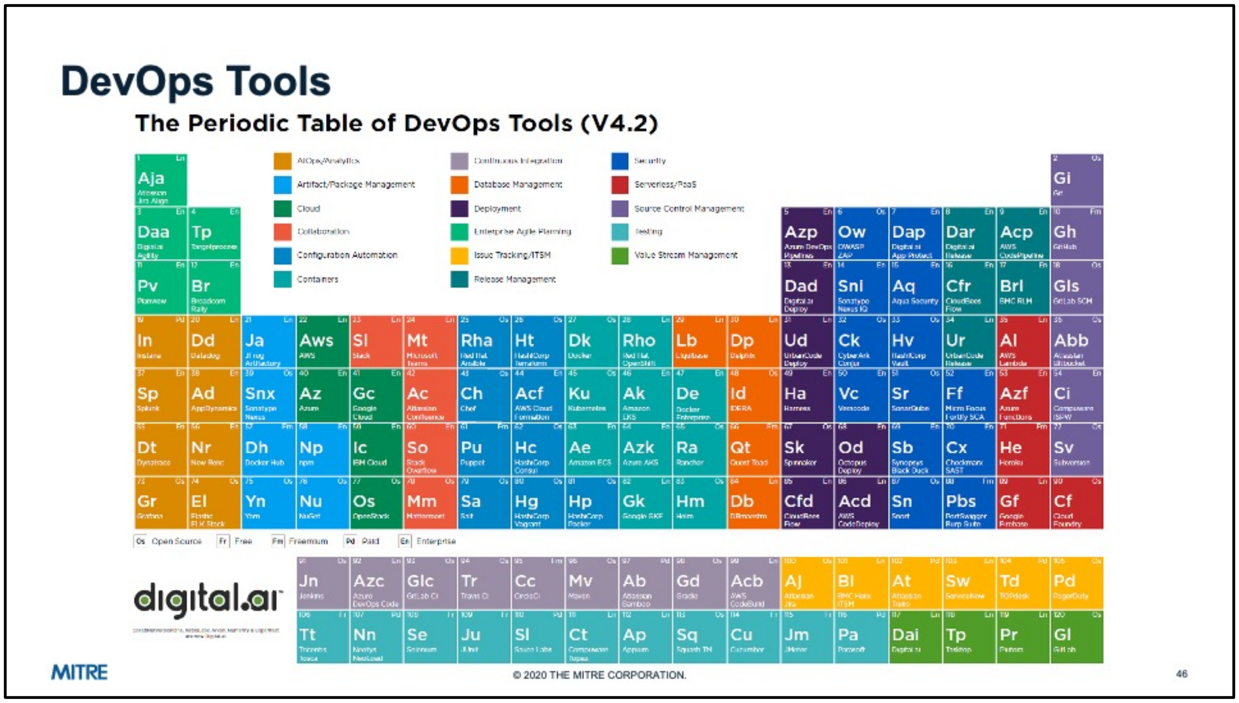


From Waterfall to DevSecOps

APPLICATION LIFETIME	DEVELOPMENT PROCESS	APPLICATION ARCHITECTURE	DEPLOYMENT AND PACKAGING	APPLICATION INFRASTRUCTURE
Months sometimes Years	Waterfall	Monolithic	Physical Servers	Hosted
Months and Weeks	Agile	N-Tier	Virtual Servers	Data Center
Weeks Sometimes Days	DevOps	Microservices	Containers	Cloud

MITRE

Slide Source: DoD Enterprise DevSecOps Initiative (Software Factory) [24]



DevOps Tools

The Periodic Table of DevOps Tools (V4.2)

🟧 AIOps/Analytics	▨ Continuous Integration	🟦 Security
🟦 Artifact/Package Management	🟧 Database Management	🟥 Serverless/PaaS
🟩 Cloud	🟪 Deployment	🟪 Source Control Management
🟥 Collaboration	🟩 Enterprise Agile Planning	🟦 Testing
🟦 Configuration Automation	🟨 Issue Tracking/ITSM	🟩 Value Stream Management
🟦 Containers	🟩 Release Management	

1 En Aja Atlassian Jira Align																	2 Os Gi Git
3 En Daa Digital.ai Agility	4 En Tp Targetprocess											5 En Azp Azure DevOps Pipelines	6 Os Ow OWASP ZAP	7 En Dap Digital.ai App Protect	8 En Dar Digital.ai Release	9 En Acp AWS CodePipeline	10 Fm Gh GitHub
11 En Pv Planview	12 En Br Broadcom Rally											13 En Dad Digital.ai Deploy	14 En Sni Sonatype Nexus IQ	15 En Aq Aqua Security	16 En Cfr CloudBees Flow	17 En Brl BMC RLM	18 Os Gls GitLab SCM
19 Pd In Instana	20 En Dd Datadog	21 En Ja JFrog Artifactory	22 En Aws AWS	23 En Sl Slack	24 En Mt Microsoft Teams	25 Os Rha Red Hat Ansible	26 Os Ht HashiCorp Terraform	27 Os Dk Docker	28 En Rho Red Hat OpenShift	29 En Lb Liquibase	30 En Dp Delphix	31 En Ud UrbanCode Deploy	32 Os Ck CyberArk Conjur	33 Os Hv HashiCorp Vault	34 En Ur UrbanCode Release	35 En Al AWS Lambda	36 Os Abb Atlassian Bitbucket
37 En Sp Splunk	38 En Ad AppDynamics	39 Os Snx Sonatype Nexus	40 En Az Azure	41 En Gc Google Cloud	42 Ac Atlassian Confluence	43 Os Ch Chef	44 En Acf AWS Cloud Formation	45 Os Ku Kubernetes	46 En Ak Amazon EKS	47 En De Docker Enterprise	48 Os Id IDERA	49 En Ha Harness	50 En Vc Veracode	51 Os Sr SonarQube	52 En Ff Micro Focus Fortify SCA	53 En Azf Azure Functions	54 En Ci Compuware ISPW
55 En Dt Dynatrace	56 En Nr New Relic	57 Fm Dh Docker Hub	58 En Np npm	59 En Ic IBM Cloud	60 En So Stack Overflow	61 Fm Pu Puppet	62 Os Hc HashiCorp Consul	63 En Ae Amazon ECS	64 En Azk Azure AKS	65 Os Ra Rancher	66 Fm Qt Quest Toad	67 Os Sk Spinnaker	68 En Od Octopus Deploy	69 En Sb Synopsys Black Duck	70 En Cx Checkmarx SAST	71 Fm He Heroku	72 Os Sv Subversion
73 Os Gr Grafana	74 Os El Elastic ELK Stack	75 Os Yn Yarn	76 Os Nu NuGet	77 Os Os OpenStack	78 Os Mm Mattermost	79 Os Sa Salt	80 Os Hg HashiCorp Vagrant	81 Os Hp HashiCorp Packer	82 En Gk Google GKE	83 Os Hm Helm	84 En Db DBmaestro	85 En Cfd CloudBees Flow	86 En Acd AWS CodeDeploy	87 Os Sn Snort	88 Fm Pbs PortSwigger Burp Suite	89 En Gf Google Firebase	90 Os Cf Cloud Foundry

Os Open Source Fr Free Fm Freemium Pd Paid En Enterprise

91 Os Jn Jenkins	92 En Azc Azure DevOps Code	93 Os Glc GitLab CI	94 Os Tr Travis CI	95 Fm Cc CircleCI	96 Os Mv Maven	97 Pd Ab Atlassian Bamboo	98 Os Gd Gradle	99 En Acb AWS CodeBuild	100 Os AJ Atlassian Jira	101 En Bl BMC Helix ITSM	102 Pd At Atlassian Trello	103 En Sw ServiceNow	104 Pd Td TOPdesk	105 Os Pd PagerDuty
106 Fr Tt Tricentis Tosca	107 Pd Nn Neotys NeoLoad	108 Fr Se Selenium	109 Fr Ju JUnit	110 Pd Sl Sauce Labs	111 En Ct Compuware Topaz	112 En Ap Appium	113 Os Sq Squish TM	114 Fr Cu Cucumber	115 Fr Jm JMeter	116 Pd Pa Parasoft	117 En Dai Digital.ai	118 En Tp Tasktop	119 En Pr Plutora	120 Os Gl GitLab

digital.ai

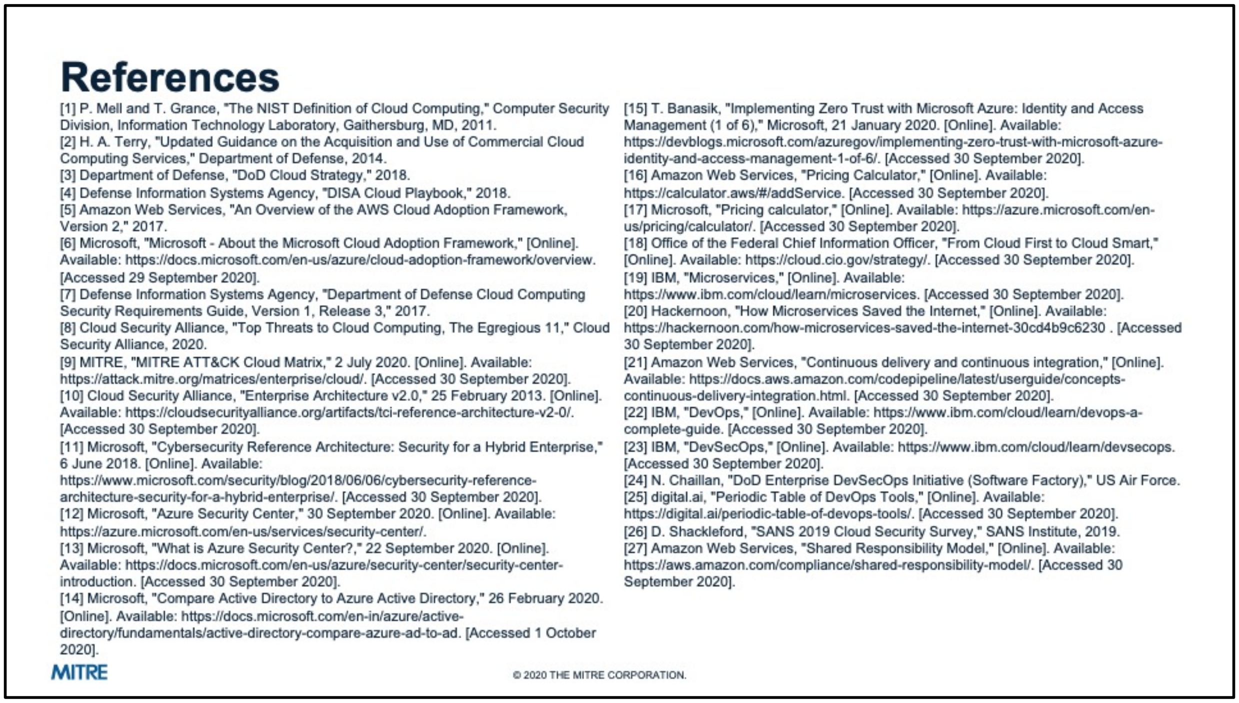
MITRE

© 2020 THE MITRE CORPORATION.

46

Slide Source: https://digital.ai/periodic-table-of-devops-tools [25]

The Periodic Table of DevOps Tools is the industry's go-to resource for identifying best-of-breed tools across the software delivery lifecycle.
Created by DevOps practitioners for DevOps practitioners, over 18,000 votes were cast across more than 400 products in 17 categories to produce the 2020 Periodic Table of DevOps Tools.
Whether you are starting fresh, filling gaps, or replacing existing DevOps tools, get started by using Periodic Table to identify the right tools for your DevOps pipeline.



References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Computer Security Division, Information Technology Laboratory, Gaithersburg, MD, 2011.

[2] H. A. Terry, "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services," Department of Defense, 2014.

[3] Department of Defense, "DoD Cloud Strategy," 2018.

[4] Defense Information Systems Agency, "DISA Cloud Playbook," 2018.

[5] Amazon Web Services, "An Overview of the AWS Cloud Adoption Framework, Version 2," 2017.

[6] Microsoft, "Microsoft - About the Microsoft Cloud Adoption Framework," [Online]. Available: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview. [Accessed 29 September 2020].

[7] Defense Information Systems Agency, "Department of Defense Cloud Computing Security Requirements Guide, Version 1, Release 3," 2017.

[8] Cloud Security Alliance, "Top Threats to Cloud Computing, The Egregious 11," Cloud Security Alliance, 2020.

[9] MITRE, "MITRE ATT&CK Cloud Matrix," 2 July 2020. [Online]. Available: https://attack.mitre.org/matrices/enterprise/cloud/. [Accessed 30 September 2020].

[10] Cloud Security Alliance, "Enterprise Architecture v2.0," 25 February 2013. [Online]. Available: https://cloudsecurityalliance.org/artifacts/tci-reference-architecture-v2-0/. [Accessed 30 September 2020].

[11] Microsoft, "Cybersecurity Reference Architecture: Security for a Hybrid Enterprise," 6 June 2018. [Online]. Available: https://www.microsoft.com/security/blog/2018/06/06/cybersecurity-reference-architecture-security-for-a-hybrid-enterprise/. [Accessed 30 September 2020].

[12] Microsoft, "Azure Security Center," 30 September 2020. [Online]. Available: https://azure.microsoft.com/en-us/services/security-center/.

[13] Microsoft, "What is Azure Security Center?," 22 September 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction. [Accessed 30 September 2020].

[14] Microsoft, "Compare Active Directory to Azure Active Directory," 26 February 2020. [Online]. Available: https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad. [Accessed 1 October 2020].

[15] T. Banasik, "Implementing Zero Trust with Microsoft Azure: Identity and Access Management (1 of 6)," Microsoft, 21 January 2020. [Online]. Available: https://devblogs.microsoft.com/azuregov/implementing-zero-trust-with-microsoft-azure-identity-and-access-management-1-of-6/. [Accessed 30 September 2020].

[16] Amazon Web Services, "Pricing Calculator," [Online]. Available: https://calculator.aws/#/addService. [Accessed 30 September 2020].

[17] Microsoft, "Pricing calculator," [Online]. Available: https://azure.microsoft.com/en-us/pricing/calculator/. [Accessed 30 September 2020].

[18] Office of the Federal Chief Information Officer, "From Cloud First to Cloud Smart," [Online]. Available: https://cloud.cio.gov/strategy/. [Accessed 30 September 2020].

[19] IBM, "Microservices," [Online]. Available: https://www.ibm.com/cloud/learn/microservices. [Accessed 30 September 2020].

[20] Hackernoon, "How Microservices Saved the Internet," [Online]. Available: https://hackernoon.com/how-microservices-saved-the-internet-30cd4b9c6230 . [Accessed 30 September 2020].

[21] Amazon Web Services, "Continuous delivery and continuous integration," [Online]. Available: https://docs.aws.amazon.com/codepipeline/latest/userguide/concepts-continuous-delivery-integration.html. [Accessed 30 September 2020].

[22] IBM, "DevOps," [Online]. Available: https://www.ibm.com/cloud/learn/devops-a-complete-guide. [Accessed 30 September 2020].

[23] IBM, "DevSecOps," [Online]. Available: https://www.ibm.com/cloud/learn/devsecops. [Accessed 30 September 2020].

[24] N. Chaillan, "DoD Enterprise DevSecOps Initiative (Software Factory)," US Air Force.

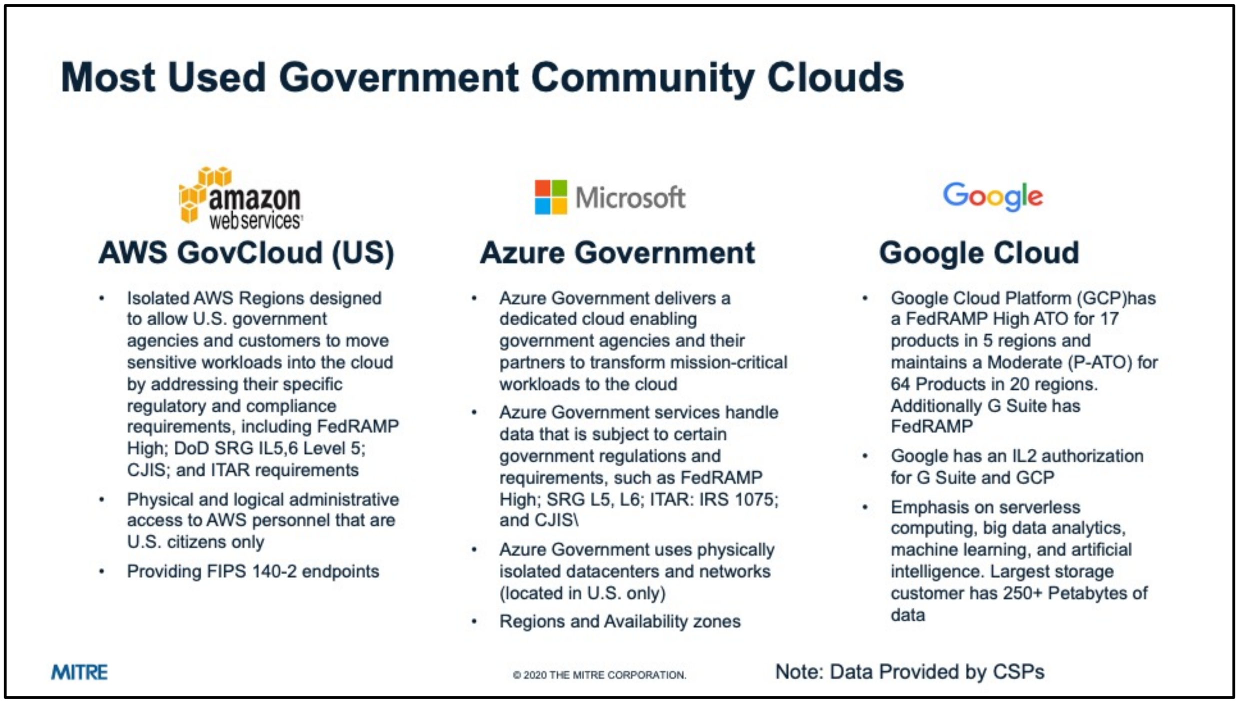
[25] digital.ai, "Periodic Table of DevOps Tools," [Online]. Available: https://digital.ai/periodic-table-of-devops-tools/. [Accessed 30 September 2020].

[26] D. Shackleford, "SANS 2019 Cloud Security Survey," SANS Institute, 2019.

[27] Amazon Web Services, "Shared Responsibility Model," [Online]. Available: https://aws.amazon.com/compliance/shared-responsibility-model/. [Accessed 30 September 2020].

MITRE

Backup



Most Used Government Community Clouds

amazon web services

AWS GovCloud (US)

- Isolated AWS Regions designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements, including FedRAMP High; DoD SRG IL5,6 Level 5; CJIS; and ITAR requirements
- Physical and logical administrative access to AWS personnel that are U.S. citizens only
- Providing FIPS 140-2 endpoints

Microsoft

Azure Government

- Azure Government delivers a dedicated cloud enabling government agencies and their partners to transform mission-critical workloads to the cloud
- Azure Government services handle data that is subject to certain government regulations and requirements, such as FedRAMP High; SRG L5, L6; ITAR: IRS 1075; and CJIS\
- Azure Government uses physically isolated datacenters and networks (located in U.S. only)
- Regions and Availability zones

Google

Google Cloud

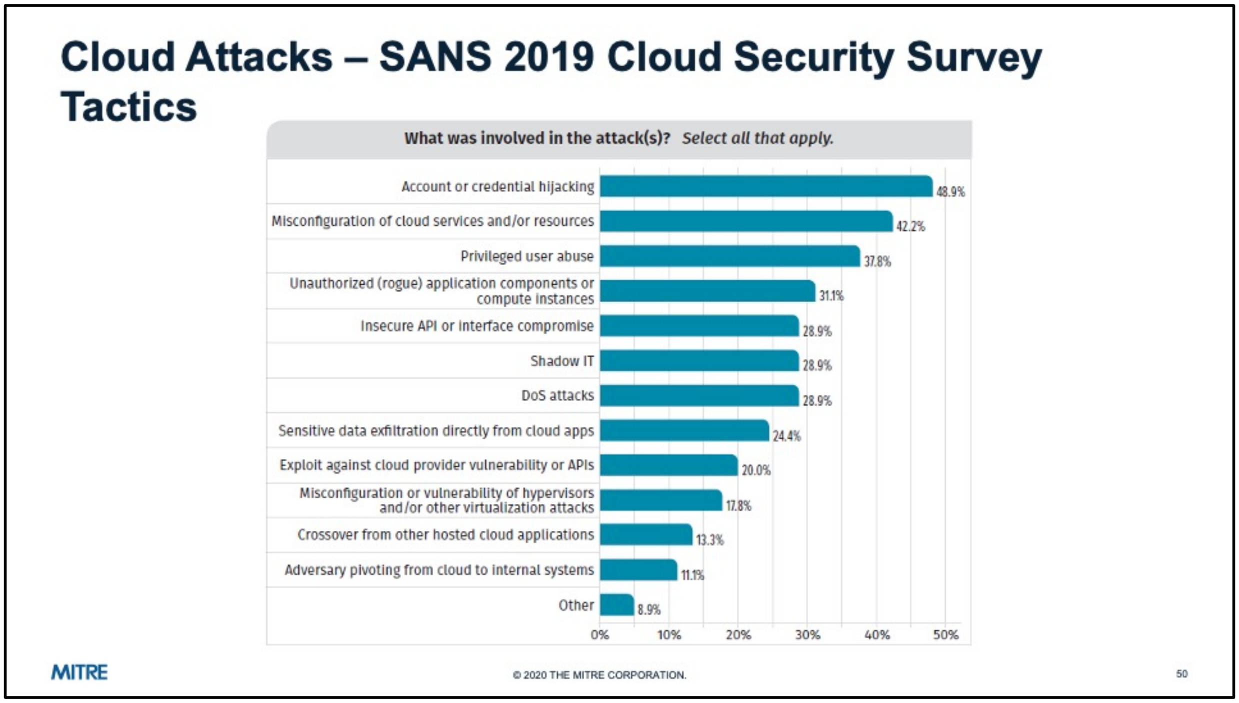
- Google Cloud Platform (GCP)has a FedRAMP High ATO for 17 products in 5 regions and maintains a Moderate (P-ATO) for 64 Products in 20 regions. Additionally G Suite has FedRAMP
- Google has an IL2 authorization for G Suite and GCP
- Emphasis on serverless computing, big data analytics, machine learning, and artificial intelligence. Largest storage customer has 250+ Petabytes of data

MITRE

Note: Data Provided by CSPs

Slide Source: MITRE

IBM and Oracle are other commonly used Commercial Government Clouds. Provisional Authority to Operate (P-ATO)



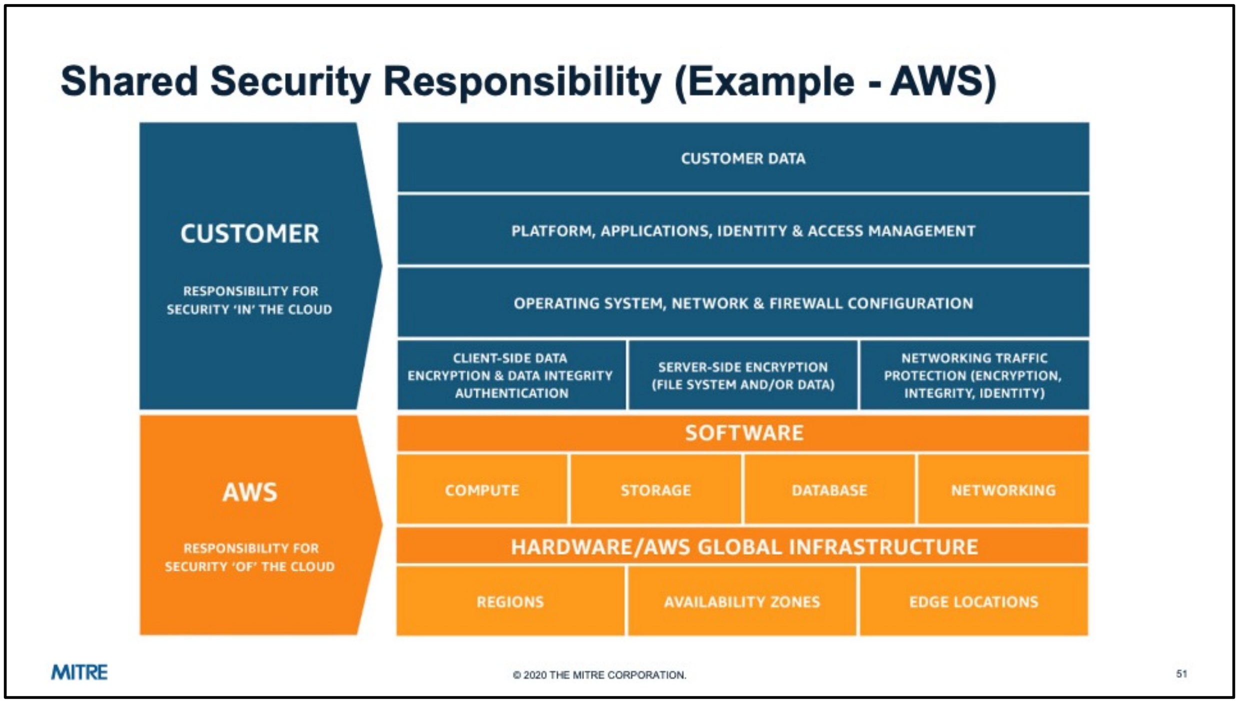
Cloud Attacks – SANS 2019 Cloud Security Survey Tactics

MITRE

© 2020 THE MITRE CORPORATION.

50

Slide Source: [26]



Shared Security Responsibility (Example - AWS)

CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

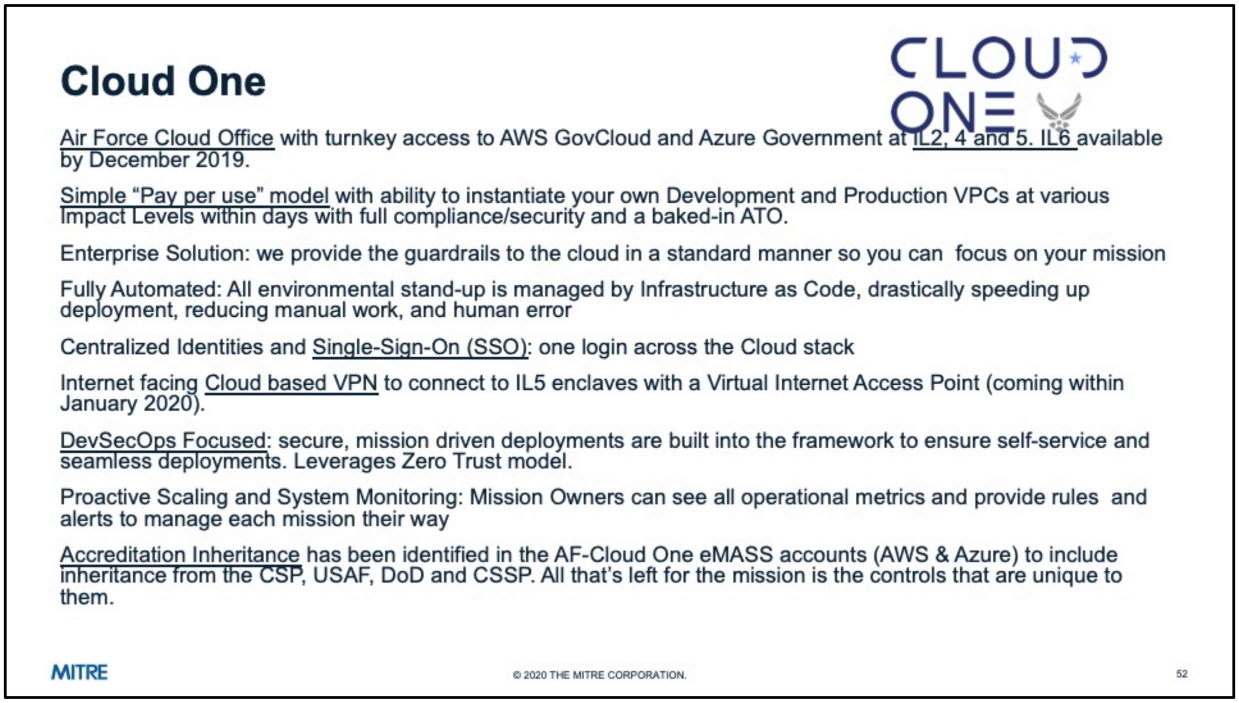
AVAILABILITY ZONES

EDGE LOCATIONS

MITRE

51

Slide Source: https://aws.amazon.com/compliance/shared-responsibility-model/ [27]



Cloud One

Air Force Cloud Office with turnkey access to AWS GovCloud and Azure Government at IL2, 4 and 5. IL6 available by December 2019.

Simple "Pay per use" model with ability to instantiate your own Development and Production VPCs at various Impact Levels within days with full compliance/security and a baked-in ATO.

Enterprise Solution: we provide the guardrails to the cloud in a standard manner so you can focus on your mission

Fully Automated: All environmental stand-up is managed by Infrastructure as Code, drastically speeding up deployment, reducing manual work, and human error

Centralized Identities and Single-Sign-On (SSO): one login across the Cloud stack

Internet facing Cloud based VPN to connect to IL5 enclaves with a Virtual Internet Access Point (coming within January 2020).

DevSecOps Focused: secure, mission driven deployments are built into the framework to ensure self-service and seamless deployments. Leverages Zero Trust model.

Proactive Scaling and System Monitoring: Mission Owners can see all operational metrics and provide rules and alerts to manage each mission their way

Accreditation Inheritance has been identified in the AF-Cloud One eMASS accounts (AWS & Azure) to include inheritance from the CSP, USAF, DoD and CSSP. All that's left for the mission is the controls that are unique to them.

MITRE

52

Slide Source: DoD Enterprise DevSecOps Initiative (Software Factory) [24]

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™