ivanti PULSE

État de l'accès sécurisé en Europe

Ces 12 derniers mois, les responsables de la sécurité et de l'IT, partout en Europe, ont connu un certain nombre de menaces de sécurité. Pour relever ce défi toujours plus pressant, ils priorisent différents projets d'accès sécurisé et prévoient de les aligner sur un protocole Zero Trust. Cependant, les priorités varient en fonction du secteur d'activité : logiciels, services financiers ou industrie manufacturière.

Ivanti et Pulse ont mené une enquête auprès de 275 responsables de l'IT et de la sécurité en Europe pour connaître leurs priorités en matière d'accès sécurisé pour ces 12 prochains mois, et savoir comment ils s'en serviront pour réduire la fréquence des problèmes de sécurité.

Les entreprises doivent définir des stratégies d'accès pour lutter contre les menaces de sécurité.

Au cours de l'année écoulée, plus de la moitié des entreprises européennes ont subi une attaque de sécurité. Le plus souvent, les entreprises de ces responsables IT et de sécurité ont été impactées par un accès non autorisé aux applis et ressources (70 %), un malware (60 %), et des failles de sécurité dans les applications mobiles ou Web (60 %).

Parmi les 5 menaces de sécurité suivantes, lesquelles ont le plus impacté votre entreprise ces 12 derniers mois ?
(Sélection multiple possible)

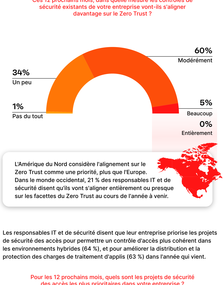
En Amérique du Nord, par contre, la menace de sécurité la plus souvent signalée est le malware (51 %), alors que la zone Asie-Pacifique Japon (APJ) a davantage souffert de failles de sécurité dans les applications mobiles ou Web (79 %).

Pour limiter l'impact de ces menaces de sécurité toujours plus pressantes, 67 % des responsables IT et de sécurité disent qu'il est important que leur entreprise définisse et applique des stratégies d'accès des utilisateurs et des périphériques. Cependant, les 3 projets les plus vitaux sont aussi les 3 plus difficiles à mettre en place.

Parmi les fonctions de sécurité suivantes, lesquelles sont les plus importantes à mettre en œuvre pour que votre entreprise limite les menaces liées à la sécurité des accès ?
(Sélection multiple possible)

Parmi les fonctions de sécurité suivantes, quelles sont les 5 plus difficiles à mettre en œuvre dans votre entreprise pour limiter les menaces/risques de sécurité des accès ? (Sélection multiple possible)

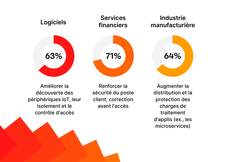
Quel est l'outil le plus important pour limiter les menaces, en fonction du secteur d'activité ?



Pour mieux prévenir les menaces de sécurité, les responsables techniques priorisent le Zero Trust et la sécurisation de l'IT hybride.

99 % des professionnels de l'IT et de la sécurité en Europe disent que leurs pratiques de sécurité vont davantage s'aligner sur une stratégie Zero Trust dans les 12 mois à venir.

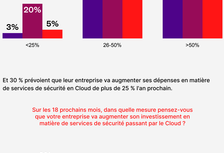
Ces 12 prochains mois, dans quelle mesure les contrôles de sécurité existants de votre entreprise vont-ils s'aligner davantage sur le Zero Trust ?



L'Amérique du Nord considère l'alignement sur le Zero Trust comme une priorité, plus que l'Europe. Dans le monde occidental, 21 % des responsables IT et de sécurité disent qu'ils vont s'aligner entièrement ou presque sur les facettes du Zero Trust au cours de l'année à venir.

Les responsables IT et de sécurité disent que leur entreprise priorise les projets de sécurité des accès pour permettre un contrôle d'accès plus cohérent dans les environnements hybrides (64 %), et pour améliorer la distribution et la protection des charges de traitement d'applis (63 %) dans l'année qui vient.

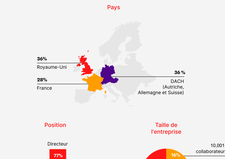
Pour les 12 prochains mois, quels sont les projets de sécurité des accès les plus prioritaires dans votre entreprise ?



Les responsables de l'IT et de la sécurité basculent vers des services de sécurité qui passent par le Cloud, et prévoient de regrouper leurs fournisseurs.

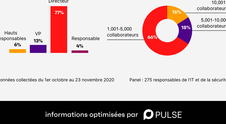
Près des deux tiers (64 %) des responsables IT et de sécurité en Europe disent que leur entreprise a basculé la majorité de ses services de sécurité vers une distribution de Cloud (taux d'adoption le plus élevé du monde).

Combien de services de sécurité votre entreprise a-t-elle basculés vers le Cloud pour remplacer les outils de sécurité sur site traditionnels ?



Et 30 % prévoient que leur entreprise va augmenter ses dépenses en matière de services de sécurité en Cloud de plus de 25 % l'an prochain.

Sur les 18 prochains mois, dans quelle mesure pensez-vous que votre entreprise va augmenter son investissement en matière de services de sécurité passant par le Cloud ?



Enfin, la très grande majorité (96 %) des personnes interrogées sont actuellement en train de réunir leurs fournisseurs de sécurité en une plateforme unifiée ou prévoient de le faire dans les mois à venir. Plus de la moitié (59 %) disent qu'ils le feront très probablement.

Quelle est la probabilité que votre entreprise réunisse ses différents outils d'accès sécurisé en une plateforme plus unifiée avec moins de fournisseurs au cours des 12 prochains mois ?

Pays

Position

Taille de l'entreprise

Données collectées du 1er octobre au 23 novembre 2020 — Panel : 275 responsables de l'IT et de la sécurité