Comparing Security Features of Windows 7 and Windows 10

Windows 10 is built to defend you against modern threats

Windows 7 has been the most successful and ubiquitous operating system in Microsoft history. While it has served us well for the last five years, the reality is that it doesn't offer the level of protection you need to deal with the new security threats that we're all facing. Although you can add layers of defense with third-party products, keep in mind that all of the organisations we've been reading about in the news already did that—and it wasn't enough.

These modern challenges require a new platform. Here are some of the ways in which Windows 10 provides that platform.

	Windows 7	Windows 10
IDENTITY PROTECTION	Today's multi-factor solutions are often cumbersome and costly to deploy.	**Microsoft Passport** is an easy-to-use and easy-to-deploy, multi-factor, password alternative.
	Phishing attacks on your users' passwords are increasingly successful.	**Windows Hello** uses biometrics to provide a more secure way of accessing your device, Microsoft Passport, apps, data, and online resources.*
	Pass the Hash attacks enable attackers to steal identities, traverse across networks, and evade detection.	**Microsoft Azure Active Directory** provides a comprehensive identity and access management solution for the cloud.
DATA PROTECTION	BitLocker offers optionally configurable disk encryption.	**BitLocker** is much improved, is highly manageable, and can be automatically provisioned on most new devices.
	Data loss prevention (DLP) requires the use of additional software and frequently third-party capability.	**Enterprise Data Protection** addresses the needs for DLP, includes a deeply integrated data separation and containerisation solution, and provides encryption at the file level.
	DLP solutions often compromise the user experience in the interest of security, resulting in low adoption and varying experience between the desktop and mobile devices.	**Enterprise Data Protection** provides a seamless user experience across mobile devices and the desktop, and is integrated with Azure Active Directory and Rights Management Services.
THREAT RESISTANCE	All apps are trusted until they're determined to be a threat or are explicitly blocked.	**Device Guard** offers protection on the desktop that is similar to lockdown on a mobile platform (full app lockdown).
	With more than 300,000 new threats per day, blocking them through detection (block on known bad) is a losing battle.	With **Device Guard,** an application must prove itself to be trustworthy before it can be run.
	Windows provides a series of defense solutions, but too many malware threats impact users before detection-based antivirus solutions can catch up.	**Device Guard** will be the most disruptive malware-resistance capability Microsoft has ever shipped in the desktop.
DEVICE SECURITY	Platform security is based entirely on what software can do on its own, and once infected there is no assurance that system defenses can perform their function and remain tamper free.	**Hardware-based security** and the level of trust it offers helps to maintain and validate hardware and system integrity.
	Malware can hide within the hardware or in the operating system itself, and there is no way to validate integrity once it has been compromised.	**UEFI Secure Boot** helps prevent malware from embedding itself within hardware or starting before the OS. Trusted Boot helps maintain the integrity of the rest of the OS.

*Windows Hello requires specialised hardware, including fingerprint reader, illuminated IR sensor or other biometric sensors.

Microsoft