Microsoft reveals how Windows 10 and Windows 11 block keyloggers

In the early 2000s, the security of Windows operating systems relied heavily on third-party antivirus software.

In 2009, Microsoft first introduced Security Essentials as a free antivirus software exclusively for Windows PCs. Over the years, Microsoft has developed Security Essentials into a powerful and comprehensive product, even surpassing other leading antivirus software in AV-TEST certification.

With Windows 8, Microsoft replaced Security Essentials with Windows Defender. By the time Windows 10 launched, Microsoft had turned Windows Defender into a generic brand for several security products, and all Windows 10/11 PCs now come with Windows Defender Antivirus built in.

Microsoft recently shared a blog post explaining how Microsoft Defender Antivirus protects Windows 10 and Windows 11 users from keylogger and screen scraper malware. Keylogger malware can record every keystroke, clipboard data, and screenshots on a PC, while screen scrapers can 'stealthily' take pictures and record videos of what's happening on a user's PC screen.

Microsoft has revealed that Microsoft Defender Antivirus now uses AI, ML algorithms, and the cloud-based Microsoft Intelligent Security Graph to block malware within milliseconds of detection. Additionally, Defender AV can even analyze behavior and process trees to stop fileless malware and human-made attacks.

Here's how Windows Defender Antivirus protects Windows 10 and Windows 11 users from keylogger malware, according to Microsoft:

1. When your PC is turned on, Windows uses Secure Boot, Trusted Boot, and Measured Boot to verify that the system's firmware, bootloader, kernel, drivers, and anti-malware software are loaded correctly. This helps prevent malware from interfering with the boot sequence and trying to infect your PC even before

Microsoft Defender Antivirus starts.
2. When your PC starts, Microsoft Defender Antivirus uses a variety of different engines to block malware as it finds it.
3. Intrusion protection prevents security tools on the system from being disabled or modified by malware.
4. Microsoft Defender SmartScreen prevents malware from being downloaded. This feature works even when Microsoft Defender Antivirus real-time scanning is turned off.
5. For enhanced security, Microsoft recommends that users use Microsoft Defender for Endpoint in addition to the built-in Defender Antivirus.

You can learn more about the security features of Windows 11 on the Microsoft blog. With multi-layered protection, Windows Defender Antivirus provides strong protection against keyloggers and other threats, demonstrating Microsoft's commitment to user security.