Contents

[2 Reference Architecture Diagram 2](#_Toc478564033)

[3 Context 3](#_Toc478564034)

[3.1 Overview 3](#_Toc478564035)

[4 Technical Configurations and Recommendations 3](#_Toc478564036)

[4.1 Network Segmentation and Security 3](#_Toc478564037)

[4.2 Data at Rest 4](#_Toc478564038)

[4.3 Logging and Auditing 5](#_Toc478564039)

[4.4 Secrets Management 5](#_Toc478564040)

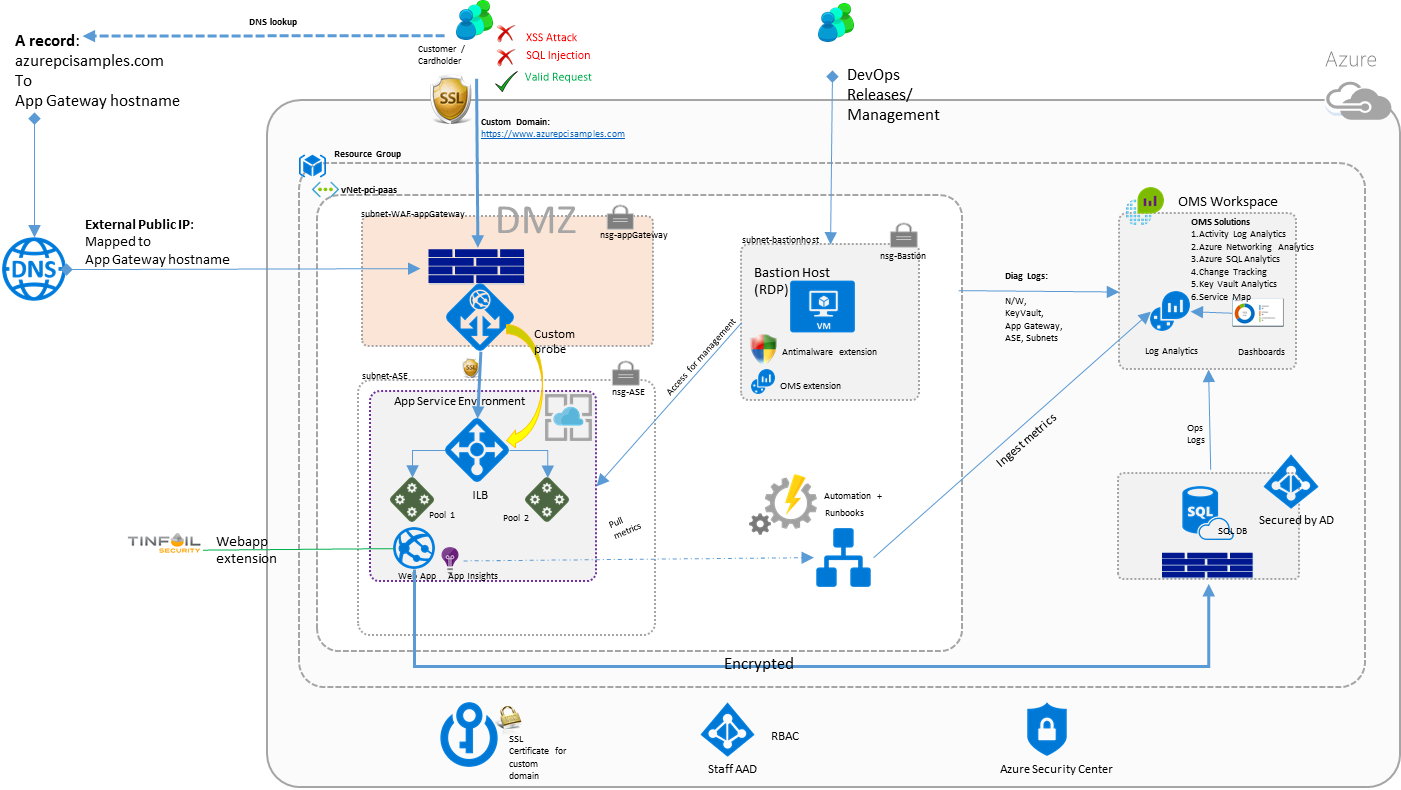
[4.5 Identity and Access 5](#_Toc478564041)

[4.6 Web and Compute 6](#_Toc478564042)

[4.7 Operations Management 8](#_Toc478564043)

[4.8 Security Center Integrations 9](#_Toc478564044)

# Reference Architecture Diagram



# Context

## Overview

The blueprint is intended to accelerate secure and compliant Azure PaaS services adoption especially for enterprise customers who want to focus on their applications and business functionality and not worry a lot about the infrastructure and operations components.

This blueprint highlights value in the following areas



# Technical Configurations and Recommendations

## Network Segmentation and Security

|  |  |
| --- | --- |
| RESOURCES | DESCRIPTION |
| Application Gateway | * [SSL Offload](https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-ssl-portal) * [Disable TLS v1.0 and v1.1](https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-end-to-end-ssl-powershell) * [Web Application Firewall](https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-webapplicationfirewall-overview) (WAF mode) * [Prevention mode](https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-web-application-firewall-portal) with OWASP 3.0 ruleset * [Diagnostics Logging](Diagnostics%20Logging%20for%20Application%20Gateway) * [Custom Health probes](https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-create-gateway-portal) |
| Virtual Network | A private virtual network with address spacing 10.0.0.0/16 |
| Network Security Groups | Each of the Network Tiers have a dedicated NSG   * A DMZ network security group for Firewall and Application Gateway WAF * An NSG for management jumpbox (bastion host) * An NSG for App Service Environment   Each of the NSGs have specific ports and protocols opened for the secure and correct working of the solution.  In addition, the following configurations are enabled for each NSG   * [Enabled Diagnostics logs and events are stored in storage account](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-nsg-manage-log) * [Connected OMS Log Analytics to the NSGs diagnostics](https://github.com/krnese/AzureDeploy/blob/master/AzureMgmt/AzureMonitor/nsgWithDiagnostics.json) |
| Subnets | Ensured each subnet is associated with its corresponding Network security group. |
| Custom Domain SSL Certificates | Https traffic enabled using custom domain SSL certificate. |

## Data at Rest

|  |  |
| --- | --- |
| RESOURCES | DESCRIPTION |
| Azure Storage | To meet encrypted Data-At-Rest requirements, all use of [Azure Storage](https://azure.microsoft.com/en-us/services/storage/) had the following   * [Storage Service Encryption](https://docs.microsoft.com/en-us/azure/storage/storage-service-encryption) |
| SQL Database | A PaaS SQL Database instance was used to showcase various security measures.   * [AD Authentication and Authorization](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication) * [Enabled Auditing Logging](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing-get-started) * [Enabled Transparent Data Encryption](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing-get-started) * [Enabled SQL DB Firewall rules](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-firewall-configure) (allowing for ASE worker pools and management clientIPs) * [Enabled Threat Detection](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-get-started) * [Enabled Always Encrypted Columns](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-always-encrypted-azure-key-vault) * [Enabled Dynamic Data masking](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-dynamic-data-masking-get-started) (using PostDeployment Powershell) |

## Logging and Auditing

* **Activity Logs**: Configure [Azure Activity Logs](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs) to provide insight into the operations that were performed on resources in your subscription.
* **Diagnostic Logs:** [Diagnostic Logs](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-of-diagnostic-logs) are all logs emitted by every resource. These logs could include Windows event system logs, blob, table, and queue logs.
* **Firewall Logs:** Application Gateway provides full diagnostics and access logs. Firewall logs are available for application gateway resources that have WAF enabled.
* **Log Archiving:** All diagnostics logs was configured to write to a centralized Azure storage account (of course encrypted) for archival and a defined retention period (2 days). Logs were then connected to Azure Log analytics (OMS) for processing, storing and dashboarding.

## Secrets Management

|  |  |
| --- | --- |
| RESOURCES | DESCRIPTION |
| Key Vault | Azure [Key Vault](https://azure.microsoft.com/en-us/services/key-vault/) helps safeguard cryptographic keys and secrets used by cloud applications and services.  Stores   * **Keys** - SQL DB Column Encryption keys (customer managed keys) * **Secrets** - Bitlocker keys for Azure Disk Encryption |

## Identity and Access

|  |  |
| --- | --- |
| RESOURCES | DESCRIPTION |
| Azure Active Directory | [Azure Active Directory](https://azure.microsoft.com/en-us/services/active-directory/) (Azure AD) is Microsoft’s multi-tenant cloud based directory and identity management service.  All users for the solution, were created in Azure Active Directory, this also included users accessing SQL Database |
| Active Directory Application | Authentication to the App is done through [Azure AD Application](https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-integrating-applications), and Service Principals associated.  Also, the [SQL DB column encryption](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-always-encrypted-azure-key-vault) is conducted using the AD App. Refer to [this sample](https://github.com/Microsoft/azure-sql-security-sample) from the Azure SQL DB team for more details. |
| Role Based Access Control | Azure [Role-Based Access Control](https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-configure) (RBAC) enables fine-grained access management for Azure. Specific Configurations for   * Subscription Access * Azure Key Vault access |

## Web and Compute

|  |  |
| --- | --- |
| RESOURCES | DESCRIPTION |
| Web Application | The [Web Apps](https://azure.microsoft.com/en-us/services/app-service/web/) feature in Azure App Service lets developers rapidly build, deploy, and manage powerful websites and web apps. Build standards-based web apps and APIs using .NET, Node.js, PHP, Python, and Java. Deliver both web and mobile apps for employees or customers using a single back end. Securely deliver APIs that enable additional apps and devices |
| Azure App Service | With [App Service](https://azure.microsoft.com/en-us/services/app-service/?b=16.52), Develop powerful applications for any platform or device, faster than ever before. Meet rigorous performance, scalability, security, and compliance requirements using a single back-end. |
| Virtual Machine | As the App Service Environment is secured and locked down, there needs to be a mechanism to allow for any DevOps releases / changes necessary. E.g. monitor WebApp using Kudu etc.  A Virtual Machine was stood up as a Jumpbox / Bastion host with the following configurations   * [Antimalware Extension](https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware) * [OMS Monitoring Extension](https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-windows-extensions-oms) * [VM Diagnostics Extension](https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-windows-extensions-diagnostics-template) * [Bitlocker Encrypted Disk](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption) using Azure Key Vault (respects Azure Government, PCI DSS and HIPAA requirements) * An [AutoShutDown Policy](https://azure.microsoft.com/en-us/blog/announcing-auto-shutdown-for-vms-using-azure-resource-manager/) – to reduce consumption of Virtual machine resources when not in use. |
| App Service Environment | An [App Service Environment](https://docs.microsoft.com/en-us/azure/app-service-web/app-service-app-service-environment-intro) is a Premium service plan is used for compliance reasons. This allowed us for the following controls/configurations   * Host inside a secured Virtual Network and Network security rules * [Internal Load Balancing mode](https://docs.microsoft.com/en-us/azure/app-service-web/app-service-environment-with-internal-load-balancer) (mode 3) * [Disable TLS 1.0](https://docs.microsoft.com/en-us/azure/app-service-web/app-service-app-service-environment-custom-settings) – a deprecated TLS protocol from PCI DSS standpoint * [Change TLS cipher](https://docs.microsoft.com/en-us/azure/app-service-web/app-service-app-service-environment-custom-settings) * [WAF – Restrict Data](https://docs.microsoft.com/en-us/azure/app-service-web/app-service-app-service-environment-web-application-firewall)   NSG configurations to let specific traffic through   * [Network Architecture Overview of App Service Environments](https://docs.microsoft.com/en-us/azure/app-service-web/app-service-app-service-environment-network-architecture-overview) * [Control Inbound Traffic to an App Service Environment](https://docs.microsoft.com/en-us/azure/app-service-web/app-service-app-service-environment-control-inbound-traffic) * [Opening outbound SQL DB traffic from ASE](https://docs.microsoft.com/en-us/azure/app-service-web/app-service-app-service-environment-network-configuration-expressroute) |
| Azure Security Center | With [Azure Security Center](https://azure.microsoft.com/en-us/services/security-center/), you get a central view of the security state of all of your Azure resources. At a glance, verify that the appropriate security controls are in place and configured correctly. And quickly identify any resources that require attention. |
| Web Apps Vulnerability Assessment via Tinfoil | For Azure Web Apps, [Tinfoil Security](https://azure.microsoft.com/en-us/blog/web-vulnerability-scanning-for-azure-app-service-powered-by-tinfoil-security/) is the only security vulnerability scanning option built into the Azure App Service management experience. |
| Antimalware extension for VMs | [Microsoft Antimalware](https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware) for Azure Cloud Services and Virtual Machines is free real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your Azure systems. |

## Operations Management

|  |  |
| --- | --- |
| RESOURCES | DESCRIPTION |
| Application Insights | Gain [actionable insights](https://azure.microsoft.com/en-us/services/application-insights/) through application performance management and instant analytics |
| Log Analytics | [Log Analytics](https://azure.microsoft.com/en-us/services/log-analytics/) is a service in Operations Management Suite (OMS) that helps you collect and analyze data generated by resources in your cloud and on-premises environments. |
| OMS Solutions | 9 OMS Solutions are pre-installed with this Reference Solution   1. [Activity Log Analytics](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs) 2. [Azure Networking Analytics](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-azure-networking-analytics?toc=%2fazure%2foperations-management-suite%2ftoc.json) 3. Azure SQL Analytics 4. [Change Tracking](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-change-tracking?toc=%2fazure%2foperations-management-suite%2ftoc.json) 5. [Key Vault Analytics](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-azure-key-vault?toc=%2fazure%2foperations-management-suite%2ftoc.json) 6. [Service Map](https://docs.microsoft.com/en-us/azure/operations-management-suite/operations-management-suite-service-map) 7. [Security and Audit](https://www.microsoft.com/en-us/cloud-platform/security-and-compliance) 8. [Antimalware](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-malware?toc=%2fazure%2foperations-management-suite%2ftoc.json) 9. [Update Management](https://docs.microsoft.com/en-us/azure/operations-management-suite/oms-solution-update-management) |

## Security Center Integrations

Default deployment is intended to provide for a clean chit of security center recommendations, indicating a healthy and secure configuration state of the solution.