Windows Sandbox is a safe new way to run untrusted .exe files

Microsoft is trying to address the fear of running an unknown .exe on your PC. While some power users set up virtual machines to check unknown apps, Microsoft has developed a simple way for anyone running Windows 10 to launch apps in an isolated desktop environment. Windows Sandbox is a new feature coming to Windows 10 next year that creates a temporary desktop environment to isolate a particular app to that sandbox.

It’s designed to be secure and disposable, so once you’ve finished running the app in this mode the entire sandbox will be deleted. You don’t need to set up a virtual machine, but it will require virtualization capabilities enabled in the BIOS. Microsoft is making Windows Sandbox available as part of Windows 10 Pro or Windows 10 Enterprise, and it’s clearly aimed at businesses primarily or power users.

It’s a clever new feature that means every time Windows Sandbox is enabled it simply creates a new lightweight (100MB) installation of Windows to run an app. Microsoft is using its own hypervisor to create a separate kernel that’s isolated from the host PC. Windows 10 testers will be able to start testing this new feature once Microsoft ships build 18305 or later. If you’re interested in more of the technical details of Microsoft’s Windows Sandbox, you’ll find plenty of them over at the company’s blog post.

https://www.theverge.com/2018/12/19/18147991/microsoft-windows-sandbox-security-safety-isolation-standalone-apps