Windows OS is like a Castle with all doors opened. SRP can close the doors, and only Administrators can open them.

Here are some simple facts about Software Restriction Policies (SRP).

1. They can be activated in all Windows versions, starting with Windows XP.
2. In Windows Pro, Enterprise and Education, SRP can be configured using secpol.msc or gpedit.msc
3. In Windows Home, SRP can be configured by tweaking Windows Registry or using some utilities: Simple Software Restriction Policies (no GUI), Hard_Configurator (with GUI).
4. SRP does not touch processes that are executed with Administrative Rights, so Windows system can work without problems. There's no need to disable SRP protection to apply Windows Updates and system scheduled tasks or install/update Universal Applications from Windows Store.
5. There are two common approaches to SRP:

★ Default Allow + Blacklist/Whitelist (used as a great part of security in CryptoPrevent and SBGuard Anti-Ransomware).

★ Default Deny + Whitelist/Blacklist (SSRP, Hard_Configurator).

6. The most effective approach is properly configured 'Default Deny', but this requires some knowledge about how SRP work. The 'Default Allow' approach has some advantages (except Windows 8+), when installing new programs. Most restrictions are active during the installation process, so accidental 0-day malware installations can be mitigated. On the contrary 'Default Deny' is better against exploits, and generally, when malicious code has been run unknowingly or accidentally (0-day, too). But, when installing new programs most restrictions are inactive. So, when the user is fooled to install by himself 0-day malware, it is not mitigated by SRP.
7. It is possible to use 'Default Deny' approach in daily work, and switch temporarily to 'Default Allow' when installing new programs (without reinstalling CryptoPrevent or SBGuard).
8. Properly configured SRP can be used even by inexperienced users, but it does not mean, that inexperienced users can configure it properly.
9. The real benefit of 'Default Deny' SRP is evident for Home users in Windows 8+, because of system-wide SmartScreen Application Reputation (on the run) and improved Windows Defender. This allows making a sensible Windows built-in security, without 3rd party real time security components.
10. Default Deny SRP + No Elevation SUA (ConsentPromptBehaviorUser=0 in UAC settings) can be used to lock down the Standard User Account - no way to run/install new programs, except Universal Applications from Windows Store.
11. Properly configured SRP can work with 3rd party antivirus, antimalware, anti-exe, anti-exploit, and HIPS solutions. But in some cases, this can be done only by experienced users.

12. SRP can prevent many 'Drive By' attacks, but can be bypassed by truly fileless malware or VBA scripts embedded in documents.
13. There are also some other bypasses which depend on SRP configuration (using Windows system files to bypass whitelisting, etc.).

What does happen when one double-click the file on the Desktop?

Something has to call into SRP (Safer APIs) and get the information about what should be blocked. Windows OS has a special API function that is triggered to manage file opening from the Desktop (also from Explorer and Internet Explorer) - it is called ShellExecute().
Suppose, that you have clicked the file 'How2BeReach.hta'. ShellExecute() function can figure out, that the sponsor mshta.exe should be used to open the HTA file. The ShellExecute() has also built-in ability to call into SRP, so if SRP are activated, then the file 'How2BeReach.hta' can be blocked. Blocking files by ShellExecute() prevents users from unknowingly or accidentally executing malicious code.

SRP has a special list of file extensions, called 'Designated File Types'. If the file extension is on this list, then ShellExecute() can prevent that file from opening. So, the file 'How2BeReach.hta' can be blocked by ShellExecute() when HTA extension is on 'Designated File Types' list. The list is configurable, and the user can add or remove the file extensions from it.
Here are the default 'Designated File Types' :
ADE, DP, BAS, BAT, CHM, CMD, COM, CPL, CRT, EXE, HLP, HTA, INF, INS, ISP, LNK, MDB, MDE, MSC, MSI, MSP, MST, OCX, PCD, PIF, REG, SCR, SHS, URL, VB, WSC.
The EXE extension is on the above list only pro forma. SRP works the same, when it is removed from the list. This is because EXE files do not use ShellExecute() function to run.

But, if you choose to open HTA file directly, using the below command:
'mshta.exe %Userprofile%\Desktop\How2BeReach.hta'
then ShellExecute() will be skipped, and SRP will not know that something is going to be executed.

Now, Windows has two possibilities:
1. Allow opening the file.
2. Use another mechanism to call into SRP.

End of part 1.