CISCO
SECURE

Cinq recommandations pour assurer la sécurité de votre environnement de travail hybride

Alors que le monde évolue vers un environnement de travail hybride plus permanent, la flexibilité apporte à la fois de nouveaux avantages et de nouveaux défis pour les employeurs et les travailleurs. Que votre équipe travaille au bureau, à distance ou entre les deux, vous n'avez pas besoin de compromettre votre sécurité pour plus de flexibilité. Voici cinq recommandations pour maintenir votre culture d'environnement de travail tout en assurant la sécurité de votre personnel et des ressources de votre entreprise.

1 Apprenez à votre personnel à adopter des pratiques de travail sécurisées

Les travailleurs s'attendent à ce que la technologie les suive partout où ils vont, mais les lieux de travail flexibles les exposent (et exposent votre entreprise) à de nouvelles menaces. Voilà pourquoi les équipes des TI et de la sécurité doivent s'assurer que l'expérience hybride est sécurisée à chaque point terminal en éduquant les utilisateurs sur les pratiques sécuritaires et les dangers potentiels.

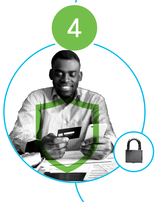
2 Vérifiez que l'utilisateur est bien la personne qu'elle prétend être

L'authentification multifacteur (AMF) est une première couche de sécurité simple dont toutes les entreprises ont besoin pour accorder l'accès aux ressources de l'entreprise. L'AMF se base sur quelque chose que vous connaissez (votre nom d'utilisateur et mot de passe) et quelque chose que vous possédez (votre téléphone) pour vérifier votre identité et l'état de votre appareil.

3 Activez un accès sécurisé de n'importe où

Le VPN fournit un tunnel sécurisé entre les utilisateurs et les applications afin que les employés puissent rester productifs et connectés lorsqu'ils sont sur la route ou à la maison. Il permet de s'assurer que seuls les utilisateurs autorisés se connectent en offrant un niveau de sécurité adéquat sans compromettre l'expérience utilisateur.

4 Protégez-vous contre les menaces à la sécurité à n'importe quel point d'entrée



La plupart des violations de sécurité ciblent les utilisateurs des points d'extrémité, nécessitant une première ligne de défense au niveau de la couche DNS et une dernière ligne pour les menaces qui parviennent à s'infiltrer. La première couche bloque les domaines associés à un comportement malveillant avant qu'ils accèdent à votre réseau ou circonscrivent les programmes malveillants s'ils sont déjà à l'intérieur, tandis que la dernière couche protège contre les menaces plus avancées.

5 Unifiez votre sécurité grâce à une plateforme simple et intégrée

N'appliquez pas de solutions disparates à votre sécurité avec des produits ponctuels et des expériences utilisateur inégales. Facilitez la sécurité et renforcez son efficacité grâce à SecureX, une plateforme intégrée et transparente qui relie vos produits Cisco Secure à votre infrastructure.

Protégez vos données, quel que soit le lieu de travail de vos employés, grâce à la solution simple et unifiée Cisco Secure Hybrid Work, vous pouvez opter pour une sécurité intégrale et favoriser le travail de vos effectifs, où qu'ils soient.

Pour en savoir plus, consultez la page cisco.com/go/securehybridwork.

cisco The bridge to possible