Soft4Europe

TS2log Security

Version 6

Nouvelle fonctionnalité :
Base de données d'adresses IP malveillantes

Accédez à vos serveurs Bureau à Distance et à vos Applicatifs EN TOUTE SÉCURITÉ

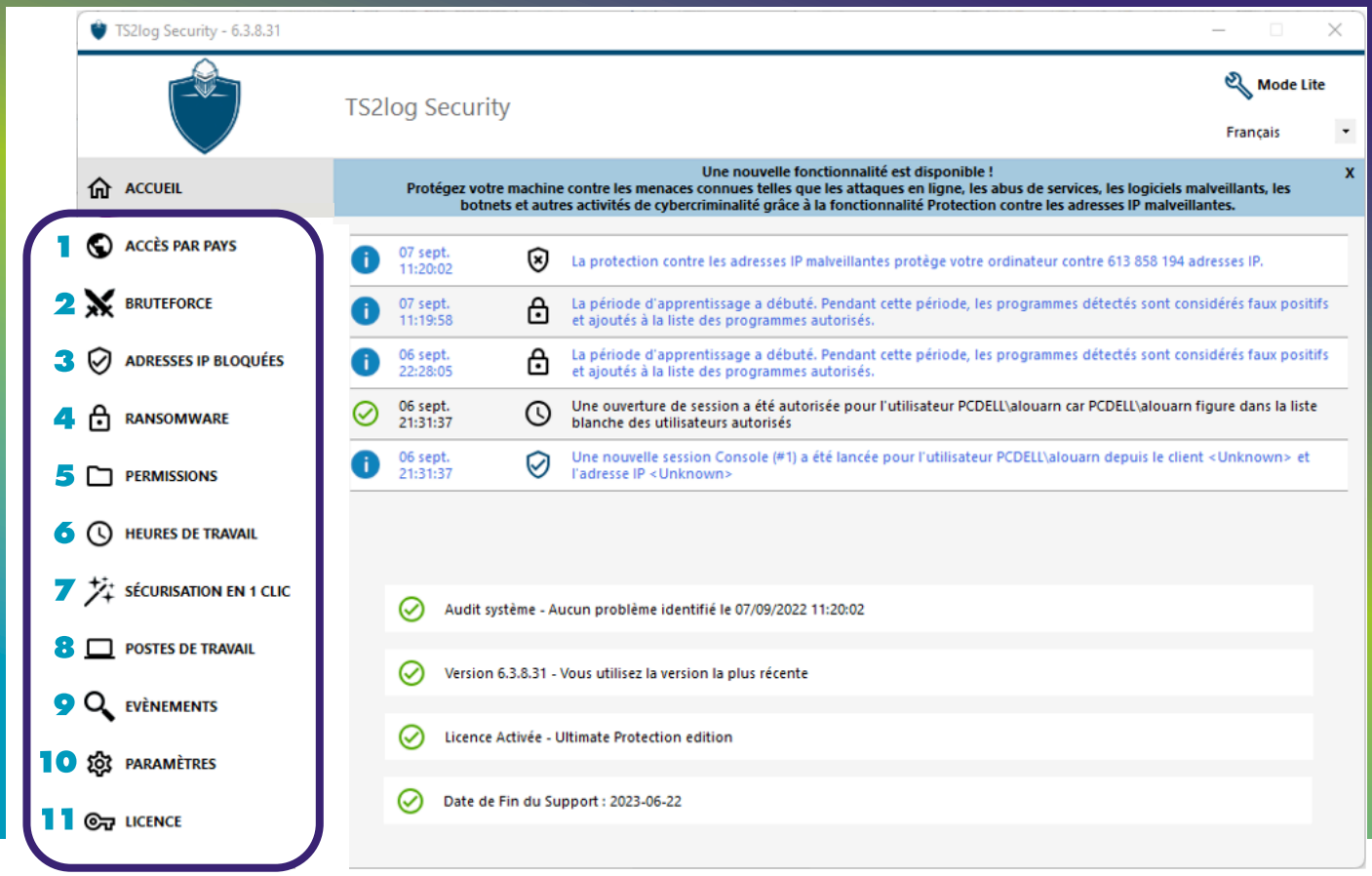
Maintenez votre serveur protégé

Que vous souhaitiez vous connecter à votre serveur Bureau Distant, votre serveur Applicatif ou encore votre ordinateur personnel depuis un site distant, TS2log Security est votre bouclier pour protéger ces machines contre les attaques non authentifiées.

Notre produit est conçu pour sécuriser les accès à distance incluant toute tentative d'accès (rdp, web, ports applicatifs comme SQL, HF-SQL, SSH, FTP, SFTP, ...), surveiller les tentatives échouées de Login/Mot de passe (Attaque par Force Brute), bloquer les connexions interdites ou suspectes et prévenir les actions non autorisées comme dans le cas des ransomware et des cryptolockers.

Par ailleurs les identifiants et les mots de passe peuvent être dérobés d'autant plus facilement quand il s'agit de connexions nomades, ouvrant ainsi la voie royale au vol de données.

L'onglet ACCUEIL vous fournit les principales informations concernant votre licence et vous alerte si une anomalie est détectée



TS2log Security apporte des protections indispensables :

1. Empêche les attaques en provenance des pays étrangers (Géo-restriction)
2. Empêche les attaques par Force Brute (Blacklistage automatique des IP suite aux échecs de connexion par mot de passe)
3. Blocage des IP (Liste blanche pour IP autorisées) et base de données d'adresses IP malveillantes
4. Détecte et bloque les attaques de ransomware (Anti-ransomware)
5. Limites les accès des fichiers et dossiers (Gestion des permissions)
6. Empêche les accès aux serveurs durant la nuit (Gestion d'accès par plages horaires)
7. Sécurise l'interface des utilisateurs (droits des utilisateurs-GPO)
8. Restreint les accès au serveur en fonction du nom NetBios du périphérique d'accès

Paramétrage des protections :

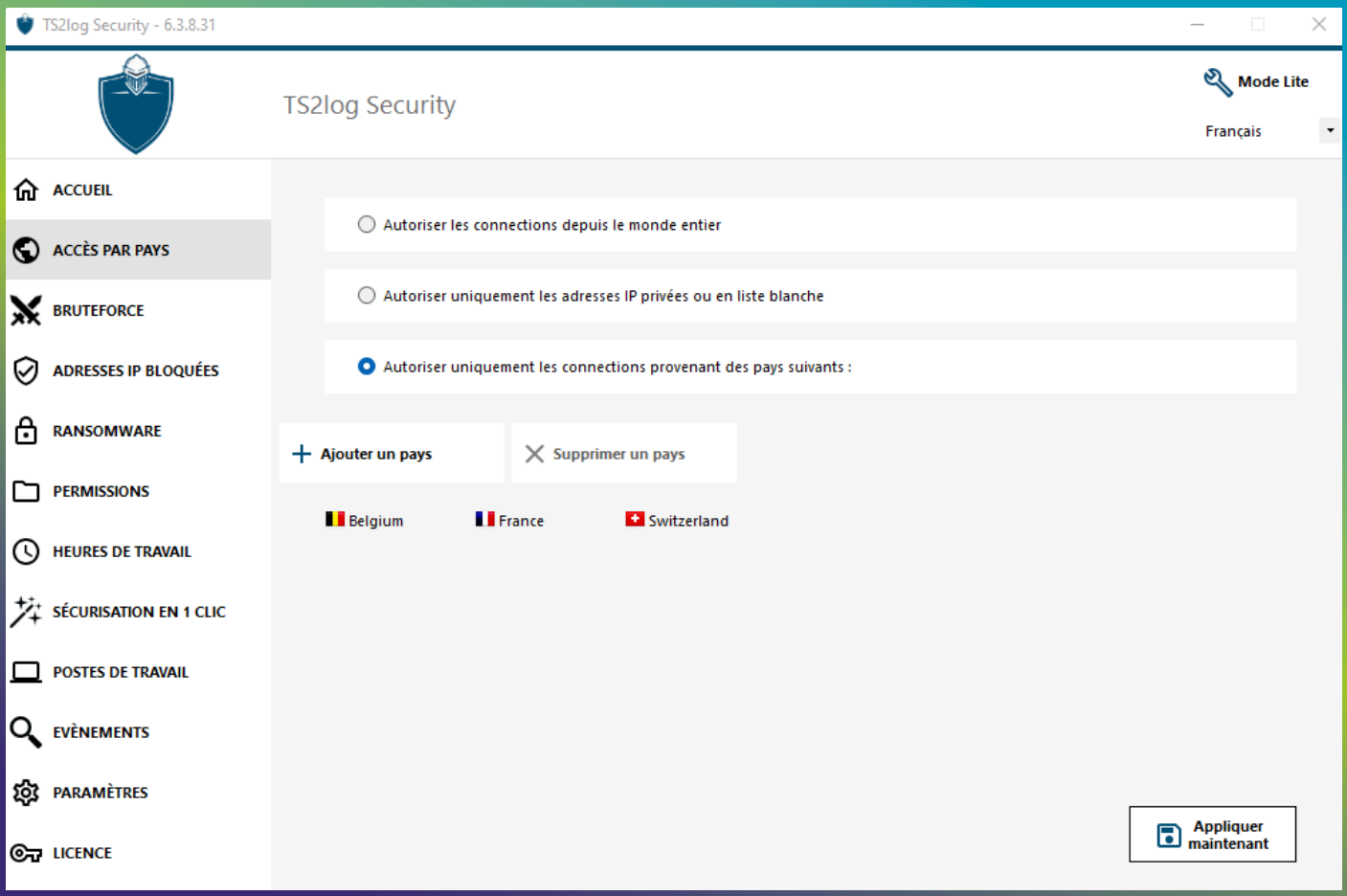
9. Permet d'appliquer des paramétrages supplémentaires aux différentes fonctionnalités

Informations utiles :

10. Historisation des principaux événements
11. Informations et activation de la licence

1 - Géo-Restriction :

Vos utilisateurs sont situés, par exemple, en France, Canada, États-Unis, Angleterre. Pourquoi quelqu'un pourrait-il pouvoir ouvrir une session depuis la Chine, l'Inde ou l'Allemagne ?
En un clin d'oeil avec TS2log-Security, vous protégez vos serveurs Bureau Distant des attaquants essayant d'ouvrir une session à partir de pays étrangers.



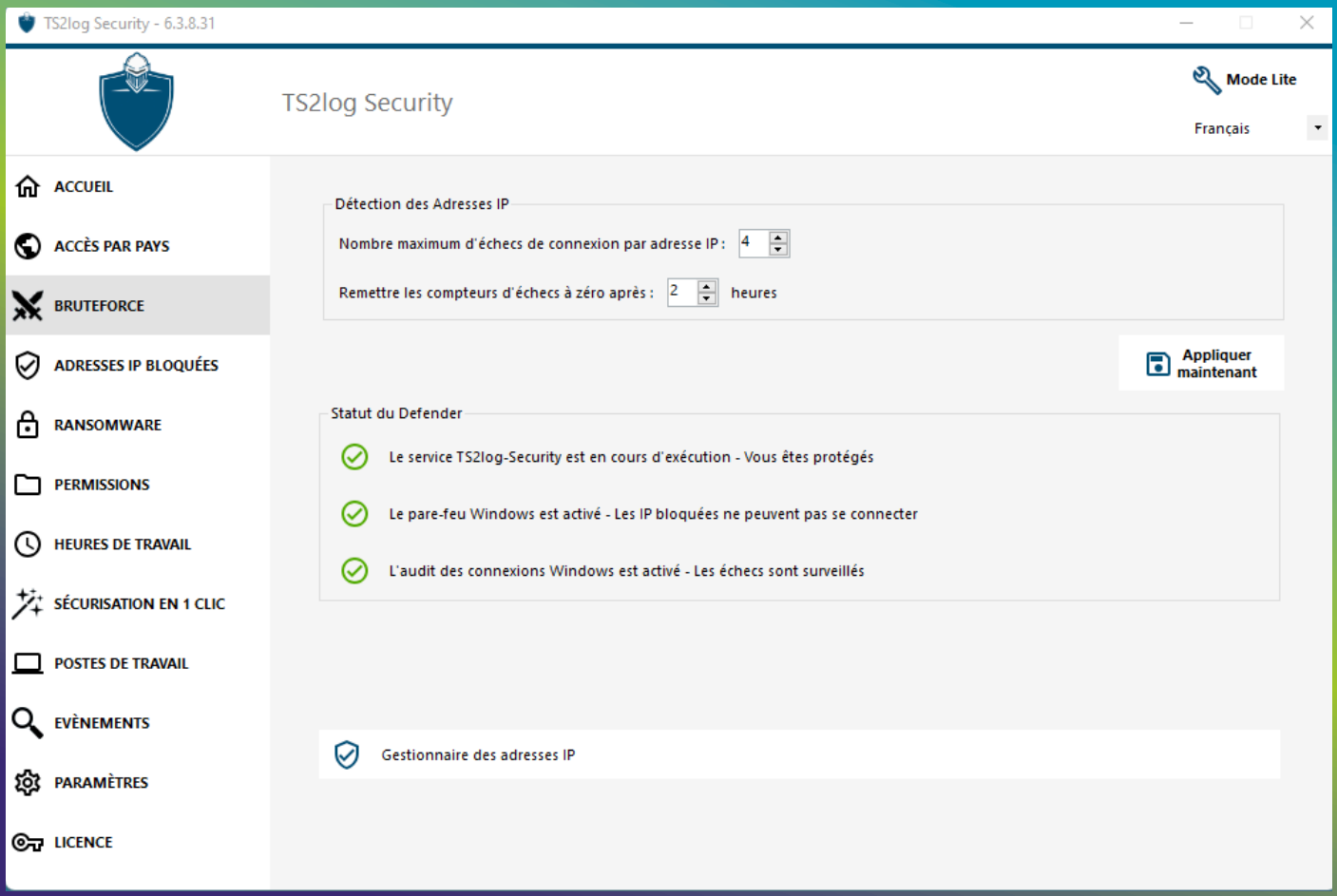
Cette fonctionnalité déclenche une analyse des flux entrants TCP/IP et bloque les flux en provenance des pays non-autorisés. Par exemple vous pouvez protéger les accès à votre serveur FTP ou à vos bases de données.

C'est extrêmement simple et puissant.

Faites-le !

2 - Bloquer les attaques par Force Brute

Si votre serveur Windows est publiquement accessible sur Internet, il existe une probabilité de 100% que les pirates informatiques, les scanneurs de réseau et les robots de Brute- Force tentent de deviner votre identifiant et votre mot de passe administrateur... pendant que vous lisez ces lignes.



À l'aide des mots-clés actuels et de dictionnaires de mot de passe, ils tentent de se connecter à votre serveur à haute fréquence (des milliers de fois par minute).

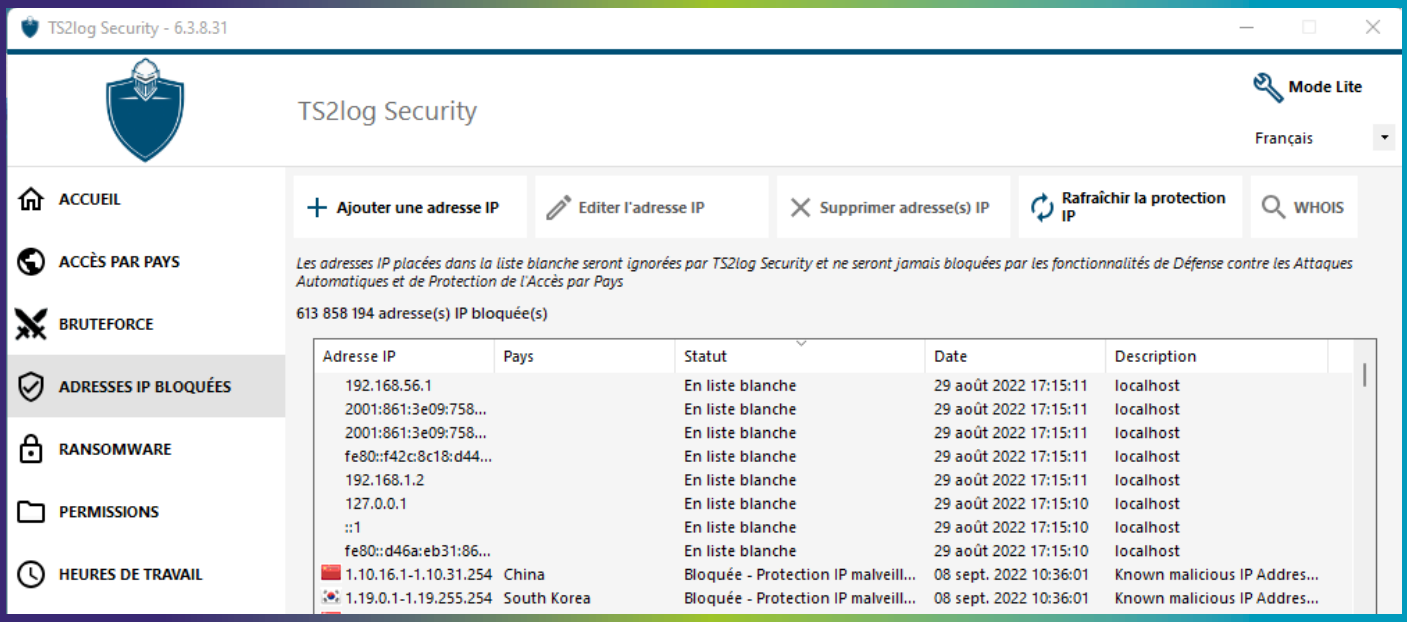
Non seulement cela est mauvais pour la sécurité de votre serveur, mais cela peut également consommer beaucoup de ses ressources (CPU et bande passante) !

TS2log Security protégera instantanément votre serveur en surveillant les tentatives de connexion échouées à Windows et établira automatiquement après plusieurs tentatives de connexion échouées la liste noire des adresses IP incriminées.

De plus, vous pouvez spécifier manuellement les adresses IP à autoriser/bloquer selon vos besoins.

3 - Gestion globale des adresses IP

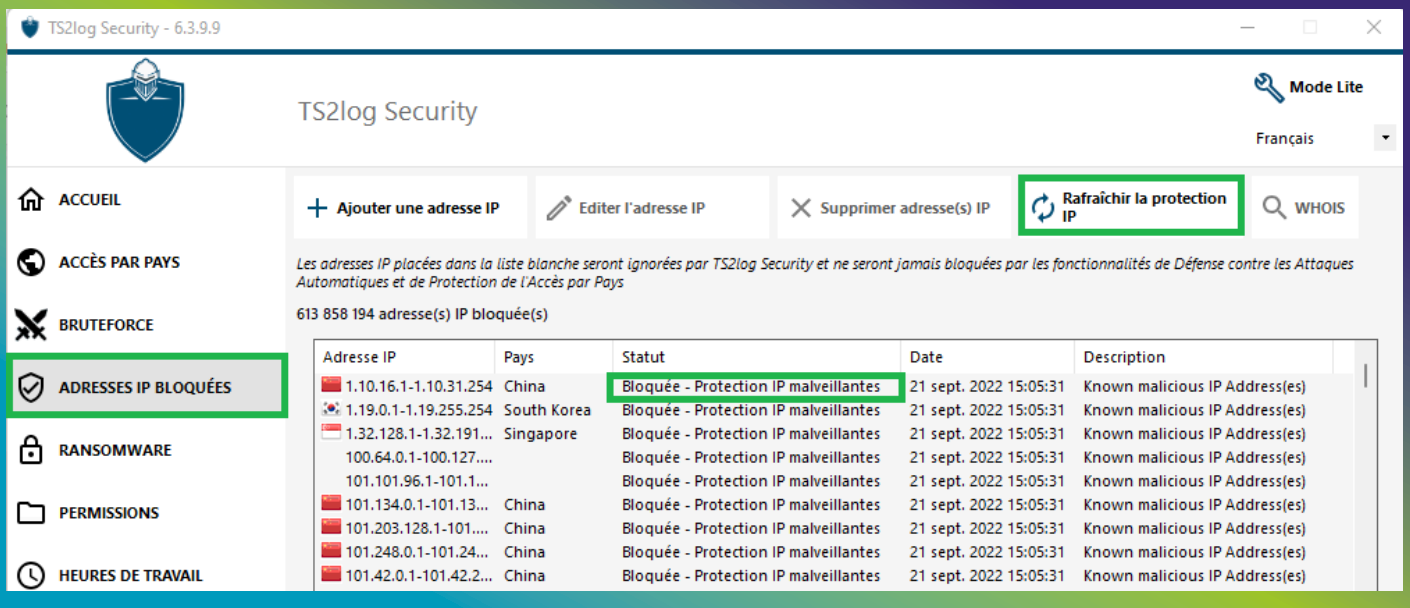
Gérez facilement les adresses IP à partir d'un seul endroit avec une seule liste pour les adresses IP bloquées et celles qui sont autorisées.



Cela signifie que toutes les IP détectées par les protections de Géo-restriction et BruteForce sont centralisées pour être vérifiées, modifiées, ajoutées ou supprimées à votre convenance.
Les listes d'adresses IP sont consultables, ce qui en facilite la gestion.

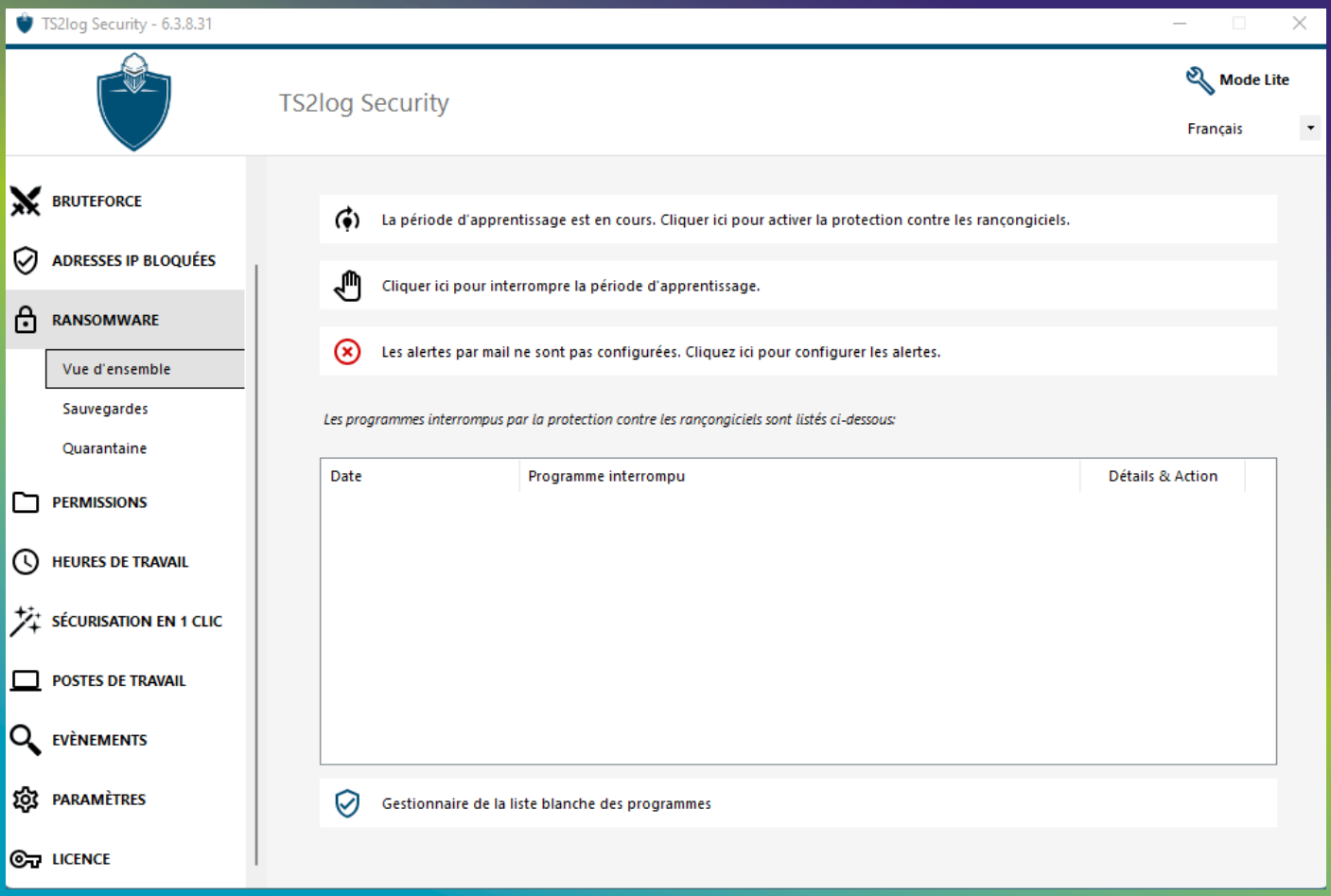
NOUVEAU : Depuis la version 6.30 vous bénéficiez d'une base de données d'adresses IP malveillantes qui est mise à jour quotidiennement.

Les règles de votre pare-feu sont mises à jour automatiquement



4 - Détecter et bloquer les Rançongiciels

Stoppez les attaques de ransomware !
Les ransomwares sont la plus importante des cybermenaces actuelles.



Il est facile de les télécharger par erreur depuis un site Web compromis, de les ouvrir via des pages de publicité malveillantes ou de les recevoir en pièce jointe à partir d'emails spammés.

Leurs actions sur vos systèmes vont soit verrouiller complètement votre accès, soit crypter la majorité de vos fichiers jusqu'à ce que vous payiez la demande de rançon des cybercriminels.

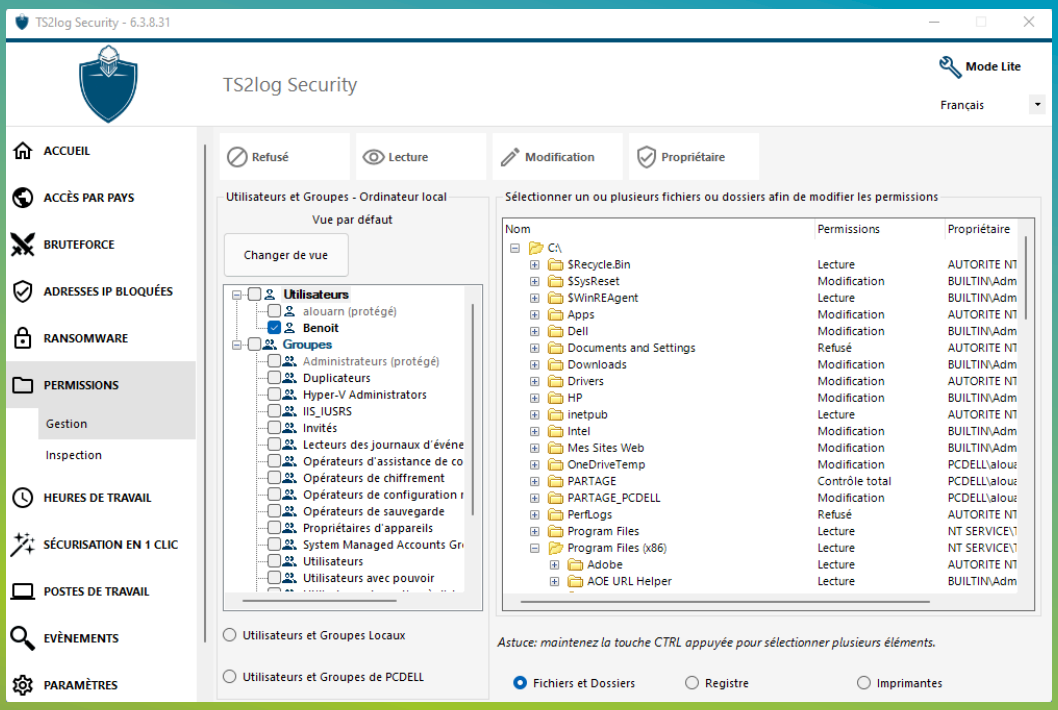
Toutefois, cela ne garantit pas la restitution de vos données et peut paralyser vos activités commerciales ou même entrainer la perte définitive de vos données.
La protection anti-ransomware de TS2log Security détectera, bloquera et empêchera efficacement les attaques de ransomware.

Vous éviterez des conséquences catastrophiques pour votre entreprise en supprimant rapidement le logiciel de ransomware.

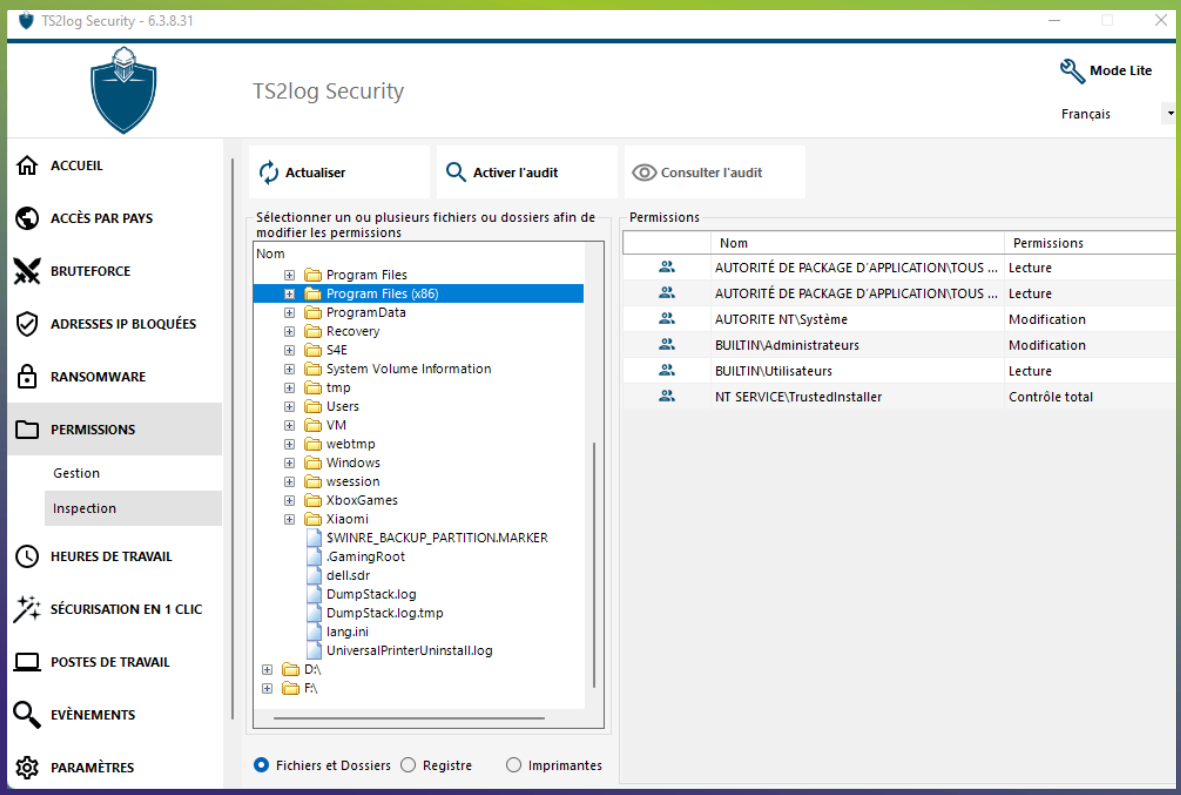
5 - Gestion et inspection des permissions sur les fichiers et dossiers

Le tableau de bord «Permissions» affiche côte à côte la liste des utilisateurs et des groupes ainsi que la liste des dossiers et fichiers disponibles.
Tout est visible à un seul endroit, ce qui simplifie l'inspection des privilèges (Security Essentials) et leurs modifications (Ultimate Protection) pour chaque utilisateur.
L'onglet Gestion permet la modification des permissions

L'onglet gestion permet la modification des permissions.



L'onglet Inspection autorise seulement la vérification des permissions



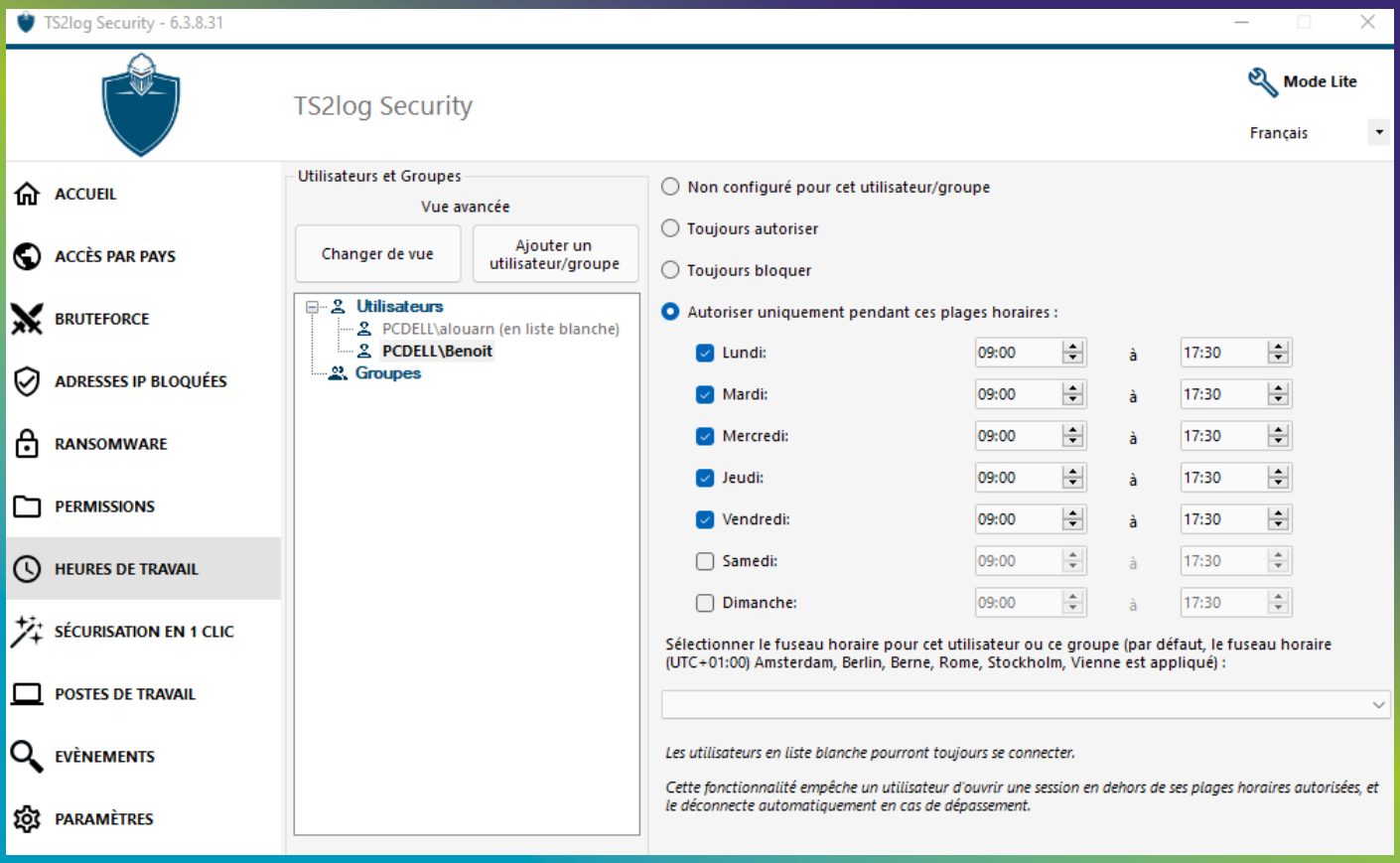
6 - Restriction d'accès par plage horaire

Bien sûr, vos utilisateurs devraient être libres de se connecter et de travailler quand ils se trouvent au bureau.
Avec L'Édition Essentials, vous pouvez spécifier une plage horaire unique* pour les utilisateurs qui ne pourront ouvrir des sessions qu'à l'intérieur de cette plage horaire. Cela contribuera ainsi à renforcer votre politique de sécurité.

Restrictions de jour et d'heure.

N'autorisez les utilisateurs ou groupes à se connecter que pendant certains jours et plages horaires. Il est possible de sélectionner un fuseau horaire spécifique en fonction de l'emplacement géographique du bureau de votre utilisateur.

** Pour gérer de multiples plages horaires pour des utilisateurs ou des groupes, choisissez TS2log-Security Ultimate*



Autorisation des utilisateurs et des groupes

Gérez les autorisations de plage horaire pour des utilisateurs ou des groupes spécifiques. Si un utilisateur appartient à plusieurs groupes, les autorisations les plus permissives s'appliquent.

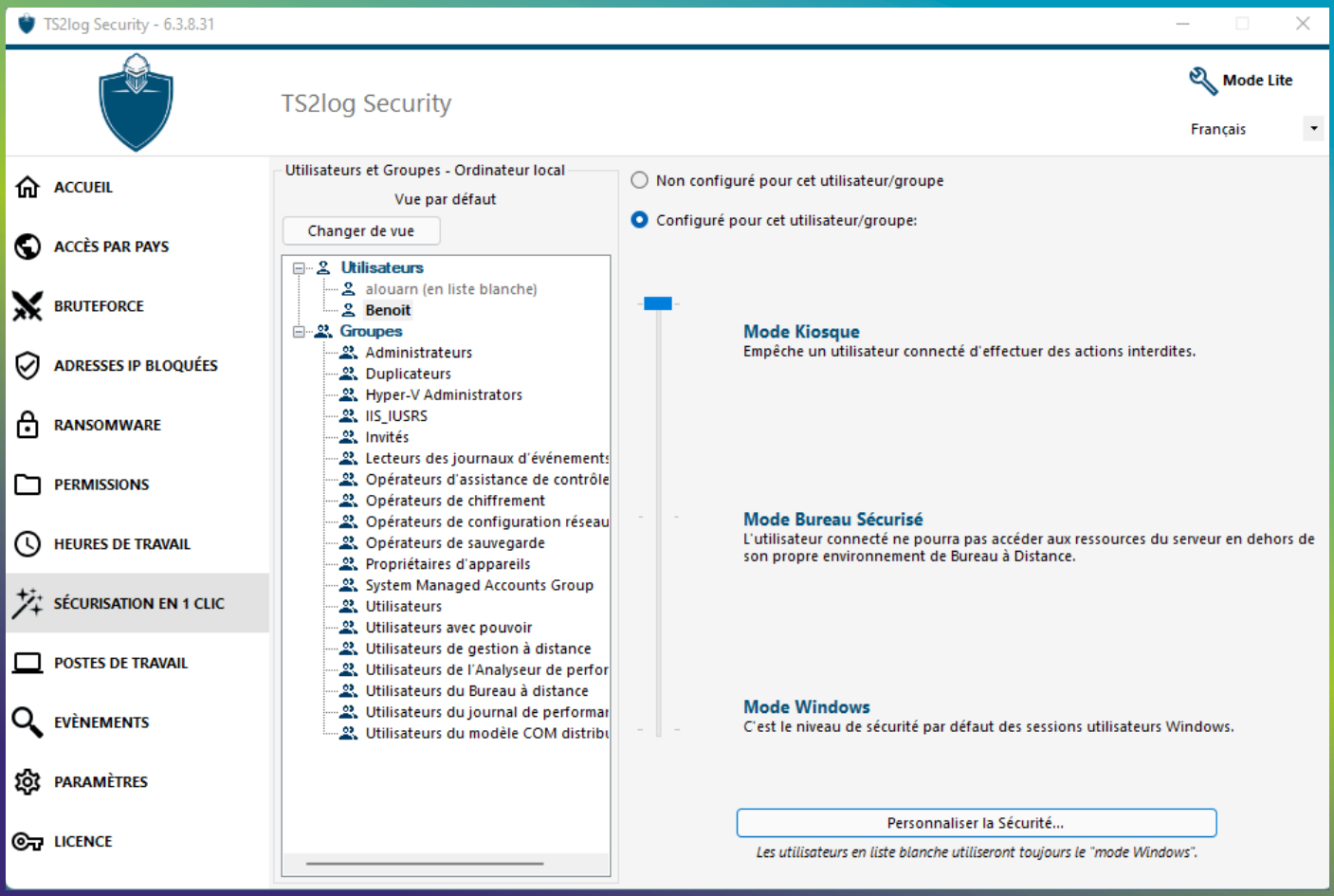
Déconnexion automatisée

Les sessions utilisateurs peuvent être automatiquement déconnectées à la fin du créneau horaire autorisé.

Avis

Programmez un message d'avertissement pour informer l'utilisateur avant qu'il ne soit automatiquement déconnecté.

7 - Définissez facilement les règles des droits des utilisateurs grâce à 3 niveaux de sécurité personnalisables :



Windows fournit de nombreuses et puissantes GPO, mais cela vous coûtera plusieurs jours d'effort pour trouver, configurer et affiner les règles de sécurité attendues.

3 Niveaux de sécurité

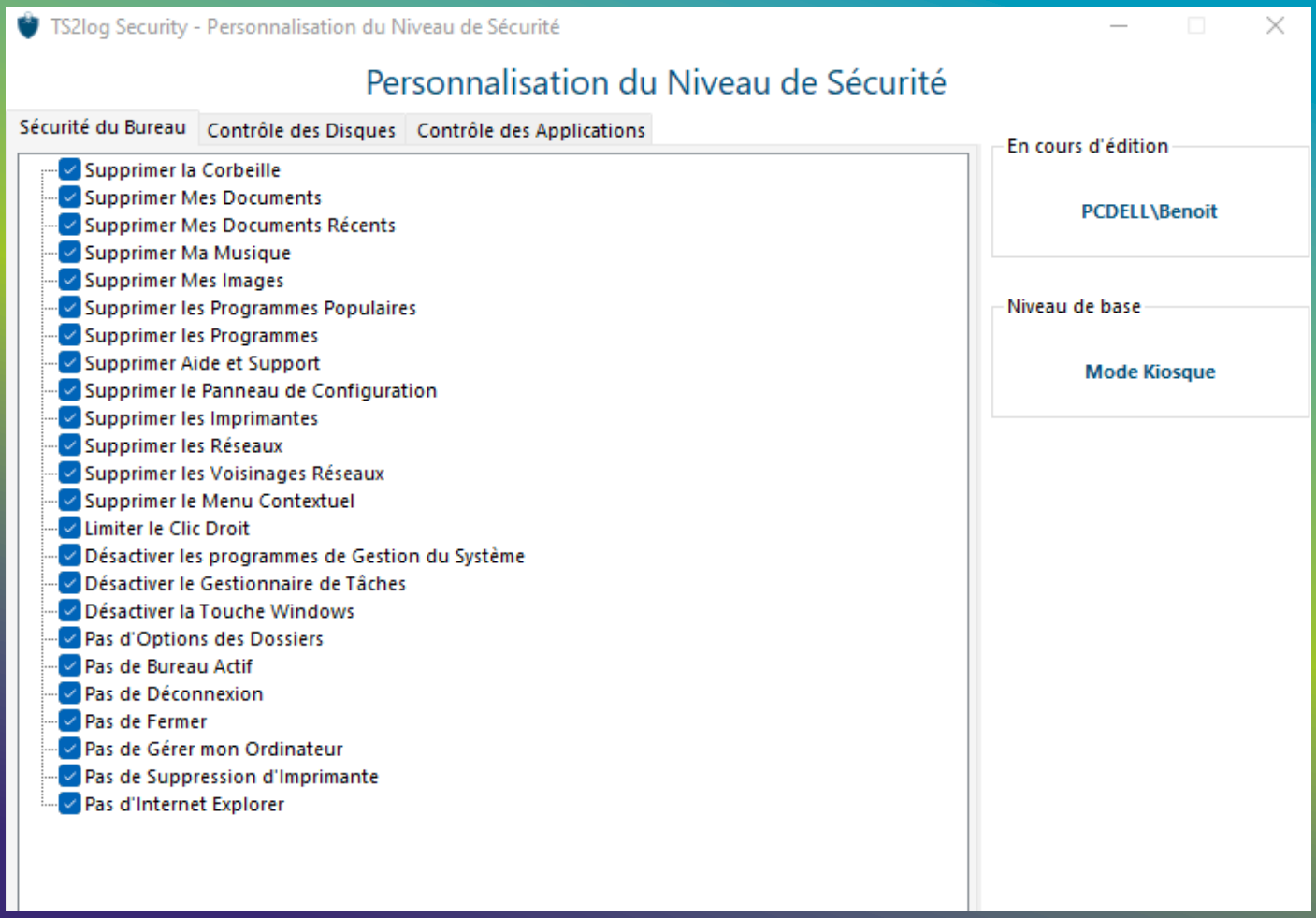
Vous pouvez configurer le niveau de sécurité pour chaque utilisateur ou groupe en sélectionnant l'un des trois niveaux de sécurité standardisés conçus selon les meilleures pratiques de l'industrie informatique :

Mode Windows : accès à la session Windows par défaut

Mode bureau sécurisé : accès aux documents, imprimantes, clé Windows et déconnexion de session

Mode Kiosque : empêche un utilisateur connecté d'exécuter des actions interdites.

Personnaliser le niveau de sécurité



Les administrateurs peuvent facilement personnaliser le niveau de sécurité de chacun des trois modes standard en fonction de leurs propres besoins.

Sélectionnez ou désélectionnez simplement des dossiers, des disques et des applications.

Limitez la possibilité de cliquer avec le bouton droit et d'accéder au menu contextuel pour empêcher les utilisateurs d'effectuer des actions indésirables.

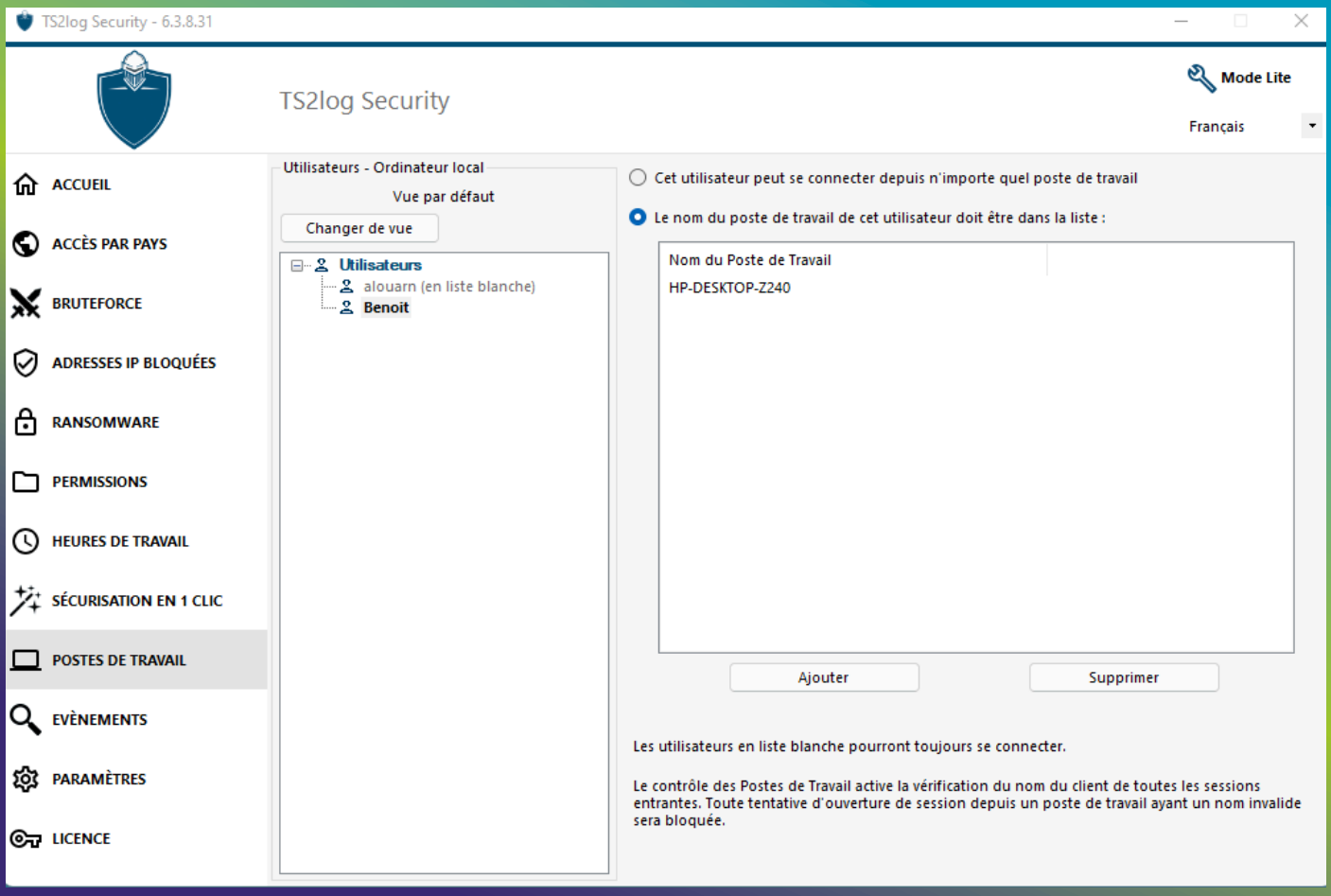
8 - Restriction d'accès par le nom NetBios du périphérique d'accès

Contrôle de l'appareil

Les administrateurs peuvent décider si un utilisateur peut se connecter à partir de n'importe quel appareil ou uniquement à partir de noms d'appareils spécifiques. TS2log Security crée automatiquement une liste des appareils qui tentent de se connecter, facilitant la tâche de l'administrateur d'accepter ou de refuser l'accès à des appareils spécifiques.

Protection des terminaux

En associant des appareils à des comptes d'utilisateurs, TS2log Security empêche l'utilisation d'informations d'identification compromises pour accéder à votre réseau, car l'attaquant aurait besoin d'un appareil autorisé pour se connecter.

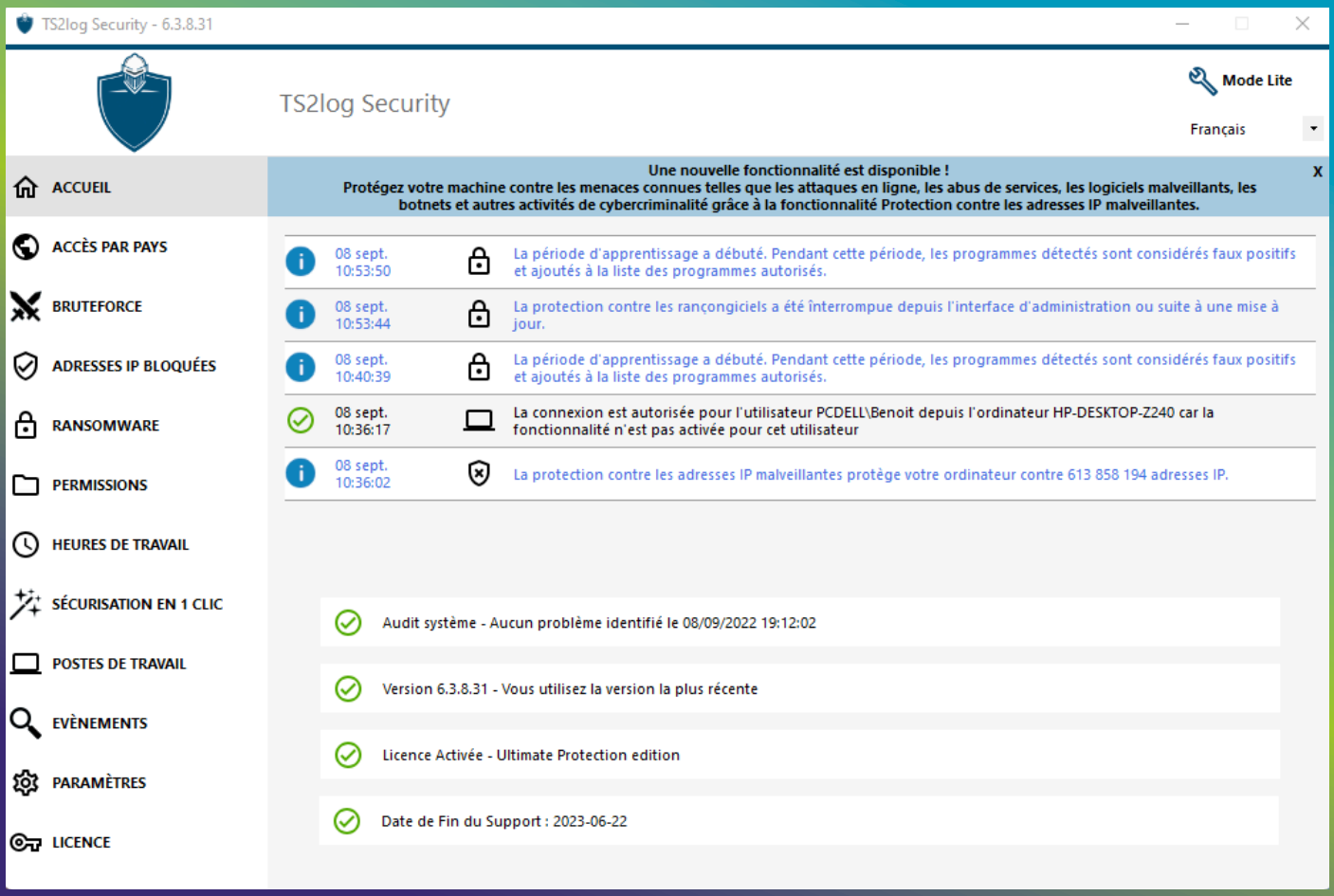


Comment ça marche ?

TS2log Security Ultimate enregistrera le nom de l'appareil à sa première connexion.
L'administrateur peut décider de restreindre l'accès pour cette connexion au seul nom de ce poste de travail (ou plusieurs).
Toute tentative de connexion à partir d'un autre appareil sera automatiquement détectée et rejetée. Cette fonctionnalité est opérationnelle uniquement avec une connexion RDP via un client de connexion ou en RemoteApp.

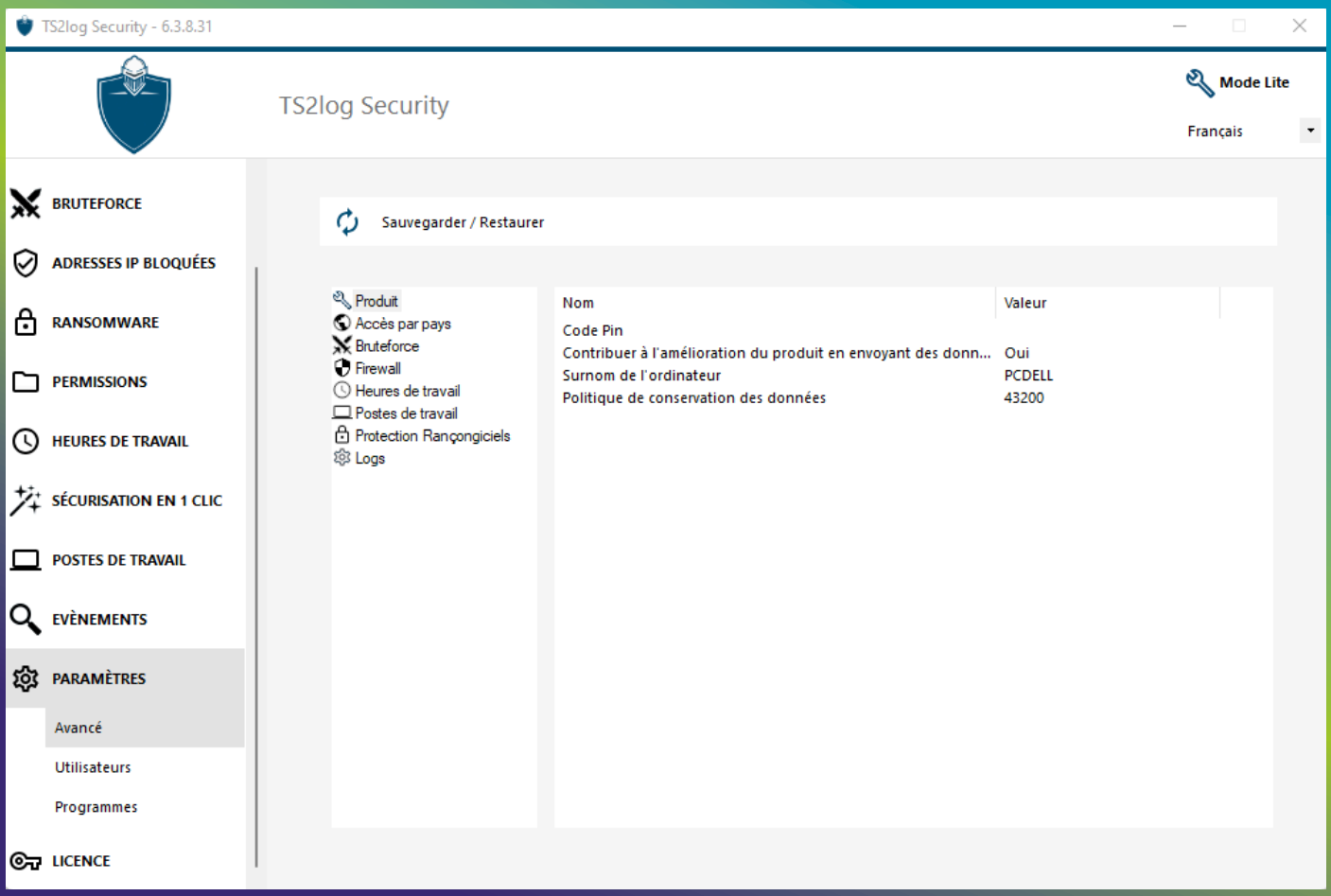
9 - Evénements

En cliquant sur cet onglet, vous aurez accès à l'historique des événements de sécurité de TS2log Security



10 - Paramètres

Dans cette rubrique, vous aurez la possibilité de configurer certaines options de TS2log Security.



Avancé :

Une option de sauvegarde/restauration est disponible
D'autres options sont disponibles telles que la mise en place d'un code PIN (Produit) pour l'ouverture sécurisée de la console d'administration de TS2log Security, la modification du message d'alerte (Heures de travail) l'activation des Logs, et bien plus encore.

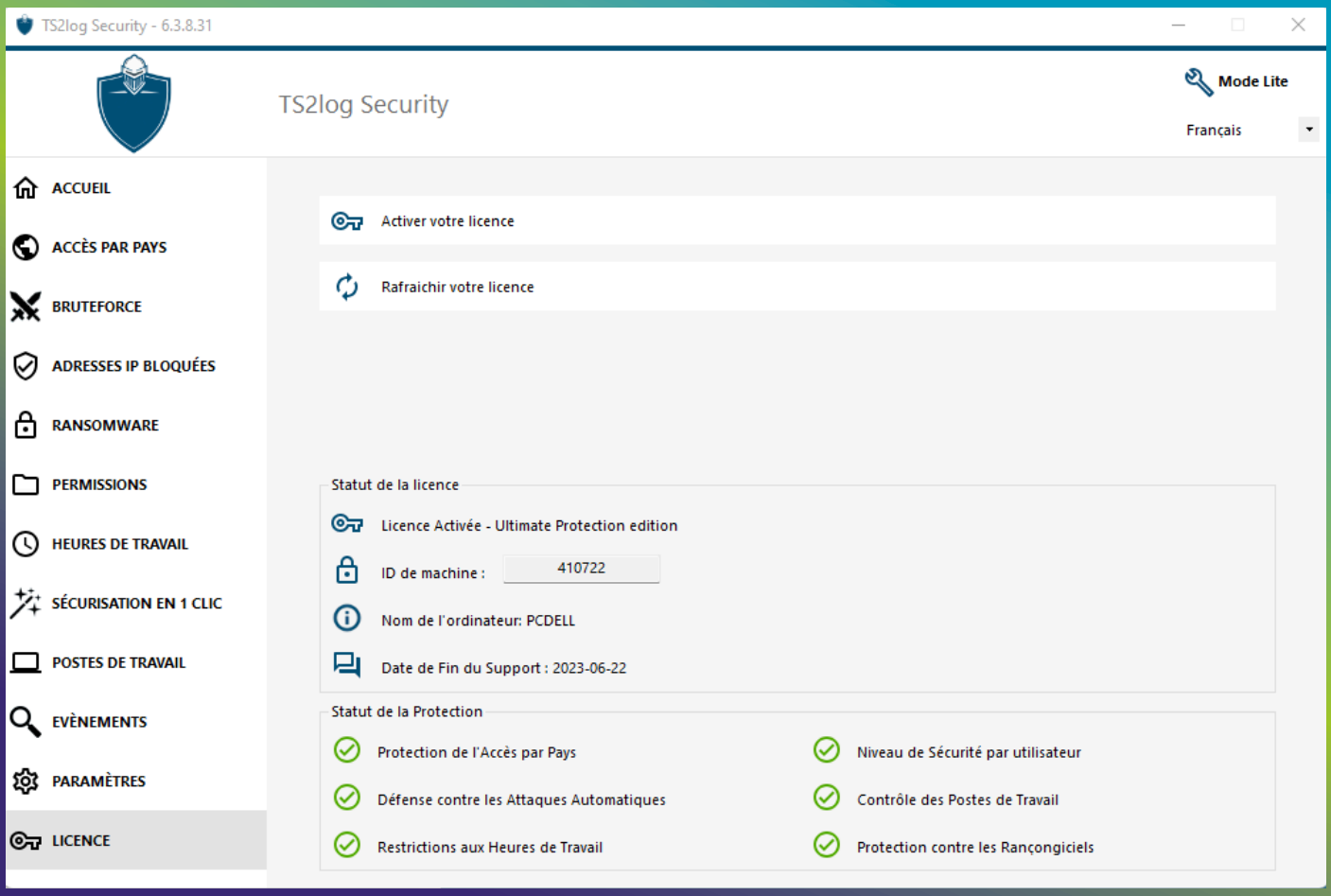
Utilisateurs :

Grâce à cette fonctionnalité, vous pourrez ajouter ou supprimer des utilisateurs en liste blanche. Par défaut, l'Administrateur du poste y sera inséré.

Programmes :

Idem pour les dossiers et applications, que vous pourrez ajouter ou supprimer de la liste blanche

11 - Licence



Dans cette rubrique, vous aurez la possibilité d'activer votre licence ou de la rafraichir en cas de modification de cette dernière (éditions et support).

Dans la seconde partie, sera remonté :

- L'édition de la licence.
- L'ID de votre machine.
- Le nom du poste Windows.
- La date de fin de la maintenance (Mise à jour, correctifs et nouvelles fonctionnalités) associée à votre Licence TS2log

Ainsi que le statut de vos protections.

Fonctionnalité	Description	Édition Essentials	Édition Ultimate
Géo-restriction	Choisissez la zone géographique (pays) à partir desquels les connexions seront autorisées	√	√
Restriction Horaire	Choisissez les horaires auxquels l'ensemble des utilisateurs auront accès à votre serveur» avec la version Essentials	√	
Restriction Horaire	Choisissez les horaires auxquels chaque utilisateur / Groupe d'utilisateurs auront accès à votre serveur» pour la version Ultimate		√
Bloque les attaques de Force Brute	Blacklistage automatique des IP attaquantes	√	√
Gestion globale des adresses IP	Gérez les adresses IP bloquées et autorisées avec une seule liste	√	√
Protection IP contre les hackers	Depuis la version 6.3.6.8 du 8 juin dernier, TS2log intègre une base de données de plusieurs centaines de millions d'adresses IP dangereuses	√	√
Inspection de permissions	Inspection centralisée des permissions sur les fichiers et dossiers	√	
Modification des permissions	Modification des permissions : Ouverture - Lecture - Modification		√
Droit des Utilisateurs	Configurez le niveau de sécurité pour chaque utilisateur ou groupe		√
Restriction par périphérique d'accès	Associez les identifiants de connexion au nom NetBios de la machine qui se connecte. Uniquement en RDP.		√
Anti-Ransomware	Détectez, bloquez et prévenez efficacement les attaques de ransomwares		√