DISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

HOSTING AND COMPUTE CENTER
Actio Non Verba
DEFENSE INFORMATION SYSTEMS AGENCY

DoD Cloud IaC

Dave Lago

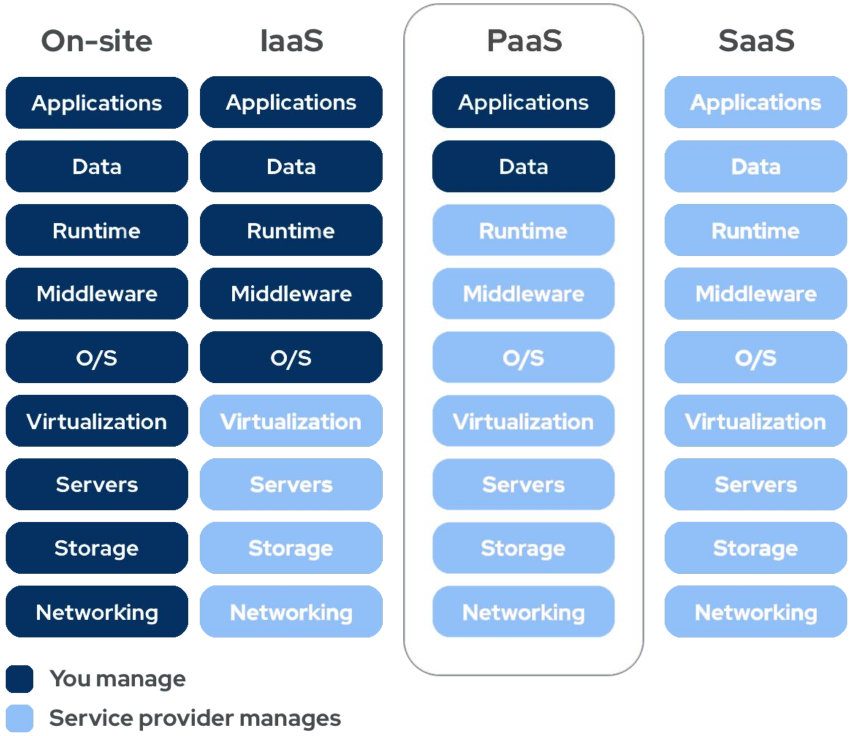
Product Manager
DISA HaCC

DoD Cloud Infrastructure as Code – Accelerate Cloud Adoption

DoD Cloud IaC are baselines that leverage IaC automation to generate **pre-configured, pre-authorized, Platform as a Service (PaaS)**-focused environments. Whenever possible, DoD Cloud IaC leverages security services offered by Cloud Service Providers (CSP) over traditional data center tools. DoD Cloud IaC helps customers adopt cloud faster.

Highlights

- **Takes 7 months off typical cloud journey**
  - Baselines for both Azure and AWS, Google in works
  - Supports IL2, IL4 and IL5 workloads. IL6 underway
  - PaaS focused; leveraging CSP Security Tools
- Only decentralized IaC baseline with ATO from DISA RME and Common Controls available for inheritance in eMASS
- Only IaC baseline available in Azure Marketplace
- Only IaC baseline developed under CRADAs w/ CSPs
- We help deploy baselines in a 3-4 hour session for free
- Completed 21 DoD Components deployments



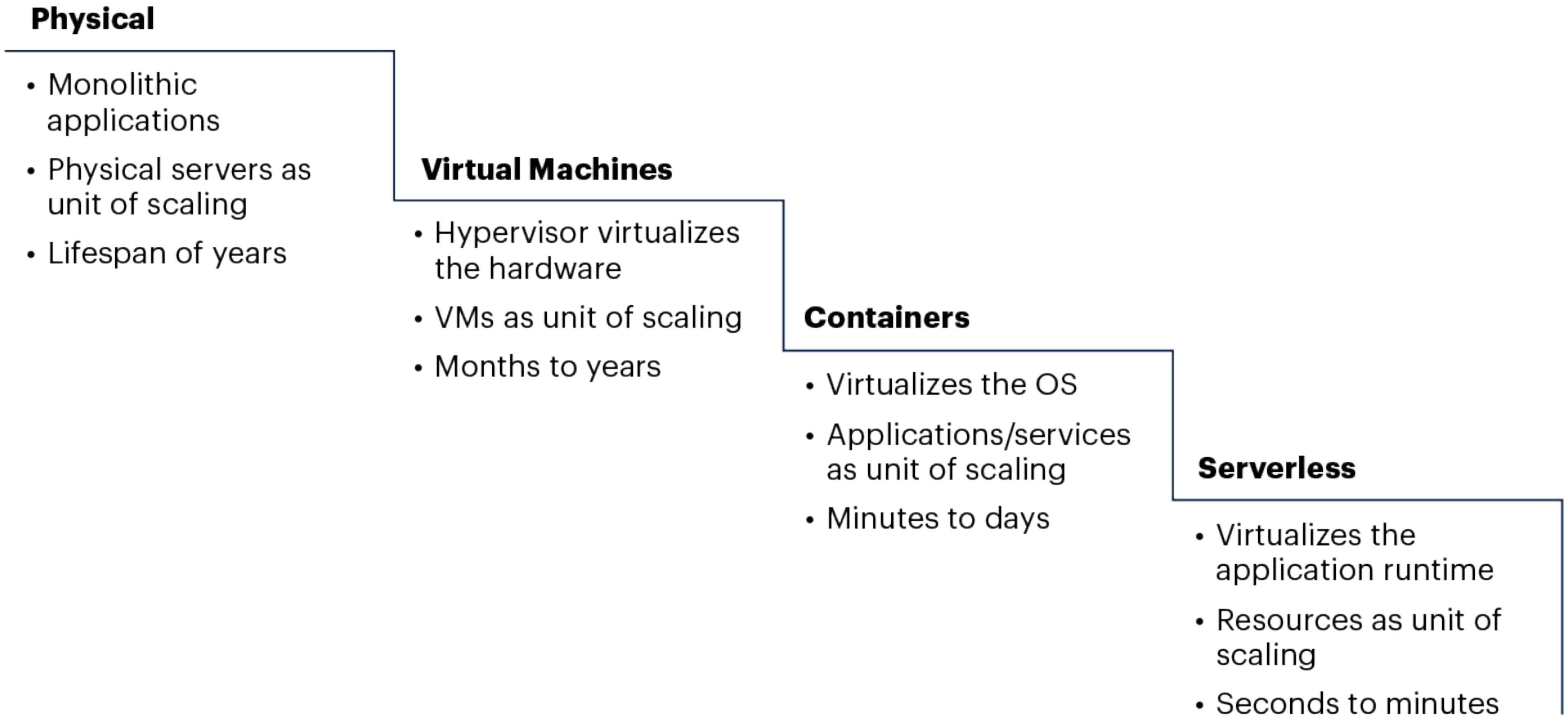
On-site	IaaS	PaaS	SaaS
■ Applications	■ Applications	■ Applications	□ Applications
■ Data	■ Data	■ Data	□ Data
■ Runtime	■ Runtime	□ Runtime	□ Runtime
■ Middleware	■ Middleware	□ Middleware	□ Middleware
■ O/S	■ O/S	□ O/S	□ O/S
■ Virtualization	□ Virtualization	□ Virtualization	□ Virtualization
■ Servers	□ Servers	□ Servers	□ Servers
■ Storage	□ Storage	□ Storage	□ Storage
■ Networking	□ Networking	□ Networking	□ Networking

■ You manage

□ Service provider manages

DoD Cloud IaC   Azure   aws   Google Cloud Platform

Workload Evolution



Physical

- Monolithic applications
- Physical servers as unit of scaling
- Lifespan of years

Virtual Machines

- Hypervisor virtualizes the hardware
- VMs as unit of scaling
- Months to years

Containers

- Virtualizes the OS
- Applications/services as unit of scaling
- Minutes to days

Serverless

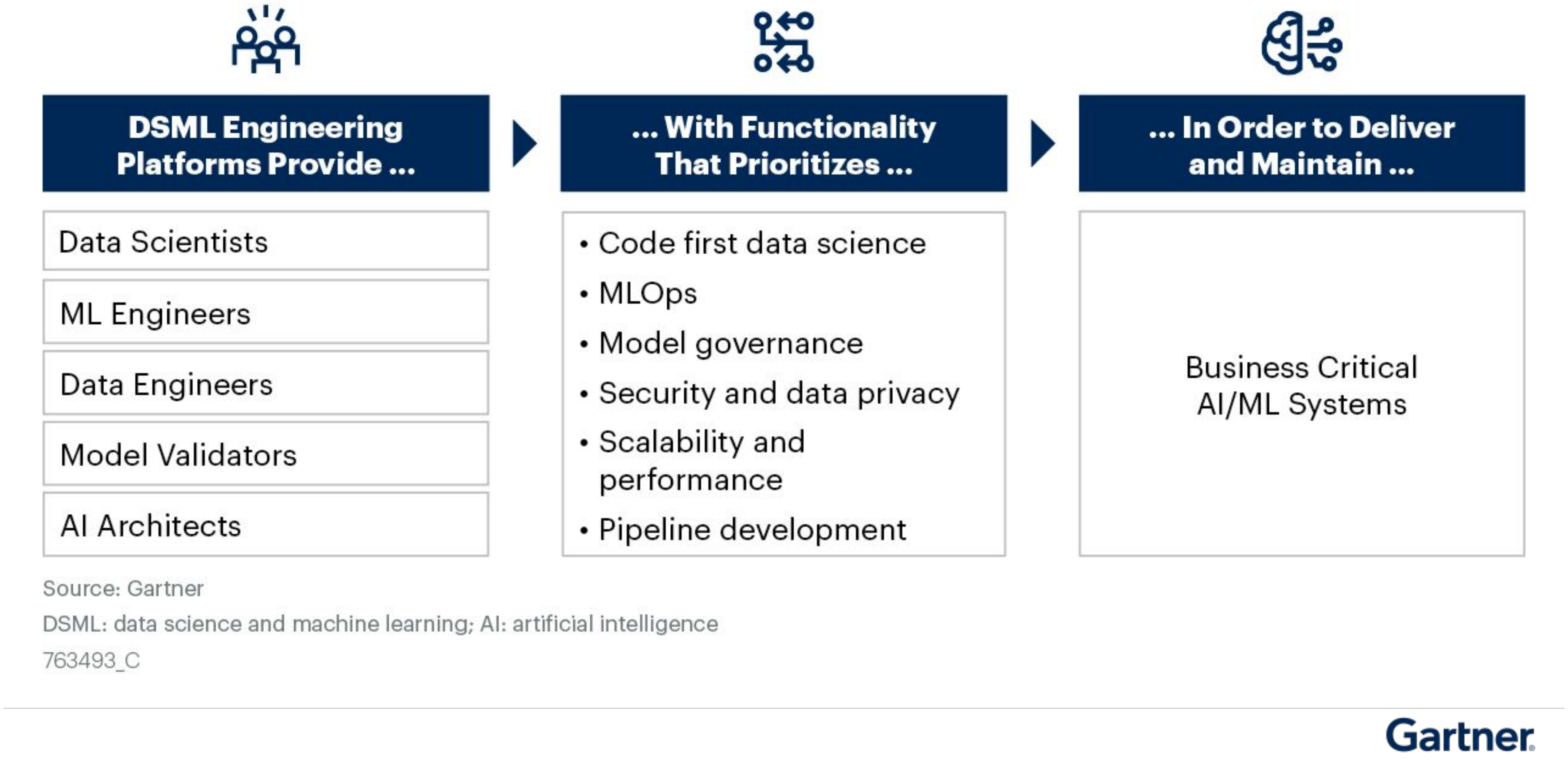
- Virtualizes the application runtime
- Resources as unit of scaling
- Seconds to minutes

Source: Gartner

716192_C

Gartner

Data Science and Machine Learning (DSML) Platforms



DSML Engineering Platforms Provide ...

- Data Scientists
- ML Engineers
- Data Engineers
- Model Validators
- AI Architects

... With Functionality That Prioritizes ...

- Code first data science
- MLOps
- Model governance
- Security and data privacy
- Scalability and performance
- Pipeline development

... In Order to Deliver and Maintain ...

Business Critical AI/ML Systems

Source: Gartner

DSML: data science and machine learning; AI: artificial intelligence

763493_C

Gartner

DoD Cloud IaC for Azure at IL2, IL4, IL5

- **Supporting Services**
  - Azure Active Directory
  - Azure Activity Logs
  - Azure Alerts
  - Azure Bastion
  - Azure Cloud Shell
  - Azure DDoS Protection
  - Azure Firewall
  - Azure Frontdoor
  - Azure Key Vault
  - Azure Log Analytics Notebook
  - Azure Network Security Groups
  - Azure Policies
  - Azure Security Center
  - Azure Sentinel
  - Azure Service Heath
  - Azure VNET
  - Azure Web Application Firewall
- **Application & DB Hosting**
  - Azure App Service
  - Azure Database
  - Azure Cosmos DB
  - Azure Cache for Redis
- **Containers**
  - Azure Kubernetes Service
  - Azure Container Registry
- **Serverless**
  - Azure Functions
  - Azure Event Hub
- **Storage**
  - Azure Blog Storage
  - Azure Data Lake
- **Virtual Machines***
  - Azure Virtual Machines
  - Azure Defender for Cloud
- **AI/ML**
  - Azure Machine Learning
- **Internet of Things (IoT)**
  - Azure IoT Hub
- **Hybrid Cloud**
  - Azure Data Factory
- **API Management**
  - Azure API Management
- **Maps**
  - Azure Maps

DoD Cloud IaC for AWS at IL2, IL4, IL5

- **Supporting Services**
  - AWS Audit Manager
  - AWS Cloud Trail
  - AWS CloudWatch
  - Amazon Cognito
  - AWS Config
  - AWS Network Firewall
  - Amazon GuardDuty
  - AWS Identity & Access Management (IAM)
  - AWS Key Management Service
  - AWS Organizations
  - AWS Security Hub
  - AWS Service Catalog
  - AWS Transit Gateway
  - Amazon Virtual Private Cloud
- **Containers**
  - AWS Elastic Kubernetes Service- Fargate*
  - AWS Elastic Container Service (ECS)- Fargate
  - Amazon Container Registry
- **Database Hosting**
  - Amazon Aurora
  - Amazon DynamoDB
- **Serverless**
  - AWS Lambda
- **AI/ML**
  - Amazon Sagemaker
- **IoT**
  - AWS IoT Greengrass
- **Hybrid**
  - AWS Storage Gateway
- **Managed Desktop**
  - Amazon AppStream 2.0

DoD Cloud IaC for Google at IL2, IL4, IL5

- **Supporting Services**
  - Google Cloud Armor
  - Google Cloud Logging
  - Google Cloud Monitoring
  - Google Cloud Identity & Access Management
  - Google Data Loss Prevention API
  - Google Cloud Security Command Center
  - Google Forseti*
  - Google Cloud IDS*
  - Google Virtual Private Cloud
  - 3rd Party Firewall
  - Google Cloud Router
  - Google Cloud Interconnect (BCAP)
  - VPC/Firewall Flow Logs
  - Google Cloud KMS
  - Identity Platform (GD)
  - Google Cloud Trace
  - Google Cloud Load Balancing
  - Google Cloud Storage

- **Containers**
  - Google Kubernetes Engine
  - Google Anthos
  - Google Container Registry
  - Container Analysis*
  - Container Threat Detection*
- **Database**
  - Google BigQuery
- **Virtual Machines**
  - Google Compute Engine
  - Persistent Disk
- **Additional VDMS Services**
  - Endpoint Protection Networking*
  - Vulnerability Scanning*

**Post MVP Enhancement*

- GCP AI/ML services are currently not available at IL4/IL5
- GCP AI/ML services will begin to be added to DoD Cloud IaC for Google baseline in Fall 2022

Google Cloud Platform

IaC in Use: Blue Heron C2 System for OAR

TRANSCOM Air Mobility Command (AMC) built a Command and Control (C2) system in 16 days w/ 3 FTE and a 10k budget to support OPERATION ALLIED REFUGE in Afghanistan

The DoD Cloud IaC for Azure baseline was used to deploy a serverless architecture to scale from pilot to production in 72 hours

Contact Us

- **To learn about DoD Cloud IaC**
  - https://www.hacc.mil/Products/DOD-IaC/
- **To review documentation - IaC Repo Instructions, Security Guide etc** (Requires CAC)
  - https://intelshare.intelink.gov/sites/ccpo/_layouts/15/start.aspx#/IaCDocuments/Forms/AllItems.aspx
- **To join the DoD Cloud IaC Community of Practice (COP)**
  - Email: osd.mc-alex.dod-cio.mbx.dod-iac@mail.mil (Limited to .mil email addresses only)
- **To ask specific questions or request a deployment session**
  - https://www.hacc.mil/Contact-Us/Product-Questions/
  - Email: dodcloudiac_support@ccpo.mil