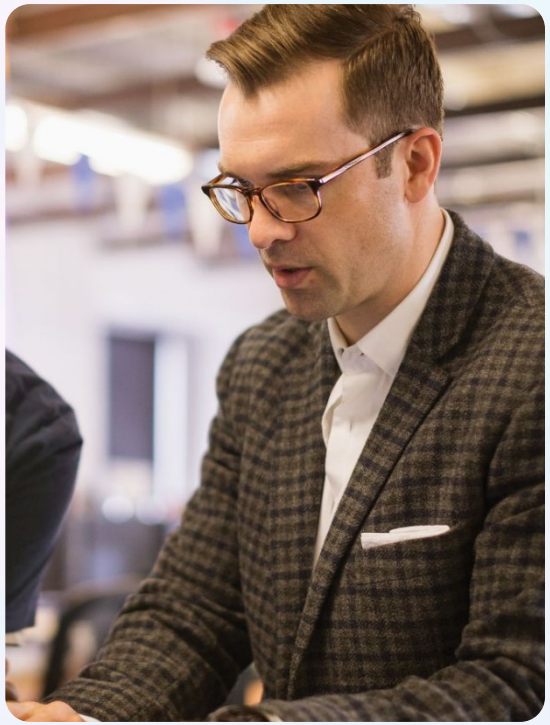
Microsoft Security

Microsoft Security

Marc Carney
Director, Security Solutions Group
Microsoft UK

17th June 2025

Driving AI skilling across the UK



2!n jmjpo!tl jmfe!cz!ui f !f oe!pg3136

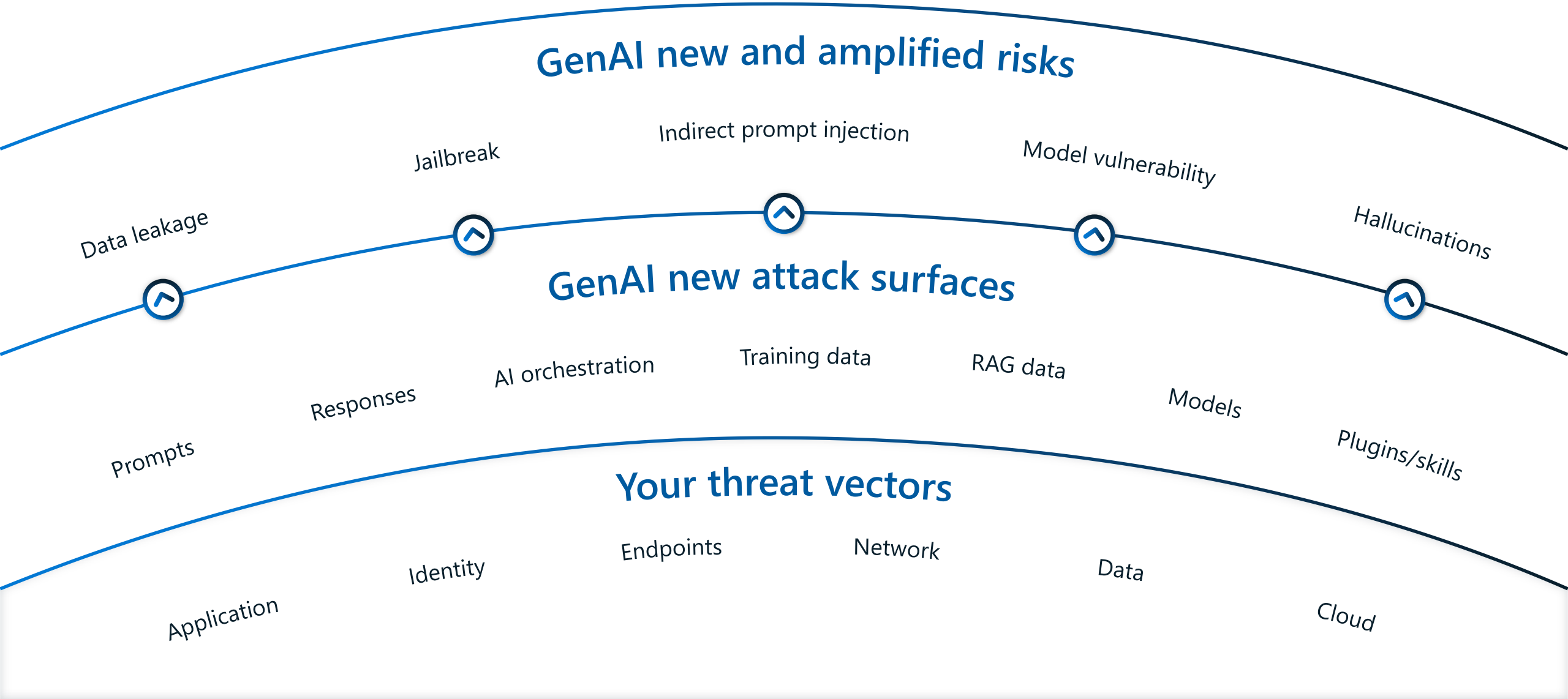
Unmatched intelligence from 50 years of experience and insight

7,000 Password attacks blocked per second

600m Attacks per day

300+ global threat groups

GenAI attack surfaces introduce new and amplified risks



AI transformation isn’t slowing down

$3.5 return on investment for every $1 invested into AI*

70% will partner with trusted cloud partners for AI platforms by 2025.**

66% of cloud applications will use AI by 2026.***

***. IDC FutureScape: Worldwide Cloud 2024 Predictions

**. IDC FutureScape – Worldwide Generative AI 2024 Predictions

*IDC

For Microsoft, security is job 1

“...prioritizing **security above all else** is critical to our company’s future”

Satya Nadella
Chairman and CEO

2 Outcomes

- A more resilient and transparent Microsoft
- Advanced security tools

3 Principles of Microsoft’s Secure Future Initiative

Secure by design

Security comes first when designing any product or service

Secure by default

Security protections are enabled and enforced by default, require no extra effort, and are not optional

Secure operations

Security controls and monitoring will continuously be improved to meet current and future threats

Announced June 4th

The European Security Program

The new 3 elements of the program

Sharing threat intelligence

Increasing AI-based threat intelligence with European governments.

Investing in cyber resilience

Expanding partnerships to disrupt and dismantle cybercriminal networks.

Cross-boarder collaboration

Free to European governments, members, the UK, Monaco, and the Vatican.

Announced June 9th

Microsoft's commitment to LASR

Investing additional resources to support the UK's national security and economic prosperity

Strengthen research efforts

Investing additional resources in the UK's Laboratory for AI Security Research to help strengthen and support research efforts.

Expand the cyber talent pipeline

Established to continue supporting the UK's national security and economic prosperity.

Provide advanced security

To **test advanced AI-assisted security tools in real-world environments** with Microsoft's security stack.

of security and risk leaders agree their company needs to have **security measures in place for their AI apps-including third-party SaaS, enterprise-ready, and custom-built apps**

Organizations face numerous security challenges when adopting AI

Data security and privacy

80%+

of leaders **cited leakage of sensitive data** as their main concern[1]

Shadow AI

78%

Users **bringing their own AI** (BYOAI) to work[2]

New vulnerabilities and threats

77%

concerned about **indirect prompt injection**[3]

Non-compliance

55%

of leaders lack understanding of AI regulations and are **seeking guidance on how to adhere** to these requirements[1]

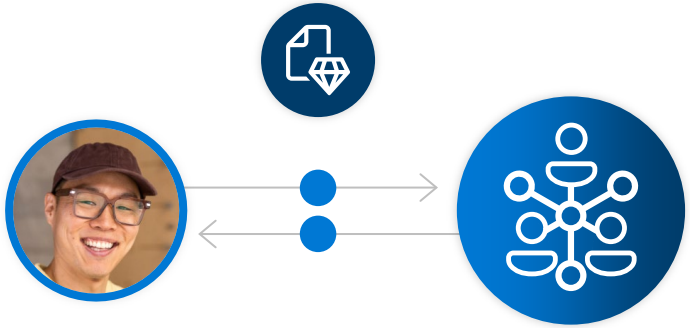
1. First Annual Generative AI study: Business Rewards vs. Security Risks, , Q3 2023, ISMG, N=400
2. 2024 Work Trend Index Annual Report, Microsoft and LinkedIn, May 2024, N=31,000.
3. Gartner®, Gartner Peer Community Poll – If your org's using any virtual assistants with AI capabilities, are you concerned about indirect prompt injection attacks? GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

For a successful AI transformation start with security first

Most common security incidents in AI

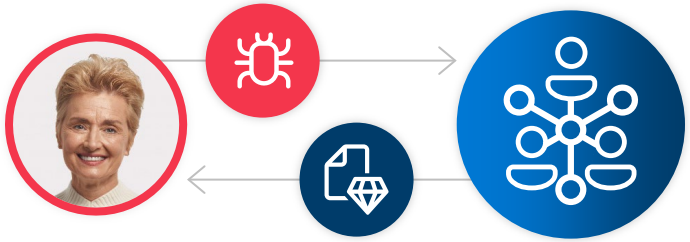
1 | Data leak and oversharing

Users may leak sensitive data to shadow AI apps or access sensitive data via AI apps



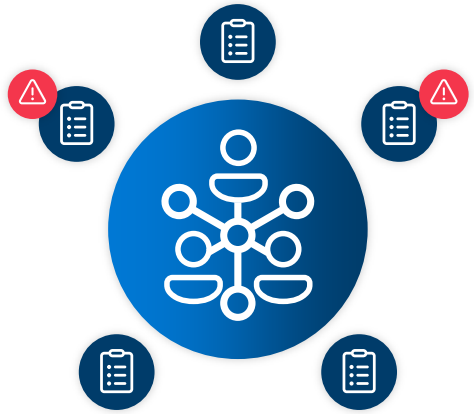
2 | Vulnerabilities and emerging threats

Bad actors may exploit vulnerabilities in AI apps to access valuable resources



3 | Non-compliance

Increasing uncertainty and liability on non-compliant AI adoption due to emerging AI regulations



Secure and govern AI with Microsoft

Prevent data leak and oversharing

- Access and endpoint controls – **Microsoft Entra & Intune**
- Data Security Posture Management for AI – **Microsoft Purview**
- Data classification, labeling, and protection – **Microsoft Purview**
- Data Loss Prevention – **Microsoft Purview**
- Anomaly and risky activities detection and response – **Microsoft Purview**
- SaaS app security – **Microsoft Defender**

Protect AI against vulnerabilities and emerging threats

- Data security and governance – **Microsoft Purview**
- Quality, safety, and security controls evaluation – **Azure AI Foundry**
- Security posture management for AI assets (apps, models, orchestrators, SDKs) – **Microsoft Defender**
- Model governance policy – **Azure Portal**
- Content safety prompt shield – **Azure AI**
- Threat protection for AI workloads – **Microsoft Defender**

Govern AI to comply with regulatory requirements

- Compliance assessments against AI regulations and standards – **Microsoft Purview**
- AI discovery and catalog – **Microsoft Defender**
- Prompt & response audits, lifecycle management, eDiscovery, communication compliance – **Microsoft Purview**
- AI reports for developers to log project details and controls – **Azure AI Foundry**
- Privacy impact assessment – **Microsoft Priva**
- Mitigation for harmful content, hallucination, and protected materials – **Azure AI Content Safety**

Our AI-first end-to-end platform

Be more secure

30+
product categories

72%
reduced likelihood of a breach*

88%
reduced time to respond to threats*

Stay compliant

90+
Global certifications and attestations, including GDPR, ISO 27001, and SOC 1/2/3

320+
Ready-to-use and customizable regulatory assessment templates to meet multicloud compliance requirements

Supports AI compliance
with the EU AI Act, NIST AI Risk Management Framework, ISO 42001, ISO 23894, code-of-conduct policies, and more

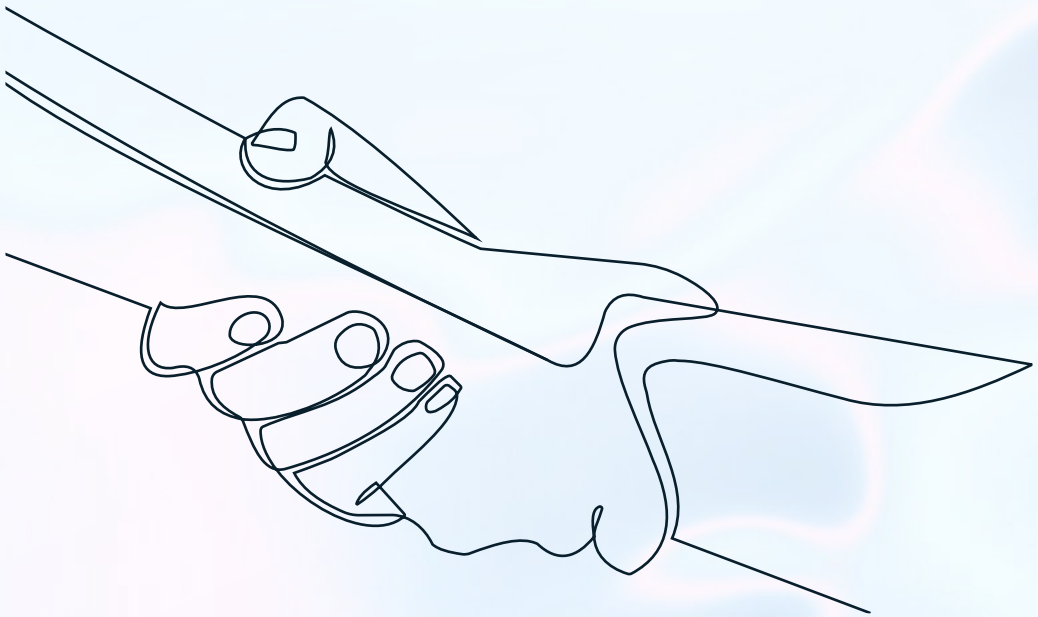
Lower total cost of ownership

60%
Potential savings with vendor consolidation

231%
Return on investment*

10,000
Security and threat intelligence experts working for you

Our mission is to make the world safer for everyone.



Microsoft Security

Thank you!