Microsoft Security

hypothesis

Rapport sur l'adoption de la confiance zéro

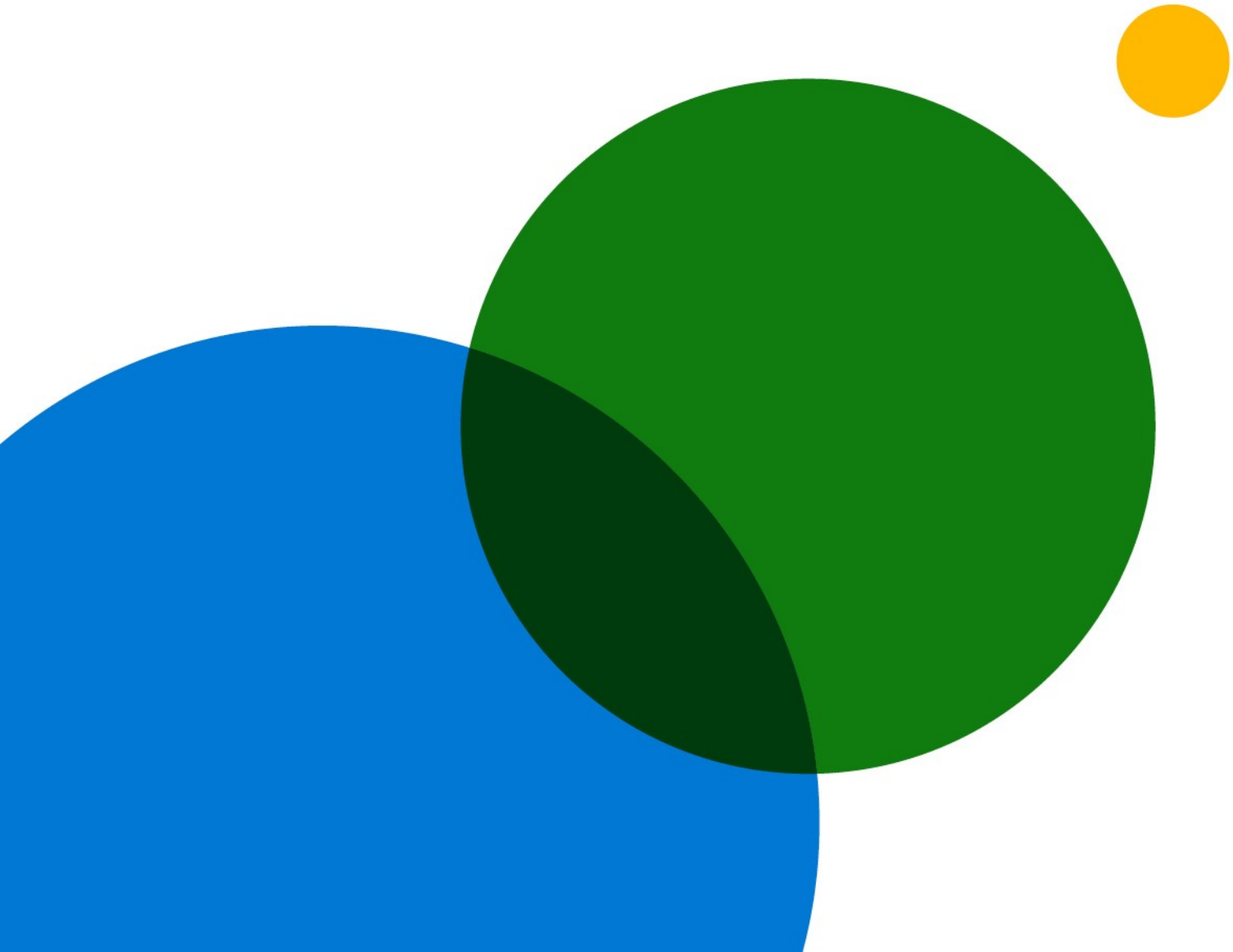


Table des matières

Introduction

Vasu Jakkal / Vice-président – Sécurité, conformité et identité

L'année que nous venons de passer a été remarquable pour l'évolution de la cybersécurité et la montée en force de la confiance zéro en tant que stratégie directrice pour le secteur et les entreprises du monde entier.

Au début de la pandémie, le milieu de travail est devenu distant presque du jour au lendemain. Ce changement a forcé de nombreuses entreprises à s'adapter rapidement afin de soutenir les employés qui accomplissaient leur travail comme ils pouvaient en utilisant des appareils personnels, en collaborant au moment des services infonuagiques et en partageant des données en dehors du périmètre du réseau d'entreprise. Tandis que les entreprises s'adaptaient à cette transformation, elles étaient également confrontées à des cybercriminels de plus en plus spécialisés qui faisaient continuellement évoluer leur ciblage, leurs stratégies et leurs ressources.

Aujourd'hui, le travail hybride fait partie de notre nouvelle réalité. Dans ce contexte de changements rapides, les entreprises que nous avons sondées nous ont dit qu'elles s'appuyaient sur la confiance zéro pour accroître leur agilité en matière de sécurité et de conformité, pour accélérer la détection et la correction des menaces, et pour augmenter la simplicité et la disponibilité des analyses de sécurité.

D'après les principes de vérification explicite, de privilège d'accès minimal et de présomption d'atteinte à la sécurité, une architecture de confiance zéro complète instaure des mesures de sécurité à travers les identités, les points de terminaison, les applications, l'infrastructure, le réseau et les données, tout en procurant une visibilité, une automatisation et une orchestration plus importantes. Non seulement nous recommandons cette approche pour nos clients et nos partenaires, mais nous l'adoptons aussi dans notre propre approche mondiale de sécurité et de développement logiciel à Microsoft.

Ce rapport apporte des précisions sur le parcours d'adoption de la confiance zéro dans divers marchés et secteurs. Nous espérons que les informations que vous en tirerez vous aideront à accélérer votre propre adoption de la stratégie de confiance zéro, mettront en lumière les progrès collectifs réalisés par vos pairs et vous fourniront des renseignements sur les conditions futures de cet espace en évolution rapide.

Méthodologie

Microsoft a chargé Hypothesis Group, une agence spécialisée dans les informations, la conception et les stratégies, de mener une recherche et de produire un rapport sur l'adoption de la confiance zéro. La recherche comportait deux phases aux États-Unis ayant pour but de connaître les tendances et l'état actuel de l'adoption de la confiance zéro. Des marchés supplémentaires étaient ensuite ajoutés lors de la deuxième phase afin de révéler les tendances à l'échelle mondiale.

La recherche initiale a eu lieu en août 2020, période à laquelle un sondage en ligne de 15 minutes a été mené aux États-Unis auprès de 300 décideurs en matière de sécurité (SDM) participant à la prise de décisions stratégiques en matière de confiance zéro dans des entreprises appartenant à un éventail de secteurs. En plus du sondage en ligne, cinq entrevues approfondies ont été menées en ligne en septembre 2020 auprès des SDM de divers secteurs aux États-Unis.

En avril 2021, des recherches mondiales ont été menées aux États-Unis, en Allemagne, au Japon, en Australie et en Nouvelle-Zélande dans un groupe semblable composé de décideurs en matière de sécurité. Plus de 900 personnes ont participé à un sondage en ligne de 15 minutes dont les questions portaient sur leur adoption d'une stratégie de confiance zéro, les pratiques exemplaires, les avantages, les défis et les projets en matière d'investissement.

Ce que vous devez savoir sur l'adoption de la confiance zéro

01 / Les entreprises sont prêtes à tirer profit d'une stratégie de confiance zéro, un mouvement accéléré par le passage à un milieu de travail hybride et la pandémie de COVID-19

Les décideurs en matière de sécurité (SDM) affirment que l'élaboration d'une stratégie de confiance zéro constitue leur priorité absolue en matière de sécurité, 96 % d'entre eux déclarant qu'elle est essentielle à la réussite de leur entreprise. Les principaux facteurs de motivation pour l'adoption d'une stratégie de confiance zéro sont l'amélioration de l'état global de la sécurité et de l'expérience de l'utilisateur final. Le passage à un milieu de travail hybride accéléré par la pandémie de COVID-19 favorise également une plus grande adoption de la confiance zéro. En effet, 81 % des entreprises ont entamé leur passage à un milieu de travail hybride, parmi lesquelles 31 % ont terminé le processus. Toutefois, 94 % sont préoccupées par la transition, particulièrement l'utilisation à mauvais escient par les employés, l'augmentation des charges de travail informatiques et les cyberattaques. Par conséquent, les principaux points dont il faut tenir compte dans l'établissement d'une stratégie comprennent une hausse de la formation pour les employés et une mise en œuvre de l'authentification multifacteur (AMF) pour assurer une expérience utilisateur et une migration en douceur.

02 / La stratégie de confiance zéro offre de la souplesse aux entreprises qui peuvent commencer à la mettre en œuvre là où elles le souhaitent tout en adaptant l'approche à leurs besoins

Moins de 15 % des entreprises ont commencé à mettre en œuvre leur stratégie de confiance zéro dans le même domaine de risque en matière de sécurité. Cela s'explique en grande partie par le fait que la mise en œuvre est abordée comme un processus de bout en bout qui s'effectue à travers les piliers et les capacités de l'architecture de sécurité, plutôt que comme une série de technologies individuelles disparates. De la même façon, l'ordre selon lequel les composantes individuelles de la confiance zéro sont mises en œuvre dans une zone de risque de sécurité particulière varie beaucoup, comme les professionnels de la sécurité ne commencent pas tous au même endroit.

03 / Bien que la stratégie de confiance zéro soit déjà largement adoptée et qu'elle améliore la capacité des entreprises à gérer les menaces, il reste encore du travail à faire

76 % des entreprises ont au moins commencé à mettre en œuvre une stratégie de confiance zéro, avec 35 % d'entre elles qui déclarent l'avoir entièrement mise en œuvre. Toutefois, ces dernières admettent ne pas avoir fini de mettre en œuvre la stratégie de confiance zéro dans tous les domaines et toutes les composantes de risque en matière de sécurité. La confiance zéro est attrayante, car elle procure une agilité accrue, une détection des menaces accélérée et une capacité améliorée à gérer la sécurité de l'Internet des objets (IdO) et de la technologie opérationnelle. L'adoption est en croissance aux États-Unis, étant passée de 70 % en août 2020 à 79 % en avril 2021. Pour ce qui est de la mise en œuvre, les États-Unis ont également une longueur d'avance sur d'autres pays qui ont commencé leur adoption plus tard. Finalement, les entreprises aux États-Unis prétendent être moins touchées par des contraintes budgétaires. Toutefois, bien que 57 % des entreprises affirment être en avance sur les autres en matière d'adoption, environ la moitié d'entre elles qui n'ont pas entièrement mis en œuvre la confiance zéro dans tous les domaines et toutes les composantes de risque en matière de sécurité ont encore du travail à faire.

04 / Dans l'avenir, la stratégie de confiance zéro demeurera une priorité absolue et nécessitera une prise de décision minutieuse pour ce qui est des employés et des fournisseurs

La confiance zéro devrait rester la priorité absolue en matière de sécurité au cours des deux années à venir, et les entreprises prévoient d'augmenter leurs investissements en ce sens. Surmonter les défis liés aux employés (notamment la dotation en personnel des équipes de sécurité et l'adhésion de la direction) sera essentiel si elles souhaitent mettre les bouchées doubles avec leurs investissements dans la confiance zéro. En ce qui concerne la stratégie relative aux fournisseurs, les décideurs en matière de sécurité préfèrent légèrement travailler avec des fournisseurs holistiques ou consolidés, étant donné que la sélection des fournisseurs dépend souvent de la disponibilité des experts à l'interne. Les avantages de l'approche « best-in-suite » comprennent une expertise, des ressources et une simplicité accrues, bien que la mise en œuvre puisse prendre plus de temps et l'intégration être plus difficile à réaliser dans l'architecture de sécurité existante, sans oublier une augmentation potentielle des vulnérabilités.

Personnes sondées

À l'échelle mondiale

Décideurs en matière de sécurité

qui travaillent dans des sociétés de calibre entreprise*

90 %
Familiers avec la confiance zéro
Autodéclarés; ont passé un test de connaissances

76 %
de la mise en œuvre de la confiance zéro

24 % de la planification et de l'évaluation de la confiance zéro

* Plus de 1 000 employés aux États-Unis; plus de 500 employés en Allemagne, au Japon, en Australie et Nouvelle-Zélande

Apprentis-sages généraux tirés de la recherche

Les entreprises sont prêtes à tirer profit d'une stratégie de confiance zéro

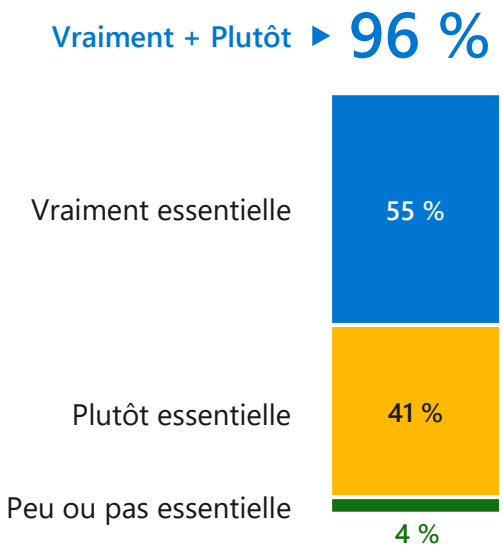
Aujourd'hui, la stratégie de confiance zéro est la priorité absolue en matière de sécurité dans tous les marchés et secteurs, et un certain nombre d'entreprises ont adopté ce modèle au cours des dernières années. Bien que la confiance zéro soit au cœur des préoccupations des entreprises partout dans le monde (53 %), cela est particulièrement vrai aux États-Unis (56 %) et en Allemagne (53 %).

Presque tous les professionnels de la sécurité (96 %) croient qu'une stratégie de confiance zéro est essentielle à la réussite de leur entreprise. (Voir l'Annexe 1) En plus de renforcer l'état de leur sécurité globale et d'améliorer l'expérience de l'utilisateur final, les professionnels de la sécurité se tournent vers la confiance zéro pour simplifier les procédures de sécurité pour les employés. (Voir l'Annexe 2)

Comme l'explique un décideur en matière de sécurité dans le secteur de l'hôtellerie aux États-Unis : *« L'objectif est d'améliorer l'état de notre sécurité globale, mais il est également question de réduire les frictions dans l'expérience de l'utilisateur final et de lui faciliter la vie. »*

De plus, 31 % des professionnels de la sécurité considèrent que la stratégie de confiance zéro constitue un outil précieux dans le passage imminent à un milieu de travail hybride après la pandémie. Ce facteur joue un rôle particulièrement important en Australie et en Nouvelle-Zélande (44 %).

Annexe 1. La confiance zéro est cruciale



Annexe 2. Facteurs de motivation en faveur de la confiance zéro

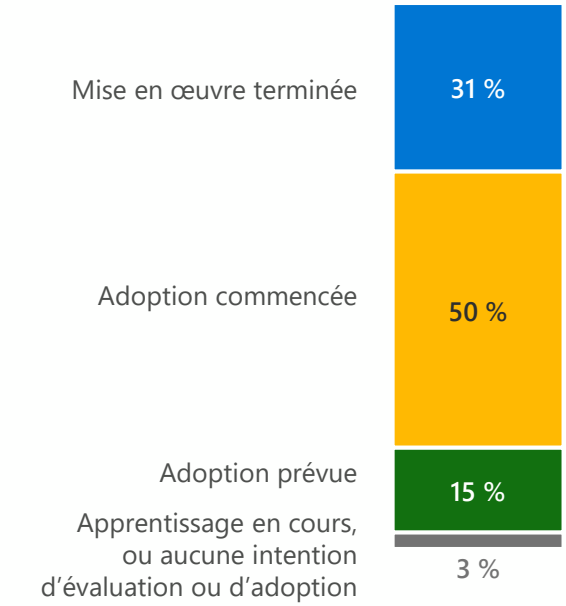
Principaux facteurs de motivation	
Améliorer la stratégie de sécurité globale	47 %
Améliorer l'expérience et la productivité des utilisateurs finaux	44 %
Transformer la façon dont les équipes de sécurité travaillent ensemble	38 %
Simplifier la pile de sécurité	35 %
Réduire les coûts liés à la sécurité	35 %

Le passage au milieu de travail hybride stimule une adoption plus large de la stratégie de confiance zéro

81 % des entreprises ont amorcé leur migration vers un milieu de travail hybride, parmi lesquelles 31 % ont terminé leur transition. Cela étant dit, les taux d'adoption complète ne sont pas constants d'un marché à l'autre. Alors que l'Australie et la Nouvelle-Zélande sont en tête du peloton avec 37 % des entreprises qui ont déjà adopté un modèle hybride, l'Allemagne est loin derrière à seulement 20 %. (Voir l'Annexe 3)

Bien que les marchés mondiaux évoluent vers un milieu de travail hybride à différents rythmes, la grande majorité (91 %) des entreprises qui n'ont pas terminé leur transition prévoient le faire au cours des cinq prochaines années. Fait important, 94 % sont inquiètes de la transition. En tête de liste de leurs préoccupations, soulignons notamment une utilisation à mauvais escient par les employés, une augmentation des charges de travail informatiques et le risque accru posé par les cyberattaques. (Voir l'Annexe 4)

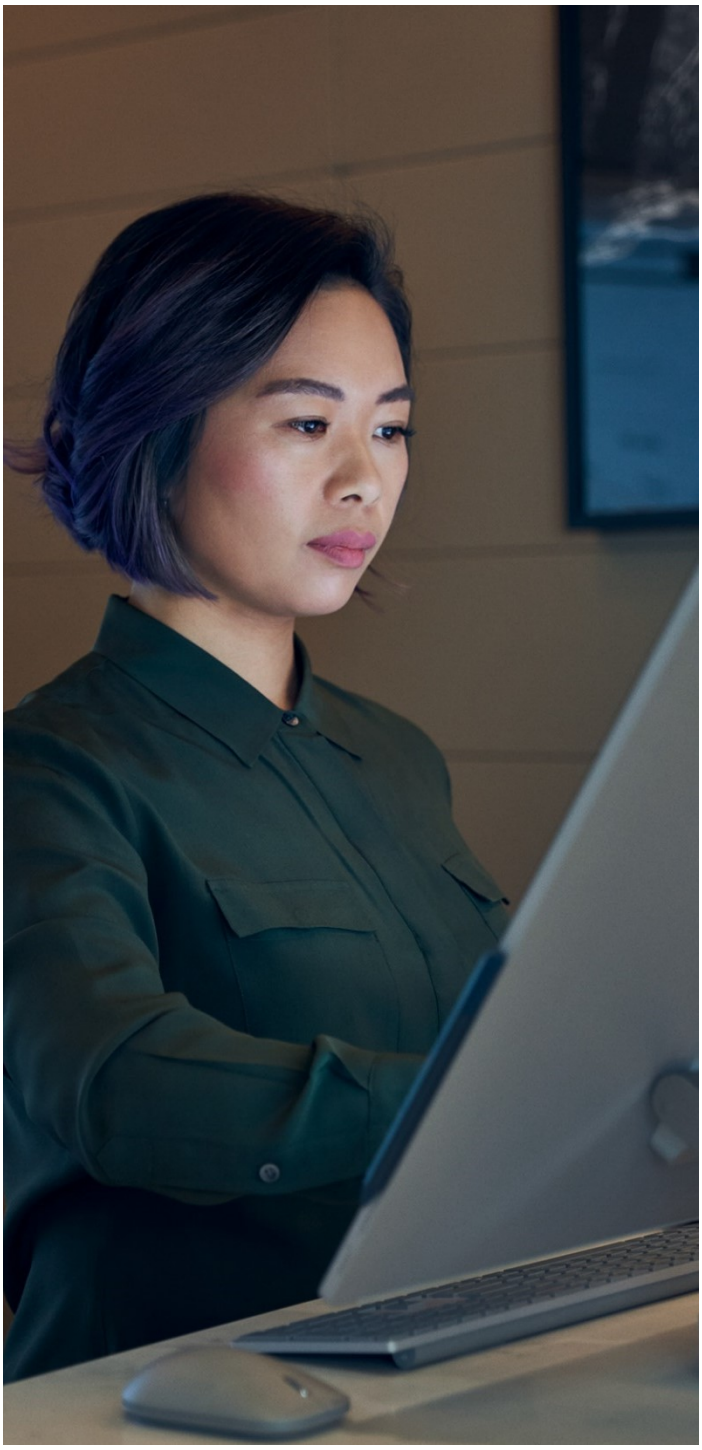
Annexe 3. Intention à l'égard du milieu de travail hybride



Annexe 4. Préoccupations liées au milieu de travail hybride

Téléchargement par les employés d'applications dangereuses	37 %
Augmentation de la charge de travail informatique	37 %
Attaques par rançongiciel	36 %
Attaques par hameçonnage	35 %
Utilisation inappropriée des appareils personnels	34 %
Accès non autorisé aux données	31 %
Incapacité à gérer tous les appareils	30 %
Utilisation des comptes de messagerie personnels	30 %
Non-conformité aux règlements en matière de données	24 %

La COVID-19 a apporté de nouveaux points qui accélèrent le passage à la stratégie de confiance zéro



Dans un souci de minimiser les éventuels problèmes, les intervenants soulignent l'importance d'une hausse de la formation pour les employés (54 %) (particulièrement au Japon [61 %] et en Allemagne [58 %]) et l'authentification multifacteur (MFA) (50 %) (particulièrement aux États-Unis [52 %] et en Allemagne [56 %]) pour assurer une expérience utilisateur et une transition harmonieuses.

Comme le travail sécurisé à distance et hybride peut être facilité par une stratégie de confiance zéro, la COVID-19 a accéléré son adoption pour 72 % des entreprises, bien que des inégalités surviennent entre les marchés. Si la pandémie a accéléré l'adoption dans environ sept entreprises sur dix aux États-Unis (76 %), au Japon (71 %) et en Australie et Nouvelle-Zélande (69 %), les taux de mise en œuvre ont été considérablement faibles en Allemagne (62 %), possiblement en raison d'une transition plus lente vers un milieu de travail hybride.

La confiance zéro est largement mise en œuvre dans le monde entier, et elle gagne du terrain aux États-Unis

La confiance zéro n'est pas seulement un concept à la mode; c'est une réalité. 76 % des entreprises ont au moins commencé à mettre en œuvre cette stratégie, et 35 % considèrent qu'elle est entièrement mise en œuvre. Ces données brossent toutefois un tableau trop optimiste, car de nombreuses entreprises qui prétendent avoir terminé leur mise en œuvre avouent ne pas l'avoir effectuée complètement dans tous les domaines de risque en matière de sécurité. Aujourd'hui, les États-Unis sont en avance par rapport à d'autres marchés quant à l'adoption de la stratégie de confiance zéro, une tendance qui s'accélère. Depuis août 2020, la mise en œuvre de la confiance zéro aux États-Unis est passée de 70 % à 79 %, ce qui représente un bond considérable en seulement huit mois. (Voir l'Annexe 5)

Bien que la stratégie de confiance zéro soit prédominante actuellement dans le domaine de la sécurité, son omniprésence est relativement nouvelle. 82 % des entreprises ont mis en œuvre des stratégies de confiance zéro au cours des 3 dernières années, dont 21 % au cours des 12 derniers mois. Toutefois, 26 % des entreprises aux États-Unis ont commencé leur mise en œuvre il y a plus de 3 ans, contre 19 % au Japon, 6 % en Australie et Nouvelle-Zélande, et 3 % en Allemagne. Cette mise en œuvre précoce aux États-Unis, parallèlement à un nombre inférieur de contraintes budgétaires, pourrait expliquer pourquoi les entreprises aux États-Unis sont en avance dans l'adoption de la confiance zéro par rapport à celles d'autres marchés. Dans un même ordre d'idées, la jeunesse relative de la confiance zéro en Allemagne aide à fournir un contexte pour ses taux d'adoption plus faibles : 97 % des entreprises allemandes ont commencé leur mise en œuvre au cours des trois dernières années seulement.

Annexe 5. Mise en œuvre de la confiance zéro

	US (2020)	US	DE	JP	AU/NZ
Mise en œuvre de la confiance zéro	70 %	79 %	75 %	76 %	71 %
• Mise en œuvre terminée	27 %	44 %	19 %	32 %	28 %
• En cours	43 %	35 %	56 %	44 %	43 %

35 % – Mise en œuvre terminée

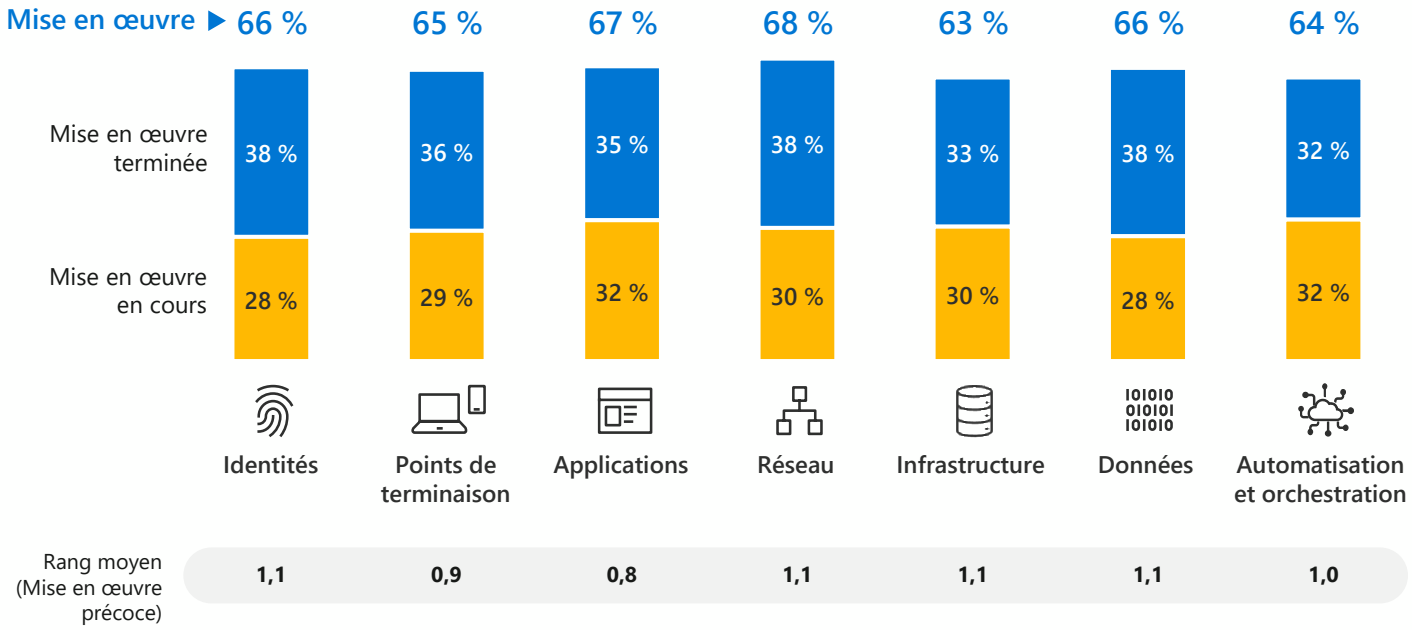
42 % – Mise en œuvre en cours

Il n'y a pas de solution unique pour la mise en œuvre de la confiance zéro, ce qui vous permet de commencer n'importe où

Aucun domaine de risque en matière de sécurité précis, que ce soit les identités, les points de terminaison, les applications, le réseau, l'infrastructure, les données, l'automatisation ou l'orchestration, ne se distingue comme point de départ principal de la stratégie de confiance zéro. En effet, moins de 15 % des entreprises commencent avec le même domaine de risque en matière de sécurité. Les organisations commencent à différents endroits, sans doute en fonction de leurs besoins et des ressources disponibles à l'interne. Enfin, les entreprises cherchent à adopter une stratégie de confiance zéro dans tous les domaines de risque en matière de sécurité afin d'assurer une protection accrue contre les menaces, de sorte que la confiance zéro est perçue comme une stratégie de bout en bout que l'on développe au fil du temps. (Voir l'Annexe 6)

Au-delà des domaines de risque en matière de sécurité de la confiance zéro, les entreprises doivent déterminer les composantes individuelles de chaque domaine de risque en matière de sécurité qui doivent être traitées en priorité. Pour les points de terminaison, les applications, le réseau, les données, l'automatisation et l'orchestration, il n'y a pas de point de départ clair. Les professionnels de la sécurité se distinguent considérablement dans les composantes auxquelles ils attribuent une priorité absolue. Cependant, une authentification forte est généralement mise en place en premier pour les identités, et les outils de détection des menaces sont d'une importance indéniable pour l'infrastructure. (Voir l'Annexe 7)

Annexe 6. Mise en œuvre actuelle de la confiance zéro – Domaines de risque en matière de sécurité



Annexe 7. Mise en œuvre de la confiance zéro (3 composantes principales) – Premier rang (mise en œuvre précoce)

Identités	
Authentification efficace (p. ex. : authentification multifacteur ou sans mot de passe)	32 %
Détection et correction automatisées des risques	27 %
Stratégies d'accès adaptatives pour réguler l'accès aux ressources	22 %

Points de terminaison	
Stratégies et contrôles de prévention de la perte de données pour tous les appareils gérés et non gérés	27 %
Évaluation des risques liés aux appareils en temps réel et détection des menaces aux points de terminaison	26 %
Les appareils sont enregistrés auprès d'un fournisseur d'identité	24 %

Applications	
Découverte de l'informatique fantôme et évaluation des risques continues	23 %
Contrôle d'accès granulaire à vos applications (comme une visibilité limitée ou en lecture seule)	22 %
Contrôle de l'accès aux applications basé sur des stratégies	20 %

Réseau	
Contrôles d'accès sécurisés pour protéger les réseaux	25 %
Protection contre les menaces et filtrage à partir de signaux basés sur le contexte	24 %
Tout le trafic est chiffré	20 %

Infrastructure	
Accès aux outils de détection des menaces par l'équipe des opérations de sécurité	25 %
Protection de la charge de travail infonuagique hybride et multinuage	19 %
Visibilité granulaire et contrôle d'accès sur toutes les charges de travail (machines virtuelles, serveurs, etc.)	17 %

Données	
Les décisions en matière d'accès sont régies par le moteur de stratégies de sécurité	21 %
Les données sont classées et étiquetées	21 %
Les fichiers les plus sensibles sont protégés de manière persistante à l'aide du chiffrement	20 %

Automatisation et orchestration	
Une visibilité de bout en bout est établie avec une plateforme centralisée pour les enquêtes et la réponse	29 %
Les données sur les menaces sont recueillies et analysées dans tous les domaines (identités, points de terminaison, applications, réseau, infrastructure)	28 %
L'enquête et la réponse automatisées sont activées	22 %

Nous ne l'avons pas traitée comme une simple série de technologies, mais plutôt comme une stratégie et une approche selon lesquelles chaque ressource utilisateur, que ce soit à l'intérieur de notre réseau ou en dehors de celui-ci, est jugée non fiable jusqu'à ce qu'une vérification soit effectuée. »

Décideurs en matière de sécurité des États-Unis

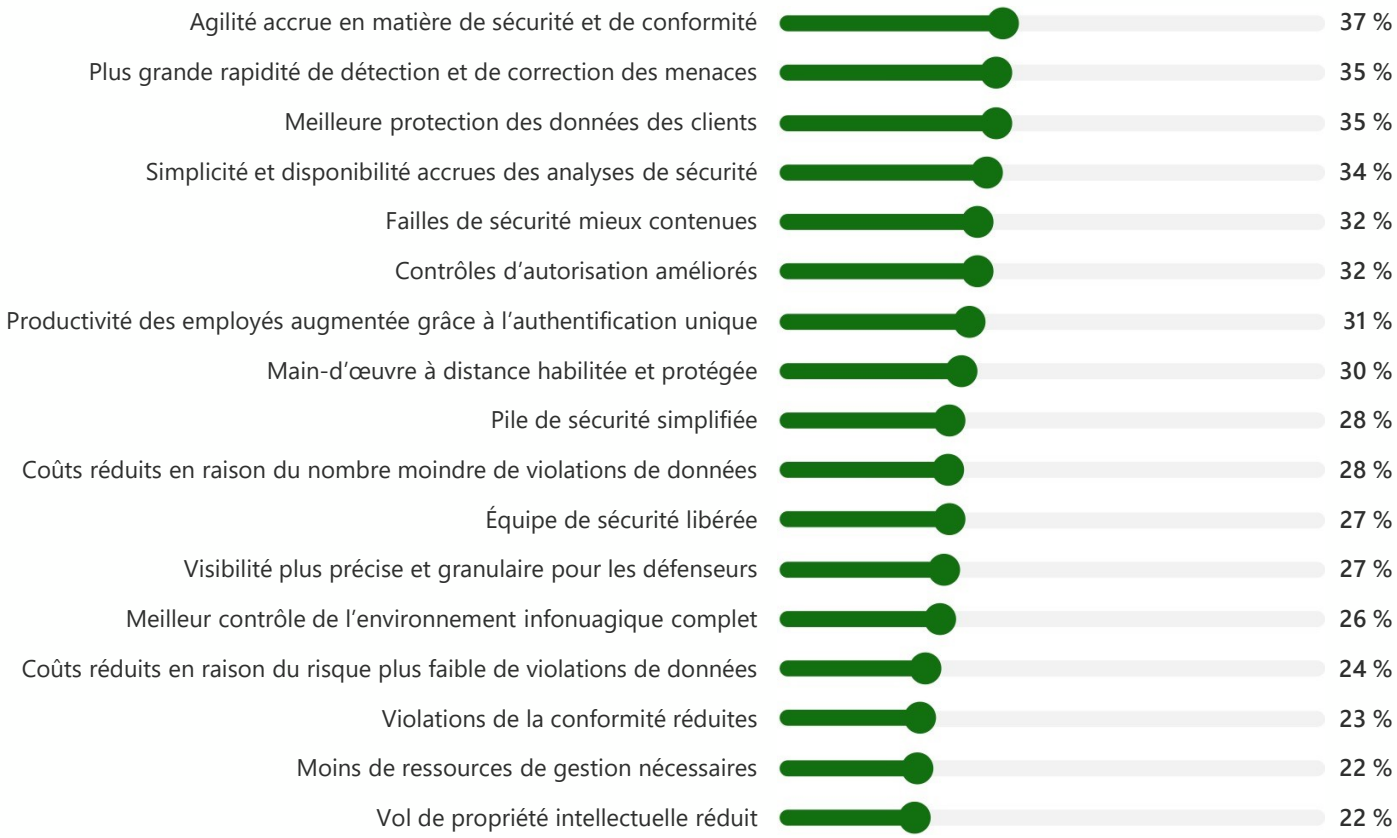
Tourisme d'accueil

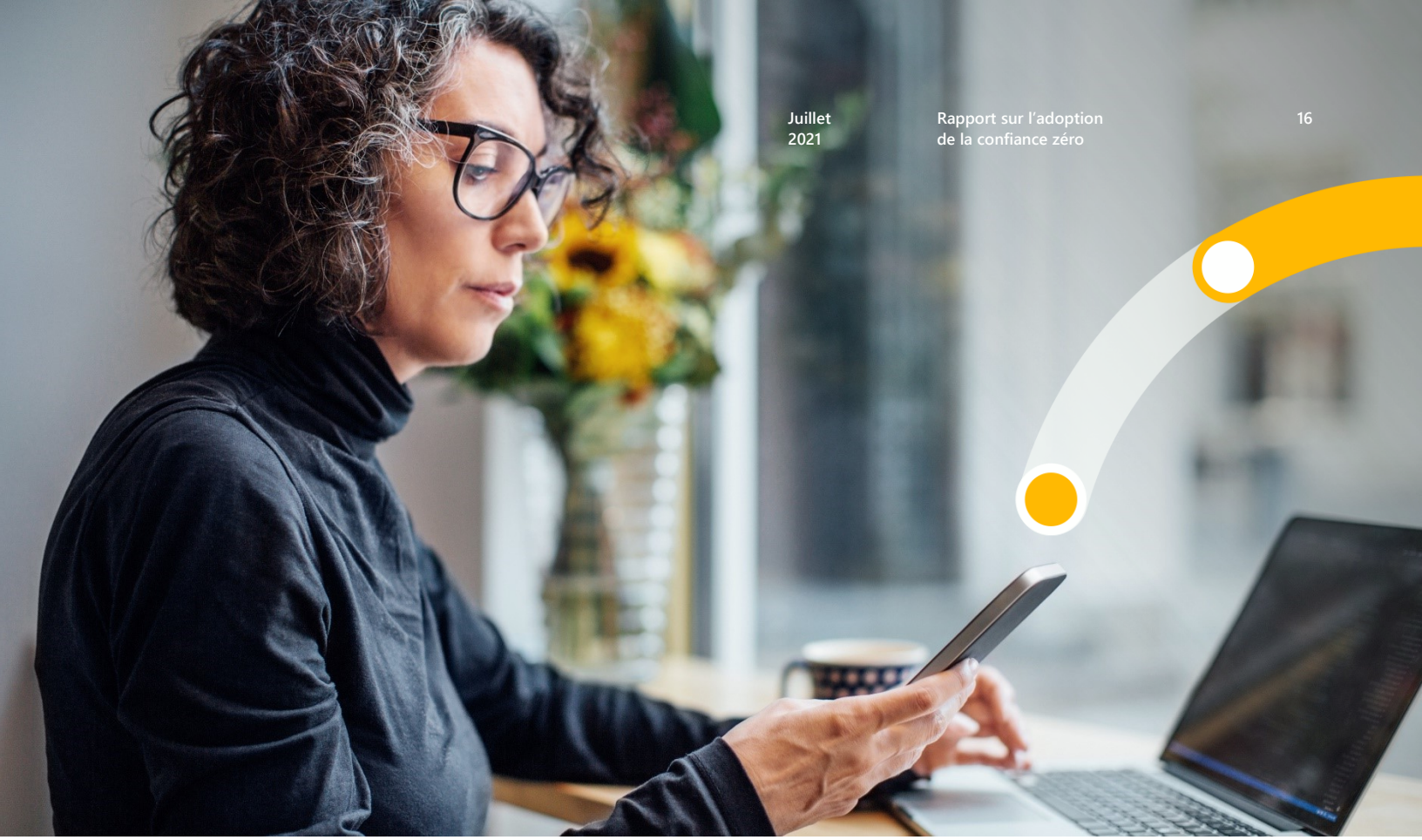
Dès que les entreprises commencent à mettre en œuvre une stratégie de confiance zéro, elles bénéficient de plusieurs avantages, dont les principaux comprennent une agilité, une vitesse et une protection accrues. Les avantages en matière de ressources sont quant à eux moins courants.

Une fois la mise en œuvre terminée, les organisations remarquent une amélioration de l'agilité (37 %), de la vitesse (35 %) et de la protection des données client (35 %). (Voir l'Annexe 8) Cependant, les avantages directs pour les employés comme une équipe de sécurité libérée (27 %) et un besoin de ressources inférieur pour la gestion de l'infrastructure (22 %) sont moins souvent réalisés.

Il est important de noter que les entreprises pensent que leur stratégie de confiance zéro les aidera à gérer la plupart des menaces et des changements qui surviennent dans leur environnement, particulièrement en ce qui concerne la sécurité de l'IdO et des technologies opérationnelles (47 %).

Annexe 8. Avantages de la confiance zéro





Les organisations se sentent capables de tirer le meilleur parti de leur stratégie de confiance zéro

79 % sont confiantes quant à leur capacité à gérer les menaces de sécurité dans leur ensemble, bien que cette confiance diminue lorsque la menace comprend une déformation de la vérité : les SDM se sentent moins en confiance lorsqu'ils sont confrontés à des identités synthétiques (20 %) et à des contrefaçons (10 %).

Compte tenu des avantages obtenus, la confiance zéro favorise généralement des sentiments positifs à son égard. Dans les quatre marchés, les SDM considèrent l'approche de leurs entreprises à la fois pratique et ambitieuse; ils la décrivent comme étant confiante (37 %), efficace (31 %), motivante (25 %), inspirante (25 %) et passionnante (25 %). Au Japon en particulier, les professionnels de la sécurité décrivent la confiance zéro comme étant à la fois exigeante (27 %) et transformationnelle (25 %), ce qui suggère que, bien qu'elle ne soit pas facile à mettre en œuvre, elle présente des avantages importants une fois adoptée.

Plusieurs entreprises pensent qu'elles sont en avance dans leur mise en œuvre de la confiance zéro, mais elles ont encore beaucoup à faire

Bien que seulement 35 % des entreprises aient pleinement mis en œuvre leur stratégie de confiance zéro, 52 % affirment être en avance par rapport à leurs prédictions, tandis que 57 % pensent qu'elles sont en avance sur les autres entreprises. Les entreprises se considèrent particulièrement en avance sur celles qui sont situées au Japon (66 %) et en Australie et Nouvelle-Zélande (63 %). Malgré une confiance débordante dans tous les marchés, il semble exister un gouffre entre la perception et la réalité : parmi les entreprises qui se croient en avance sur les autres, seulement 42 % affirment avoir pleinement mis en œuvre leur stratégie de confiance zéro. (Voir l'Annexe 9)

Même si bon nombre d'entreprises croient en leur stratégie de confiance zéro et se sentent prêtes à gérer les menaces de sécurité futures, elles ont encore beaucoup à accomplir pour la mettre en œuvre complètement dans l'ensemble des domaines de risque. Par exemple, près de la moitié des entreprises qui considèrent que leur stratégie de confiance zéro est entièrement mise en œuvre ne l'ont pas encore déployée dans tous les domaines de risque en matière de sécurité, parmi lesquels l'infrastructure et les identités sont les moins susceptibles d'avoir été abordés.

Annexe 9. Comparaison de la mise en œuvre de la confiance zéro

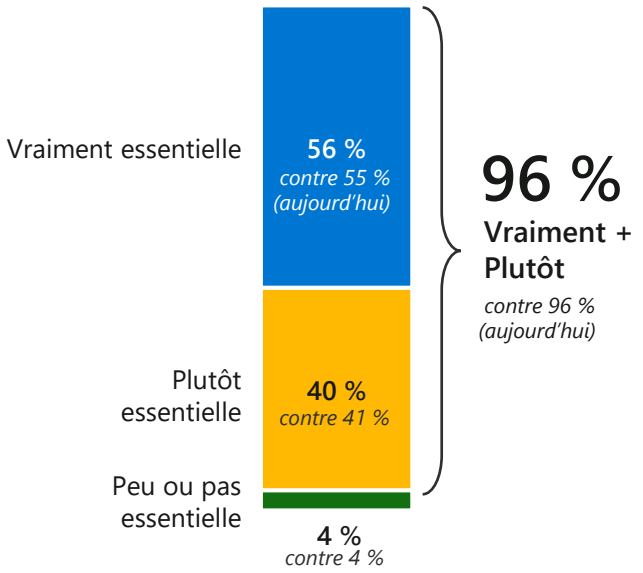
	US	DE	JP	AU/NZ
En avance	59 %	46 %	66 %	63 %
À égalité	40 %	52 %	34 %	32 %
En retard	2 %	2 %	0 %	6 %

Au cours des deux prochaines années, la confiance zéro demeurera une priorité absolue en matière de sécurité

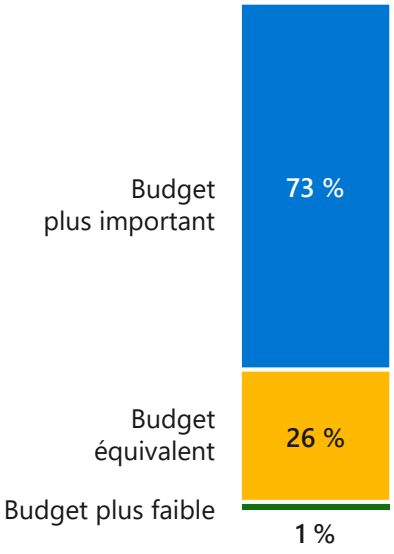
Les entreprises choisissent d'investir dans une stratégie de confiance zéro, et les décideurs affirment que celle-ci continuera d'être une priorité absolue en matière de sécurité au cours des deux prochaines années. L'importance relative de la stratégie de confiance zéro en tant qu'initiative de sécurité devrait augmenter (passant de 53 % à 58 %) d'ici 2023. En effet, les SDM prévoient que cette stratégie demeurera essentielle à la réussite globale de l'entreprise (96 %). (Voir l'Annexe 10)

L'importance anticipée est particulièrement élevée chez les entreprises japonaises; 70 % d'entre elles affirment que la stratégie de confiance zéro sera vraiment essentielle au cours des deux prochaines années, par rapport à une moyenne globale de 56 %. Les fonds dédiés à la confiance zéro devraient également augmenter, avec 73 % des entreprises qui s'attendent à une hausse des budgets. Ce nombre est légèrement inférieur en Allemagne (67 %), où 31 % des répondants prévoient que leurs budgets resteront les mêmes. (Voir l'Annexe 11)

Annexe 10. Importance anticipée de la confiance zéro au cours des deux prochaines années

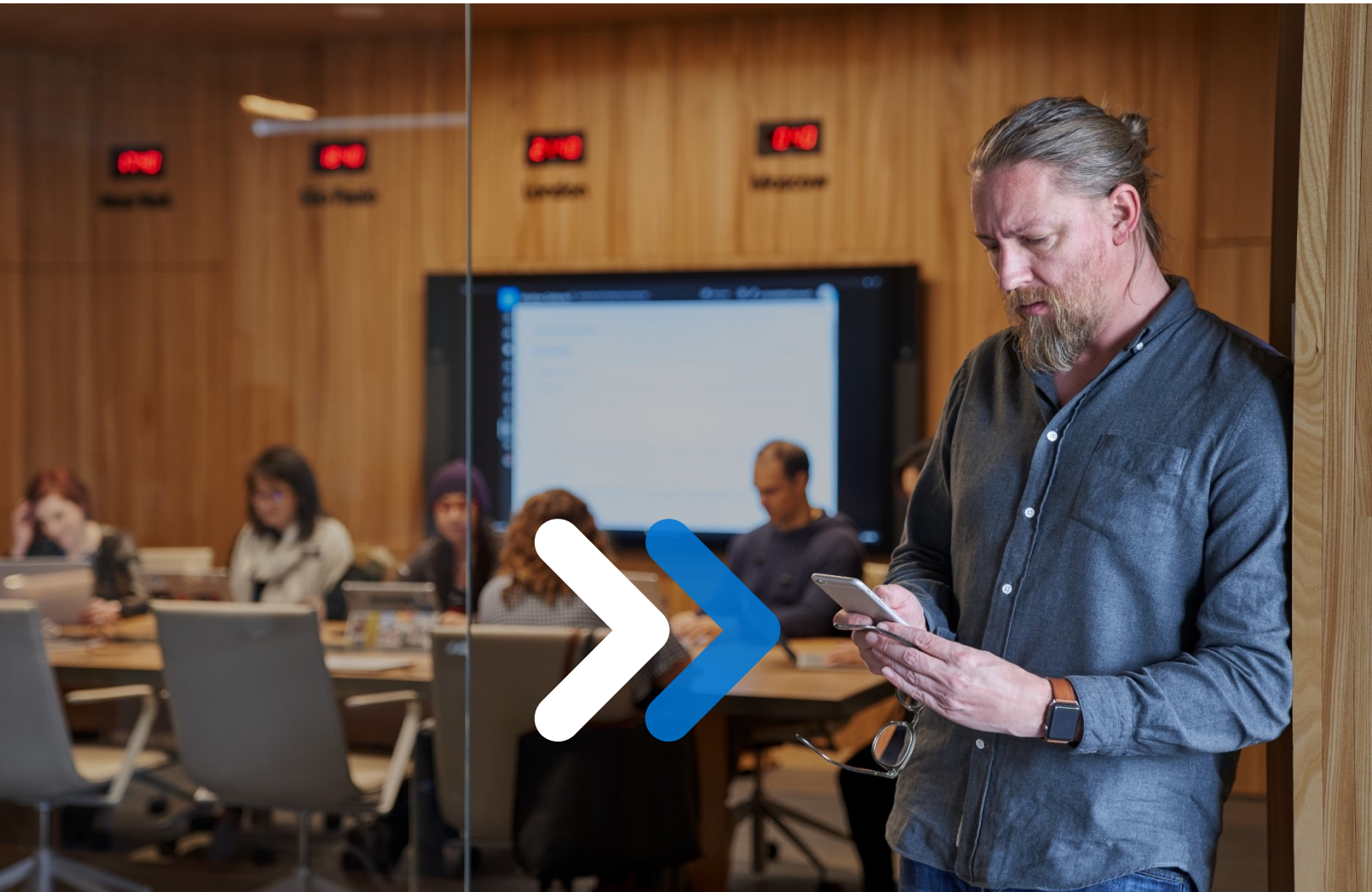


Annexe 11. Budget prévu pour la confiance zéro au cours des deux prochaines années



Démontrer les victoires de la stratégie de confiance zéro pourrait occasionner d'autres investissements

Les entreprises qui ont pleinement adopté la confiance zéro s'attendent à augmenter leurs investissements au cours des deux prochaines années, et celles qui n'ont pas encore commencé leur adoption risquent de prendre encore davantage de retard. Non seulement ces entreprises traînent derrière leurs homologues qui ont terminé la mise en œuvre lorsqu'il est question d'accorder la priorité à la confiance zéro dans leurs plans de sécurité (42 % contre 66 %) et d'anticiper les augmentations budgétaires (66 % contre 72 %), mais elles se sentent également beaucoup moins confiantes quant à la gestion de la sécurité de l'IdO et des technologies opérationnelles dans le futur (40 % contre 53 %).



Il sera essentiel de surmonter les défis relatifs aux employés afin d'accroître l'investissement dans la confiance zéro

Malgré les progrès rapides réalisés dans l'adoption d'une stratégie de confiance zéro, les entreprises doivent surmonter une myriade de défis si elles veulent progresser davantage dans leur mise en œuvre. (Voir l'Annexe 12) Les défis en matière de ressources et de leadership sont les plus courants dans ces catégories. En tête de liste des obstacles figurent le délai de mise en œuvre des stratégies de confiance zéro et le manque de soutien de la part de la haute direction, ce dernier étant particulièrement important en Australie et en Nouvelle-Zélande (65 %).

De plus, les contraintes budgétaires, que 45 % des entreprises définissent comme étant un obstacle, entrent probablement aussi en compte dans les défis en matière de ressources et de leadership.

Par exemple, 21 % des SDM affirment qu'une difficulté à démontrer le rendement du capital investi d'un investissement dans la confiance zéro est un obstacle à la mise en œuvre, défi qui peut conduire à un manque d'adhésion de la part de la direction. Comme les marchés à l'extérieur des États-Unis sont plus susceptibles d'avoir des contraintes budgétaires (60 % des entreprises au Japon; 57 % des entreprises en Allemagne; 57 % des entreprises en Australie et Nouvelle-Zélande), il est possible que cela ait un effet d'entraînement, conduisant à une mise en œuvre des stratégies de confiance zéro au Japon, en Allemagne et en Australie et Nouvelle-Zélande plus faible et plus lente qu'aux États-Unis.

Annexe 12. Obstacles de la confiance zéro

Défis en matière de ressources 60 %	Leadership 53 %	Technologie 46 %	Fournisseurs 46 %	Contraintes budgétaires 45 %
20 % Délai de mise en œuvre trop long	**20** % Manque de soutien de la part de l'équipe élargie de la haute direction	**21** % Difficulté à intégrer des solutions de sécurité	**21** % Besoin de soutien de la part des fournisseurs pour la mise en œuvre	**21** % Coût de la mise en œuvre d'une stratégie de confiance zéro
19 % Manque de gestion interne du changement	**19** % Manque de soutien de la part des intervenants	**19** % Incompatibilité avec les systèmes existants	**21** % Difficulté à trouver les bons fournisseurs	**21** % Difficulté à démontrer le rendement du capital investi
18 % Matériel éducatif insuffisant	**19** % Besoin d'aide pour mettre en place une analyse de rentabilité convaincante	**19** % Difficulté à évoluer à l'échelle de l'organisation	**17** % Incapacité à trouver des partenaires innovants	**14** % Budget insuffisant
17 % Pas nécessaire étant donné la taille de l'entreprise	**18** % Adhésion insuffisante au sein de l'entreprise			
16 % Manque de talents pour effectuer une mise en œuvre adéquate				

« L'adhésion fut difficile au début, mais une fois que nous nous sommes mis d'accord en tant qu'intervenants, tous les autres ont suivi. »

Décideurs en matière de sécurité des États-Unis

Technologies financières

Les décideurs en matière de sécurité ont une légère propension pour les fournisseurs holistiques ou consolidés

Pour ce qui est de la stratégie de confiance zéro des fournisseurs, les entreprises sont confrontées à une approche de type « best-in-suite » ou « best-in-breed ». La première stratégie consiste à acheter une suite de produits pour l'ensemble de l'architecture de confiance zéro auprès d'un fournisseur holistique ou consolidé, une solution qui, selon les SDM, offre plus d'expertise, de ressources et de simplicité pour les entreprises qui manquent de ressources à l'interne. Toutefois, cette approche présente des risques de vulnérabilité accrue et un manque de souplesse. (Voir l'Annexe 13)

Cette dernière stratégie, soit « best-in-breed », consiste à obtenir des composantes individuelles en technologie de confiance zéro auprès de fournisseurs spécialisés. Contrairement à l'approche « best-in-suite », cette stratégie s'appuie sur des fournisseurs qui sont des experts dans différents domaines; elle offre ainsi une souplesse accrue et permet de se conformer plus étroitement à la stratégie de l'entreprise. Cela étant dit, les professionnels de la sécurité considèrent que cette stratégie est plus coûteuse, qu'elle nécessite plus de ressources et qu' elle nuit à la visibilité, des inconvénients qui mènent au bout du compte à des difficultés en matière de fournisseurs et de budgets. (Voir l'Annexe 14)

Bien que les entreprises soient largement divisées, une légère majorité des SDM (55 %) préfèrent travailler avec des fournisseurs holistiques (« best-in-suite »). (Les entreprises en Australie et Nouvelle-Zélande penchent cependant dans la direction opposée, avec 52 % d'entre eux qui préfèrent des fournisseurs spécialisés [« best-in-breed »].)

Annexe 13. Avantages et obstacles de l'approche « best-in-suite » – Deuxième rang

⊕ Avantages de l'approche « best-in-suite »	
Le fournisseur possède une expertise propre au secteur dans toutes les solutions	24 %
Plus de ressources disponibles pour aider à planifier la stratégie de confiance zéro	23 %
Pile de sécurité simplifiée	22 %

⊖ Inconvénients de l'approche « best-in-suite »	
Recours à un seul fournisseur, ce qui augmente la vulnérabilité	34 %
Intégration plus complexe nécessaire avec une architecture existante	33 %
Moins de souplesse pour un fonctionnement spécialisé	29 %

Annexe 14. Avantages et obstacles de l'approche « best-in-breed » – Deuxième rang

⊕ Avantages de l'approche « best-in-breed »	
Liberté de rechercher les meilleures solutions pour n'importe quelle composante de la stratégie de confiance zéro	33 %
Capacité d'adapter plus étroitement la solution à l'architecture ou à la stratégie de son entreprise	30 %
Possibilités accrues d'innovation avec divers fournisseurs	26 %

⊖ Inconvénients de l'approche « best-in-breed »	
Coûts plus élevés	29 %
Incapacité à partager des données entre différentes solutions	26 %
Volume élevé de solutions à adopter et à gérer pour les équipes internes	26 %

Réflexions finales

Tandis que les risques de sécurité deviennent non seulement plus nombreux, mais aussi plus néfastes, les entreprises de tous les marchés et tous les secteurs optent pour une stratégie de confiance zéro qui nous recommande de « ne jamais faire confiance, toujours vérifier ». La stratégie de confiance zéro est la priorité absolue en matière de sécurité pour les entreprises qui visent à améliorer l'état global de leur sécurité, leur expérience utilisateur et leur productivité, à simplifier les procédures de sécurité pour les employés et à réduire les coûts. Cependant, bien que les avantages d'une stratégie de confiance zéro soient bien établis, les ressources limitées et le scepticisme des dirigeants font obstacle à sa mise en œuvre universelle.

L'adoption d'une stratégie de confiance zéro s'est accélérée au cours des trois dernières années, en partie en raison de la pandémie de COVID-19. Fondamentalement, le passage aux milieux de travail distants et hybrides stimule une adoption plus large des approches de confiance zéro, qui promettent de protéger les systèmes et les données même lorsque les employés y accèdent depuis l'extérieur du réseau d'entreprise, parfois sur des appareils personnels. Une adoption accélérée par la COVID est un bon indicateur de la préparation à la confiance zéro dans son ensemble. En effet, les entreprises qui ont adopté la stratégie durant la pandémie ont mis en œuvre plus de domaines de risque en matière de sécurité que leurs homologues.

Cela étant dit, même les utilisateurs les plus avancés de la confiance zéro ont encore du travail à faire. Par ailleurs, les perceptions erronées des entreprises concernant leur propre maturité de confiance zéro peut faire en sorte qu'elles négligent certaines vulnérabilités qu'elles n'ont pas conscience d'avoir.

Une majorité d'entreprises sur tous les marchés croient que l'importance d'adopter une stratégie de confiance zéro ne fera que croître avec le temps, et s'attendent à ce que leurs budgets augmentent par le fait même. Ce changement anticipé de priorités est particulièrement crucial dans les marchés en dehors des États-Unis, où les préoccupations budgétaires sont les principaux obstacles à l'adoption. La recherche d'une mise en œuvre complète peut être accablante sur le plan financier et logistique. Néanmoins, les avantages d'une approche de confiance zéro sont indéniables, et Microsoft s'engage à être là pour guider et soutenir les entreprises qui mettent le cap sur ce marché florissant.

Pour soumettre votre entreprise à une évaluation de la maturité en matière de confiance zéro et en savoir plus à ce sujet, consultez le site

aka.ms/zerotrust

Détails sur les objectifs de recherche et l'échantillon

Les objectifs de la recherche étaient les suivants :

Comprendre l'état actuel des approches de confiance zéro

Découvrir les mentalités, les pratiques exemplaires, les avantages et les défis de l'adoption des approches de confiance zéro

Explorer l'avenir des approches de confiance zéro

Contextualiser les innovations et les tendances dans les approches de confiance zéro

Aux fins de sélection, les décideurs en matière de sécurité devaient répondre aux critères suivants :

Responsable de la sécurité dans leur entreprise, notamment la cybersécurité, les opérations de sécurité, la protection contre les menaces, la gestion des identités, la gestion des risques, la sécurité des applications, les analyses numériques et la réponse aux incidents

Employé à temps plein dans une société de calibre entreprise (plus de 1 000 employés aux États-Unis; plus de 500 employés en Allemagne, au Japon, en Australie ou en Nouvelle-Zélande)

Âgé de 25 à 75 ans

Familiers avec la confiance zéro

Participe à la prise de décision pour l'élaboration et la mise en œuvre de la stratégie de confiance zéro

Parmi les 911 décideurs en matière de sécurité sondés dans le cadre de la vague de recherche d'avril 2021 :

Aux États-Unis, 477 SDM ont été interrogés

En Allemagne, 201 SDM ont été interrogés

En Australie et Nouvelle-Zélande, 126 SDM ont été interrogés

Au Japon, 107 SDM ont été interrogés

Remarque : La recherche a été menée pendant la pandémie mondiale de COVID-19, qui en était à divers niveaux de gravité ou de confinement

Microsoft Security hypothesis