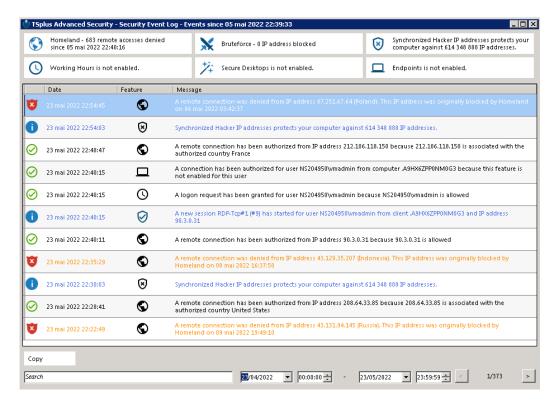


Events

The security events are a great source of information as they display the operations performed by TSplus Advanced Security to protect your computer.

The Events window can be opened from the TSplus Advanced Security main window, by clicking directly on the last 5 events displayed or on the Events tab. The information displayed on the Events window are refreshed automatically every few seconds.

The list of security events presents 4 columns, which describes the severity, the date of the check or performed operation, the associated feature icon and the description.



The example above ilustrates real life denied connection attempts blocked by TSplus Advanced Security.

The description of the event often explains why the action was performed or not. As illustrated, retaliatory actions are often written in red and highlighted with a red shield icon.

Events window can be moved around and does not prevent you from using the other TSplus Advanced Security feature.

Following feature status at a glance

The 6 tiles at the top of the window displays a status for each corresponding TSplus Advanced Security features.





In the example above, **Homeland Protection** status shows 673 blocked connections since May 2022. Also, the example warns that the **Endpoint Protection** feature is not enabled. The status are displayed according to the security events recorded. The window title highlights the oldest security events.

Navigating and Searching through events

- A deep global search is now available in order to find specific events quickly.
- Next to the global search, 2 date and time pickers filters the displayed events according to the date the event was raised.
- On the right, arrows allows to change pages and navigate to view older events.

Interacting with events

Finally, it is also possible to act on the event by clicking on a button located in the bottom menu, or right-clicking on the desired event:

- Copy the event message
- Copy the IP Address
- Unblock the IP address
- · Unblock and add to IP addresses allow list

