

UNIVERSITY OF OSLO

TEK5530 Measurable Security for the Internet of Things

L14 Cloud Principles & Cloud Security

Josef Noll
Professor
Department of Technology Systems

UNIVERSITY
OF OSLO



<https://beststructured.com/intrusion-detection-intrusion-prevention-and-antivirus-the-differences/>





Cloud – Security – IoT

- What is cloud computing
- Delivery models and shared responsibility
- Cloud architecture
- Cyber- vs Cloud Security

What is cloud computing

- A remote pool of (shared) resources on different levels
- Dynamic provisioning, elastic use of resources, pay-as-you-go
- A type of outsourcing

- Increased utilization of resources, economy of scale
- Multi-tenancy
- Global reach
- Running expense vs capital expense
- High availability – but assumes (fast) internet connectivity
- Deployment: public, private, hybrid and community

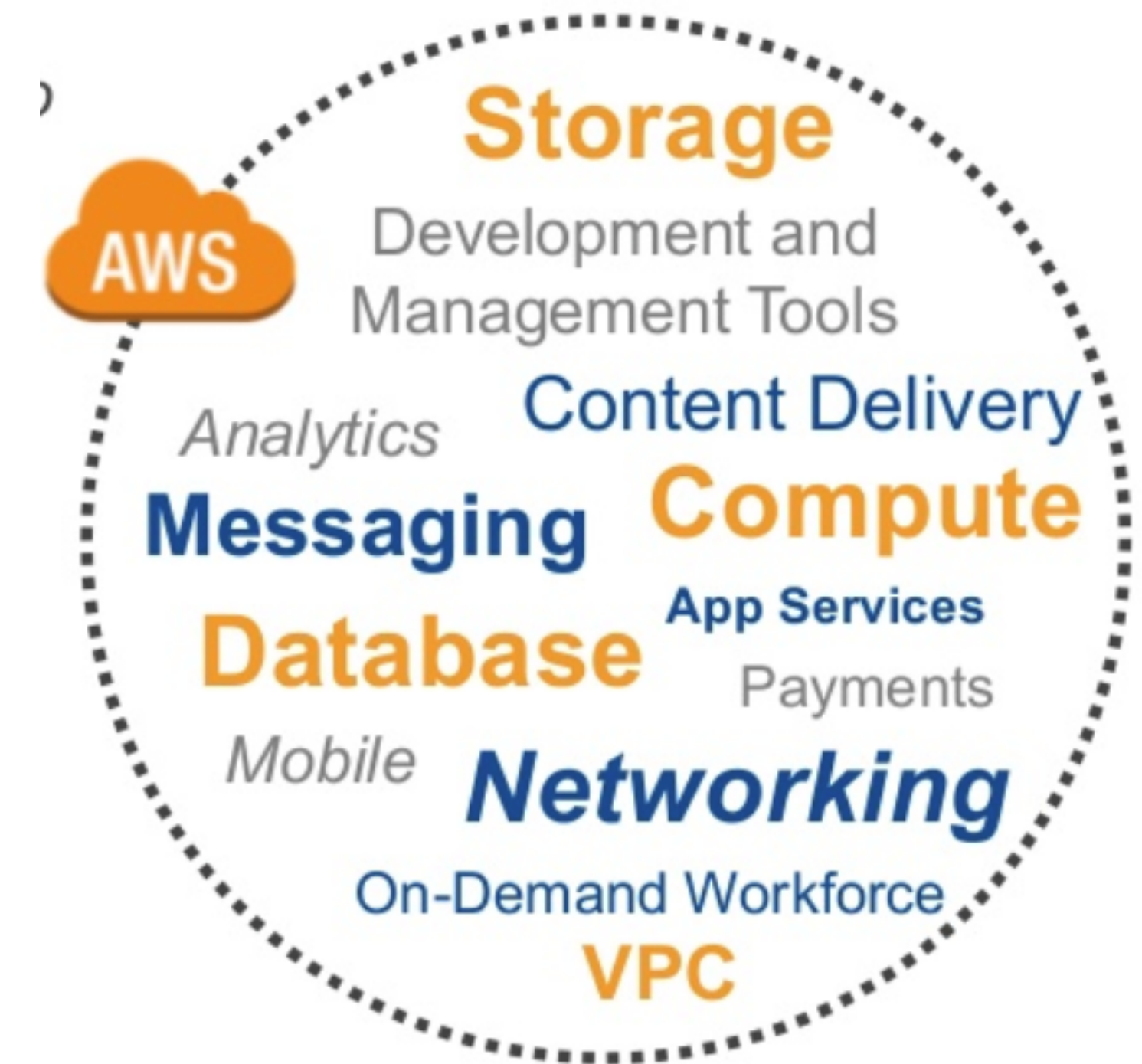
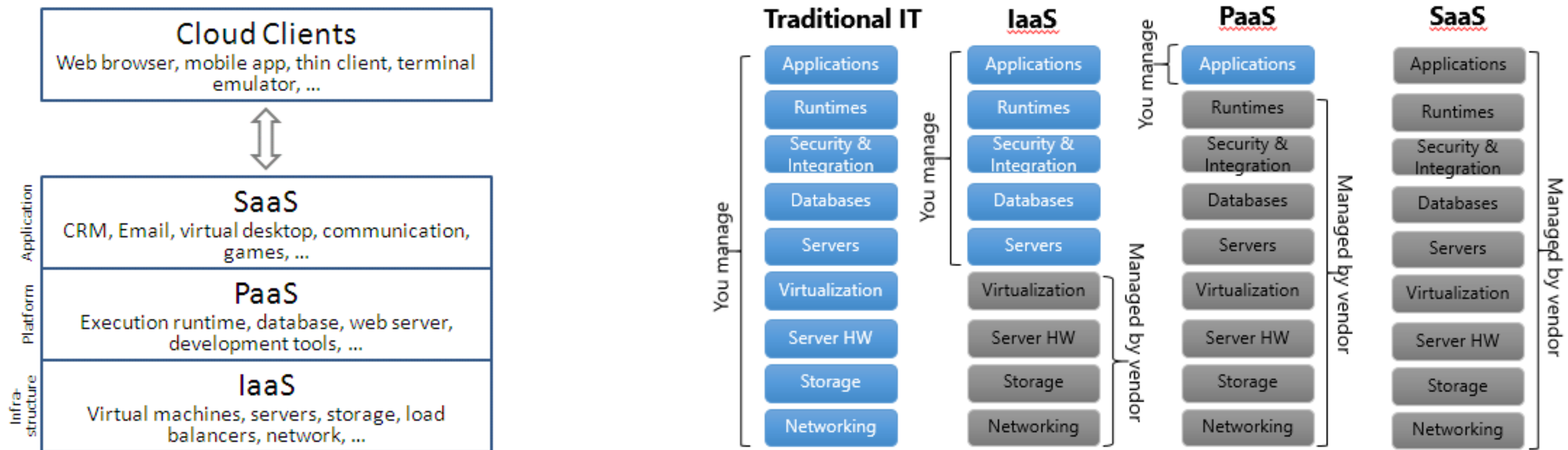


Figure from <https://www.slideshare.net/AmazonWebServices/awesome-day-nashville-2018training>

Delivery models

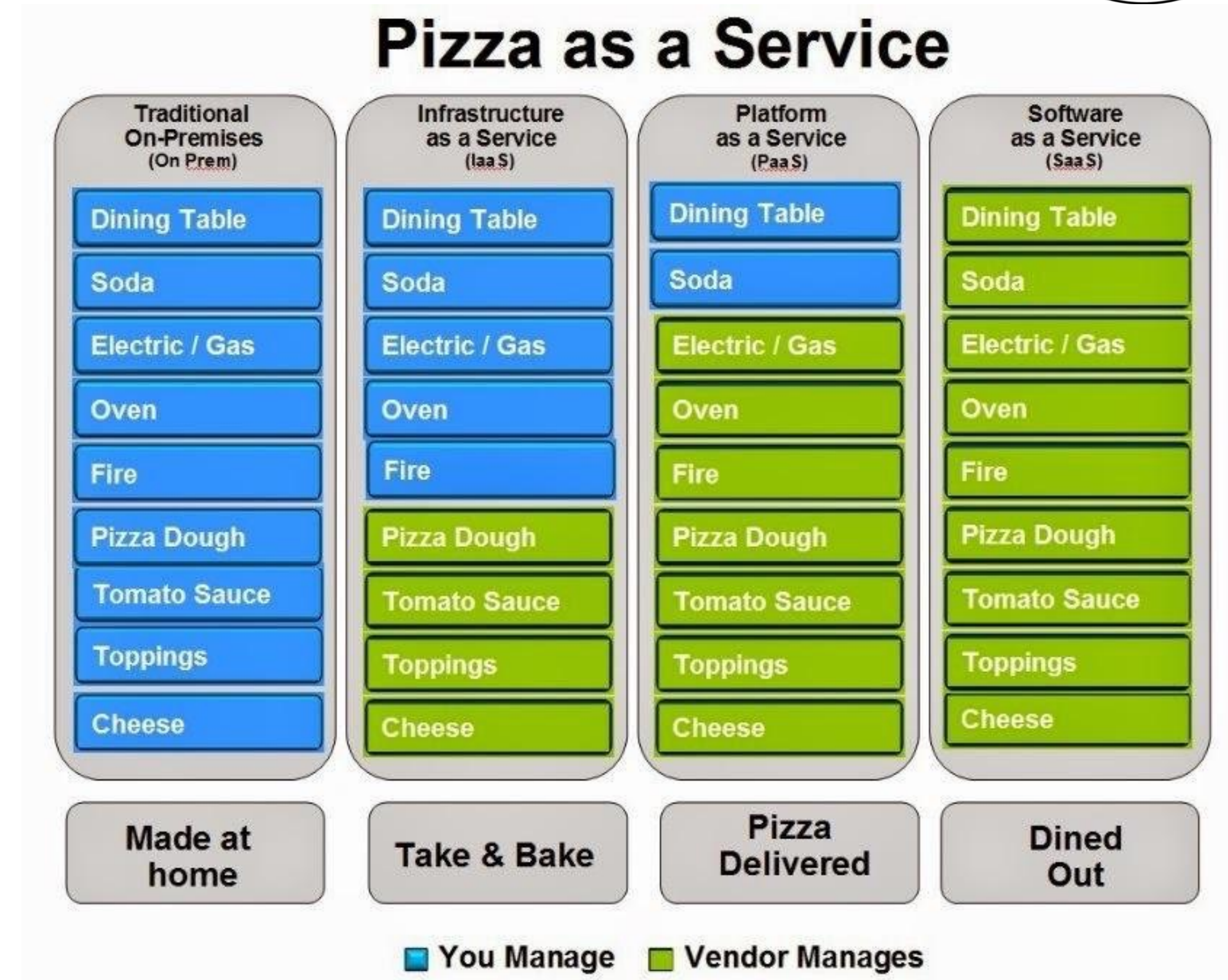
- ➔ Infrastructure as a Service (IaaS)
- ➔ Platform as a Service (PaaS)
- ➔ Software as a Service (SaaS)



Both figures are from: <http://oracle-help.com/oracle-cloud/cloud-computing-stack-saas-paas-iaas/>

Delivery models contd.

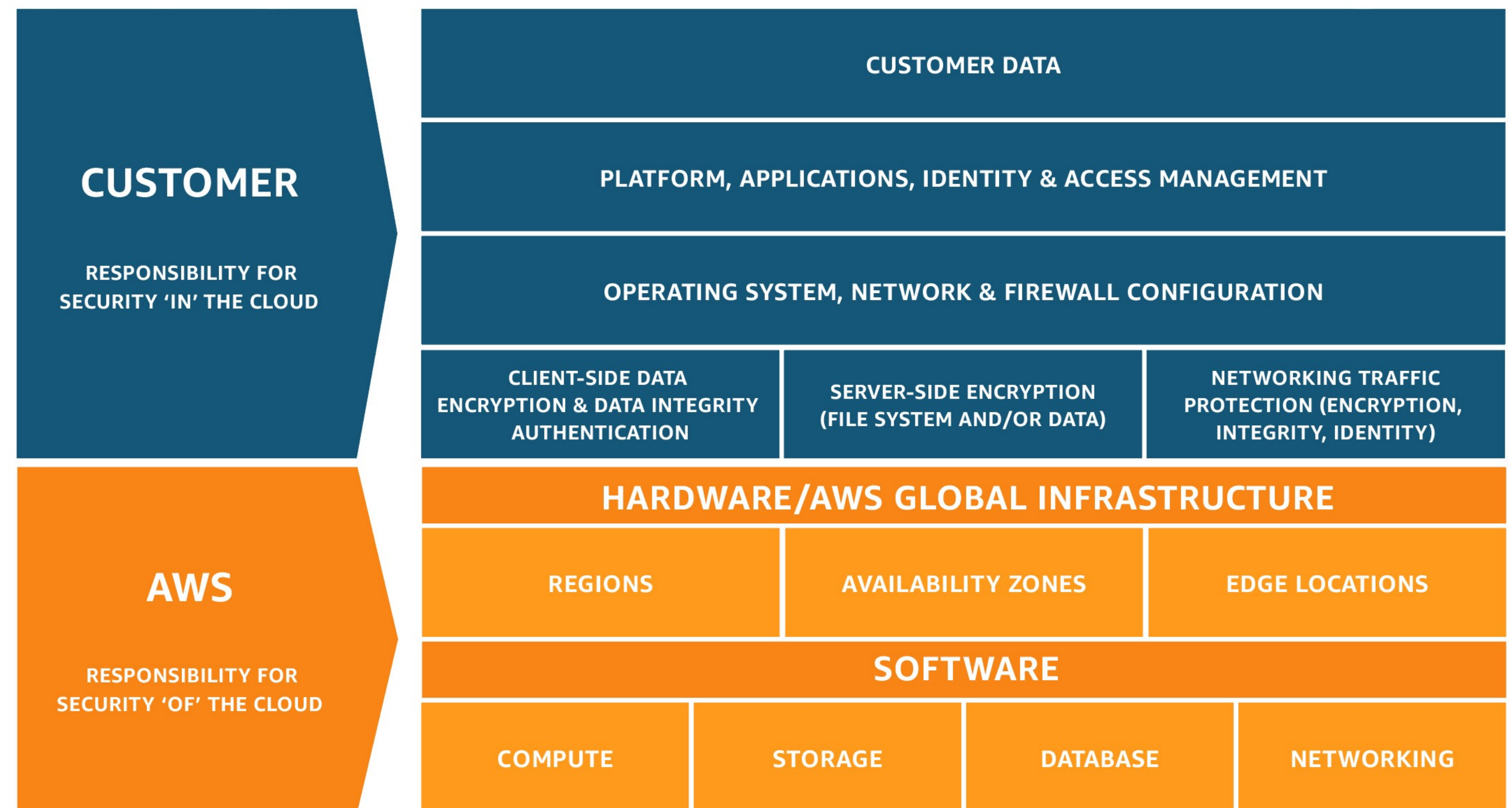
→ A perfect figure from Fred Bals at Episerver



<https://www.episerver.com/learn/resources/blog/fred-bals/pizza-as-a-service/>

AWS Shared Responsibility Model

- ➔ AWS responsibility is to provide a reliable and secure infrastructure, where the customer services can be built on, a «foundation»
- ➔ Customer responsibility is determined by the services chosen
- ➔ Wide range of services
- ➔ And third party deliveries

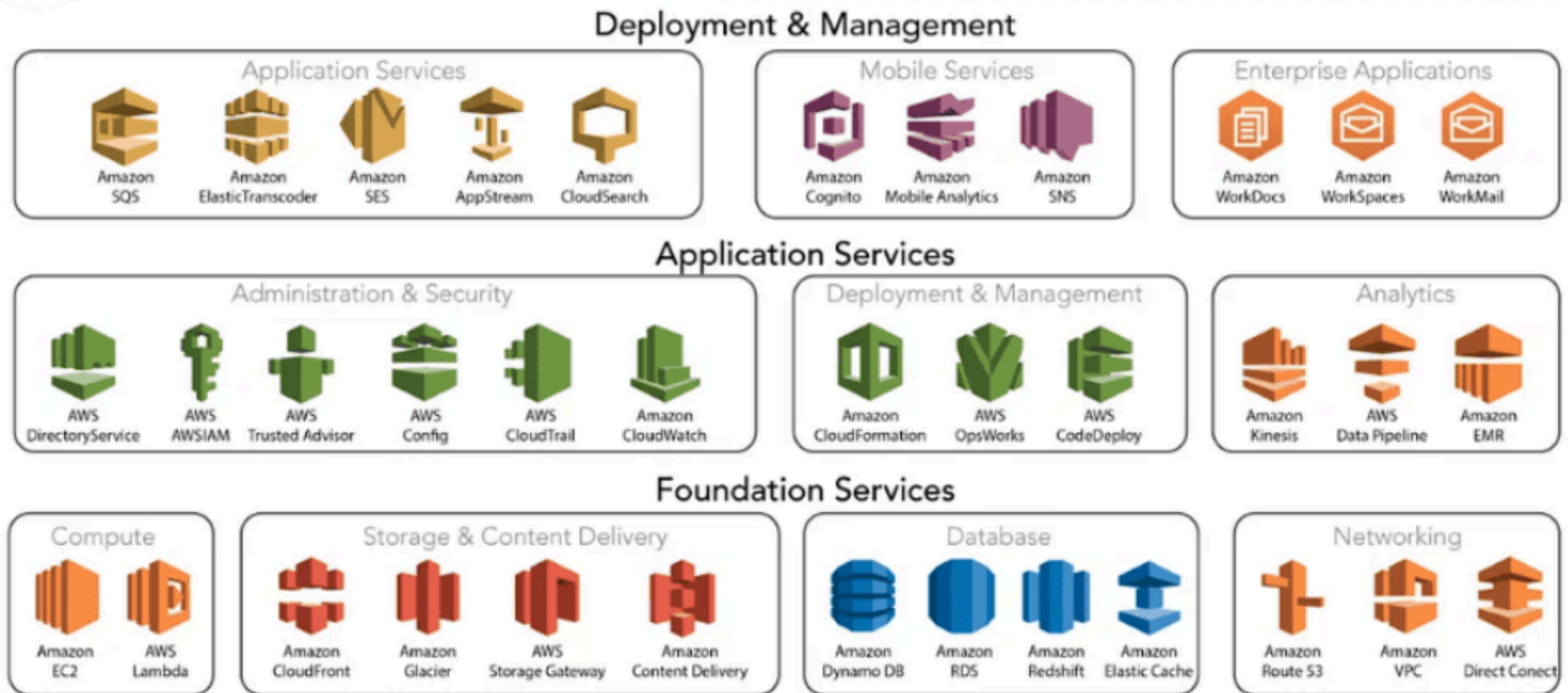


<https://aws.amazon.com/compliance/shared-responsibility-model/>

AWS in a nutshell

<https://k21academy.com/amazon-web-services/overview-of-amazon-web-services-concepts/>

- Launched in 2006, originally to utilise computing capacity investment for Christmas season
- 100+ features released every year, 200+ applications



Security infrastructure

- Principles and tools
- Identity and Access Management, Certificates
- Security services
 - Security Group, Internet gateway, NAT gateway
 - Network security: Intrusion Detection System (IDS), Web Application Firewall (WAF), network functions
 - Vulnerability management
 - Data encryption and protection

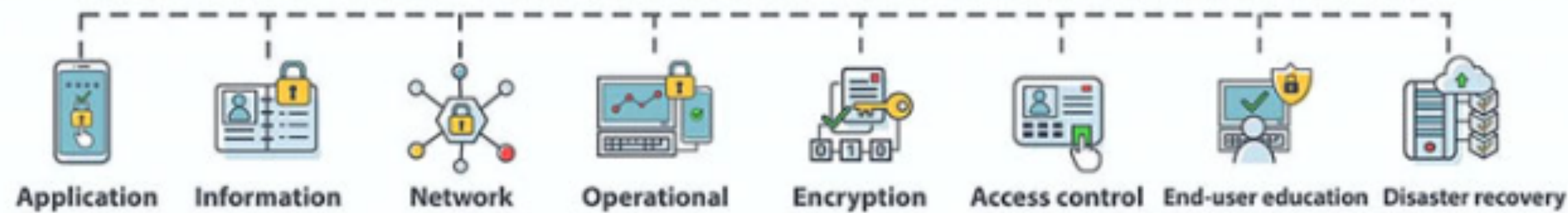
WAF layered defenses

- | **Cloudflare managed rules** offer advanced zero-day vulnerability protections.
- | Core **OWASP rules** block familiar “Top 10” attack techniques.
- | **Custom rulesets** deliver tailored protections to block any threat.
- | **WAF Machine Learning** complements WAF rulesets by detecting bypasses and attack variations of RCE, XSS and SQLi attacks.
- | **Exposed credential checks** monitor and block use of stolen/exposed credentials for **account takeover**.
- | **Sensitive data detection** alerts on responses containing sensitive data.
- | **WAF content scanning** protects your web servers and enterprise network from malware by scanning files uploaded to your application in-transit.
- | **Advanced rate limiting** prevents abuse, DDoS, brute force attempts along with API-centric controls.
- | **Flexible response options** allow for blocking, logging, rate limiting or challenging.

<https://www.cloudflare.com/en-gb/application-services/products/waf/>

Cyber vs Cloud Security

CYBER SECURITY



- ➔ Cloud Security Threats, a.o.
 - DDoS
 - Data breaches
- ➔ Reasons
 - cloud misconfiguration
 - insider attacks
- ➔ Main defence: infrastructure, people, layers
 - Access control, two-factor authentication, passwordless solutions
 - Minimum privilege
 - Monitoring



CLOUD SECURITY VS NETWORK SECURITY

NETWORK SECURITY	CLOUD SECURITY
Network security is the superset of cloud security	Subset of network security
Combines multiple layers of defences at the edge and in the network. Comprises of both hardware and software-based solutions	Is centralised cloud-based security solutions that focuses on software solutions
Network security solutions include email security, firewalls, anti-virus, anti-malware, app security, access control, mobile devices security, VPN, wireless security	Cloud security solutions include data centre security, threat detection, threat prevention, threat mitigation, and legal compliance
High infrastructure cost in case of on-premise	Low upfront infrastructure required
Slow scaling in case of on-premise	Quickly scalable
Encompasses both on-premises and on-cloud security	For on-cloud security only

<https://secureops.com/blog/cloud-vs-cyber/>

Identity and Access Management (IAM)

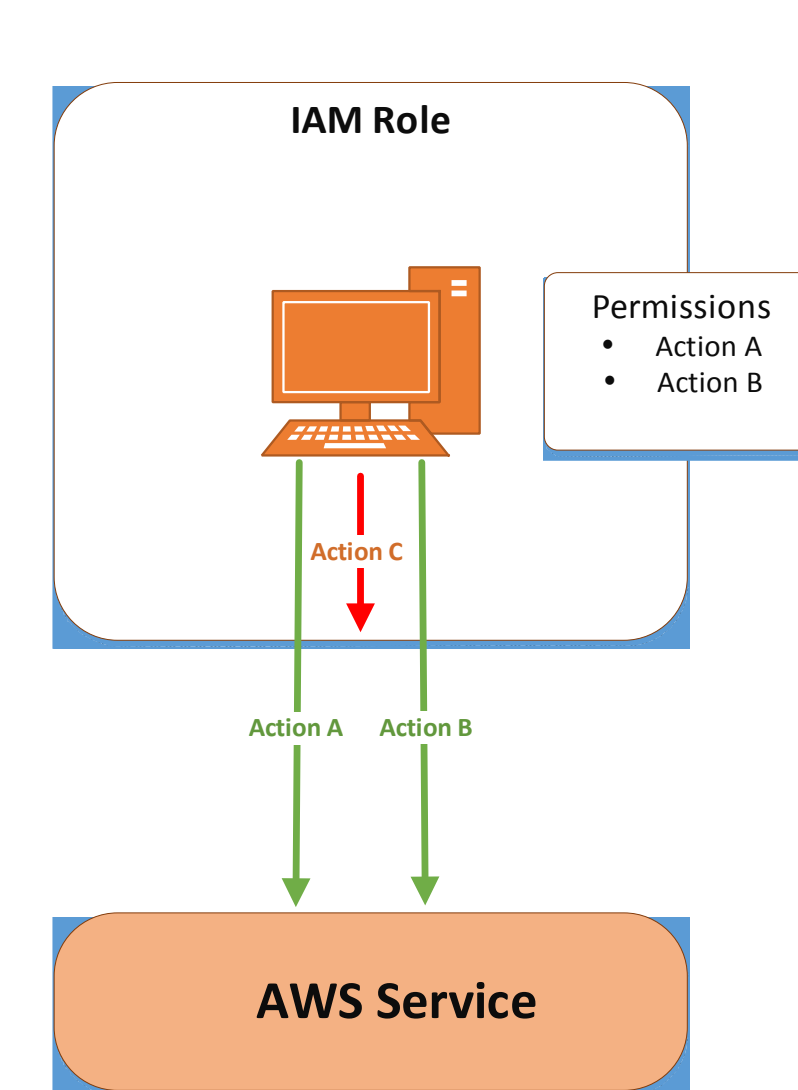
- Controls access to resources and services run on AWS
 - Manage and set up permissions for users and applications
 - Supports federation through standard interfaces
- Main components are: policy, role and group:
 - Policy defines the actions, resources and other options
 - Role is an identity with policies connected to it
 - Group is an entity, which can connect to multiple common policies



Why have they not introduced S-ABAC?

Identity and Access Management best praxis

- Minimise root account use,
 - multi-factor authentication is a must for root, enable at first use,
 - create own Identity & Access Management (IAM) role at once, root shall not be used for management
- Create individual user accounts
 - use personal accounts, helps both in forensics and keeping your users cautious
- Use groups and roles, avoid granting an access rule directly to a user
- Use own roles for applications e.g. run on EC2
- Use AWS default policies if you can - least privilege



Cryptographic services – storage and database

- S3 server side (encryption after data is received):
 - S3-managed keys: SSE-S3
 - AWS Key management Service (KMS)
 - Customer-provided keys: SSE-C
- S3 client side (encryption before data is sent):
 - Use an AWS KMS-managed customer master key
 - Use a client side master key
- Database:
 - server side with KMS, server side with Hardware Security Models (HSM),
 - client side, support depends on the actual database solution (most support for KMS)

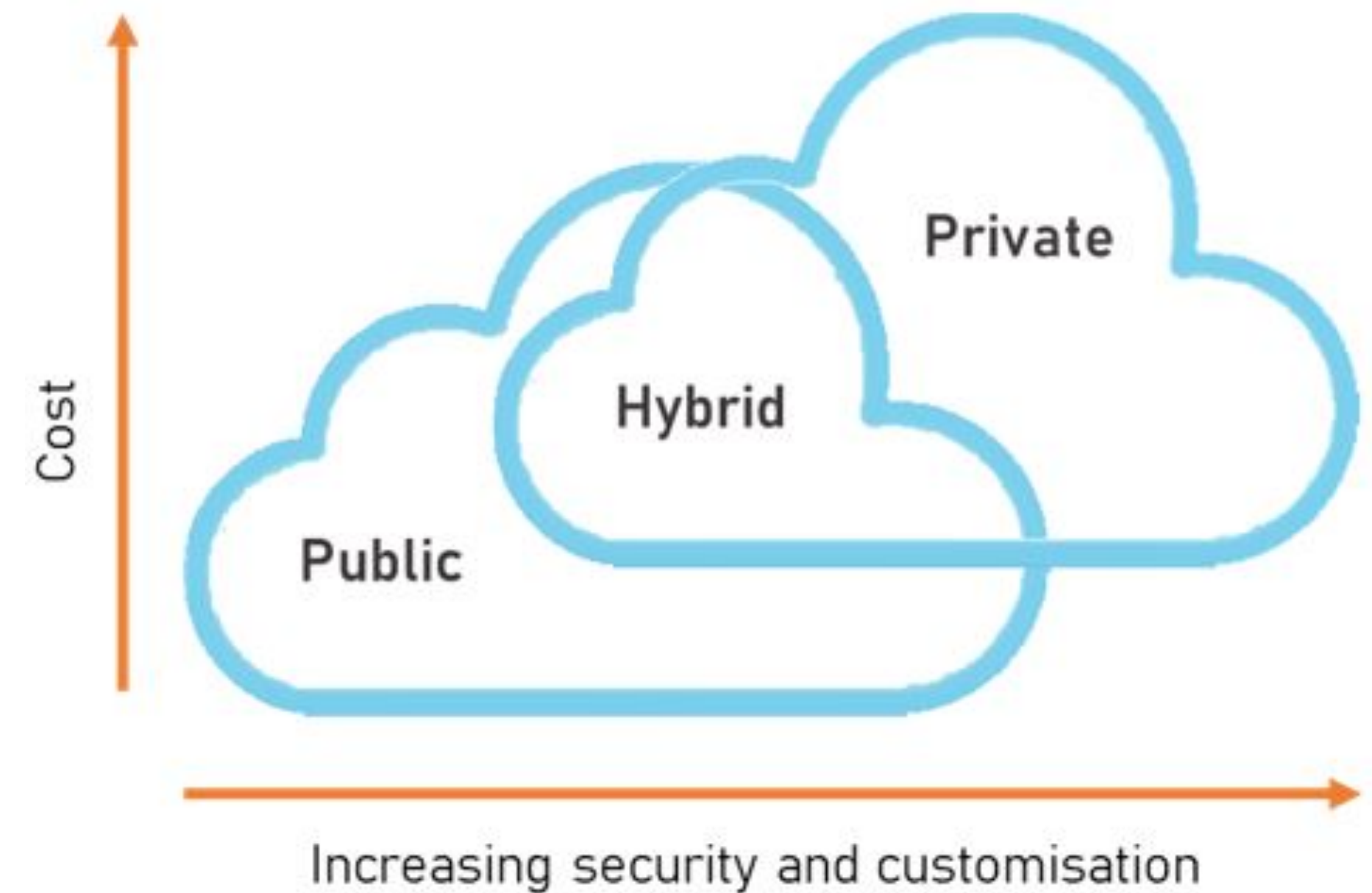
Hardware Security Module (HSM)



<https://youtu.be/szagwwSLbXo> Hardware Security Models

AWS Logging: monitoring, forensics and compliance

- Sources:
 - CloudTrail: records AWS API calls
 - CloudWatch logs and events (alarms)
 - Load balancer logs
 - S3 logs
 - AWS Identity & Access Management (IAM)
 - Virtual Private Cloud (VPC) flowlogs
 - This looks like e.g. a wireshark capture
- Add-on services, e.g. Splunk
 - Security Analysis and Response
 - Security and Compliance



<https://www.businesstechweekly.com/operational-efficiency/cloud-computing/private-cloud-vs-public-cloud/>

AWS IoT

- In general: exploit the global reach, flexible infrastructure
- Larger operations are especially interesting: predictive maintenance, traffic management, logistics, demand estimation
- Provides infrastructure to get information from the edge and process it with AWS services.
- An interesting feature is the Rules engine, which can be queried with SQL-like expressions
- Higher-level services built on the acquired data (e.g. traffic stats -> prediction)
- Device Shadow, use Lambdas

Main steps in AWS IoT

“Securely connect one or one-billion devices to AWS, so they can interact with applications and other devices”

1

Securely connect any physical device to AWS



Connect any device via MQTT/HTTP securely. Quickly get started with AWS IoT Starter Kits and Scale to billions of messages across millions of devices

2

Respond to signals from your fleet of devices and take action with Rule Engine



Shift business logic from device to cloud and route data to AWS service of your choice for storage and analysis using rules engine.

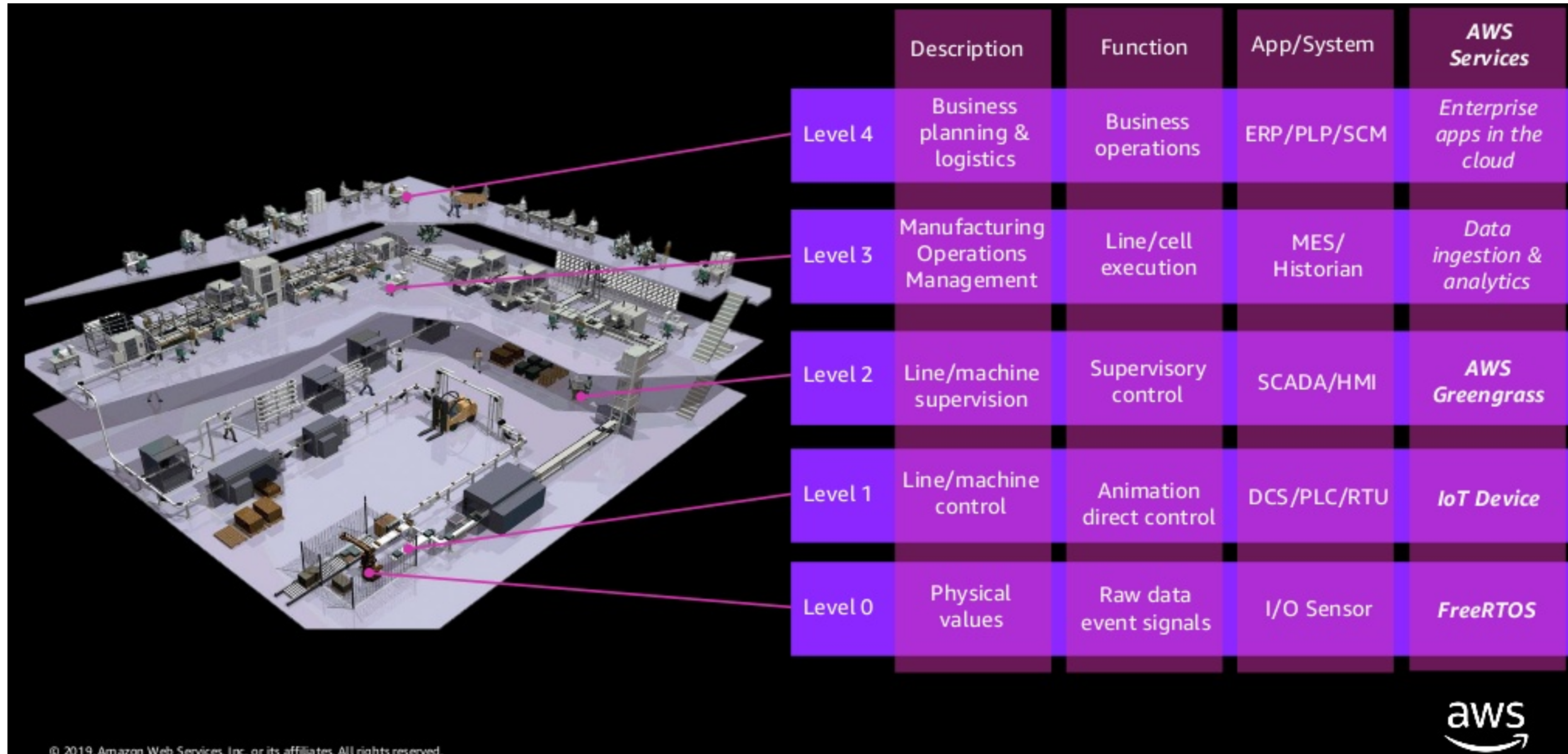
3

Create Web and Mobile Applications that Interact with Devices reliably at any time



Easily build applications on web and mobile that interact with devices, even when they are offline, with AWS SDK and Device Shadow.

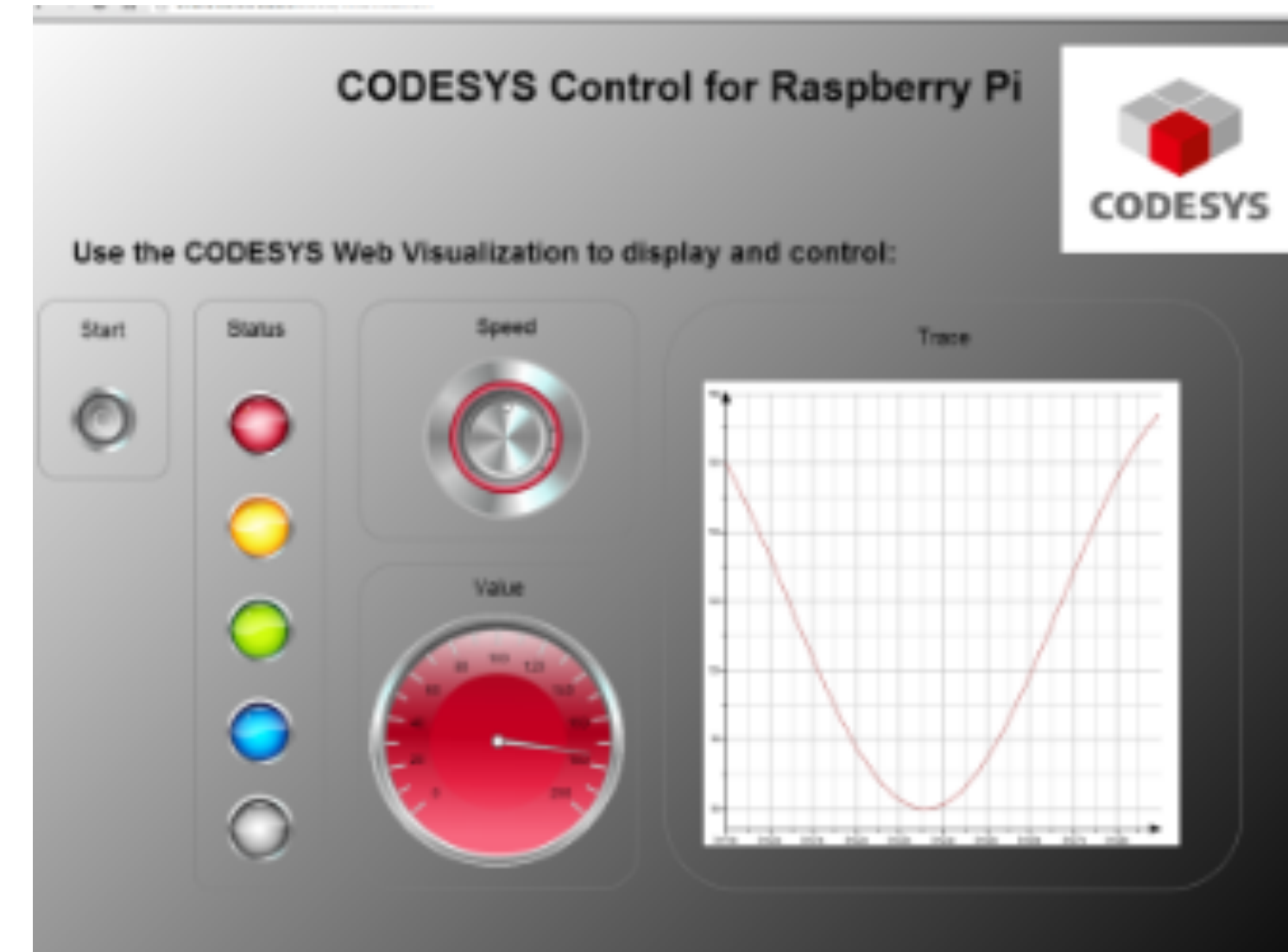
AWS in relation to ISA-95



<https://www.slideshare.net/AmazonWebServices/aws-intelligent-at-edge-for-iiot>

Cutting Automation Costs

- ➔ Software solutions
 - virtualisation
 - small-scale, e.g. PLC for Raspberry Pi (55 €)
- ➔ how do you control?



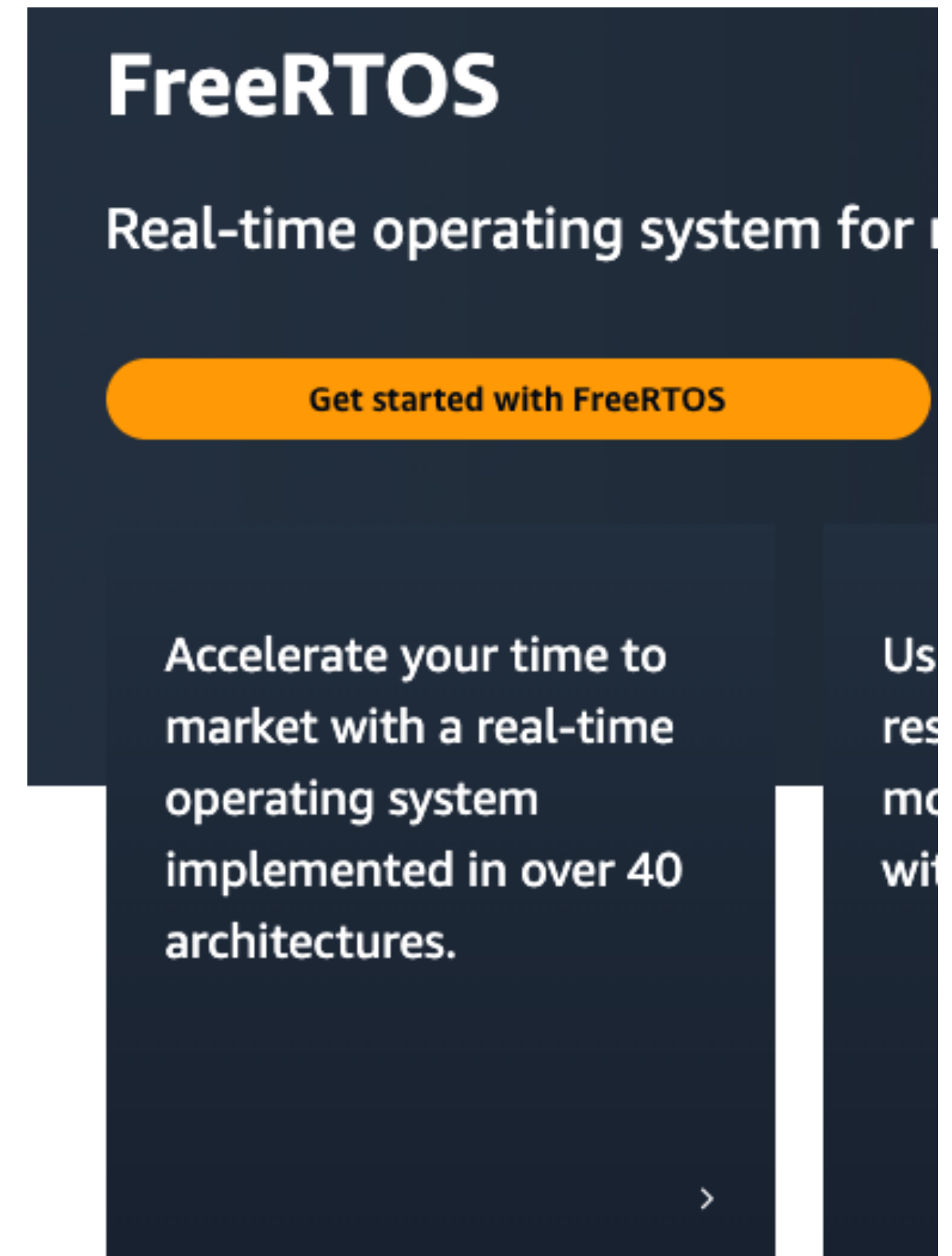
<https://store.codesys.com/codesys-control-for-raspberry-pi-sl.html>

PLC + PC + SCADA	Soft PLC + SCADA	SBC + SCADA
<i>Required for control:</i>	<i>Required for control:</i>	<i>Required for control & remote data:</i>
PLC (CPU 416-3 PN/DP) ----- €8.000	Panel PC (Windows) ----- €3.400	Raspberry Pi 3 model B+ ----- €33
PLC components ----- €3.600	Simatic Net Licentie ----- € 600	Raspberry Pi components ----- €50
Brewmaxx Express V9 500 ----- €11.000	SoftPLC ViCA (Pentair owned) ----- €0	Codesys control for RPi SL ----- €50
Panel PC ----- €3.400	Office home and business ----- €200	Codesys Runtime Key, kompakt ---- €45
Office home and business ----- €200		15" Flat panel ----- €760
<i>Required for remote data</i>		
Simatic Net Licentie ----- € 600		
Raspberry Pi cloud gateway ----- € 83*		
Total costs ----- €26.883	Total costs ----- €4.200	Total costs ----- €950

<https://www.slideshare.net/AmazonWebServices/aws-intelligent-at-edge-for-iot>

AWS FreeRTOS

- A free RTOS with extensions to connect to AWS services
 - Key importance for getting market share
 - OS is important in the budget of embedded projects

A promotional banner for FreeRTOS. It features the text "FreeRTOS" in large white font, followed by "Real-time operating system for" in smaller white font. Below this is an orange button with the text "Get started with FreeRTOS". Further down, it says "Accelerate your time to market with a real-time operating system implemented in over 40 architectures." and "Us res mo wi". There is a white arrow pointing right at the bottom right of the banner.

FreeRTOS
Real-time operating system for

Get started with FreeRTOS

Accelerate your time to market with a real-time operating system implemented in over 40 architectures.

Us res mo wi

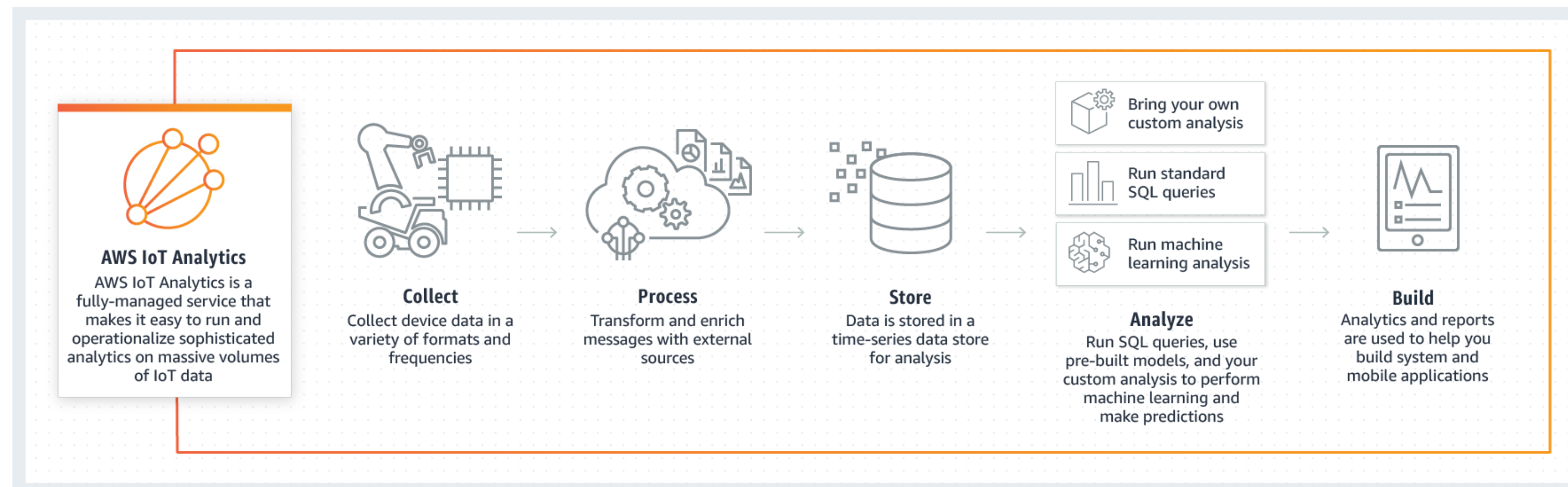
<https://aws.amazon.com/freertos/>

IoT and analytics - SiteWise

→ A combination of insight into IoT and processing power and analytics in cloud allows us to work on optimisations in different fields:

- Classification
- Route optimisation
- Anomaly detection
- Prediction and forecast
- Language processing
- KPI identification

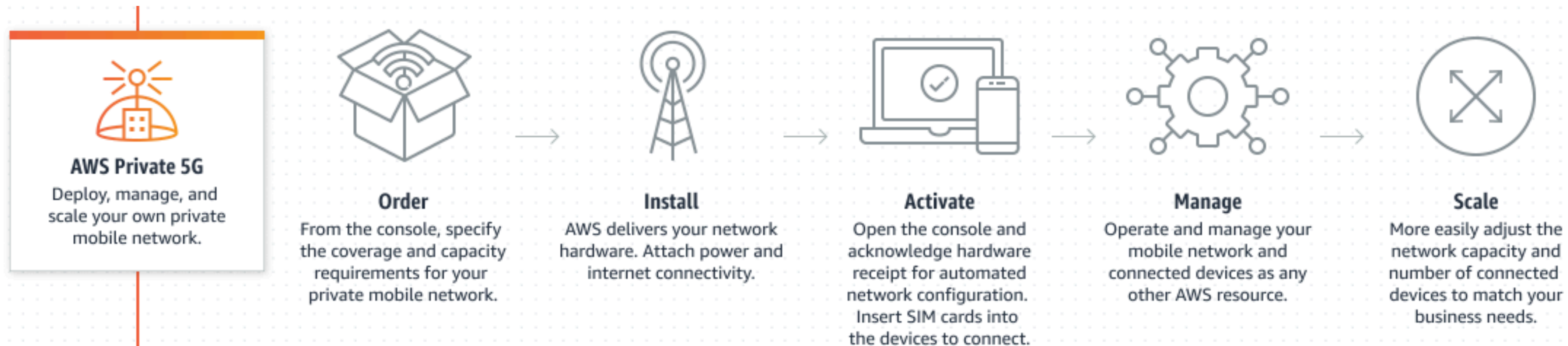
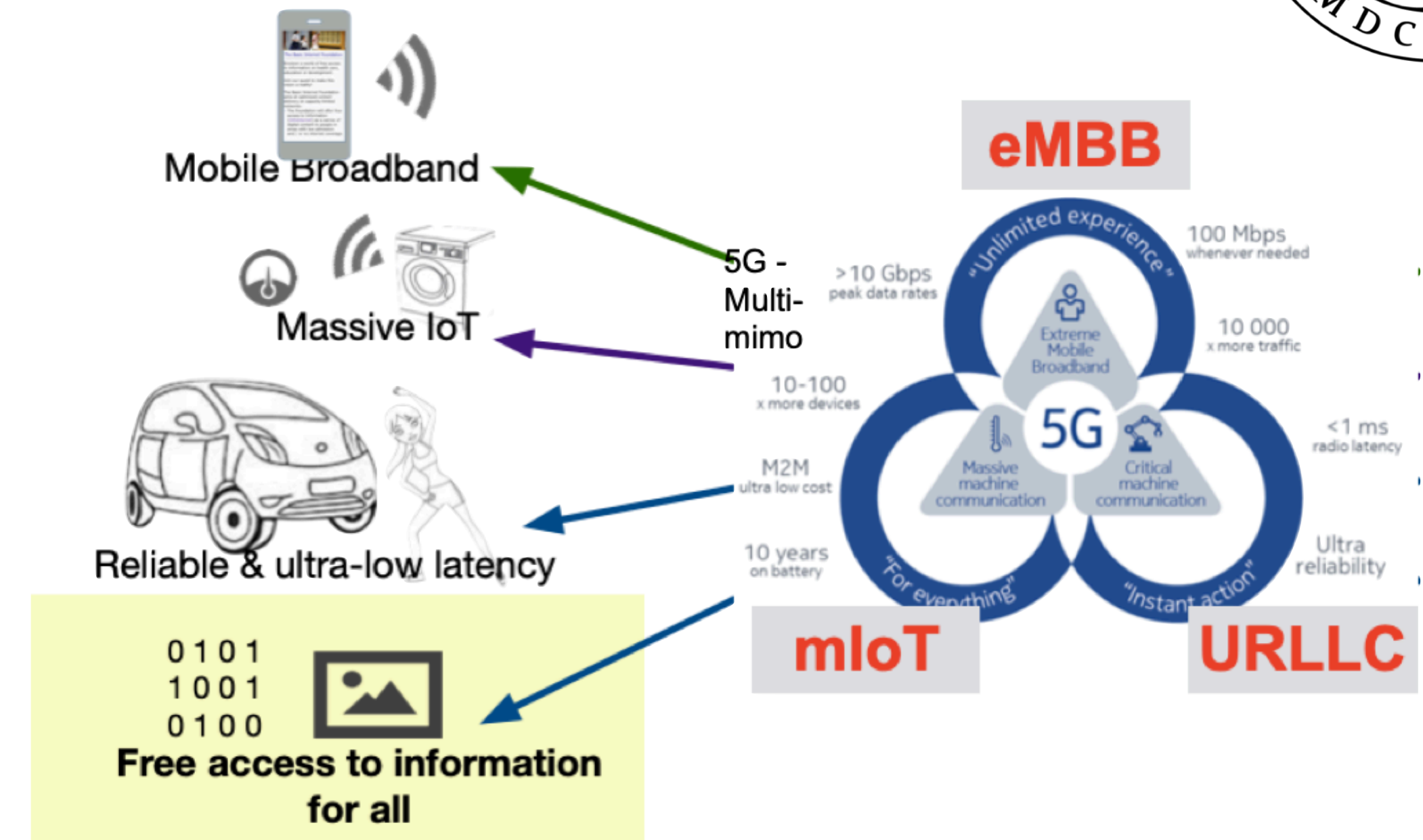
→ Data lake: store unstructured data and run analytics on it



IoT private 5G integration

- Extends to private 5G network
- *Who needs a private network?*

<https://aws.amazon.com/private5g/>



Take away from L14 Cloud & Cloud Security

- ➔ Delivery models
 - Infrastructure (IaaS), Platform (PaaS), Software (SaaS) as a Service

- ➔ Responsibility of Cloud provider, and of Customer

- ➔ Cyber vs Cloud Security
 - Threats, reasons, main defence

