Deploy Windows 10 in an enterprise: Protection solutions

What IT professionals need to know to successfully implement Windows 10 protection capabilities in their enterprise environments.

Two tiers of protection for Windows 10 devices

Windows 10 includes many protection capabilities. We know it can be challenging to implement the right set of capabilities for your organization.

Our capabilities are recommended in two tiers — out-of-box protection and increased protection that you can turn on to strengthen your protections.

It's important to use consistent levels of protection across your data, identities, and devices. For example, if you turn on some of the increased protections for your data, you must also protect the identities and devices that access this data at a comparable level.

For full protection, use Windows 10 capabilities together with capabilities in Enterprise Management + Security (EMS) and Office 365. For more information, see these companion documents:

File Protection Solutions in Office 365

Identity and Device Protection for Office 365 and other SaaS Services

1 Out-of-box protection

Microsoft provides advanced security for protecting data, as well as the identities and devices that access your data. Windows 10 includes strong, out-of-the box baseline protections, which will meet the needs of many organizations. For organizations that need more protection than the baseline, there are the increased security features, which can be turned on alongside the out-of-box protections.

2 Increased protection

Some customers have a subset of users that must be protected at higher levels because they have access to sensitive data or they are greater targets for attackers. You can apply increased protection to specific users in your organization.

Summary of capabilities

Out-of-box protection

Windows Defender System Guard
Helps maintain and validate the integrity of a device's firmware, operating system, and system defenses by ensuring that only trusted software can run during start-up.

Windows Defender Exploit Guard
Includes a series automatic mitigations designed to block vulnerability exploit techniques that can let an attacker inject malicious code into a system to gain control of apps or the system itself.

Windows Defender Firewall
Protects against unauthorized access.

Windows Defender Antivirus
Uses the power of the cloud, wide-optics, precise machine learning models, and behavior analysis to protect devices from emerging threats, in real-time.

Windows Defender SmartScreen
Checks for malicious apps and sites, warning and blocking users from accessing content that could harm their devices.

BitLocker Encryption*
Auto-encrypts all data at rest on the device and protects it against offline attacks. No provisioning required.

* Only available on InstantGo devices.

Windows updates
Protects against new threats.

Increased protection

Windows Defender System Guard (with optional features enabled)
Allows sensitive services and data to be isolated, ensuring low-level tampering can be detected and remediated without impact.

Windows Defender Exploit Guard (with optional features enabled)
Uses a set of intrusion prevention capabilities to reduce the attack and exploit surface of apps; helping to prevent attacks from security threats, such as ransomware.

Windows Defender Application Guard
Malware and hacking threats encountered online while using Microsoft Edge won't be able to compromise the device, apps, data, or the broader business network.

Windows Defender Application Control
Helps address malware threats by enabling your IT department to decide which trusted software vendors and apps can run on devices.

Windows Defender Device Guard
Uses Hypervisor Code Integrity (HVCI) from Windows Defender Exploit Guard plus the "allow listing" feature from Windows Defender Application Control to provide advanced tamper-proofing for the system core and application control policies.

BitLocker Encryption
Allows provisioning of a customized encryption configuration on the broadest range of Windows device types; protecting data at rest on the device against offline attacks.

Windows Information Protection
Protects enterprise apps and data against accidental data leak on enterprise-owned devices and personal devices.

Windows Defender Advanced Threat Protection
Helps detect, investigate, and respond to advanced attacks on your networks.

Windows Defender Credential Guard
Uses virtualization-based security and Windows Defender System Guard container technology to isolate the Windows authentication stack and user secrets (such as, NTLM and TGT), so they can remain secure even if the operating system is compromised.

Windows Hello
Replaces passwords with strong two-factor authentication, providing instant access to your Windows 10 devices using fingerprint or facial recognition.

Microsoft