

# Adopting Public Cloud as A Platform for Innovation in Healthcare

Josh Perkins, Field CTO



**himss**

**CENTRAL & SOUTHERN OHIO** *Chapter*

# Adopting Public Cloud as A Platform for Innovation in Healthcare

New Workloads, New Operating Paradigms, Improved Healthcare Outcomes

# Overview

Digital Transformation in Healthcare

Public Cloud Use Cases

Lessons Learned

#1 Security

#2 Skills

#3 Master One Cloud First

Questions



By 2020, 40% of healthcare providers will realize their electronic health record (EHR) technology cannot fully support their care delivery needs.

---

**Mike Jones, VP Analyst**

*How Healthcare Provider CIOs Can Successfully Achieve Digital Care Transformation*  
**Gartner (2019)**

# The Path to Digital Healthcare

The vertical path encompasses the digitization of the business of healthcare management

- Nonclinical activities
- Removal of waste
- Real-time orchestration of healthcare resources

The horizontal path encompasses the digitization of clinical capabilities and lies at the heart of every organization's value proposition.

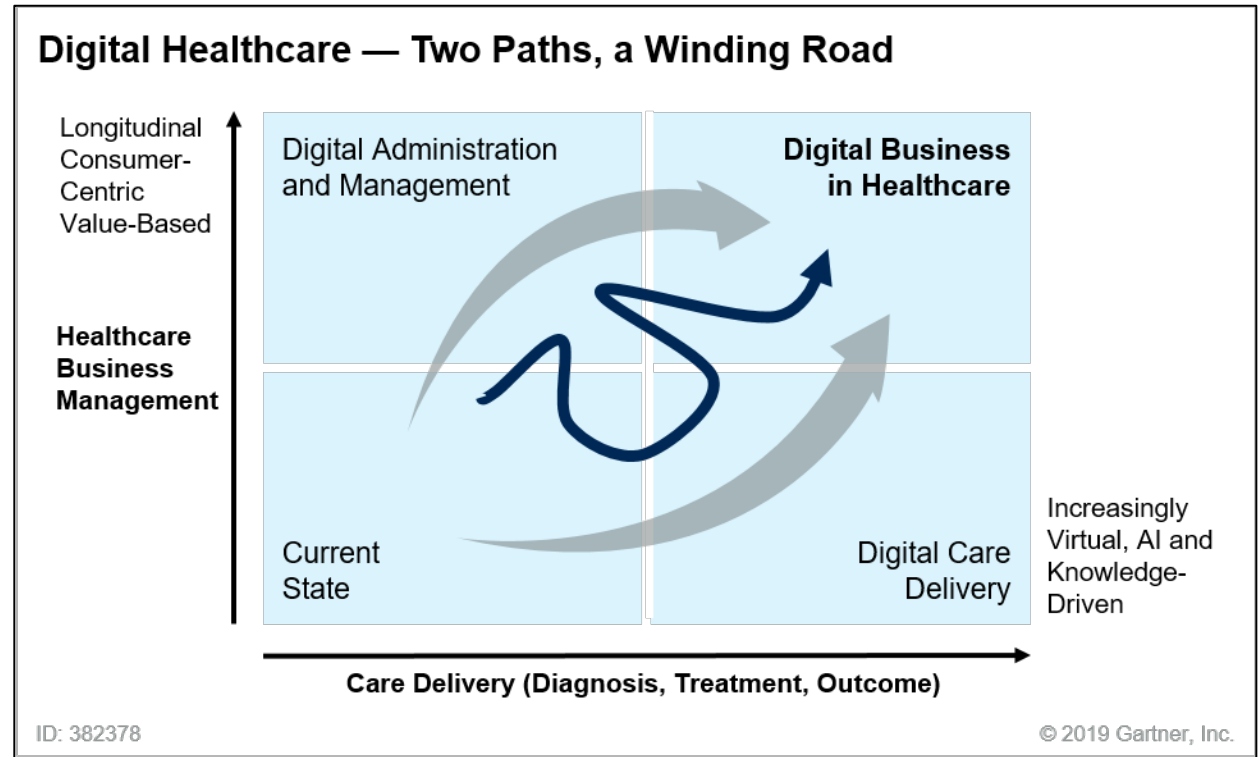
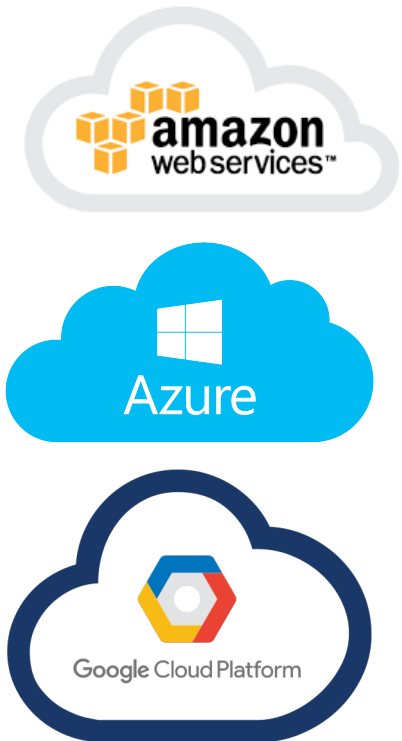
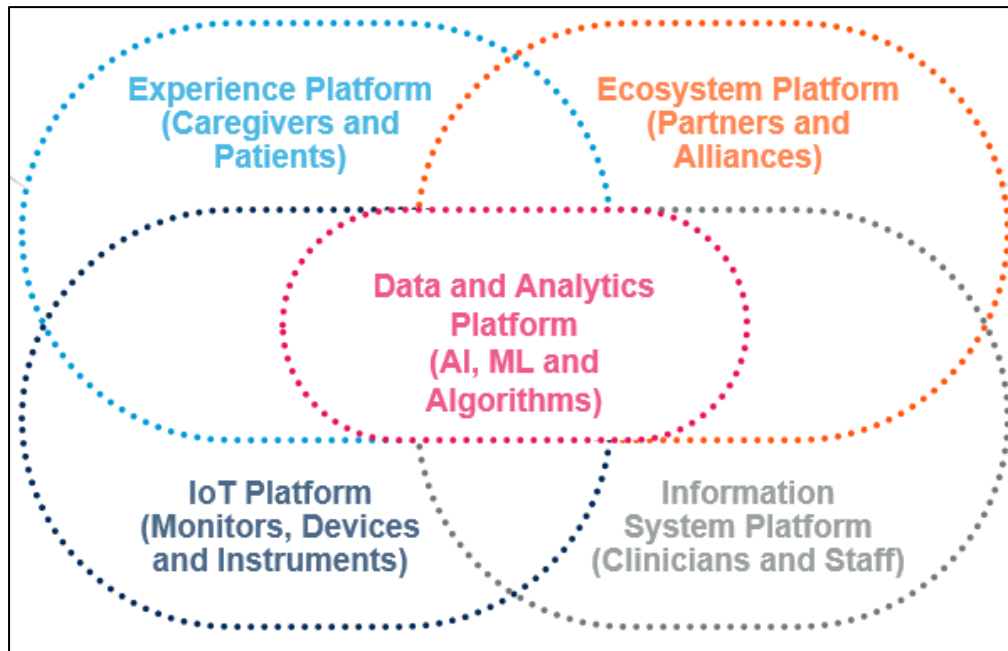


Photo Credit: Gartner 2019

<https://www.gartner.com/document/3904769?ref=TypeAheadSearch&qid=e4bbec1ccb3e44d0e4ce2c>

# New Capabilities = New Digital Platform

These New Capabilities Are Driving Public Cloud Consumption



# Public Cloud Use Cases in Healthcare IT



## Business Intelligence Analytics

---

- Denial Management
- Population Cost Prediction
- Fraud, Waste, Abuse
- Rx Cost Variance



## Research ML / AI

---

- Genomic Sequencing
- Cancer Research
- Molecular Biology
- Radiology
- Pathology



## Operational Efficiency ML / AI

---

- Census Forecasting
- Patient Bed Scheduling
- Ambulatory Scheduling



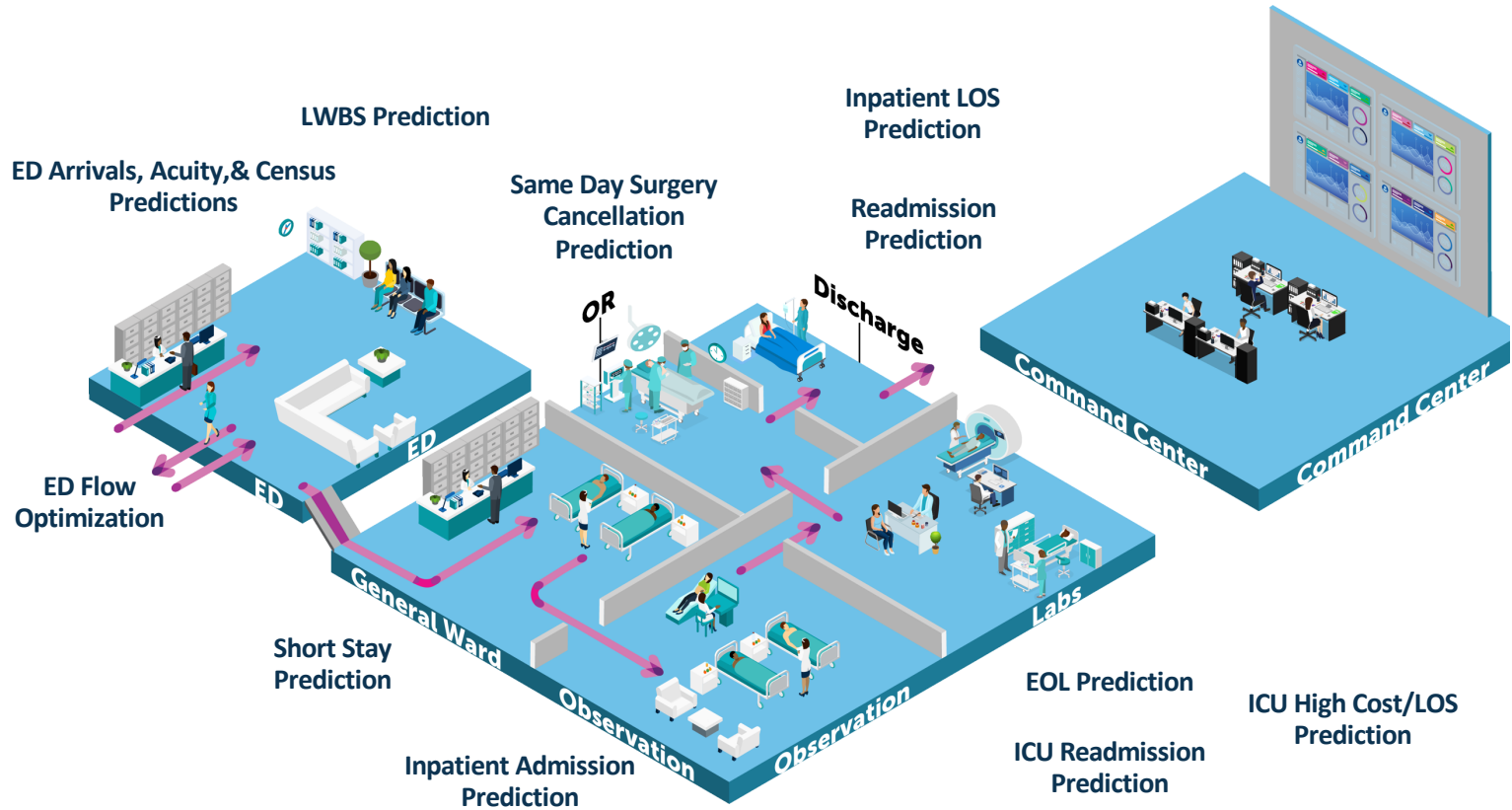
## Collaboration SaaS

---

- Telemedicine
- Health Information Exchange
- Physician Collaboration
- Remote IoT Devices

# Healthcare IT Use Cases: AI / ML

## AI in Patient Flow, Staffing and Bed Management





# Leveraging Applied AI in Healthcare IT

0

## VARIATION ANALYSIS

#1	Pharmacy
#2	LOS

## CARE MANAGEMENT

Risk Stratification    Readmissions Reduction    Disease Progression    End of Life Optimization

CKD    CHF    Diabetes    COPD

## ACUTE PATIENT FLOW

Staffing Optimization    Length of Stay Prediction    Census Forecasting

Surgery Scheduling    Inpatient Deterioration    ED Load Prediction

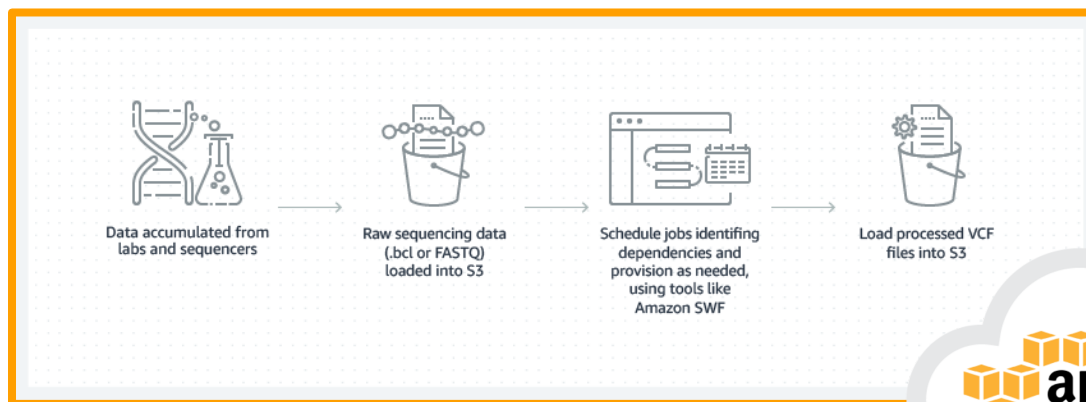
## UTILIZATION

Population Cost Prediction    Predictive Hot Spotting    PMPM Analyzer    Fraud, Waste & Abuse

## REVENUE OPTIMIZATION

Rx Cost Variance    Denials Management    Internal Cost Analysis    Leakage Prediction    No Show Prediction

# Building Analytics Pipelines for Genomic Sequencing



Upload Sequencing Data to the Cloud



“Using AWS, we are able to offer our customers a lower cost, high-performance genomic-analysis platform, which can help them speed their time to answers.”

Andy Nelson - Informatics & Cloud Operations,  
Illumina

<https://aws.amazon.com/solutions/case-studies/illumina/>

# Telemedicine and Remote IoT



## Distance Medicine

- Audio & Video Conferencing
- Remote Clinics
- Mobile Appointments
- Guided Diagnostics / Scheduling



## Remote IoT Sensor Data

- Pulse
- Blood Glucose
- Electrocardiogram (ECG)



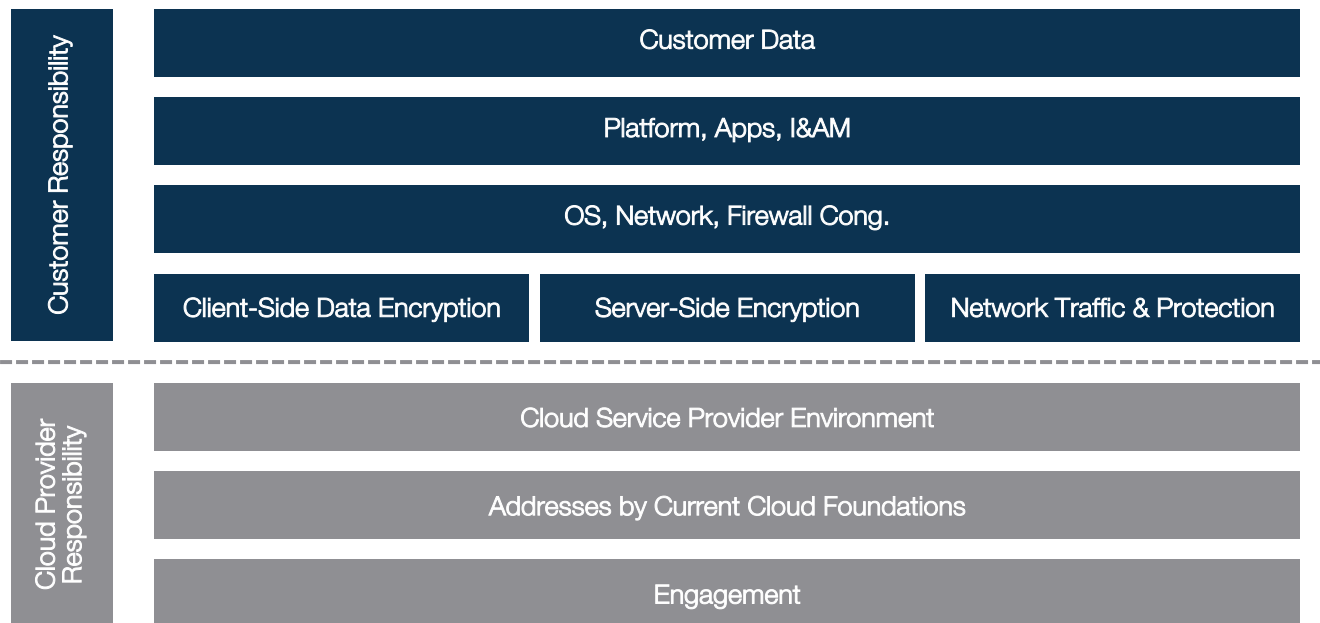
# Lesson Learned #1 – Security

Managing PHI and HIPAA Compliance

# Public Cloud Shared Responsibility Model



Customer



# Eliminate Confusion – Example HIPAA

- Understanding roles and responsibility

When you sign your BAA with the cloud provider you will receive language in your contract similar or exactly like this:

When you accept the BAA, AWS requires you to do the following:

- Use only **'HIPAA Eligible' services** to create, receive, maintain, or transmit PHI
- Implement appropriate privacy and security safeguards in order to protect PHI
- Utilize the highest level of audit logging in connection for all HIPAA Eligible Services we choose to use
- Maintain the maximum retention of logs in connection of our use of all HIPAA Eligible Services we choose to use
- Must encrypt all PHI in rest and transit

# What are CIS Controls?

CIS Critical Controls are a set of standards that are used to define what a secure configuration is when configuring your cloud resources AND operating systems in the cloud including security processes that support the OS



## Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

## Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

## Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises



# Understanding Tools in AWS / Azure

This is a useful tool





# Understanding Tools in AWS / Azure

This is a useful tool

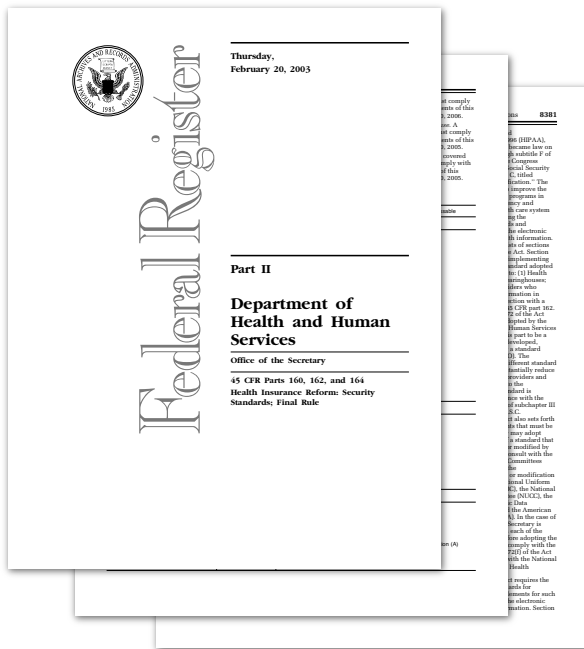


You still have to use the tool properly



# Eliminate Confusion – Example HIPAA

## What Are the Guidelines Under HIPAA Section 164?



<https://www.hhs.gov/hipaa/for-professionals/security/index.html>

# Eliminate Confusion – Example HIPAA

We analyzed every HIPAA 164.3x security control and aligned them to corresponding CIS 20 Control categories

## CIS Control 1: Inventory and Control of Hardware Assets

- 1.1 Utilize an Active Discovery Tool
- 1.2 Use a Passive Asset Discovery Tool
- 1.3 Use DHCP Logging to Update Asset Inventory
- 1.4 Maintain Detailed Asset Inventory
- 1.5 Maintain Asset Inventory Information
- 1.6 Address Unauthorized Assets
- 1.7 Deploy Port Level Access Control
- 1.8 Utilize Client Certificates to Authenticate Hardware Assets

## CIS Control 2: Inventory and Control of Software Assets

- 2.1 Maintain Inventory of Authorized Software
- 2.2 Ensure Software Is Supported by Vendor
- 2.3 Utilize Software Inventory Tools
- 2.4 Track Software Inventory Information
- 2.5 Integrate Software and Hardware Asset Inventories
- 2.6 Address Unapproved Software
- 2.7 Utilize Application Whitelisting
- 2.8 Implement Application Whitelisting of Libraries
- 2.9 Implement Application Whitelisting of Scripts
- 2.10 Physically or Logically Segregate High Risk Applications

## CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

- 6.1 Utilize Three Synchronized Time Sources
- 6.2 Activate Audit Logging
- 6.3 Enable Detailed Logging
- 6.4 Ensure Adequate Storage for Logs
- 6.5 Central Log Management
- 6.6 Deploy SIEM or Log Analytic Tools
- 6.7 Regularly Review Logs

## CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

- 9.1 Associate Active Ports, Services and Protocols to Asset Inventory
- 9.2 Ensure Only Approved Ports, Protocols and Services Are Running
- 9.3 Perform Regular Automated Port Scans
- 9.4 Apply Host-Based Firewalls or Port Filtering
- 9.5 Implement Application Firewalls

## CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

- 11.1 Maintain Standard Security Configurations for Network Devices
- 11.2 Document Traffic Configuration Rules
- 11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes
- 11.4 Install the Latest Stable Version of Any Security Related Updates on All Network Devices
- 11.5 Manage Network Devices Using Multifactor Authentication and Encrypted Sessions
- 11.6 Use Dedicated Workstations For All Network Administrative Tasks
- 11.7 Manage Network Infrastructure Through a Dedicated Network

## CIS Control 16: Account Monitoring and Control

- 16.1 Maintain an Inventory of Authentication Systems
- 16.2 Configure Centralized Point of Authentication
- 16.3 Require Multi-Factor Authentication
- 16.4 Encrypt or Hash all Authentication Credentials
- 16.5 Encrypt Transmittal of Username and Authentication Credentials
- 16.6 Maintain an Inventory of Accounts
- 16.7 Establish Process for Revoking Access

## CIS Control 8: Malware Defenses

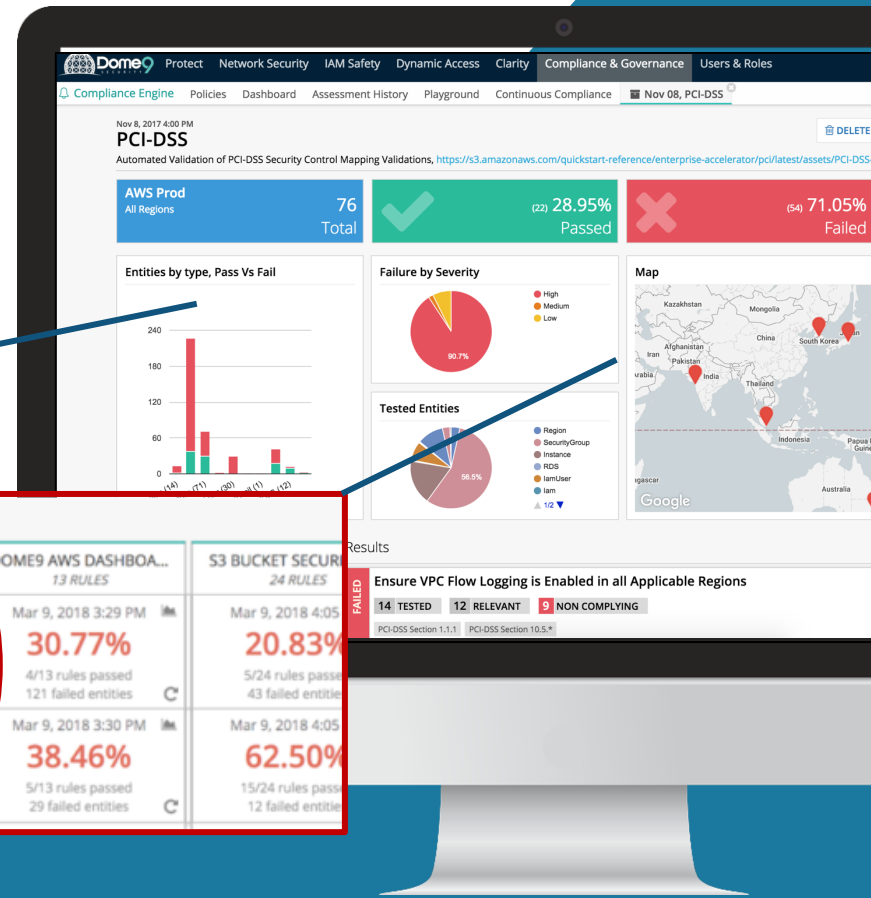
### CIS Control 8.1 - 8.8: Malware Defenses

- CIS Control 12.1 - 12.12: Boundary Defense
- CIS Control 16.8 - 16.13: Account Monitoring and Control
- CIS Control 19.1 - 19.8: Incident Response and Management
- CIS Control 20.1 - 20.8: Penetration Tests and Red Team Exercises

# Advanced Tooling

## Maintaining HIPAA Compliance Over Time

- Maintaining compliance without tolling after initial deployment can be hard
- Leveraging advanced 3<sup>rd</sup> party tools and alerting is imperative



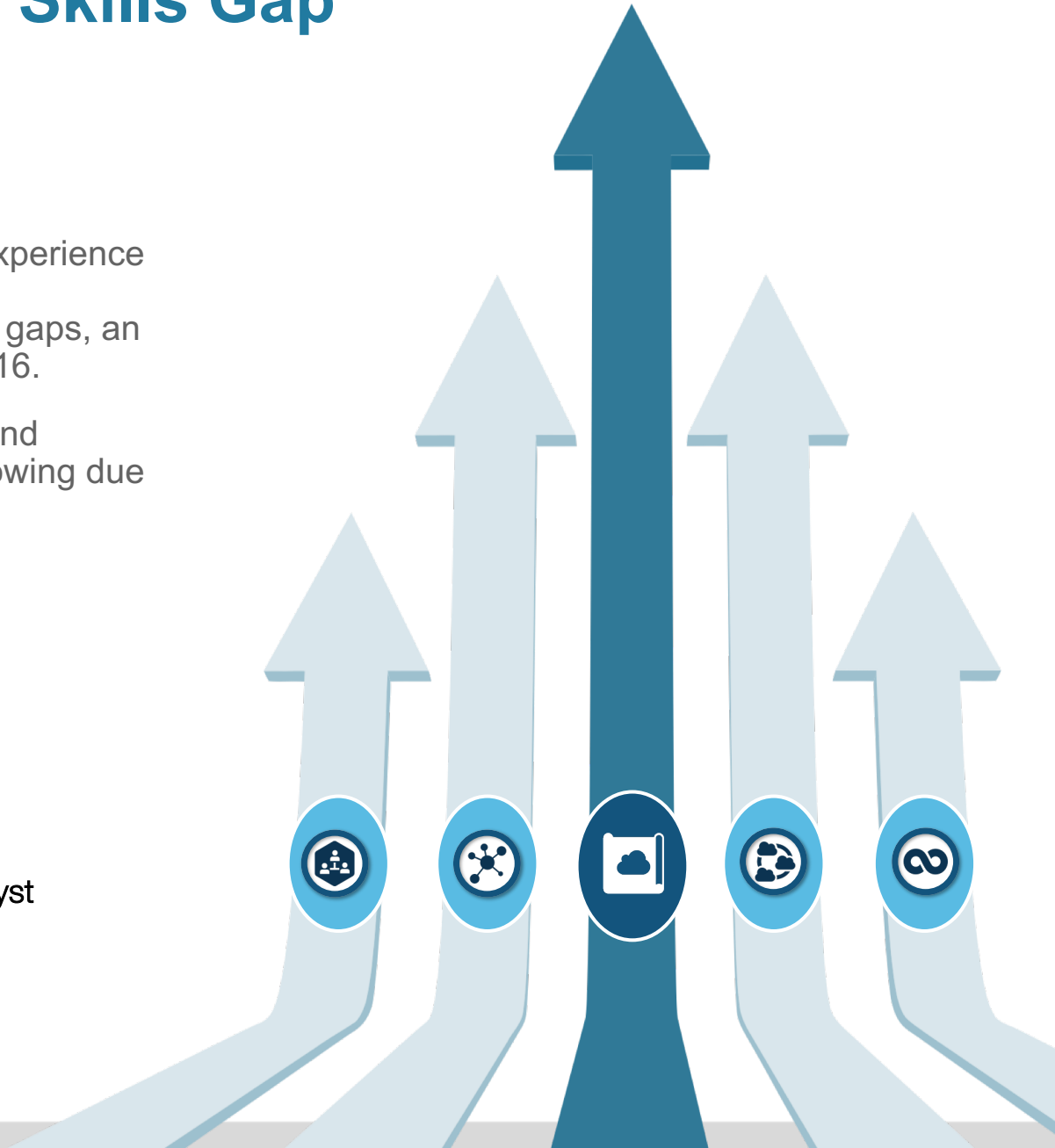
# Lesson Learned #2 – Skills Gap

Challenges of Managing The Current Enterprise Skills Gap

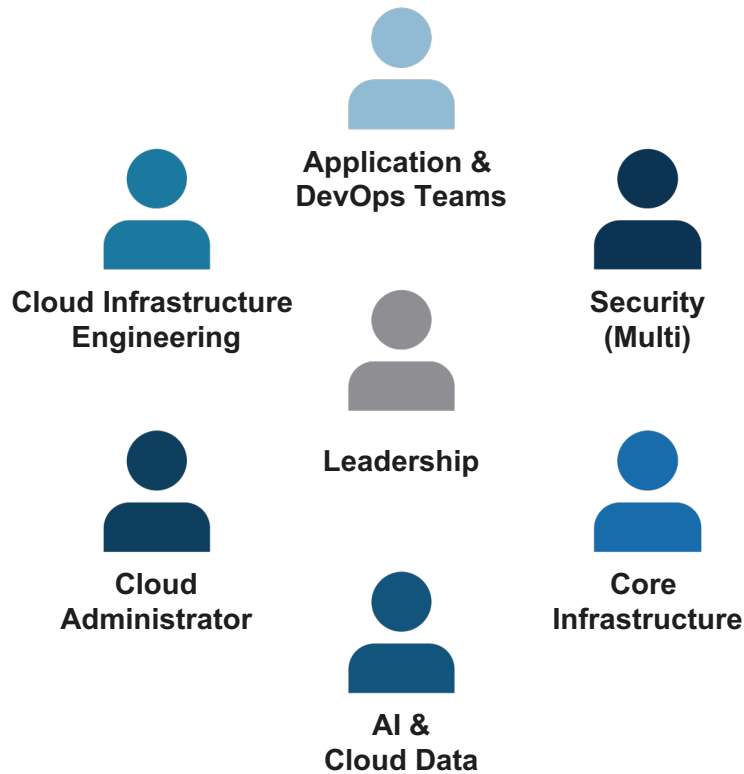
# Current Enterprise Skills Gap

- By 2020, 75% of enterprises will experience visible business disruptions due to infrastructure and operations skills gaps, an increase from less than 20% in 2016.
- Leaders confirm that the number and complexity of requirements are growing due to;
  - Internet of Things (IoT)
  - Hybrid IT infrastructure
  - Cloud migrations
  - DevOps requirements

Claudio Da Rold, Distinguished VP Analyst  
Gartner (2018)



# Create a Cloud Community of Excellence



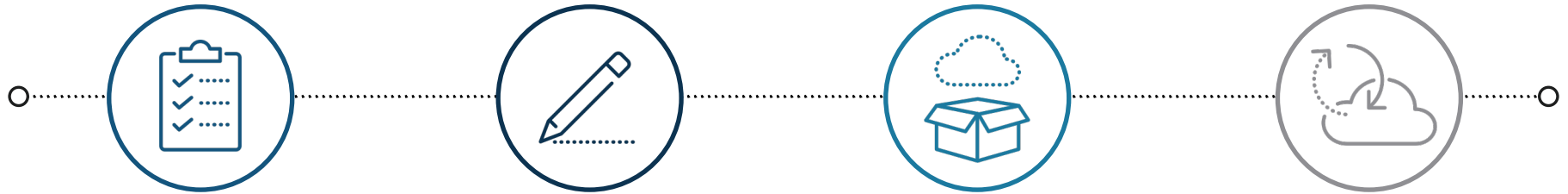
**Q:** Why Community vs Center of Excellence?

**A:** Center creates walls. Community enables and empowers people

## Charter

- Provide Business and Application Team with expertise to support digital transformation initiatives
- Culture and alignment of expectations
- Focused on ensuring Security, Performance, Availability, Cost Controls, Governance

# Cloud Team Responsibilities



## Governance

- Prioritize Services
- Validate Roadmap
- Analyze Costs & Financials Assess Staffing
- Establish Technical Direction
- Evangelize Cloud Services

## Plan

- Standardize Infrastructure Configurations
- Review Infrastructure Code
- Define Service Offerings
- Assess Application Placements
- Standardize Provisioning Process
- Resource Preservation Management

## Build

- Automate Services
- Implement & Maintain Code
- Analyze Capacity Management
- Develop OS Configurations
- Implement Security Policies

## Run

- Perform Compliance Monitoring
- Enforce security Configurations
- Report on Change Control Impacts
- Perform Private Cloud Fabric Additions
- Maintain Operational Uptime

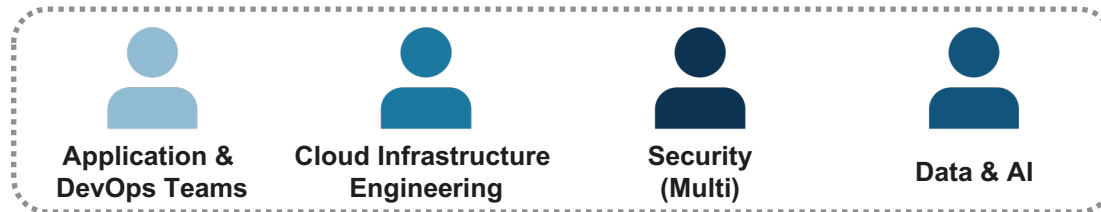


# Project Team Examples

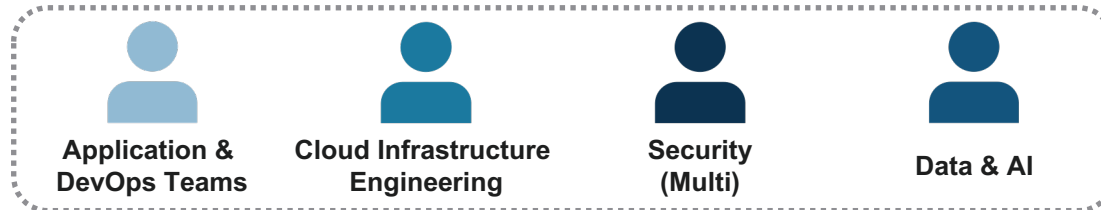


Leadership

3 Tier Stack



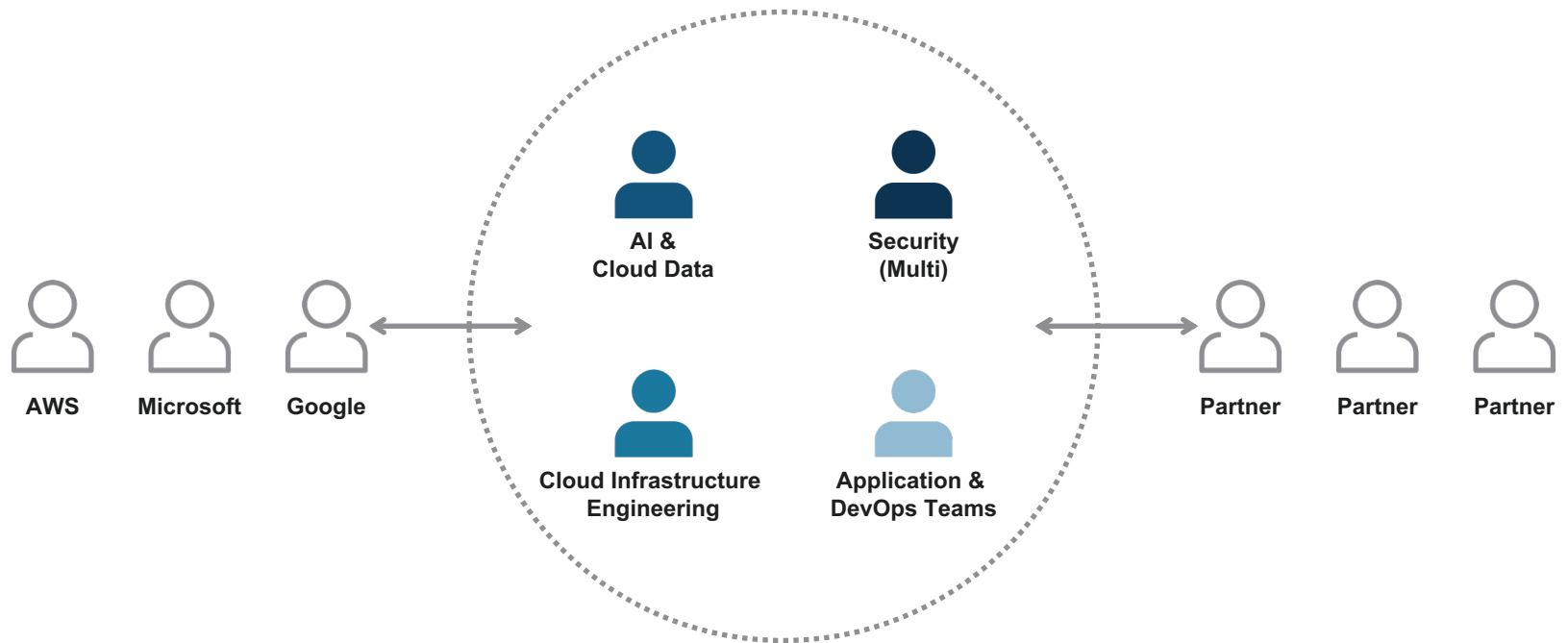
IoT Application



Simple App Service  
with Standard  
Security Framework



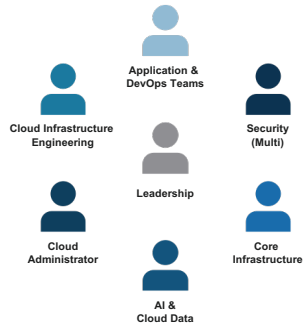
# Incorporate Vendors & Partners



\*Don't let Vendors/Partners become your CCOE

# Who's doing what?

## Tiger Team and Community



- Be the start
- Explore and evangelize services
- Drive POCs
- Training and Sharing
- Change control review

## Cost Optimization and Security (KTLO)



Group of people with responsibilities for keeping house in order.

- Cost Optimization
- Sprawl
- Weekly/Monthly Checks (Scheduled)

## Architecture Review Board

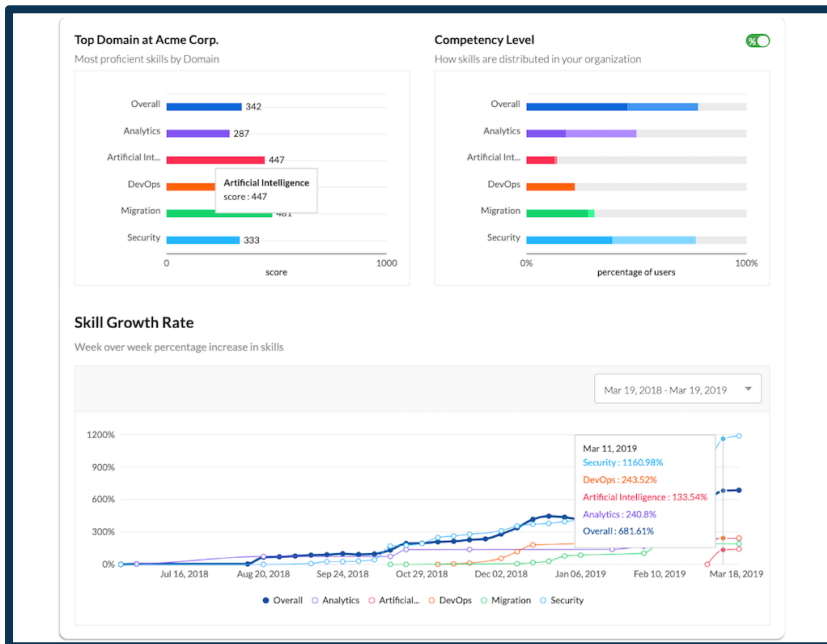


- Review architectures before deployment
- Enforce Standards
- Review Automation Processes

# Developing Training Plans

Skill Assessments  
(Establish Baseline)

Develop Customized Training Plans  
(Assess, Assign, and Keep Training on Track)



Status	Teams	Title	Progress	Exam Score	Tracking
✓	Cloud Developer	Fundamentals of AWS	89%	75%	--
✓	Data Engineer	Fundamentals of AWS	100%	73.12%	--
✓	Network Engineer	Fundamentals of AWS	100%	80.47%	--
✓	DevOps Engineer	DevOps Tools	100%	80.42%	--
✓	Security Engineer	Fundamentals of AWS	100%	98.09%	--
✓	Solutions Architect	Fundamentals of AWS	100%	90%	--
●	Cloud Developer	Full-Stack Developer - AWS - Starter	94%	91.25%	4 days ahead
✓	Digital Skills Off...	Business Manager Fundamentals	100%	72.5%	--
✓	Data Engineer	Big Data on AWS	0%	0%	--
✓	Security Engineer	AWS Security	100%	100%	--
✓	Solutions Architect	Solutions Architect Associate Certification for AWS	100%	80.95%	--
●	DevOps Engineer	DevOps Engineer Certification for AWS	96%	14.28%	3 days behind
✓	Digital Skills Off...	Fundamentals of AWS	100%	94.66%	--
✓	Data Engineer	Big Data on Azure and GCP	26%	80.62%	--

# Lesson Learned #3 – Master One Cloud First

Concentrate First on Getting One Cloud Provider Right

# The Multi-Cloud Myth



## Impact on Skills, Training, and Hiring



For most organizations, we recommend seeking deep technical and specialist talent within a single public cloud in order to maximize efficiency and engineering depth.

## Operationalizing a Single Cloud Provider



Build the right enterprise guardrails, security, and operational controls and get those right in one platform rather than try to duplicate them across multiple cloud providers.

## Concentrate First on Getting One Cloud Provider Right



While there are benefits to a multi-cloud strategy, the potential risks outweigh the gains.

# Build a Public Cloud Operating Model



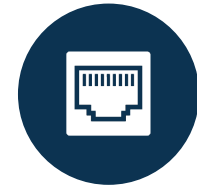
Education



Account  
Structure



Common  
Services



Network



Storage, Backup and  
Disaster Recovery



Identity and Access  
Management



Automation and  
Orchestration



Enterprise Service  
Management Integration



Monitoring and  
Operations



Security



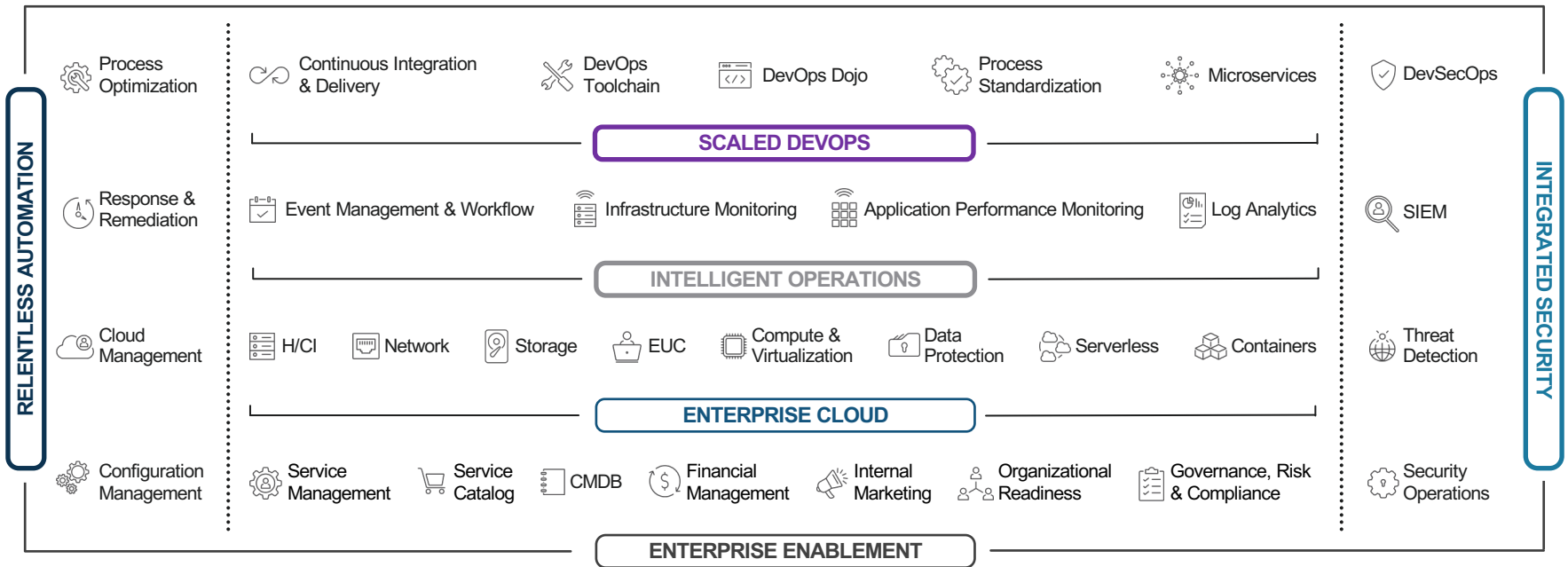
Cost Controls



Governance

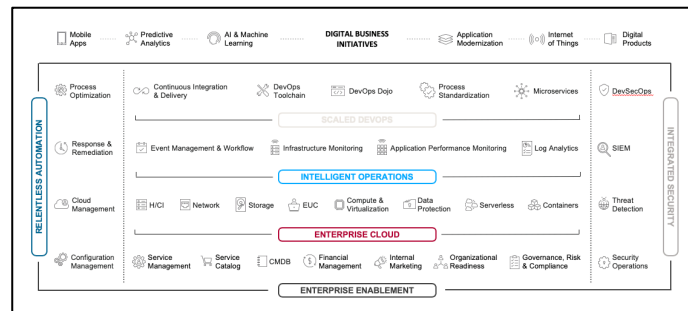
# Digital Delivery Platform

Mobile Apps ..... 
 Predictive Analytics ..... 
 AI & Machine Learning ..... 
 **DIGITAL BUSINESS INITIATIVES** ..... 
 Application Modernization ..... 
 Internet of Things ..... 
 Digital Products





# Enterprise Ready Cloud Platform



Digital Delivery Platform

# Questions?



# **BUILDING DIGITAL PLATFORMS FOR HEALTHCARE**