Microsoft Security

AI is here

How will you keep your business secure?

The landscape is shifting

One suspicious email. One careless click. One upload to a public AI platform.

Breaches can occur from the smallest oversights—but over 80% of growing businesses are not financially prepared to recover[1] from a serious breach. AI is changing the threat landscape for growing businesses by increasing the speed and sophistication of threats and by introducing new risks. But AI can also work in your favor. With the right approach, it can help you identify risks earlier and respond faster, without requiring a large security team.

Growing businesses face the same threats as enterprises, but often with fewer resources. That's why it's critical to adopt an integrated, AI-powered security approach that helps you stay protected while continuing to grow.

1 in 3 SMBs have been victims of cyberattacks[2]

For growing businesses every customer interaction, transaction, and system depends on trust. And trust is built on security. The challenge is, you face the same threats as enterprise-level organizations, but you may not have a team of dedicated security experts to protect against them.

82% of ransomware attacks target SMBs[3]

But AI can also strengthen security and act as a force multiplier when coupled with your workers. Built into an end-to-end platform and integrated into workstreams and productivity apps your employees already use, AI can help you speed response and limit damage from breaches without a dedicated security team. AI-powered intelligence can actively block malicious traffic while helping you understand what to do next. When breaches do occur, AI can contain in minutes threats that used to take days to neutralize.

Consolidating security with a trusted partner can reduce your security spend by replacing a patchwork of tools and licenses. Microsoft makes the same end-to-end protections developed for enterprises available, affordable, and ready to integrate in your workstreams—so you can stay ahead of threats and focus on running your business.

Analysis paralysis

~20 SMBs use about 20 security solutions on average[4]

Challenge

AI enables cybercriminals to launch faster, more convincing attacks. Many growing businesses respond by adding more tools, but this creates complexity and security gaps.

Solution

Eliminate the need to add point solutions as you grow. Choose a trusted partner and an end-to-end solution that offers quick setup and streamlined integration with the apps your business already uses—and close gaps created by multiple tools.

Stop threats before they reach your employees

4.5X AI-automated phishing is 4.5x more effective than traditional attacks.[5]

Challenge

A convincing phishing email deceives one employee who clicks a malicious link.

Solution

Choose a platform that scans emails, links, and attachments in real time, helping stop threats before they even reach your people.

Give your employees AI you can trust

80% of SMB AI users are bringing their own AI to work[6]

Challenge

Trying to be more productive, an employee uploads sensitive data to a public AI. You lose control over where the data goes from there.

Solution

Give your employees a powerful AI built into the apps they already use, so you maintain visibility, control, and security while they gain productivity.

So many alerts, such limited attention

42% of security alerts go uninvestigated[7]

Challenge

The scale of AI attacks can result in a steady stream of alerts. An overwhelmed IT staff may not be able to prioritize responses efficiently.

Solution

Provide them with security that surfaces the most important alerts, explains what's happening in plain language, and recommends clear next steps.

Protecting your data by protecting identities

1.6M/hr fraudulent account attempts blocked by Microsoft[8]

Challenge

AI-guided attacks can find gaps even with multifactor authentication, enter your system, and spread before you know you've been breached.

Solution

Use AI to monitor login behavior and restrict suspicious access. Employ phishing-resistant authentication to make stolen passwords effectively useless.

Staying ahead means securing today

Staying ahead of threats doesn't always require overhauling your systems or hiring security specialists. A single, connected solution featuring tools and apps your employees already use can enhance security, help keep expenses predictable, and reduce overlapping costs. Explore the ways Microsoft provides the foundation of trust you need to build security for your AI-enabled future.

- Find a plan that provides the best security for your business
- Talk to a pro about securing your business

[1] "10 Small Business Cyber Security Statistics That You Should Know – And How To Improve Them" by Ashley Lukehart, Cybersecurity Magazine, May 20, 2021

[2] "New research: Small and medium business (SMB) cyberattacks are frequent and costly" by Microsoft Security. An online survey of 2,000 IT security product decision-makers/influencers at U.K. and U.S. companies from September 10-26, 2024. Stats for businesses that have 25-299 employees.

[3] "The Devastating Impact of Ransomware Attacks on Small Businesses" by Quinn Cleary, April 4, 2023

[4] Gartner SMB Cybersecurity Survey (2023) via internal sales enablement deck; Forrester Consulting (suite preference) via internal enablement; Microsoft Defender for Business FAQ (up to 300 users).

[5] "Microsoft Digital Defense Report 2025: Lighting the path to a secure future" Microsoft Threat Intelligence Report, October 2025

[6] "Workers worldwide are embracing AI, especially in small and medium-size businesses" by Brenna Robinson, June 5, 2024

[7] "Unify now or pay later: New research exposes the operational cost of a fragmented SOC" by Rob Lefferts, February 17, 2026

[8] "Cyber Signals Issue 9 | AI-powered deception: Emerging fraud threats and countermeasures" by Microsoft Security Team, April 16, 2025

© 2026 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