

NTRglobal offre des solutions de support à distance basées sur les technologies les plus avancées. NTRsupport utilise des mesures de sécurité à tous les niveaux pour assurer la protection absolue des données du client et du technicien au cours de chaque session de support à distance:

#### **Conformité TRUSTe**

NTRglobal est titulaire d'une licence TRUSTe et se conforme ainsi aux exigences draconiennes de TRUSTe en matière de confidentialité, qui interdisent toute divulgation non autorisée d'informations personnelles ou professionnelles à une tierce partie. TRUSTe est une organisation indépendante à but non lucratif dont la mission est de bâtir la confiance des utilisateurs en Internet par la promotion des pratiques équitables en matière d'information.

#### **Cryptage ultramoderne**

Pour une sécurité maximale, NTRglobal utilise le système de cryptage de données AES (Advanced Encryption Standard) 256 bits, ainsi que des protocoles standards tels que le SSL pour assurer la protection de vos données. Tous les échanges en cours de session, y compris le chat, les images, l'audio, la vidéo, le partage de bureau et le transfert de fichier, sont totalement sécurisés.

#### **Sécurité par identifiant et mot de passe**

NTRsupport utilise l'authentification par mot de passe et limite l'accès à toutes ses applications par identifiants et mots de passe. Les mots de passe sont hachés et cryptés et ne voyagent jamais par Internet. La procédure d'identification utilise une règle de « trois essais » pour bloquer temporairement un identifiant lorsqu'un mot de passe incorrect est entré trois fois de suite. De plus, vous pouvez limiter les identifiants à une série d'adresses IP spécifiques, individuelles ou de groupe, et donc restreindre l'accès Opérateur et Administrateur à NTRsupport. Pour se conformer aux règles internes sur les mots de passe, vous pouvez définir la force d'un

mot de passe et la fréquence à laquelle il doit être changé.

Les fonctions de NTRsupport ne sont accessibles qu'avec les autorisations attribuées à chaque Opérateur par l'Administrateur. Par exemple, un Administrateur peut décider quels Opérateurs peuvent avoir accès aux fonctions telles que le co-surfing ou le contrôle à distance. Il peut également limiter les modes de contrôle disponibles pour autoriser le mode observateur ou démonstration (un utilisateur peut voir mais ne peut interférer avec un autre bureau).

Les Administrateurs peuvent également demander à ce que les sessions entre l'Opérateur et l'utilisateur emploient une connexion SSL quel que soit le mode de navigation sélectionné par l'utilisateur, garantissant ainsi que le cryptage des données en circulation est utilisé pour toutes les transmissions.

#### **Connectivité sécurisée**

NTRsupport utilise les paquets TCP et les ports standards et est compatible avec les firewalls et les serveurs proxy qui exécutent des règles NAT (Network Address Translations). Les connexions peuvent être établies par LAN (Local Area Network) ou toute autre connexion Internet. Cela signifie qu'un Opérateur peut travailler hors entreprise ou à partir d'un autre pays sans connexion VPN et peut néanmoins se connecter au service NTRsupport de la société via un navigateur pour fournir un support à distance à un autre PC ou Mac connecté à Internet.

Les fonctions de chat sont 100% Web et n'utilisent que les protocoles JavaScript et HTTP par les ports standards 80 ou 443. Les sessions de contrôle à distance

peuvent être établies en utilisant les connexions point-à-point (peer-to-peer) à l'intérieur du même réseau ou via le serveur relais de NTR par les ports standards. Les Administrateurs NTRsupport peuvent également attribuer un port spécifique à un Opérateur.

#### **Suppression automatique de la surface d'encombrement**

A la fin de chaque session de contrôle à distance, tous les composants actifs de la session de contrôle à distance sont automatiquement supprimés de la machine de l'utilisateur, empêchant ainsi tout accès non autorisé dans le futur.

#### **Autorisation et contrôle d'accès pour le support à distance**

Les sessions de contrôle à distance sont toujours codées avec le cryptage AES 256 bits de bout en bout. NTRsupport demande systématiquement l'autorisation du client avant de commencer une session de support à distance à la demande ou de surveillance. Une fois l'autorisation accordée par le client, le technicien peut voir l'ordinateur du client comme s'il était assis devant.

Pendant une session de support à distance, le client peut mettre fin au partage d'écran ou à la visualisation de l'écran, refuser des téléchargements ou des transferts de fichiers et reprendre le contrôle du bureau à tout moment. Le client a ainsi toujours le contrôle final sur sa machine.

#### **Sélection d'application sécurisée**

En utilisant la fonction Sélection d'application, l'utilisateur dont le bureau est contrôlé à distance peut, à partir d'une liste de toutes les applications, sélectionner celles qui sont disponibles pour être visualisées ou utilisées. Cette fonction permet au technicien et au client de limiter le contrôle à distance à une application ou

un groupe d'applications spécifiques, lorsque l'un ou l'autre est réticent à autoriser une visibilité totale ou un contrôle total.

#### **Changement de direction de la visualisation, uniquement après autorisation expresse**

Vous pouvez modifier la direction de la visualisation ou le mode de contrôle à distance sans vous déconnecter complètement du client. Cependant, chaque modification de mode ou de visualisation nécessite l'accord du client. Par conséquent, cela n'est possible qu'avec l'autorisation expresse du client.

#### **Bloquer des utilisateurs**

Pour protéger les Opérateurs du harcèlement ou des utilisateurs indésirables, NTRsupport comporte une fonction qui permet aux Opérateurs de bloquer temporairement, et aux Administrateurs de bloquer de manière permanente, certains utilisateurs afin de les empêcher d'accéder aux Opérateurs. L'Administrateur du site gère cette fonction de blocage et peut également identifier les adresses IP des utilisateurs indésirables.

#### **Data Center hautement sécurisé**

Les serveurs de NTRsupport résident dans des centres d'hébergement (Data Center) de dernière génération, totalement dédiés aux applications Internet critiques. Ces centres appliquent les mesures les plus strictes et les meilleures pratiques pour assurer les plus hauts niveaux de sécurité et de disponibilité. Parmi ces pratiques, la surveillance du réseau 24h/24 et 7j/7, le contrôle de l'accès au site par carte d'accès et reconnaissance biométrique, la protection incendie, la connectivité hautement redondante, le contrôle électrique et environnemental, afin d'assurer que les serveurs sont continuellement disponibles et opérationnels dans les conditions optimales.