



Protégez les connexions Bureau à distance et les environnements d'accès à distance.

Logiciel de cybersécurité tout-en-un conçu pour l'accès à distance

TSplus Advanced Security est une technologie qui répond aux besoins des petites et grandes entreprises. Il offre les protections fondamentales nécessaires aux administrateurs de serveurs distants. Il propose sept mesures différentes qui peuvent être activées pour définir le bon niveau de sécurité pour le réseau. Il offre deux niveaux de protection : Essentials et Ultimate.

Protection nationale: Restreignez l'accès à distance aux personnes qui en ont besoin :

- Restriction par pays : Bloquez les pays indésirables et autorisez l'accès depuis des pays spécifiques.
- Restriction d'accès Internet et IP : Restreignez l'accès depuis Internet.
- Processus surveillés : Ajoutez ou supprimez les processus surveillés par la fonction de protection nationale.

Défense contre les attaques par force brute: Protège les systèmes contre les pirates et les robots. Brute Force Defender vous permet de protéger votre serveur public contre les pirates, les scanners réseau et les robots par force brute qui tentent de deviner votre nom d'utilisateur et votre mot de passe administrateur. Surveillez les tentatives de connexion échouées de Windows et bloquez automatiquement les adresses IP incriminées après un nombre prédéterminé d'échecs.

Gestion globale des adresses IP: Gérez facilement les adresses IP à partir d'une liste unifiée d'acceptation/blocage.

- Gestion facile : Liste unique pour les blocages et les autorisations.
- Barre de recherche
- Description de l'adresse IP
- Édition multi-adresses

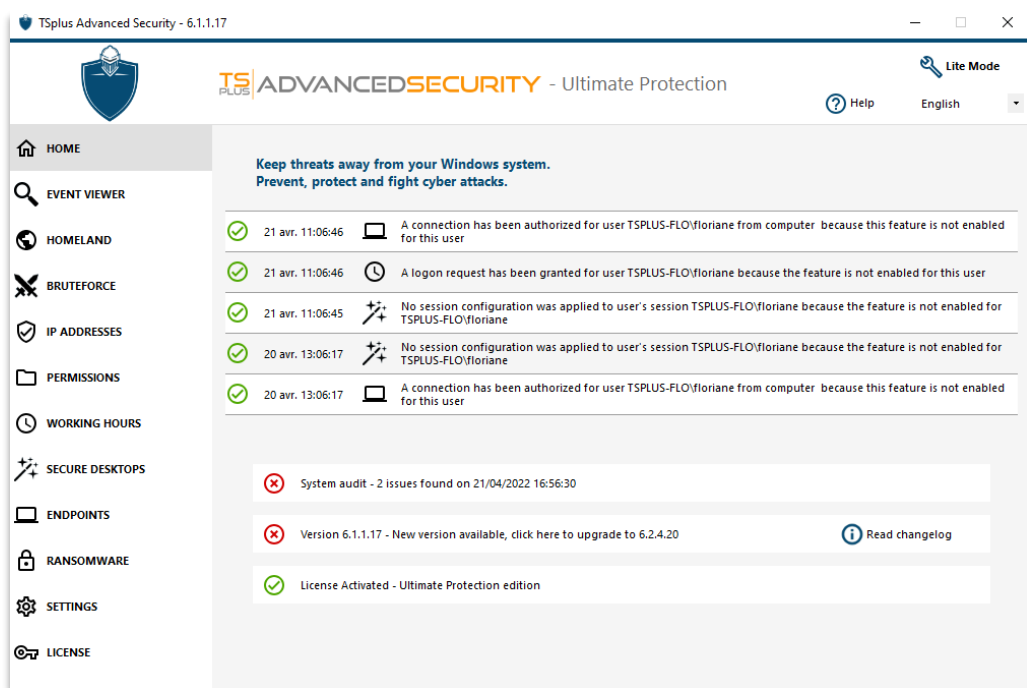
Heures de travail: Limitez l'accès à distance aux heures de bureau.

- Restrictions de jour et d'heure : par jours et créneaux horaires. Il est possible de sélectionner un fuseau horaire spécifique.
- Autorisations pour utilisateurs et groupes
- Déconnexion automatisée
- Notifications

Protection contre les ransomwares: Détectez, bloquez et prévenez efficacement les attaques de ransomwares. TSplus Advanced Security réagit dès qu'il détecte un ransomware sur votre serveur. Il possède une analyse statique et comportementale : L'analyse statique permet au logiciel de réagir immédiatement lorsqu'un nom d'extension change. L'analyse comportementale examine comment un programme interagira avec les fichiers et détecte de nouvelles souches de ransomwares.

- Période d'apprentissage transparente
- Arrête automatiquement l'attaque et met en quarantaine les programmes et fichiers affectés. Les administrateurs peuvent passer en revue la liste des éléments mis en quarantaine et décider de valider des entrées spécifiques.
- Rapports : Apprenez à anticiper les menaces en identifiant la source des attaques et en analysant les processus en cours répertoriés dans les rapports.
- Alertes par e-mail : Réagissez rapidement
- Instantanés : Identifiez rapidement et récupérez les fichiers affectés après une attaque. Les administrateurs peuvent également modifier la période de rétention des instantanés.
- Extensions de fichiers ignorées : Définissez facilement les extensions de fichiers à exclure des analyses de protection contre les ransomwares.





Permissions: Gérez les autorisations d'accès à distance pour les utilisateurs, les groupes et les fichiers.

- Tableau de bord d'autorisations: Inspectez et modifiez facilement les autorisations des utilisateurs, groupes, fichiers, dossiers et imprimantes dans un tableau de bord listant ces éléments côte à côte.
- Choisissez parmi quatre autorisations : Interdire, Lire, Modifier ou Propriété.
- Inspectez les autorisations : D'un simple clic sur un dossier, un sous-dossier ou un fichier affiché sur une vue arborescente. Auditez des fichiers spécifiques pour surveiller les autorisations dans l'observateur d'événements.

Bureau sécurisé: Configurez le niveau de sécurité pour chaque utilisateur ou groupe.

- Niveaux de sécurité standard (selon les meilleures pratiques de l'industrie) : Mode Windows - accès à la session Windows par défaut, Mode Bureau sécurisé - accès aux documents, imprimantes, touche Windows et déconnexion de session, et Mode Kiosque - empêche un utilisateur connecté d'exécuter des actions interdites.
- Outil de personnalisation
- Restrictions du clic droit et du menu contextuel

Protection des points d'extrémité et contrôle des périphériques: Bloquez les informations d'identification compromises et les périphériques indésirables.

- Contrôle des périphériques : Les administrateurs peuvent décider si un utilisateur peut se connecter à partir de n'importe quel périphérique ou uniquement de périphériques spécifiques. Une liste est automatiquement créée chaque fois qu'un périphérique tente de se connecter.
- Protection des points d'extrémité : En associant des périphériques aux comptes d'utilisateur, la protection des points d'extrémité empêche l'utilisation de données d'identification compromises pour accéder à votre réseau.

Protection des adresses IP des hackers: Bénéficiez de notre liste noire communautaire mondiale des menaces connues : attaques en ligne, abus de services en ligne, logiciels malveillants, botnets et autres activités de cybercriminalité. La protection des adresses IP des hackers tire parti des informations fournies par la communauté des utilisateurs de Advanced Security pour mettre automatiquement sur liste noire plus de 368 millions de menaces identifiées quotidiennement.

Outil d'administration: Gérez et configurez facilement toutes les fonctionnalités de sécurité.

- Tableau de bord convivial
- Journal des événements et état des fonctionnalités
- Actions sur les événements (barre de recherche, clic droit)
- Audit système (surveillance des opérations et de la sécurité)
- Mode Lite disponible pour les utilisateurs novices

Prérequis:

1) Matériel

TSplus Advanced Security prend en charge les architectures 32 bits et 64 bits.

2) Système d'exploitation

Votre serveur doit utiliser l'un des systèmes d'exploitation suivants :

- Microsoft Windows version 7, Service Pack 1 (build 6.1.7601)
- Windows 2008 R2, Service Pack 1 (build 6.1.7601) ou version ultérieure.
- Le framework requis est la version .NET 4.5.3 ou version ultérieure.
- Microsoft Windows 7 SP1 et Windows 2008 R2 SP1 nécessitent une mise à jour supplémentaire pour prendre en charge la signature croisée SHA2 (KB4474419). Cette mise à jour permet au pare-feu intégré à TSplus Advanced Security et à la protection contre les ransomwares de fonctionner correctement. La version d'essai d'Advanced Security est l'Édition Ultimate entièrement fonctionnelle. Elle est autorisée par serveur.

Contact us

TSplus SAS
63 Rue André Bollier,
69007 Lyon, FRANCE
+33 4 13 68 74 91