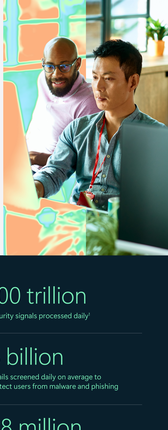
Microsoft Security

MICROSOFT DIGITAL DEFENCE REPORT 2025

AI's double-edged influence: Defending and disrupting the digital landscape

We are living through a defining moment in cybersecurity, where threats no longer affect business but also society. The *2025 Microsoft Digital Defence Report* highlights how AI has become a double-edged influence, empowering both defenders and threat actors. The report recommends a new approach grounded in Zero Trust, AI-powered intelligence and collaboration.



Our unique vantage point

With billions of users, millions of organisations and a vast network of partners, we have a comprehensive perspective on today's dynamic cybersecurity threat landscape.

100 trillion
security signals processed daily[1]

5 billion
emails screened daily on average to protect users from malware and phishing

38 million
identity risk detections analysed in an average day

Threat actors are upending the cyber risk paradigm

Cyber criminals are moving faster than ever, blending human manipulation with technical precision to outpace traditional defences. Opportunistic threat actors often target known security gaps and vulnerable sectors, such as government, information technology and critical manufacturing, which may run on legacy systems and have limited response capabilities.

Countries where customers are most frequently impacted by cyber threats (January–June 2025)

Source: Microsoft Threat Intelligence

Threats are evolving in scale, speed and sophistication

Scale

90%

of 15.9 billion account creation attempts monitored were bot-driven.

Speed

54%

click-through rate for AI-automated phishing emails – a 4.5× increase compared to 12% for standard attempts.

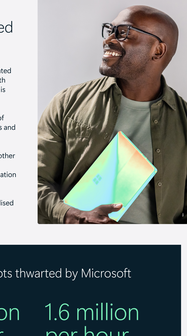
Sophistication

82%

of ransomware incidents now involve large-scale data theft.

AI gives – and AI takes away

AI-driven defences help security teams automatically remediate threats from traditional vectors. But the same technology also exposes vulnerabilities, expanding your organisation's attack surface with methods like prompt injection, data poisoning, malicious tool invocation and credential abuse.



AI makes identity attacks easier

As organisations improve their hardening against traditional cybersecurity threats, threat actors increasingly turn to AI-enabled social engineering, spurred by generative AI, to gain initial access. Download our Five Generative AI Security Threats You Must Know About guide to learn more.

32%
increase in identity-based attacks in the first half of 2025.

87%
increase in campaigns disrupting Azure cloud customer environments through actions like ransomware or mass deletion.

35%
increase in ransomware attacks involving both on-prem and cloud components from 2023.

Four enterprise AI usage security principles

Organisations must develop adaptive approaches to managing emerging AI risks effectively. Explore our incident response resources for the latest defence strategies.

Prepare
Establish policies, training and secure foundations, including your cloud infrastructure and identity perimeter.

Design for resilience through Zero Trust, which operates on the principle of always assume breach and is embedded across Microsoft environments.

Discover
Gain visibility into all AI usage by monitoring AI applications, agents and data movement and uncovering shadow AI.

Protect
Safeguard sensitive data and AI apps and agents to prevent data leakage and prompt injection attacks.

Govern
Enforce AI policies and oversight. Audit AI interactions and ensure compliance with evolving regulations.

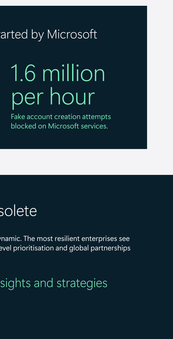
Harnessing AI-powered defence

As adversaries use AI to achieve unprecedented speed and scale, defenders must counter with AI-driven automation. Here's how Microsoft is using AI to protect customers:

AI-driven identity systems analyse billions of sign-ins and user signals to detect anomalies and block attacks in seconds.

Guardian Agents – AI systems that protect other AI systems – provide real-time visibility into model behaviour, prevent malicious manipulation and surface hidden threats.

Microsoft's Digital Crimes Unit uses specialised AI tools to track, investigate and disrupt cybercriminal networks worldwide.



Fraud and fake bots thwarted by Microsoft

USD 4 billion in one year
Value of fraud schemes blocked by Microsoft from Apr 2024–Apr 2025.

1.6 million per hour
Fake account creation attempts blocked on Microsoft services.

Yesterday's playbook is obsolete

For modern security leaders, the future of defence is dynamic. The most resilient enterprises see cybersecurity as constantly evolving, requiring board-level prioritisation and global partnerships with peers and even competitors.

Stay ahead with the latest data, insights and strategies shaping cybersecurity.

Download the *Microsoft Digital Defence Report 2025*.

[1] Unless otherwise stated, all data cited are from Microsoft Detection and Response Team (DART) data collected between July 1, 2024 and June 30, 2025