

Windows 10 commercial edition comparison

Windows 10
Home

Windows 10
Pro

Windows 10
Pro for Workstation

Windows 10
E3

Windows 10
E5

Intelligent Security

Threat protection (Windows Defender Advanced Threat Protection)

Attack Surface Reduction	Windows 10 Home	Windows 10 Pro	Windows 10 Pro for Workstation	Windows 10 E3	Windows 10 E5
Integrity enforcement of operating system boot up process	●	●	●	●	●
Integrity enforcement of sensitive operating system components	●	●	●	●	●
Advanced vulnerability and zero-day exploit mitigations	●	●	●	●	●
Reputation based network protection for Microsoft Edge, Internet Explorer and Chrome	●	●	●	●	●
Host based firewall	●	●	●	●	●
Ransomware mitigations	●	●	●	●	●
Hardware based isolation for Microsoft Edge		●	●	●	●
Application control powered by the Intelligent Security Graph		●	●	●	●
Device Control (e.g.: USB)		●	●	●	●
Network protection for web-based threats				●	●
Enterprise management of hardware-based isolation for Microsoft Edge				●	●
Host intrusion prevention rules				●	●
Customizable allow/deny lists (e.g.: IP/URL, Files, Certificates)					●
Device-based conditional access					●

Windows 10 commercial edition comparison

	Windows 10 Home	Windows 10 Pro	Windows 10 Pro for Workstation	Windows 10 E3	Windows 10 E5
Centrally manageable tamper protection of operating system					●
Next Generation Protection	●	●	●	●	●
Pre-execution emulation executables and scripts	●	●	●	●	●
Runtime behavior monitoring	●	●	●	●	●
In memory anomaly and behavior monitoring	●	●	●	●	●
Machine learning and AI based protection from viruses and malware threats	●	●	●	●	●
Cloud protection for fastest responses to new/unknown web-based threats	●	●	●	●	●
Protection from fileless based attacks	●	●	●	●	●
Advanced machine learning and AI based protection for apex level viruses and malware threats					●
Advanced cloud protection that includes deep inspection and detonation					●
Emergency outbreak protection from the Intelligent Security Graph					●
Monitoring, analytics and reporting for Next Generation Protection capabilities					●

Windows 10 commercial edition comparison

	Windows 10 Home	Windows 10 Pro	Windows 10 Pro for Workstation	Windows 10 E3	Windows 10 E5
Endpoint Detection and Response					●
Behavioral-based detection for advanced and targeted attacks (post-breach)					●
Centralized security operations management with Windows Defender Security Center					●
Rich investigation tools					●
Forensic collection					●
Response actions					●
Advanced detonation service with deep file analysis					●
Upload of Indicators of Compromise (IOC) for custom alerts					●
Flexible hunting queries over historical data					●
Custom alerts via powerful advanced hunting queries					●
Discover and report SaaS app usage to MCAS					●
Machine risk level to trigger conditional access					●
Monitoring, analytics and reporting					●
Automatic Investigation and Remediation					●
Automated alert investigations using Artificial Intelligence					●
Automated remediation of advanced threats					●
Monitoring, analytics and reporting					●

Windows 10 commercial edition comparison

	Windows 10 Home	Windows 10 Pro	Windows 10 Pro for Workstation	Windows 10 E3	Windows 10 E5
Security Score				●	●
Assess and improve your organization security posture using Microsoft Secure Score for Windows				●	●
Threat Analytics shows your organizations exposure to threats				●	●
Security Management					●
Monitoring, analytics and reporting					●
Rich Power BI dashboards and reports					●
Enterprise-grade Extensibility and Compliance					●
Integrated endpoint protection for 3rd party platforms (macOS, Linux, iOS, Android)					●
Open Graph APIs to integrate with your solutions					●
Integration with Microsoft Advanced Threat Protection (ATP) products					●
ISO 27001 compliance					●
Geolocation and sovereignty of sample data					●
Sample data retention policy					●

Windows 10 commercial edition comparison

Windows 10
Home

Windows 10
Pro

Windows 10
Pro for Workstation

Windows 10
E3

Windows 10
E5

Identity and access control

Multi Factor and password-less Authentication¹

Industry standards based multifactor authentication

Support for biometrics (Facial and Fingerprints)

Support for Microsoft Authenticator

Support for Microsoft compatible security key

Supports for Active Directory and Azure Active Directory

Credential Protection

Hardware isolation of single sign-in tokens

Centralized management, analytics, reporting, and operations



Windows 10 commercial edition comparison

Windows 10
Home

Windows 10
Pro

Windows 10
Pro for Workstation

Windows 10
E3

Windows 10
E5

Information protection

Full Volume Encryption²



Automatic encryption on capable devices



Advanced encryption configuration options



Removable storage protection



Direct Access & Always On VPN device Tunnel



Centralized BitLocker management (key recovery, reporting, enforcement) and enforcement



Data Loss Prevention³



Personal and business data separation



Application access control



Copy and paste protection



Removable storage protection



Integration with Microsoft Information Protection



Windows 10 commercial edition comparison

Windows 10
Home

Windows 10
Pro

Windows 10
Pro for Workstation

Windows 10
E3

Windows 10
E5

Flexible management

Deliver enterprise-ready devices

Windows Autopilot⁴

User-driven mode

Self-deploying mode

For existing devices

Remote reset

Local reset

Forced enrollment

Windows Subscription Activation⁵

Simplify device management

Device Management

Industry standards based MDM

Kiosk mode⁶

Active Directory Join

Azure Active Directory Join

● ● ● ●

● ● ● ●

● ● ● ●

● ● ● ●

● ● ● ●

● ● ● ●

● ● ● ●

● ●

◐ ◐ ● ●

● ● ● ●

● ● ● ●

● ● ● ●

● ● ● ●

Windows 10 commercial edition comparison

	Windows 10 Home	Windows 10 Pro	Windows 10 Pro for Workstation	Windows 10 E3	Windows 10 E5
Hybrid Azure AD Join ⁷		●	●	●	●
Manage Start menu and Taskbar, unbranded boot, and custom login		●	●	●	●
Resilient File System			●	●	●
SMB Direct			●	●	●
Persistent Memory ⁸			●	●	●
Windows To Go				●	●
Manage Cortana				●	●
Managed Store Access				●	●
Dynamic Management				●	●
Microsoft User Experience Virtualization (UE-V) ⁹				●	●
Application Management	🕒	🕒	●	●	●
Mobile Application Management	●	●	●	●	●
Microsoft Store for Business ¹⁰		●	●	●	●
Local virtualization support		●	●	●	●
Microsoft Application Virtualization (App-V) ⁹				●	●

Windows 10 commercial edition comparison

Windows 10
Home

Windows 10
Pro

Windows 10
Pro for Workstation

Windows 10
E3

Windows 10
E5

Simplified updates

Streamline deployment and updates

	Windows 10 Home	Windows 10 Pro	Windows 10 Pro for Workstation	Windows 10 E3	Windows 10 E5
Windows as a Service					
In-place upgrades					
Express updates					
Delivery optimization					
Windows Analytics Upgrade Readiness					
Windows Analytics Update Compliance					
Windows Update for Business					
Windows Analytics Device Health					
30 months of support for September targeted releases					
Windows 10 LTSC Access					
Application compatibility					
Ready4Microsoft365.com					
Windows Insider Program for Business					
Desktop App Assure					

Windows 10 commercial edition comparison

Windows 10
Home

Windows 10
Pro

Windows 10
Pro for Workstation

Windows 10
E3

Windows 10
E5

Enhanced Productivity

	Windows 10 Home	Windows 10 Pro	Windows 10 Pro for Workstation	Windows 10 E3	Windows 10 E5
Work smarter	●	●	●	●	●
Microsoft Edge	●	●	●	●	●
Microsoft search in Windows 10 ¹¹	●	●	●	●	●
Windows user experience	●	●	●	●	●
Cortana ¹⁰	●	●	●	●	●
Cultivate collaboration	●	●	●	●	●
Office 365 on Windows	●	●	●	●	●
Nearby Sharing	●	●	●	●	●
Microsoft Whiteboard	●	●	●	●	●
OneNote for Windows 10	●	●	●	●	●
Empower workstyles	●	●	●	●	●
Work across devices ¹²	●	●	●	●	●
Accessibility	●	●	●	●	●
Windows devices	●	●	●	●	●
Windows Ink ¹³	●	●	●	●	●
3D in Windows 10	●	●	●	●	●

Windows 10 commercial edition comparison

Windows 10
Home

Windows 10
Pro

Windows 10
Pro for Workstation

Windows 10
E3

Windows 10
E5

- ¹ Windows Hello for Business with biometric authentication requires specialized hardware, such as a fingerprint reader, illuminated IR sensor, depending on the authentication method.
- ² Requires TPM 1.2 or greater for TPM-based key protection.
- ³ Windows Information Protection requires either MDM or System Center Configuration Manager to manage settings. Sold separately.
- ⁴ Requires Azure AD. Sold separately.
- ⁵ Requires Azure AD for automatic MDM enrollment. Requires Microsoft Intune for Blocking Status page. Sold separately.
- ⁶ Requires Microsoft Intune or third-party MDM service. Sold separately.
- ⁷ Requires Azure AD and Microsoft Intune, sold separately.
- ⁸ Non-volatile memory modules (NVDIMM) is required.
- ⁹ Requires either App-V Server (available at no additional cost as part of Windows 10 Assessment and Deployment Kit) or System Center Configuration Manager (sold separately).
- ¹⁰ Available in select markets. Functionality and may vary by region and device.
- ¹¹ Requires Bing for business to search across company resources and portals. Requires Office 365 subscription, sold separately, to search across OneDrive for Business and SharePoint locations.
- ¹² Users must link their mobile phone to their PC in PC settings, install the appropriate app for their device, and follow the setup prompts.
- ¹³ Touch capable device required. Pen accessory sold separately.