Windows 11 Pro

THE POWERS *of* ME

To accelerate business success, make everyone secure by default

With powerful out-of-the-box protection, Windows 11 Pro PCs enable employees to do their best work—and be their boldest selves—anywhere and anytime.

Introduction

Today, IT leaders are regarded as change agents, responsible for harnessing technologies to drive business innovation and growth. But yesterday's challenges still remain. In fact, cyberthreats are exploding in scale and sophistication as bad actors relentlessly probe endpoints for footholds to infiltrate corporate networks.

In a highly competitive landscape, simply locking everything down is not the answer. IT leaders need solutions that not only strengthen security but also enhance productivity. And those solutions need to be compatible with existing technologies and easy to implement without disrupting business.

Many IT leaders are turning to devices engineered for security as well as business transformation. New Windows 11 Pro PCs come with protection by default and AI experiences on tap, enabling team members to outperform anywhere, unlock their full potential, and make their ingenuity a competitive advantage.

How Microsoft can help

Windows 11 Pro devices are secure out-of-the-box with layers of hardware-backed protection, for a reported 58% drop in security incidents.[1] You can easily implement modern security management across the organization, in Microsoft 365 apps[2] or Copilot on Windows[3] with commercial data protection. And your teams can do their best work anywhere, backed by the most secure Windows ever and assisted by industry-leading AI.

Read on to learn how you can deploy powerful protection by default and supercharge employees to drive the business forward.

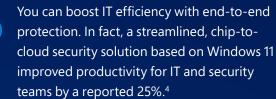# How to accelerate business success with Windows 11 Pro

You can protect critical business data and control apps and access to information anywhere with end-to-end security management—for a reported 3.1x reduction in firmware attacks.[1]

With layers of security enabled out-of-the-box, employees can thrive anywhere, shielded by powerful cybersecurity across hardware, software, identities, and data—for a reported 58% drop in security incidents.[1]

You can defend against evolving threats with the latest safeguards, like enhanced phishing protection, and enjoy the peace of mind that comes with a reported 2.8x fewer instances of identity theft.[1]

You can boost IT efficiency with end-to-end protection. In fact, a streamlined, chip-to-cloud security solution based on Windows 11 improved productivity for IT and security teams by a reported 25%.[4]

As cyberthreats proliferate in a highly competitive market, IT leaders are choosing devices designed for security and business transformation to boost workforce productivity and enable employees to thrive anywhere. New Windows 11 Pro devices with Copilot deliver those benefits on a secure, compatible, and business-ready platform.

Discover how powerful protection by default delivers a transformative effect for leaders who want to accelerate business success

Safeguard business data

Windows 11 Pro PCs are engineered to protect valuable data and control apps and access to information anywhere with end-to-end security management. A 3.1x reduction in firmware attacks has been reported.[1]

Copilot on Windows with commercial data protection shields both business and personal information at no additional cost when you sign on with Microsoft Entra ID.[5] And you can securely support employees and reduce your attack surface with Intune Endpoint Privilege Management.[6] For even more hardened security, **token protection for sign-in** sessions cryptographically binds security tokens to a device.[7]

And Windows 11 Pro streamlines security for IT teams. You'll appreciate the **hassle-free management and backup of local admin account passwords** on Microsoft Entra ID-joined or Windows Server AD devices local administrator password solution (LAPS).[8] And it's easy to **reduce the threats of data exposure or theft** by enhancing file and system protection, making sensitive data inaccessible when BitLocker-protected devices are lost or recycled.

Most secure Windows ever

Help your teams work fearlessly anywhere and anytime with layers of protection built in and enabled by default—for a reported 3.1x reduction in firmware attacks and 2.8x fewer instances of identity theft.[1]

With powerful **out-of-the-box protection**, you'll spend less time responding to threats and more time enabling employees to make a bigger impact. **TPM 2.0** provides hardware-backed protection for credentials and other sensitive data, while **Windows Hello for Business**[9] makes signing in passwordless and secure. In fact, by replacing passwords with a passkey,[10] your people can **sign in with their face, fingerprint, or PIN**.[9]

The most secure Windows ever also provides **virtualization-based security** (VBS) and **hypervisor-protected code integrity** (HVCI) enabled by default to protect the kernel against cyberattacks. **Microsoft Defender Antivirus** is always on, protecting Windows devices in real time from viruses, malware, and other threats. And **secure startup**[11] protects user data from the moment you power on by preventing malicious software from loading.

Protect against evolving threats

Proactively defend against cyberthreats with the latest safeguards for better peace of mind—including a reported 2.8x fewer instances of identity theft.[1]

New Windows 11 Pro devices allow you to catch threats even before they occur. **Enhanced phishing protection with Microsoft Defender SmartScreen** warns employees when they're trying to enter their Microsoft credentials into a malicious app. And simple, effective features like **lock on leave/wake on approach**[9] use presence settings to keep user data and privacy safe from unwanted intrusions.

You'll stay ahead of cyberattackers without even trying, thanks to **Windows Update for Business**.[12] It keeps your fleet of devices always up to date with the latest security and Windows features by directly connecting to the Windows update service. And you can protect every device from risky drivers with **Microsoft vulnerable driver block list**[13] on Windows 11 Pro devices.

Move to Windows 11 Pro devices before support ends for Windows 10 on October 14, 2025.[14] Out-of-date devices increase vulnerability, and upgrading to Windows 11 Pro will give you the latest security features, while ensuring you're supported and up to date. Get started now to optimize deployment and benefit from the latest features, including Copilot on Windows.

My best me   Confident me

Pick confident me for end-to-end protection, simplified

The best of both worlds: better security and better IT efficiency. A streamlined, chip-to-cloud security solution based on Windows 11 improved productivity for IT and security teams by a reported 25%.[4]

You can protect access to system resources while keeping everyone productive with **Intune Endpoint Privilege Management** (EPM).[6] Most employees sign in as standard users without administrator rights, while tasks that need elevated privileges can still be accomplished. And your teams can get secure access to their work emails, Teams meetings, and other content through Microsoft Edge on their personal or BYOD devices with **MAM for Windows**.

In fact, Windows 11 Pro devices make signing in simple and secure in every way. For example, **token protection**[7] binds security tokens for apps and services to their intended devices, preventing cyberthieves from impersonating users on other devices. And **Microsoft Entra ID**[5] **lets you automate local admin password account management** and improve security with LAPS.[8]

To accelerate business success, help users thrive anywhere

Powerful protection by default and industry-leading AI in Windows 11 Pro bring out the best in your teams, making them more confident and creative, and enabling them to outperform anywhere. When technology protects and maximizes employees, they can achieve the extraordinary. And when employees thrive, so do businesses. Here's how you can transform your own organization with Windows 11 Pro devices

1 ## What can my employees gain when I invest in new Windows 11 Pro devices?

With Copilot you can streamline tasks and experience less clutter and more innovation and creativity. They'll become not just more productive, but more effective and satisfied in their role—confident partners who will help you win.

2 ## How will switching to Windows 11 Pro impact my IT team?

IT teams will be delighted by the simplicity of integrating AI across the organization, and the productivity gains for both users and IT staff. A streamlined, chip-to-cloud security solution based on Windows 11 Pro improved productivity for IT and security teams by a reported 25%.[4]

3 ## How will the transition to Windows 11 Pro devices empower the whole organization?

Organizations that invest in Windows 11 Pro devices can expect to be more efficient and secure, but also nimbler and more successful—backed by a workforce full of instinctive problem solvers, all empowered by leading-edge technology.

4 ## How can Microsoft help?

If you're ready to unlock your AI advantage,[15] reach out to learn more about the most secure Windows ever, designed for business.

Footnotes

1 SMB Windows 11 Survey Report. Techaisle, February 2022. Windows 11 results are in comparison with Windows 10 devices.

2 Sold separately.

3 Copilot on Windows (in preview) is available in select global markets and will roll out starting in summer 2024 to Windows 11 PCs in the European Economic Area. Copilot with commercial data protection is available at no additional cost for users with an Entra ID and an enabled, eligible Microsoft 365 or Office 365 license.

4 Commissioned study delivered by Forrester Consulting, "The Total Economic Impact™ of Windows 11 Pro Devices," December 2022. Note, quantified benefits reflect results over three years combined into a single composite organization that generates $1 billion in annual revenue, has 2,000 employees, refreshes hardware on a four-year cycle, and migrates the entirety of its workforce to Windows 11 devices.

5 Enabled, eligible Microsoft 365 license required. Sold separately.

6 Endpoint Privilege Management requires Microsoft Entra ID and an additional license beyond the Microsoft Intune Plan 1 license. You can choose between a stand-alone license that adds only EPM, or license EPM as part of the Microsoft Intune

Suite. For more information, see Use Intune Suite add-on capabilities.

7 Developer enablement required.

8 Requires Azure Active Directory and Microsoft Intune or other modern device management solution product required; sold separately.

9 Hardware dependent.

10 Passkeys are securely stored on Windows in TPM 2.0, and users can manage them through Settings.

11 Secure startup is used with a TPM like Microsoft TPM 2.0.

12 Windows Update for Business works with Microsoft Entra ID, sold separately.

13 Vulnerable driver blocklist rules can be enabled and configured using Microsoft Intune, mobile device management (MDM), Microsoft Endpoint Configuration Manager, Group Policy, and PowerShell. Sold separately.

14 Blog: Plan for Windows 10 EOS with Windows 11, Windows 365, and ESU. Learn more.

15 Microsoft Responsible AI.

Windows 11 Pro