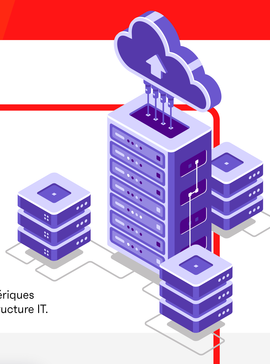
ivanti

VOTRE STRATÉGIE DE CYBERSÉCURITÉ

Avec le passage rapide au télétravail, de nombreuses vulnérabilités de sécurité sont apparues dans le nouvel **EVERYWHERE WORKPLACE**, rendant nécessaire une stratégie de cybersécurité complète et évolutive pour minimiser les menaces potentielles.

Voici 6 étapes indispensables pour un parcours de cybersécurité fiable et solide.

1. Obtenir une visibilité complète des biens



Pourquoi :

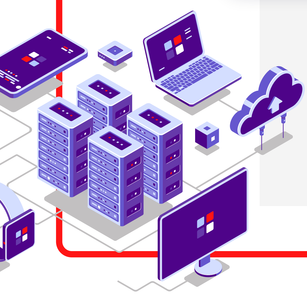
Vous ne pouvez pas gérer ce que vous ne connaissez pas.

Sans inventaire précis des actifs (Cloud, logiciels, matériel), votre entreprise est vulnérable aux risques de sécurité.

Comment :

Obtenez une visibilité complète en temps réel de tous les périphériques connectés pour mieux gérer, organiser et optimiser votre infrastructure IT.

2. Moderniser la gestion des périphériques



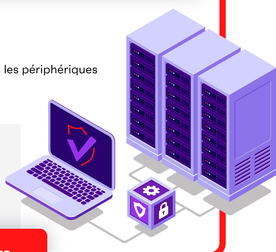
Pourquoi :

La surveillance de la conformité de tous les utilisateurs et périphériques distants est cruciale pour les opérations sécurisées, notamment la mise à jour des logiciels et la résolution rapide des problèmes.

Comment :

Déployez l'UEM dans le cadre de votre stratégie.

3. Mettre en place une bonne hygiène des périphériques



Pourquoi :

L'établissement d'exigences de sécurité universelles sur tous les périphériques rend le diagnostic des problèmes plus rapide et plus facile.

Comment :

Utilisez l'automatisation pour détecter et gérer proactivement tous les problèmes de sécurité liés à l'hygiène des périphériques.

4. Sécuriser vos utilisateurs

Pourquoi :

Les mots de passe manquent de contexte (périphérique, appli, réseau, menace), si bien qu'il est impossible de distinguer les utilisateurs autorisés de ceux qui ne le sont pas.

Comment :

Zero Sign-On : Sans mot de passe, aucun risque de se faire voler des références d'authentification/mots de passe de connexion.

5. Fournir l'accès approprié

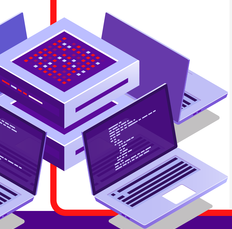
Pourquoi :

Limiter les utilisateurs aux seules ressources d'entreprise dont ils ont besoin limite les menaces de sécurité liées aux accès.

Comment :

Utilisez un accès réseau Zero Trust pour suivre, surveiller et contextualiser l'accès des utilisateurs aux données de l'entreprise.

6. Automatiser la conformité et la gestion des risques



Pourquoi :

La gestion manuelle prend du temps, est inefficace et présente davantage de risques de sécurité.

Comment :

Il faut être proactif, pas réactif : déployez une stratégie de conformité et de gestion des risques universelle et automatisée.

Vous voulez en savoir plus sur l'élaboration d'une stratégie de cybersécurité solide ? Consultez l'eBook « Programme MAP (Manage, Automate, Prioritize - Gérer, automatiser, prioriser) pour votre parcours de cybersécurité » dès maintenant :

Télécharger l'eBook

ivanti