ivanti

Cybersecurity
INSIDERS

Rapport 2023 sur la progression du Zero Trust

ivanti.com

Vue d’ensemble

Le Zero Trust et son mantra « ne jamais faire confiance, toujours vérifier » s’imposent comme le socle des pratiques de cybersécurité actuelles.

Le rapport 2023 sur la progression du Zero Trust restitue les résultats d’une enquête menée auprès de 431 professionnels IT et de cybersécurité et analyse en profondeur l’adoption croissante, les principales difficultés et les stratégies efficaces des modèles d’accès Zero Trust dans les entreprises d’aujourd’hui.

L’enquête révèle que 68 % des professionnels interrogés prévoient ou s’efforcent d’adopter un modèle d’accès Zero Trust. Pour y parvenir, les entreprises privilégient une approche globale de la sécurité : 57 % priorisent la gestion des identités et des accès (IAM) et 52 % visent à sécuriser l’accès aux applications Cloud. Ces choix, qui viennent compléter l’EDR (détection et réponse des terminaux) et améliorer la remédiation des vulnérabilités, confirment en outre l’adoption croissante des pratiques de sécurité Zero Trust.

Les périphériques à risque qui accèdent aux ressources réseau représentent la principale difficulté selon 48 % des personnes interrogées, ce qui illustre l’importance de la vérification stricte et de la surveillance continue des périphériques. L’accès de collaborateurs aux privilèges trop élevés, source d’inquiétude pour 47 % des personnes interrogées, montre l’urgence à implémenter le principe d’accès au moindre privilège dans une structure Zero Trust.

L’effort d’investissement dans l’authentification multifacteur (MFA) arrive en tête des priorités pour 65 % des personnes interrogées, ce qui en fait un pilier de l’architecture Zero Trust. Et le fait que plus de la moitié des entreprises (54 %) utilisent 2 à 4 produits pour le Zero Trust suggère une approche par couche de l’implémentation.

À mesure que l’environnement cyber évolue, les entreprises n’auront d’autre choix que d’adopter les principes du Zero Trust et de les aligner sur les priorités de sécurité si elles veulent efficacement atténuer les risques et protéger leurs actifs.

Nous remercions Ivanti pour son soutien à cette enquête essentielle. Nous espérons qu’elle vous sera utile dans vos efforts continus de protection de vos environnements IT.

Avec nos remerciements,

Holger Schulze

Holger Schulze
PDG et fondateur
Cybersecurity Insiders

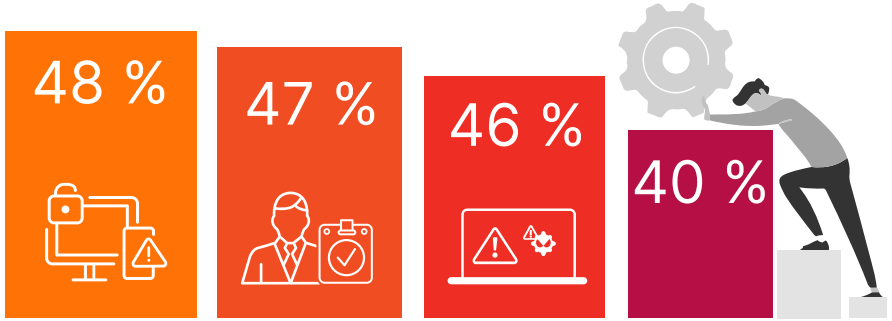
Cybersecurity INSIDERS

Le défi de l'accès sécurisé

En matière de sécurisation de l'accès aux applications et aux ressources, les principales difficultés sont étroitement liées aux grands principes Zero Trust. En première place des préoccupations avec 48 % des réponses cette année se trouvent les périphériques exposés aux risques qui ont accès aux ressources réseau. Ce classement souligne le besoin impérieux de vérifier rigoureusement les périphériques et de les surveiller en permanence auquel répond le Zero Trust, qui garantit que seuls les périphériques de confiance obtiennent l'accès aux ressources sensibles.

Autre inquiétude majeure : l'accès des collaborateurs aux privilèges trop élevés pour 47 % des personnes interrogées. Dans le contexte du Zero Trust, cette deuxième place montre l'urgence à implémenter le principe du moindre privilège qui garantit que les utilisateurs disposent uniquement des droits d'accès strictement nécessaires à leurs tâches.

Quelles sont les principales difficultés de la sécurisation de l'accès aux applications et aux ressources dans votre entreprise ?[1] [n = 424]



Périphériques fantômes à risque (Shadow IT) accédant aux ressources réseau (postes client inconnus, non approuvés, non conformes)

Accès de collaborateurs aux privilèges trop élevés

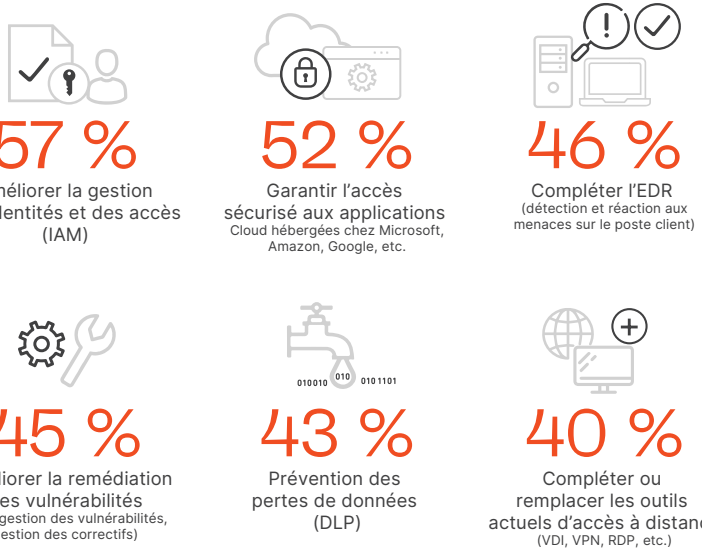
Cyberattaques ex., déni de service, scripts intersites, par interception « man-in-the-middle », hameçonnage

Shadow IT

Des priorités de sécurité en phase avec l'objectif du Zero Trust

Les priorités de sécurité qui ressortent suggèrent que les entreprises adoptent une approche globale de la sécurité, à plusieurs couches. L'accent mis sur l'IAM (57 %) et l'accès sécurisé aux applications Cloud (52 %) plaide en faveur de la sécurité Zero Trust. En effet, ces priorités sont alignées sur les principes de vérification des identités des utilisateurs et des périphériques, et de contrôle de l'accès aux ressources. De plus, l'importance des mesures complémentaires à l'EDR (46 %) et d'amélioration de la remédiation des vulnérabilités (45 %) correspond au principe Zero Trust de surveillance continue et de réponse rapide aux menaces. Dans l'ensemble, ces priorités montrent que les entreprises adoptent toujours plus les pratiques de sécurité Zero Trust en renfort de leur posture générale de sécurité.

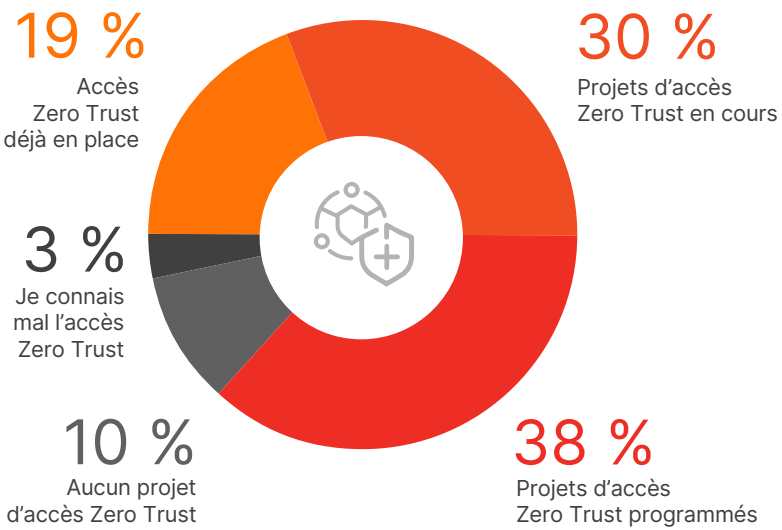
Quelles sont les priorités actuelles de votre entreprise en matière de sécurité ? [n = 421]



Plans d’adoption du Zero Trust

Le Zero Trust est déjà en place dans une entreprise sur cinq (19 %). Pour les autres, une grande partie (38 %) des professionnels interrogés ont des projets d’implémentation d’accès Zero Trust et 30 % ont déjà commencé à mettre en œuvre leurs plans. Ainsi, la majorité des entreprises interrogées (68 %) prévoiraient d’adopter un modèle d’accès Zero Trust ou y travailleraient déjà activement.

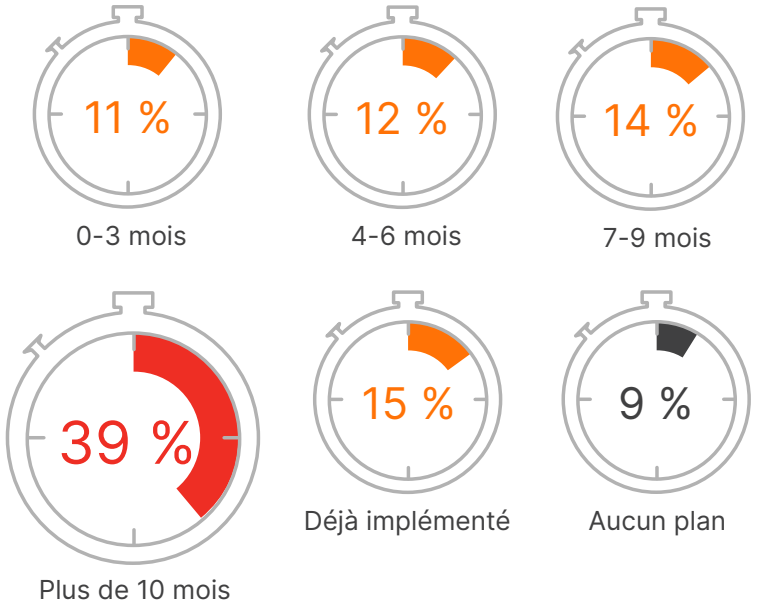
Avez-vous prévu d’adopter un modèle d’accès Zero Trust dans votre entreprise ? [n = 424]



Délais d’adoption du Zero Trust

Le rythme d’adoption de la sécurité Zero Trust varie d’une entreprise à l’autre. Si une large portion d’entre elles a déjà implémenté ce modèle (15 %) et d’autres prévoient d’y arriver prochainement (dans les 9 mois pour 37 %), bon nombre d’entreprises admettent qu’il leur faudra sans doute plus de 10 mois pour passer entièrement à la sécurité Zero Trust (39 %).

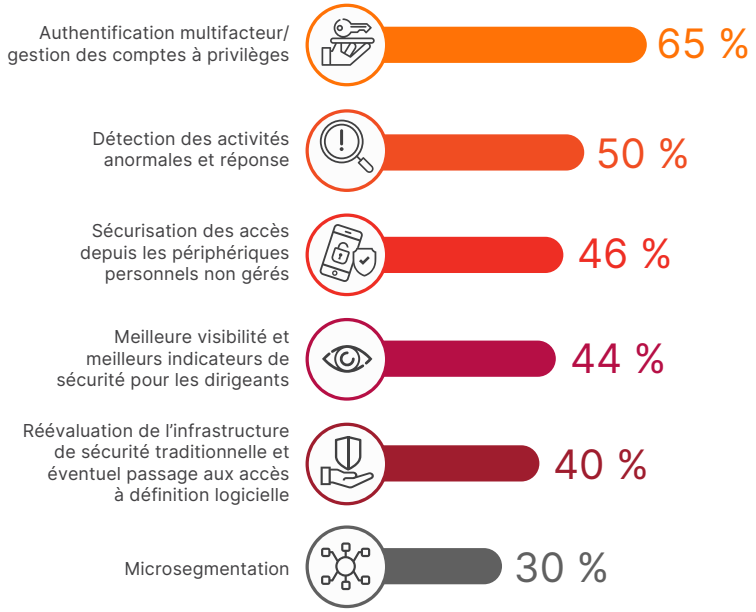
À quel horizon prévoyez-vous d’adopter la sécurité Zero Trust ? [n = 423]



Les priorités de l'accès sécurisé

Les entreprises s'intéressent à plusieurs priorités d'accès sécurisé qui reflètent précisément les principes du Zero Trust, comme le MFA (65 %), la détection des menaces en temps réel (50 %) et la sécurisation des accès depuis des périphériques personnels (46 %). Ces préoccupations correspondent bien au grand principe Zero Trust, « ne jamais faire confiance, toujours vérifier » qui garantit la bonne authentification et l'autorisation des utilisateurs avant de leur donner accès à des ressources sensibles.

Quelles sont vos priorités d'accès sécurisé pour les 1 ou 2 ans à venir ? [n = 430]

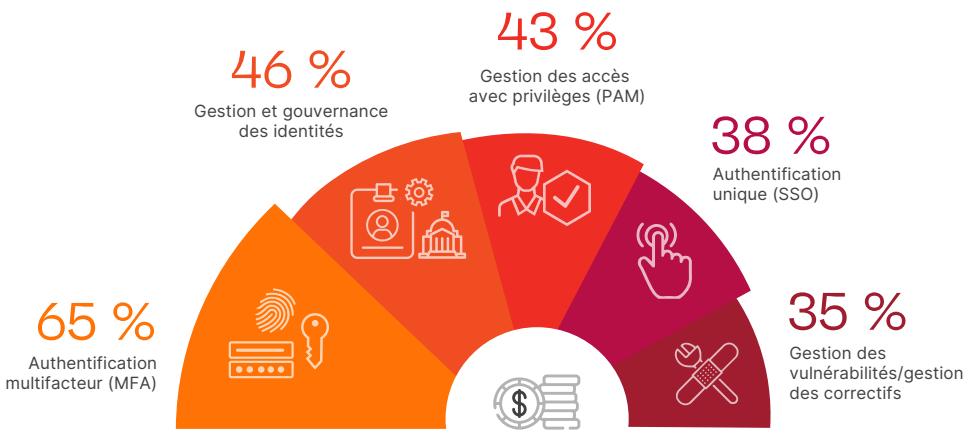


Plans d'investissement

Dans les entreprises, les priorités d'investissement dans les outils de contrôle des identités, des accès et du Zero Trust ciblent principalement l'authentification des utilisateurs, la gestion des droits d'accès et le maintien de la sécurité globale du système. L'authentification multifacteur (MFA, élément clé du Zero Trust) se distingue comme priorité absolue, 65 % des personnes interrogées prévoyant d'y investir.

Ces axes reflètent les principes majeurs du Zero Trust, ce qui montre l'intérêt croissant que les entreprises portent à l'adoption de ce cadre de sécurité.

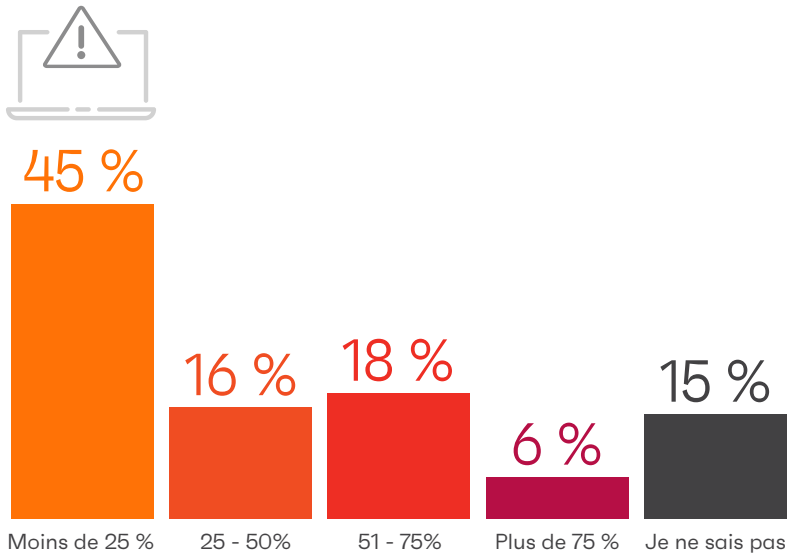
Parmi les contrôles des identités/accès et Zero Trust suivants, quelles sont les priorités d'investissement de votre entreprise dans les 12 prochains mois ? [2] [n = 431]



Risques liés aux privilèges d'accès excessifs

Près de la moitié des professionnels interrogés (45 %) estiment que l'accès avec de trop grands privilèges cause moins de 25 % des incidents de sécurité. Ainsi, même si l'accès avec de trop grands privilèges est inquiétant, pour beaucoup d'entreprises, ce ne serait pas le principal facteur des incidents de sécurité. Un tiers des entreprises (34 %) ont constaté que 25 % à 75 % des incidents résultent de privilèges d'accès excessifs. Ces résultats soulignent l'importance d'implémenter le principe Zero Trust de l'accès au moindre privilège pour limiter les risques de sécurité liés aux privilèges d'accès trop élevés.

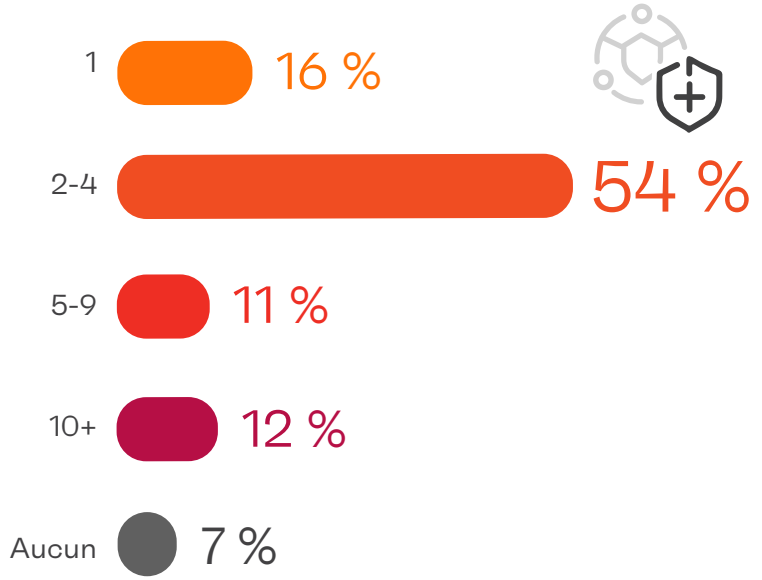
D'après vous, quel pourcentage approximatif des incidents de sécurité dans votre entreprise ces 12 derniers mois est causé par des utilisateurs finaux aux privilèges d'accès supérieurs à ceux nécessaires à leur travail quotidien ? [n = 431]



Approche multicouche du Zero Trust

La majorité des professionnels interrogés (54 %) utilisent 2 à 4 produits pour le Zero Trust/l'accès sécurisé. La plupart des entreprises auraient ainsi une approche multicouche de l'implémentation du Zero Trust avec des produits différents pour gérer les diverses facettes de ce modèle (gestion des accès, vérification des périphériques, segmentation réseau, etc.). Dans le contexte du Zero Trust, ces résultats indiquent que les entreprises adoptent des approches et des niveaux de complexité différents quand elles implémentent un programme d'accès sécurisé.

Combien de produits utiliseriez-vous (ou utilisez-vous déjà) pour un programme d'accès sécurisé Zero Trust dans votre entreprise ? [n = 429]



Meilleures pratiques Zero Trust

Le modèle de sécurité Zero Trust repose sur le principe qu'aucune confiance préalable n'est accordée sur le réseau d'une entreprise et applique une vérification stricte de chaque utilisateur, périphérique et demande. Pour implémenter efficacement le Zero Trust, les entreprises doivent se fier aux meilleures pratiques de base suivantes :

Implémenter l'authentification multifacteur (MFA)
Renforcez l'authentification en cumulant plusieurs méthodes, comme la biométrie ou les jetons, en plus des traditionnels noms d'utilisateur et mots de passe.

Adopter le principe du moindre privilège (POLP)
Quand vous attribuez aux utilisateurs uniquement les droits d'accès minimaux nécessaires à leurs tâches, vous réduisez les menaces internes et les risques de fuite de données.

Vérifier et surveiller les périphériques en continu
Pour vous assurer que seuls les périphériques de confiance accèdent aux ressources sensibles, appliquez une vérification stricte des périphériques et une surveillance en continu.

Sécuriser l'accès aux applications Cloud
Adoptez les principes Zero Trust pour l'accès aux ressources Cloud et mettez en place des mesures de sécurité comme le chiffrement, le contrôle d'accès et la journalisation.

Réexaminer et mettre à jour régulièrement les contrôles d'accès
Évaluez et ajustez constamment vos mesures de contrôle d'accès pour qu'elles restent pertinentes et sûres, alignées sur l'évolution des rôles et des responsabilités au sein de votre entreprise.

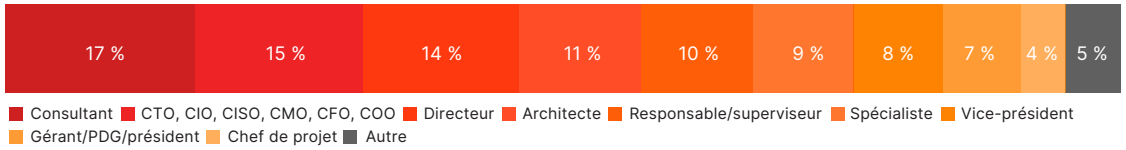
Implémenter la détection et la réponse aux anomalies
Incorporez des technologies avancées de détection et de réponse, comme l'EDR (détection et réponse des terminaux) et le XDR (détection et réponse étendues), pour rapidement identifier les menaces et en atténuer les risques.

Sensibiliser à la sécurité
Formez vos collaborateurs aux principes Zero Trust et aux réflexes de sécurité en ligne, apprenez-leur à repérer et à signaler les menaces de sécurité, et réduisez ainsi la probabilité d'incidents de sécurité dus à l'erreur humaine.

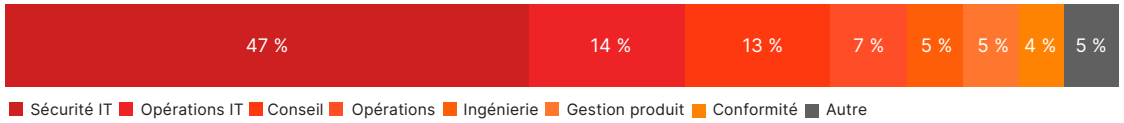
Méthodologie et personnes interrogées

Ce rapport restitue les résultats d'une enquête en ligne complète auprès de 431 professionnels de l'IT et de la cybersécurité aux États-Unis, menée en mars 2023 pour connaître les dernières tendances d'adoption, les difficultés, les lacunes et les solutions préférées des entreprises en matière de sécurité Zero Trust. Nous avons interrogé divers acteurs, des responsables techniques aux techniciens de sécurité informatique, pour constituer un panel représentatif d'entreprises de toutes tailles dans plusieurs secteurs d'activité.

Postes

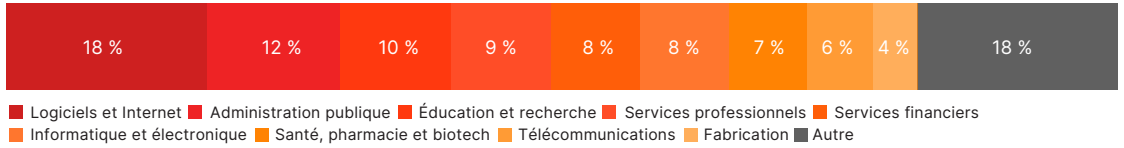


Département



Taille de l'entreprise

Secteur d'activité



ivanti.fr
33 (0)1 76 40 26 20
contact@ivanti.fr

ivanti

Ivanti rend possible l'Everywhere Workplace. Dans l'Everywhere Workplace, les collaborateurs utilisent une multitude de périphériques pour accéder aux données et aux applications du département IT sur différents réseaux, afin de rester productifs en travaillant de partout.

La plateforme d'automatisation Ivanti Neurons connecte les solutions Ivanti de gestion unifiée du poste client (UEM), de sécurité Zero Trust et de gestion des services d'entreprise (ESM), leaders du marché, afin de créer une plateforme IT unifiée permettant l'autoréparation et l'autosécurisation des périphériques, et le self-service aux utilisateurs.

Plus de 40 000 clients, dont 78 des entreprises Fortune 100, ont choisi Ivanti pour découvrir, gérer, sécuriser et servir leurs actifs IT, du Cloud à la périphérie, ainsi que pour fournir une expérience utilisateur d'excellence aux collaborateurs, où qu'ils se trouvent et quelle que soit la façon dont ils travaillent.

Pour en savoir plus, visitez le site www.ivanti.fr et suivez @GoIvanti.

1 Processus manuels complexes qui empêchent de réagir rapidement 37 % | Accès non sécurisé des partenaires aux applis et ressources 33 % | Périphériques mobiles vulnérables, débridés ou perdus accédant aux ressources 17 %

2 Microsegmentation 34 % | Réseaux privés virtuels (VPN) 33 % | Gestion des appareils mobiles (EMM) 29 % | Antihameçonnage 28 % | Broker de sécurité d'accès Cloud (CASB) 28 % | Contrôle complet de l'accès réseau Zero Trust 27 % | Pare-feu d'application Web (WAF) 26 % | Contrôle des accès réseau (NAC) 25 % | Analyse des identités 24 % | Périmètre défini par logiciel (SDP) 24 % | Invisibilité des périphériques réseaux aux menaces 20 % | Prévention des pertes de données (DLP) 17 % | Défense contre les menaces mobiles 16 % | Services d'annuaire d'entreprise 13 % | Gestion des droits numériques (DRM) 9 % | Autre 5 %

Cybersecurity
INSIDERS

Cybersecurity Insiders est une communauté en ligne qui compte plus de 500 000 membres. Conçue pour les professionnels de la sécurité de l'information, elle regroupe les meilleurs cerveaux qui se consacrent aux progrès de la cybersécurité et à la protection des entreprises de toute taille dans tous les secteurs d'activité, quelles que soient les fonctions de sécurité existant en interne.

Nous offrons aux spécialistes du marketing de la cybersécurité des opportunités marketing uniques pour atteindre ce public qualifié, et fournir un contenu décisionnel basé sur des faits et validé par des tiers, des programmes de génération de demande et une visibilité des marques sur le marché de la cybersécurité.

Pour en savoir plus, visitez le site www.cybersecurity-insiders.com