Pets, Cattle and Now Insects

Applying Security Practices To Containers & Functions

SHANE BALDACCHINO | CHIEF ARCHITECT MICROSOFT AUSTRALIA

whoami

seek

aws

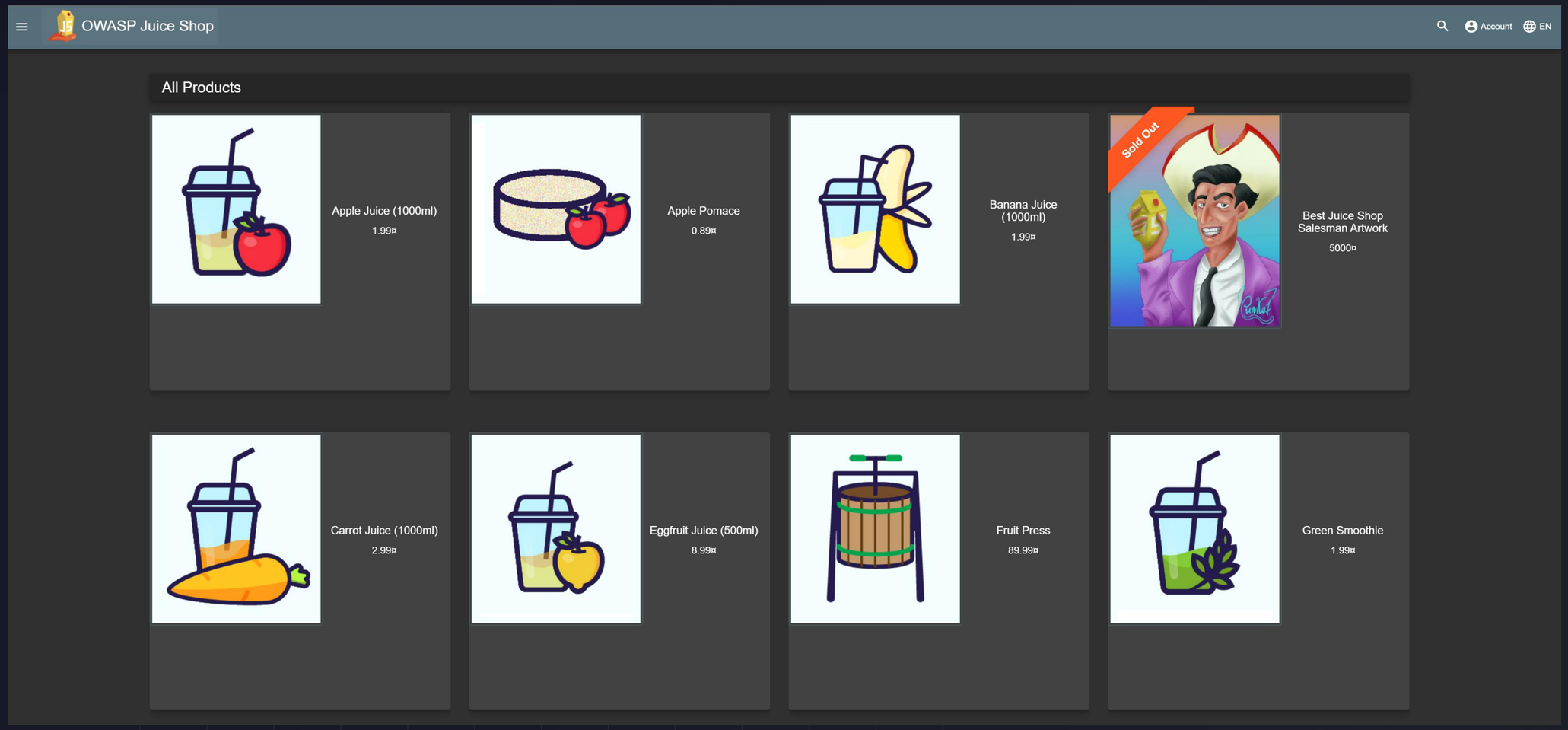
Microsoft

Attacks, They Be Changing

OWASP Style Attacks

Critical Web Application Security Risks

OWASP Juice Shop



Recent Attacks

CodeCov

Breach

Vulnerable developer secrets
Vulnerable supply chain

Electronic Arts

Breach

Vulnerable Applications
Vulnerable ID Verification

:(

Your device ran into a problem and needs to restart. We're just collecting some error info, and then you can restart.

100% complete

For more information about this issue and possible fixes, visit https://www.windows.com/stopcode

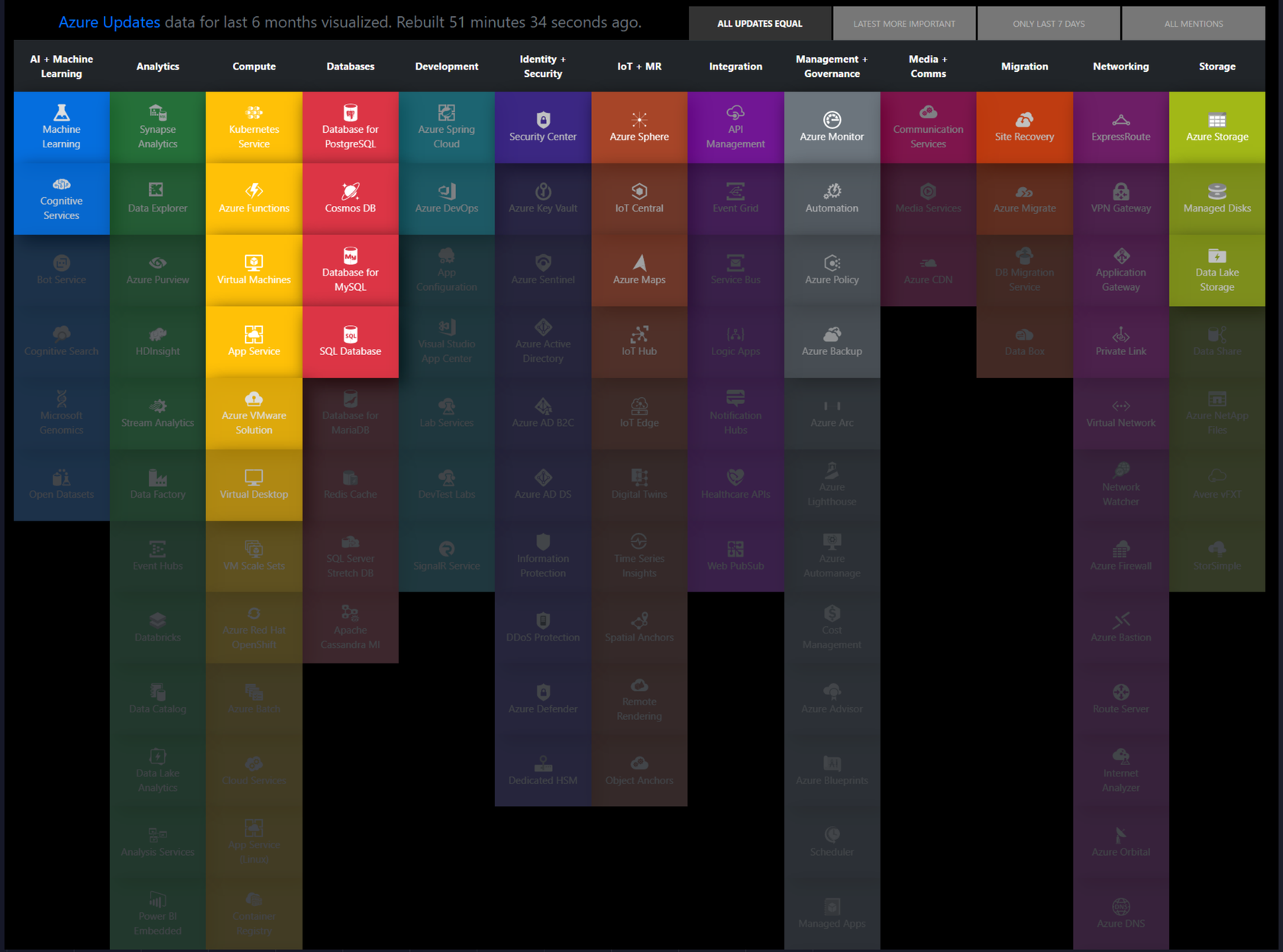
If you call a support person, give them this info:

Stop code: SESSION1_INITIALIZATION_FAILED

Traditional Controls Don’t Work
The Game Has Changed

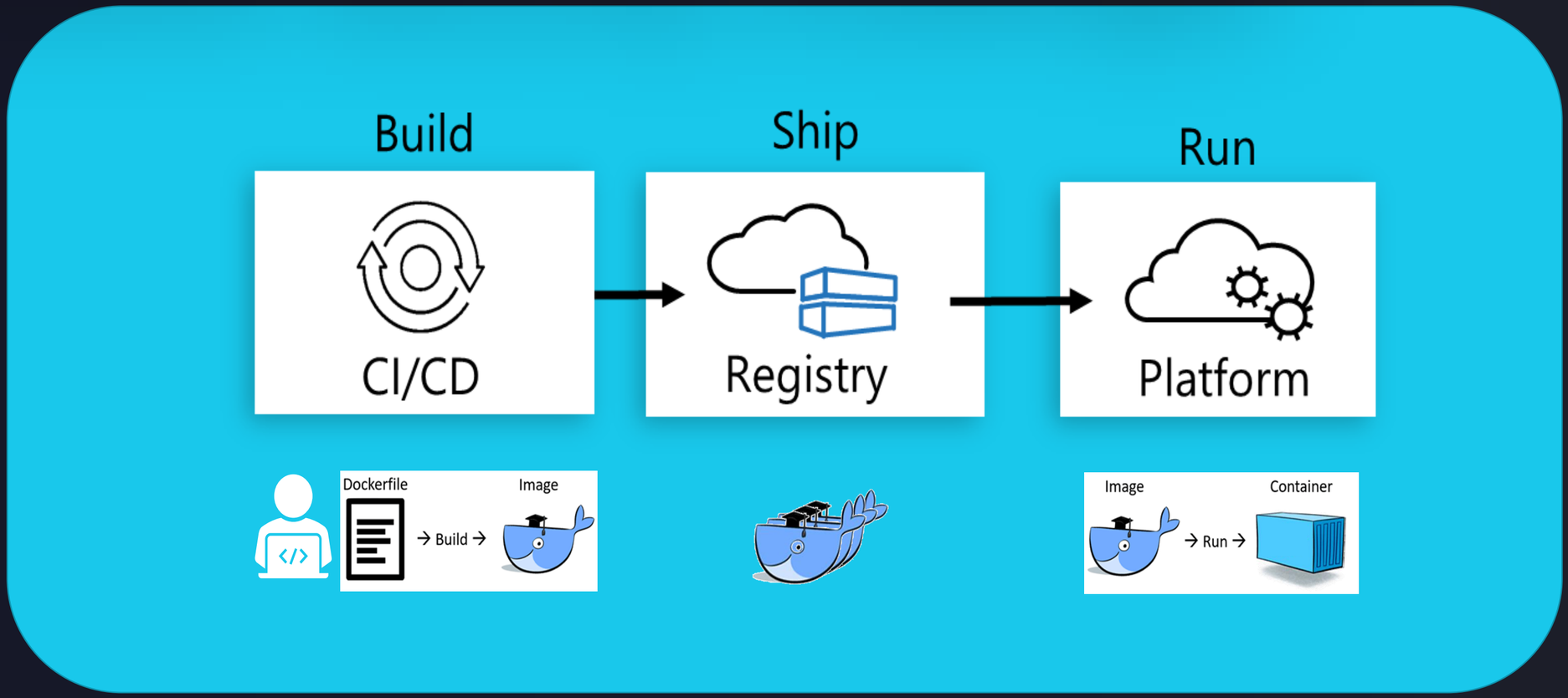
Protecting Cloud Native Compute

Azure Heat Map



Protecting Cloud Native Compute

Container Security Challenges



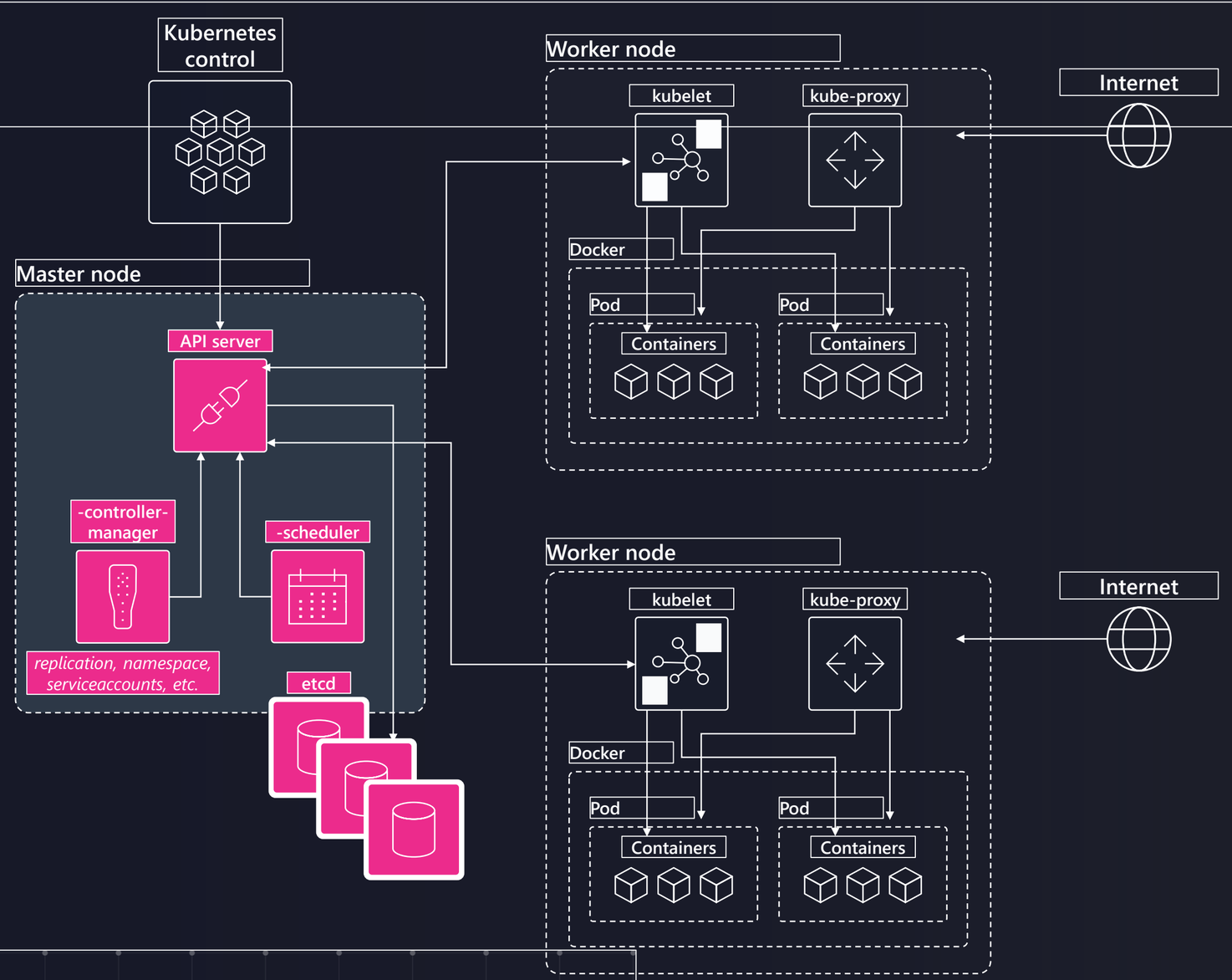
Resulting in demand for “agentless" offerings with extra focus on shift-left

Container Market Maturity Is Adolescent

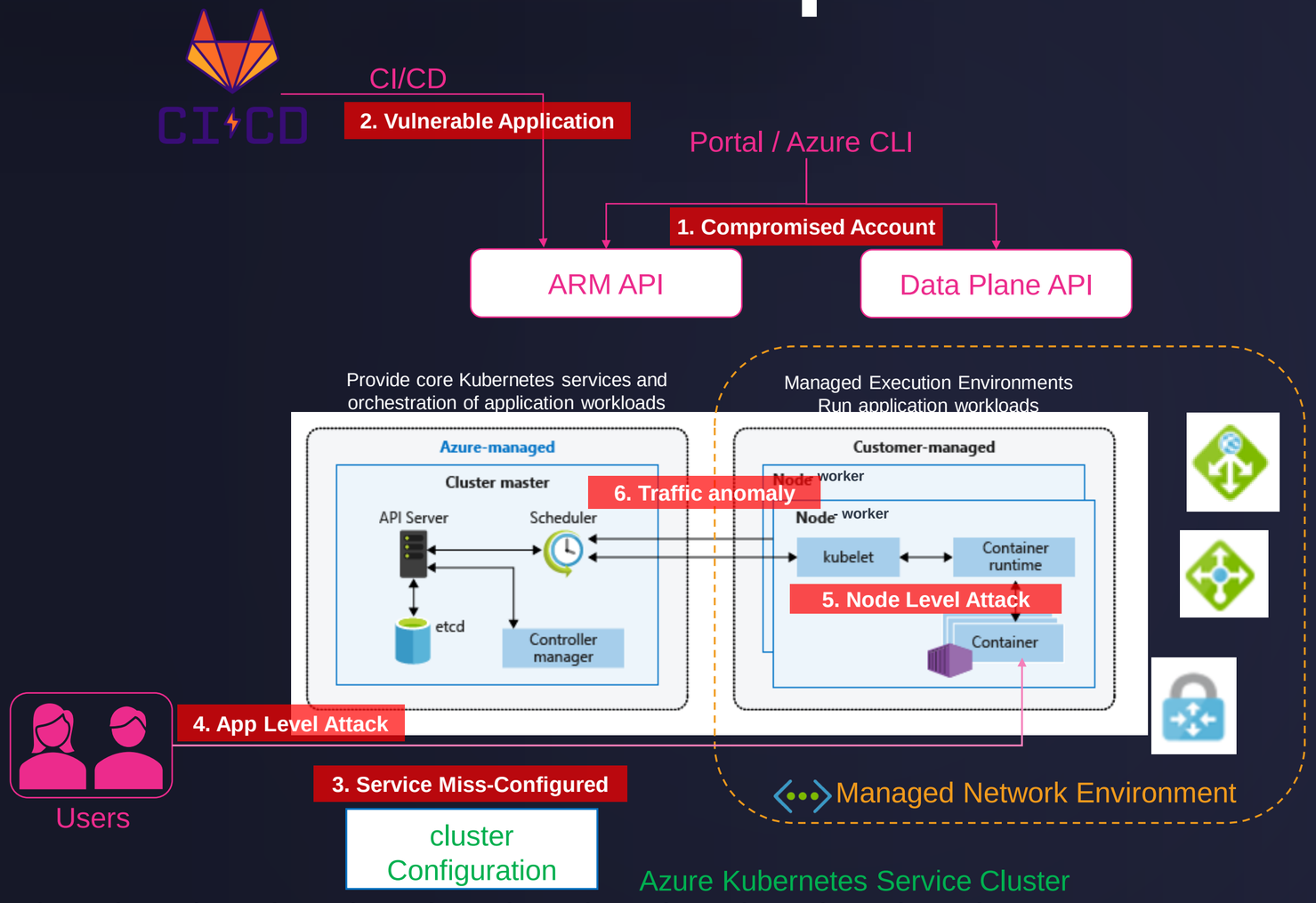
Company	Founded	Acquired by	Acq. time
Aqua Security	2015	-	-
Twistlock	2015	Palo Alto	2019 (July)
Octarine	2017	VMware	2020 (May)
PortShift	2018	Cisco	2020 (Oct)
StackRox	2014	IBM security	2021 (Jan)
Alcide IO	2016	Rapid7	2021 (Feb)

The market is consolidating (in technology and vendors)

K8 101


Kubernetes control
Master node
API server
-controller-manager
-scheduler
replication, namespace, serviceaccounts, etc.
etcd
Worker node
kubelet
kube-proxy
Docker
Pod
Containers
Pod
Containers
Internet
Worker node
kubelet
kube-proxy
Docker
Pod
Containers
Pod
Containers
Internet

K8 Threat Landscape



Microsoft ♡'s OpenSource

K8 – Att&ck matrix

https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/

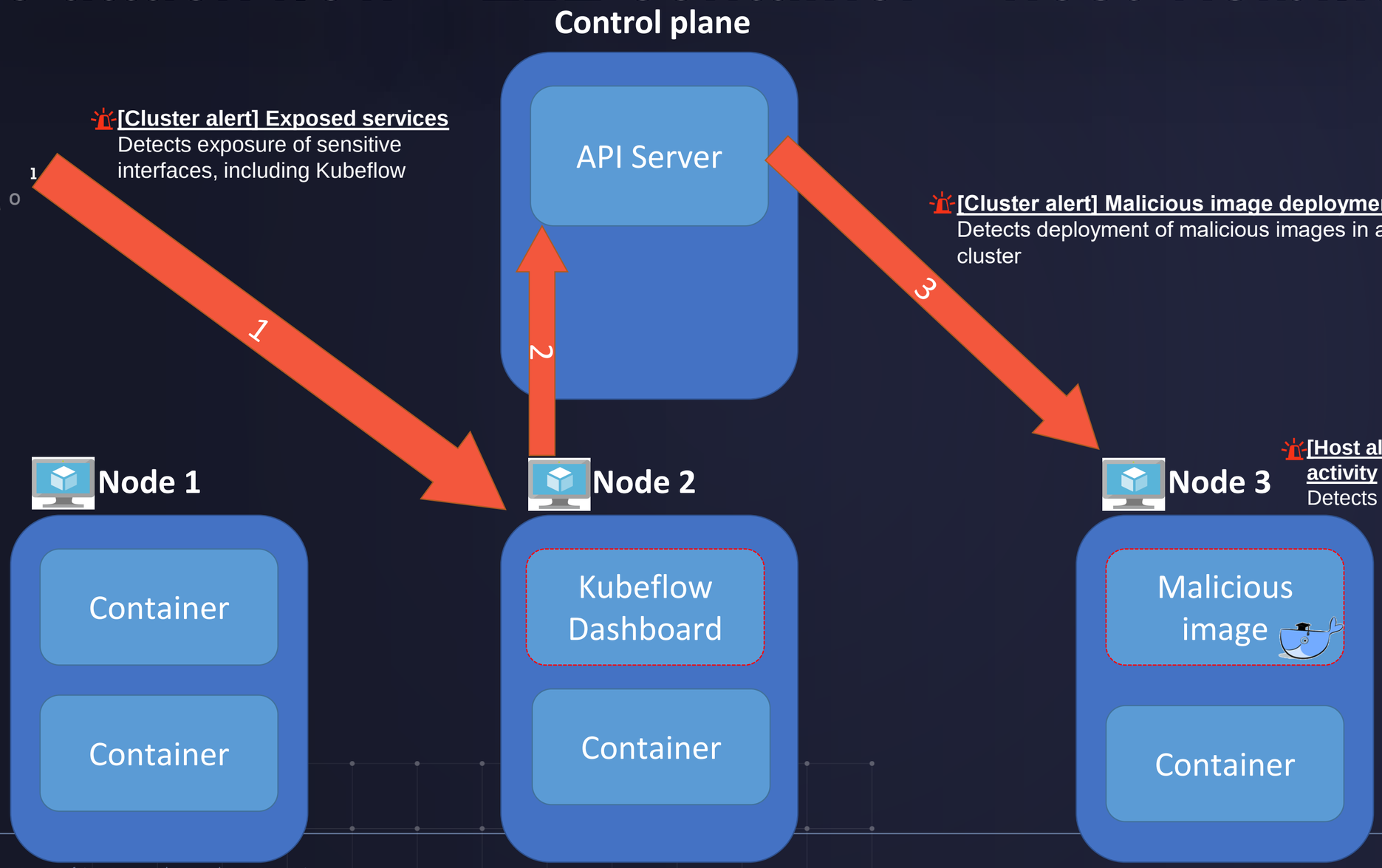
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral Movement	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Data destruction
Compromised images in registry	Bash / cmd inside container	Writable hostPath mount	Cluster-admin biding	Delete K8S events	Mount service principle	Access Kubelet API	Container service account	Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal network	Denial of service
Application vulnerability	Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files	
Exposed dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access Kubernetes dashboard	
							Access tiller endpoint	

The attack flow – E2E container + host visibility

[Cluster alert] Exposed services
Detects exposure of sensitive interfaces, including Kubeflow

[Cluster alert] Malicious image deployment
Detects deployment of malicious images in a cluster

[Host alert] Digital currently mining activity
Detects activity of digital currently mining



K8 – Att&ck matrix

https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral Movement	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Data destruction
Compromised images in registry	Bash / cmd inside container	Writable hostPath mount	Cluster-admin biding	Delete K8S events	Mount service principle	Access Kubelet API	Container service account	Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal network	Denial of service
Application vulnerability	Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files	
Exposed dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access Kubernetes dashboard	
							Access tiller endpoint	

Container Security Domains

Security Domain	Development Lifecycle			Customer Adoption / Maturity
	Build	Ship	Run	
Vulnerability Management	V	V	V	 Crawl
Hardening Hosts, Cluster hygiene	V	V	V	 Walk
Kubernetes Policy & Enforcement	V	V	V	 Walk
Runtime Protection			V	 Walk
Network & identity- Service Mesh			V	 Run
Compliance	V	V	V	 Crawl

Image Scanning

Security Domain	Development Lifecycle Build	Ship	Run	Customer Adoption / Maturity
Vulnerability Management	V	V	V	Crawl
Hardening Hosts, Cluster hygiene	V	V	V	Walk
Kubernetes Policy & Enforcement	V	V	V	Walk
Runtime Protection			V	Walk
Network & identity- Service Mesh			V	Run
Compliance	V	V	V	Crawl

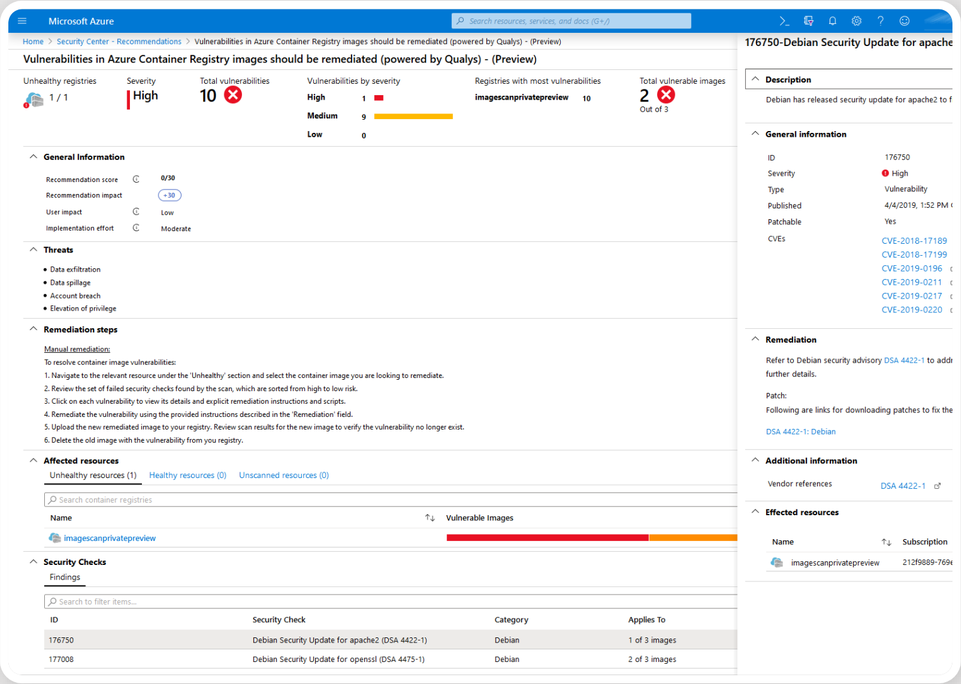
Seamless deployment and configuration

Image scan in ship

Discover ACR registries, scan all pushed images, and get visibility to vulnerable images

Image scan in runtime

Continuous scanning of recently pulled images



K8 – Protection

Security Domain	Development Lifecycle			Customer Adoption / Maturity
	Build	Ship	Run	
Vulnerability Management	V	V	V	Crawl
Hardening Hosts, Cluster hygiene	V	V	V	Walk
Kubernetes Policy & Enforcement	V	V	V	Walk
Runtime Protection			V	Walk
Network & identity- Service Mesh			V	Run
Compliance	V	V	V	Crawl

AKS cluster and nodes hygiene

Harden and audit clusters according to security benchmarks and follow the Docker CIS benchmark on container nodes

Runtime threat detection

Detect suspicious behavior in Kubernetes workloads via a unique agentless approach leveraging Kubernetes audit log, in addition to Kubernetes workers dedicated detections

Admission control policy management

Mandate/audit security best practices on Kubernetes workloads

Admission control policies

Security best practices for Kubernetes workloads

Security Domain	Development Lifecycle			Customer Adoption / Maturity
	Build	Ship	Run	
Vulnerability Management	V	V	V	Crawl
Hardening Hosts, Cluster hygiene	V	V	V	Walk
Kubernetes Policy & Enforcement	V	V	V	Walk
Runtime Protection			V	Walk
Network & identity- Service Mesh			V	Run
Compliance	V	V	V	Crawl

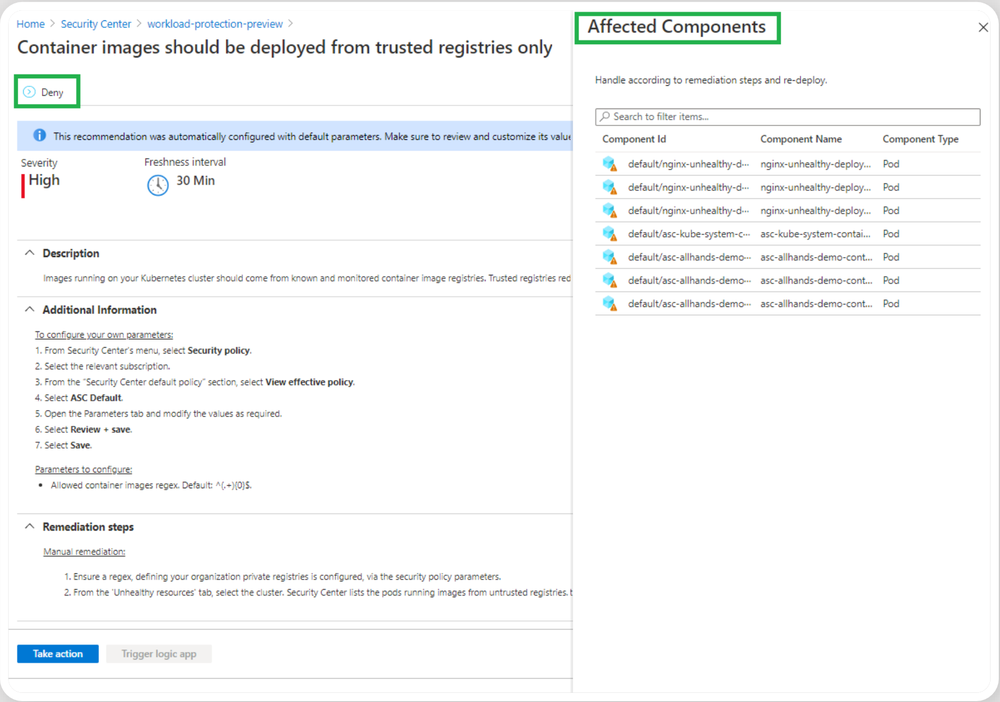
Kubernetes level hardening recommendations
A set of best practices for protecting Kubernetes workloads spawning across the security controls

Shifting left with the open–source Gatekeeper v3 admission controller

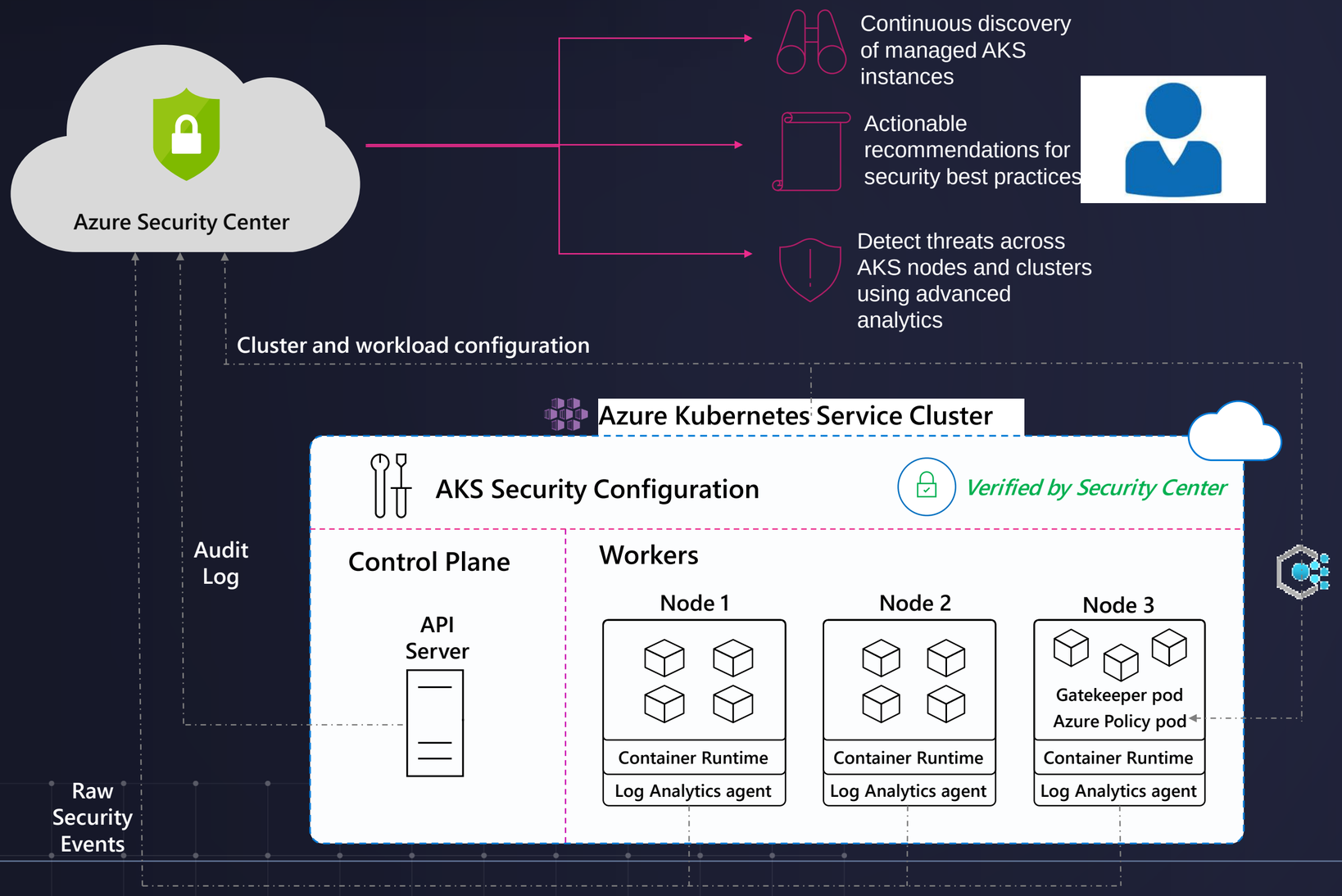
Every request to the Kubernetes API server is monitored **before being persisted to the cluster**

A **list of unhealthy workloads** running in the clusters

Deny option to mandate recommendations, ensuring workloads are **secure by default**



Behind The Scenes -



Know Your Roadmap

Search or jump to... / Pull requests Issues Marketplace Explore

Azure / AKS Public

Watch 329 Star 1.3k Fork 142

Code Issues 307 Pull requests 1 Discussions Actions Projects 2 Security Insights

Azure Kubernetes Service Roadmap (Public)

Updated 11 hours ago

Filter cards Fullscreen Menu

14 Backlog

- Enable AKS Control Plane Logging during AKS cluster provisioning
  #1443 opened by jayush
  client/AzCLI feature-request
- Region: South Africa West
  #1700 opened by jluk
  action-required feature-request regions
- Least Privilege Node Access
  #2180 opened by miwithro
  Needs Information security
- Provide more flexible resource reservations for User Node Pools
  #1339 opened by ondrejhlavacek
  feature-request nodepools/mode nodepools
- Allow effortless migration from Basic LB to Standard
  #1687 opened by rlevchenko
  feature-request networking/load-balancers
- [Feature] OSM addon support for Windows
  #2095 opened by keikhara
  stale windows
- [Feature] Support Windows Hyper-V isolation
  #1792 opened by keikhara
  feature-request windows
- [Feature] Azure Security Center support on Windows AKS
  #1909 opened by keikhara
  feature-request windows
- Configurable log levels for addons
  #2306 opened by pierluigilenoci

7 Planned (Committed)

- [Feature Request] Alpha Clusters
  #2058 opened by palma21
  action-required
- AKS allows creation of NodePools in different Subnets (Kubenet)
  #1500 opened by jluk
  feature-request networking/kubenet nodepools
- Update Default TLAs (Taints, Labels, Annotations)
  #1537 opened by armandgrillet
  feature-request
- Certificate Authorities are difficult to customize on nodes
  #2259 opened by jabbera
  feature-request
- [Feature Request] Built-in support for Kubernetes Event-driven Autoscaling (KEDA)
  #1479 opened by tomkerkhove
  feature-request
- [Feature Request] AKS API to enable retrieval of supported SKUs on AKS
  #1571 opened by jluk
  feature-request nodepools
- [Feature request] Ability to install InfiniBand drivers
  #1947 opened by denniszielke
  feature-request

34 In Progress (Development)

- Add Support for a KMS provider for Encrypting Secrets
  #845 opened by RehanSaeed
  feature-request security
- Trusted VM Support in AKS
  #2562 opened by miwithro
  feature-request security
- Azure Confidential VM Support in AKS
  #2563 opened by miwithro
  feature-request security
- Deploy AKS on Azure Dedicated Hosts
  #1916 opened by palma21
  action-required feature-request
- [Feature] Support WS2022 on Windows
  #2115 opened by keikhara
  feature-request windows
- [Feature] Privilege container support on Windows AKS
  #1975 opened by keikhara
  feature-request windows
- Azure Defender for Kubernetes Process Runtime Security
  #2526 opened by miwithro
  action-required Needs Attention security
- Azure Defender for Kubernetes Inventory
  #2527 opened by miwithro
  action-required Needs Attention security
- Continual scanning of Pods through Azure Defender Add-on

24 Public Preview (Shipped & Improving)

- Custom Policy support for AKS
  #2525 opened by miwithro
  feature-request security
- GPU Multi Instance Support
  #2539 opened by palma21
  feature-request GPU nodepools
- Kubernetes v1.22
  #2502 opened by PixelRobots
  feature-request
- FIPS-enabled Nodes
  #2379 opened by palma21
  feature-request
- AKS in VNET behind company HTTP proxy
  #205 opened by markwaldkat
  enhancement feature-request
- [Feature] Emit AKS event through Azure EventGrid
  #1812 opened by jluk
  azure/eventgrid feature-request Upgrade
- Cluster Scale-Down Mode
  #2061 opened by palma21
  feature-request
- [Feature] Support ContainerD on Windows AKS
  #1976 opened by keikhara
  containerd feature-request windows
- [Feature] User Password reset on Windows AKS
  #2261 opened by keikhara
  feature-request windows

4 Generally Available (Done)

- Azure Policy Support for Regex- allowing granular exclusions/inclusions in AKS specific policies.
  #2267 opened by miwithro
  action-required Needs Attention security
- Support of Ultra SSD
  #1712 opened by palma21
  enhancement feature-request storage
- Remove Local Accounts (clusters with no --admin)
  #2063 opened by palma21
  enhancement feature-request security
- [Availability Zone] Korea Central, Norway East, Central India, East Asia, Sweden Central
  #2576 opened by keikhara
  availability zones

8 Archive (GA older than 1 month)

- Enable CSI storage drivers in AKS
  #1757 opened by palma21
  feature-request storage
- Kubernetes v1.21
  #2175 opened by miwithro
  feature-request k8s-versions
- [New Region] - Sweden South & Central
  #2169 opened by keikhara
  action-required feature-request regions
- Container CI/CD static analysis through Azure Security Center
  #2269 opened by miwithro
  feature-request
- Kubelet User Assigned Managed Identity
  #1955 opened by palma21
  feature-request Managed Identity resolution/shipped
- AKS Run Command - Simplified kubectl access to private cluster
  #2059 opened by palma21
  enhancement feature-request Private-cluster resolution/shipped
- Simplified DNS for Private Cluster
  #2176 opened by miwithro
  feature-request networking
- [Feature] Private Cluster: Simplify BYO VNet and DNS setup by decoupling node -> control plane communication from private DNS zone.
  #1686 opened by TomGeske
  enhancement feature-request Private-cluster resolution/shipped

Run Your Code In Response To Events

Serverless

Shane ♡ Serverless

Serverless 101

Integrated programming model

Use built-in triggers and bindings to define when a function is invoked and to what data it connects

Enhanced development experience

Code, test and debug locally using your preferred editor or the easy-to-use web-based interface including monitoring

Hosting options flexibility

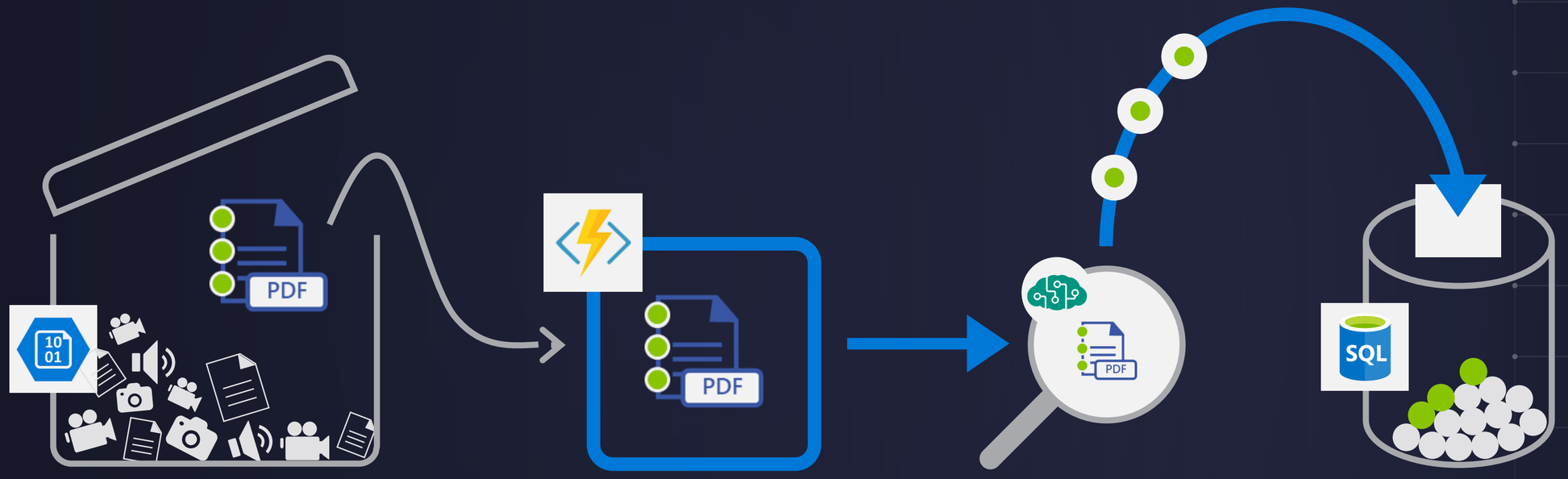
Choose the deployment model that better fits your business needs without compromising development experience

Making It Real

Scenario Example

Healthcare

Patient records are securely uploaded as PDF files. That data is then decomposed, processed using OCR detection, and added to a database for easy queries.



PDF file added to Blob Storage

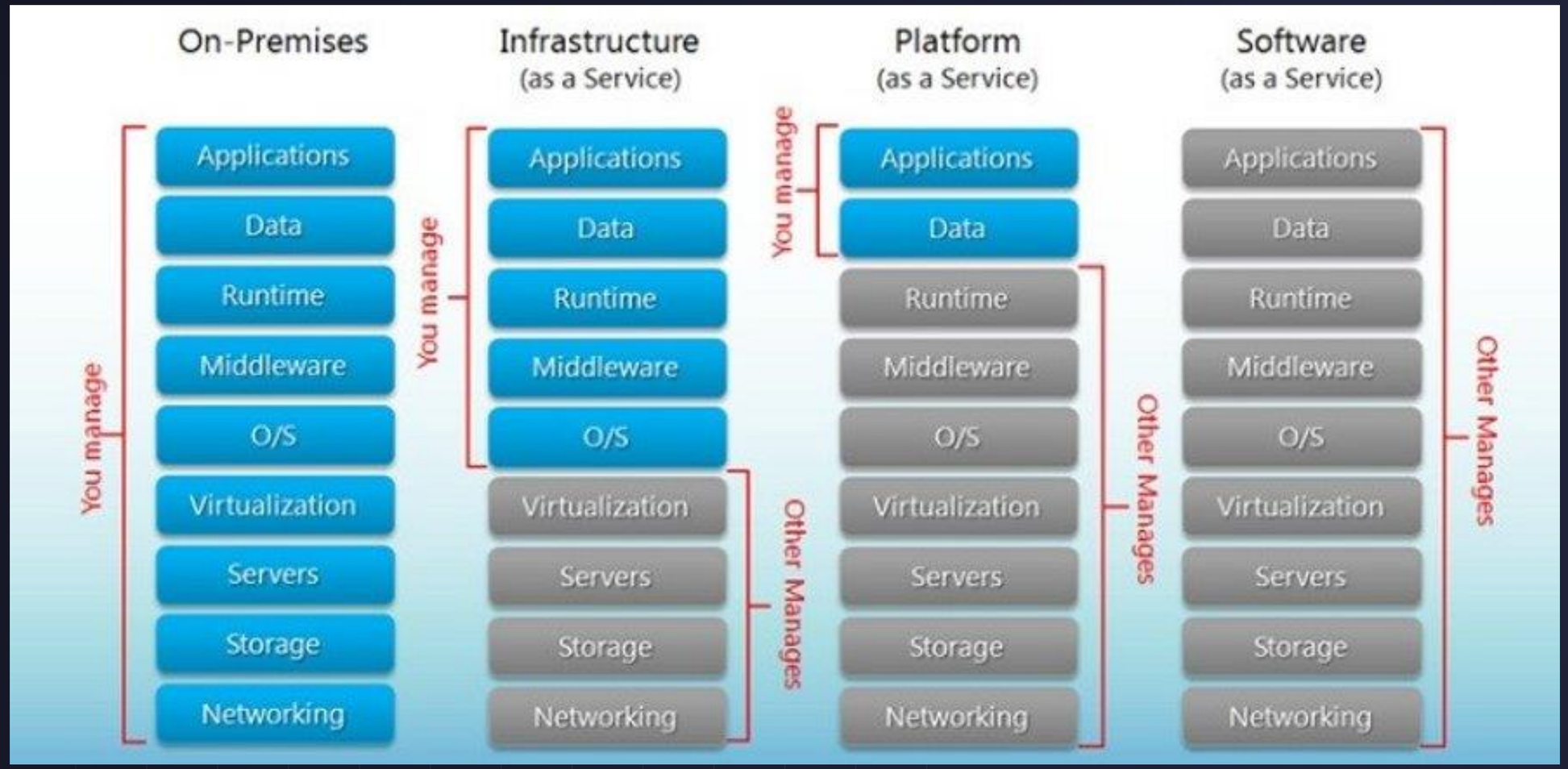
A function decomposes PDF file…

…and sends it to Cognitive Services for OCR detection

Structured data from file sent to SQL DB

Shared Responsibility Model

https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility



Securing Functions

Virtual Walls

Prevent lateral movements

Usage Quotas

Monitor resource hijacking

Secure Endpoints

Evaluate vNEt / VPC integration

RBAC

Remove Shared Secrets

DDoS Mechanisms

Split large function in to smaller units

Test Functions Defensively

Could you handle 100x load?

What About Fully Managed Containers?

But What Is Common
It’s Your Pipeline

It’s A Bugs Life

- Shift security left
- Unite DevOps and SecOps teams
- Accelerate secure innovation
- Improve threat remediation time

Lets Be Friends…..

SHANE BALDACCHINO | CHIEF ARCHITECT MICROSOFT AUSTRALIA

LinkedIn : https://www.linkedin.com/in/shanebaldacchino/
Twitter : sbaldacchino
Web : https://automation.baldacchino.net