PARTNER BROCHURE

The critical role of security features in AI scenarios

Secure creativity and collaboration for the hybrid workforce with Microsoft 365 Business Premium

Securing AI productivity

AI is transforming productivity, decision-making, and user engagement, but it also introduces new challenges. From data leakage to identity spoofing, AI scenarios demand enterprise-grade security at every layer.

With 75% of employees using AI, businesses face increasing cyber risk, and for those navigating their AI transformation journey with a hybrid or remote workforce, security is a priority.*

Microsoft Security solutions address this new AI reality by working together to safeguard users' data and interactions in Microsoft 365 Copilot and other AI applications, helping businesses:

- **Identify potential AI risks**, like sensitive data leaks and unauthorised access to high-risk applications.
- **Secure AI applications** and the sensitive data they process or generate, including prompts and responses.
- **Govern AI use** responsibly by retaining and logging interactions, detecting policy violations, and investigating incidents.

*Microsoft & LinkedIn, 2024 Work Trend Index Annual Report, 2024.

Microsoft 365 Business Premium with Microsoft 365 Copilot

Purpose-built for small and medium businesses (SMBs), Microsoft 365 Business Premium offers secure remote access, protection against data loss, and defence against cyberthreats with five powerful products all included in one subscription.

Customers benefits from all the Business Basic/Standard core features, plus:

- MFA with conditional access based on identity, device, location, and network.
- eDiscovery case management and legal hold for Copilot prompts and interactions.
- Manual sensitivity and retention labels for content processed by Copilot in files and emails.
- Data loss prevention (DLP) policies to help protect sensitive data from Copilot in files and emails.

Microsoft 365 Business Premium security features

1. Identity and access management with Microsoft Entra ID

A comprehensive Identity and Access Management (IAM) solution across hybrid and cloud environments that reduces AI risk, ensuring employees can securely access business applications from anywhere.

2. Device management with Microsoft Intune

A cloud-based endpoint management solution with built-in endpoint security, mobile app management, and endpoint analytics for better hybrid work experiences and lower TCO (Total Cost of Ownership).

3. Ransomware and device protection with Microsoft Defender for Business

Proactive, AI-powered device protection that goes beyond traditional antivirus with vulnerability management and enterprise-grade protection to block new and emerging threats.

4.Phishing protection with Microsoft Defender for Office 365

Includes enhanced spoof intelligence for better detection and mitigation of sophisticated spoofing attacks across email and collaboration tools.

5. Data security with Microsoft Purview

Reduces risk and complexity with unified data security, governance, and compliance solutions that dynamically secure data throughout its lifecycle, wherever it lives.

Office 2016 and 2019 EOS

With Office 2016 and 2019 reaching end of support on October 14th 2025, this is an ideal time to guide customers toward modern, secure, and AI-powered productivity solutions like Microsoft 365 Business Premium.

Discover more opportunities with Arrow partnership

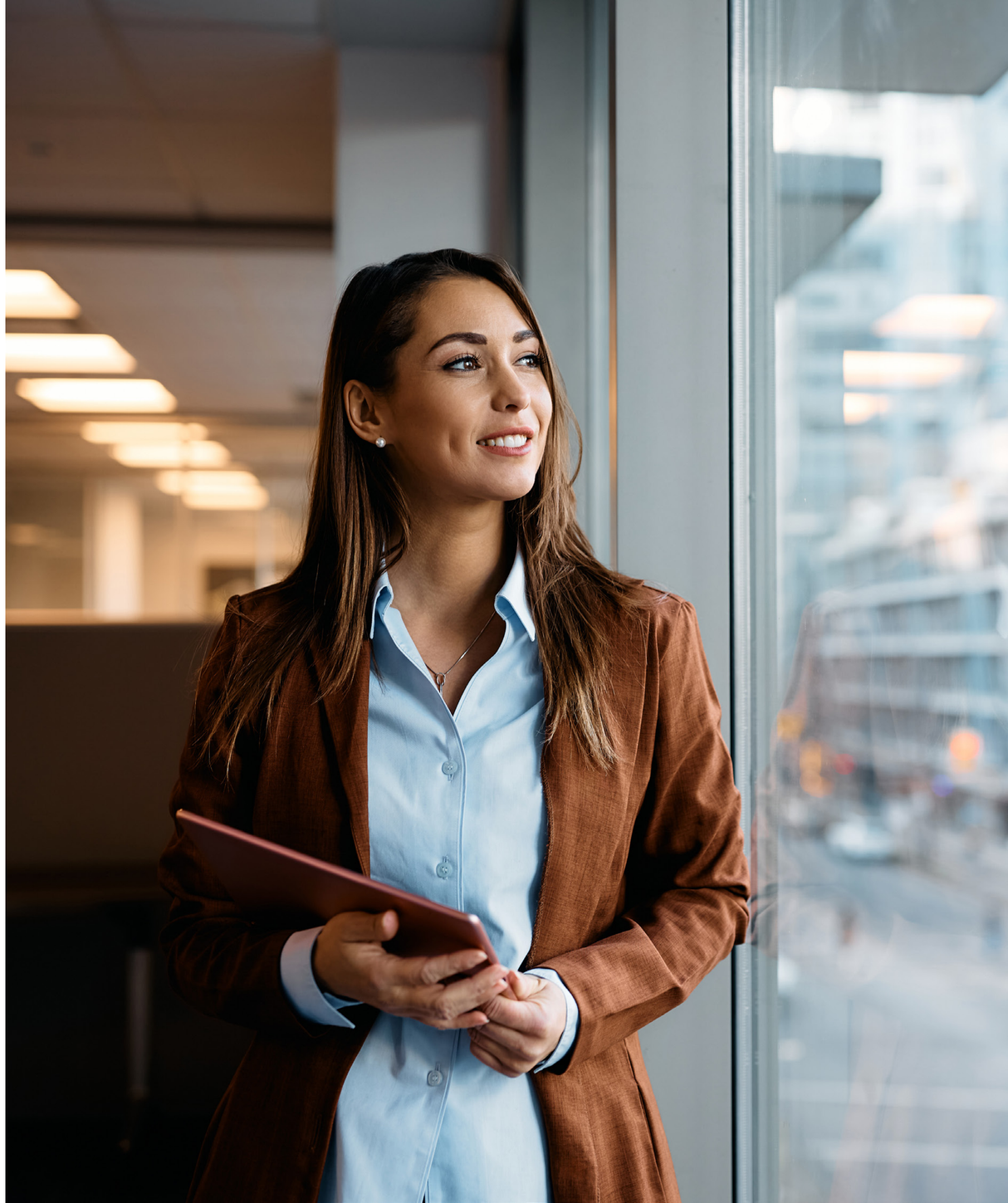
Let us help you support your customers' AI journey by securing their environments with the Microsoft Security portfolio.

Take advantage of our strong relationship with Microsoft, our proven expertise and full-service offering to access everything you need in one place to build and grow a successful secure business in the era of AI.

Get in touch with your local Arrow representative to learn more.

Explore Copilot Specialisation

Discover Arrow's Cloud backup managed service



The critical role of security features in AI scenarios