



EBOOK

Microsoft Azure

A compelling choice of cloud computing platform
for organisations of all sizes and industries.



Microsoft Azure

Contents

Introduction	2
Azure Well Architected Framework	3
Infrastructure as a Service	4
Azure Virtual Desktop	5
Azure Files	6
Azure Backup and DR	7
Azure Geo-Redundant Backup	7
Azure Site Recovery	8
Azure Firewall	9
Azure Monitor	10
Azure Infrastructure as Code	11
Wavenet Support	12

Introduction

What is Microsoft Azure?

Microsoft Azure is a versatile cloud computing platform that offers a wide range of services that can be used for virtual computing, storage, analytics, and networking, for example. It allows organisations to innovate, grow, and manage applications in the cloud on a global network of Microsoft-managed data centres, providing flexibility, scalability, security, integration, hybrid cloud capabilities, and cost-effectiveness.

ON PREMISES	INFRASTRUCTURE AS A SERVICE	PLATFORM AS A SERVICE	SOFTWARE AS A SERVICE	BENEFITS
APPLICATIONS	APPLICATIONS	APPLICATIONS	APPLICATIONS	OPTIMISED COSTS FLEXIBILITY SCALABILITY ENHANCED SECURITY COMPLIANCE BACKUP, RECOVERY, AND FAILOVER SIMPLIFIED MONITORING AND MANAGEMENT INTEGRATION HYBRID CAPABILITIES
DATA	DATA	DATA	DATA	
RUNTIME	RUNTIME	RUNTIME	RUNTIME	
MIDDLEWARE	MIDDLEWARE	MIDDLEWARE	MIDDLEWARE	
OPERATING SYSTEM	OPERATING SYSTEM	OPERATING SYSTEM	OPERATING SYSTEM	
VIRTUALISATION	VIRTUALISATION	VIRTUALISATION	VIRTUALISATION	
SERVERS	SERVERS	SERVERS	SERVERS	
STORAGE	STORAGE	STORAGE	STORAGE	
NETWORKING	NETWORKING	NETWORKING	NETWORKING	
DEPLOYED AND SERVICED IN AZURE				

- You can outsource your IT infrastructure and create your own web apps on Azure, paying for what you use, without purchasing or maintaining the groundwork.
- The payment options include a pay-as-you-go model for usage and scaling, and a reserved instances model for consistent monthly costs.
- Wavenet's Azure expertise will optimise your solution to reduce costs, increase resilience and security, and improve operational excellence throughout.
- Azure can be used to replace or supplement your on-premise servers.
- Azure perfectly integrates with Microsoft products such as Office 365, Outlook, and SharePoint, with license synergy.
- The support for open-source technologies enables developers to use their preferred languages, frameworks, operating systems, databases, and devices for tailored integrations.
- Connect your on-premises infrastructure to Azure for increased mobility and a reliable hybrid cloud platform.
- Azure ensures strong security and compliance with certifications like ISO 27001, HIPAA, and GDPR.

Azure Well Architected Framework

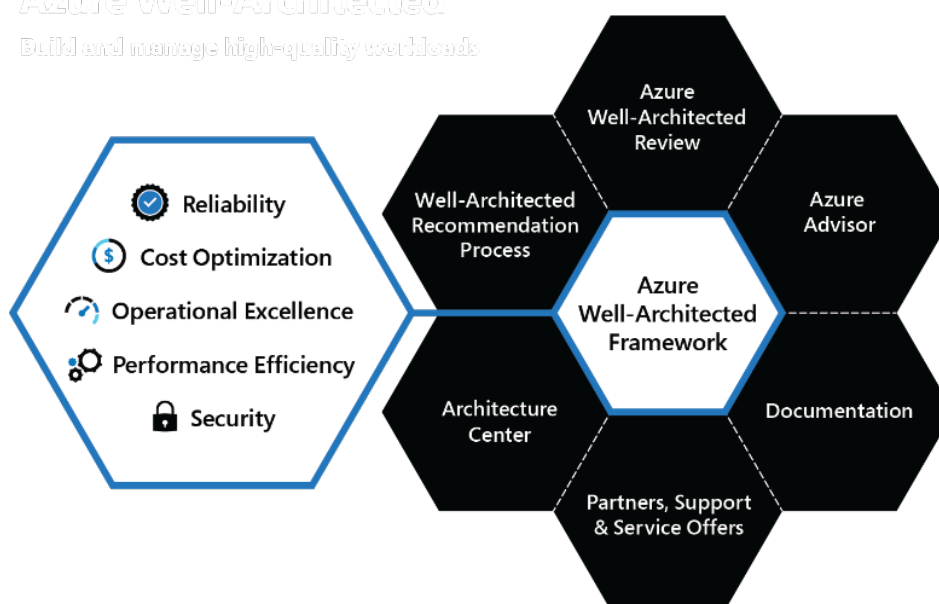
The Azure Well-Architected Framework is a set of best practices and guidelines developed by Microsoft that help customers design, build, and deploy applications on Azure in a secure, scalable, and efficient manner.

The framework consists of five pillars.

- **Cost Optimisation:** This pillar focuses on optimising costs and maximising value by using cost-effective solutions, monitoring usage, and optimising resource utilisation.
- **Operational Excellence:** This pillar focuses on ensuring the reliability, performance, and security of applications by using automated processes, monitoring and logging, and incident management.
- **Performance Efficiency:** This pillar focuses on designing solutions that are optimised for performance by using scalable architectures, caching, and leveraging Azure services.
- **Security:** This pillar focuses on ensuring the confidentiality, integrity, and availability of applications by using Azure security services and implementing security best practices.
- **Reliability:** This pillar focuses on ensuring the availability and recoverability of applications by using high availability architectures, disaster recovery solutions, and backup and restore capabilities.

Azure Well-Architected

Build and manage high-quality workloads



The Azure Well-Architected Framework provides a comprehensive and flexible approach to designing, building, and deploying applications on Azure. It helps customers align their applications with Azure best practices, assess their applications against the framework, and continuously improve their solutions based on feedback and best practices.

Infrastructure as a Service (IaaS)

Azure IaaS

Azure Infrastructure as a Service (IaaS) is a cloud computing model that provides virtualised computing resources, such as virtual machines (VMs), storage, and networking, over the internet.

By using Azure IaaS, you can easily migrate your on-premises workloads to the cloud, extend your data centre to Azure, and build new applications with high scalability and availability, flexibility and cost-effectiveness.

Key features and benefits of Azure IaaS

- **Virtual Machines:** Azure IaaS provides a wide range of VM sizes and types, including Windows and Linux VMs, GPU-optimised VMs, and memory-optimised VMs, to meet various workload requirements.
- **Storage:** Azure IaaS provides different types of storage options, including performance-tiered options for Azure Files, and Azure Managed Disk Storage, Object Storage, Table Storage and more, to meet various data storage requirements.
- **Networking:** Azure IaaS provides networking services, such as Azure Virtual Network, Azure Load Balancer, and Azure VPN Gateway, to enable secure connectivity between your on-premises network and Azure.
- **Security:** Azure IaaS provides security features, such as Azure Security Centre, Azure Firewall, and Azure DDoS Protection, to help protect your resources and data in the cloud.
- **Scalability:** Azure Virtual Machine Scale Sets provides automatic scaling of virtual machines based on demand, enabling you to easily handle spikes in traffic or usage.
- **Hybrid Cloud:** Azure IaaS enables you to integrate your on-premises infrastructure with the cloud, enabling hybrid cloud scenarios such as disaster recovery, backup, and extending your data centre to Azure.

Billing of Microsoft Azure services commence from the point in which resources are provisioned. This means that you may be paying for the new Azure services as well as your existing environment for a short period of time during the migration process.



Azure Virtual Desktop (AVD)

What is Azure Virtual Desktop (AVD)?

Azure Virtual Desktop is a cloud-based virtual desktop infrastructure (VDI) solution provided by Microsoft Azure that allows you to securely access your Windows desktop and applications from anywhere, on any device. It provides a flexible and scalable solution for remote access, with features for user management, security, and cost optimisation.

An organisation often adopts Azure Virtual Desktop to mitigate risks that are related to contracts, regulations, compliance, sovereignty, an elastic workforce, and to support the modernisation of their desktop environment and flexible working / BYOD culture.

AVD target outcomes



**Productivity on a
PC, Laptop, Phone,
Tablet or Browser**



**Safe access to
company data
& applications**



**Supporting end
users during cloud
migration & transition**



**Optimising the
costs of enabling
the workforce**

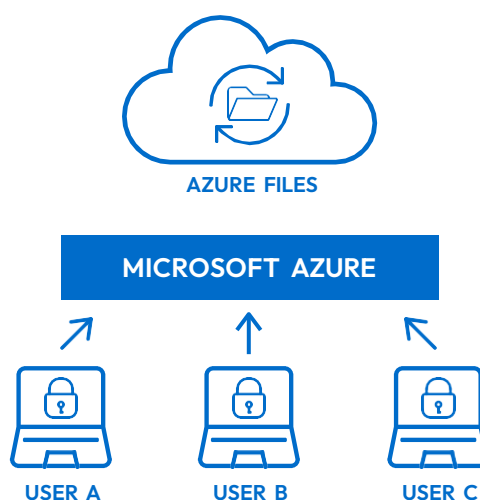
Key features and benefits of Azure Virtual Desktop

- **Remote access:** Azure Virtual Desktop provides remote access capabilities, allowing you to securely access your Windows desktop and applications from anywhere, on any device.
- **Multi-session Windows 11:** Azure Virtual Desktop supports multi-session Windows 11, allowing you to run multiple users on a single virtual machine, reducing the number of VMs required and optimising costs.
- **Integration with Microsoft 365:** Azure Virtual Desktop integrates with Microsoft 365, allowing you to run your desktop and applications with the latest version of Office and other Microsoft productivity tools.
- **Security:** Azure Virtual Desktop leverages security features and services, such as Microsoft Entra ID, Conditional Access and Multi-Factor Authentication, ensuring the protection of your virtual desktop and applications.
- **User management:** Azure Virtual Desktop provides user management capabilities, allowing you to manage users and assign desktops and applications based on their roles and responsibilities.
- **Scalability:** Azure Virtual Desktop is highly scalable, allowing you to easily add or remove virtual desktops and applications based on your business needs.

Azure Files

What is Azure Files?

Azure Files is a cloud-based file storage service provided by Microsoft Azure that enables you to create fully managed file shares in the cloud, offering a familiar experience to users accustomed to on-premises file shares without the management overhead of the underlying infrastructure (PaaS). It provides a simple and scalable solution for storing and sharing files in the cloud, with features for high availability, performance, and security.



Key features and benefits of Azure Files

- **Fully managed file storage:** Azure Files provides a fully managed file storage solution, eliminating the need for you to manage and maintain file servers in your on-premises environment.
- **Scalability:** Azure Files is highly scalable, allowing you to store and share large amounts of data across multiple file shares.
- **High availability:** Azure Files provides high availability, with automatic failover and built-in redundancy to ensure that your files are always available.
- **Performance:** Azure Files provides high-performance access to your files, with support for multiple protocols including Server Message Block (SMB) and Network File System (NFS).
- **Security:** Azure Files provides built-in security features, including encryption, access control, and network isolation, ensuring that your files are protected from unauthorised access.
- **Integration with other Azure services:** Azure Files integrates with other Azure services, such as Azure Active Directory, Azure Backup, and Azure Site Recovery, allowing you to easily manage and protect your files

Azure Backup and DR

Backup and Disaster Recovery

In the case of service disruption or accidental deletion or corruption of data, Azure backup and disaster recovery can reestablish your business services in a timely and orchestrated manner, with an end-to-end backup and disaster recovery solution that is simple, secure, scalable, cost-effective and can also be integrated with an on-premises data protection solution.

Azure Geo-Redundant Backup (GRS)

Azure GRS (Geo-Redundant Storage) Backup is a backup and disaster recovery solution provided by Microsoft Azure that helps you to protect your data and applications against unplanned outages and data loss. It provides a geographically dispersed backup solution, with data replication to a secondary Azure region, ensuring that your data is available even in the event of a regional disaster.

Key features and benefits of Azure GRS Backup

- **Data replication:** Azure GRS Backup replicates your data to a secondary Azure region, providing a geographically dispersed backup solution that ensures data availability in the event of a regional disaster.
- **Automatic failover:** Azure GRS Backup provides automatic failover to the secondary region, allowing your applications to continue running even in the event of an outage in the primary region.
- **Continuous data protection:** Azure GRS Backup provides continuous data protection, ensuring that your data is always up-to-date and available for restore.
- **Encryption:** Azure GRS Backup provides encryption for your data both at rest and in transit, ensuring that your data is protected against unauthorised access.
- **Granular backup and restore:** Azure GRS Backup provides encryption for your data both at rest and in transit, ensuring that your data is protected against unauthorised access and accidental or malicious deletion.
- **Integration with other Azure services:** Azure GRS Backup integrates with other Azure services, such as Azure Site Recovery, providing a comprehensive backup and disaster recovery solution for your Azure resources.
- **Default policies include:** 30 daily restore points, 12 monthly restore points, UK South to UK West backup regions. Additional recovery points can be added at additional cost and are subject to your exact requirements. Azure backup policies can be tailored on a per resource basis and aligned to budgetary and compliance requirements to ensure they remain cost effective.

This is a point-in-time backup and is not live replication. For high availability and replicated backups Azure Site Recovery (ASR) should be considered for Zonal failover. Additional recovery points can be added at additional cost and are subject to your exact requirements.



Azure Site Recovery

Azure Site Recovery helps your business to keep doing business, even during major IT outages.

Azure Site Recovery is a disaster recovery and business continuity service provided by Microsoft Azure that helps you to protect and recover your on-premises and Azure applications and data in the event of an outage. It is easy to deploy with failover, and failback processes that help to keep your applications running during planned and unplanned outages.

Key features and benefits of Azure Site Recovery

- **Replication:** Azure Site Recovery provides replication capabilities, allowing you to replicate your on-premises infrastructure to Azure and existing Azure infrastructure to other Azure Zones or Regions for disaster recovery purposes.
- **Failover:** Azure Site Recovery provides failover capabilities, allowing you to failover to Azure in the event of an outage, ensuring business continuity.
- **Testing:** Azure Site Recovery provides testing capabilities, allowing you to test your disaster recovery plan without impacting production workloads.
- **Integration with other Azure services:** Azure Site Recovery integrates with other Azure services, such as Azure Backup, Azure Virtual Machines, and Azure Storage, providing a comprehensive solution for disaster recovery and business continuity.
- **Scalability:** Azure Site Recovery is highly scalable, allowing you to protect and recover large-scale and complex environments with ease.

Firewall for Azure

Is a firewall required in Azure?

In an on-premises environment, a firewall is one of the most essential security components. If you are using a virtual machine in Azure, you need to ensure that you have a firewall in place in order to protect your data.

Without a firewall, your data is at risk of being compromised by malicious actors. Azure has multiple firewall offerings depending on use case, such as Azure Firewall and Azure Web Application Firewall.

Azure Firewall has a number of security features built into their firewall depending on the SKU chosen, such as Denial of Service protection, access control lists, and traffic monitoring.

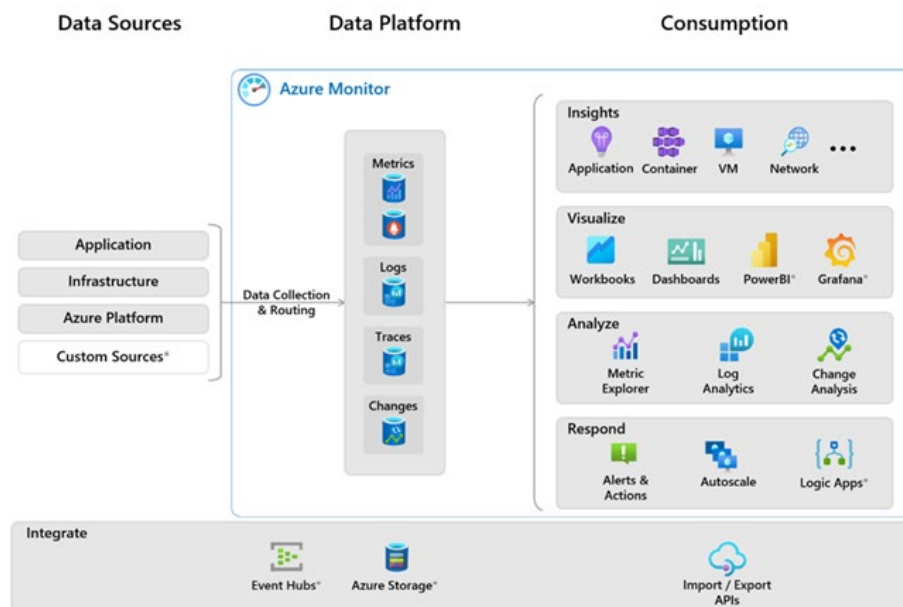
Azure also supports third-party Network Virtual Appliances (NVAs) from many leading firewall vendors, such as Watchguard, Fortinet, Cisco, Palo Alto, which can be used to offer consistency with the protection already offered to your on-premises networks. Wavenet's Azure consultants will advise you on the best firewall solution to meet the needs of your business.



Azure Monitor

What is Azure Monitor?

Azure Monitor is a cloud-based monitoring and analytics solution provided by Microsoft Azure that helps you to monitor and analyse the performance and health of your applications, services, and infrastructure. It provides a comprehensive and scalable solution for monitoring and troubleshooting your resources, with features for data collection, visualisation, alerting, and analysis.



Key features and benefits

- **Data collection:** Allows the collection of performance data, logs, and other metrics from your applications, services, and infrastructure.
- **Visualisation:** Allows you to visualise your performance data in charts, graphs, and dashboards, providing a real-time view of the health and performance of your resources.
- **Alerting:** You can set up alerts based on thresholds and conditions, and receive notifications when issues arise.
- **Azure Monitor:** Provides analysis capabilities, allowing you to analyse your performance data to identify issues, troubleshoot problems, and optimise performance.
- **Integration with other Azure services:** Provides comprehensive solution for monitoring and troubleshooting your resources with integrations such as Azure Virtual Machines, Azure Kubernetes Service, and Azure Storage.
- **Highly scalable:** Allows you to monitor and analyse large-scale and complex environments with ease.

Azure Infrastructure as Code

What is Azure Infrastructure as Code (IaC) ?

Infrastructure as Code (IaC) on Azure works by allowing Wavenet developers to script and automate the provisioning and management of Azure resources using declarative or imperative code, which simplifies the configuration and makes it more maintainable. Throughout the development process, Azure provides feedback and alerts on the status of the infrastructure for the troubleshooting of issues that may arise.

The result is a fully provisioned and configured Azure environment, set up exactly as defined in the IaC code. This process can be repeated consistently and reliably, enabling teams to manage their infrastructure more effectively and reduce manual errors.

Using Infrastructure as Code (IaC)

Using Infrastructure as Code (IaC) allows Wavenet to define and manage your cloud infrastructure using machine-readable files, rather than manually configuring resources through a user interface such as the Azure Management Portal. The use of Infrastructure as Code (IaC) is in adherence to the principles laid out in the Azure Well Architected Framework (WAF).

Infrastructure as Code allows Wavenet to describe your desired infrastructure configuration, including virtual machines, networks, storage, and more, using domain-specific coding languages such as Bicep and Terraform. These templates are stored in a secure, externally hosted code repository, to serve as blueprints for your infrastructure enabling consistent and repeatable deployments and allowing for any deviation from the baseline configuration to be automatically remediated. By automating the provisioning and configuration of resources, IaC reduces the risk of human error and ensures infrastructure consistency across environments. Externally managed code repositories interface with Azure DevOps and Azure Pipelines to provide additional versioning, testing, and deployment functionality infrastructure code, enabling continuous integration and delivery practices.

During the pre-project consultancy and discovery phase, Wavenet's team of Azure specialist consultants will determine the suitability of deploying your Azure infrastructure as code. This may depend on the size and complexity of the proposed solution and your requirements in terms of ongoing Wavenet managed service and support.

Wavenet Support

Wavenet's UK service desk can provide managed IT support and maintenance for your Azure and MS365 environments.

Our support telephone lines are open between 8.45am and 5.30pm Monday to Thursday and 5.00pm Friday (excluding Bank Holidays).

Additional extended hours agreements are available for earlier starts, later finishes and weekend cover if required.

Service Levels

All faults are validated when reported and subsequently classified as below. These Target Service Levels will apply unless contract specific agreements are already in place.

Priority	Definition
P 1	Critical – Outage across whole organisation, total loss of service (Site Down)
P 2	High – Service is available but either reduced functionality or degradation is creating significant business impact
P 3	Medium – Service is available and reduced functionality or degradation is limited to one/small number of users, or is not having a significant business impact
Service Requests	Service Requests/Change Request/Informational – “How to” queries, and requests for changes to either service or configuration of equipment.

SLA's

Issue Type	Remote Response Time
Critical Equipment and Server OS Support	1 hour
End Point Support and Desktop OS Support	2 hours
Service Requests	8 hours

WAVENET.CO.UK

0333 234 0011

Wavenet Limited
One Central Boulevard
Blythe Valley Park
Solihull, West Midlands
B90 8BG
publicsector@wavenet.co.uk

 **wavenet**



Networking &
Connectivity



Unified
Communications
& Voice



Contact Centres



Mobile Solutions
& IoT



IT, Cloud
& Technology



Network
Intelligence



Cyberguard