## SECURITY FEATURES: Comparing Windows 7 to Windows 10

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 3rd party products, keep in mind that all of the organizations 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
- **Identity Protection**
  - Phishing attacks on your users’ passwords are increasingly successful.
  - Today’s multifactor solutions, like smartcards, are often cumbersome and costly to deploy.
  - BYOD devices have limited network access due to security risk.

- **Information Protection**
  - BitLocker offers optionally configurable disk encryption.
  - Information protection often compromise the user experience in the interest of security, resulting in low adoption and varying experience between the desktop and mobile devices.

- **Threat Resistance**
  - Most OS breaches are initiated in the browser and are executed quickly, leaving the user and IT with little to no ability to respond.
  - Anti-virus (AV) protection not included in-box requiring additional software.

- **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 tamper free.

### Windows 10
- **Identity Protection**
  - Windows Hello is an easy to use and deploy multi-factor password alternative that can use biometrics* or other factors for authentication.* (Mandiant, 2016)

- **Information Protection**
  - BitLocker is much improved, is highly manageable, and can be automatically provisioned on many new devices.

- **Threat Resistance**
  - Microsoft Edge uses sandboxing technology to isolate the browser from the OS and plugins, like Flash: If there is a breach, OS can’t be compromised.

- **Device Security**
  - Hardware based security and the level of trust it offers helps to maintain and validate hardware and system integrity.

### BitLocker
- BitLocker is a full disk encryption solution that protects data at rest. It uses hardware-based encryption and requires a trusted platform module (TPM) to be enabled. With BitLocker, you can encrypt your entire hard drive, making it unreadable to anyone who doesn’t have the proper decryption key.

### Windows Hello
- Windows Hello is a biometric authentication system for Windows 10, enabling seamless sign-in with a fingerprint, face, or iris scan. It is designed to provide a more secure and user-friendly alternative to passwords and PINs.

### Microsoft Edge
- Microsoft Edge is the default web browser for Windows 10, designed to provide a more secure browsing experience. It includes features like Enhanced Protection Mode and Intelligent Blocking to prevent malicious websites from loading.

### Windows Defender Advanced Threat Protection (ATP)
- Windows Defender ATP enables Windows enterprise customers to detect, investigate, and remediate advanced persistent threats and data breaches on their networks. It uses a combination of behavioral analysis, machine learning, and threat intelligence to identify and respond to threats.

## Footnotes
1. To use Windows Hello with biometrics, specialized hardware, including fingerprint reader, illuminated IR sensor, or other biometric sensors, is required. Hardware based protection of the Windows Hello credential/keys requires TPM 1.2 or greater; if no TPM exists or is configured, credential/keys protection will be software-based.  
2. Companion devices must be paired with Windows 10 PC’s via Bluetooth. To use a Windows Hello companion device that enables the user to roam with their Windows 10 PC and authenticate to their business resources without using a password.  
3. Separate subscription for Azure Active Directory required.  
4. Requires TPM 1.2 or greater for TPM based key protection.  
5. Windows Information Protection; formerly Enterprise Data Protection (EDP), requires either Mobile Device Management (MDM) or System Center Configuration Manager to manage settings. Active Directory makes management easier, but is not required.