**Security Features in Windows OS**

Windows is a popular system. It is designed to be able to meet, with satisfaction, the needs of all its users: professionals, developers, gamers, administrators, etc.

The popularity of Windows makes it a prime target for hackers who, ready or indirectly, seek by all means to access user data without authorization or fraudulently.

Therefore, the biggest concern of Microsoft as it develops the Microsoft Windows operating system is to improve Windows by providing it with robust security features to protect its users from hacker threats and all other potential vulnerabilities.

Thus, these security features are implemented in the system to ensure security at four main levels:

1. Data security: Windows is an operating system widely used around the world, making it an attractive target for computer attackers. If Windows is not protected properly, it can lead to the loss or theft of sensitive data, which can lead to serious consequences for businesses and individuals.
2. Malware prevention: Malware, such as viruses, Trojans, and ransomware, is a constant threat to Windows users. Protecting Windows can help prevent malware infections and minimize the damage they can cause.
3. Privacy: Windows collects a considerable amount of user data, which can pose a privacy risk. Windows protection can help reduce the amount of data collected and protect users' privacy.
4. System stability: Windows protection can help maintain system stability by preventing malware and system errors from causing problems.

To ensure data security, prevent malware, protect privacy, and maintain system stability, security features are implemented within Microsoft Windows to perform different roles, the main ones being:

1. Protection against viruses and malware: Windows has implemented several protective measures to keep users and the operating system safe from viruses and malware. These protective measures constitute the set of features of Windows Security which includes Windows Defender, the antivirus built by Microsoft for the Windows Operating System.
2. Two-factor authentication: In addition to the traditional password authentication that has existed within Windows since its previous versions, two-factor authentication has been added since Windows 10 as an additional layer to ensure system security. This two-factor authentication is done either with a mobile phone or a security key (USB key or any other physical security device that can be used for connection).
3. Network traffic filtering: Windows uses a firewall to filter network traffic in and out of your computer. This firewall is enabled by default and can be configured to allow or block certain connections at the convenience of users.
4. Data encryption: This feature is important to protect sensitive data from unauthorized access. Data encryption within Windows is primarily the function of the two tools: BitLocker to encrypt data on disk (HDD or SSD), and Encrypted File System (EFS) designed to protect or encrypt individual files.
5. Management and control of user accounts. User account management is used to manage system administration privileges. Thus, administration is limited to only those users who need it. User Account Control (UAC) notifies when changes are made to the system. It helps prevent unauthorized changes to the system by requesting permission from the user before performing a task that requires administrator privileges.
6. Web traffic filtering: Web content filtering can help prevent users from accessing malicious or inappropriate websites.
7. Group policies: Group policies within Windows represent the set of configuration rules for managing computers and users in a Windows environment. They are used to control the behavior and functionality of Windows and applications installed on computers (individual or groups of computers). Group policies are configured through the Local Group Policy Editor for individual computers or through the Group Policy Management Console for corporate networks.
8. Regular application of security patches: Security patches are software updates that address vulnerabilities in the Windows operating system or in applications embedded or installed on your Windows computer. Microsoft regularly releases updates to improve and fix system vulnerabilities through Windows Updates which can be configured to apply updates automatically or not.
9. Parental controls: Family controls are a feature of Windows that allows parents or caregivers of children to control and monitor their children's computer usage. This feature allows you to limit access to certain applications, websites, and games, and restrict computer usage to certain times of the day. Windows parental controls can be activated via the operating system settings or via the "Microsoft Family Safety" application available for free in the Microsoft store.

The security tools responsible for protecting the Microsoft Windows Operating System are numerous, including Windows Defender, Windows Firewall, Windows Update, User Account Control, Windows Hello, Windows Event Viewer, BitLocker, Encrypted File System, Windows Task Manager, Trusted Platform Module, Virtualization Based-Security, Hypervisor-Protected Code Integrity, UEFI Secure Boot, Local Security Policy, Command netstat, etc. We will come back to these tools in detail in future articles.

In conclusion, it should be borne in mind that attack mechanisms evolve as much as technology. The more techniques are developed to protect against cybercrime, the more cybercriminals imagine and invent new mechanisms to circumvent them. As such, Microsoft is constantly working to improve Windows security by performing security scans, responding quickly to discovered security vulnerabilities, and collaborating with the IT security community to improve Windows security. However, users should also employ security measures to protect themselves and their computers from malicious spirits. These include security measures such as using strong passwords and installing third-party security software to enhance protection.