Windows

Windows 11 security guide: Start secure, protect what matters, prepare for AI

Introduction

Businesses are under pressure to work smarter, move faster, and do more with their time, technology, and talent. They are modernizing operations, connecting business processes, and finding more efficient ways to get work done. Hybrid intelligence, the ability to run AI locally and in the cloud, gives organizations flexibility to adopt solutions tailored for unique business needs. Today, hybrid intelligence and new agent experiences can help streamline workflows and create new opportunities for growth.

At the same time, IT teams manage an increasingly complex environment that can include physical and cloud-based PCs, servers, networks, diverse applications, human and agent identities, and data spread across geographies. Work moves daily across this environment, while attackers look for gaps between systems and controls. Their targets include human and agent identities, applications running on devices or in the cloud, and sensitive business and personal data.

As AI changes how work gets done and how threats evolve, the fundamentals of security matter more than ever. Resilient organizations need technology they can trust, including the ability to protect identities and data and enforce security policies at scale. Those requirements become even more important as companies automate business processes and give agents greater access and responsibility.

Windows is the execution layer at the heart of this security foundation. Windows is where people sign in, applications run, and data is accessed and transformed. Windows turns security policies into protection enforced on the endpoint, helping organizations start secured, stay secured, and protect what matters wherever work happens. Windows also enables organizations to extend those principles to new ways of working, including the automation and orchestration of complex workflows with agents.

Businesses run on Windows, the security foundation for endpoints and AI.

Build on a secure foundation

Security begins before an application launches, or an agent starts a task. Organizations need confidence that the endpoints they rely on start in a secure state and continue to operate as intended.

Establish hardware-backed root of trust

Modern attacks can target credentials, firmware, and critical system components, as well as the operating system. Windows integrates hardware and software to help establish and verify device integrity and protect sensitive operations.

Built-in protection on Windows 11 PCs includes Trusted Platform Module (TPM) 2.0, secure boot, virtualization-based security, and hypervisor-protected code integrity working together to establish a strong security foundation. On supporting devices like Copilot+ PCs, the Microsoft Pluton security processor provides an additional layer of hardware-backed protection. Pluton is integrated directly into the CPU to strengthen protection for sensitive information, including encryption keys and credentials.

Make protection part of the platform

Businesses should not have to assemble fundamental endpoint protections piece by piece. Windows includes layers of protection by default to protect credentials, applications, and the operating system from common and emerging attack techniques.

Microsoft Defender Antivirus, Microsoft Defender SmartScreen, Credential Guard, and App Control for Business are examples of protections built into Windows rather than added as an afterthought.

This integrated approach can also simplify the work of IT. A consistent platform foundation provides a clearer starting point for establishing security policies, deploying devices, and maintaining security over time. It also enables organizations to put AI to work at scale with confidence, optimizing potential while minimizing risk.

Protect identity from the first sign-in

Cyber risk is accelerating, and many attacks start with a compromised identity.[1] Reducing dependence on passwords can limit credential exposure while improving the sign-in experience. Windows Hello for Business, passkeys,[2] and supported phishing-resistant authentication methods help businesses protect access without creating unnecessary friction for employees.

Windows Hello is designed to enable fast, dependable sign-in wherever people work. Enhancements such as PIN after reboot, the coordinating biometric recognition and PIN entry option, and adaptive screen brightness[3] help deliver a more consistent sign-in experience across restarts, devices, and environments.

Windows Hello works with Microsoft Entra ID[4] to support phishing-resistant authentication with passkeys based on FIDO standards. IT admins can use Windows Hello for Business policies in management solutions like Microsoft Intune[4] to manage PIN requirements and other authentication settings. Passkeys can be safeguarded by Windows Hello or an external security key. By replacing passwords and one-time codes with public-key cryptography, passkeys help prevent credentials from being captured or replayed through phishing. Together, these capabilities help organizations strengthen identity protection while providing a simpler sign-in experience across managed Windows devices.

Secured foundation at a glance

- Hardware-rooted protection and platform integrity
- Built-in protection against common attack paths
- Passwordless and phishing-resistant authentication

Maintain security across the organization

Establishing a secure state is only the beginning. Devices change. New applications and emerging technologies enter the workplace. Employees move between locations. Servers and cloud services scale to support critical workloads. Policies and business requirements change, and so do cyberthreats. Maintaining security means continuously managing, verifying, updating, remediating, and, when necessary, recovering that environment.

Windows, especially when managed with Microsoft Intune or other management solutions, offers a consistent way to manage protection across this changing environment without getting in the way of productivity. Built-in management capabilities help Windows endpoints connect to cloud-based services such as Microsoft Intune and Microsoft Entra ID, allowing IT admins to apply and maintain security policies at scale. Automated update processes with Windows Autopatch and hotpatch help keep security protections current while minimizing restarts and disruption.[5]

Keep policy and configuration aligned and consistent

Windows works with Microsoft Intune to help organizations configure, deploy, and maintain security policies across managed physical endpoints and Windows 365 Cloud PCs.[4]

Managed in the Microsoft 365 Admin Center,[4] Windows baseline protection (preview)[6] brings together core Windows protections – like secure boot, virtualization-based security and memory integrity – into one state that is easily verified across devices.

Organizations can then maintain a strong security baseline with Windows declared configuration,[7] which helps keep devices in an IT-defined state by monitoring settings and correcting configuration drift.

The business value is straightforward: less time spent correcting avoidable inconsistencies, a more predictable employee experience, and clearer control across a distributed fleet. Together, these capabilities make the desired state easier to define, apply, monitor, and maintain.

Protect identity, access, and data

Employees need secure, reliable access to the information and tools they need, while IT needs to protect identities, control access, and safeguard sensitive data. Windows works with Microsoft Entra, Microsoft Intune, Microsoft Defender, and Microsoft Purview[8], so organizations can use each solution to help manage identity and access, device management, threat protection, and data protection.

Organizations can apply access policies based on identity, device state, and risk, while extending protection to the data people access and create. BitLocker helps protect data on lost or stolen devices through full-volume encryption, while TPM-based protection helps verify the integrity of the device during startup. New support for configuring BitLocker with TPM + PIN[8] for standard users through Microsoft Intune adds another authentication layer before Windows starts, strengthening pre-boot protection.

Combined with least-privilege approaches and Microsoft Purview data security and governance capabilities, these protections help safeguard sensitive information across physical and cloud-based work environments.

Generate the signals to detect and respond to threats

Windows provides endpoint telemetry, security signals, logging, and audit information. Microsoft Defender uses relevant signals to help detect, investigate, and respond to threats in real time. Together, these capabilities give organizations greater visibility into potential threats and help them respond more quickly.

Maintaining security at a glance

- Keep policy and configuration aligned
- Protect identity, access, and data
- Use device health signals to inform access and compliance decisions

Build resilience and keep work moving

Strong security is about more than prevention. Businesses also need to keep operations running, limit the impact of disruption, and recover with less manual effort. A failed update, configuration problem, device issue, or security

incident can interrupt productivity and stall important workflows well beyond the affected endpoint. For example, servers host applications, data, and services that many business workflows depend on. Building resilience therefore requires protection across Windows PCs, servers, identities, and cloud services, with controls appropriate to each part of the environment.

Reduce the risk of exposure

Keeping Windows current helps reduce exposure to known vulnerabilities and supports a consistent operating environment. Windows Autopatch provides options for orchestrating updates across supported devices.[9] Recent enhancements add additional control and visibility, both for updates and what those updates contain. Windows Autopatch also covers Windows Servers, making it easier to keep updated using the same tools. With tools like Intune Enterprise Application Management, organizations are better able to discover and deploy applications and keep them up to date.

Recover when a device cannot start or comply

When a device cannot start or no longer meets policy, IT needs a practical way to contain the issue and restore service. Capabilities such as Quick Machine Recovery[10] and remote device actions can support response and recovery. These capabilities can help reduce downtime and the need for hands-on intervention.

Restore devices and keep work moving

Recovery is also about restoring the employee experience and keeping work moving. Windows settings backup and restore,[11] Cloud Rebuild (preview),[12] point-in-time restore,[8] and Windows 365 continuity[8] options can help businesses restore devices, settings, or access to work, subject to availability and applicable requirements.

With point-in-time, organizations can minimize downtime by rolling a Windows PC back to an earlier working state, including the OS, apps, settings, and local files. If a physical device is lost, damaged, or otherwise unavailable, Windows 365 Reserve[8] helps maintain business continuity by enabling people to continue working from a Cloud PC.

Faster recovery can help employees return to work sooner, reduce operational disruption, and give IT a clearer path forward when an incident occurs.

Building resilience to ensure business continuity

- Reduce window of exposure
- Recover devices
- Restore productivity

Apply security principles to AI

Businesses are rethinking workflows, automating routine processes, and looking for ways to make better use of information. Agents can support this shift by researching information, coordinating tasks, interacting with applications, and helping complete multi-step business processes. The value is not the technology itself. It is the ability to reduce manual effort, improve insights and accuracy, accelerate results, and help people focus on higher-value work.

Apply familiar security principles to agents

As agents gain access to information, tools, and business systems, organizations need to know what they can access, what actions they are authorized to take, and how their activity can be audited and reviewed. Identity, scoped permissions, policy, visibility, governance, audit, and human approval, where appropriate, help extend established security practices to agents as a new class of workload.

Some organizations may find that following a Zero Trust model also works for securing their agents: verify explicitly, use least privilege, and assume breach. With Microsoft Agent 365[8] and Microsoft security solutions, organizations can enable agents to act while enforcing identity, isolation, policy, and oversight.

Contain execution and limit impact

Windows has long used isolation and containment to separate code execution, isolate specific workloads, and reduce unnecessary access. Those principles can also extend to agent workloads. Process, session, and cloud-hosted boundaries can be matched to the workload and scenario, with policy and access decisions flowing to the execution environment and relevant security and audit signals flowing back to connected services.

Microsoft Execution Containers (MXC)[13] help organizations contain apps and agents, and limit the resources they can access. Working with management and security solutions such as Microsoft Intune, MXC provides flexible containment options based on workload needs, access requirements, and the appropriate level of separation.

Containment can help limit the impact of compromise and make response more manageable for agents, just as it does other executable code. For agents, this gives organizations greater control over where activity runs, what resources it can reach, and how that activity can be monitored.

Prepare for changing threats and requirements

The threat landscape will continue to change. Windows continues to advance hardware-backed security, platform protections, cryptographic capabilities, and support for emerging standards. Post-quantum cryptography is one example of work that helps organizations prepare for future risk, including the transition of applications, protocols, and data protection practices over time.

Organizations cannot predict every new threat or new way of working. They can build on a security foundation designed to anticipate and evolve with both. Windows combines built-in protections and on-device controls with Microsoft security and management solutions to help organizations establish a secure state and maintain it as conditions change, and apply established security principles as AI becomes part of everyday work.

Applying security principles to AI

- Give agents scoped identities and permissions
- Contain execution and limit impact
- Maintain visibility and human oversight
- Prepare for changing threats and requirements

Windows security architecture at a glance

Windows security brings together protections across layers of the technology stack, from the security foundation and hardware through the operating system, applications, identity, and cloud services. Privacy protections span these layers. Within each layer, capabilities are organized around the security outcomes they support.

Security foundation. Security begins with how Windows is engineered, validated, and delivered through **secure engineering and research, certification, and secure supply chain**.

Hardware. Hardware-backed protections establish foundational device trust and help isolate sensitive operations through **hardware root of trust and silicon-assisted security**.

Operating system. Built-in security **protects** Windows as it starts, runs, connects, stores data, and is managed. These span **system integrity, driver security, built-in threat protection, network security, encryption and data protection, and device management**.

Application and agentic security. Built-in protections help control what can run, contain applications and workloads, and establish security boundaries for agents through **control, containment, and security**.

Identity. Identity protections help people securely prove who they are and protect the credentials and tokens used to access resources through **passwordless sign-in and advanced credential protection**.

Cloud. Cloud-connected services extend Windows security and management beyond the physical device by **centrally managing endpoints and security policies, protecting work and personal information, and providing cloud-based PCs**.

Explore the security capabilities

Each area of the Windows security architecture is supported by individual security features and services. The detailed view below shows where these capabilities fit across the architecture.



Learn more about Windows security

Windows security documentation on Microsoft Learn builds on this guide with deeper technical guidance across hardware-rooted security, identity protection, application security, device management, data protection, recovery, and other Windows security capabilities.

Windows

Thank you.

[1] Microsoft Digital Defense Report 2026 – Executive Summary
[2] The passkey can be saved locally to the Windows device and authenticated via Windows Hello or Windows Hello for Business. Hardware dependent.
[3] Hardware dependent
[4] Sold separately
[5] Requires Microsoft 365 Business Premium or other eligible license. Managed via Microsoft Intune (may be sold separately). Learn more.
[6] Feature in preview. Availability, features and timing subject to change. Hardware and software requirements may apply.
[7] Requires Microsoft Intune, sold separately. Availability, features and timing subject to change. Learn more about declared configuration.
[8] Additional licensing, subscriptions, and/or usage charges may apply. Learn more about licensing.
[9] Additional licensing, subscriptions, and/or usage charges may apply. Learn more about Autopatch and hotpatch.
[10] Additional licensing, subscriptions, and/or usage charges may apply. Learn more about quick machine recovery.
[11] Microsoft Entra ID required, sold separately. Learn more about Windows settings backup and restore.
[12] Feature in preview. Availability, features and timing subject to change.
[13] Availability, features and timing subject to change. Additional licensing, subscriptions, and/or usage charges may apply. Learn more about MXC.

Published November 2026