Securing AI in the enterprise: the Microsoft tools to help

AI is transforming productivity and decision-making; but it also introduces new risks. Sensitive data can leak through prompts, malicious actors can exploit vulnerabilities like prompt injection, and compliance obligations demand strict governance.

Key concerns for leaders include:

- **Data privacy:** 80% of business leaders cite data leakage via AI as **a top concern.**
- **Compliance:** Emerging global AI regulations require robust controls.
- **Security posture:** AI expands the attack surface, creating new identity and access risks.

But, with a strong security baseline and effective tools, you can utilise AI without exposing your business to dangers.

Integrated approach

Together, these tools implement Zero Trust for AI:

- **Discover AI usage and sensitive data (Purview, Defender).**
- **Protect identities and access (Entra).**
- **Govern compliance (Compliance Manager).**
- **Monitor and improve AI safety (Azure AI Studio, Copilot safeguards).**

Microsoft tools for securing AI usage

1. Microsoft Copilot

Prevent data exposure through AI-generated content, with an AI tool build for enterprise security.

- Enforces existing Microsoft 365 security and compliance controls (DLP, sensitivity labels, encryption).
- Built-in responsible AI safeguards to reduce harmful or biased responses.
- Admin controls for safe deployment and usage policies.

2. Microsoft Purview

Eliminate the risk of sensitive data leakage in prompts and improve auditability.

- Data Loss Prevention (DLP) prevents sensitive info from being shared with AI.
- Audit & eDiscovery captures AI interactions for compliance investigations.
- Insider Risk Management flags risky Copilot usage.

3. Microsoft Entra

Prevent unauthorised access to AI services and identity misuse.

- Agent ID manages non-human identities for AI agents.
- Conditional Access applies risk-based policies for AI apps and Copilot.

4. Microsoft Defender

Reduce the risk of prompt injection attacks and shadow AI.

- Defender for Cloud Apps discovers and blocks unauthorised AI tools.
- Detects malicious AI activity and vulnerabilities in AI components.

5. Azure AI Studio & Responsible AI Toolbox

Limit harmful, biased or unreliable AI outputs.

- Content Safety filters harmful or unsafe responses.
- Responsible AI dashboard monitors fairness, reliability and explainability.

6. Compliance Manager & Priva

Minimise the threat of regulatory non-compliance and privacy breaches.

- Maps AI usage to frameworks like GDPR, EU AI Act and ISO standards.
- Automates privacy impact assessments for AI workflows.

Ready to move forward with AI, securely and confidently? Book a call and discover how our experts can help you implement Microsoft tools to safeguard your business.

Get in touch