NUMATA®

Microsoft 365

Secure your SME for AI adoption

A practical guide to Microsoft 365 Business Premium & Copilot.

A Numata business IT guide for SME decision-makers

info@numata.co. | **numata.co**

SMBs face new security challenges in the age of AI

All too many SMBs are still operating with significant security gaps that increase the risk of cyberattacks, create compliance challenges and become even more problematic as businesses adopt artificial intelligence (AI) tools that can access and analyse large volumes of their sensitive information. The numbers are sobering:

- Nearly half of all cyberattacks now target small businesses, yet only a fraction feel prepared to defend themselves.
- Up to 60% of SMBs hit by a major breach close within six months.
- Phishing remains the #1 attack vector, and ransomware incidents can cost smaller firms upwards of $250,000 per event.

Regulations like POPIA and GDPR require businesses of all sizes to demonstrate responsible data handling. The gap between what is expected and what is in place is often significant, especially for organisations running on basic Microsoft 365 plans without structured security controls. Doing nothing is the riskiest option.

But the good news is that solutions tailored for SMB budgets and technology environments exist and they are simpler and more accessible than most SMBs realise. Microsoft 365 Business Premium provides a practical, cost-effective way to strengthen security, close common gaps and create the foundation needed for safe AI adoption.

This guide discusses how to use Microsoft 365 Business Premium to establish a strong security baseline, reduce cyber risk and prepare your organisation for Microsoft 365 Copilot and the next generation of AI-powered productivity.

Common SMB security gaps

The average SME has numerous gaps in its cyber defences. Some of the common vulnerabilities include:

- **No multi-factor authentication (MFA):** A compromised password allows attackers full access to email, files, financials and other sensitive data.
- **No device management:** Personal phones and unencrypted laptops are able to access company data with no oversight.
- **Lack of disk encryption:** A thief can access any information on a lost or stolen notebook because the data is not encrypted.
- **Consumer-grade antivirus:** Basic antimalware software is not up to addressing today's most sophisticated ransomware and virus attacks.
- **Basic email security only:** A lack of authentication protocols, anti-phishing policies and external sender warnings makes the business more vulnerable to phishing attacks.
- **Manual updates:** Patches and updates to address the latest security vulnerabilities in applications and operating systems are applied ad hoc, if at all.
- **No Data Leak Protection (DLP) or sensitivity labels:** There are no special controls on how sensitive data is stored, managed and shared.
- **Absence of Conditional Access policies:** Anyone can log in from anywhere and from any device.

These gaps add up to poor compliance with most of the recommended security controls set out in industry standards such as CIS. In addition to exposing your business to a higher risk of data breaches and infrastructure attacks, poor alignment with security best practices may lead to higher cyber insurance premiums. It also exposes your business to new security risks as you accelerate AI adoption.

Microsoft 365 Business Premium: A foundation for a secure business

One of the most straightforward and cost-effective ways to close these security gaps is to adopt Microsoft 365 Business Premium as the security foundation for your business. Microsoft 365 Business Premium combines the familiar Office 365 apps your team already knows with enterprise-grade security features in a single subscription.

CAPABILITY	WHAT IT DOES FOR YOU
Identity & Access (Entra ID P1)	Enforces MFA and conditional access, blocking over 99% of credential-based attacks. Only verified users on trusted devices get in.
Device Management (Microsoft Intune)	Manages and secures all devices (Windows, Mac, iOS, Android). Enforces encryption, patching, and compliance policies, even on personal devices.
Threat Protection (Defender for Business)	Enterprise-grade endpoint detection and response (EDR). Automatically detects, isolates and remediates malware and ransomware.
Email Security (Defender for Office 365)	Protects against phishing, spoofing, and malicious attachments with Safe Links, Safe Attachments and AI-driven anti-phishing.
Data Protection (Purview)	Data Loss Prevention (DLP), sensitivity labels, encryption and retention policies to control how sensitive information is shared and stored.

You no longer need to stitch together multiple standalone tools, each with its own cost, console and complexity, to protect your business. Business Premium gives you a unified platform that is easier to manage and more effective to operate. It is the same security technology used by large enterprises, packaged for smaller businesses with up to 300 users.

The baseline advantage

One of the most powerful and underused features in Business Premium is Microsoft Intune's security baselines. Instead of manually adjusting hundreds of settings or hoping defaults are good enough, you apply a Microsoft-recommended template that automatically enforces best-practice controls across every managed device.

What baselines do:

- Enforce disk encryption (BitLocker), firewall rules patching and exploit protection across all Windows devices.
- Require up-to-date antivirus, automatic patching and strong password policies.
- Restrict local admin privileges and disable insecure legacy protocols.
- Continuously monitor compliance and flag (or auto-remediate) devices that fall out of line.

How this helps your business:

- No guesswork: You do not need a security specialist to know what to configure. Microsoft's experts have done that for you.
- Consistency: Every device under management gets the same protections.
- Compliance confidence: Baselines are aligned to industry standards (CIS, NIST) and give you documented evidence of security controls for auditors, clients and cyber insurers.
- Reduced incidents: Companies that implement strong baselines see significant drops in malware infections and support costs.

Secure today, AI-ready tomorrow

Business Premium is not just about protecting your business today. It is the foundation that makes adoption of AI tools like Microsoft 365 Copilot safe, practical and worthwhile.

Microsoft 365 Copilot works by accessing and analysing information across your Microsoft 365 environment to deliver AI-powered insights and automation. This means Copilot will interact with your most sensitive data, including emails, documents, chats and calendars. Without proper governance and controls, adopting AI amplifies existing risks and introduces new threats.

How Business Premium makes you AI-ready:

- MFA + Conditional Access ensures only verified users on compliant devices can trigger AI interactions.
- Intune baselines guarantee that every endpoint is hardened and monitored before AI tools access data from it.
- DLP and sensitivity labels set boundaries that Copilot respects. It will not surface what it should not.
- A stable, incident-free environment means your team can focus on innovation rather than fighting fires.

The roadmap to a secure business

It can take as little as two months to transform your SMB into a secure, AI-ready business with Microsoft 365 Business Premium. This is what the roadmap might look like:

Week	What was done
Week 1–2	Email security hardened. DKIM, DMARC, anti-phishing policies, external sender warnings enabled.
Week 3–4	MFA enforced for all users. Conditional Access policies deployed, blocking sign-ins from unmanaged devices and untrusted locations.
Week 5–6	All company devices enrolled in Microsoft Intune. Security baselines applied, enforcing BitLocker encryption, firewall rules, automatic patching and compliance checks.
Week 7–8	Defender for Business deployed across all endpoints. DLP policies and sensitivity labels applied to protect financial and client data.
Data Protection (Purview)	Data Loss Prevention (DLP), sensitivity labels, encryption and retention policies to control how sensitive information is shared and stored.

Your next step: A free Microsoft 365 security assessment

Contact us for a complimentary Microsoft 365 Security Assessment, a no-obligation review of your current environment against Microsoft's recommended best practices.

What you will get:

- A clear view of your current security status
- Identification of critical gaps (MFA, device management, data protection, email security)
- A prioritised, practical roadmap to strengthen your environment
- Guidance on how Business Premium can address your risks

About Numata

Numata is a Business Technology Strategist for SMEs, helping organisations align technology to business outcomes. As a Microsoft Partner, we specialise in Microsoft 365 security, modern work enablement, and managed IT services — providing the strategic guidance and hands-on support that SMBs need to operate securely and grow confidently. We don't just deploy technology — we help you understand it, use it effectively, and get real value from it.

Ready to get started?

Contact us to schedule your free Microsoft 365 Security Assessment.

Statistics and industry data referenced throughout this guide are sourced from publicly available research and are intended as general guidance only.