



Overcoming today's escalating cyberthreats

with new Windows 11 Pro devices
and a security-by-default strategy

Table of contents

Securing every opportunity	3
Navigating cybersecurity threats	4
How working styles influence device and OS needs	5
Three risk factors in the modern era of work	7
Windows 11 Pro PCs: Layers of protection for modern business	11
Windows 11 Pro PCs: Securing tomorrow's work landscape	13
Securing the future of work	20
Sources and acknowledgements	21

Securing every opportunity

The ever-evolving security threat landscape is creating challenges on a scale previously unseen. Organizations are grappling with complex threats such as phishing, ransomware, and distributed denial of service (DDoS) attacks. These threats are continuing to escalate, demanding increasingly robust defenses.

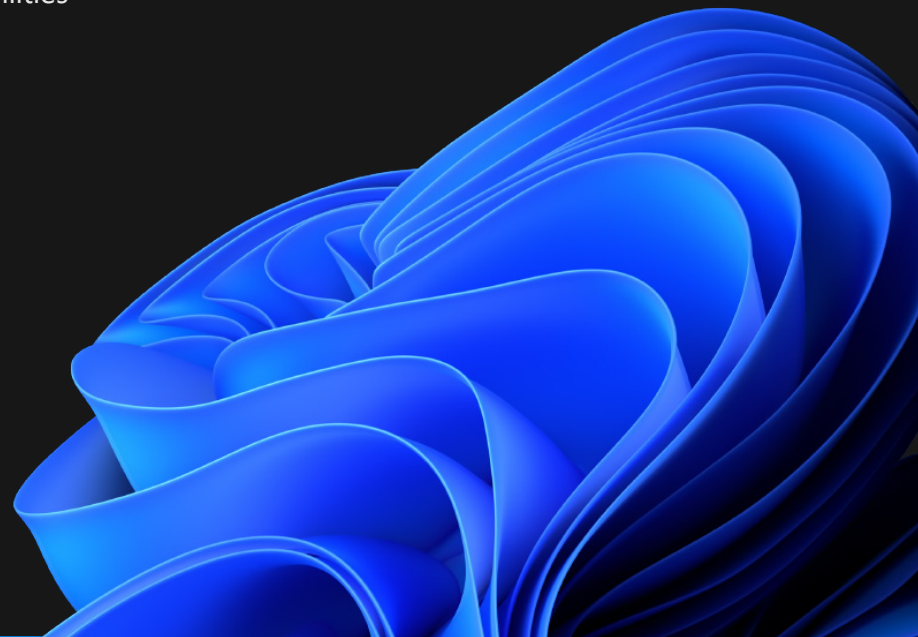
Human error adds complexity to this challenge, accounting for 46% of all cybersecurity incidents.² Add to this the rise of diverse work styles and flexible work environments and the risk is substantially amplified, broadening the potential points of vulnerability.

Yet businesses cannot let security concerns hinder business growth—opportunities must be secured at every turn. In response, a global movement toward “secure-by-default” measures is gaining momentum. Organizations are minimizing their attack surface by implementing solutions designed to prevent threats before they happen. This proactive approach minimizes vulnerabilities and reduces the likelihood of breaches.

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

Secure by design and secure by default, Windows 11 Pro is the most defended Windows ever, building on Microsoft’s commitment to empower organizations in today’s multifaceted threat environment.

Read on to learn about the current cybersecurity landscape and the growing diversity of work styles and environments. Explore how these trends are both driving innovation and introducing new security challenges. Then find out how Windows 11 Pro devices, built with a security-first perspective, offer default protection and chip-to-cloud security design to enable organizations to improve their security posture and proactively mitigate risk.



Navigating cybersecurity threats

Rapid digital transformation, combined with shifting job preferences, has resulted in a radical rethinking of the traditional workplace. The increased flexibility of modern work presents a complicated and challenging cybersecurity environment, as employees seek seamless experiences to collaborate and maintain productivity from anywhere.

Startlingly, 23% of organizations have faced a cybersecurity incident,³ nearly half enabled by human or staff errors.² This underscores the need for both technology-based defenses as well as a strong security hygiene.

The data highlights some alarming trends: Microsoft's internal data reflects an almost threefold increase in the number of password attacks in the past year—now at 4,000 per second.⁴

There are also more than 101 million daily phishing attacks,² a 130% annual increase in ransomware threats,⁵ and a continuous surge of DDoS attacks, with nearly 2,000 occurrences daily² (rising by 40% each year²). Collectively, these trends threaten to disrupt services and business operations.

We must be clear: The battle is not merely against external threats, but a clarion call for a robust security awareness within organizations. A comprehensive approach to cybersecurity is essential, where human awareness, vigilance, and technology synergize to safeguard present and future organizational operations. Understanding how diverse and emerging work styles can modify security risk profiles is also critical.


The deployment of Windows 11 Pro PCs represents a significant advancement, relieving employees of the burden of worrying about security wherever they work, while providing organizations with the means to strengthen their security posture amid these relentless threats.


 **23%**


of businesses have experienced a cybersecurity incident³

 **46%**

of all cybersecurity incidents caused by human/staff error²

 **345M+**
password attacks/day⁴

 **101M+**
phishing attacks/day²

 **130%**
increase in ransomware attacks year-on-year⁵

 **1,955**
DDoS attacks/day²

40%
increase in DDoS attacks year-on-year²

How working styles influence device and OS needs

Microsoft, in collaboration with LinkedIn and GitHub, has conducted its most extensive research project to date, the “New Future of Work” initiative. This research unveils critical insights into the role of new devices and operating systems in shaping the future of work and combatting an ever-evolving cybersecurity landscape.

Flexible work styles and locations are becoming more prevalent, reflecting a shift that encompasses not only market trends but also genuine employee preferences. 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.⁶

These emerging work dynamics bring new security challenges, especially in flexible work environments. Yet, as work and technology continue to evolve together, better practices can enhance productivity. The adoption of modern devices can lead to not only more effective meetings and strategic management but also broader productivity 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 artificial intelligence (AI), including Windows Copilot and Microsoft 365 Copilot,⁷ in transforming the work landscape is becoming increasingly prominent. 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, constructed with a secure-by-design framework, 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, designed with enhanced security measures and user-centric features, addresses these concerns. It enhances employee satisfaction and well-being by providing an accessible, intuitive user experience and robust defenses against emerging cybersecurity threats.



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.

Working seamlessly with Microsoft Teams, Windows 11 Pro's comprehensive security suite safeguards activities, while its smart videoconferencing features—like intelligent noise canceling, background blur, and the ability to share files and mute/unmute from the taskbar—make collaboration easier. Snap layouts also make staying organized between work locations a breeze.



Influence on the broader organization

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

Windows 11 Pro emerges as a vital asset, enabling secure communication across various work environments, providing system-wide protection, and ensuring continuity in operations.



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

95% of CIOs indicated that their role was expanding beyond traditional IT responsibilities.⁸

71% of CIOs are creating more diverse and inclusive teams to drive new thinking, with **38%** investing in modern technology to drive business innovation.⁹

Outdated systems and devices can inhibit an organization's ability to innovate and compete in a rapidly evolving business environment. Aging technology often fails to support advanced applications and services, hindering adoption of transformative technologies.

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?
- What are the costs of system downtime due to aging hardware and software?
- 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.**¹⁰

Only **29.1%** of IT employees have high intent to remain with their current employer, **10.2%** lower than non-IT workers.¹¹

The average cost of a data breach for enterprise companies is **USD 4.45 million.**¹²

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.

Considerations for leaders:

- What percentage of IT resources is spent on maintaining aging devices, and how does this impact strategic focus?
- Are our older systems compatible with modern IT management tools for security and compliance?
- 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.¹³

60% of technology and business leaders indicate that improving employee experience is a top IT priority.¹⁴

Companies with a strong tech-related employee experience report a **25% higher profit** than those with a weaker tech experience.¹⁵

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. The increased risk from cyberthreats, as older systems are softer targets, can lead to sensitive data breaches, further undermining employee confidence and causing reputational damage.

Considerations for leaders:

- 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?
- What are the financial and reputational costs of a data breach involving sensitive employee and customer data?

Preparing for the artificial intelligence era

As the “New Future of Work” evolves, AI becomes a guiding force.

Advancements in foundational language models, breakthroughs in AI technology, and the digital transformation ignited by the pandemic place organizations at a pivotal crossroads. Never has there been a more consequential opportunity to reshape the way we work.

Organizations at the forefront of the AI revolution are now asking: How can AI help us overcome our innovation barriers, ease strained IT resources, and boost employee confidence and productivity? The answer is becoming clear.

With Windows 11 Pro, Microsoft has embarked on this path. The introduction of Windows Copilot with Bing Chat Enterprise brings intelligent tools together in your desktop, for easy, secure access to AI at work. This feature has immense potential to enhance productivity, paving the way for AI-infused experiences that transform Windows applications across cloud and edge.

Switching to Windows 11 Pro devices can be the catalyst that enables organizations to adeptly steer through the complex currents of the next work era. By leveraging AI’s transformative power, organizations are not just adapting to the future of work but also actively shaping it, tapping into the vast potential that this innovative technology offers.



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.¹⁶ Building upon Windows 10's 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 (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 Intune¹⁷ to manage their devices are now able to configure App Control for Business in the admin console, including setting up Intune¹⁷ as a managed installer.

To 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 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 features give peace of mind when stepping away with lock on leave and wake on approach capabilities.¹⁸



Connecting to cloud services

Windows Update for Business 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.¹⁷ 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.⁷ By meeting the contemporary requirements for security and flexibility, Windows 11 Pro modern PCs, paired with Microsoft 365 Business Premium,⁷ 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 adapt to a transformative work landscape, they need a platform that unites robust security, effortless management, and diverse work style 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 dynamic 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, shield against risks, and gain the momentum to grow. This prepares them to excel in a constantly evolving business landscape.



More security. Less cost.

Security out-of-the-box

Windows 11 Pro ensures robust security at every level, achieving a 3.1x reduction in firmware attacks.¹ Multiple layers of protection, including hardware-backed credential protection with TPM 2.0 and VBS for enhanced kernel protection, are built-in and enabled by default.

Stay ahead of evolving threats

Features including enhanced phishing protection with Microsoft Defender SmartScreen resulted in a reported 2.8x reduction in identity theft.¹ Additionally, Windows Hello enables passwordless sign-in, enhancing ease of use and security. Windows Presence features safeguard you with lock on leave and wake on approach. The built-in vulnerable driver block list, enabled by default, wards off potential risky drivers.

Mission-critical app protection

By running Windows desktop applications in a separate environment through Win32 apps in isolation, Windows 11 Pro provides added protection against malware. The use of AppControl for Business (previously called Windows Defender Application Control), coupled with modern device management, helps ensure that only trusted applications run on devices.

End-to-end protection, simplified

Utilizing Windows 11 Pro's streamlined chip-to-cloud security, organizations can protect system access through Intune Endpoint Privilege Management (EPM)¹⁷ and enable secure employee access to content on unmanaged devices using Mobile Application Management (MAM) for Windows. Moreover, Windows 11 Pro ensures robust security with features like token protection for sign-in sessions and automation of local admin password account management through the Local Administrator Password Solution (LAPS) with Microsoft Entra (previously Azure AD) in public preview.

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**, 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, 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 demonstrated.¹⁹

Up to a 20% reduction
in the chance of successful
security attacks with
Windows 11 Pro devices.¹⁹

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 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.²⁰

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 of the Windows interface ensures an uninterrupted workflow, contributing up to a 15% productivity increase with Windows 11 Pro devices.¹⁹

Windows 11 Pro devices also offer enhancements such as up to 61% longer battery life,^{20,21} responsive performance, and capabilities to support high-quality presentations on multiple 4K monitors. Various working modes enabled by peripherals, including pen, ink, touch, or voice¹⁸ 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 are also 99.7% app compatible, making it easy to use printers, displays, and other hardware.²² 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,^{20,21} 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, 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**, 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.¹⁹

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.¹⁹ 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.¹⁹

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, keeping sensitive data safe. These systems result in an impressive productivity boost of up to 20%.¹⁹

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 and, coupled with a reduction in helpdesk requests,¹⁹ allowing 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.¹⁹

Up to a 25% efficiency gain reported when deploying Windows 11 Pro devices.¹⁹

Technologies such as **Microsoft Intune**,¹⁷ **Microsoft Configuration Manager**, and **Windows Autopilot** simplify device provisioning, configuration management, and software updates across the organization, helping to

reduce expenses and improve compliance.²³ Windows Autopilot also enhances efficiency by allowing zero-touch deployment of preconfigured devices to remote employees, resulting in significant time and cost savings.²³

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, 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.

Securing the future of work

To thrive in today's competitive marketplace, success hinges on aligning strategy, resilience, and innovation. The deployment of Windows 11 Pro devices stands as a key strategic initiative, not merely as an IT security solution, but also as a robust platform that fuels organizational growth.

Facing an unpredictable and dynamic cyberthreat landscape, Windows 11 Pro is designed with security at its core, implementing the robust principles of security-by-default and security-by-design. The control it offers IT administrators is not just powerful; it's precise, coupled with the flexibility to craft a technology environment that meets your unique organizational needs. For employees, it's an assurance of unparalleled hardware-based security with the freedom of passwordless protection, fostering seamless integration with any work style.

With Windows 11 Pro devices, organizations can not only benefit from a potential reduction in cybersecurity incidents; they can also increase productivity and collaboration and unburden their IT infrastructure. With end-to-end protection, effortless support for flexible workforces, and innovative technology that accelerates workflows, Windows 11 Pro enables businesses to secure any opportunity.

Assess your cybersecurity risk

Evaluate your business's device risk profile with our **Interactive Landscape and Risk Profiler**. Glean insights into your current cybersecurity state and the transformative potential of Windows 11 Pro to strengthen your defenses and reduce risk.

[Start assessment >](#)

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.

[View Windows 11 Pro devices >](#)

Sources and acknowledgements

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. Microsoft Research: Security in the New Working Environment, 2022.
4. [Microsoft Security, Microsoft Entra expands into Security Service Edge and Azure AD becomes Microsoft Entra ID](#), Joy Chik, July 11, 2023.
5. [Microsoft Security, Protect your organization from ransomware](#), accessed September 11, 2023.
6. [Microsoft New Future of Work Report 2022](#), Microsoft.
7. Subscription required.
8. CIO from IDG, 2020 State of the CIO.
9. IDG, 2021 State of the CIO.
10. [Predictions 2023: Security Pros Face Greater Internal Risks](#), 2022, Forrester.
11. [Gartner Global Labor Market Survey, 2022](#), Gartner.
12. [IBM Cost of a Data Breach Report, 2022](#), IBM.
13. [In a Hybrid World, Your Tech Defines Employee Experience](#), 2022, Harvard Business Review.
14. [Digital Workplace Trends To Watch Out For In 2023](#), 2022, Forrester.
15. [Building Business Value with Employee Experience](#), 2017, MIT Center for Information Systems Research.
16. [Security Signals](#), March 2021, Microsoft and Hypothesis Group.
17. Microsoft Intune sold separately.
18. Hardware dependent.
19. [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.
20. Compared to Windows 10 devices. Improve your day-to-day experience with Windows 11 Pro laptops, Principled Technologies, February 2023.
21. Battery life varies based on settings, usage, device and other factors.
22. App Assure program data.
23. Autopilot requires Microsoft Intune and Microsoft Entra ID (formerly Azure Active Directory). Sold separately.