BOSCH

High Velocity Engineering

Apurva Ohm

Technical Architect

BOSCH

Four Business Sectors

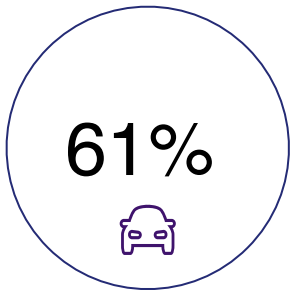
Key Figures 2017*

Bosch Group

€ 78.0 billion euros in sales

400,500 associates

Mobility Solutions	One of the world's largest suppliers of mobility solutions
Industrial Technology	Leading in drive and control technology, packaging, and process technology
Energy and Building Technology	One of the leading manufacturers of security and communication technology Leading manufacturer of energy-efficient heating products and hot-water solutions
Consumer Goods	Leading supplier of power tools and accessories Leading supplier of household appliances



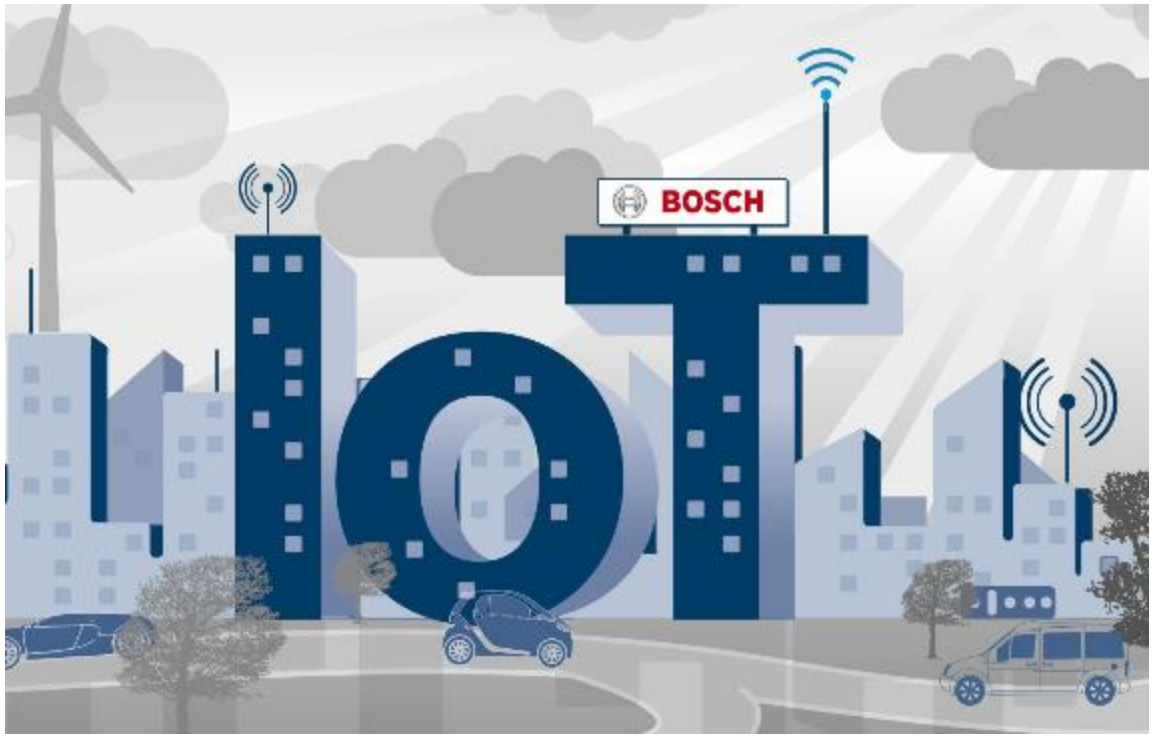
Share of sales

* Preliminary, rounded figures as of 12.17

RBNA/HRC1.32 I 2018-03-29

BOSCH

IoT@Bosch - Transformation into an IoT Company



Bosch plans to...

...make all its electronic products web-enabled by 2022

...offer new, connected services with its web-enabled products

...in this way expand its product and services business with connected solutions, and generate additional sales as a result

What is Bluehound?

Vision: Be the central hub that construction assets flow through

BLUEHOUND

User Driven Customization

Cost Accounting

Certification Tracking

Asset information storage

Delivery Tracking

Hierarchy Asset Assignment

BOSCH

How it works?

1 Purchase a plan that suits your project needs.

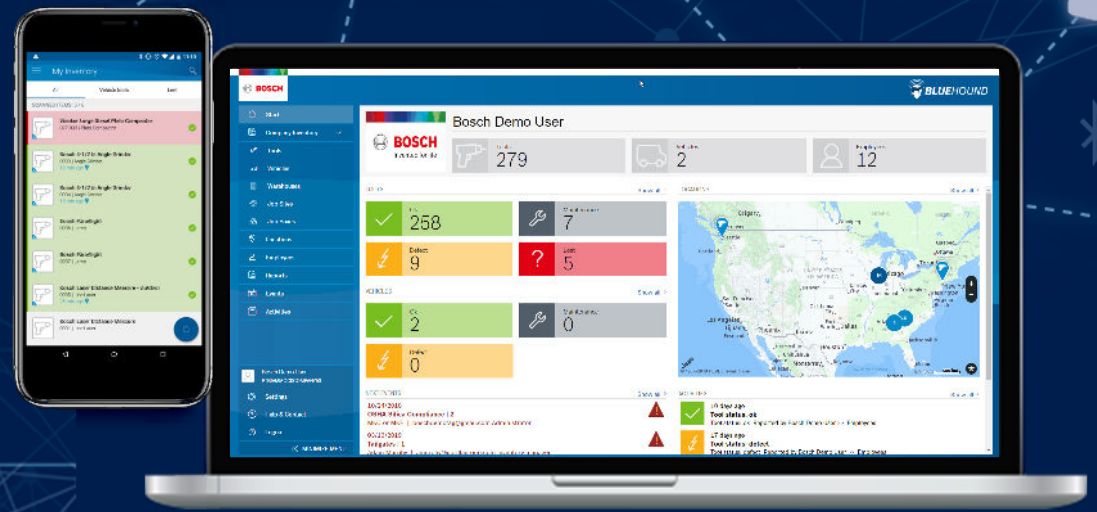
2 Attach the tag to your tool or equipment.

3 Assign your beacons on the web portal and start tracking.

LET BLUEHOUND DO THE WORK FOR YOU

BLUEHOUND

- Delivery tracking from warehouse to jobsite with notifications when product arrives.
- End of day site walk to check inventory in job box.
- Easily trace any asset via serial number, inventory number, model number, warranty information, etc.
- Maintenance alerts and updates to keep track of safety equipment and scheduled asset maintenance.
- Asset assignment to jobsite, job box, warehouse and individual for complete transparency to where a tool is assigned.
- Employee certification storage.
- Document storage linked to an asset.



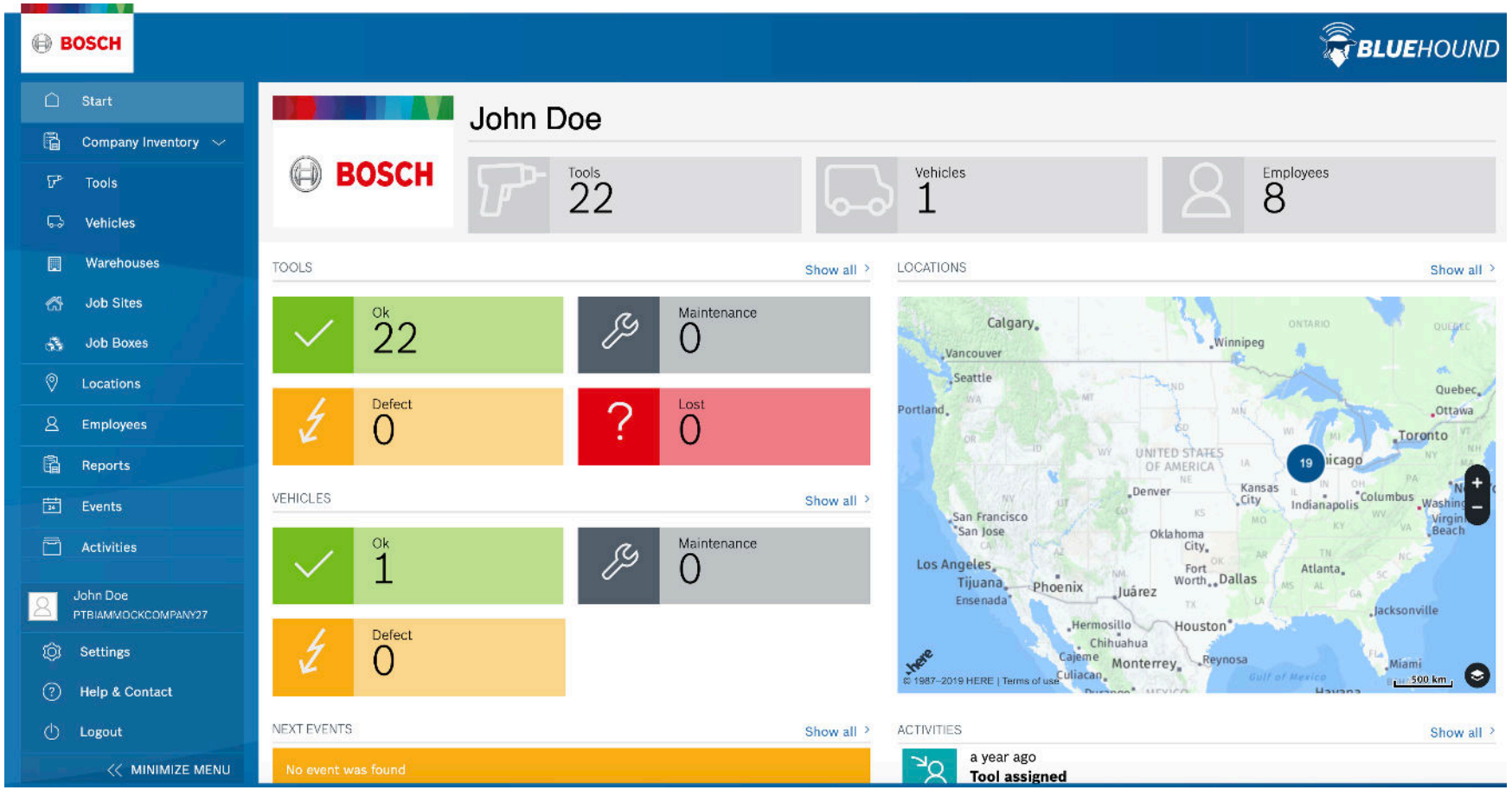
Professional
BOSCH

ANDROID APP ON Google play

Available on the App Store

BOSCH

Bluehound Dashbord



BOSCH

Demo!

Technical Overview

Bluehound Backend Is Composed Of Containerized Microservices Orchestrated By Kubernetes

What is Kubernetes?

- *Kubernetes manages container-based applications and their associated networking and storage components.*

- *Benefits of using Kubernetes as the orchestrator*
  - *Declarative approach to deployments*
  - *Backed by a robust set of APIs for management operations*
  - *Ensures Scalability, Availability and Reliability*
  - *Polyglot , Microservices - based architecture*

Why we chose Kubernetes ?

Scalability

Fueled by customer usage and demand

Avoid down time

Canary deployments

Reduce cost

Resource request and limit on deployments

Infrastructure abstraction

Shift focus from underlying infrastructure to application workloads

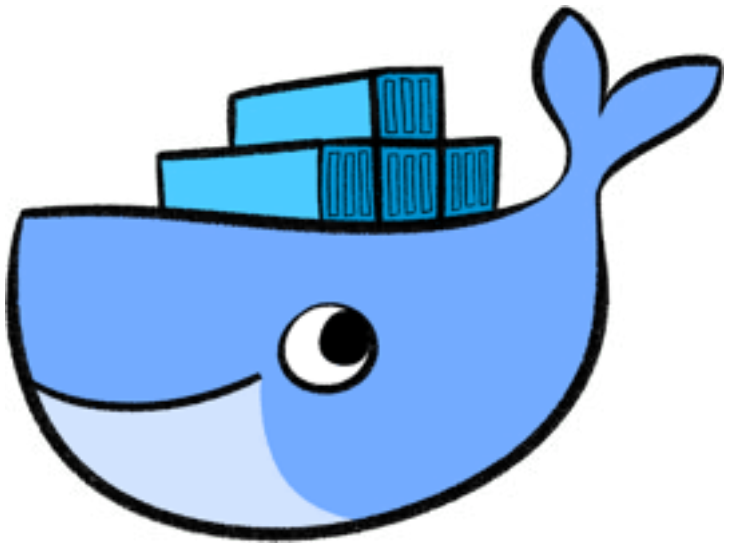
Greater Developer velocity !

Quick, easy and automatic deployments

BOSCH

Drivers of High Velocity Engineering

Containerization



BOSCH

Drivers of High Velocity Engineering

- *Docker images are first class citizens.*
- *Docker Native Workflows.*
- *Once we have a validated image we do not have to care about dependencies associated with our application, the underlying OS, or the underlying infrastructure.*

BOSCH

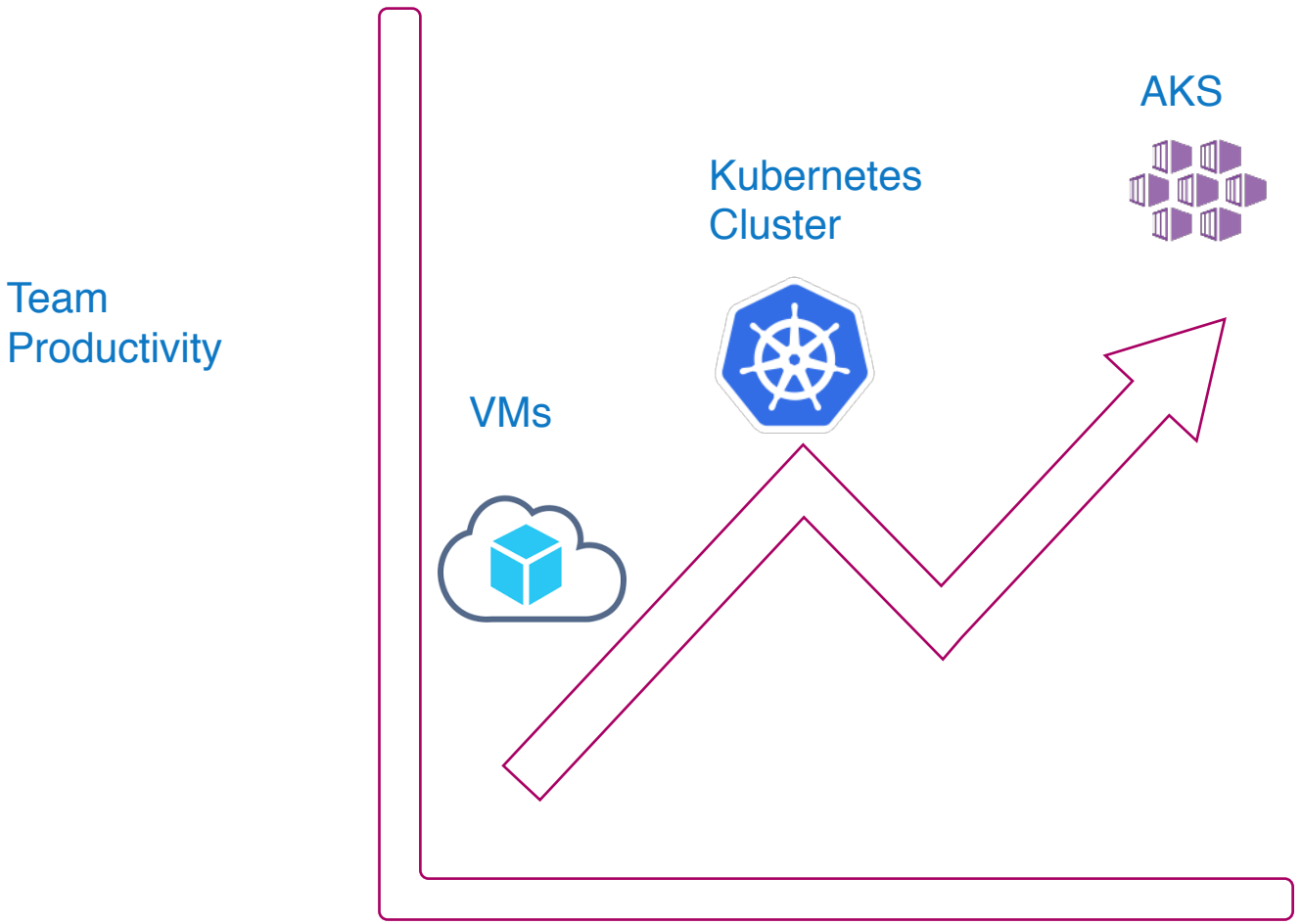
Drivers of High Velocity Engineering

- *If it ran in development, it will run in production.*
  Immutable images
- *Closely couple with code repository.*
  Tag images with commit sha
- *Reproducing bugs is a lot easier.*
  Debug prod image in dev
- *Easy rollbacks.*
  Rollback previous image from private registry (ACR)

Drivers of High Velocity Engineering

Managed Kubernetes Cluster - AKS

Drivers of High Velocity Engineering



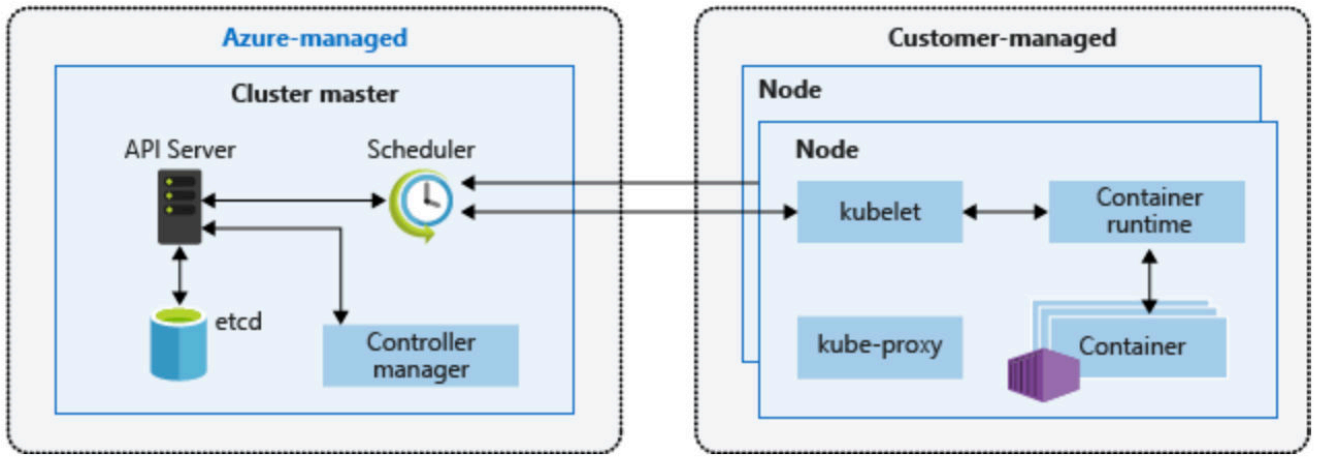
- *AKS does a lot of heavy lifting.*
  - *Reduces complexity for cluster deployment.*
  - *Core management tasks (cluster upgrades, k8 Control plane, Cluster security, Network plugins)*

- *Azure is building easy AKS integrations with other Azure resources.*

BOSCH

Drivers of High Velocity Engineering

1. Azure managed cluster master nodes



- *Azure managed, cluster master nodes, provide core kubernetes services and orchestration of application workloads.*

BOSCH

Drivers of High Velocity Engineering

2. Node security in AKS

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: security-context-demo
spec:
  containers:
    - name: security-context-demo
      image: nginx:1.15.5
    securityContext:
      runAsUser: 1000
      fsGroup: 2000
      allowPrivilegeEscalation: false
      capabilities:
        add: ["NET_ADMIN", "SYS_TIME"]
```

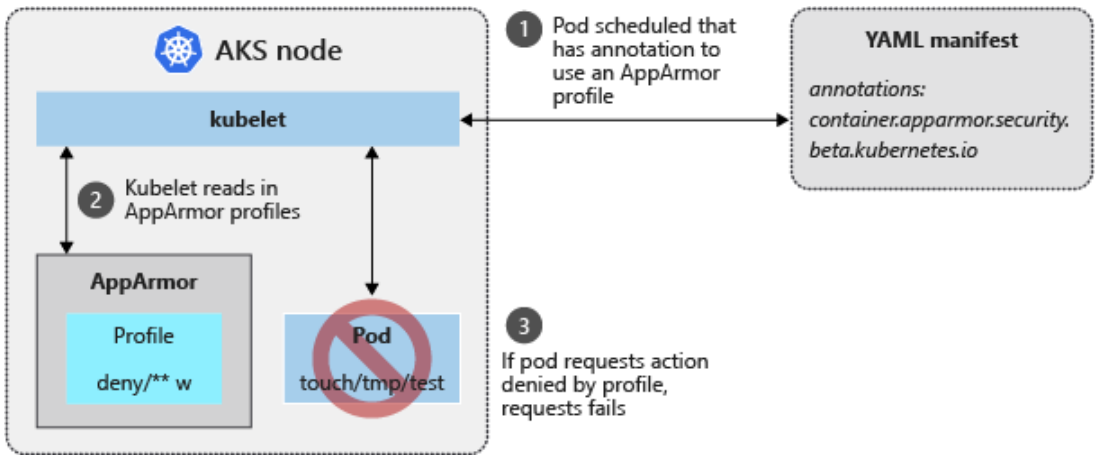
- *Pod security contexts are built in to Kubernetes and lets you define additional permissions.*
  - *Define the user or group to run as.*
  - *Avoid use of root privileged escalation (Set allowPrivilegeEscalation: false in the pod manifest to).*
  - *Define what Linux capabilities to expose. Containers should be limited to only the actions and processes that they need.*

- *For more granular control of container actions, you can also use built-in Linux security features such as AppArmor and seccomp.*

BOSCH

Drivers of High Velocity Engineering

2. Node security in AKS



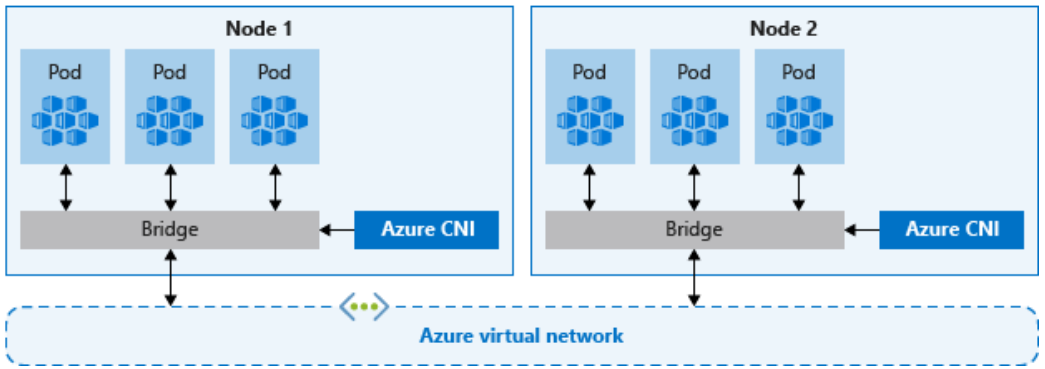
- *AppArmor*
  - *Linux kernel security module (works for any Linux application)*
  - *Available as part of underlying AKS node OS, and is enabled by default (restrict access to / proc /sys locations)*
  - *You can create additional AppArmor profiles that restrict actions such as read, write, or execute, or system functions such as mounting filesystems*
  - *This features are defined at the node level, and then implemented through a pod manifest annotation: container.apparmor.security.beta.kubernetes.io*

- *Seccomp*
  - *Linux kernel security module (works at process level)*
  - *Supported by docker runtime used by AKS nodes (works at the process level)*
  - *You can create additional seccomp filters that, for example, prevents changing permissions on a file.*
  - *This features are defined at the node level, and then implemented through a pod manifest annotation: seccomp.security.alpha.kubernetes.io*

BOSCH

Drivers of High Velocity Engineering

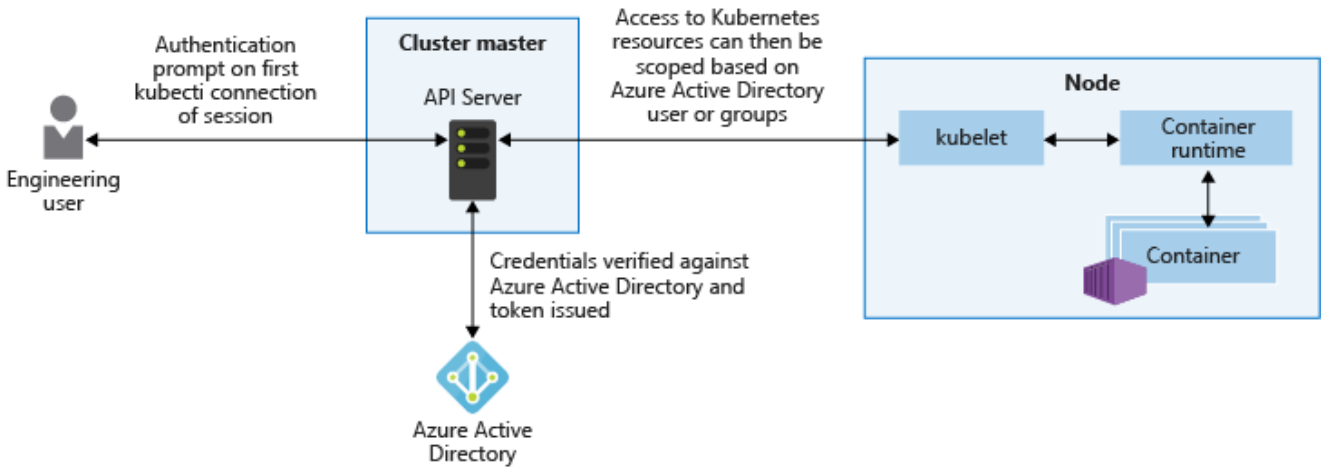
3. Networking in AKS



- *Azure Container Networking Interface (CNI)*
  - *Every pod gets a unique IP address from the subnet and can be accessed directly.*
  - *Default network model is Kubenet, where only the nodes receive a routable IP address, and the pods use NAT to communicate with other resources outside the AKS cluster. NAT can become a bottleneck as number of pods on a Node grows.*

Drivers of High Velocity Engineering

4. Azure Active Directory Integration enables enhanced AKS cluster security

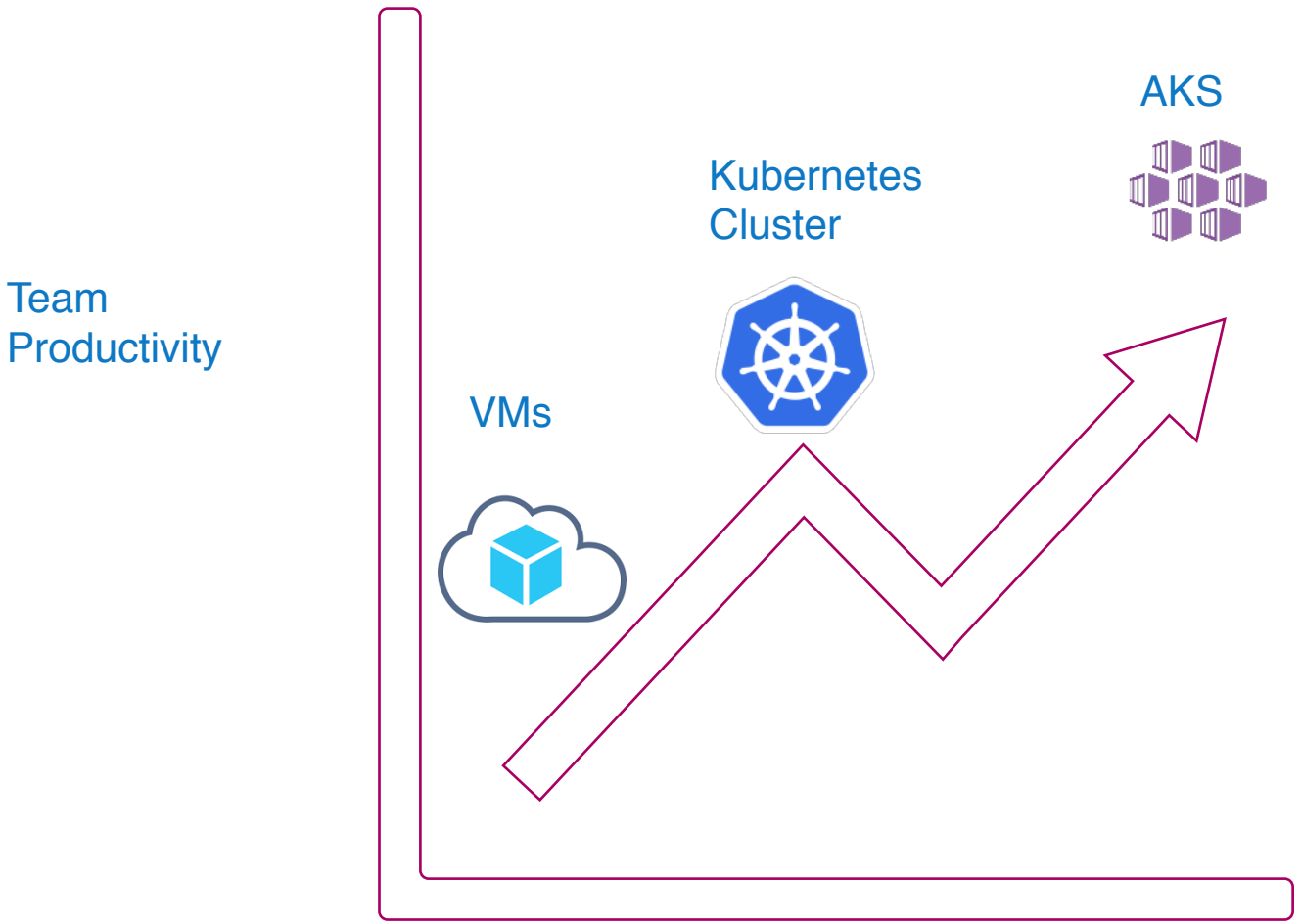


- *Secure access to API server (AD RBAC)*
  - *Kubernetes doesn't provide an identity management solution: hard to provide a granular way to restrict access to the API server.*
  - *Use existing AD users, groups to authenticate users.*

- *Kubernetes RBAC*
  - *Enforce Role Based Access Control (RBAC) using Roles and RoleBindings within cluster.*

BOSCH

Drivers of High Velocity Engineering



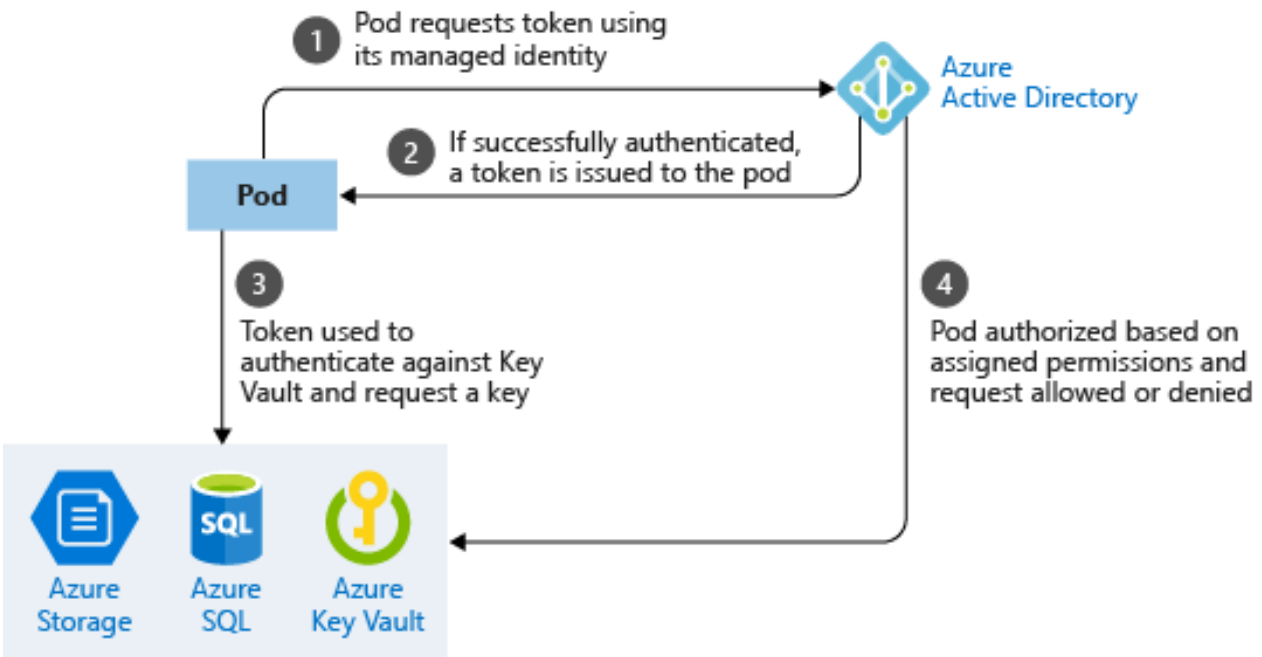
- *AKS does a lot of heavy lifting.*
  - *Reduces complexity for cluster deployment.*
  - *Core management tasks (cluster upgrades, k8 Control plane, Cluster security, Network plugins)*

- *Azure is building easy AKS integrations with other Azure resources.*

BOSCH

Drivers of High Velocity Engineering

4. Azure Active Directory Integration enables enhanced AKS cluster security

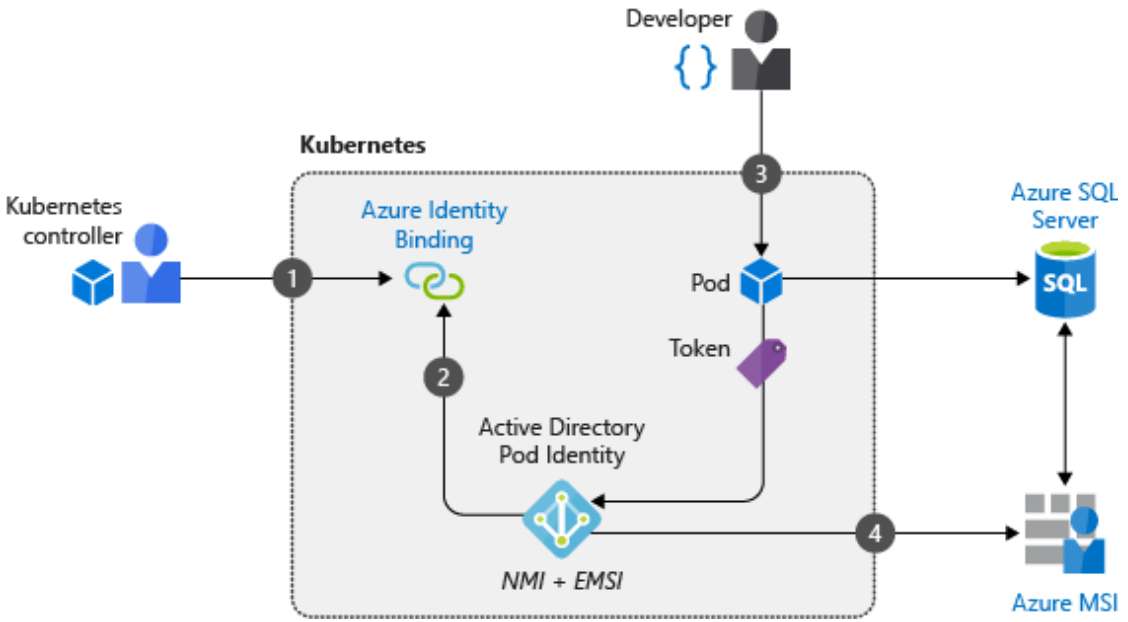


- *Managed identities for Azure resources let you automatically request access to services through Azure AD.*
  - *You don't define credentials for pods (container image, secrets), instead they request an access token in real time, and can use it to access only their assigned Azure services.*

BOSCH

Drivers of High Velocity Engineering

4. Azure Active Directory Integration enables enhanced AKS cluster security



- *AKS needs two components to use pod managed identity :*
  1. *Node Identity management (NMI) server*
  2. *Managed Identity Controller (MIC)*
  - *NMI server (DaemonSet) listens for pod requests to Azure services, queries the MIC -> The MIC checks for Azure identity mappings in the AKS cluster -> The NMI server then requests an access token from Azure Active Directory (AD) based on the pod's identity mapping.*
- *Limit Credential Exposure (of non azure resources) by using Pod Managed Identity, and Azure Key Vault FlexVol driver.*

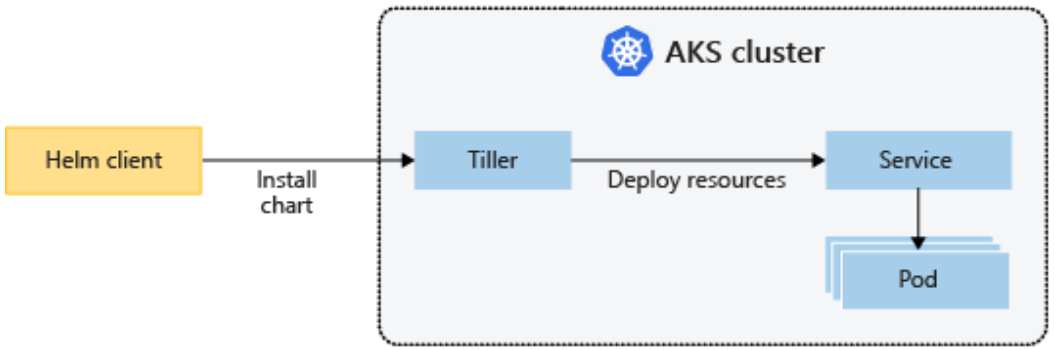
BOSCH

Drivers of High Velocity Engineering

Helm Charts

BOSCH

Drivers of High Velocity Engineering



- *Package Management with Helm.*
  - *Tiller and Helm client.*
  - *ACR configured to be Helm repository.*

BOSCH

Drivers of High Velocity Engineering

- *Applications can be tested in an ephemeral (short-lived) environment quickly.*
  You could define your own application stack with all its dependencies, configurations in a helm chart and deploy.

- *Deploy Infrastructure Services.*
  You can build and use existing public Helm charts that contain a packaged version of application code and Kubernetes YAML manifests to deploy resources.

- *Easy rollbacks.*
  You can rollback your services with all the configuration information if something goes wrong.

- *Production releases are smoother.*

- *Onboarding new engineers is quicker.*

Drivers of High Velocity Engineering

CI/CD with Codefresh

BOSCH

Drivers of High Velocity Engineering

Kubernetes

Container Native Services

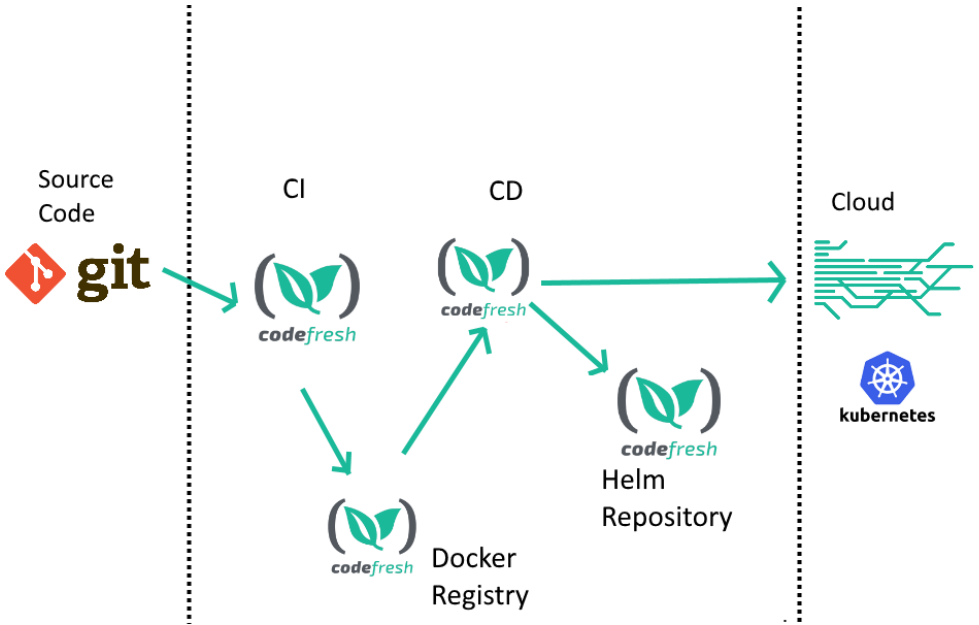
Helm Charts

CI/CD with Codefresh

BOSCH

Drivers of High Velocity Engineering

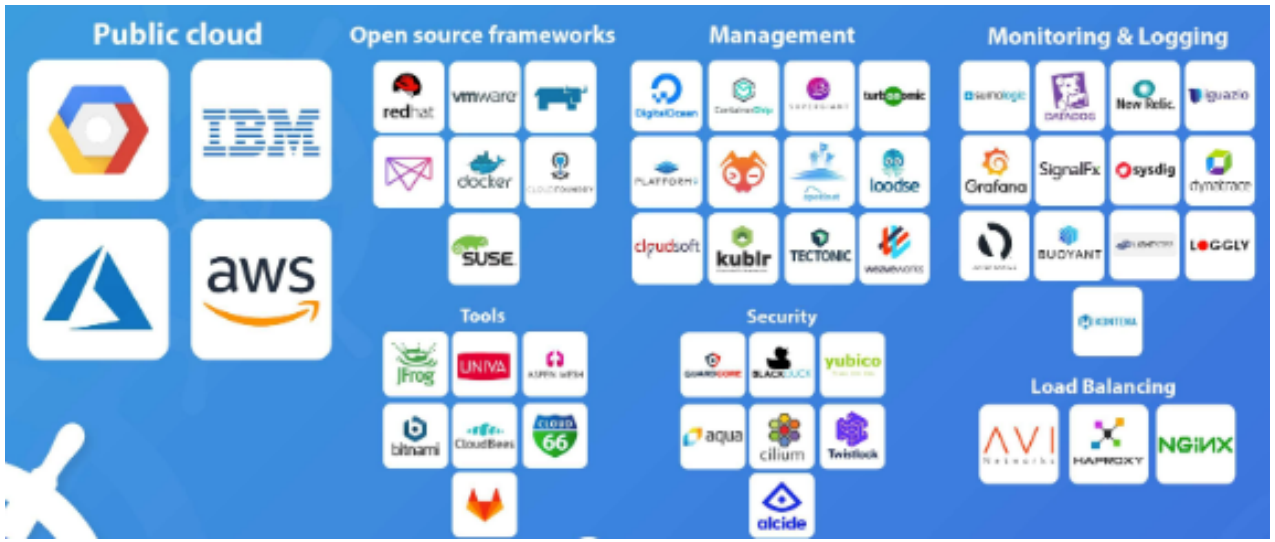
CI/CD Workflow



BOSCH

Drivers of High Velocity Engineering

The Kubernetes Ecosystem



Drivers of High Velocity Engineering

Growing number of Tools and Services in the Kubernetes ecosystem

BOSCH

Drivers of High Velocity Engineering

Thank you!

BOSCH