10 PILIERS d'un datacenter Zero Trust

Intégrer le Zero Trust à votre datacenter, c'est donner la priorité à l'expérience utilisateur.

Avec à la clé :

- *Des accès rapides, fiables et évolutifs*
- *Des utilisateurs et appareils protégés*
- *Des applications et workloads qui verrouillent les données*
- *Une agilité accrue*

10 VISIBILITÉ SUR L'INVISIBLE

On ne peut protéger que ce que l'on voit.

D'où l'importance d'une vue du réseau complète et transverse à tous les environnements, y compris dans la façon dont chaque pan est sécurisé du client jusqu'au workload.

9 SEGMENTATION MULTIPLE

Dressez des remparts internes au réseau.

Des utilisateurs et appareils aux applications et workloads, la segmentation et le contrôle granulaires contribuent à prévenir les accès non autorisés et les failles de sécurité.

8 ATTRIBUTION D'IDENTITÉ AUX UTILISATEURS, APPAREILS ET WORKLOADS

Les utilisateurs ont une identité…

les appareils et workloads aussi. L'identité se compose de multiples facteurs qui permettent de détecter les risques sur le réseau à tout moment.

7 APPLICATION DES POLITIQUES SANS CONTRAINTE DE LIEU

Protégez les utilisateurs, appareils et applications où qu'ils se trouvent.

Les utilisateurs, applications et workloads sont toujours en mouvement. Assurez-vous que les politiques de sécurité les suivent en permanence pour limiter les vecteurs d'attaque potentiels.

6 ANALYSE DES INTENTIONS DU TRAFIC RÉSEAU

Où se dirige le trafic et à quelles fins ?

Collectez autant de données que possible sur l'ensemble du trafic réseau, y compris le trafic chiffré. Pour commencer, analysez des indicateurs et des comportements spécifiques au trafic.

5 AUTOMATISATION MAXIMALE

Automatisez autant que vous le pouvez !

En plus de vous faciliter la tâche, l'automatisation renforce l'efficacité entre les équipes. Elle permet d'appliquer les changements à l'intégralité du réseau et de répondre aux menaces avant qu'elles ne se transforment en incidents.

4 SURVEILLANCE ET UTILISATION DE TOUS LES POINTS DE CONNEXION

La sécurité est désormais l'affaire de tout le réseau.

Utilisez vos routeurs et commutateurs pour détecter les menaces et renforcer la protection de tous les environnements de votre datacenter.

3 EFFICACITÉ CONTRE LES ATTAQUES DE BASE

Votre solution de sécurité ne vous protège pas des menaces connues ? C'est clairement un investissement en pure perte.

Les données ne mentent pas ! Faites vos recherches et identifiez les fournisseurs de sécurité les mieux à même de protéger votre réseau.

2 OPTIMISATION DE LA DISPONIBILITÉ DES APPLICATIONS

Pas le droit à la panne.

Pour qu'une entreprise tourne, son réseau doit rester disponible et ses ressources connectées à chaque instant. Mais la sécurité ne peut s'opérer aux dépens des performances du réseau. Optez pour une solution de sécurité fiable, garante de basculements ultra-rapides et d'un débit à la hauteur de vos exigences métiers.

1 CHAQUE PAS EST UN PROGRÈS

Poursuivez vos efforts.

Vous pensez ne pas encore tout maîtriser sur le Zero Trust ? Pas d'inquiétude. Commencez petit en vous concentrant sur un élément particulier à implémenter. Étape par étape, vous parviendrez à ériger une architecture Zero Trust complète pour votre datacenter.

À vous de jouer !

N'OUBLIEZ PAS LA PÉRIPHÉRIE !

Chaque initiative de sécurité a pour but de protéger les données. Une bonne protection du datacenter commence donc à la périphérie, là où les accès aux données sont contrôlés. Protéger les accès des utilisateurs et des appareils aux applications et aux données qui résident dans votre datacenter, c'est mieux protéger l'ensemble de votre réseau.

JUNIPER NETWORKS

3050187-001-FR Août 2023