BONNE PRATIQUE :

ZTNA

Accès réseau zero-trust

Il est toujours bon de garder à l'esprit
ces bonnes pratiques ZTNA :

- → Accorder les accès en appliquant le principe du moindre privilège.
- → Utiliser la MFA et des IdP cloud pour vérifier les identités.
- → Définir des exigences de conformité pour gérer et sécuriser les utilisateurs, les appareils et plus.
- → Ne jamais faire confiance, toujours vérifier, et ce en continu même après l'accès initial.

Vous débutez avec la gestion moderne des identités et des accès ?
Lisez la suite pour savoir comment mettre en place votre stratégie.

jamf

Vous entrez dans votre banque pour effectuer un retrait. Votre identité est vérifiée à l'aide de votre numéro de compte et de votre pièce d'identité. Si votre nom figure sur le compte, vous avez accès à ce compte, et à ce compte seulement. Maintenant, imaginez : vous présentez votre pièce d'identité et le guichetier vous conduit directement au coffre-fort, et son contenu est à votre disposition. Ça paraît fou, non ? Alors pourquoi gérer l'accès à votre réseau de la même façon ?

Un VPN (réseau privé virtuel) permet aux utilisateurs d'accéder à l'ensemble de votre réseau, qu'ils aient ou non besoin d'un accès complet. Et cela met vos données en danger. **L'accès réseau Zero-Trust (ZTNA) verrouille le coffre-fort des informations de votre entreprise en accordant uniquement l'accès aux ressources dont les employés ont besoin, tout en vérifiant strictement l'identité de l'utilisateur et de l'appareil pour chaque application.** Il réduit également la demande en bande passante sur votre réseau, et préserve la confidentialité des utilisateurs grâce au tunnelage partagé. Soyons clairs : le VPN doit disparaître.

Comment fonctionne ZTNA ? À son niveau le plus simple, cette approche cherche à confirmer trois aspects :

1. **Identité :** qui êtes-vous, êtes-vous la personne que vous prétendez être et avez-vous une autorisation ?
2. **Sécurité :** votre appareil est-il sécurisé ?
3. **Contexte :** demandez-vous l'accès aux seules ressources dont vous avez besoin ?

La mise en œuvre d'une technologie ZTNA performante doit répondre à ces questions. Le ZTNA exige que l'utilisateur et son appareil prouvent leur identité. L'appareil doit être connu et autorisé. Pour ce faire, vous pouvez inscrire l'appareil dans votre solution de gestion des appareils en l'associant à un utilisateur spécifique L'utilisateur doit également fournir des identifiants et des réponses correctes à l'authentification multifacteur de son fournisseur d'identité cloud.

Malgré la confirmation de l'identité, il faut également vérifier que l'appareil est sûr pour réduire les risques d'accès non autorisé aux ressources de l'entreprise. L'appareil doit donc être conforme à vos règles de sécurité et disposer d'un système d'exploitation à jour, doté de tous les correctifs de sécurité.

Une fois l'identité et la sécurité vérifiées, les utilisateurs ont accès aux applications dont ils ont besoin. Dans l'architecture ZTNA, les utilisateurs ne peuvent voir que ce à quoi ils ont le droit d'accéder. Pour ce faire, seules des applications préalablement approuvées sont fournies à chaque utilisateur. De cette façon, lorsqu'un utilisateur tente d'accéder à ses applications, il est normalement déjà autorisé à le faire.

Jamf fait tout cela pour vous : gestion des appareils, approvisionnement des applications, intégrations avec les fournisseurs d'identité cloud, mises à jour des logiciels, protection des terminaux et plus encore. Découvrez nos solutions ZTNA transparentes dans notre e-book Introduction à l'accès réseau zero-trust.

Vous voulez verrouiller l'accès à vos données avec le ZTNA ? Découvrez comment mettre en place ce type de stratégie – et bien plus – avec Trusted Access de Jamf.

jamf

www.jamf.com/fr/