Introduction

La région EMEA présente la plus forte incidence de ransomwares au monde et la plus faible maturité de segmentation

Les entreprises de la région EMEA considèrent désormais la segmentation comme mécanisme de contrôle fondamental. Par conséquent, son adoption s'est considérablement répandue : 90 % des entreprises mettent en place la segmentation du réseau sous une forme ou une autre. Pourtant, malgré des taux d'adoption élevés, la maturité de la segmentation représente un défi majeur dans la région. Seul un quart des entreprises de la région EMEA sont passées à la microsegmentation. Il s'agit de la région avec le taux le plus faible.

Cela n'est pas anodin, puisque c'est également la région recensant la plus forte incidence de ransomwares au monde, ce qui révèle un écart critique entre l'exposition et le niveau de préparation. Les entreprises reconnaissent les enjeux. L'adoption de la cyberassurance s'élève à 75 % et, pour la plupart des entreprises, la protection contre les ransomwares, l'isolement des ressources à haut risque et la protection contre les menaces internes sont devenus des priorités absolues. Mais l'intention ne produit pas de résultats. Moins de 70 % des entreprises indiquent être parvenues à atteindre leurs propres objectifs de confinement, preuve indéniable qu'il existe un écart persistant en matière de mise en œuvre.

En outre, les entreprises de la région EMEA appliquent la segmentation à moins de ressources (serveurs, points de terminaison et terminaux IoT), mettent à jour les règles moins fréquemment et sous-utilisent les plateformes centralisées par rapport aux autres grandes régions. La plupart des entreprises de la région EMEA persistent à mettre en œuvre des règles de pare-feu statiques, bien qu'elles ne soient pas suffisantes dans les environnements hybrides à haut risque actuels.

À retenir :

Si la région EMEA n'accélère pas la mise en œuvre, l'augmentation des budgets ne permettra pas d'assurer la résilience et la région demeurera la cible privilégiée des ransomwares.