



EBOOK

Microsoft 365

A compelling, cloud-based collaboration solution
for your business.



Contents

Introduction	2
What is Microsoft 365?	2
Why Microsoft 365?	3
Microsoft Entra ID	4
Microsoft Intune	5
Microsoft Exchange Online	7
Microsoft SharePoint Online	8
Microsoft Purview Information Protection	9
Solution Design and Delivery	10
Migration Options	11
Identity and Access Review	13
Wavenet Support	14

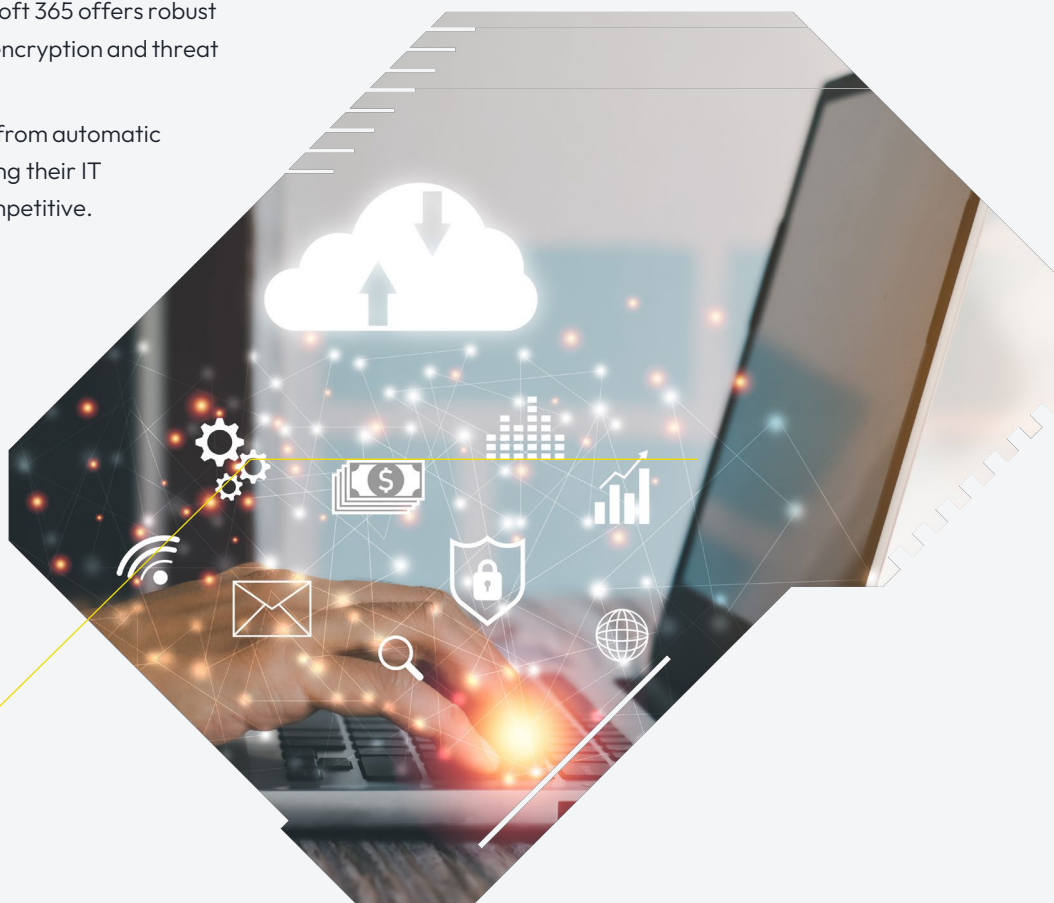
Introduction

What is Microsoft 365 ?

Microsoft 365, formerly recognised as Office 365, stands as one of the world's most widely used cloud-based solutions. Its popularity stems from seamless integration with the Microsoft Office suite, which is already in use by most businesses globally.

Whether you choose to adopt Microsoft 365 services to complement your existing infrastructure or to replace your current solution in its entirety, there are numerous benefits that your organisation can benefit from:

- **Cost-Efficiency:** Subscription-based pricing eliminates the need for upfront software purchases and costly hardware investments.
- **Reliable Uptime:** Microsoft's robust infrastructure ensures high availability, minimizing downtime and disruptions to business operations.
- **Anywhere, Anytime Access:** Microsoft 365 provides cloud-based access, allowing work from virtually anywhere with an internet connection.
- **Collaboration:** Microsoft 365 includes powerful collaboration tools like Teams, SharePoint, and OneDrive, promoting teamwork and productivity.
- **Security and Compliance:** Microsoft 365 offers robust security features, including data encryption and threat protection.
- **Regular Updates:** Clients benefit from automatic updates and new features, keeping their IT environment up-to-date and competitive.



Introduction continued

Why Microsoft 365 ?

The way organisations operate has changed. The way people work has changed. There is an increasing emphasis on cloud services. Security threats are similarly evolving to target cloud-based services as well as your on-premises networks.

Company boundaries are no longer defined by bricks and mortar, or the use of company-issued and company-controlled computers. Remote working and the use of employee-owned devices has become normal, and these use cases serve to highlight the limitations of a typical managed, on-premises IT solution. Often organisations don't even know that, despite their published security policies, employees are introducing serious risks of deliberate or accidental security breaches when taking their devices outside of a secure, managed corporate network.

Microsoft 365 is core to most organisations' IT services and the appropriate use of security tools within Microsoft is a key step to gaining and maintaining a secure environment regardless of where devices and data are located. The Microsoft 365 licensing stack options act as an extension of your existing IT infrastructure to support a modern workplace approach, or to act as the first steps towards a fully cloud-based infrastructure.

Wavenet's Secured Microsoft 365 solution provides you with the implementation of a recommended set of preventative security controls. We align the controls to the requirements of Cyber Essentials, a UK Government backed security scheme that addresses the most common Internet-based threats. We also tailor the controls based on our own experience and wider recommended good practice.

Key features and benefits

- Defend your business against advanced cyberthreats with sophisticated phishing and ransomware protection.
- Control access to sensitive information using encryption to help keep data from being accidentally shared.
- Secure devices that connect to your data and help keep iOS, Android, Windows, and MacOS devices safe and up to date.
- Get the latest features and capabilities with always up-to-date versions of Outlook, Word, Excel, PowerPoint, Teams.
- Edit and share documents, photos, and other files from anywhere on all your devices.
- Activate Microsoft 365 security controls to help guard against viruses, spam, unsafe attachments, suspicious links, and phishing attacks.
- Leverage Conditional Access policy to enforce Multi-Factor Authentication (MFA) and grant access to business resources based on additional factors such as user location and device compliance.
- Apply security policies to help protect business data on company-owned and employee devices.
- Keep company data within approved apps and easily remove business data from lost or stolen devices.

Microsoft Entra ID

Microsoft Entra ID is a cloud-based identity and access management service that enables your employees access to internal and external resources. It serves as a comprehensive platform for identity management, providing robust features to streamline user authentication, authorisation, and provisioning processes. With Entra ID, administrators gain granular control over user access permissions, ensuring that sensitive data remains protected while facilitating collaboration and productivity across teams.

Key features

- User and Group Management
- On-premises directory Synchronisation
- Basic Reports
- Self-Service Password Resets for Cloud Users
- Single Sign On across Azure, Microsoft 365, and many SaaS applications
- Hybrid user access both on-premises and cloud resources
- Advanced administration such as dynamic groups
- Self-service group management

Entra ID extends its capabilities beyond user identity management to include comprehensive device authentication and management solutions. Entra ID enables businesses to enforce security policies, manage device configurations, and monitor device health from a centralised dashboard. This unified approach to identity and device management enhances security posture, reduces administrative overhead, and ensures compliance with regulatory requirements.

In managing device registrations and joins with Entra ID, organisations have several options, each offering varying levels of management capabilities.

- **Mobile Application Management (MAM)** Is typically leveraged for Bring your Own Device situations to enable administrations to manage and secure mobile applications, control app distribution, protect data, and enforce compliance standards at the application level.
- **Entra ID Registration** is used to register devices providing users with support for bring your own device (BYOD) or mobile device scenarios.
- **Hybrid Entra ID Joined** is used for organisations who have an existing Active Directory implementation on-premises. Entra ID Connect is used in this instance to synchronise your on-premises AD with Entra ID.
- **Full Entra ID Joined** is typically used for organisations who are moving fully to the cloud and have no on-premises servers. This process requires more configuration as the user device needs to be freshly joined to Entra ID and removed from the existing AD environment.

Microsoft Intune

Protect and manage endpoints in one place

As organisations support hybrid and remote workforces, they are challenged with managing the different devices that access organisation resources. Employees and students need to collaborate, work from anywhere, and securely access and connect to these resources. Admins need to protect organisation data, manage end user access, and support users from wherever they work.



Microsoft Intune is a cloud-based endpoint management solution. It manages user access to organisational resources and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints.

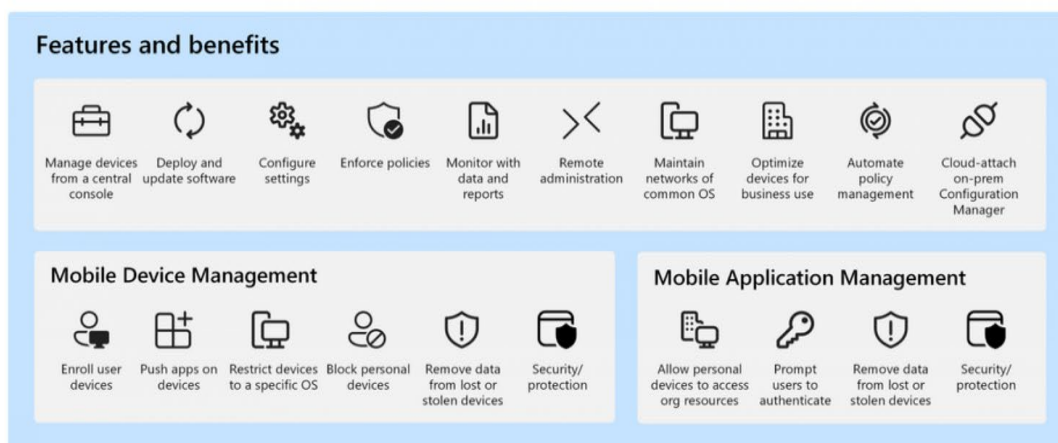
You can protect access and data on organisation-owned and user's personal devices and Intune has compliance and reporting features that support the Zero Trust security model.

Microsoft Intune

Wavenet will tailor the Intune policies specific to your organisations requirements.

Key features and benefits of Microsoft Intune

- Manage users and devices, including devices owned by your organisation and personally owned devices. Microsoft Intune supports Android, Android Open-Source Project (AOSP), iOS/iPadOS, Linux Ubuntu Desktop, macOS, and Windows client devices. With Intune, you can use these devices to securely access organisation resources with policies you create.
- Simplified app management with a built-in app experience, including app deployment, updates, and removal. You can connect to and distribute apps from your private app stores, enable Microsoft 365 apps, deploy Win32 apps, create app protection policies, and manage access to apps & their data.
- Automate policy deployment for apps, security, device configuration, compliance, conditional access, and more. When the policies are ready, you can deploy these policies to your user groups and device groups. To receive these policies, the devices only need internet access.
- Employees and students can use the self-service features in the Company Portal app to reset a PIN/password, install apps, join groups, and more. We can customise the Company Portal app to help reduce support calls.
- Intune integrates with mobile threat defence services, including Microsoft Defender for Endpoint and third-party partner services. With these services, the focus is on endpoint security, and you can create policies that respond to threats, do real-time risk analysis, and automate remediation.
- Use a web-based admin centre that focuses on endpoint management, including data-driven reporting. Admins can sign into the Intune admin centre from any device that has internet access.
- This admin centre uses Microsoft Graph REST APIs to programmatically access the Intune service. Every action in the admin centre is a Microsoft Graph call.
- The Microsoft Intune Suite offers advanced endpoint management and security. The suite has optional add-on features, including Remote Help, Endpoint Privilege Management, Microsoft Tunnel for MAM, and more.



Microsoft Exchange Online

Hosted email that's easy to use and easy to manage.

Exchange Online is designed for businesses that require a robust, cloud-based email solution. It provides essential features to facilitate seamless email management and collaboration within organisations.

You can access business email, calendar, and contacts on your PC, phone, and web browser with Exchange Online.

Key features

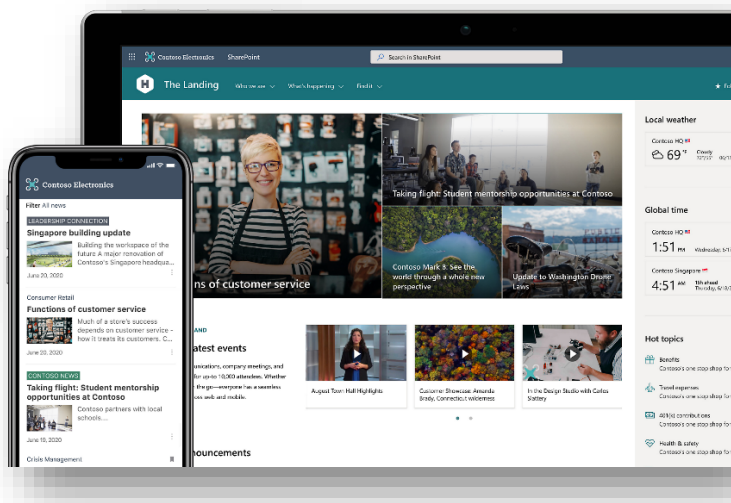
- Generous mailbox storage for each user.
- Send and receive email with a custom domain (e.g., user@yourcompany.com).
- Share calendars and schedule meetings with ease.
- Store and manage contact information.
- Access your email, calendar, and contacts from anywhere using the Outlook Web App (OWA).
- Access email, calendar, and contacts on the go using the Outlook mobile app or compatible email clients on iOS, Android, and Windows devices.
- Benefit from built-in anti-malware and anti-spam protection, as well as continuous data backup.
- Meet regulatory and legal requirements with features like archiving, retention policies, and eDiscovery search.



Microsoft SharePoint Online

Empower teamwork and find information quickly

Microsoft SharePoint is a web-based collaboration and document management platform developed by Microsoft. It is part of the Microsoft 365 suite and designed for businesses of all sizes to create, store, organise, and share information securely. SharePoint helps streamline workflow, improve communication, and enhance productivity within an organisation. Typically, your Microsoft 365 subscription will include 1TB of SharePoint online pooled storage for your organisation and then each subscribed user will add an additional 10GB storage to the pool.



Key features and benefits

- Create team sites, communication sites, or hubs for departments, projects, or other purposes to centralise information and resources.
- Store, organise, and manage documents with version control, metadata, and powerful search capabilities.
- Work together on documents in real-time, co-authoring with colleagues, and tracking changes.
- Organise, manage, and categorise information using lists and libraries, which support custom metadata, views, and filtering.
- Automate business processes and tasks using built-in workflows or create custom workflows with Power Automate.
- Seamlessly integrate with other Microsoft 365 applications, such as Word, Excel, PowerPoint, OneDrive for Business, and Microsoft Teams.
- Control access to sensitive information with granular permissions, while leveraging features like built-in encryption, and multi-factor authentication.
- Customise the look and feel of SharePoint sites and extend functionality with apps from the SharePoint Store or custom-built solutions.

Microsoft Purview Information Protection

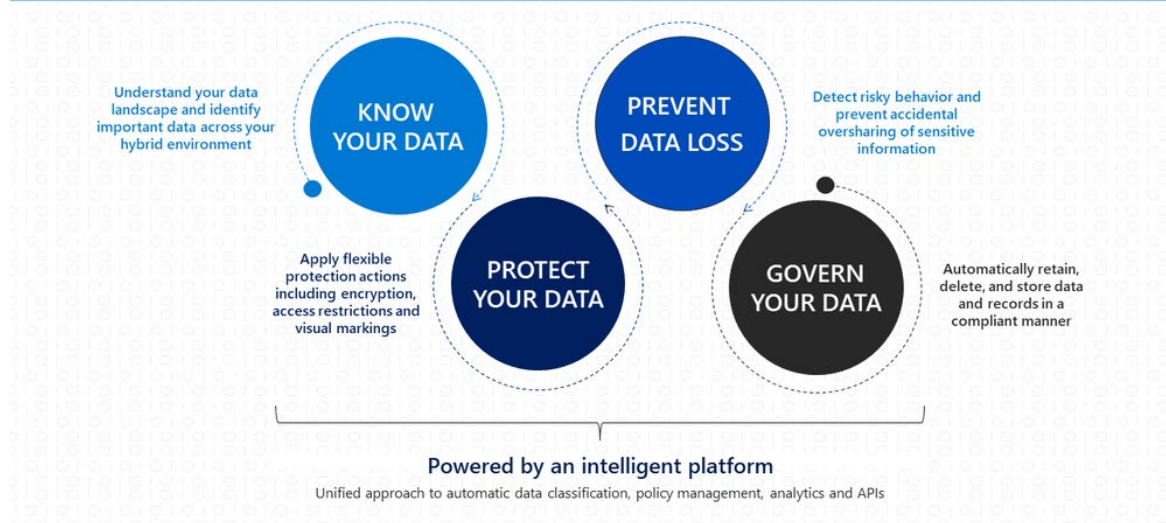
Microsoft Purview Information Protection is a feature of Microsoft Purview that provides automated classification and labelling of sensitive data assets based on the organisation's policies and compliance requirements. It helps organisations identify and protect sensitive data, such as personally identifiable information (PII), intellectual property, financial information, and confidential business information.

Key features and benefits

- Automates the classification of data based on the organisation's policies and compliance requirements, making it easier to identify and protect sensitive data.
- Enables users to apply labels to sensitive data assets, such as Confidential, Highly Confidential, or Restricted, helping users to manage data more effectively.
- Enables organisations to comply with regulations such as GDPR, CCPA, and HIPAA, helping organizations to avoid penalties and legal liabilities.
- Integrates with various Microsoft and third-party applications, enabling users to manage data across different platforms and environments.
- Collaboration between teams and stakeholders, enabling users to share and work with sensitive data assets across the organisation.
- Enables organisations to protect sensitive data from unauthorised access or misuse, ensuring that data is protected and secure.

Information Protection & Governance

Protect and govern data – **wherever** it lives



Solution Design and Delivery

Pre-contract

Identify requirements and high level gaps between the existing service provision and the desired secure configuration

Scope the software and services that are required

Provide a high level design and proposal to confirm the scope and cost of the required software and services

Implementation Discovery & Design

Wavenet will undertake a more detailed discovery and design exercise to identify the specific controls that will be implemented.

The detailed design will identify the responsibilities of Wavenet and the customer, high level impact on users, considerations for IT processes and policies, and roll-out.

Run any pilot stages and User Acceptance Testing

Solution Implementation

The implementation will proceed in accordance with the agreed design and delivery plan.

This may include phases or implementation and deployment to groups of pilot users prior to company wide roll-out.

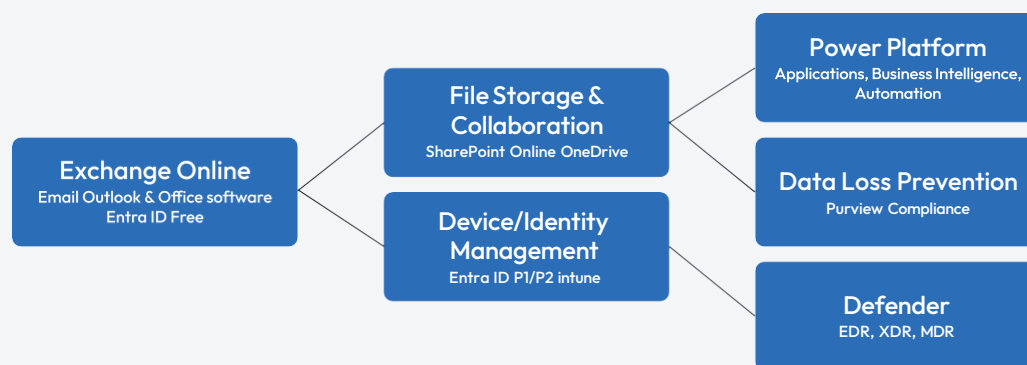
Support and Managed Service

Full handover into Support with the design documentation pack.

Migration Options

Microsoft 365 is an identity-based product. This identity (a user account residing in the Microsoft Entra ID identity and authentication service) will have varying levels of functionality depending on what licences are assigned to it. These licences vary from offering simple email functionality to desktop-based Microsoft Office software, to enterprise-grade security software.

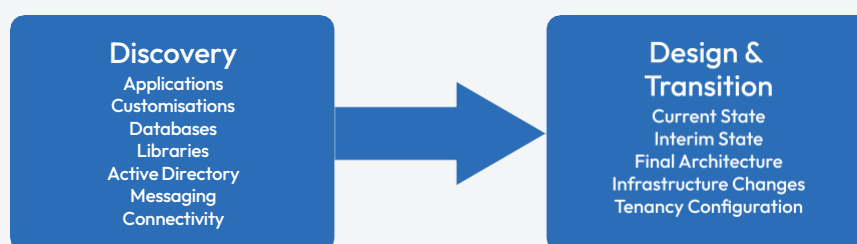
When considering a migration to Microsoft 365, a typical migration path may start with simple email functionality before progressing into more advanced file storage, device administration, collaboration, and security-focused offerings:



Migration Decision Factors

Once your organisation decides to migrate to Microsoft 365, Wavenet will conduct a discovery process whereby key business workloads, processes and requirements are analysed and discussed to determine the best route forward. The migration approach can typically follow one of two routes:

- **Full** migration of all data in one move, for example where all Exchange mailboxes or network shares are migrated to Microsoft 365. This method is suitable for organisations with Software as a Service (SaaS)-based workloads without on-premises requirements.
- **Hybrid** migration is suited to larger or more complex organisations where a diverse set of workloads is distributed across any combination of on-premises datacentres and/or multi-cloud.



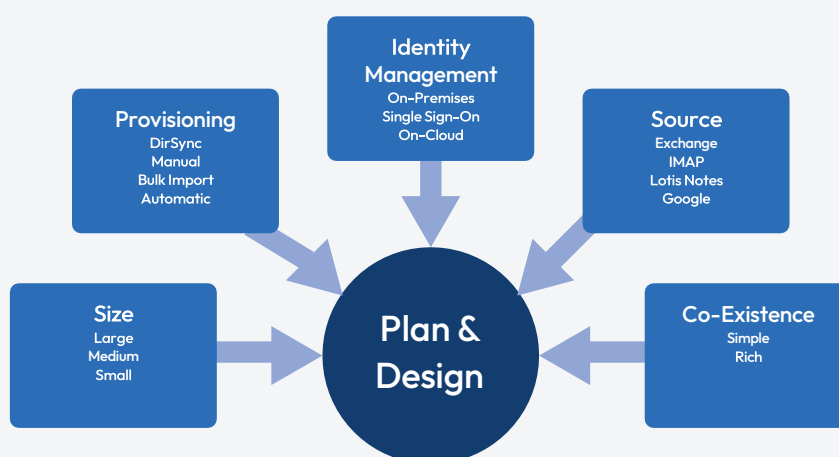
Migration Options

Common challenges to be considered

Microsoft 365 does present some differences and limitations when moving from on-premises to cloud, or from another cloud. However, our dedicated 365 Wavenet engineering team will explore and design ways to overcome them.

Not all workloads are cloud-friendly!

Not all of an organisation's applications and software will lend themselves to easy migration. It is possible that a like-for-like migration for a legacy system may not always exist.



Some systems lend themselves well to migration to Microsoft 365, while others are more complicated. For example:

- A linked Excel spreadsheets in SharePoint can create issues when migrated to Microsoft 365.
- Templates in legacy Microsoft applications may not work as expected in the migrated environment and might need to be updated and applied.
- Legacy applications may require older software versions than those provided as part of a Microsoft 365 subscription. These should be carefully considered and securely hosted elsewhere for security purposes.
- Some applications require dedicated server infrastructure and cannot be run from Microsoft 365. In these cases a hybridised approach may be desirable.

Your on-premises environment may require some additional housekeeping before it is migrated to Microsoft 365 to ensure the best results by preventing legacy data and redundant user profiles from being migrated unnecessarily.

Managing Costs

Each migration method will incur deployment costs depending on the complexity and size of the migration (data and users) and the expert time required to execute the deployment. Wavenet advise and help you with the development of a cost-effective migration plan.

It is also important to consider the long-term cost savings of migrating to Microsoft 365, when you will have reduced infrastructure costs, increased productivity and collaboration, and improved security of your company data.

Identity and Access Review

This pillar of the Wavenet Azure Professional Services offering focuses on businesses who are already utilising Microsoft's cloud-based identity provider, Entra ID, and want to evaluate their current Identity and Access architecture in the context of security and governance against Microsoft's best practices.

This service aims to help your business make the most of the Microsoft 365 & Entra ID licenses you are currently paying for, and to identify any potential requirements or gaps in functionality that would justify a licensing upgrade.

Assessment Details

Whilst the assessment may vary in scope and approach depending on the size of your business and number of workloads using Entra ID as an Identity Provider, Wavenet's methodology when performing the Identity and Access Review is as follows:

- Review of any existing user onboarding processes, including any potential for HR-based user provisioning
- Review of any existing user and group naming conventions
- Identification of security groups, group owners and existing access reviews (membership review)
- Review of all known instances where an Identity is required (for example Entra ID Enterprise Applications, VPNs) and identification of opportunities for identity centralisation for Single Sign On (SSO) via an appropriate federation mechanism
- Assessment of the application of the Principle of Least Privilege
- Assessment of the application of the Zero Trust Principle
- Assessment of Multi-Factor Authentication (MFA) and Conditional Access use and policies
- Evaluation of current Remote Access solutions
- Evaluation of current utilisation of licensed features from an Identity Perspective (depending on your current Microsoft Entra ID licencing tier), with recommendations for enhancement where applicable

Key Deliverables

After the assessment process is completed, Wavenet will generate a detailed document summarizing any findings and recommendations for enhancing your Identity and Access solution. This document will pinpoint any 'non-compliance' with Microsoft's best practices for Identity and Access and expand on the necessary steps and costs required to resolve these issues. Additionally, it will include an evaluation of your current utilisation of licensed Entra ID features, along with suggestions for licensing upgrades as appropriate.

Wavenet Support

Wavenet's UK service desk can provide managed IT support and maintenance for your Microsoft 365 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
P1	Critical – Outage across whole organisation, total loss of service (Site Down)
P2	High – Service is available but either reduced functionality or degradation is creating significant business impact
P3	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