Six points déterminants pour sécuriser le travail hybride

La nouvelle norme veut que les entreprises évaluent les façons de préserver leurs processus opérationnels tout en reconnaissant que le travail hybride semble s'inscrire dans la durée. Le travail hybride est sécurisé lorsque la sécurité et la connectivité sont rapides, faciles à utiliser et en mesure de protéger les transactions où que se trouvent les personnes et les données, tout en garantissant à l'employé la même expérience d'utilisateur productif que lorsqu'il utilise la technologie dans un bureau classique.

Voici six points déterminants pour vous assurer que vous sécurisez correctement le travail hybride de votre personnel.

S'assurer que la sécurité applique les principes du zero trust

Les pirates suivent les entreprises dans le cloud, car c'est là que sont stockées la plupart des données. Et comme la main-d'œuvre hybride peut accéder à ces données à partir d'un certain nombre d'appareils et de réseaux, la notion de « confiance implicite » n'est plus viable. Le zero trust consiste à passer d'une approche « faire confiance puis vérifier », à une approche « vérifier, puis faire confiance » bâtie sur les concepts d'accès de moindre privilège en fonction du contexte et d'évaluation continue.

Pour approfondir un peu plus la question du zero trust, consultez le site

Concevoir la sécurité de manière à maximiser la visibilité et le contrôle de votre environnement orienté cloud

La protection de vos données, systèmes et périphériques dans un environnement de travail hybride nécessite une visibilité et un contrôle des applications cloud et SaaS. (Selon Statista, l'entreprise moyenne utilise plus de 110 applications SaaS, dont la grande majorité n'est pas managée : c'est ce que l'on appelle de l'informatique « fantôme » ou « Shadow IT ») La possibilité de visualiser, guider et contrôler l'activité de chacun dans l'entreprise améliore considérablement la sensibilisation et la détection des risques.

Lisez l'article de notre blog

Ne pas perdre de vue l'expérience utilisateur

La solution de sécurité idéale doit tenir compte de chacun des points précédents, mais elle doit le faire de manière à avoir un impact minimal sur l'expérience utilisateur en mode hybride. Évitez les solutions de sécurité qui imposent des pénalités de latence élevées ou obligent le trafic à emprunter des détours contraignants. En outre, les contrôles de sécurité ne doivent pas accaparer les ressources du système ou nécessiter un certain nombre de clics supplémentaires.

Lire la suite : La sécurité ne ralentit pas nécessairement les performances du réseau (en anglais)

Concevoir pour tous les cas d'usage liés à la protection des données : web, cloud, email, applis privées et devices

Le travail hybride a fait disparaître la notion de périmètre de sécurité et a étendu l'entreprise au-delà du site. Votre sécurité doit prendre en compte le trafic provenant du Web, du cloud, des applications privées et des devices. Les technologies CASB, SWG, ZTNA et tous les autres aspects d'une architecture SSE (Security Service Edge) traitent les données qui se déplacent et sont stockées sur tous ces vecteurs.

Lisez le livre blanc sur la protection des données dans le cloud :

Concevoir la sécurité en fonction du contexte

Le travail hybride complique considérablement les différentes façons dont les utilisateurs peuvent interagir avec les applications et les données. Par conséquent, la sécurité doit disposer d'une meilleure conscience contextuelle pour prendre des décisions relatives aux accès et aux politiques. La sécurité doit surveiller en permanence le trafic après l'octroi de l'accès, effectuer une analyse contextuelle des sessions, prendre des décisions fondées sur des informations concernant les risques provenant de tiers, détecter les changements dans les profils de risque et neutraliser les actions dangereuses.

En savoir plus sur la plateforme Cloud XD de Netskope

Consolider les fournisseurs pour améliorer l'efficacité de votre sécurité et réduire les coûts

L'entreprise moyenne emploie 76 outils de sécurité. Le SSE ne les remplacera pas tous, mais vous pourrez dire adieu à la complexité et au casse-tête qu'implique un environnement de sécurité disparate avec des dizaines de fournisseurs. Une suite complète unifiée, provenant d'un seul fournisseur, remplace les anciennes solutions de sécurité mal coordonnées. Les fonctionnalités ainsi fusionnées simplifient la gestion et l'administration, garantissent une application cohérente des politiques, rationalisent le traitement du trafic et améliorent le coût total de possession.

Découvrez ce que Netskope Intelligent SSE peut faire pour vous !

netskope

Netskope, leader mondial de la cybersécurité, réinvente la sécurité du cloud, des données et du réseau, permettant aux organisations d'appliquer les principes du zero trust afin de protéger leurs données. La plateforme Netskope Intelligent Security Service Edge (SSE) est rapide, facile à utiliser et sécurise les personnes, les appareils et les données partout. Pour savoir comment Netskope aide ses clients à être prêts à toute épreuve dans leur passage au SASE, visitez netskope.com.