Dr.Backup™
data protection service

Making Zero Trust Security Filter Updates to Your Device

Planned Maintenance: If you or your tech team are planning to make substantial software changes to your PC/Server, please call our office during normal business hours to schedule a Zero Trust Security Filter *maintenance window* for each device you plan to update.

At the start of a pre-scheduled window, our automated systems will place your device into **"learning mode"** so you can install software, change configurations, use network diagnostic tools, update firmware or drivers, and access remote control support tools without interruption.

We implicitly trust that you will take care to only install applications from known/secure sources during the window. Make sure to exercise the functions of your new software and verify correct operation. At the end of the scheduled window, learning mode will end and your device will once again be secured.

Update Existing Software: If you need to perform an ad hoc update of previously installed software, begin the update process and *when a pop-up menu appears, provide the requested information*. Our Security Operations Center (SOC) personnel generally respond to these routine requests within 15 minutes, seven days a week. If you provided an email address when you completed the pop-up menu, you will be notified of the status of your request. Once you receive this notification, retry the blocked application.

Initial Use of Common Software: If you are attempting to install or use a software application for the first time, and have *NOT scheduled a maintenance window*, you will see a pop-up menu. *Complete the requested information on the pop-up menu and include your security PIN.* If the requested application is already on our commonly used/safe list, the SOC can usually approve your request and update your security filters within 15 minutes. The email address you provide will be notified.

Initial Use of Other Privileged Software: If the individual using your device attempts to install or activate software which: 1) has not previously been approved, or 2) has the potential to disrupt normal operation of your device, or 3) could be used for nefarious purposes -- this is considered a high-risk situation. Our SOC will mark these requests for further investigation. Be sure to include your security PIN code so that we can proceed without needing to validate the requester's identity. Researching the safety of a software package typically occurs during our normal business hours.

After Hours: If you or your technician are going to be performing after hours or weekend work on your system(s), **please make every effort possible to pre-schedule a maintenance window by *calling our customer support department at 301-560-4534* during normal business hours.**

Zero Trust requests to execute privileged software after hours will generally not be actioned until the next business day.