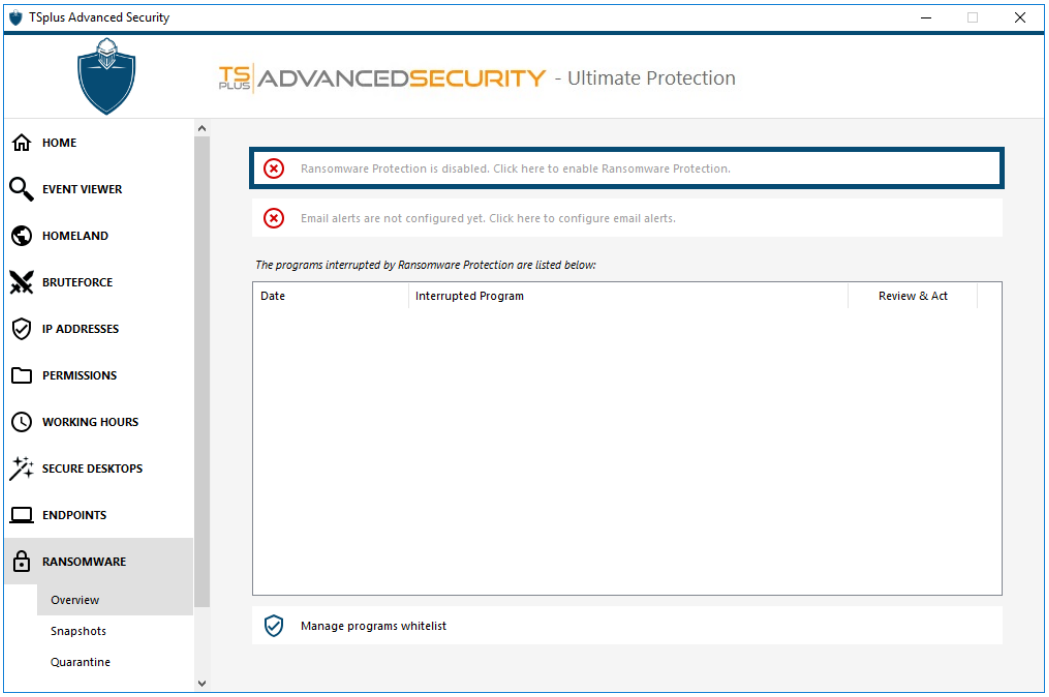
Ransomware Protection

The Ransomware Protection enables you to efficiently DETECT, BLOCK and PREVENT ransomware attacks. TSplus Advanced Security reacts as soon as it detects ransomware on your session. It possesses both **static and behavioral analysis**:

- The **static analysis** enables the software to react immediately when an extension name changed,
- The **behavorial analysis** looks at how a program will interact with files and detect new strain of ransomware.

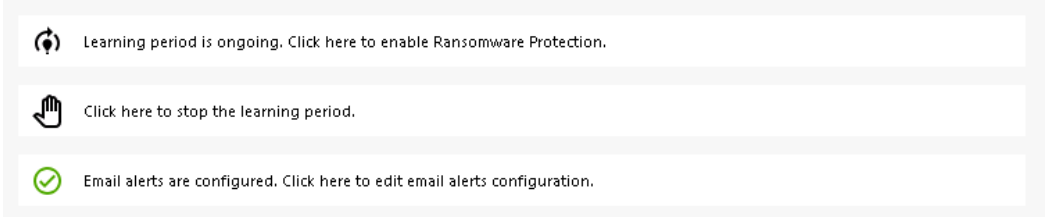
You can enable it by clicking on the "Enable Ransomware Protection" on the Ransomware Protection tab:



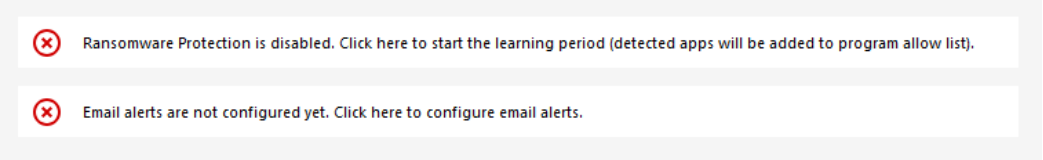
Learning Period

After enabling the Ransomware Protection feature, the Learning Period is automatically activated. During the Learning Period, all programs detected by the Ransomware Protection feature will be considered as false positive and will be able to resume their execution. The programs detected as false positive will be automatically added to the list of allowed programs.

This feature allows to configure Ransomware Protection on a production server without disrupting its activity. We recommend to start with a 5 days Learning Period to identify all legit business applications.



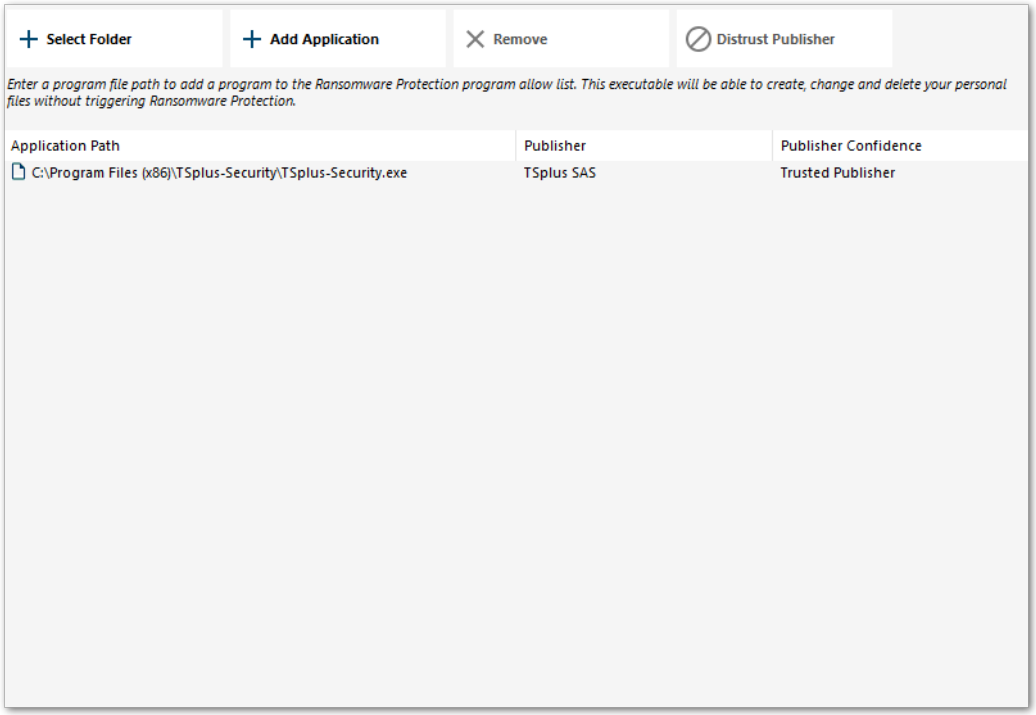
If you stop the Learning Period, it will deactivate the Ransomware Protection. Click on the "Ransomware Protection is disabled" button to reactivate the Learning Period.



Ransomware Protection Action

It quickly scans your disk(s) and displays the file(s) or program(s) responsible, in addition to providing a list of the infected items. TSplus Advanced Security automatically stops the attack and quarantines the program(s) along with the file(s) encrypted before its intervention.

Only the administrator can whitelist them, by entering the path of the desired program on the bottom line and by clicking on "Add":



Ransomware Protection Report

TSplus Advanced Security prevents catastrophic events for businesses by removing ransomware at an early stage.

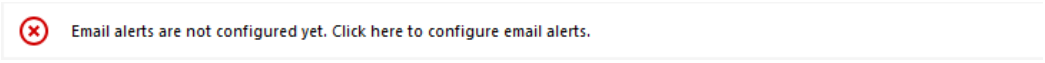
The administrator has access to information regarding the source of the attack and running processes, and therefore learns how to anticipate these threats.

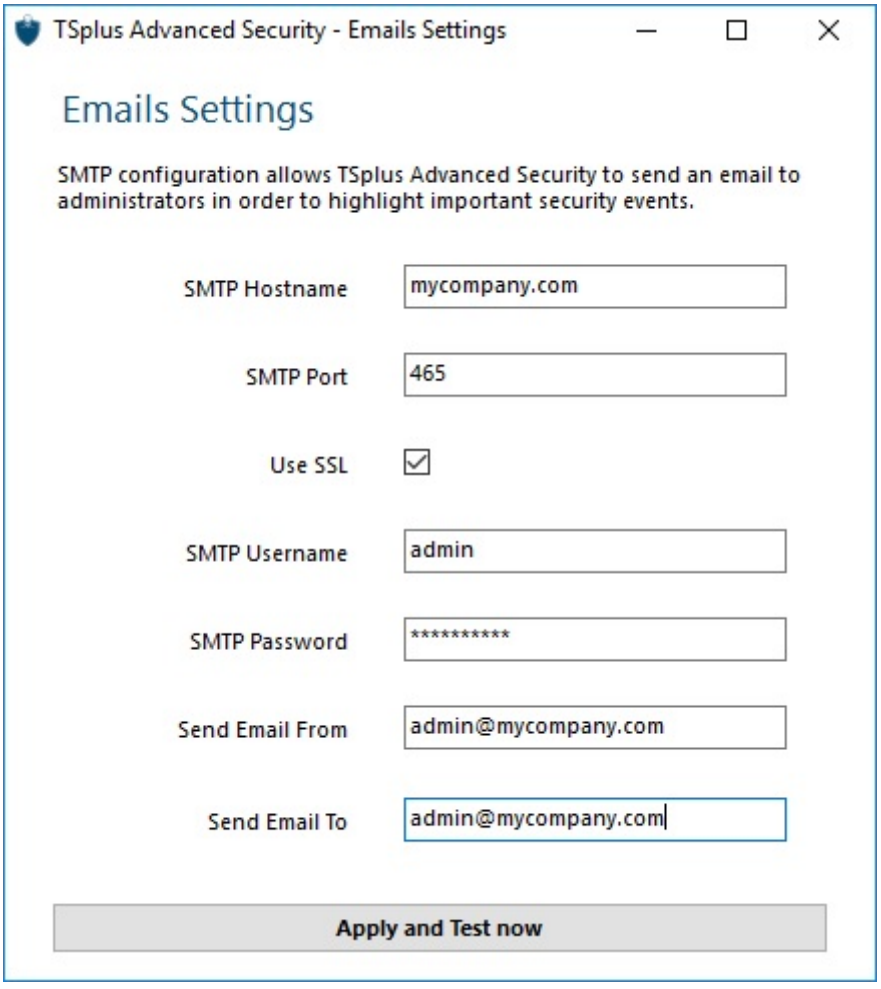
Note: Ransomware Protection observes how programs interact with system and personal files. To ensure a greater level of protection, Ransomware Protection creates bait files in key folders where ransomware often begins its attack. Therefore, a few hidden files may appear in the users' desktop and documents folders, as well as in other locations. When it detects a

malicious behaviour, it stops the ransomware immediately (or ask if the logged user is an administrator). Ransomware Protection uses pure behavioural detection techniques and does not rely on malware signatures, allowing it to catch ransomware which does not exist yet.

Add an SMTP configuration - Email Alerts

You can configure your SMTP settings in order for TSplus Advanced Security to send you email alerts to highlight important security events by clicking on the button below the Ransomware activation one:





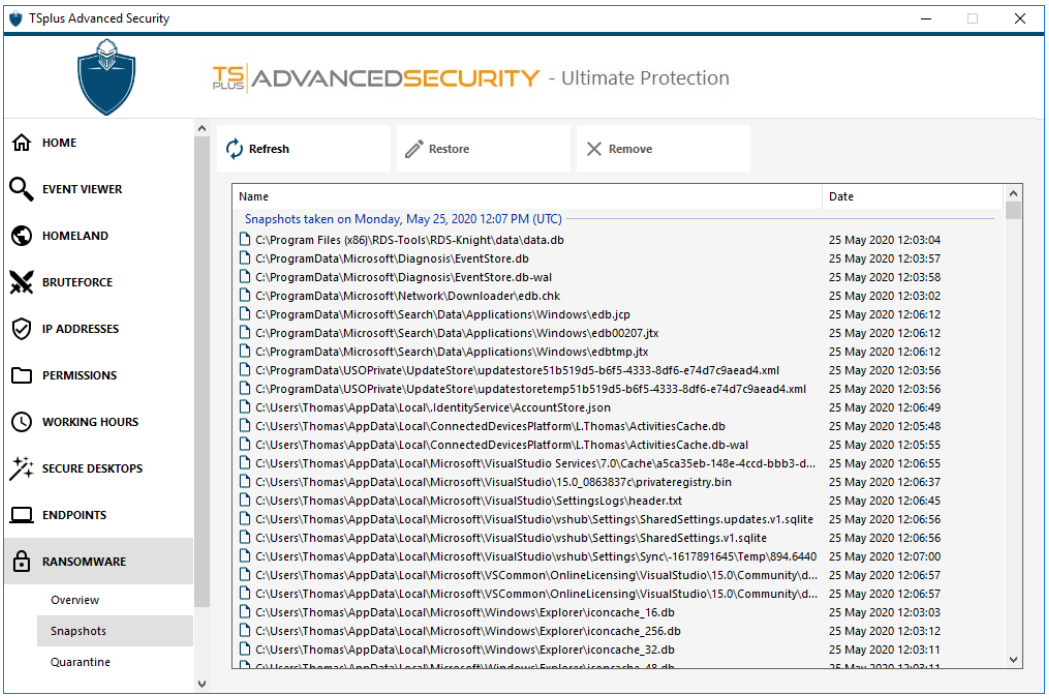
Enter your SMTP Hostname, Port and check the Use SSL box and change change the port from 25 to 465 if you wish to use SSL.

Enter the SMTP Username and Password, as well as the sender and receiver addresses.

Email Settings can be validated by sending a test when saving SMTP settings.

Snapshots

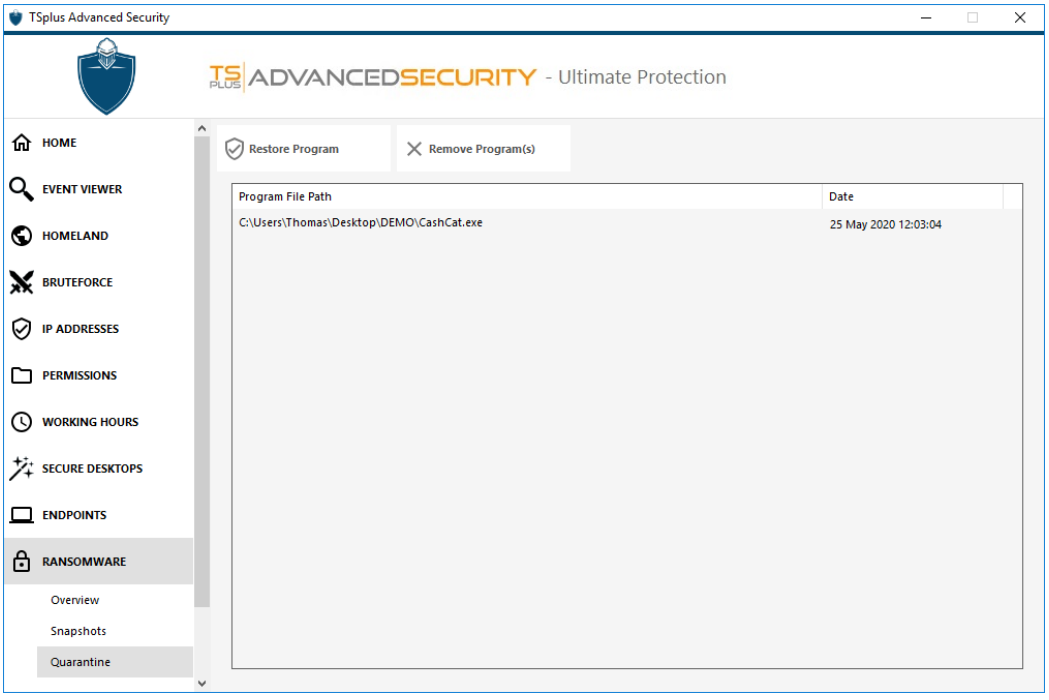
Snaphshots taken by Ransomware Protection are visible under the Snapshots tab:



The list can be refreshed by clicking on the corresponding button. Each element can be restored or removed.

Quarantine

Quarantined programs are visible under the Quarantine tab:



Each element can be restored or removed.

List of Ignored by Default File Extensions

Ignored files are not used to detect possible malicious actions and are not saved when they are modified. The idea is to exclude any operation on large or irrelevant files (such as log files).

- sys
- dll
- exe
- tmp
- ~tmp
- temp
- cache
- lnk
- 1
- 2
- 3
- 4
- 5
- LOG1
- LOG2
- customDestinations-ms
- log
- wab~
- vmc
- vhd
- vhdx
- vdi
- vo1
- vo2
- vsv
- vud
- iso
- dmg
- sparseimage
- cab
- msi
- mui
- dl_
- wim
- ost
- o
- qtch
- ithmb
- vmdk
- vmem
- vmsd
- vmsn
- vmss
- vmx
- vmxf
- menudata
- appicon
- appinfo
- pva
- pvs
- pvi

- pvm
- fdd
- hds
- drk
- mem
- nvram
- hdd
- pk3
- pf
- trn
- automaticDestinations-ms

Caution about Backup Files Extension

The file extension used for saving modified files is: **snapshot.** The driver prohibits any modification or deletion action on these files other than by the TSplus Advanced Security service. Stopping the service deletes the backed up files. In order to delete these files manually, you must temporarily unload the driver.

Backup File Configuration

By default, the directory of saved files is located in the installation directory of TSplus Advanced Security and is called "snapshots". However, it is possible to define another location for this directory. This can allow the administrator to define a directory located on a faster disk (SSD) or on a larger disk according to his needs. The backup directory path must not be a UNC path, in the form of:

```
\\<computer name>\<backup directory>\
```

Adding Backup Utilities to the Whitelist

We recommend adding backup utilities in the Whitelist.