TeamViewer

TeamViewer prend la **protection de vos données** au sérieux.

En tant qu'entreprise allemande, nous nous efforçons de répondre aux exigences élevées des normes de sécurité allemandes. Nous mettons en place différentes mesures pour assurer la sécurité de vos données, la confidentialité sur votre lieu de travail et votre protection contre les fraudes. TeamViewer offre non seulement une sécurité en arrière-plan grâce au cryptage, à la signature du code, à l'authentification à deux facteurs et bien plus, mais également d'autres fonctions utiles assurant le maintien de la sécurité au quotidien.

Sécurité TeamViewer

L'ID TeamViewer
Unique et propre à votre appareil, l'ID TeamViewer est généré et vérifié automatiquement avant chaque session.

Les normes de sécurité les plus élevées au monde Notre principal centre de données répond aux normes de sécurité industrielle ISO 27001.

Protection contre les attaques par force brute
Avec TeamViewer, le temps entre les tentatives de connexion échouées est augmenté de manière exponentielle et n'est réinitialisé qu'une fois que le mot de passe correct a été entré. Les dispositifs d'accès à distance ou les partenaires de connexion sont également protégés contre d'autres types d'attaques.

Le mot de passe TeamViewer
TeamViewer génère automatiquement un nouveau mot de passe de session dynamique après chaque redémarrage du service TeamViewer. Il existe cependant également un paramètre optionnel permettant de définir un mot de passe de façon dynamique après chaque session. Ce mot de passe est par défaut alphanumérique et se compose de six caractères, ce qui signifie que plus de 2,1 milliards de combinaisons sont possibles.

Secure Remote Protocol (SRP)
TeamViewer utilise le protocole SRP pour l'authentification et le cryptage des mots de passe. Le mot de passe n'est jamais envoyé sur Internet, même crypté, et est donc protégé de manière optimale contre tout accès extérieur. Les mots de passe font également l'objet d'un cryptage au niveau du backend.

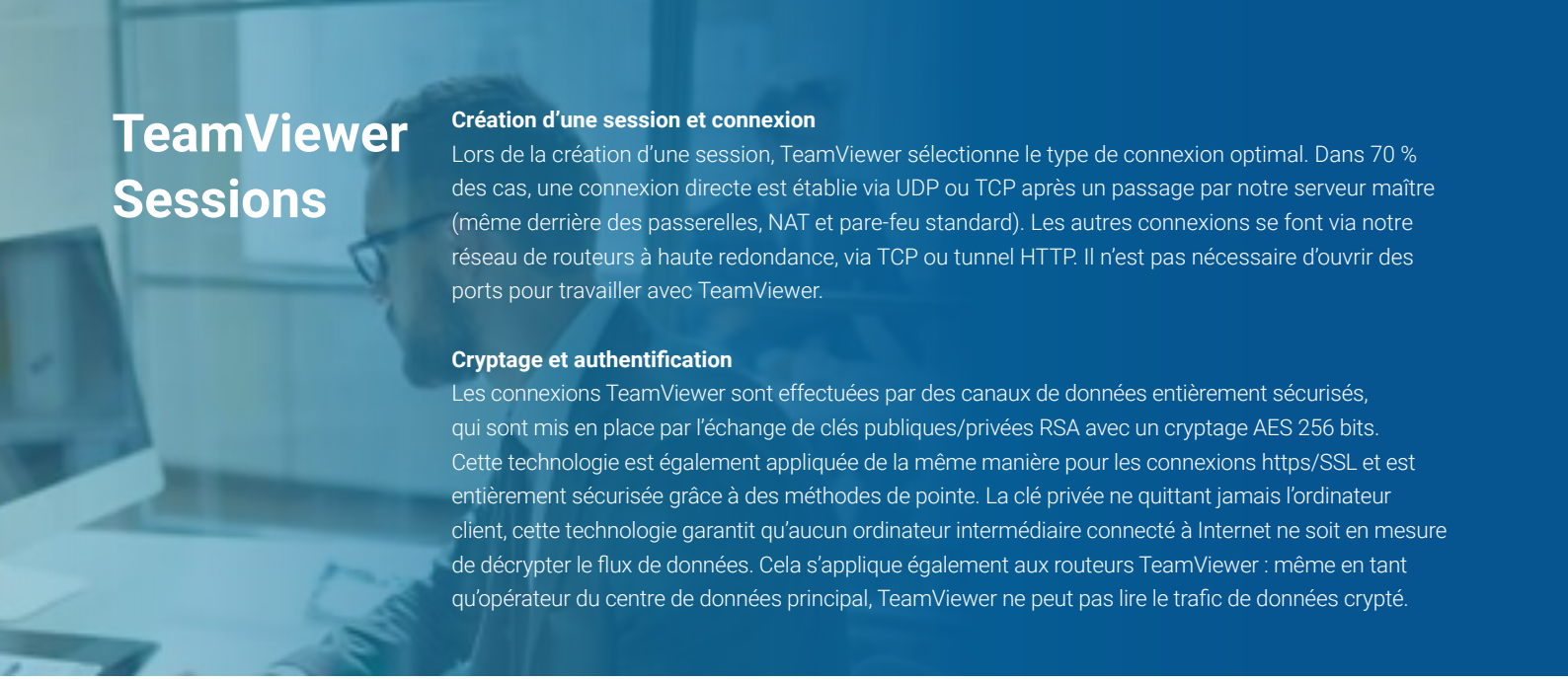
Cryptage
Toutes les interactions via TeamViewer, y compris les transferts de fichiers, le VPN, le chat, etc., sont protégées par un cryptage de bout en bout avec une clé publique/privée RSA 2 048 bits.

Accès conditionnel*
L'accès conditionnel vous permet d'appliquer les règles d'accès à distance afin de prévenir toute activité non autorisée et d'adapter les directives de sécurité.

Authentification à deux facteurs
Dans ce cas, la connexion s'effectue à l'aide d'un nouveau code unique, généré à chaque fois par un algorithme et affiché sur un appareil mobile.

**Disponible avec TeamViewer Tensor. Offre soumise à conditions.*

AICPA SOC · A-LIGN HIPAA · südcert ISO 9001 · VeriSign Trusted · ISO ISO/IEC 27001



TeamViewer Sessions

Création d'une session et connexion
Lors de la création d'une session, TeamViewer sélectionne le type de connexion optimal. Dans 70 % des cas, une connexion directe est établie via UDP ou TCP après un passage par notre serveur maître (même derrière des passerelles, NAT et pare-feu standard). Les autres connexions se font via notre réseau de routeurs à haute redondance, via TCP ou tunnel HTTP. Il n'est pas nécessaire d'ouvrir des ports pour travailler avec TeamViewer.

Cryptage et authentification
Les connexions TeamViewer sont effectuées par des canaux de données entièrement sécurisés, qui sont mis en place par l'échange de clés publiques/privées RSA avec un cryptage AES 256 bits. Cette technologie est également appliquée de la même manière pour les connexions https/SSL et est entièrement sécurisée grâce à des méthodes de pointe. La clé privée ne quittant jamais l'ordinateur client, cette technologie garantit qu'aucun ordinateur intermédiaire connecté à Internet ne soit en mesure de décrypter le flux de données. Cela s'applique également aux routeurs TeamViewer : même en tant qu'opérateur du centre de données principal, TeamViewer ne peut pas lire le trafic de données crypté.

Conformité et protection des données

Appareils de confiance
Trusted Devices garantit que l'authentification est demandée la première fois qu'un nouveau dispositif tente de se connecter à un compte TeamViewer existant.

Intégrité des données
L'intégrité des données offre une protection contre les cybercriminels : le système vérifie en permanence tout comportement inhabituel sur un compte d'utilisateur et génère une réinitialisation automatique du mot de passe si un comportement suspect est effectivement détecté.

Liste blanche/liste noire
Cette fonction offre une protection spéciale si TeamViewer est installé sur des ordinateurs sur lesquels des opérations de maintenance sont effectuées sans surveillance. La liste blanche est utilisée pour définir les clients autorisés à y accéder, la liste noire pour bloquer certains ID et comptes TeamViewer.

Signature du code
Tous les programmes TeamViewer sont signés numériquement par VeriSign, ce qui permet d'identifier à tout moment l'éditeur à l'aide d'un ID unique.

ISO/IEC 27001
Notre centre de données principal est certifié selon la norme ISO/IEC 27001, qui est la norme internationale pour la gestion et les contrôles de sécurité.

ISO 9001:2015
TeamViewer est également certifié conforme à la norme ISO 9001:2015 pour le système de gestion de la qualité (QMS).

Règlement général de l'Union européenne sur la protection des données (RGPD)
Le 25 mai 2018, le Règlement général de l'Union européenne sur la protection des données (RGPD) est entré en vigueur, ce qui souligne l'importance de la protection des données dans un monde toujours plus numérique. TeamViewer est une entreprise internationale, et nous accordons de l'importance à ce que les informations personnelles de nos clients et de notre personnel soient traitées conformément au RGPD. Pour en savoir plus sur l'engagement envers la confidentialité des données et la préparation au RGPD de TeamViewer, consultez notre base de connaissances.

Certification HIPAA, HITECH et SOC2
TeamViewer a reçu les certifications HIPAA, HITECH et SOC2 de A-LIGN, un fournisseur de sécurité et de conformité opérant sur l'ensemble du territoire américain. Les certifications HIPAA et HITECH sont essentielles pour les organisations de soins de santé afin de garantir la confidentialité et la sécurité des données sensibles et des informations de santé protégées.

La SOC2 représente quant à elle une structure de rapports essentielle permettant aux organisations de fournisseurs services de réaliser des rapports sur les contrôles internes non financiers, qui permettent à leur tour à leurs clients de mieux comprendre la mise en œuvre des cinq principes de services de confiance TSP (Trusted Service Principles).

TeamViewer

US TeamViewer
5741 Rio Vista Dr
Clearwater, FL 33760
États-Unis
Téléphone : (877) 258-3157

Restez connecté