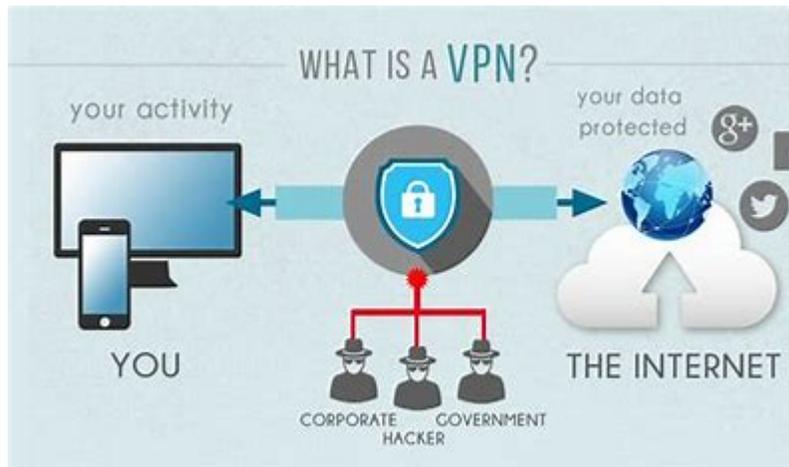


# Comment utiliser un VPN et 4 étapes faciles pour commencer

**Apprenez à configurer et à utiliser un VPN en seulement quatre étapes faciles.**

**Ce guide étape par étape vous explique comment sécuriser votre connexion et vos données en ligne.**

Luis Millares :



L'utilisation d'un VPN ou d'un réseau privé virtuel peut sembler compliquée au premier abord, mais c'est un logiciel étonnamment facile à configurer et à utiliser.

Que vous fassiez partie d'une petite entreprise ou d'une grande organisation, l'intégration d'un VPN est un excellent moyen de sécuriser les informations importantes de l'entreprise.

Dans cet article, nous allons vous expliquer comment configurer un VPN, comment l'utiliser et comment vous pouvez optimiser les fonctionnalités pour votre organisation.

Aller à :

1. [Choisissez un VPN](#)
2. [Acheter un VPN](#)
3. [Configurer le VPN](#)
4. [Utiliser le VPN](#)

## 1. Choisissez un VPN

Bien que tous les VPN cryptent la connexion entre un appareil et un réseau, chaque service apporte sa propre saveur et ses caractéristiques spéciales.

Par exemple, ExpressVPN offre une interface claire et facile à comprendre, tandis que CyberGhost VPN donne la priorité à un vaste réseau de serveurs répartis sur 100 emplacements.

Il est important de savoir pourquoi vous avez besoin d'un VPN.

Voulez-vous plus de sécurité et de confidentialité ?

En avez-vous besoin pour débloquer du contenu ?

Combien d'appareils avez-vous besoin de protéger via le VPN ?

Les réponses à ces questions vous indiqueront quel VPN répondra le mieux à vos besoins.

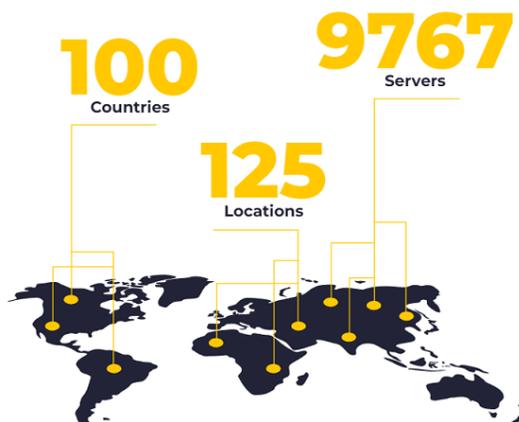
★ Trustpilot  4.3 out of 5

## Discover the Best VPN Servers

Choose from a global fleet of fast servers in 100 countries & browse anonymously

Get CyberGhost VPN

Find Recommended Server



CyberGhost se concentre sur les serveurs.

Crédit photo : VPN CyberGhost

La recherche de la réputation et des antécédents d'un VPN en matière de protection des données des utilisateurs doit faire partie du processus de prise de décision.

On s'attend à ce que les VPN protègent les données contre les acteurs malveillants, et non qu'ils les vendent ou les enregistrent pour leur propre bénéfice.

Un bon indicateur de cela est si un VPN a une politique claire de non-enregistrement des données des utilisateurs qui est soutenue de manière indépendante par un tiers.

Si vous avez besoin d'une longueur d'avance sur le choix d'un VPN, vous pouvez consulter notre sélection des [4 meilleurs VPN pour les petites entreprises](#).

Pour les besoins de ce guide, prenons [l'exemple d'ExpressVPN](#).



ExpressVPN

What is a VPN? What We Offer Download VPN Support Blog My Account English [Get Started](#)

# The VPN that just works

Go further with the #1 trusted leader in VPN

[Get ExpressVPN →](#)

30-DAY MONEY-BACK GUARANTEE

Site officiel d'ExpressVPN. Crédit photo : ExpressVPN

ExpressVPN est l'un des meilleurs fournisseurs de VPN disponibles et est réputé pour sa fiabilité et sa facilité d'utilisation.

## 2. Achetez un VPN

Après avoir choisi un VPN, il est temps de s'inscrire et de payer un abonnement.

La plupart des VPN proposent plusieurs options d'abonnement mensuel, annuel ou de deux ans.

Plus la durée est longue, plus le prix mensuel que vous payez est bas.

D'une manière générale, je recommande d'opter pour un abonnement annuel, car il vous offre un bon équilibre entre des tarifs plus bas et une durée raisonnable pour le contrat.

J'encourage également à tirer le meilleur parti des garanties de remboursement des fournisseurs de VPN. De nombreux fournisseurs accordent 30 jours ou plus après l'inscription initiale aux clients pour tester le logiciel et demander un remboursement dans le délai imparti si le VPN n'est pas adapté.

Your digital life protected from \$0.22 a day

**STEP 1** Select a plan that works for you:

Plan	Price	Guarantee
1 Month	\$12.95 per month	30-day money-back guarantee.
12 Months + 3 MONTHS FREE	Save 49% <del>\$12.95</del> \$6.67 per month	30-day money-back guarantee.
6 Months	\$9.99 per month	30-day money-back guarantee.

30-day money-back guarantee

Prix ExpressVPN.

Crédit photo : ExpressVPN

Dans le cas d'ExpressVPN, vous pouvez choisir entre un forfait de 12 mois pour 6,67 \$, un forfait de six mois pour 9,99 \$ et un forfait d'un mois pour 12,95 \$ par mois.

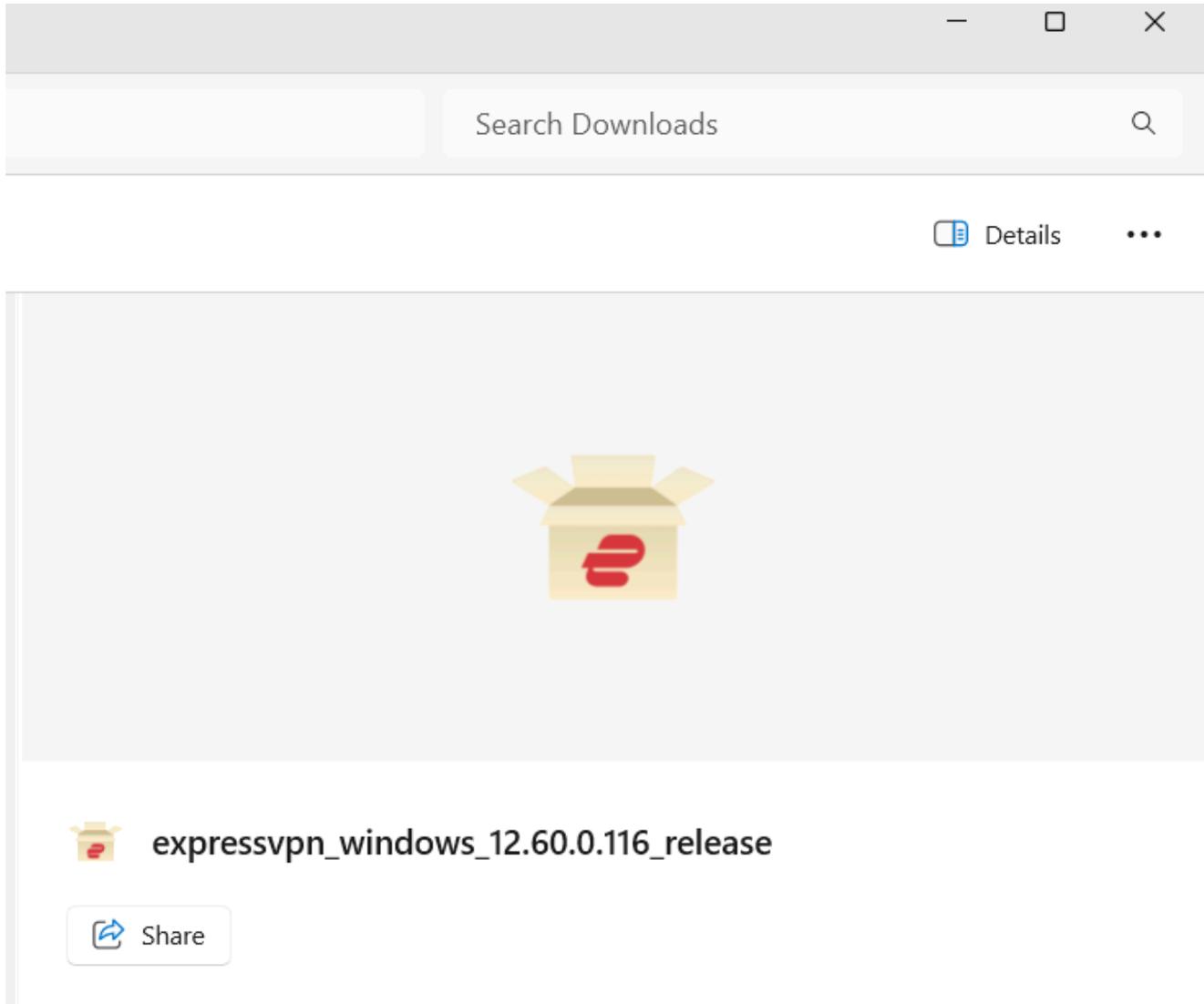
Il existe des options VPN gratuites, mais celles-ci se font généralement au prix d'une sécurité inférieure, de vitesses plus lentes et d'un manque d'autres fonctionnalités.

## 3. Configurer le VPN

Une fois que vous avez payé pour le VPN, l'étape suivante consiste à télécharger et à installer l'application VPN.

Si vous téléchargez le VPN pour votre Windows ou Mac, assurez-vous de l'obtenir sur le site officiel du VPN.

Après avoir cliqué sur télécharger, le fichier d'installation du VPN apparaîtra dans votre dossier de téléchargements.



Programme d'installation d'ExpressVPN.

Crédit photo : ExpressVPN

En cliquant sur le fichier d'installation, vous accédez au processus de configuration du VPN. Suivez simplement les instructions présentées jusqu'à ce que le VPN soit installé sur votre système.

## 4. Utilisez le VPN

Heureusement, les VPN modernes sont relativement faciles à utiliser.

Une fois installés, les VPN disposent généralement d'un bouton de connexion/déconnexion en un clic et d'une liste de serveurs auxquels vous pouvez vous connecter.

Par défaut, les VPN se connectent au serveur le plus rapide de votre région.

Cela signifie généralement que vous devez vous connecter à un emplacement de serveur le plus proche de l'endroit où vous vous trouvez.

Vous pouvez, bien sûr, choisir un emplacement de serveur spécifique en fonction de vos besoins et de vos préférences.

Avec ExpressVPN, il y a un gros bouton d'alimentation au milieu qui contrôle votre connexion, et le menu du serveur est commodément placé en dessous.

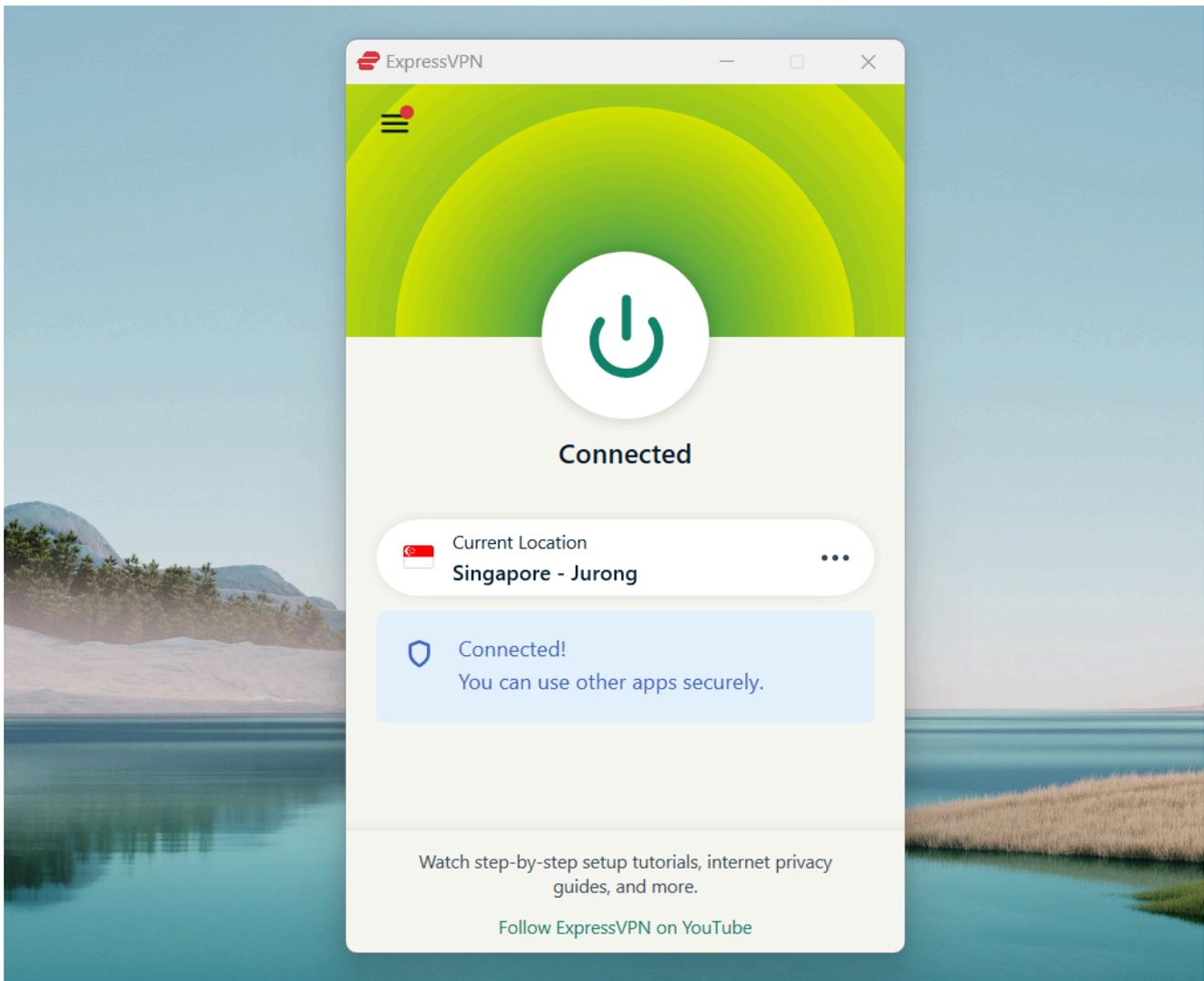


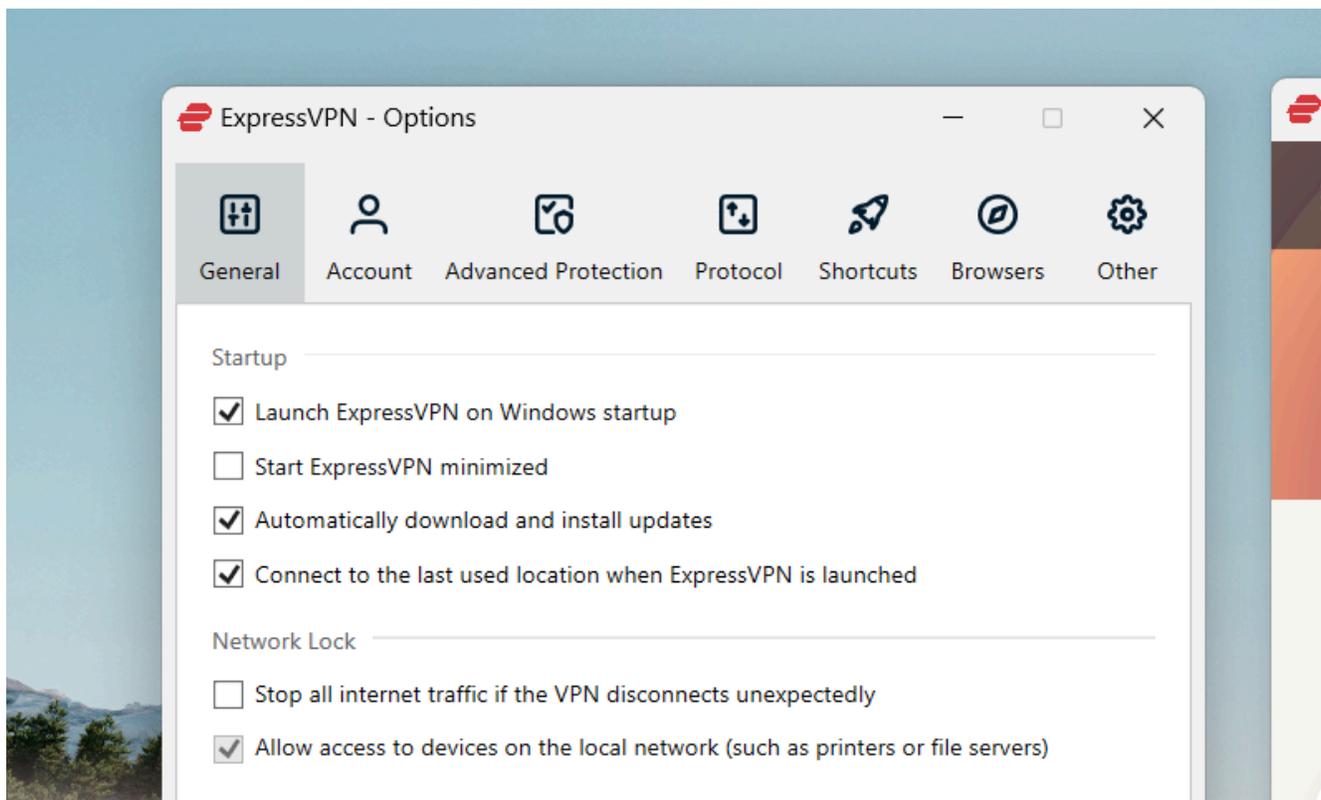
Tableau de bord ExpressVPN.

Crédit photo : ExpressVPN

Une fois que vous avez choisi un serveur, vous pouvez cliquer sur se connecter, et voilà, vous utilisez maintenant une connexion VPN sécurisée.

Certaines personnes se demandent peut-être si vous devez vous connecter manuellement à un serveur à chaque fois et la réponse est non.

En règle générale, la plupart des VPN peuvent être configurés pour se lancer au démarrage et se connecter au serveur préféré de votre choix.



ExpressVPN au démarrage de Windows.

Crédit photo : ExpressVPN

Il est important de noter que la fermeture d'une fenêtre de bureau VPN ne ferme généralement pas complètement le programme.

Les VPN sont des logiciels qui s'exécutent en arrière-plan, vous devrez donc fermer l'application VPN soit via le gestionnaire de tâches de Windows, soit en quittant manuellement l'application sur un Mac.

Si vous constatez que le VPN ne fonctionne pas comme il est censé le faire, une bonne règle de base est de vous déconnecter du serveur et de redémarrer l'application.

Si cela ne fonctionne pas, les VPN fournissent un support client soit sur leur site, soit dans l'application elle-même.

Les fournisseurs de VPN de qualité offrent une assistance par chat en direct 24h/24 et 7j/7 pour vous aider en cas de problème.

Si ce n'est pas le cas, vous pouvez envoyer un e-mail en utilisant la page d'assistance ou le système de tickets du VPN.

## Les meilleures façons d'utiliser un VPN pour votre entreprise

Les VPN ont une variété de cas d'utilisation. Ils peuvent être utilisés pour accéder à des services de streaming, pour télécharger des fichiers torrent en toute sécurité ou pour avoir une meilleure expérience de jeu.

Ils peuvent également être utilisés pour améliorer les opérations quotidiennes d'une entreprise. Voici quelques façons de le faire :

### Protéger les ressources de l'entreprise et des clients

Étant donné que les VPN cryptent la connexion entre le réseau et un appareil connecté, toutes les données transmises entre eux sont protégées.

Cela signifie que les ressources de l'entreprise et des clients seront protégées contre les mauvais acteurs.

Les VPN sont un excellent moyen de protéger les documents confidentiels, les communications internes et d'autres actifs contre les cyberattaques et le piratage.

Pour en savoir plus sur le fonctionnement des VPN, vous pouvez consulter notre guide [ici](#).

## Sécurisez l'accès aux télétravailleurs

Un autre avantage des VPN est la sécurisation de l'accès des travailleurs à distance à un réseau d'entreprise.

Étant donné que les travailleurs à distance travaillent généralement à domicile, ils ont tendance à se connecter aux ressources de l'entreprise via une connexion non protégée.

Le cryptage VPN garantit que les données sensibles auxquelles les travailleurs à distance accèdent sont illisibles et intraquables, même si elles tombent entre de mauvaises mains.

## Gagnez en flexibilité géographique

Les VPN vous donnent la possibilité de sélectionner une autre adresse IP et un autre emplacement que le vôtre.

Cela vous permet d'accéder facilement à du contenu géo-bloqué dans le monde entier.

Cela peut être utile pour les employés qui voyagent régulièrement et qui ont besoin de consulter du contenu verrouillé par région, comme des articles d'actualité, des services de streaming et des sites Web locaux.

Cette flexibilité profite également aux employés à distance qui peuvent avoir du mal à accéder à des ressources en dehors de leur lieu de travail.

## Comment vous assurer que vous optimisez votre VPN

L'intégration d'un VPN est un grand pas vers l'augmentation de la sécurité, mais il y a quelques choses que vous pouvez faire pour tirer le meilleur parti du service.

- **La vérification des applications VPN disponibles pour votre téléphone** permet aux employés de sécuriser les informations liées au travail sur leurs téléphones personnels.  
Alors que de plus en plus d'organisations s'appuient sur des appareils mobiles pour communiquer et effectuer d'autres tâches, l'installation de l'application iOS ou Android d'un service VPN garantit que la sécurité renforcée est maintenue sur tous les appareils.
- **L'utilisation d'extensions de navigateur VPN** vous permet d'utiliser un VPN directement depuis le navigateur.  
Certaines extensions VPN peuvent même être autonomes sans l'application de bureau installée, ce qui facilite le travail sécurisé sur un autre ordinateur.
- **Se renseigner sur les abonnements d'équipe** est un excellent moyen de réduire les coûts si vous êtes une entreprise à la recherche d'un VPN.

En plus du VPN lui-même, les abonnements d'équipe incluent normalement des tarifs plus bas, une facturation centralisée et une console d'administration pour les gestionnaires.

## VPN recommandés et faciles à utiliser

Le cryptage VPN peut devenir technique, mais trois services qui se distinguent par leur facilité d'utilisation sont ExpressVPN, CyberGhost VPN et TunnelBear VPN.

ExpressVPN est doté d'une interface utilisateur moderne et facile à comprendre.

Son extension de navigateur agit également comme une télécommande pratique pour l'application de bureau, vous permettant d'accéder facilement à Express directement depuis le navigateur.

Vous pouvez lire notre avis complet sur ExpressVPN [ici](#).

CyberGhost VPN organise intelligemment ses serveurs en serveurs pour le streaming, le torrenting et les jeux. Étant donné qu'il propose plus de 9 370+ serveurs dans 100 pays, les catégories aident à distinguer quel serveur convient le mieux aux différents utilisateurs.

Vous pouvez consulter notre avis complet sur CyberGhost VPN [ici](#).

TunnelBear présente l'interface utilisateur la plus conviviale pour les débutants et la moins intimidante avec son application de bureau sur le thème des ours.

Chaque serveur est représenté par un tunnel, et lorsque vous passez à un nouveau serveur, l'ours TunnelBear apparaît une fois la connexion établie.

Vous pouvez consulter notre critique complète de TunnelBear [ici](#).

*Recherche et mise en page par:*

*Michel Cloutier*

*CIVBDL*

*20240229*

*"C'est ensemble qu'on avance"*