**CORE SERVICE DESIGN:**

**Defender for Cloud**

atabricks

|  |  |
| --- | --- |
| IT Owner Details | |
| **Department** | DTS |
| **Contact Name** | Dominic Panzera |
| **Address** | 375 Manningham Road, Doncaster, Victoria 3108 |

|  |  |
| --- | --- |
| Document Control | |
| Title | Ambulance Victoria – Defender for Cloud Core Service Design |
| **File Name** | Ambulance Victoria – Defender for Cloud Core Service Design v1.0.docx |
| **Version** | 1.0 |
| **Status** | Released |
| **Release Date** | 8/03/2024 |

|  |  |  |  |
| --- | --- | --- | --- |
| Preparation |  |  |  |
| **Prepared** | Daniela Nikolic |  |  |
| **Authorised** | Dileep Pradeep |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version Tracking | | | |  |
| Version | Remarks | Change Requested | Pages Affected | Release Date |
| 1.0 | Initial Release | N/A | All | 8/03/2024 |

Table of Contents

[1. Overview 5](#_Toc160795807)

[1.1 Purpose and Audience 5](#_Toc160795808)

[1.2 Scope and Key Deliverables 5](#_Toc160795809)

[1.3 Glossary and Definitions 6](#_Toc160795810)

[2. Executive Summary 7](#_Toc160795811)

[3. Resource Cost 8](#_Toc160795812)

[4. WAF and Security Control Alignment 8](#_Toc160795813)

[4.1 Reliability 9](#_Toc160795814)

[4.1.1 Overview 9](#_Toc160795815)

[4.1.2 Defender for Cloud Reliability Checklist 9](#_Toc160795816)

[4.2 Cost Optimisation 9](#_Toc160795817)

[4.2.1 Overview 9](#_Toc160795818)

[4.2.2 Defender for Cloud Cost Optimisation Checklist 9](#_Toc160795819)

[4.3 Operational Excellence 10](#_Toc160795820)

[4.3.1 Overview 10](#_Toc160795821)

[4.3.2 Defender for Cloud Operational Excellence Checklist 10](#_Toc160795822)

[4.4 Performance Efficiency 10](#_Toc160795823)

[4.4.1 Overview 10](#_Toc160795824)

[4.4.2 Defender for Cloud Performance Efficiency Checklist 10](#_Toc160795825)

[4.5 Security 11](#_Toc160795826)

[4.5.1 Overview 11](#_Toc160795827)

[4.5.2 Defender for Cloud Security Checklist 11](#_Toc160795828)

[5. Architecture Summary 12](#_Toc160795829)

[5.1 Resource Overview 12](#_Toc160795830)

[5.1.1 Defender CSPM 12](#_Toc160795831)

[5.2 RBAC 13](#_Toc160795832)

[5.3 Design Decisions and Justifications 14](#_Toc160795833)

[5.3.1 Enabling Defender on all resources 14](#_Toc160795834)

[5.3.2 Deployment via Policy 14](#_Toc160795835)

[6. Azure Policies 15](#_Toc160795836)

[7. Configuration Template 16](#_Toc160795837)

[8. Acceptance 17](#_Toc160795838)

# Overview

This document covers the baseline design for the Defender for Cloud core service. The intention of this document is to define the overall resource design in isolation from a specific application. It is aimed to highlight the general process and requirements for building a Defender for Cloud in a repeatable fashion with consistent configurations. Design decisions and justifications have been included in the Architecture section, and this document can be used as a reference for new builds that require a Defender for Cloud.

This design caters to a Level 2 design which covers both Microsoft’s WAF (Well Architected Framework)[[1]](#footnote-2) and the Department of Health Control list.

Any deviations required to the standards defined in this document will require separate exemption and approval from the Cloud Governance Forum if they are required for any reason for a specific build.

## Purpose and Audience

This document will outline the standard design and configuration of this Azure service in Ambulance Victoria’s Azure tenancy as a baseline for any application infrastructure deployments.

This design is intended to:

* Meet Microsoft WAF standards.
* Meet the controls stipulated by the Department of Health.
* Define the baseline required for the deployment of the resource.

The audience for this document is those involved in the planning, designing, and implementing of the Application/Data infrastructure. This includes:

* + Ambulance Victoria IT staff

It is assumed that the reader knows and is familiar with Azure Cloud concepts and related topics.

## Scope and Key Deliverables

The scope of this core service design is to define the baseline deployment requirements and standards for the Defender for Cloud core service.

The key deliverables for this are:

* This design to outline the service definition Level 2 baseline standards.
* A technical configuration document that defines the deployment of this resource for each of the Service Tiers, or for any other logical standard such as size
* IaC templates for repeatable deployment of this core service

## Glossary and Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **AV** | Ambulance Victoria |
| **WAF** | Well Architected Framework |
| **CAF** | Cloud Adoption Framework |
| **Level 1** | Refers to a resource that has been designed to a CAF standard |
| **Level 2** | Refers to a resource that has been designed to a WAF standard with Department of Health controls overlayed |
| **AZ 2** | Refers to Ambulance Victoria’s legacy Azure Landing Zone still in use in some regards |
| **AZ 3** | Refers to Ambulance Victoria’s current Azure Landing Zone, also referred to as the Enterprise landing zone. This is the target state for migrations. |
| **SLA** | Service Level Agreement as defined by Microsoft |
| **DH** | Department of Health |
| **IaC** | Infrastructure as Code |
| **NSG** | Network Security Groups |

Table : Glossary and definitions

# Executive Summary

This design covers the baseline standards for the Defender for Cloud Core Service. This service has been assessed against the five pillars of WAF as well as the Department of Health Security Controls.

This section contains a summary of the major design decisions that have been made for defining the baseline of this resource as an outcome of the WAF and Security analysis detailed throughout this document.

Of the five WAF Pillars, it was found that Security was relevant.

This feature dictates security across the environment across all resources, so it is assumed to always be a Platinum service. Some of the main configurations include:

* Defender for all resources will be enabled across all subscriptions including Defender CSPM and Defender for workloads.
* Azure Policy will be used to enforce Defender plans being enabled automatically.

# Resource Cost

Defender for Cloud pricing varies depending on the underlying resource type. Typically it is a per instance per unit of time pricing[[2]](#footnote-3):

|  |  |  |
| --- | --- | --- |
| Resource Type | Resource | Price |
| Servers | Microsoft Defender for Servers Plan 1 | **$0.011**/Server/hour |
|  | Microsoft Defender for Servers Plan 2 | **$0.031**/Server/hour |
| Containers | Microsoft Defender for Containers | **$0.0144**/vCore/hour4 |
| Databases | Microsoft Defender for SQL on Azure-connected databases | **$0.032**/Instance/hour2 |
|  | Microsoft Defender for SQL outside Azure | **$0.023**/Instance/vCore/hour3 |
|  | Microsoft Defender for MySQL | **$0.032**/Instance/hour |
|  | Microsoft Defender for PostgreSQL | **$0.032**/Instance/hour |
|  | Microsoft Defender for MariaDB | **$0.031**/Instance/hour |
|  | Microsoft Defender for Azure Cosmos DB5 | **$0.0019** per 100 RU/S/hour |
| Storage | Microsoft Defender for Storage1 | **$0.0205** per storage account/hour6 |
|  | Malware Scanning7 (add-on to Defender for Storage) | **$0.230**/GB of data scanned |
| Service Layer | Microsoft Defender for App Service | **$0.031**/Instance/hour |
|  | Microsoft Defender for Key Vault | **$0.38**/Vault/month |
|  | Microsoft Defender for Resource Manager | **$7.70**/Subscription/month |

Table : Pricing construct for Defender for Cloud

# WAF and Security Control Alignment

The following are the five pillars of the Microsoft Well Architected Framework:

* [Reliability](https://learn.microsoft.com/en-us/azure/well-architected/#reliability)
* [Cost optimization](https://learn.microsoft.com/en-us/azure/well-architected/#cost-optimization)
* [Operational excellence](https://learn.microsoft.com/en-us/azure/well-architected/#operational-excellence)
* [Performance efficiency](https://learn.microsoft.com/en-us/azure/well-architected/#performance-efficiency)
* [Security](https://learn.microsoft.com/en-us/azure/well-architected/#security)

For this design, the security section will also cover the Department of Health Controls in addition with any Microsoft Security Best Practices. Each of these sections will detail relevant controls or baseline requirements for this core service that will be put in place.

## Reliability

### Overview

The term reliability refers to the availability of the system and its ability to recover from failure[[3]](#footnote-4). Resiliency strategies must be built into each element of the architecture. The pillars of reliability include:

* Design for business requirements
* Design for failure
* Observe application health
* Drive Automation

### Defender for Cloud Reliability Checklist

There is no specific guidance for Defender for Cloud under the Reliability pillar of the Well Architected Framework.

## Cost Optimisation

### Overview

The cost optimisation pillar is structured to support creating cost-effective workloads in the cloud[[4]](#footnote-5). It looks at removal of unnecessary spend and improving operational efficiency. The principles of cost optimisation revolve around:

* Choosing the correct resources
* Setting up budgets and maintaining cost constraints
* Dynamically allocate and deallocate resources
* Optimising workloads whilst aiming for scalable costs
* Continuously monitoring and cost managing

### Defender for Cloud Cost Optimisation Checklist

There is no specific guidance for Defender for Cloud under the Cost Optimisation pillar of the Well Architected Framework.

## Operational Excellence

### Overview

Operational Excellence aims to ensure that once the architecture is built, the ongoing operations are flawless. This includes repeatable and reliable deployments, automating to eliminate human error. To do this the following must be considered:

* Optimise the build and release process (including CI/CD and IaC)
* Understand Operational Health
* Test recovery and failure
* Focus on continuous improvement
* Use loosely coupled architecture

### Defender for Cloud Operational Excellence Checklist

There is no specific guidance for Defender for Cloud under the Operational Excellence pillar of the Well Architected Framework.

## Performance Efficiency

### Overview

Performance Efficiency refers to the ability of your systems and applications to meet user demands without breaking or creating a negative user experience[[5]](#footnote-6). This covers capacity and scalability:

* Design for horizontal scaling
* Run stress and performance tests
* Continuously monitor performances, particularly in Production systems

### Defender for Cloud Performance Efficiency Checklist

There is no specific guidance for Defender for Cloud under the Performance Efficiency pillar of the Well Architected Framework.

## Security

### Overview

Security refers to the ability of the environment to resist and manage threats.

This section covers both Microsoft Best Practices as well as relevant security controls provided by the Department of Health. With respect to the Microsoft WAF, Security is underpinned by the following[[6]](#footnote-7):

* Plan resources and how to harden them
* Automate and use least privilege
* Classify and encrypt data
* Monitor system security, plan incident response
* Identify and protect endpoints
* Protect against code-level vulnerabilities
* Model and test against potential threats

In addition to the Microsoft controls, the Department of Health has mandated security posture to Ambulance Victoria. Note there may be duplication between the Microsoft Security Best Practices and the Department of Health controls.

### Defender for Cloud Security Checklist

There is no specific guidance for Defender for Cloud. However, it supports meeting the following Microsoft Security Benchmark items across all supported resources:

* LT-1 Enable threat detection.

# Architecture Summary

## Resource Overview

Defender for Cloud is the Azure native threat detection and protection capability, with inbuilt security measures and practices that are designed to protect the Cloud from various threats. Within it are capabilities for[[7]](#footnote-8):

* A cloud security posture management (CSPM) solution that surfaces actions that you can take to prevent breaches
* A cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads

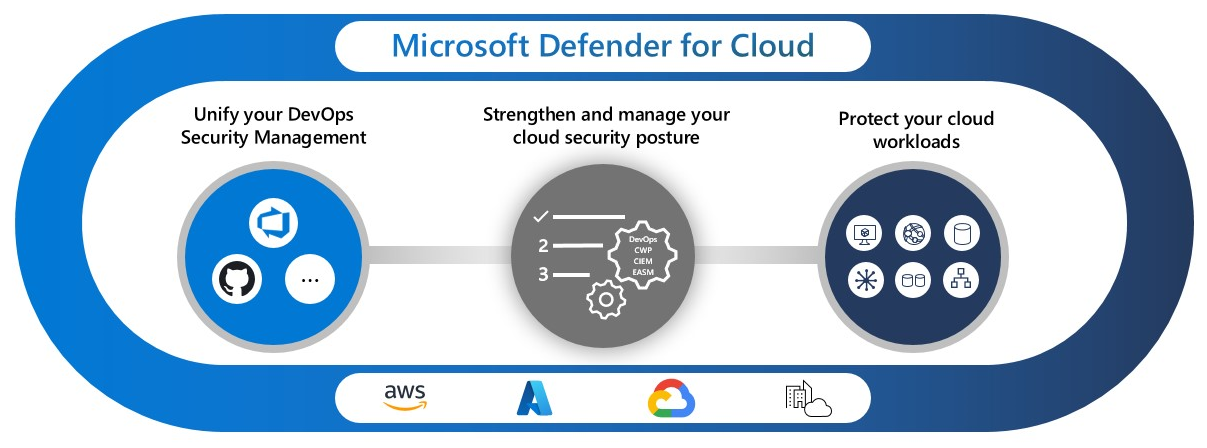


Figure : Defender for Cloud capabilities

### Defender CSPM

Defender Cloud Security Posture Management is a solution that is aimed at improving security posture overall. There are some foundational free capabilities that are default on the platform, with more advanced capabilities that can be enabled.

|  |  |  |  |
| --- | --- | --- | --- |
| Capability | CPSM (Free) | Defender CSPM | |
| Centralized policy management | | a | a |
| Secure score | | a | a |
| Multicloud coverage | | a | a |
| Cloud Security Posture Management (CSPM) | | a | a |
| Advanced Cloud Security Posture Management | |  | a |
| Data-aware Security Posture | |  | a |
| Attack path analysis | |  | a |
| Cloud Security Explorer | |  | a |
| Security governance | |  | a |
| Microsoft Entra Permissions Management | |  | a |
| Security governance | |  | a |

Table : Feature comparison of CPSM free tier vs paid tier

## RBAC

The following roles can be applied to Defender for Cloud[[8]](#footnote-9):

|  |  |
| --- | --- |
| Role Name | Description |
| Security Admin | View and update permissions for Microsoft Defender for Cloud. Same permissions as the Security Reader role and can also update the security policy and dismiss alerts and recommendations. |
| Security Assessment Contributor | Lets you push assessments to Microsoft Defender for Cloud |
| Security Reader | View permissions for Microsoft Defender for Cloud. Can view recommendations, alerts, a security policy, and security states, but cannot make changes. |

Table : RBAC roles relevant for this core service

## Design Decisions and Justifications

This section covers the design decisions and justifications that reflect the findings of the WAF and Security alignment. This will form the baseline requirements for the Defender for Cloud core service and will be captured in the accompanying Configuration Template with a set of pre-approved deployment settings for this resource. Any changes, modifications or removals to the pre-approved deployments must have specific approval from the Cloud Governance Forum prior to deployment.

### Enabling Defender on all resources

**Design Decision**: All Defender plans will be enabled for each subscription.

**Design Justification**: All available plans will be enabled for the following resources:

* Defender for Servers
* Defender for App Service
* Defender for Databases
* Defender for Storage
* Defender for Containers
* Defender for Key Vault
* Defender for Resource manager
* Defender for APIs

### Deployment via Policy

**Design Decision:** Azure Policy will be used to enable Defender for Cloud on subscriptions.

**Design Justification:** Using Azure Policy to ensure Defender is enabled on all resources on new subscriptions removes a manual step required to enable the plans on new subscriptions. It will automatically set the plans as each subscription is created.

# Azure Policies

The following Azure Policies will be applied to enable Defender on subscriptions as they are created:

|  |  |
| --- | --- |
| Policy Name | Scope |
| Azure Defender for App Service should be enabled | av management group |
| Azure Defender for Azure SQL Database servers should be enabled | av management group |
| Azure Defender for Key Vault should be enabled | av management group |
| Azure Defender for open-source relational databases should be enabled | av management group |
| Azure Defender for Resource Manager should be enabled | av management group |
| Azure Defender for servers should be enabled | av management group |
| Azure Defender for SQL servers on machines should be enabled | av management group |
| Azure Defender for SQL should be enabled for unprotected Azure SQL servers | av management group |
| Azure Defender for SQL should be enabled for unprotected PostgreSQL flexible servers | av management group |
| Azure Defender for SQL should be enabled for unprotected SQL Managed Instances | av management group |
| Azure Defender for Storage should be enabled | av management group |
| Azure Defender for Kubernetes should be enabled | av management group |
| Azure Defender for container registries should be enabled | av management group |

Table : Azure Policies

# Configuration Template

There is no specific configuration template for this deployment. The following table shows the list of plans that will be enabled for each new subscription:

|  |  |  |
| --- | --- | --- |
| Workload | Plan | Sub-components enabled |
| Servers | Plan 2 enabled | Agent deployment  Vulnerability Assessment  Endpoint Protection  Agentless scanning |
| App Service | N/A | N/A |
| Databases | SQL Databases  SQL server on machines  Open-source relational  Azure Cosmos DB | Azure Monitoring Agent for SQL server on machines |
| Storage | N/A | Malware scanning  Sensitive data discovery |
| Containers | N/A | Defender agent in Azure  Azure Policy for Kubernetees  Agentless discovery for Kubernetes  Agentless container vulnerability assessment |
| Key Vault | N/A | N/A |
| Resource Manager | N/A | N/A |
| APIs | Plan 1 | N/A |

# Acceptance

Signature of this page by appropriately delegated representatives of ​Ambulance Victoria​ signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

Signature of this page by appropriately delegated representatives of Ambulance Victoria signifies acceptance of this design document.

Logicalis will commence build and implementation work once it receives a signed copy of this design document.

|  |  |
| --- | --- |
| Project | Core Services |
| Document Version | 1.0 |

**Signed on behalf of Ambulance Victoria**

|  |  |
| --- | --- |
| Name | Dan Howarth |
| Position |  |
| Signature |  |
| Date signed |  |

**Signed on behalf of Logicalis Australia**

|  |  |
| --- | --- |
| Name | Daniela Nikolic |
| Position | Senior Cloud Engineer |
| Signature |  |
| Date signed |  |

1. https://learn.microsoft.com/en-us/azure/well-architected/ [↑](#footnote-ref-2)
2. There is no specific guidance for Defender for Cloud under the Performance Efficiency pillar of the Well Architected Framework. [↑](#footnote-ref-3)
3. https://learn.microsoft.com/en-us/azure/well-architected/resiliency/overview [↑](#footnote-ref-4)
4. https://learn.microsoft.com/en-us/azure/well-architected/cost/overview [↑](#footnote-ref-5)
5. https://learn.microsoft.com/en-us/azure/well-architected/scalability/overview [↑](#footnote-ref-6)
6. https://learn.microsoft.com/en-us/azure/well-architected/security/security-principles [↑](#footnote-ref-7)
7. https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction [↑](#footnote-ref-8)
8. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles [↑](#footnote-ref-9)