TSPLUS
ADVANCED SECURITY

Cyber Criminals Know You Use Remote Desktop systems.

Most organizations assume that the hackers who threaten them will be motivated by the value of the informationthe company uses to provide its services.

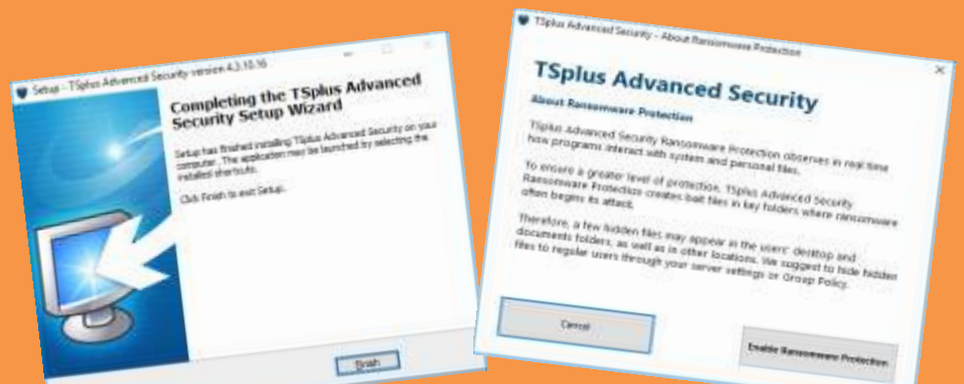
The truth is that cyber criminals don't necessarily care about the value of corporate, personal and/or Financial data.

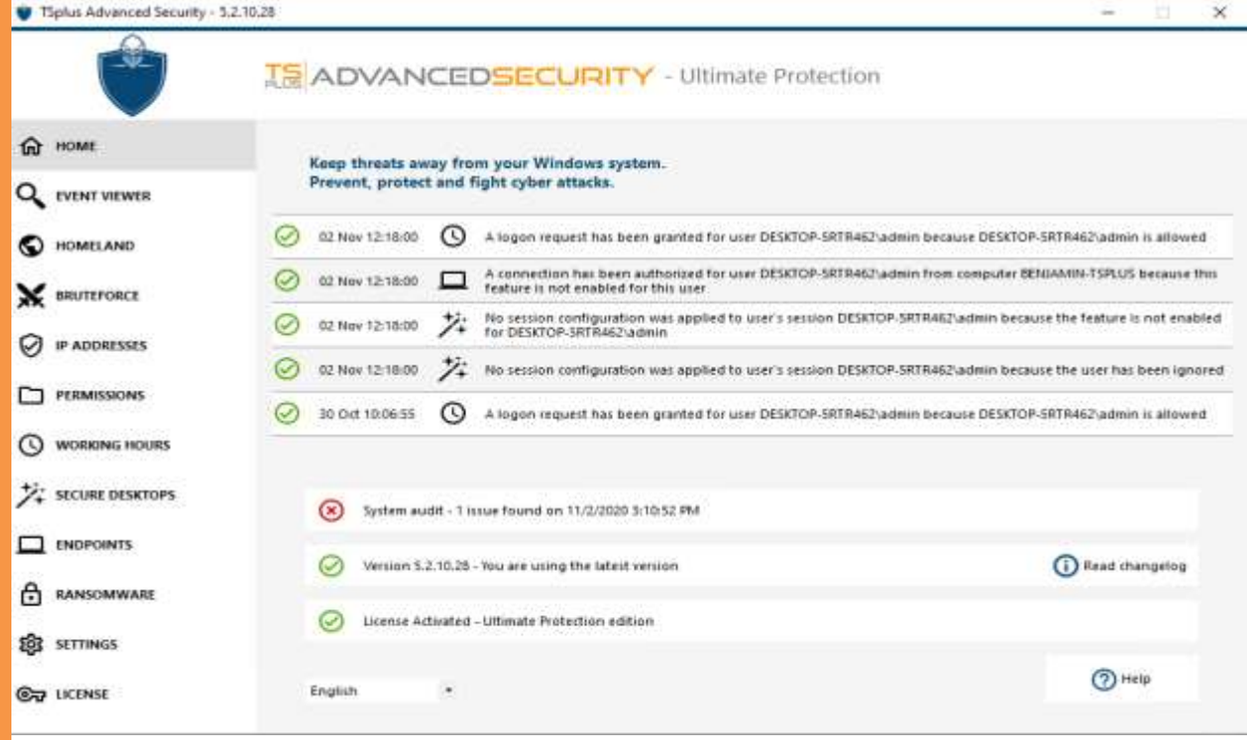
Many attacks are perpetrated on systems because there's value in the processing power of the systems themselves.

In terms of business risks and associated consequences, Remote Desktop must be shielded and protected.

No longer an 'if' question, cyber-crime is undoubtedly a 'when'.

Cyber security is now a high priority for every organization!





THE RIGHT WEAPON AGAINST CYBER-CRIMINALS

As Windows infrastructures grow and evolve, it gets more and more difficult for security experts to see all the endpoints in their architecture.

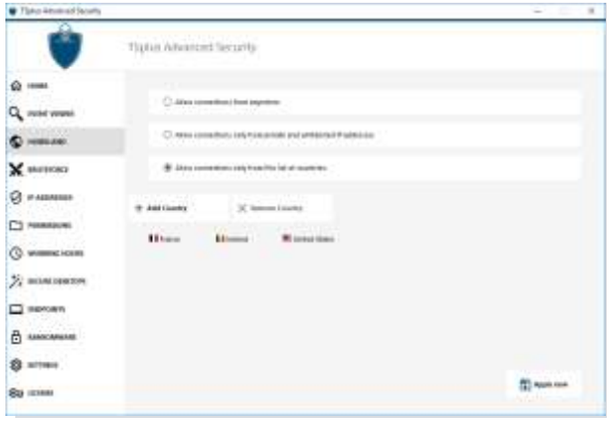
And you need to know your Remote Desktop vulnerabilities to mitigate your risk. **TS*plus Advanced Security*** consists of a robust set of security features to protect against these Remote Desktop attacks.

This software approach combines advanced technology as well as the latest lessons and insights our elite team of Remote Desktop cyber security specialists brings back from real world missions.

TS*plus Advanced Security* is available in two editions: **Security Essentials** (5 features) and **Ultimate Protection** (7 features).

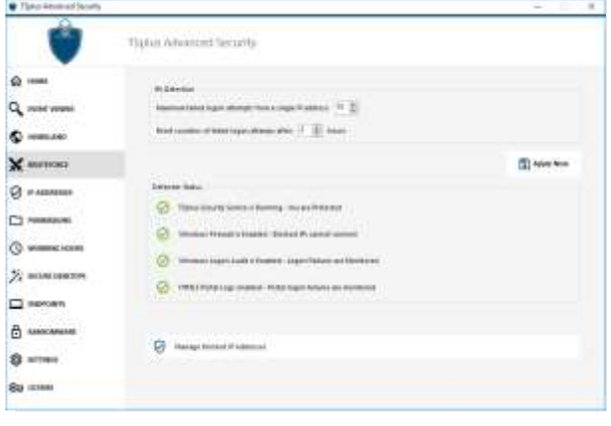
The best package to keep your Remote Desktop connection safe, with powerful protection features. The security solution you can apply to all W7/W10 Pro RDP accesses.

ESSENTIALS EDITION



PREVENT USERS TO CONNECT AT NIGHT

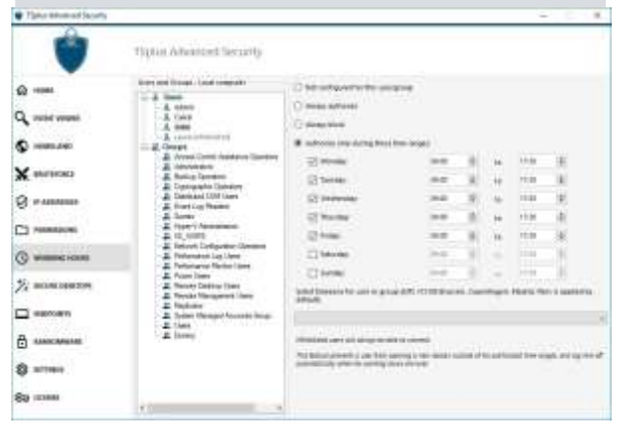
Users are working during daytime and they are not allowed to connect out of their working hours. It is as simple as that! Any user connecting at night will be automatically logged out of the system.



PREVENT FOREIGNERS TO OPEN A SESSION

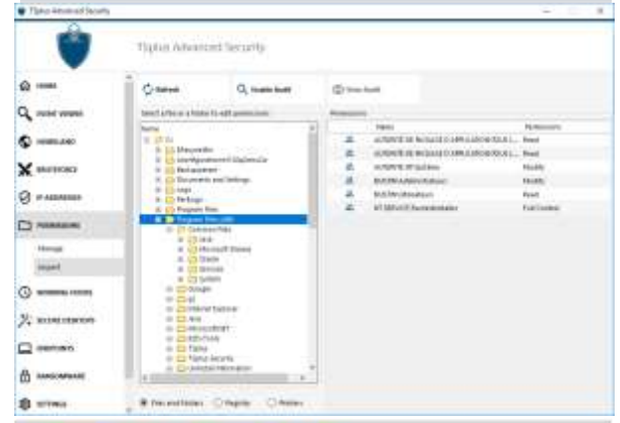
Your users are located in Germany, France, Italy and the USA. Why would you allow any user to connect from other countries?

In a snap with ***Advanced Security***, protect your TSplus servers from hackers trying to open a session from foreign countries.



AVOID BRUTE FORCE ATTACKS

Stop the constant attacks right now with ***Advanced Security*** Brute-Force Attacks Defender. It will instantly protect your server by monitoring Windows failed login attempts and automatically blacklist the offending IP addresses after several failures. Moreover, you can configure it to match your needs.



PERMISSIONS - *INSPECT*

On Windows, permissions are taken care of by the Operating System which defines, by default, the scope of privileges for each user profile (read, write, modify) and automatically prevents access to sensitive locations on the server.

There are times, however, when it's necessary to manually configure permissions for the best network security. That's the case if your organization uses Remote Desktop technology.

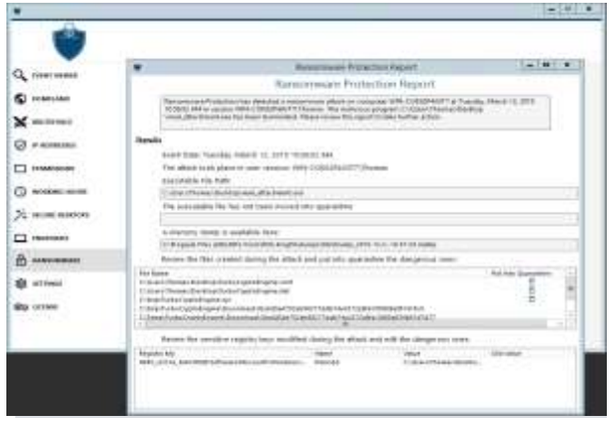
If important files do not have the best permissions in place, successful connection by malicious users can quickly lead to compromised data.

The Permissions dashboard displays the list of users and groups and the list of available folders, side-by-side.

With ***Advanced Security®*** - Essentials Edition, everything is visible at one spot and you can quickly Inspect Windows access rights per users & groups.

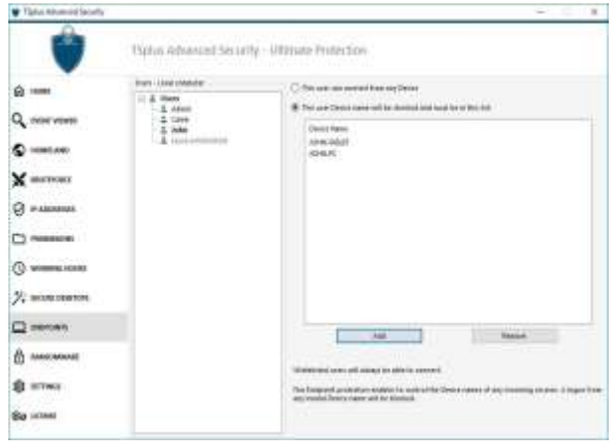
The security tool every Windows Server administrator 'Must Have'. Everything you need to effectively protect your user environment and prohibit malicious actions.

ULTIMATE EDITION



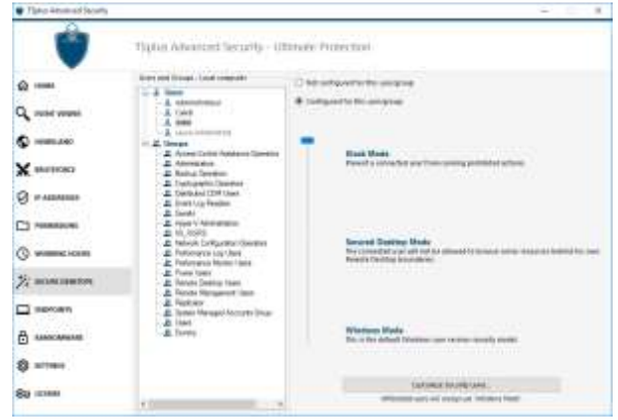
PROTECT USERS PROFILES

Windows systems are providing too many parameters and only few experts can properly manage this kind of complexity to set up security rules and to hide Windows features from users' Remote Desktops. Like a dream, ***Advanced Security***, will enforce for you the security level you want to secure your RDS server. You can do it "user per user", or per group.



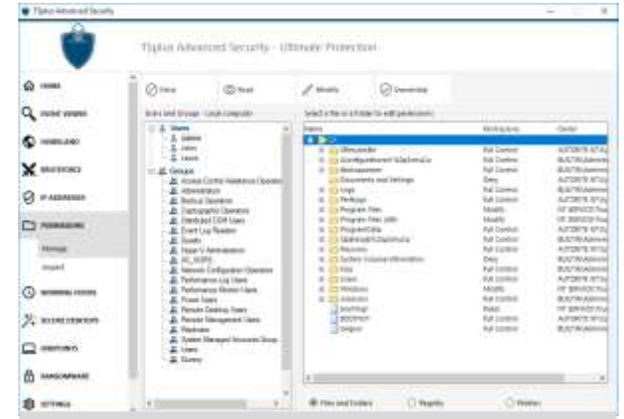
DETECT AND STOP RANSOMWARE

Ransomware is the most significant of today's cyber threats. A ransomware intrusion on your servers can completely block your access or encrypt most of your files until you pay the ransom cyber criminals request. Ransomware protection will efficiently detect, block and prevent ransomware attacks at an early stage to avoid dramatic damages.



PROHIBIT CONNECTION FROM NON-AUTHORIZED DEVICES

With the rise of BYOD and remote working, you need to be sure that every device can be controlled and kept safe. Thanks to ***Advanced Security***, you can either allow your user to use any device, or just allow him/her an access with a specific registered device.



PERMISSIONS - *MANAGE*

In Windows, permissions are taken care of by the Operating System which defines, by default, the scope of privileges for each user profile (read, write, modify) and automatically prevents access to sensitive locations on the server.

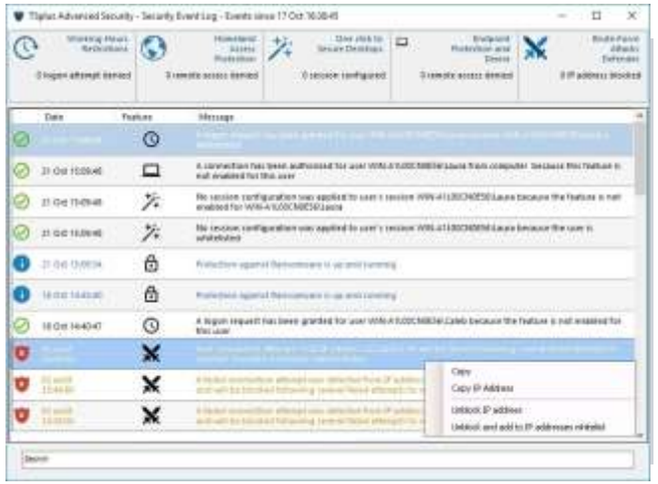
There are times, however, when it's necessary to manually configure permissions for the best network security. That's the case if your organization uses Remote Desktop technology.

If important files do not have the best permissions in place, successful connection by malicious users can quickly lead to compromised data.

The Permissions dashboard displays the list of users and groups and the list of available folders, side-by-side.

With ***Advanced Security***- Ultimate Edition, everything is visible at one spot and you can quickly Inspect and Edit Windows access rights per users & groups.

EFFICIENT PROTECTION AND EASY MANAGEMENT



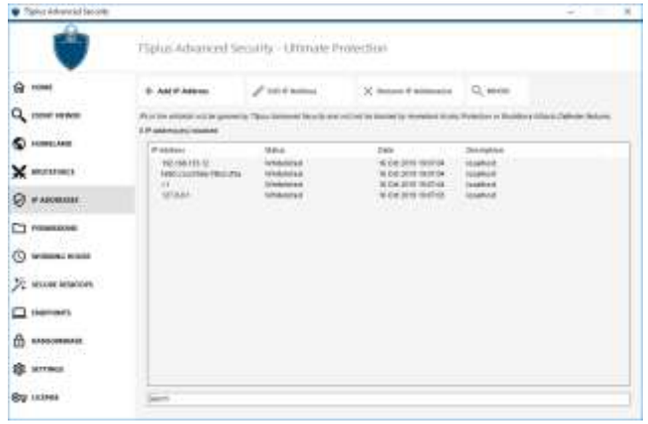
Check TS*plus* Advanced Security in Real-time.

With the Security Event Log, display all detailed information regarding the last 2500 events, and keep track of any logon request and configuration in real time.

The Event Log Monitors security events such as -

- Blocked, Failed or Granted connections.
- Stopped Attacks and Quarantined files.
- Configured User Sessions.

This offers a more relevant alternative to a full audit solution. In addition, a deep global search is also available for finding specific events quickly.



Unified and Efficient IP Address Management

IP address management is made easy with a single list to manage both blocked and whitelisted IP addresses.

A convenient search bar provides search capabilities based on all information provided.

Further, administrators can perform actions on several selected IP addresses with a single click, such as unblocking and adding to whitelist multiple blocked IP addresses.

It's also possible to provide meaningful descriptions to any IP address!

Pre-requisites:

TSplus Advanced Security is compatible with the following 32 and 64-bit OSs:

- ☑ Windows 7 to Windows 10
- ☑ Windows Server 2008 R2 to Windows Server 2019

KEEP THREATS OUT OF YOUR WINDOWS SYSTEM.

TSplus Advanced Security will protect you against Remote Desktop attacks.

Add it now to your TSplus Server!