



Build AI Agents Securely Without Losing Momentum

Deliver scalable, compliant, and performant AI apps and agents—without the security tradeoffs or infrastructure bottlenecks

AI is scaling fast—and so are the threats that follow



Shift left—Security starts in your code

Given all the emerging challenges, developers must lead the charge in embedding security, compliance, and responsible AI practices from day one. So, how can you help protect data pipelines, manage access, and ensure traceability across the AI lifecycle?

Here is your playbook for building secure, compliant AI:



Apply secure-by-default data handling and guardrails

to prevent oversharing and exposure in AI workflows.



Design models with explainability and governance built in

ensuring traceability for compliance and audits.



Automate discovery and classification of sensitive data

across environments with dynamic policies.



Embed security from the start

by integrating AI agent identity validation, vulnerability testing, and secure-by-default practices into development workflows—so risks are addressed before code reaches production.



Partner early with security and compliance teams

to build resilient, regulation-ready AI systems—without slowing innovation or delivery.

Unify security. Simplify governance. Stay ahead of the curve.

While your team is cranking out code, spinning up agents, and shipping features, security still has to keep up—with threats, compliance rules, and a whole lot of unknowns.

The best solutions



Catch risks early

(before they catch you)



Lock down data

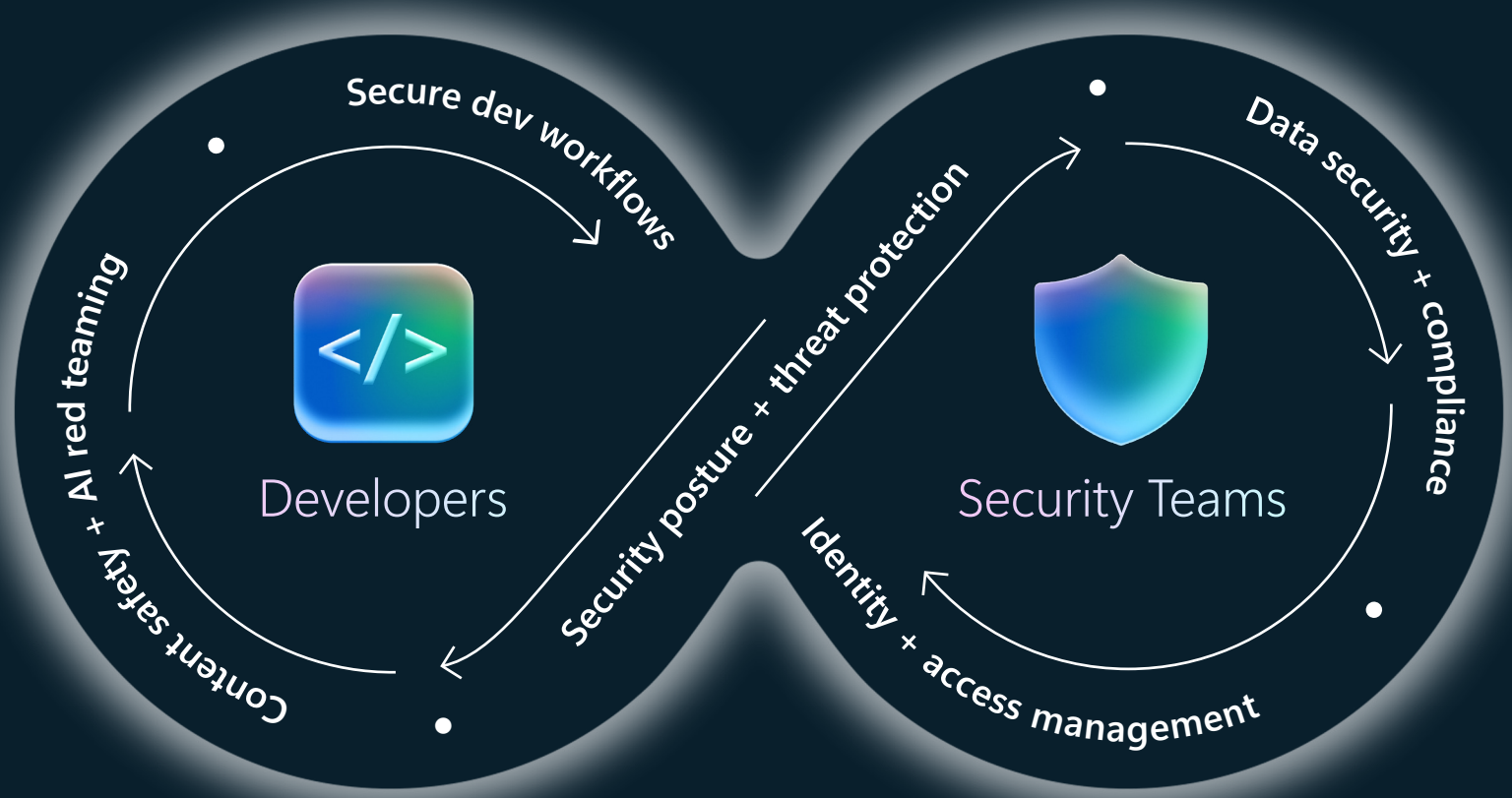
without slowing devs down



Keep everything compliant

even the weird edge cases

Protect cloud and AI from code to runtime



Start secure and stay secure with Microsoft



Microsoft Defender for Cloud

Continuous threat detection & protection



Microsoft Purview

Data security & governance



Microsoft Foundry

Responsible AI & built-in content safety

Staying ahead means securing AI now.

[Read the full guidance](#)

¹ "Accelerate AI transformation with strong security: The path to securely embracing AI adoption in your organization." Microsoft.
² Microsoft Work Trend Index Survey 2025.
³ "Gartner Predicts 40% of AI Data Breaches Will Arise from Cross-Border GenAI Misuse by 2027." Gartner.

©2025 Microsoft Corporation. All rights reserved. This document is provided "as is." Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Microsoft Security