Advantage
transform the way you work

MICROSOFT **AZURE**

What is Microsoft Azure?

Azure is a cloud platform created by Microsoft.

HELLO@ADVANTAGE.CO.UK | 020 3004 4600 | WWW.ADVANTAGE.CO.UK

Advantage
transform the way you work

What is the **cloud?**

Among all the possible definitions, one captures the essence of the cloud in the simplest way:

"The cloud is a huge pool of resources that supports a variety of services."

The foundation of the cloud is a large pool of storage, computers and networking resources. A key value proposition of the cloud is that you can acquire any amount of these resources at any time, from anywhere, without needing to worry about managing any underlying infrastructures; and when you are done with these resources, you can return them to the cloud just as easily to avoid the unnecessary cost to keep them around.

"Everything is going to be connected to cloud and data... All of this will be mediated by software."

Satya Nadella, CEO, Microsoft

Azure's Global Footprint

Microsoft has built huge datacentres that have a combined total of more than 1 million servers. These datacentres are strategically placed at different geographic locations and are connected by high performance fibre-optic networks. They provide continuous support to more than 200 cloud services. Azure operates in 54 regions and 140 Countries. Each region contains one or more datacentres.

Trustworthy Computing

Although the adoption of the cloud has been accelerating, many organisations still have doubts when it comes to handling their valuable business data and mission critical workloads to a third party.

Cloud platforms such Azure need to work with the highest standards and greatest transparency to build their credibility as trust-worthy business partners. It is the policy of Microsoft that security, privacy, and compliance are a shared responsibility between Azure and Azure's customers.

Azure takes over some of the burden for implementing operational processes and technical safeguards, including (but not limited to) the following:

Physical security and continuous surveillance

Azure data centres are protected by physical barriers and fencing, with integrated alarms, cameras and access control. The facilities are constantly monitored from the operations centre.

Protection against virus, malware, and DDoS attacks

Azure scans all software components for malware and viruses during internal builds and deployments. Azure also enables real-time protection, on-demand scanning and monitoring for Cloud Services and VM's. To prevent attacks such as DDoS, Azure performs big data analysis of logs to detect and respond to intrusion risks and possible attacks.

Activity monitoring, tracing and analysis, and abnormality detection

Security events are continuously monitored and analysed. Timely alerts are generated so that hardware and software problems can be discovered and mitigated early.

System patching, such as applying security patches

When patch releases are required, they are analysed and applied to the Azure environment based on the severity. Patches are also automatically applies to customer guest VMs unless the customer has chosen manual upgrades, in which case the customer is responsible for patching.

Customer data isolation and protection

Azure customers are logically isolated from one another. An Azure customer has no means to access to another customer's data, either intentionally or unintentionally.

Advantage
transform the way you work

Azure Keeps Your Data Secure

Azure safeguards data in facilities that are protected by industry leading physical security systems and are compliant with a comprehensive portfolio of standards and regulations including, but not limited to:

CYBER ESSENTIALS PLUS · FCA · BANK OF ENGLAND PRUDENTIAL REGULATI AUTHORITY · GDPR · EU General Data Protection Regulation · HIPAA COMPLIANT · ISO 27001 · HM Government G-Cloud Supplier

Find out more at **http://azure.microsoft.com/en-us/support/trust-center/**

What is Azure SQL?

Azure SQL is a relational database service in the cloud based on the Microsoft SQL Server engine.

Azure SQL Database delivers predictable performance, scalability with no downtime, business continuity and data protection.

When you use SQL Database, you automatically take advantage of its many built-in features.

SQL Database high availability

All SQL Databases have an uptime Service Level Agreement (SLA) of 99.99%.

Each SQL Database has three replicas running at any given time. If the primary replica fails, SQL Database automatically fails-over to the secondary replica to ensure continuous data access. If replica fails, a new one is automatically created to always maintain three replicas.

Automated Backups

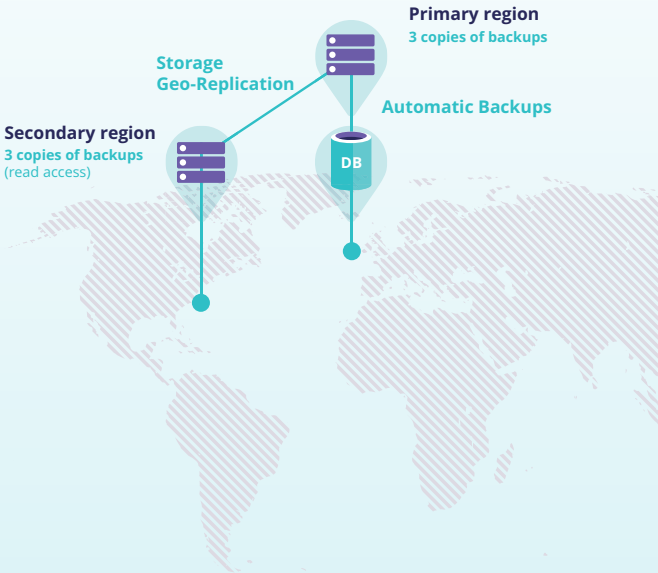
The Azure SQL Database service protects all databases with an automated backup that is retained for 35 days.

Full backups are taken every week, differential backups every day, and log backups every 5 minutes.

The backups are scheduled automatically and managed silently in the background. Backup files are stored in a Read Access GeoRedundant Storage (RA-GRS).

RA-GRS maintains six copies of your data, with three copies residing in the primary region, and another three copies residing in a backup secondary region that is hundreds of miles away from the primary region.

When the primary region becomes unavailable RA-GRS provide read access to data in the secondary region.



Point-In-Time Restore

Point-In-Time Restore allows you to restore a database to any point of time within a database's retention period.

You can restore an existing database as new database. You cannot overwrite the existing database. If you are restoring the database for recovery purposes you can treat the restored database as a replacement for the original database or use it to retrieve data from and then update the original database.

The time taken to restore a database depends on many factors, including the size of the database, the number of transaction logs, the time point selected, and the amount of activity that needs to be replayed to reconstruct the state at the selected point. Automatic backups and Point-In-Time Restore protect your databases from accidental data corruption or data deletion.

Geo – Restore

Geo-Restore allows you to restore a database from a copy of the most recent daily backup in geo-replicated storage (RA-GRS) to a server in any other region, in the event of large-scale outage in primary region where the database is hosted.

All backups are geo-replicated and can have a delay between when the backup is taken in primary region and geo-replicated to the storage in a secondary region. This delay can be up to an hour so in the event of a disaster there can be up to 1-hour data loss. Geo-Restore is the most basic of the disaster recovery solutions available in SQL Database.

Active Geo – Replication

Active Geo-Replication provides a database-level disaster recovery solution from a permanent loss of an entire datacentre or parts of a datacentre caused by natural disasters, catastrophic human errors, or malicious acts.

Active Geo-Replication enables you to configure up to 4 readable secondary databases in different data centre locations (regions).

After the secondary database has been created, updates to the primary database are asynchronously replicated to the secondary database automatically.

If for any reason your primary database fails, or simply needs to be taken offline, you can failover to any of your secondary databases. A secondary database is promoted to a new primary. When the failed primary recovers and is available again, the system will automatically mark it as a secondary and bring it up-to-date with the new primary.

Advantage
transform the way you work

Manual Backup (Import/ Export)

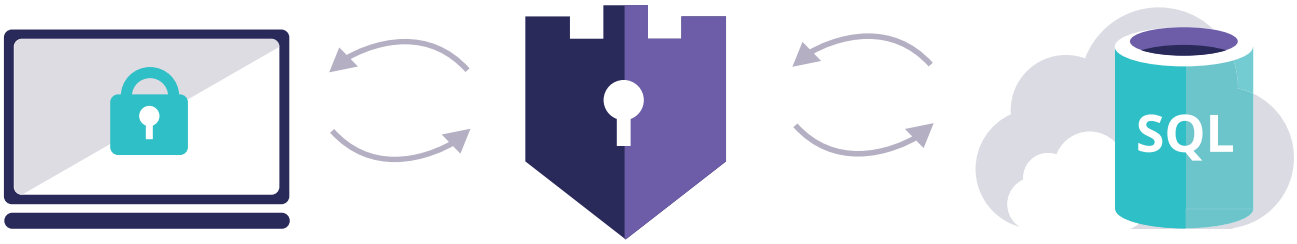
Azure SQL provide the alternative features that allow you manually backup your databases. You can use SQL Database Import and Export Service to export BACPACK files, which contain a logical copy of the schema as well as the data of a database. You can then import the file back to your database for disaster recovery.

We encourage you to use Point-In-Time Restore as part of your business continuity strategy, and only to use export as needed for longer term archival or data migration purposes.

Layers of protection

SQL Database provides multiple layers of data protection for a Dynamics ERP, such as NAV or GP, deployment. Your data is protected by encrypting data while at rest, in motion or in use, authenticating only authorized users against the database or application, and limiting user access to the appropriate subset of the data.

Additionally, SQL Database provides continuous monitoring and auditing of activities to help detect potential threats and provide a record of critical events in case of a breach. These features are balanced by the ability to quickly implement features and mitigate security risk without compromising developer productivity or a customer's experience.



Threat detection and alerts

Threat Detection detects anomalous database activities indicating potential security threats to the database.

Threat Detection provides a new layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities. With threat and anomaly detection, SQL Database has built-in behavioural analysis, real-time alerts, a configurable threat policy, an audit log, and intelligent ways to detect and fix unusual patterns.

Transparent Data Encryption

Azure SQL Database transparent data encryption helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest.

Firewall

Prevent all access to your database server until you specify which computers have permission. The firewall grants access to databases based on the originating IP address of each request. You can create firewall rules at the server and database levels.

Azure Virtual Machines – Features & Benefits for Dynamics ERP Solutions

- Virtual machines (VM's) are part of the Microsoft Azure Infrastructure-as-a-Service (IaaS) offering.
- Azure Virtual Machines are a flexible and powerful option for deploying workloads into the cloud.
- Virtual Machines can provide the on-ramp for migrating workloads from on-premises to Azure because they are usually the most compatible with existing solutions.
- Azure VMs also provide you full control over operating system, along with advanced configuration options for networking and storage.
- VMs are managed through a centralised web-based portal.

Azure VM High Availability

You can configure VMs on Azure two ways: single-instance and multi-instance.

Single-instance VMs are stand-alone VMs.

Azure periodically performs planned maintenance on the hosting infrastructure. Many of these maintenances occur without any impact to hosted VMs. However, some of these updates will require your VMs to be shut down or rebooted. If your application is deployed on a single instance VM, the application will become unavailable during this maintenance window. To help preclude any problems, Microsoft sends emails notices to single-instance customers, indicating the exact time on which the maintenance is scheduled.

During unplanned maintenance that is carried out in response to unexpected events, such as a hardware failure, your application will be unavailable.

Multi-instance VMs are joined to a same logical group called an Availability Set. When Azure performs planned maintenance, it guarantees that not all machines in the same Availability Set will be shut down in the same time. At the hardware level multiple VMs don't share a common power source or network switch, so the probability of two VMs falling at the same time is low, in case of unexpected physical infrastructure problems.

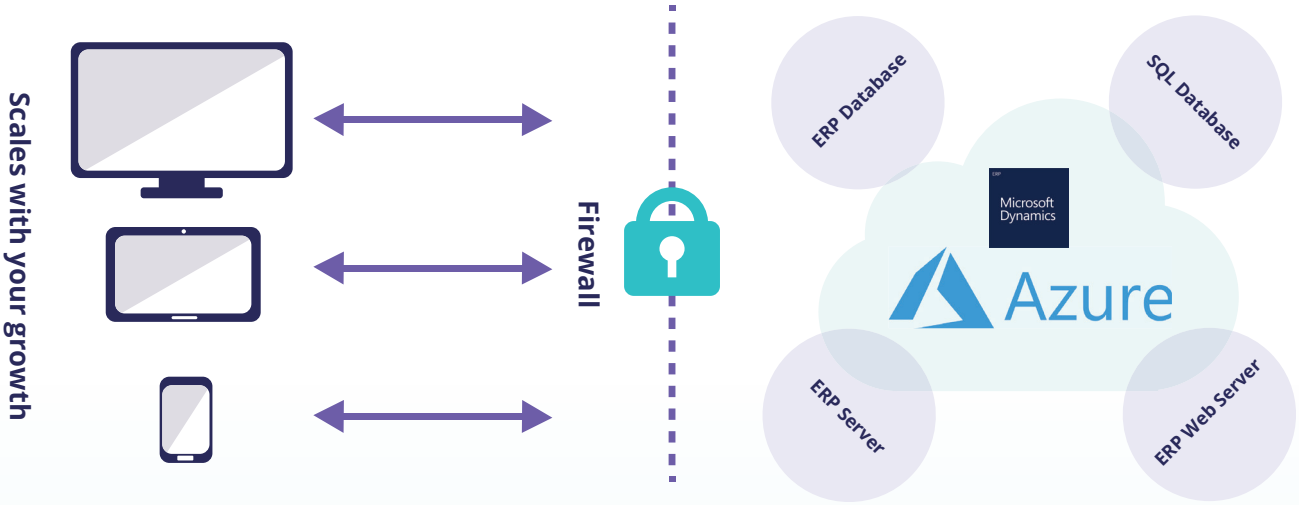
To ensure your applications high availability, you should deploy your application on an Availability Set with at least two VMs. Only multi-instance VMs qualify for the Service Level Agreement (SLA) provided by Azure.

Deploying ERP on Azure as a Managed Service

We've seen how the combination of Azure, Azure SQL Databases and Azure VM Services can benefit a Microsoft Dynamics ERP Cloud deployment. The configuration of these services can be a complex one with errors that could prove to be very costly. What does a Dynamics ERP solution on Azure look like?

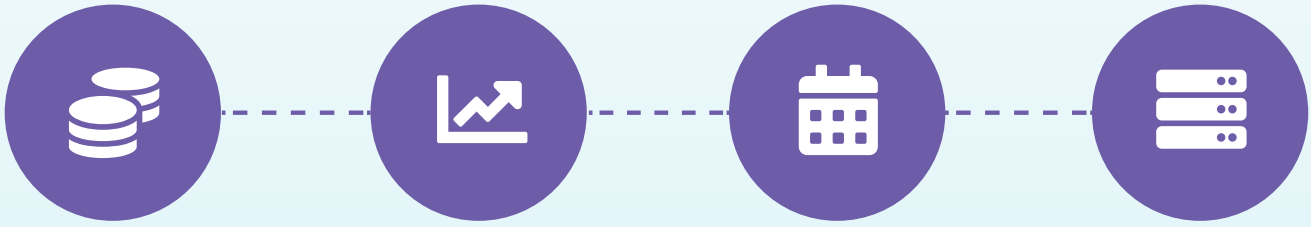
The End Goal – Scalable ERP Deployment on Azure

- A Microsoft Dynamics ERP on Azure deployment scales alongside your business.
- Your data is protected and safeguarded by Microsoft's data centre security.
- Your application layer is automatically backed up and upgraded when required.



… but why transition from an On-Premise Deployment?

There are many reasons why you might need to migrate or transition from a traditional on-premise solution to a Microsoft Dynamics ERP Implementation on Azure. Typically, an on-premise requires inhouse IT staff members to maintain, repair and support a local server infrastructure – this can be prohibitively difficult due to the complexity of an on-premise deployment.



Infrastructure Costs

Staffing Resource & Utilisation Costs

Backups & DR Planning

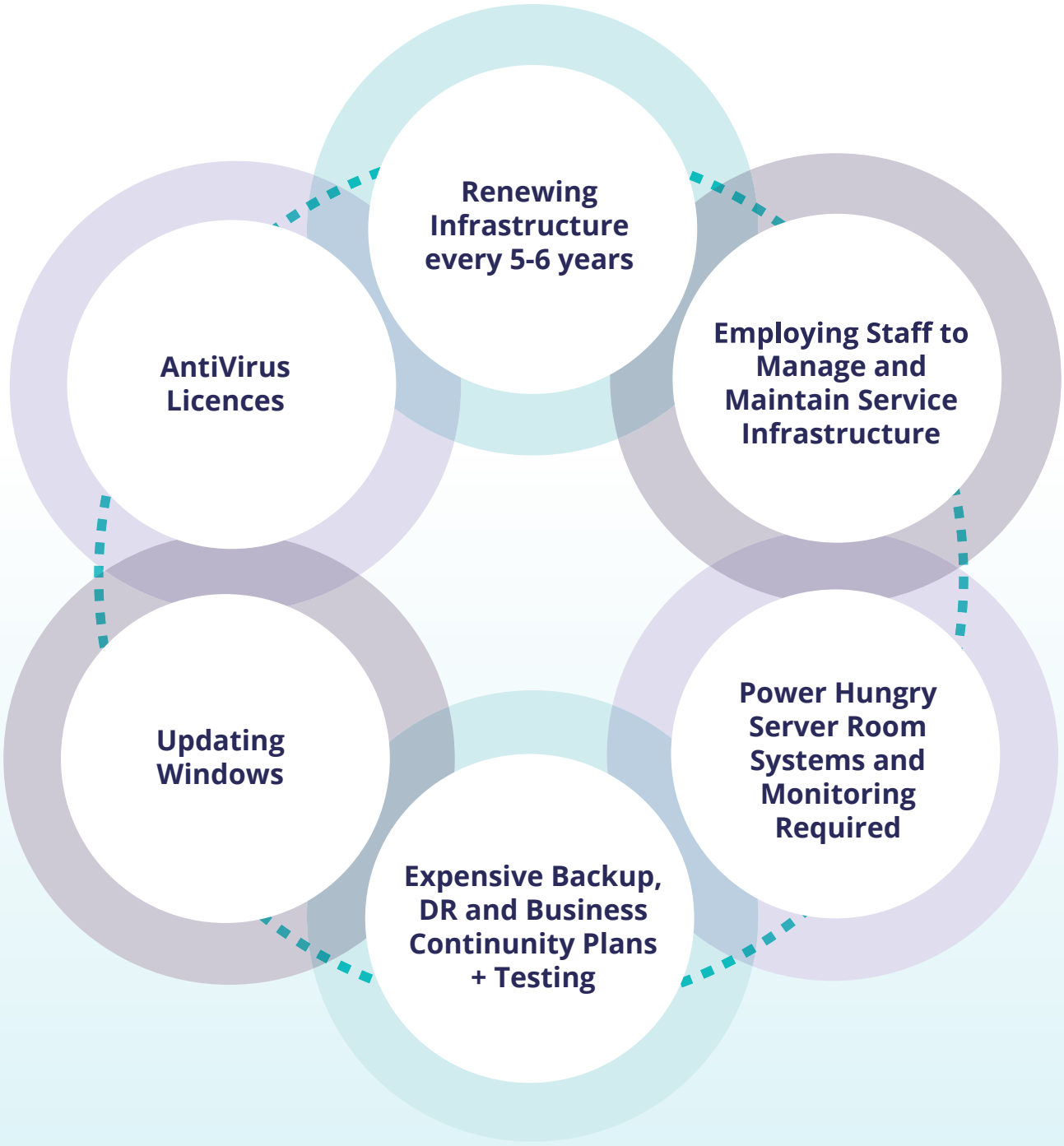
Software Updates License Renewals

HELLO@ADVANTAGE.CO.UK | 020 3004 4600

Key Drawbacks of an On-Premise Solution

As a customer with an on-premise solution, you are responsible for the data classification and accountability, client and end-point protection, identity and access management, application level control, network control, host infrastructure and physical security of your Microsoft Dynamics ERP deployment.

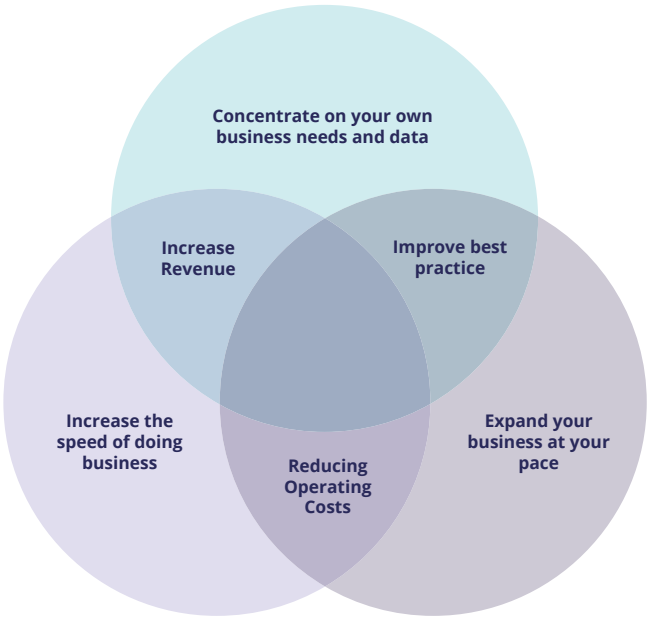
On-Premise Problems



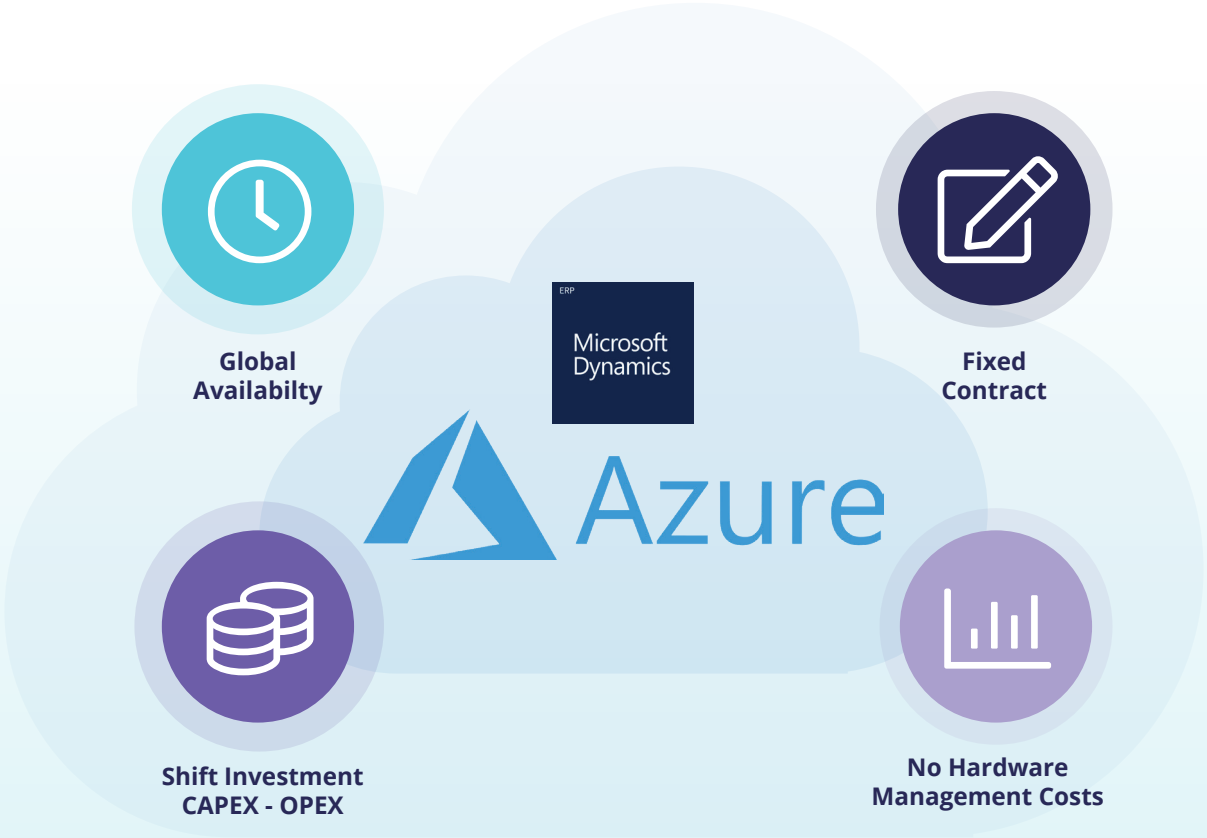
Problems Solved with Microsoft Dynamics ERP solutions on Azure

With Microsoft Dynamics NAV on Azure, managed as a service by an expert provider, such as Advantage the client need only manage their data classification and accountability.

- Concentrate on your own data
- Grow at your own pace
- Increase the speed of doing business
- Reduce Operating Costs



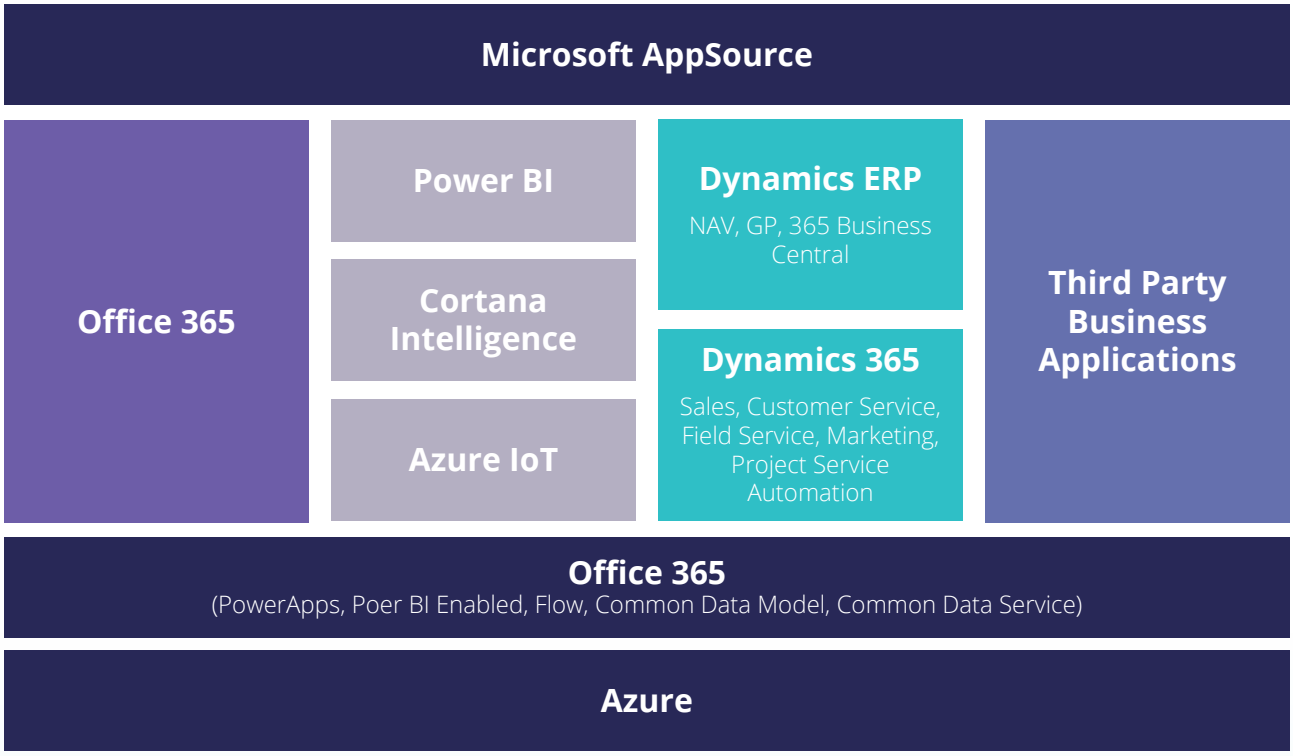
Core Benefits of Deploying Dynamics ERP on Azure



Integration with the Microsoft Office 365 Stack

A Microsoft Dynamics ERP deployment on Azure provides security and integration with the full Microsoft stack. This integration extends to the secure sign-on protocols such as MFA / ADFS SSO & Static IP.

Combined with conditional access and access log analytics built into Office 365 you will have a clear picture of who, when and where you users are accessing your system.



How is the Dynamics ERP solution on Azure Environment Secured

Operating a digital business in a constantly changing cyber threats environment is a serious matter. In the interest of protecting the business interests of our clients, Advantage have developed and implemented tailored cyber-security policies aligned to industry standards and best practices.

- Each ERP on Azure client should be configured with hosted security best practices.
- All open ports on the ERP Virtual Machine are secured with Static IP Addresses.
- Monitoring and Alerts should be configured on the hosted environment.
- Availability Groups should be configured for all Production Virtual Machines.

For more information

More information can be found on:
https://www.advantage.co.uk/cloud-services/microsoft-azure/dynamics-navgp-azure/

Or contact us on:

HELLO@ADVANTAGE.CO.UK | **020 3004 4600**

Advantage
transform the way you work