Microsoft security

The value leader protecting small businesses.

By choosing the right Microsoft 365 tools, you can enable access from any device while ensuring centralised management and security of your users' desktops.

This allows you to evaluate which users and devices can access work data by selecting options to block users from logging in from home computers, unapproved apps or outside of work hours.

Enterprise-grade protection

Protect devices against ransomware and other cyberthreats with industry-leading Defender technologies, like endpoint detection and response and threat and vulnerability management.

Easy to use

Wizard-based onboarding quickly sets up your environment. Pre-configured policies and automated threat detection and response ensure continuous protection against the latest threats, allowing you to focus on what matters most.

Cost-effective

Security that works without compromising your budget. Available in two flexible plans: Microsoft 365 Business Premium or as a standalone solution.

Steps to security success with Microsoft 365

1. Secure Users
2. Secure Devices
3. Secure Data
4. Secure Beyond

Microsoft security

Pax8 is here to help you elevate your security expertise. Our new Microsoft Security Accelerator programme equips you with the tools to design, implement, sell and support your clients effectively.

Baseline	Better	Best
Microsoft 365 Business Premium (for up to 300 users)	**Microsoft 365 E3 + E5 Security add-on***	**Microsoft 365 E5**
Multi-Factor Authentication (MFA) Requires more than one method of authentication to verify the user's identity for a transaction or login.	**Privileged Identity Management*** A service that enables you to manage, control and monitor access within your organisation. This includes providing just-in-time privileged access to Entra ID and Azure resources, enforcing on-demand, time-bound access to resources, and requiring approval to activate privileged roles.	**Defender for Identity** A suite fully integrated with Microsoft Defender XDR, it leverages signals from both on-premises Active Directory and cloud identities to enhance your ability to identify, detect and investigate advanced threats directed at your organisation.
Conditional Access Policies Control access based on specific conditions to ensure only authorised users and devices can access critical resources.	**Access Reviews*** A feature that enables organisations to efficiently manage group memberships and role assignments. It ensures that the right individuals have appropriate access to resources, reducing the risk of excessive or unnecessary permissions that could lead to security vulnerabilities.	**Defender for Cloud Apps** Microsoft Defender for Cloud Apps delivers full protection for SaaS applications, helping you monitor and protect your cloud app data across the following feature areas: Cloud Access Security Broker (CASB), SaaS Security Posture Management (SSPM), Advanced Threat Detection and app-to-app protection.
Manages Sensitivity Labels Classifies, labels and protects documents and emails based on the content.	**Defender for Endpoint** Monitors and protects individual endpoint devices, quickly reacts to suspicious behavior, recovers from security incidents and proactively searches for sophisticated cyberthreats.	**Defender for O365 + Endpoint (Plan 2)** Microsoft Defender for Office 365 has a seamless integration with Microsoft 365 subscriptions that protects against threats in email, links (URLS), file attachments and collaboration tools.
Microsoft Defender for Business Provides next-generation protection, endpoint detection and response and threat and vulnerability management for devices.	**Automated Detection and Response** A suite of capabilities designed to safeguard your endpoints, complemented by intelligent automated investigation and response features that enable IT administrators to focus solely on critical security events.	**Defender for IoT** Delivers real-time asset discovery, vulnerability management and cyberthreat protection for IoT and industrial infrastructure. It includes both enterprise IoT and operational technology (OT) devices.