Step-by-step: Passive / Non-blocking flow

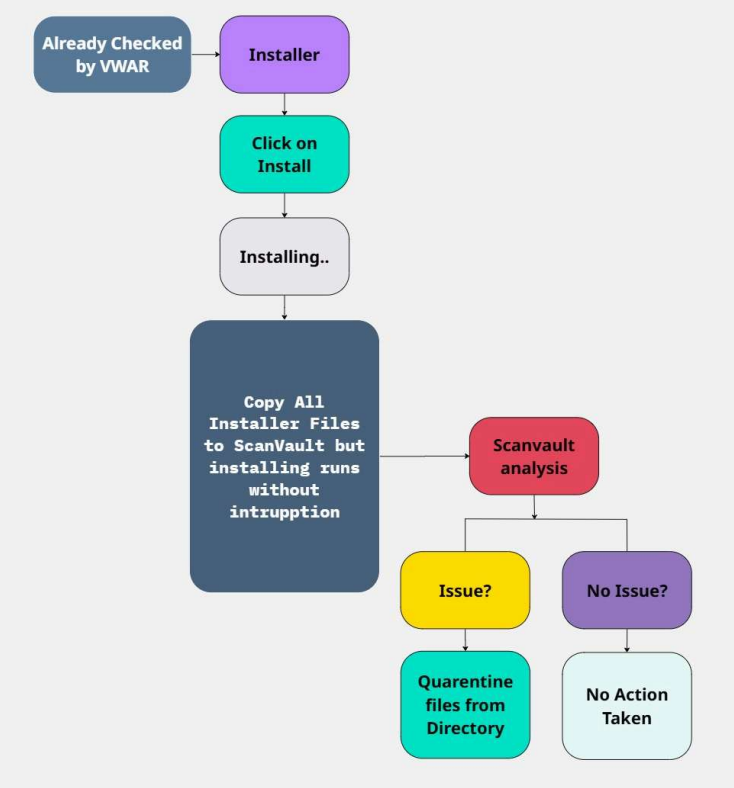
Goal:

Allow installers to run without interruption while ensuring a copy of installer files is analyzed by ScanVault and infected files get quarantined later.

Steps:

1. **Pre-check:**
   Installer process checks whether the package has already been scanned/flagged by VWAR ("Already Checked by VWAR" node). If pre-checked clean → continue.
2. **User action:**
   User clicks **Install**.
3. **Start installation:**
   Installer begins the normal installation steps (writing files to target directories, registering services, etc.).
4. **Background copy:**
   Concurrently the installer (or an installed agent helper) copies *all installer files* to the ScanVault input area. This copy must be done **non-blocking** (background thread/process) so the installer doesn't wait on the copy.
5. **ScanVault analysis:**
   ScanVault receives the files and performs analysis asynchronously. Analysis can be multi-step (signature + heuristics + YARA rules).
6. **Analysis result: Two outcomes:**
   - **No Issue:**
     ScanVault marks files as clean
     → **No Action Taken**. Optionally log the clean report and retention.
   - **Issue found:**
     ScanVault flags files
     → **Quarantine files from Directory**. The system moves infected files to a secure quarantine store or flags them for removal.
7. **Post-detection remediation:** If files were quarantined *after* installation, additional remediation may be necessary: notify user/admin, remove or roll back the installed components, and optionally push a system restore/uninstall action.

Pros	Cons
Very safe: can catch malware hidden inside installers.	Harder to make; more complex to develop.
Very safe: can catch malware hidden inside installers.	Can slow down installation (copying and scanning files takes time).
Doesn’t bother users while installing.	Might break some installers if they are sensitive.
Can use advanced scanning methods (like signature or behavior scan).	Might delete a good program by mistake (false alarms).
	Undoing all changes (files, registry, services) is tricky.



Step-by-step: Active / Blocking protection flow

Goal:

Block installation from proceeding until the path is added to VWAR exceptions (whitelisted), or until administrator chooses to allow it.

Steps:

1. **Pre-check:**
   Installer touched or attempted to write into a protected path while ScanVault active.
2. **Protection decision:**
   ScanVault's real-time protection component blocks the operation and presents the user with the message: "Installation Cannot Proceed – ScanVault Protection Active".
3. **User prompt:**
   Display message: *"Add this path to the VWAR exceptions to continue with the installation."* with Yes/ No options.
4. **If user chooses "Yes":**

- Prompt to confirm the exact path that will be added by user from VWAR (show e.g., `E:\my-app`).
- Add the path to VWAR exception list (persist as absolute path, validated by admin policy).
- Continue installation (installer resumes) → Installing.. → Installed Successfully.

5. **If user chooses "No":**

- Block remains active; return user to VWAR UI to either review the detection, run an on-demand scan, or choose a different action (Back to VWAR).

Pros	Cons
Very easy to set up and stable.	All programs on an allowed drive can install – not very strict.
Doesn’t slow down the computer.	Won’t protect inside the exception drive or folder.
Stops programs from installing on unsafe drives.	

Users can control which drives are allowed (exception list).	
Rarely makes mistakes.