Uplifting employees and organizations

with security by default

Windows 11 Pro

TABLE *of* CONTENTS

Accelerate business success with always-on protection

As IT leaders harness new technologies to drive growth, they must simultaneously protect the business in an ever-evolving security threat landscape. Complex threats such as phishing, ransomware, and distributed denial of service (DDoS) attacks are continuing to escalate, demanding increasingly robust and proactive defenses.

Human error adds complexity to this challenge, accounting for 46% of all cybersecurity incidents.[2] Diverse workstyles and flexible work environments amplify the risk by broadening the potential points of vulnerability.

In a highly competitive business environment, simply locking everything down is not the answer. IT leaders must turn to solutions that not only strengthen protection but also enhance productivity—devices engineered for security as well as business transformation.

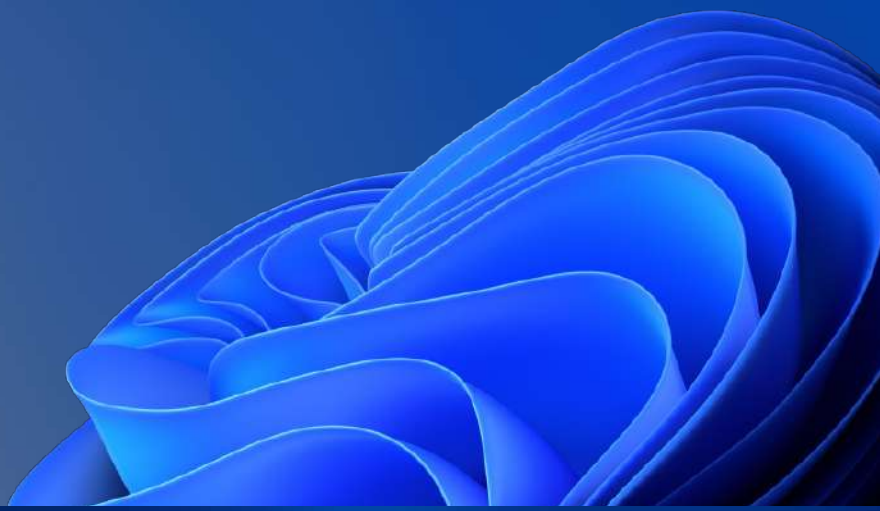
Windows 11 Pro PCs are designed to help block cyberthreats, boost innovation and efficiency, solve problems, and achieve more with less time, effort, and cost.

> Windows 11 Pro is backed by layers of powerful protection that can **drop security incidents a reported 58%.**[1]

Systemwide intelligence proactively protects against threats, finds better answers, enhances videoconferencing, improves accessibility, and helps reduce your carbon footprint. And the most secure Windows ever delivers the latest feature and security updates straight to your desktop.

Best of all, Windows 11 Pro PCs come with Copilot in Windows[3] to help increase insights and efficiency.

Read on to learn how your team members can benefit from protection by default and AI experiences on tap, enabling them to outperform anywhere, unlock their full potential, and make their ingenuity a competitive advantage for your company.



More innovation, less cybercrime

The increased flexibility of modern work presents a challenging cybersecurity environment, as IT leaders look for solutions to increase productivity, collaboration, and innovation while keeping employees safe anywhere. The good news is, it's possible to protect against over 99% of successful cyberattacks by adhering to a few fundamental security hygiene practices: enabling multifactor authentication (MFA); applying zero-trust principles; using antimalware and extended detection and response (XDR); keeping firmware, OS, and apps up to date; and managing and safeguarding business-critical data.[4]

Many of these practices are as easy to implement as upgrading your PCs. 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] With Windows 11 Pro and Microsoft Intune,[5] you can easily implement modern security management across the organization, including for Microsoft 365 apps[6] and Copilot. And you can guard employee credentials with built-in features like enhanced phishing protection in Microsoft Defender SmartScreen. Lock on leave/wake presence sensing[7] also helps keep your content and privacy safe; your PC locks when you leave and uses Windows Hello[7] with presence detection sensors to securely sign in when you approach.

As a result, your teams can do their best work anywhere, backed by the most secure Windows ever and assisted by industry-leading AI. And while Copilot in Windows can improve workflow for almost everyone in your organization, your IT team can also leverage Copilot for Security to identify threats and provide tailored insights and next steps to accelerate incident response. In fact, AI is assuming increasing importance in an ever-more-complex cyber ecosystem, offering the potential to change the security landscape by augmenting the skill, speed, and knowledge of defenders.

> The 2023 Microsoft Digital Defense Report shows how AI offers the potential to change the security landscape by augmenting the skill, speed, and knowledge of defenders.
>
> **Download the report >**

Microsoft security experts analyze over 65 trillion signals each day with the help of AI. In fact, Microsoft's investments in security research, innovation, and the global security community include:[4]

65 trillion
signals synthesized daily using sophisticated data analytics and AI algorithms

10,000+
security and threat intelligence experts across the globe

4,000
identity authentication threats blocked per second

15,000+
partners with specialized solutions in our security ecosystem

135 million
managed devices providing security and threat landscape insights

300+
threat actors tracked, including 160 nation-state actors and 50 ransomware groups

100,000+
domains utilized by cybercriminals removed

How a secure-by-default strategy drives business success

As IT leaders focus on strategic initiatives, their business data must still be protected, their endpoints safeguarded, and their workforce enabled for success. Any security plan must address not only protection but also productivity, collaboration, and operational efficiency.

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

By deploying Windows 11 Pro devices, IT leaders can implement a secure-by-default strategy to minimize their attack surface and help prevent threats before they happen—for a reported 58% drop in security incidents.[1] They can take advantage of modern security management to enforce policies across devices, apps, and the cloud. And with powerful protection that's always on, they can spend less time responding to threats and more time driving growth and innovation.

Windows 11 Pro PCs: Powerful protection by default

Safeguard business data

Windows 11 Pro devices deploy end-to-end security management to protect valuable data and to control apps and access to information anywhere. Hardware-enabled protection is tightly integrated with software for a reported 3.1x reduction in firmware attacks.[1]

Protects against evolving threats

As bad actors relentlessly probe for weak spots in your network, you can defend against cyberthreats with the latest safeguards for better peace of mind—including a reported 2.8x fewer instances of identity theft.[1] And you can safeguard your identities and data with token protection, Windows Hello Enhanced Sign-in Sessions, and enhanced phishing protection. You can also guard data using presence sensing with Windows Hello, which helps keep data safe from unwanted intrusions by securely waking when you approach and locking when you leave.[7]

Most secure Windows ever

Windows 11 Pro PCs come with layers of security already enabled, so team members can dive into work anywhere, shielded by powerful cybersecurity across hardware, software, identities, and data. TPM 2.0 provides hardware-backed protection for credentials and other sensitive data, while Windows Hello for Business[7] makes signing in easy, secure, and passwordless.

End-to-end protection, simplified

You can protect access to system resources while keeping everyone productive with Intune Endpoint Privilege Management (EPM).[8] 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. A streamlined, chip-to-cloud security solution based on Windows 11 improved productivity for IT and security teams by a reported 25%.[9]

How working styles influence device and OS needs

Since 2020, Microsoft research has unveiled critical insight into the role of new devices and operating systems in shaping the future of work and combating an ever-evolving cybersecurity landscape.

Flexible workstyles and locations continue to become more prevalent, reflecting a lasting shift that is transforming how employees engage with their work and their employer. Employees are seeking greater autonomy and convenience, and many organizations are recognizing the benefits of embracing these changes, such as increased productivity and work satisfaction.[10]

This seemingly embedded change in working dynamics continues to bring new security challenges, especially in flexible work environments. Yet, as work and technology continue to evolve together, better practices can enhance productivity. Embracing AI by investing in new devices can lead to not only a reduction in digital debt but also broader productivity and problem-solving gains that include better well-being, improved work-life balance, and an overall enhanced employee experience.

Changing working styles aren't limited to *where* things get done—there are also major shifts in *how* work is getting done. This is where the role of AI, including Copilot in Windows and Copilot for Microsoft 365,[6] is becoming increasingly prominent in transforming the work landscape. As work-related data generation accelerates at an unprecedented pace, aging devices and outdated operating systems pose a genuine roadblock to the innovation these technologies promise.

To thrive amid a rapidly changing marketplace, businesses require the right tools that can foster innovation with the security to thrive anywhere. Windows 11 Pro devices, with powerful protection by default, enable organizations to tackle these challenges by leveraging the power of emerging workplace technologies.

In this section, we embark on a comprehensive exploration of how diverse working styles are reshaping not only the individual working experience but also the dynamics within collaborative teams, the broader organization, and even the fabric of society itself.

Flexible work at scale: Understanding different demographics

Impact on the individual

Flexible work arrangements allow for a blend of remote and in-office tasks, offering individuals greater flexibility and autonomy. The ability to work from various locations can enhance work-life balance but requires new tools, technologies, and security measures tailored to different environments.

Windows 11 Pro offers employees a lot more than a productivity boost. They can streamline tasks and become more creative, innovative, and self-reliant with Copilot in Windows. And intuitive user experiences like controlling your PC with your voice[7] remove barriers to participation and enable everyone to make a bigger impact.

Effect on collaborative teams

The shift toward flexible work necessitates a rethinking of how teams collaborate. Although flexible work fosters a more versatile and global talent pool, it demands robust, secure collaboration platforms and tools that enable seamless communication and coordination, regardless of physical location.

Team members can collaborate with speed, flexibility, and style using Microsoft Teams on the latest Windows 11 Pro devices. AI-powered recommendations help them work not just faster, but also smarter. Organizations have reported 50% faster workflows and collaboration on average.[11]

Influence on the broader organization

Organizations grapple with complex issues such as cross-team communication, systemic loneliness, and major workforce shifts. Potential organization-level threats include sophisticated ransomware attacks that can cripple entire networks.

Windows 11 Pro allows businesses to embrace uncertainty, enabling secure communication across various work environments. Systemwide intelligence proactively protects against threats, finds the right files, enhances videoconferencing, improves accessibility, and helps reduce your carbon footprint.

Repercussions for society

On a societal scale, changing work geographies and their effects are under examination. Amid these disruptions, cybersecurity threats can jeopardize entire sectors.

Windows 11 Pro equips organizations to adapt securely amid these global shifts, ensuring business continuity and productivity while providing robust protections against escalating cybersecurity threats.

Three risk factors in the modern era of work

The imperative for organizations is clear: In order to navigate current and future work landscape uncertainties, robust cybersecurity strategies and up-to-date systems and devices must form the core of their operational blueprint. The following three risk factors are rooted in real-world consequences and, if not proactively dealt with, may profoundly influence an organization's security posture and overall business success.

1. Stifled innovation

58% more threats blocked on average,[1] saving time for innovation.

64% of IT leaders believe that cybersecurity concerns are negatively impacting their organization's willingness to invest in innovative tech.[12]

Outdated systems and devices can inhibit an organization's ability to innovate and compete in a rapidly evolving business environment. As an example, a business that delays in capitalizing on AI runs the risk of being overtaken by more innovative competitors who are elevating the ingenuity of their workforce.

Additionally, older systems are prone to failure, causing disruptive downtime that reduces productivity and threatens client relationships and business opportunities. This can also impact an organization's ability to attract and retain top talent. Ensuring every employee is equipped with secure and accessible technologies that enable connection and contribution to an organization's innovation agenda is essential.

Considerations for leaders:

- How does outdated technology affect our innovation and competitiveness?
- How can we structure and upskill our teams to make AI an innovation accelerant?
- How does our current technology align with the diverse working styles within our organization?
- Can our infrastructure attract and retain the talent needed for modern work dynamics?

2. Overburdened IT resources

66% of security team members **experience significant stress at work. 64%** have had work stress **impact their mental health**.[13]

For IT professionals who report high levels of burnout, **42% are considering quitting** their company within the next six months, according to survey data from Yerbo. Even among those who report low or moderate levels of burnout, **25% express a desire to leave** their company in the near future.[14]

3.4 million estimated openings for skilled security professionals due to a global shortage of talent.[15]

Older systems require more maintenance, often straining IT resources and diverting focus from strategic tasks. Incompatibility with modern IT management tools also complicates maintaining robust security and compliance. And aging systems often lack the latest security updates, exposing them to cybersecurity threats, potentially resulting in costly data breaches that could impact customer trust.

As a result, more and more IT leaders are seeking end-to-end protection that relieves the burden on their staff. In fact, a streamlined, chip-to-cloud security solution based on Windows 11 improved productivity for IT and security teams by a reported 25%.[9]

Considerations for leaders:

- What percentage of IT resources is spent on maintaining aging devices, and how does this impact strategic focus?
- Can we free up IT resources while implementing end-to-end defense at the speed and scale of AI with Copilot in Windows?
- How vulnerable are our aging devices to cybersecurity threats like password attacks and ransomware?
- What are the potential financial and reputational costs of a data breach from outdated security?

3. Eroded employee confidence and productivity

Employees are **230% more engaged** and **85% more likely to stay beyond three years** in their jobs if they feel they have the technology that supports them at work.[16]

60% of technology and business leaders indicate that improving employee experience is a top IT priority.[17]

Top-performing companies are nearly twice as likely as all other organizations to be in a state of advanced digitalization and **89% more likely** to have significantly increased their levels of employee satisfaction.[18]

Aging devices can hamper employee productivity and satisfaction. Slow performance and incompatibility with new tools often lead to frustration, affecting morale and the bottom line. And, of course, older systems are softer targets for cyberattackers.

Could generative AI at work mitigate some or all of these issues? A recent Work Trend Index report showed that early Copilot users saw impressive gains in quality and speed, productivity and creativity, and focus time. Download the report here.

Considerations for leaders:

- Can we increase employee engagement and retention by improving user experiences with generative AI?
- How are older devices' performance issues affecting employee productivity and satisfaction?
- Are employees able to use necessary new tools, or are they hampered by compatibility problems?
- How is employee confidence influenced by increased cyberthreat exposure due to older systems?

Windows 11 Pro PCs: Layers of protection for modern business

Security decision-makers agree: Almost 90% of survey respondents believe outdated hardware increases vulnerability to attacks, and modern hardware is essential for future protection.[19] Building upon Windows 10 innovations, Windows 11 Pro, in collaboration with our manufacturing and silicon partners, introduces additional hardware security capabilities to support modern work and respond to the evolving threat landscape.

Enhanced hardware and operating system security

Windows 11 Pro elevates protection with hardware-based security such as TPM 2.0, which safeguards sensitive information like encryption keys and user credentials from unauthorized access and manipulation. For enhanced kernel protection, Windows 11 Pro devices come with isolation technologies now enabled by default, including virtualization-based security (VBS) and hypervisor code integrity (HVCI).

Robust application security and privacy controls

Many organizations cite application control as one of the most effective means of defending against executable file-based malware. App Control for Business[8] (previously called Windows Defender Application Control) is the next-generation app control solution for Windows and provides IT powerful control over what applications run in your environment. Customers using Microsoft Intune[5] to manage their devices are now able to configure App Control for Business in the admin console, including setting up Intune as a managed installer.

To help ensure the safety of both personal and business data, Windows 11 Pro employs multilayered application security. Principles such as application isolation, code integrity, privacy controls, and least-privilege enable developers to embed security and privacy from the onset. Windows 11 Pro also empowers users with increased control over privacy features like location, camera, and microphone access.

Secured identities

With cybercriminals frequently targeting passwords, Windows 11 Pro employs robust protection against credential theft. Enable multifactor authentication and credential protection with Windows Hello for Business[7] for easy, secure sign-in without a password, using PIN, face, or fingerprint. Microsoft Defender SmartScreen provides proactive protection against credential theft with built-in enhanced phishing protection, while Windows presence-sensing features give peace of mind when stepping away with lock on leave and wake on approach capabilities.[7]

Connecting to cloud services

Windows Update for Business[20] is a no-cost cloud service that enables IT administrators to keep Windows client devices in their organization up to date with the latest security protections and Windows features by directly connecting these systems to Windows Update service. Windows 11 Pro also has built-in device enrollment and management clients, enabling organizations to enforce security policies and take advantage of modern device management (MDM) tools like Microsoft Intune.[5] Windows 11 Pro works with on-premises and cloud-based management solutions.

For an easy path to cloud management, combine Windows 11 Pro with Microsoft 365 Business Premium.[5] By meeting the contemporary requirements for security and flexibility, Windows 11 Pro modern PCs, paired with Microsoft 365 Business Premium, represent a vital step toward a more resilient and efficient working environment.

To learn more, please download the Windows 11 Security Book

Windows 11 Pro PCs: Securing tomorrow's work landscape

As organizations look to accelerate business performance in a work landscape transformed by AI, they need a platform that unites robust security, effortless management, and diverse workstyle support. The deployment of Windows 11 Pro devices offers an advanced solution extending beyond traditional IT security, addressing not only protection but also productivity, collaboration, and operational efficiency.

Windows 11 Pro devices are more than a security measure; they enhance productivity and collaboration, adapting to a rapidly changing workplace. This adaptation boosts employee confidence and offsets potential productivity decline. By simplifying deployment and provisioning, these devices relieve strained IT resources, fostering innovation and lowering costs.

Windows 11 Pro devices lay the groundwork for the future. By shifting to cloud-based operations and using new technologies, organizations can grasp opportunities, safeguard business data, and gain the momentum to succeed. This prepares them to excel in a constantly evolving business landscape.

Additional protection when you need it

Windows 11 Pro devices come with an array of security features, including optional hardware-based root-of-trust through the **Microsoft Pluton security processor**, and integrated elements like **BitLocker, Windows Hello for Business**,[7] and **TPM 2.0**.

Advanced Hardware-Enforced Stack Protection synergizes software and hardware defenses against threats like memory corruption and zero-day exploits. Regular updates to the root-of-trust firmware maintain a well-shielded device environment.

Organizations deploying Windows 11 Pro devices can dramatically reduce their attack surface, allowing them to pursue opportunities without compromising security, enhancing both adaptability and growth.

Windows 11 Pro key benefits

Businesses: A robust security foundation

Windows 11 Pro can help reduce cyberthreats by up to 58%.[1] Organizations can confidently pursue growth opportunities without compromising security.

IT teams: Reduce incidents and safeguard data

From hardware-based root-of-trust to integrated protections like BitLocker and Windows Hello,[7] IT teams benefit from the comprehensive security features of Windows 11 Pro.

Employees: Work securely and efficiently

Windows 11 Pro devices receive regular, automatic firmware updates, giving employees confidence that their data is protected so they can focus on productivity.

Advanced protection in an ever-changing threat landscape

Windows 11 Pro devices, equipped with modern CPUs and default security features like TPM 2.0 for hardware root-of-trust, secure boot, and BitLocker drive encryption, enhance security posture. When integrated with third-party security software, a 20% reduction in successful security attacks was reported.[9]

> **Up to a 20% reported reduction** in the chance of successful security attacks with Windows 11 Pro devices.[9]

The inclusion of TPM 2.0 in new and upgraded devices supports key functions such as secure storage, encryption, key generation, and boot integrity, foundational to features like Windows Hello for Business[7] and Windows Defender System Guard. This establishes a consistent hardware root-of-trust, ensuring readiness for future security capabilities.

Windows 11 Pro key benefits

Businesses: Fueling business transformation

With comprehensive security that ranges from chip to cloud, businesses can confidently embrace new opportunities and navigate the future. Enhanced performance, security advances, and AI integration empower organizations to operate anywhere and drive forward without compromise.

IT teams: Streamlined management and compatibility

Compatibility with existing software and hardware simplifies deployment, while modern management capabilities allow IT to do more with less. Windows 11 Pro stands as a milestone in reducing costs and effort, enabling a seamless, secure, and efficient environment for organizational success.

Employees: Empowering exceptional work anywhere

AI-powered experiences, intelligent workflows, and personalized settings enable employees to work the way they want, fostering well-being and productivity. Windows 11 Pro offers an empathetic approach that transcends mere functionality, enhancing both satisfaction and business results.

Developed for productivity and collaboration

The new features in Windows 11 Pro, when paired with modern devices, have the potential to increase employee productivity, allowing them to get more done faster. Purpose-built for business growth, modern Windows 11 Pro devices blend superior performance with robust flexibility. Ready to use and secured as soon as employees receive them, Windows 11 Pro devices combine hardware-enabled protection that reportedly results in a 3.1x reduction in firmware attacks,[1] without hampering system performance or employee productivity.

> Businesses surveyed reported a **50% boost** in productivity and collaboration compared to previous Windows devices.[11]

Features such as snap layouts enable efficient desktop organization, fostering productivity and simplifying multitasking. Combined with AI enhancements for seamless videoconferencing, these features are further bolstered by the high-quality cameras and speakers integrated into new devices. This familiarity with the Windows interface helps ensure an uninterrupted workflow, with projects being completed 42% faster on average.[11]

Windows 11 Pro devices also offer enhancements such as up to 61% longer battery life,[11,21] responsive performance, and capabilities to support high-quality presentations on multiple 4K monitors. Various working modes enabled by peripherals, including pen, ink, touch, or voice[7] in addition to the conventional keyboard and mouse, offer flexible work methods.

Windows 11 Pro key benefits

Businesses: Engineered to boost growth

Windows 11 Pro devices offer a reduction in successful firmware attacks with increased malware resistance, all without impacting performance.[1] From supporting presentations on multiple 4K monitors to enabling increased productivity, Windows 11 Pro aligns with your business objectives, enabling you to seize opportunities effortlessly.

IT teams: Unparalleled control and security

Purpose-built for streamlined integration, Windows 11 Pro devices not only offer hardware-enabled protection and responsive performance but also are compatible with 99.7% of applications[22] and designed to work with almost any hardware, including printers, displays, and other accessories. With Windows 11 Pro, IT teams can focus on innovation, knowing the systems are secure, reliable, and easy to use.

Employees: Designed to adapt to any working style

Snap layouts and AI-enhanced videoconferencing make collaboration and multitasking easy. And with up to 61% longer battery life,[11,21] integrated high-quality cameras, and responsive performance, Windows 11 Pro devices prioritize flexibility and convenience for every task.

Increased productivity for security and IT teams

Based on a Forrester Report commissioned by Microsoft,[9] Windows 11 Pro devices alleviate overburdened IT resources. Because devices come with security features out-of-the-box, such as **virtualization-based security** (VBS), **hypervisor-protected code integrity** (HVCI), **Windows Hello for Business**,[7] and **Trusted Boot,** IT teams can focus more on strategic tasks rather than security settings.

> **A reported 80%** reduction in helpdesk requests over three years.[9]

VBS employs hardware virtualization to host a secure kernel separated from the operating system. This means that even if the operating system is compromised, the secure kernel is still protected. HVCI, in tandem with VBS, helps prevent attacks that attempt to modify kernel-mode code, such as drivers, maintaining the integrity of the hardware-level code and safeguarding against unauthorized alterations.

This advanced, proactive security setup amplifies IT productivity significantly, exemplified by a 20% increase in productivity within Forrester's composite organization's security team.[9] Furthermore, the inherent, default-enabled security features of Windows 11 Pro devices are coupled with self-service capabilities, contributing up to an 80% reduction in incoming helpdesk requests over three years.[9]

Windows 11 Pro key benefits

Businesses: Growth with minimal overhead

With security features like virtualization-based security (VBS) and hypervisor-protected code integrity (HVCI), Windows 11 Pro devices can help reduce exposure to threats, helping to keep sensitive data safe. These systems result in a reported productivity boost of up to 20% for security and IT teams.[9]

IT teams: Simplifying the daily routine

Windows 11 Pro devices offer automatic activation of features that cut down on constant troubleshooting, leaving more time for proactive system enhancements. Coupled with a reduction in helpdesk requests,[9] they allow IT teams to focus on implementing new technologies and strategies, rather than putting out fires.

Employees: A smoother workday

Windows 11 Pro devices provide a user-friendly, secure work environment that adapts to any working style. With built-in advanced security features, employees can confidently focus on work, knowing that data and systems are protected.

A leap forward in deployment, provisioning, and security

The implementation of Windows 11 Pro devices not only accelerates the deployment and provisioning process but also offers robust protection for both devices and the applications integral to today's business operations.

The seamless integration of hardware and software reduces the need for extensive hardware checks and compatibility assessments. This efficient deployment process is reportedly up to 25% faster.[9]

> **Up to a 25%** efficiency gain reported when deploying Windows 11 Pro devices.[9]

Technologies such as **Microsoft Intune**,[5] **Microsoft Entra ID**,[23] and **Windows Autopilot**[24] simplify device provisioning, configuration management, and software updates across the organization, helping to reduce expenses and improve compliance. Windows Autopilot also enhances efficiency by allowing zero-touch deployment of preconfigured devices to remote employees, resulting in significant time and cost savings.

Windows 11 Pro key benefits

Businesses: The platform for business innovation

By combining Windows 11 Pro devices with modern cloud management, organizations can strengthen security, unlock new efficiencies, and enable business anywhere.

IT teams: Streamline device management

Windows 11 Pro devices simplify the IT management process, cutting down on time-consuming hardware checks and compatibility assessments. By implementing Windows 11 Pro devices with an MDM solution,[5] IT teams can accelerate the onboarding process and reduce the need for manual intervention.

Employees: Quickly enable and update devices

Windows 11 Pro devices can be regularly and quickly updated, leading to quicker deployment and more robust application security. With devices ready for zero-touch deployment, employees can dive into work without delay.

Protection that elevates employees and accelerates business success

As cyberthreats continue to increase in scale and sophistication, IT leaders need solutions that not only strengthen protection but also enhance productivity. Those solutions must be easy to implement and compatible with the organization's existing technologies. In short, the most effective protection shouldn't slow down the business; it should accelerate it.

That's why Windows 11 Pro PCs are engineered for both security and business transformation. Powerful protection by default and industry-leading AI bring out the best in employees, make ingenuity their default state, and empower them to work and thrive anywhere. And the less time IT leaders spend on threat mitigation, the more time they have for strategic initiatives.

When technology protects the organization, supercharges every employee, and frees up IT teams to focus on growth and innovation, businesses win.

With powerful protection by default, you can accelerate success by:

Safeguarding business data with end-to-end security management for a reported **3.1x** reduction in firmware attacks.[1]

Adopting the most secure Windows ever with layers of security already enabled for a reported **58%** drop in security incidents.[1]

Protecting against evolving threats with the latest safeguards for a reported **2.8x** reduction in instances of ID theft.[1]

Deploying a streamlined, chip-to-cloud security solution that boosted IT team productivity by a reported **25%.**[9]

Discover Windows 11 Pro devices

Explore the world of Windows 11 Pro devices, designed to cater to all business needs. From innovative 2-in-1 devices and sleek, lightweight laptops to high-powered workstations, there's a Windows 11 Pro device for every role in your organization. Learn how you can upgrade to Windows 11 Pro today with qualifying devices.

Act soon

Out-of-date devices increase vulnerability, and end of support for Windows 10 is coming soon on October 14, 2025.[25] Upgrading to Windows 11 Pro will give you the latest security features, while ensuring you're supported and up to date. Move to Windows 11 Pro devices before support ends for Windows 10 on October 14, 2025. Get started now to optimize deployment and benefit from the latest features, including Copilot in Windows.

View Windows 11 Pro devices

Sources and acknowledgments

1. SMB Windows 11 Survey Report. Techaisle, February 2022. Windows 11 results are in comparison with Windows 10 devices.
2. Microsoft Digital Defense Report 2022, Microsoft.
3. Copilot in 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. Microsoft Digital Defense Report, Microsoft, 2023.
5. Sold separately.
6. Microsoft 365 subscription required; sold separately.
7. Hardware dependent.
8. 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.
9. 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.
10. Microsoft New Future of Work Report 2022, Microsoft.
11. Compared to Windows 10 devices. Principled Technologies, "Improve your day-to-day experience with Windows 11 Pro laptops," February 2023.
12. Innovation vs. risk: IT leaders share security concerns regarding tech innovation, but can they afford to let risk hold them back? HPE, September 2023.
13. Predictions 2023: Security Pros Face Greater Internal Risks, 2022, Forrester.
14. CIO, Burnout: An IT epidemic in the making, November 2023
15. Introducing Microsoft Security Copilot: Empowering defenders at the speed of AI, Microsoft, March 2023.
16. In a Hybrid World, Your Tech Defines Employee Experience, 2022, Harvard Business Review.
17. Digital Workplace Trends To Watch Out For In 2023, 2022, Forrester.
18. 2023 Global Employee Experience Trends Report, NTT DATA, Inc.
19. 2022 Windows 11 Security Book: Powerful security from chip to cloud.
20. Windows Update for Business works with Microsoft Entra ID, sold separately.
21. Battery life varies based on settings, usage, device and other factors.
22. App Assure program data.
23. Enabled, eligible Microsoft 365 license required; sold separately.
24. Requires Microsoft Intune and Entra ID; sold separately.
25. Blog: Plan for Windows 10 EOS with Windows 11, Windows 365, and ESU. Learn more.