TS PLUS ADVANCED SECURITY

Protect Remote Desktop connections and Remote Access environments.

All-in-one cybersecurity software designed for remote access

TSplus Advanced Security is a technology that caters to the requirements of both small and large businesses. It provides the fundamental protections needed by remote servers administrators. It offers seven different measures which can be activated to set the right level of security for the network. It offers two levels of protection: Essentials and Ultimate.

Homeland Protection

Restrict remote access to the people that need it:

- Country Restriction: Block unwanted countries and allow access from specific countries.
- Internet and IP Access Restriction: Restrict access from the Internet.
- Watched Processes: Add or remove processes that are watched by the Homeland Protection feature.

Brute Force Defender

Protects systems from Hackers and bots. Brute Force Defender enables you to protect your public server from hackers, network scanners and brute-force robots that try to guess your Administrator login and password. Monitor Windows failed login attempts and automatically block the offending IP addresses after a pre-determined number of failures.

Global IP Management

Easily manage IP addresses from a unified allow/block list.

- Easy Management: Single list for blocked and whitelisted
- Search Bar
- IP Address Description
- Multi-address Editing

Working Hours

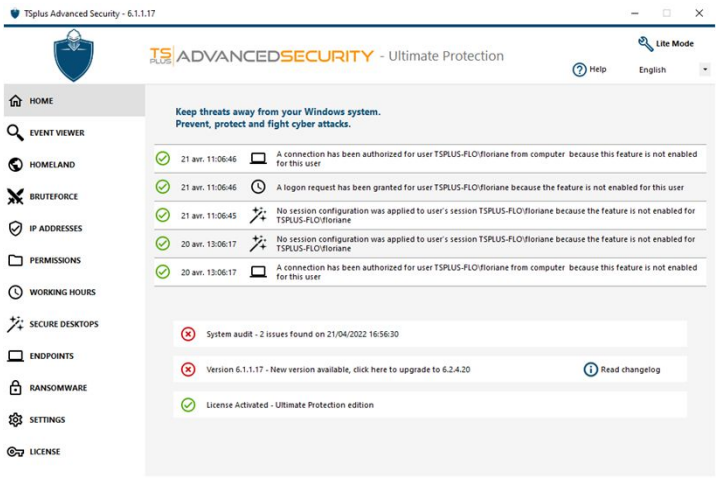
Limit remote access to business hours.

- Day and Time Restrictions: per days and timeslots. It is possible to select a specific time zone.
- User and Groups Permission
- Automated disconnection
- Notifications

Ransomware Protection

Efficiently detect, block and prevent ransomware attacks. TSplus Advanced Security reacts as soon as it detects ransomware on your server. It possesses both static and behavioral analysis:

- The static analysis enables the software to react immediately when an extension name changes.
- The behavioral analysis looks at how a program will interact with files and detect new strains of ransomware.
- Seamless Learning Period
- Automatically stops the attack and quarantines the affected programs and files. Administrators can review the list of quarantined items and decide to whitelist specific entries.
- Reports: Learn to anticipate threats by identifying the source of attacks and analyzing running processes listed in reports.
- Email Alerts: React in no time
- Snapshots: Quickly identify and recover affected files after an attack. Administrators can also edit the retention period of snapshots.
- Ignored file extensions: Easily define the file extensions that need to be excluded from the Ransomware Protection analyses.



Permissions

Manage remote access permission for users, groups and files.

- Side-by-side Permission Dashboard: Easily inspect and edit permissions of users, groups, files, folders and printers in a dashboard listing those elements side-by-side.
- Choose from four permissions: Deny, Read, Modify or Ownership.
- Inspect Permissions: Just with a click on a folder, subfolder or file displayed on a tree view. Audit specific files to monitor permissions in the event viewer.

Secure Desktop

Configure the security level for each user or group.

- Standard Security Levels (according to the Industry's best practices): *Windows Mode* - access to default Windows session, *Secure Desktop Mode* - access to documents, printers, Windows key and session disconnection, and *Kiosk Mode* - prevent a connected user from running prohibited actions..
- Customization tool
- Right Click and Context Menu Restrictions

Endpoint Protection and Device Control

Block compromised credentials and unwanted devices.

- Device Control: Administrators can decide whether a user can connect from any device or only specific device names. A list is automatically created anytime a device tries to connect.
- Endpoint Protection: By pairing devices to user accounts, Endpoint Protection prevents compromised credentials from being used to access your network.

Hacker IP Protection

Benefit from our worldwide Community blacklist of known threats: on-line attacks, on-line service abuse, malware, botnets and other cybercrime activities. Hacker IP Protection leverages the information provided by the community of Advanced Security users to **automatically blacklist more than 368 million identified threats daily.**

Admin Tool

Easily manage and configure all security features.

- User-friendly Dashboard
- Event log and features status
- Event interaction (search bar, right click)
- System Audit (monitor the operations and security)
- Lite Mode available for first-time users

Pre-Requisites:

1) Hardware

TSplus Advanced Security supports 32-bit and 64-bit architectures.

2) Operating system

Your server must use one of the following operating systems:

- Microsoft Windows version 7, Service Pack 1 (build 6.1.7601)
- Windows 2008 R2, Service Pack 1 (build 6.1.7601) or higher.

The required framework is .NET version 4.5.3 or higher.

Microsoft Windows 7 SP1 and Windows 2008 R2 SP1 require an additional update to support SHA2 Cross Signing (KB4474419). This update allows TSplus Advanced Security built-in firewall and ransomware protection to run properly.

The trial version of Advanced Security is the fully-featured Ultimate Edition. It is licensed per server.

Contact us

TSplus corporation
300 Spectrum Center Drive,
Irvine, CA 92618, USA
+1 949-561-1771