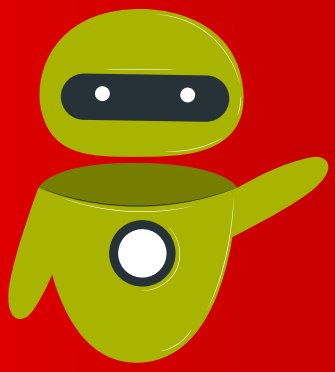
You **can't** fight **AI-powered threats** without **AI-powered defence**

The top 3 reasons AI is now essential for your cybersecurity

vodacom business

Why AI has become a **must** for security teams

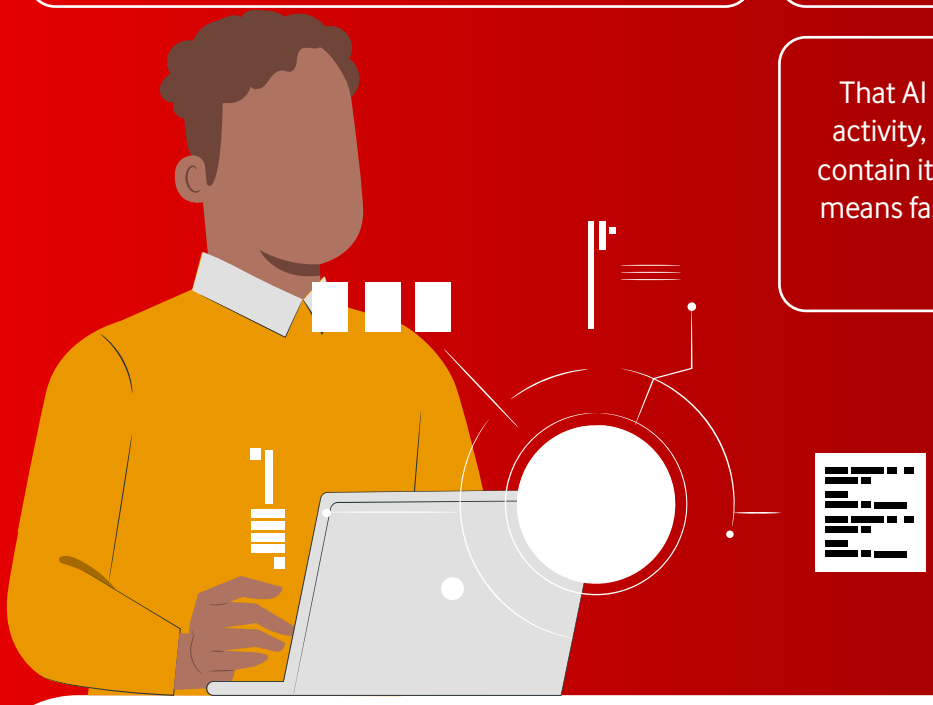
Attackers are already using AI to craft smarter, faster, and more convincing threats. That shift puts pressure on defenders. If your team isn't using AI too, it's easier to fall behind.



This guide outlines three clear reasons why AI is no longer optional. It explains how Microsoft's tools help teams detect threats earlier, cut down on manual work, and stay focused where it matters most.

1 AI gives you **enterprise-grade** detection power

Without AI	With AI
Security teams rely on manual monitoring and predefined rules to catch threats. But attackers move quickly, and the sheer volume of activity across networks, endpoints, and identities makes it nearly impossible to detect every anomaly in time.	Microsoft Defender helps security teams detect threats earlier by using AI trained on over 84 trillion signals daily across Microsoft's global ecosystem, giving it the context to identify emerging threats quickly.



That AI powers Defender's ability to spot unusual activity, like a file suddenly encrypting others, and contain it automatically. For lean security teams, this means faster detection, quicker response, and fewer missed threats.

2 **AI** helps you **act faster without more analysts**

Without AI	With AI
Every alert demands context. Analysts must review logs, investigate relationships, and document their findings. That takes time, and when alert queues grow, delays and missed incidents become more likely.	Security Copilot pulls in Microsoft's global threat intelligence and uses large language models to summarise incidents and suggest next steps. It can explain what happened, why it matters, and what to do next. So, instead of spending an hour on analysis and write-ups, teams get fast, high-quality insight that frees them up to act.

3 **AI cuts through the noise** so you can focus on what matters

Without AI	With AI
User-reported phishing emails pile up. Reviewing every message waste time and slows down response to actual threats.	The Phishing Triage Agent is part of Security Copilot and runs directly within Microsoft Defender. It uses AI to review emails reported by users, assessing tone, intent, and context to determine whether a message is a threat. The agent classifies each email, explains its reasoning in clear language, and flags high-risk cases for follow-up.

In 2024, Microsoft blocked over 30 billion phishing emails. With that volume, AI-powered triage is essential for helping security teams stay focused and effective.

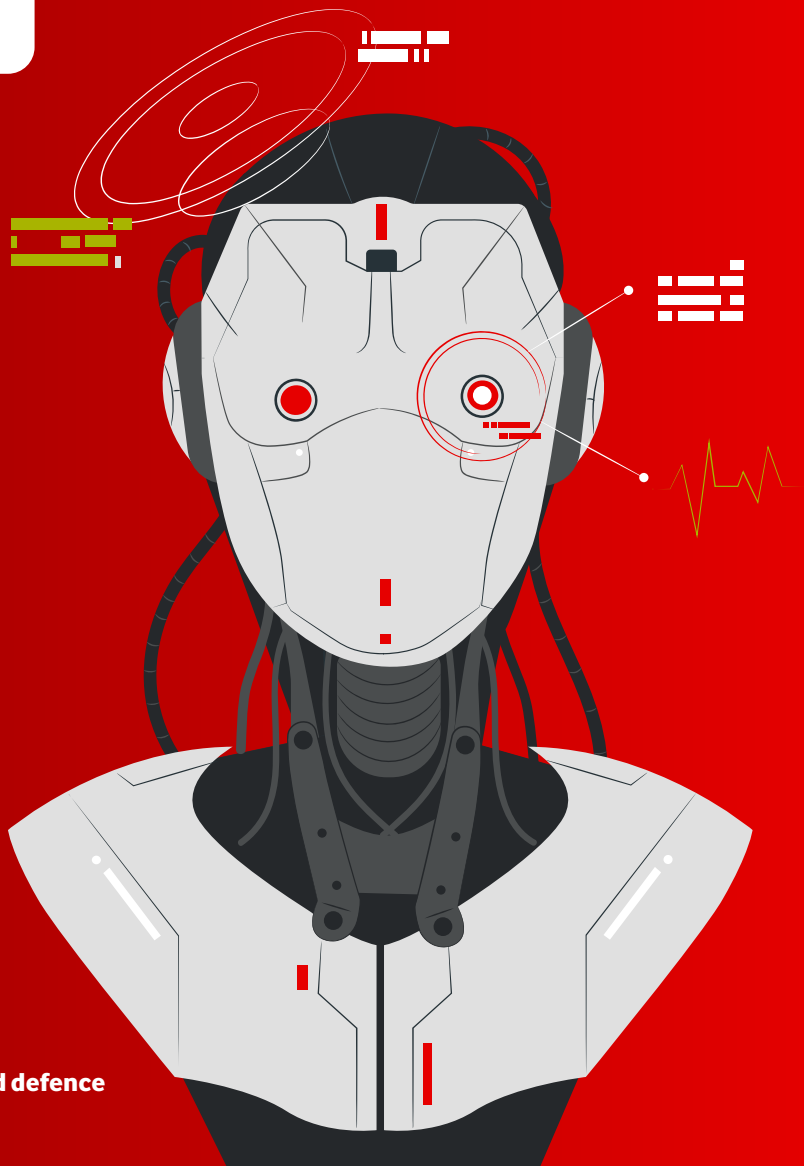
What to do next

AI is already changing the way security teams work. It reduces the time spent on low-value tasks, improves incident detection and response, and brings enterprise-grade protection to organisations of any size.

Start by identifying where your team spends the most time or struggles to keep up. Then explore how Microsoft Defender, Security Copilot, and Microsoft 365 Copilot can help close those gaps.

But using AI well is only part of the job. You also need to be aware of how cybercriminals are using AI to create faster, more convincing attacks. Our companion guide breaks down the offensive side of AI, and why awareness is just as important as defence.

Read it here.



vodacom
business