SONICWALL

NOTE DE SYNTHÈSE : POURQUOI UN ACCÈS MOBILE SÉCURISÉ EST UN IMPÉRATIF STRATÉGIQUE D'ENTREPRISE

L'accès mobile permet à votre entreprise de rester productive dans un monde dynamique et perturbé

Résumé

À l'échelle mondiale, la main-d'œuvre mobile est appelée à se maintenir, et à se développer. Les avantages en termes de flexibilité, de continuité et de productivité font de l'accès mobile sécurisé un impératif stratégique pour l'entreprise d'aujourd'hui. Cependant, pour soutenir efficacement ce personnel, le service informatique est confronté à plusieurs défis, notamment une explosion des terminaux, des menaces plus intelligentes et la nécessité d'accéder aux ressources internes et SaaS, tout en fonctionnant avec un budget allégé.

Introduction

Au quotidien, les gros titres présentent des défis en termes de perturbation qui nécessitent des solutions technologiques dynamiques. Les urgences liées à la santé publique, les catastrophes naturelles comme les tremblements de terre, les tsunamis, les ouragans et les blizzards, et les crises politiques peuvent tous empêcher les déplacements ou l'accès physique à un site pour les employés essentiels. Pour garantir la continuité des affaires, les entreprises doivent être suffisamment flexibles pour mener leurs activités de n'importe où et à n'importe quel moment.

En même temps, de nombreuses entreprises cherchent à tirer profit de l'augmentation de la productivité et de la rétention du personnel, ainsi que de la réduction des frais généraux d'exploitation liés à l'entretien des installations de bureaux physiques, en permettant au personnel de travailler de n'importe où et à n'importe quel moment.

Selon une enquête mondiale 2019 IWG menée auprès de plus de 15 000 professionnels de différents secteurs d'activité dans 80 pays :

- 85 % ont confirmé une hausse de la productivité grâce à une plus grande flexibilité
- 65 % ont déclaré que le travail flexible a permis de réduire les dépenses d'investissement/d'exploitation et de gérer le risque
- 75 % considèrent maintenant le travail flexible comme la nouvelle norme
- 62 % des entreprises du monde entier disposent aujourd'hui de politiques pour le travail flexible

- Plus de la moitié des salariés dans le monde travaillent à distance plus de 2,5 jours par semaine
- Plus de 80 % des travailleurs choisiraient un emploi flexible plutôt qu'un emploi non flexible
- L'économie américaine à elle seule pourrait bénéficier d'un coup de pouce de 4 500 milliards de dollars grâce au travail flexible

En conséquence, les entreprises se sont de plus en plus appuyées sur l'accès mobile aux ressources depuis des appareils autorisés et BYOD en dehors de leurs périmètres de réseau traditionnels.

Une cybersécurité efficace doit inclure un accès mobile sécurisé

Proposer un accès mobile n'importe où et n'importe quand dans le monde hyper-distribué d'aujourd'hui ouvre une multitude de points d'exposition sur une myriade de terminaux mobiles potentiellement non sécurisés.

La faillibilité humaine et les comportements en ligne risqués font qu'on ne peut pas faire confiance aux employés quand il s'agit d'assurer la sécurité de leurs propres appareils mobiles.

En outre, l'éventail des types de menaces s'élargit, s'approfondit et devient plus intelligent, avec notamment les ransomware ciblés, les menaces inédites, les logiciels malveillants basés sur la mémoire, les attaques par canal auxiliaire et les menaces chiffrées.

Au final, la sécurité de votre réseau mobile doit correspondre à celle de votre réseau filaire. Cela nécessite une position de confiance zéro vis-à-vis de tout appareil mobile qui tente de se connecter aux ressources de l'entreprise, que ces ressources soient sur site ou dans le cloud. Un accès mobile sécurisé est un élément essentiel d'une approche de confiance zéro pour un accès à tout moment et de n'importe où.

Le service informatique doit également sécuriser l'accès à partir de ces terminaux mobiles avec un budget et un personnel qualifié limités. Cela signifie qu'il faut simplifier le déploiement, la disponibilité et la prise en charge afin de réduire le coût total de possession. Pour être efficace, la cybersécurité doit fournir aux employés mobiles un accès facile et sécurisé 24 h/24 et 7 j/7 aux ressources stratégiques de l'entreprise d'une manière souple, facile à utiliser, rentable et évolutive.

Conclusion

Qu'il s'agisse d'assurer la continuité de l'activité ou d'améliorer la rétention et la productivité de la main-d'œuvre, un accès mobile sécurisé est un impératif stratégique d'entreprise. La solution d'accès mobile sécurisé (SMA) de SonicWall fournit un accès à tout moment et de n'importe où dans les entreprises hyper-distribuées. Cela donne à votre entreprise la flexibilité nécessaire pour rester opérationnelle, quels que soient les gros titres de demain.

Pour en savoir plus, rendez-vous sur www.sonicwall.com/products/remote-access.

© 2020 SonicWall, Inc. TOUS DROITS RÉSERVÉS.

SonicWall est une marque commerciale ou déposée de SonicWall Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales et déposées sont la propriété de leurs sociétés respectives.

Les informations figurant dans le présent document concernent les produits proposés par SonicWall Inc. et/ou ses sociétés affiliées. Ce document n'implique la concession d'aucune licence, expresse ou tacite, par forclusion ou autre, concernant les droits de propriété intellectuelle, ou en lien avec la vente de produits SonicWall. À L'EXCEPTION DE CE QUI EST PRÉVU DANS LES CONDITIONS GÉNÉRALES VISÉES DANS L'ACCORD DE LICENCE DE CE PRODUIT, SONICWALL ET/OU SES SOCIÉTÉS AFFILIÉES N'ASSUMENT AUCUNE RESPONSABILITÉ QUELLE QU'ELLE SOIT, ET RÉFUTENT TOUTE GARANTIE EXPRESSE, TACITE OU PRÉVUE PAR LA LOI EN LIEN AVEC LEURS PRODUITS, Y COMPRIS MAIS SANS S'Y LIMITER, TOUTE GARANTIE TACITE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER OU D'ABSENCE DE CONTREFAÇON. EN AUCUN CAS LA SOCIÉTÉ SONICWALL ET/OU SES SOCIÉTÉS AFFILIÉES NE SAURAIENT ÊTRE TENUES RESPONSABLES DE TOUT DOMMAGE DIRECT, INDIRECT, ACCESSOIRE, PUNITIF, SPÉCIAL OU CONNEXE (Y COMPRIS MAIS SANS S'Y LIMITER, TOUS DOMMAGES POUR PERTE DE PROFITS, INTERRUPTION D'ACTIVITÉ OU PERTE D'INFORMATIONS) DÉCOULANT DE L'UTILISATION OU DE L'IMPOSSIBILITÉ D'UTILISER LE PRÉSENT DOCUMENT, ET CE MÊME SI LA SOCIÉTÉ SONICWALL ET/OU SES SOCIÉTÉS AFFILIÉES ONT ÉTÉ INFORMÉES DE LA POSSIBILITÉ DE TELS DOMMAGES. SonicWall et/ou ses sociétés affiliées ne font aucune déclaration et n'offrent aucune garantie quant à l'exactitude ou l'exhaustivité des informations contenues dans le présent document, et se réservent le droit d'apporter des modifications aux spécifications et aux descriptions des produits à tout moment et sans préavis. SonicWall Inc. et/ou ses sociétés affiliées ne prennent aucun engagement quant à la mise à jour des renseignements contenus dans le présent document.

À propos de SonicWall

Depuis plus de 27 ans, SonicWall lutte contre la cybercriminalité pour défendre les PME, les grandes entreprises et les agences gouvernementales du monde entier. S'appuyant sur les travaux de recherche des Capture Labs de SonicWall, nos solutions primées de détection et de prévention des intrusions en temps réel sécurisent plus d'un million de réseaux et leurs e-mails, applications et données dans plus de 215 pays et territoires. Ces entreprises peuvent ainsi fonctionner plus efficacement sans crainte pour leur sécurité. Pour en savoir plus, rendez-vous sur www.sonicwall.com ou suivez-nous sur Twitter, LinkedIn, Facebook et Instagram.

Si vous avez la moindre question concernant votre utilisation potentielle du présent contenu, merci de contacter :

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035 - États-Unis

Consultez notre site Internet pour plus d'informations.
www.sonicwall.com