Microsoft Security

hypothesis

Rapport sur l'adoption de la Confiance Zéro

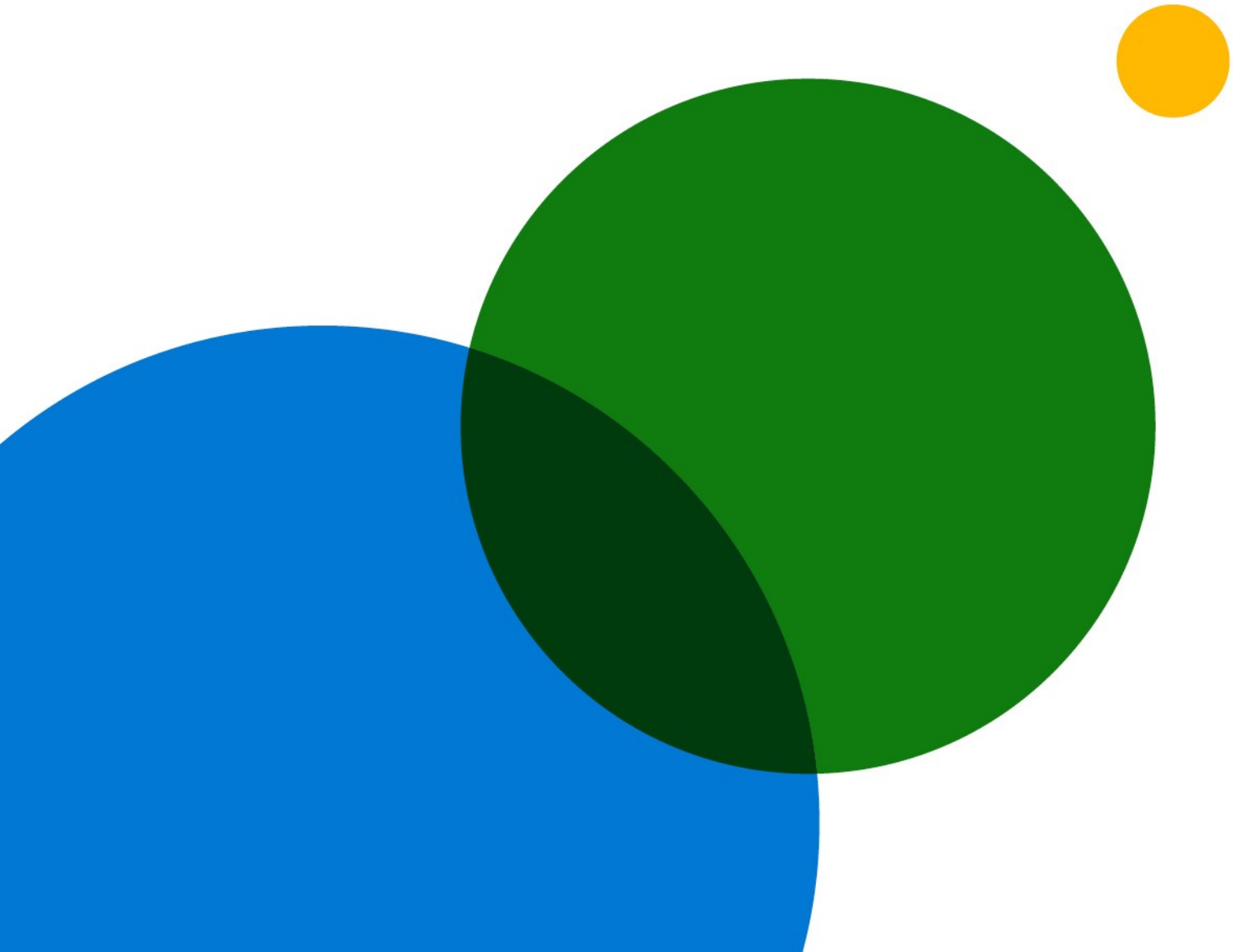


Table des matières

Introduction

Vasu Jakkal/Vice-président de la sécurité, de la conformité et de l'identité

L'année qui vient de s'écouler a été remarquable au niveau de l'évolution de la cybersécurité et de l'essor de la Confiance Zéro en tant que stratégie de guidage pour notre secteur et nos entreprises dans le monde entier.

Au début de la pandémie, le télétravail est devenu la norme pratiquement du jour au lendemain. Ce changement a contraint de nombreuses entreprises à s'adapter rapidement pour aider les employés qui devaient absolument travailler, à utiliser des appareils personnels, à collaborer via des services Cloud et à partager des données en dehors du périmètre du réseau de l'entreprise. À mesure que les entreprises s'adaptaient à cette transformation, elles étaient également confrontées à des cybercriminels de plus en plus sophistiqués qui évoluent continuellement dans leur ciblage, leurs tactiques et leurs ressources.

Aujourd'hui, le travail hybride est la nouvelle réalité. Dans ce contexte, et face à un changement rapide, les entreprises que nous avons interrogées nous ont dit qu'elles s'appuient sur la stratégie Confiance Zéro pour augmenter l'agilité en matière de sécurité et de conformité, accélérer la détection des menaces et la correction, et augmenter la simplicité et la disponibilité des analyses de sécurité.

En se basant sur les principes de la vérification explicite, de l'utilisation de l'accès le moins privilégié et des failles potentielles, une architecture de type Confiance Zéro complète crée des mesures de protection au sein et à travers les identités, les points de terminaison, les applications, l'infrastructure, le réseau et les données, tout cela associé avec une visibilité accrue, une automatisation et une orchestration. Non seulement nous recommandons cette approche à nos clients et à nos partenaires, mais ici chez Microsoft, nous l'adoptons aussi dans notre approche de la sécurité globale et du développement de logiciels.

Ce rapport illustre le parcours de l'adoption de la Confiance Zéro sur différents marchés et secteurs d'activité. Nous espérons que les enseignements tirés de cette étude peuvent vous aider à accélérer votre propre adoption de la stratégie Confiance Zéro, à faciliter la progression collective de vos pairs et à fournir des informations sur l'état futur de ce domaine en constante évolution.

Méthodologie

Microsoft a chargé Hypothesis Group, une agence d'étude, de conception et de stratégie, d'exécuter cette recherche et ce rapport sur l'adoption de la Confiance Zéro. L'étude s'est déroulée en deux phases : aux États-Unis tout d'abord, pour mettre en évidence les tendances et le dynamisme de l'adoption de la Confiance Zéro, puis dans une deuxième phase, au niveau mondial, pour mettre en évidence les marchés supplémentaires afin de découvrir les tendances.

La recherche initiale a eu lieu en août 2020. Une enquête en ligne de 15 minutes a ainsi été menée aux États-Unis auprès de 300 décisionnaires de sécurité impliqués dans des décisions stratégiques concernant la stratégie Confiance Zéro dans des entreprises de différents secteurs. En plus de l'enquête en ligne, cinq entretiens approfondis ont été menés en ligne en septembre 2020 auprès de décisionnaires des États-Unis dans un large éventail de secteurs.

En avril 2021, une recherche mondiale a été réalisée aux États-Unis, en Allemagne, au Japon et en Australie/Nouvelle-Zélande à travers un groupe similaire de décisionnaires de sécurité. Plus de 900 participants ont participé à une enquête en ligne de 15 minutes comportant des questions sur leur adoption de la stratégie Confiance Zéro, les meilleures pratiques, les avantages, les défis et la façon dont ils envisagent d'investir à l'avenir.

Choses à savoir sur l'adoption de la Confiance Zéro

01/ Les entreprises sont prêtes à tirer parti de la stratégie Confiance Zéro, accélérée par le passage à un environnement de travail hybride et l'épidémie de COVID-19

Les décisionnaires de sécurité affirment que le développement d'une stratégie Confiance Zéro est leur priorité numéro 1 en matière de sécurité, et 96 % d'entre eux indiquent qu'elle est essentielle au succès de leur entreprise. Les principaux facteurs motivant l'adoption d'une stratégie Confiance Zéro sont l'amélioration de leur niveau de sécurité global et de l'expérience de l'utilisateur final. La transition vers un environnement de travail hybride, accélérée par l'épidémie de COVID-19, favorise également l'adoption d'une stratégie Confiance Zéro : 81 % des entreprises ont commencé à migrer vers un environnement de travail hybride, et 31 % ont complètement migré. Toutefois, 94 % sont préoccupées par la transition. Ces préoccupations concernent principalement les usages abusifs de la part des employés, l'augmentation des charges de travail informatiques et les cyberattaques. Ceci étant dit, les principales considérations relatives à une stratégie incluent une formation accrue pour les collaborateurs et l'authentification multifacteur (MFA) pour garantir une expérience utilisateur et une transition fluides.

02 / Une stratégie Confiance Zéro offre de la flexibilité aux entreprises qui peuvent ainsi commencer à la mettre en œuvre afin que l'approche puisse être adaptée à leurs besoins

Moins de 15 % des entreprises ont commencé à mettre en œuvre une stratégie Confiance Zéro dans la même zone de risque de sécurité. Cela est dû en grande partie au fait que la mise en œuvre est abordée comme un processus end-to-end entre les piliers et les capacités de l'architecture de sécurité plutôt que comme une série de technologies individuelles disparates. De même, l'ordre dans lequel les composants individuels de la stratégie Confiance Zéro au sein d'une zone présentant un risque de sécurité sont mis en œuvre est très variable. En effet, les professionnels de la sécurité diffèrent sensiblement dans la manière dont ils commencent à mettre en œuvre les composants.

03 / Bien que la stratégie Confiance Zéro soit largement adoptée et améliore la capacité des entreprises à gérer les menaces, il reste encore du travail à faire

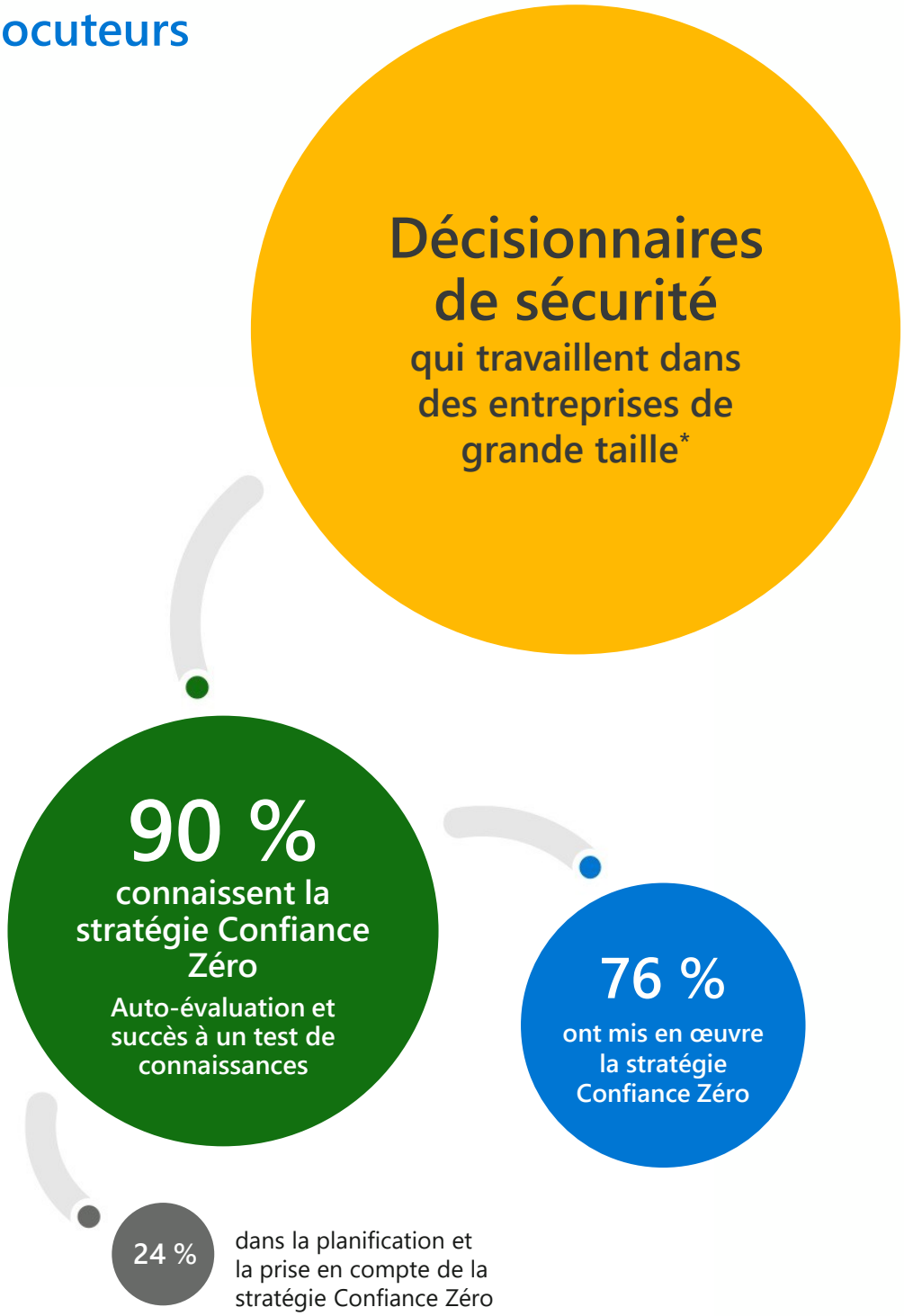
76 % des entreprises ont au moins commencé à mettre en œuvre une stratégie Confiance Zéro, et 35 % prétendant avoir complètement terminé. Toutefois, celles qui prétendent avoir complètement terminé admettent qu'elles n'ont pas fini la mise en œuvre de la stratégie Confiance Zéro dans tous les domaines et composants de risque de sécurité. La stratégie Confiance Zéro est convaincante parce qu'elle offre une agilité accrue, une rapidité de détection des menaces et une meilleure capacité de gestion de la sécurité de l'Internet des objets (IoT) et de la technologie opérationnelle (OT). L'adoption est en croissance aux États-Unis (70 % en août 2020 à 79 % en avril 2021). Les États-Unis sont également plus en avance sur la mise en œuvre du modèle Confiance Zéro par rapport aux autres pays qui ont commencé à l'adopter plus tard, et les entreprises aux États-Unis prétendent être moins contraintes par les budgets. Toutefois, bien que 57 % des entreprises prétendent être en avance sur les autres en matière d'adoption, environ la moitié ont encore plus de travail à faire, car elles n'ont pas entièrement mis en œuvre le modèle Confiance Zéro dans tous les domaines et composants présentant un risque de sécurité.

04 / À l'avenir, la stratégie Confiance Zéro restera une priorité absolue et nécessitera une prise de décision réfléchie concernant les collaborateurs et les fournisseurs

La stratégie Confiance Zéro devrait demeurer la priorité numéro 1 en matière de sécurité dans deux ans et les entreprises anticipent l'augmentation de leur investissement. Il sera essentiel de surmonter les défis avec les collaborateurs (y compris doter les équipes de sécurité en personnel et obtenir l'adhésion de l'équipe dirigeante) pour doubler les investissements dans la stratégie Confiance Zéro. En ce qui concerne la stratégie des fournisseurs, les décisionnaires de sécurité ont une légère préférence pour travailler avec des fournisseurs globaux. En effet, la sélection des fournisseurs est souvent tributaire de la disponibilité de l'expertise interne. Les avantages de ce type d'approche incluent une expertise, des ressources et une simplicité accrues, bien que cela puisse prendre plus de temps à mettre en œuvre, être plus difficile à intégrer à l'architecture de sécurité existante et augmenter la vulnérabilité potentielle.

Nos interlocuteurs

Mondial



*plus de 1 000 collaborateurs aux États-Unis ; plus de 500 collaborateurs en Allemagne, au Japon, en Australie/Nouvelle-Zélande

Enseigne-ments tirés

Les entreprises sont prêtes à tirer parti de la stratégie Confiance Zéro

La stratégie Confiance Zéro est actuellement la priorité numéro 1 en matière de sécurité sur l'ensemble des marchés et des secteurs, et un certain nombre d'entreprises l'ont adoptée au cours de ces dernières années. La stratégie Confiance Zéro est importante pour beaucoup (53 %), il s'agit d'une priorité particulièrement élevée pour les entreprises situées aux États-Unis (56 %) et en Allemagne (53 %).

Presque tous les professionnels de la sécurité (96 %) estiment qu'une stratégie Confiance Zéro est essentielle au succès de leur entreprise. (Voir Figure 1) En plus de renforcer leur niveau de sécurité global et d'améliorer l'expérience des utilisateurs finaux, les professionnels de la sécurité recherchent une stratégie Confiance Zéro pour simplifier les procédures de sécurité pour les collaborateurs. (Voir Figure 2)

Comme l'explique un décisionnaire des États-Unis dans le domaine de l'hôtellerie, *« L'objectif est d'améliorer globalement la sécurité, mais il s'agit de réduire les frictions dans l'expérience des utilisateurs et de leur faciliter la vie. »*

En outre, 31 % des professionnels de la sécurité considèrent que la stratégie Confiance Zéro est un outil important dans la transition imminente vers un environnement de travail hybride post-pandémie ; ce facteur est particulièrement pertinent en Australie/Nouvelle-Zélande (44 %).

Figure 1. Une stratégie Confiance Zéro est importante

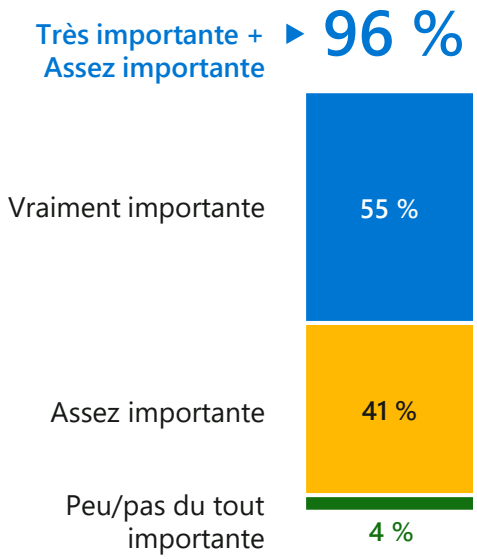


Figure 2. Facteurs de motivation pour la stratégie Confiance Zéro

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

Le passage à un environnement de travail hybride favorise l'adoption d'une stratégie Confiance Zéro

81 % des entreprises ont commencé à migrer vers un environnement de travail hybride, et 31 % ont déjà complètement terminé. Ceci dit, les taux d'adoption diffèrent selon les marchés : l'Australie et la Nouvelle-Zélande arrivent en tête avec 37 %, l'Allemagne est loin derrière, avec seulement 20 % des entreprises qui ont déjà adopté un modèle hybride. (Voir la Figure 3.)

Même si les marchés mondiaux évoluent vers un environnement de travail hybride à des taux disparates, la grande majorité des entreprises (91 %) qui n'ont pas terminé la transition prévoient de le faire au cours des cinq prochaines années. 94 % des entreprises sont préoccupées par la transition. Les usages abusifs de la part des employés, l'augmentation des charges de travail IT et le risque accru de cyberattaques arrivent en tête de la liste des préoccupations. (Voir la Figure 4.)

Figure 3. Intentions en matière d'environnement de travail hybride

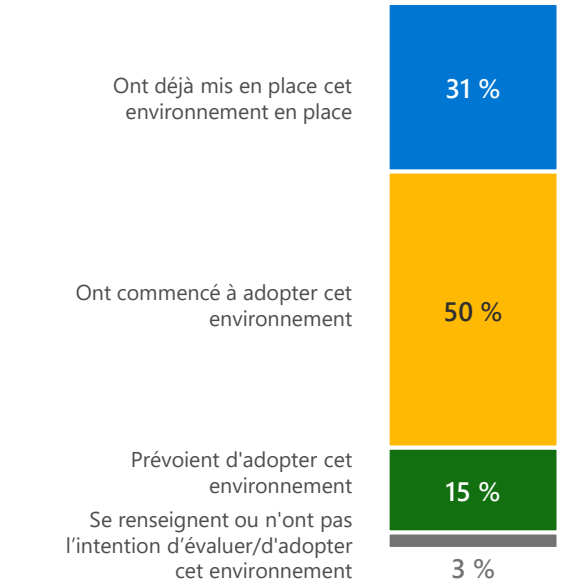
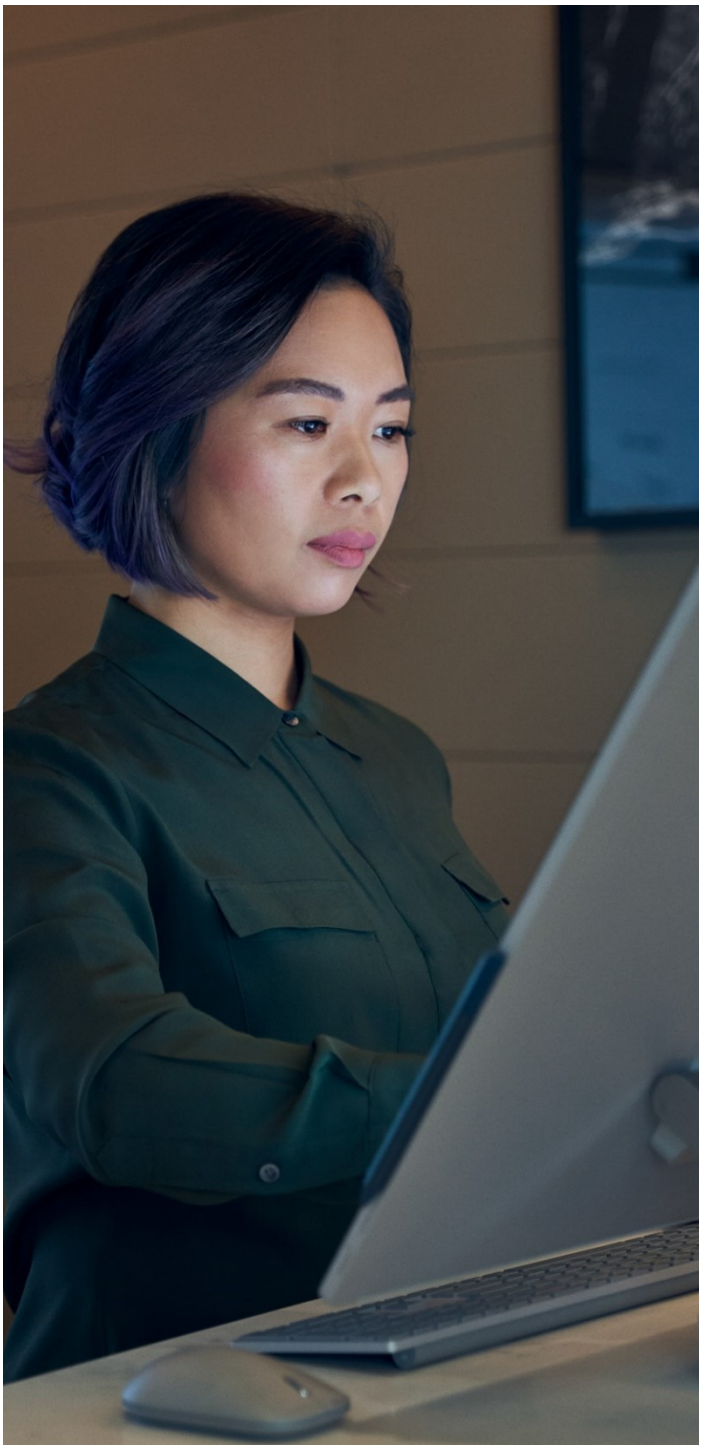


Figure 4. Préoccupations en matière d'environnement de travail hybride

Téléchargement d'applications non sécurisées par les employés	37 %
Augmentation de la charge de travail informatique	37 %
Attaques de ransomware	36 %
Attaques de hameçonnage	35 %
Utilisation incorrecte des appareils personnels	34 %
Accès non autorisé aux données	31 %
Incapacité à gérer tous les appareils	30 %
Utilisation de comptes de messagerie personnels	30 %
Non-conformité aux réglementations relatives aux données	24 %

De nouvelles problématiques sont apparues avec l'épidémie de Covid-19 et ont accéléré la transition vers la stratégie Confiance Zéro



Dans le but de minimiser les problèmes potentiels, les parties prenantes soulignent l'importance d'une formation accrue pour les collaborateurs (54 %) (en particulier au Japon (61 %) et en Allemagne (58 %)) et de l'authentification multifacteur (AMF) (50 %) (en particulier aux États-Unis (52 %) et en Allemagne (56 %)) pour garantir une expérience utilisateur et une transition fluides.

Comme le travail hybride et à distance sécurisé peut être facilité par une stratégie Confiance Zéro, le COVID-19 a accéléré l'adoption d'une telle stratégie pour 72 % des entreprises, même si des différences émergent entre les marchés. Bien que la pandémie ait catalysé l'adoption d'environ sept entreprises sur dix aux États-Unis (76 %), au Japon (71 %) et en Australie/Nouvelle-Zélande (69 %), les taux de mise en œuvre ont été notablement inférieurs en Allemagne (62 %), peut-être en raison d'une transition plus lente vers un environnement de travail hybride.

La stratégie Confiance Zéro est largement mise en œuvre dans le monde entier et se développe aux États-Unis

La stratégie Confiance Zéro n'est pas seulement un mot à la mode ; c'est une réalité. 76 % des entreprises ont au moins commencé à mettre en œuvre cette stratégie et 35 % estiment avoir complètement terminé. Toutefois, ces données dépeignent une image trop optimiste, car de nombreuses entreprises qui considèrent avoir complètement terminé la mise en œuvre n'ont pas, de leur propre aveu, terminé l'exécution dans tous les domaines présentant un risque de sécurité. Aujourd'hui, les États-Unis sont en avance en matière d'adoption de la stratégie Confiance Zéro comparé aux autres marchés et continuent de croître rapidement : par rapport au mois d'août 2020, la mise en œuvre de la stratégie Confiance Zéro aux États-Unis est passée de 70 à 79 %, ce qui représente une montée en flèche en seulement huit mois.
(Voir la Figure 5.)

Bien que la stratégie Confiance Zéro prédomine actuellement dans l'espace de sécurité, son omniprésence est relativement nouvelle. 82 % des entreprises ont mis en œuvre des stratégies Confiance Zéro au cours des trois dernières années, dont 21 % au cours des 12 derniers mois. Cela dit, 26 % des entreprises américaines ont commencé cette mise en œuvre il y a 3 ans, contre 19 % des entreprises japonaises, 6 % des entreprises en Australie/Nouvelle-Zélande et 3 % des entreprises en Allemagne. Cette mise en œuvre précédente aux États-Unis (associée à moins de contraintes budgétaires) peut permettre d'expliquer pourquoi les entreprises là-bas sont en avance dans l'adoption de la stratégie Confiance Zéro par rapport aux entreprises sur d'autres marchés. Dans le même ordre d'idées, la relative émergence de la stratégie Confiance Zéro en Allemagne contribue à la mise en contexte de ses taux d'adoption inférieurs : 97 % des entreprises allemandes ont seulement commencé la mise en œuvre ces trois dernières années.

Figure 5. Mise en œuvre de la stratégie Confiance Zéro

	États-Unis (2020)	États-Unis	Allemagne	Japon	Australie/Nouvelle Zélande
Mise en œuvre de la stratégie Confiance Zéro	70 %	79 %	75 %	76 %	71 %
• Entièrement mise en œuvre	27 %	44 %	19 %	32 %	28 %
• En cours	43 %	35 %	56 %	44 %	43 %

35 % Entièrement mise en œuvre

42 % Mise en œuvre en cours

Il n'existe pas d'approche unique pour la mise en œuvre de la stratégie Confiance Zéro, ce qui permet de commencer n'importe où

Aucun domaine présentant un risque de sécurité particulier (identités, points de terminaison, applications, réseau, infrastructure, données, automatisation et orchestration) ne constitue le point de départ principal de la stratégie Confiance Zéro. En effet, moins de 15 % des entreprises commencent par le même domaine présentant un risque de sécurité. Les entreprises commencent à différents endroits, en fonction de leurs besoins et des ressources internes disponibles. Elles cherchent au final à adopter une stratégie Confiance Zéro dans tous les domaines présentant un risque de sécurité afin de garantir une protection encore plus grande contre les menaces. Ainsi, la confiance zéro est perçue comme une stratégie de bout en bout qui se déroule au fil du temps. (Voir Figure 6)

Outre les domaines présentant un risque de sécurité, les entreprises doivent aussi identifier, dans chacun de ces domaines, les composants individuels à prioriser. Pour les points de terminaison, les applications, le réseau, les données et l'automatisation/l'orchestration, il n'y a pas de point de départ clair ; les professionnels de la sécurité ne classent pas du tout les mêmes composants comme leur priorité absolue. Toutefois, l'authentification forte est généralement mise en œuvre en premier lieu pour les identités, et les outils de détection des menaces sont une priorité claire au sein de l'infrastructure. (Voir Figure 7)

Figure 6. Mise en œuvre actuelle de la stratégie Confiance Zéro – Domaines présentant un risque de sécurité

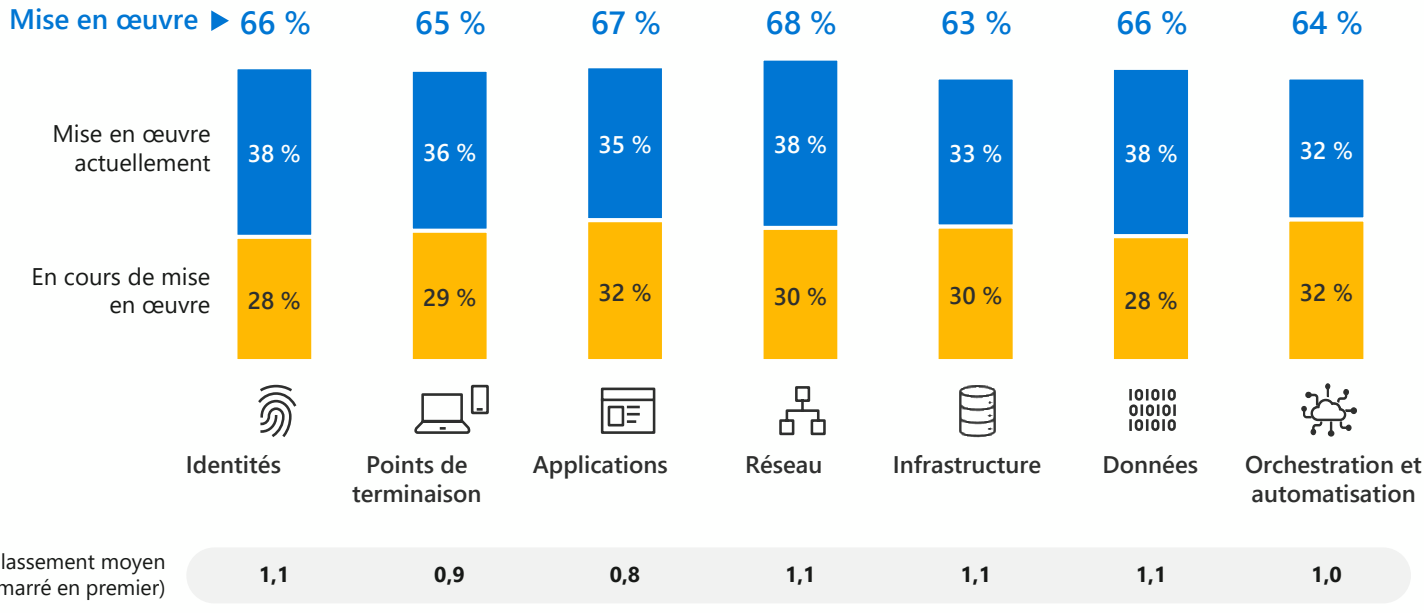


Figure 7. Mise en œuvre du composant Confiance Zéro (Top 3) - Points considérés comme prioritaires (mis en œuvre en premier)

Identités	
Authentification forte (c.-à-d. authentification multifacteur, authentification sans mot de passe)	32 %
Détection et résolution automatisées des risques	27 %
Stratégies d'accès adaptatives pour donner accès aux ressources	22 %

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

Applications	
Découverte continue de l'informatique fantôme et évaluation des risques	23 %
Contrôle d'accès granulaire à vos applications (par exemple, visibilité limitée ou lecture seule)	22 %
Contrôle d'accès basé sur les stratégies pour les applications	20 %

Réseau	
Contrôles d'accès sécurisés pour protéger les réseaux	25 %
Protection contre les menaces et filtrage avec des signaux basés sur le contexte	24 %
Chiffrage de tout le trafic	20 %

Infrastructure	
Accès aux outils de détection des menaces par l'équipe chargée des opérations de sécurité	25 %
Protection de la charge de travail dans le Cloud sur plusieurs Clouds hybrides	19 %
Visibilité et contrôle d'accès granulaires sur toutes les charges de travail (machines virtuelles, serveurs, etc.)	17 %

Données	
Décisions d'accès régies par le moteur de stratégie de sécurité	21 %
Classement et étiquetage des données	21 %
Protection constante des fichiers les plus sensibles par le chiffrement	20 %

Orchestration et automatisation	
Visibilité de bout en bout avec une plateforme centralisée d'investigation et de réponse	29 %
Collecte et analyse des données concernant les menaces dans différents domaines (identités, points de terminaison, applications, réseau, infrastructure)	28 %
Investigation et réponse automatisées activées	22 %

Nous n'avons pas considéré cette stratégie comme une simple série de technologies, mais comme une approche pour traiter chaque ressource utilisateur, que ce soit au sein de notre réseau ou à l'extérieur de notre réseau, comme non fiable jusqu'à ce qu'elle puisse être vérifiée. »

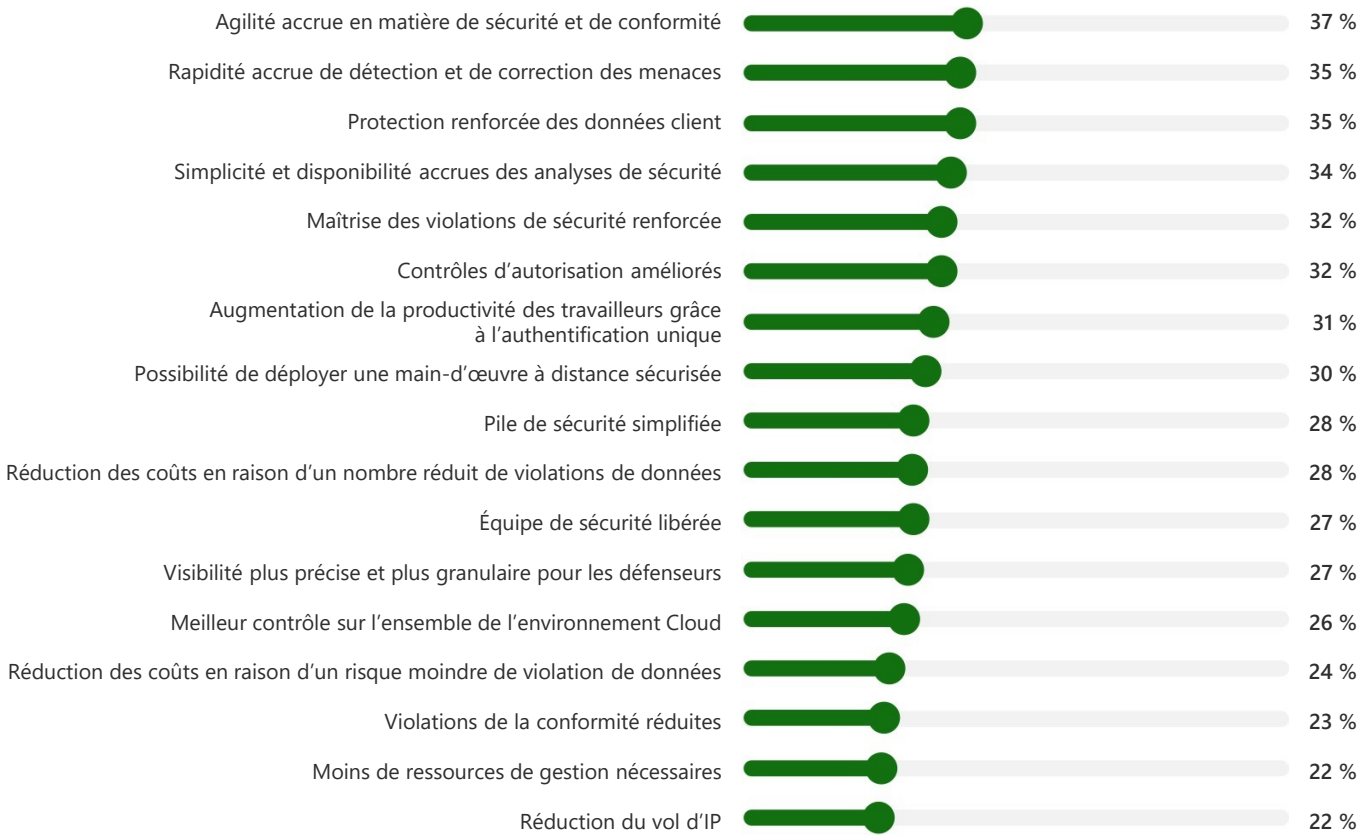
Décisionnaire en sécurité
Hôtellerie

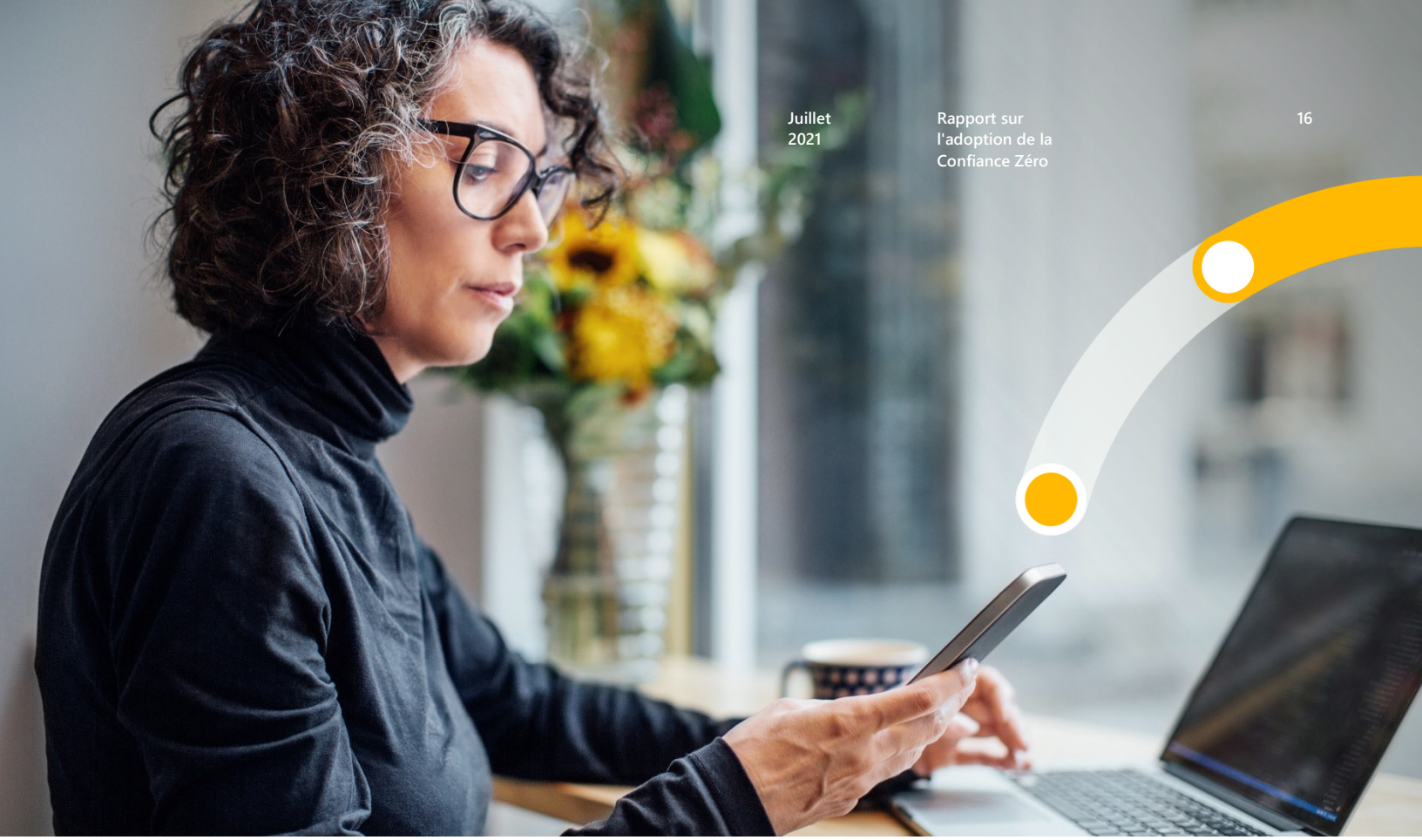
Une fois que les entreprises commencent à mettre en œuvre une stratégie Confiance Zéro, les principaux avantages incluent une agilité, une rapidité et une protection accrues ; les avantages en termes de ressources sont moins courants

Une fois la stratégie Confiance Zéro mise en œuvre, les entreprises bénéficient d'une agilité accrue (37 %), d'une plus grande rapidité (35 %) et d'une meilleure protection des données client (35 %). (Voir la Figure 8) Toutefois, il y a moins d'avantages directs pour les collaborateurs (une équipe de sécurité plus libérée (27 %) et un besoin moindre en ressources pour gérer l'infrastructure (22 %).

Plus important encore, les entreprises estiment que leur stratégie Confiance Zéro les aidera à gérer la plupart des menaces et des changements dans l'environnement, en particulier en ce qui concerne la sécurité de l'IoT et de l'OT (47 %).

Figure 8. Avantages de la stratégie Confiance Zéro





Les entreprises sont convaincues de pouvoir tirer pleinement parti de leur stratégie Confiance Zéro

79 % sont convaincues de pouvoir gérer les menaces de sécurité dans leur ensemble, bien que cette confiance diminue lorsque la menace implique une invention de la vérité : les décisionnaires se sentent moins confiants face aux menaces impliquant des identités synthétiques (20 %) et les deepfakes (10 %).

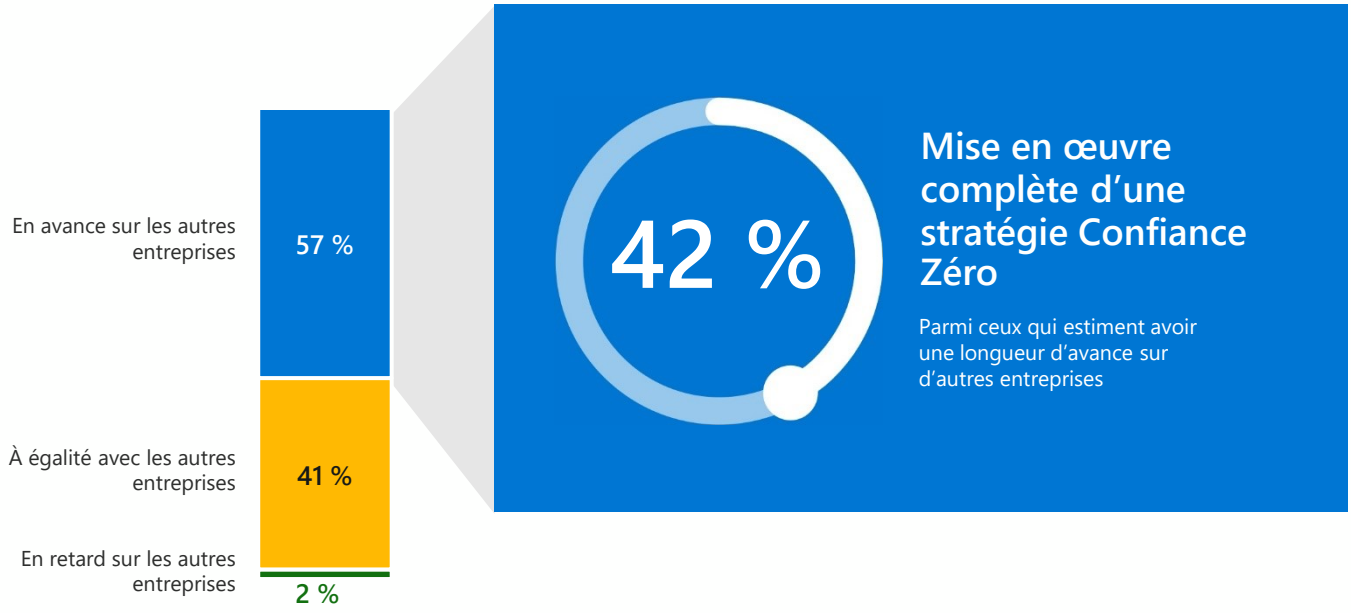
Compte tenu des avantages obtenus, la stratégie Confiance Zéro recueille généralement des associations positives. Sur les quatre marchés, les décisionnaires voient l'approche de l'entreprise vis à vis de cette stratégie à la fois comme une pratique et une aspiration, la qualifiant de stratégie de confiance (37 %) et efficace (31 %), ainsi que de motivation (25 %), d'inspiration (25 %) et d'exaltation (25 %). Au Japon, en particulier, les professionnels de la sécurité décrivent la stratégie Confiance Zéro comme exigeante (27 %) et transformationnelle (25 %), suggérant que, bien qu'elle ne soit pas facile à mettre en œuvre, ses avantages sont énormes, une fois adoptés.

Beaucoup estiment qu'ils sont en avance avec la mise en œuvre de la stratégie Confiance Zéro, mais il leur reste encore beaucoup à faire

Bien que seulement 35 % des entreprises aient entièrement mis en œuvre leur stratégie Confiance Zéro, 52 % déclarent qu'elles sont en avance sur ce qu'elles avaient prévu et que 57 % estiment qu'elles sont en avance sur d'autres entreprises. Les entreprises se considèrent comme particulièrement en avance sur d'autres au Japon (66 %) et en Australie/Nouvelle-Zélande (63 %). Bien que la confiance regorge sur les marchés, il semble y avoir un fossé entre la perception et la réalité : parmi ceux qui se sentent en avance sur d'autres entreprises, seulement 42 % prétendent avoir entièrement mis en œuvre une stratégie Confiance Zéro. (Voir la Figure 9.)

Bien que de nombreuses entreprises aient confiance dans leur stratégie Confiance Zéro et se sentent prêtes à gérer les futures menaces de sécurité, il reste encore beaucoup à faire pour la mettre en œuvre dans l'ensemble des domaines présentant un risque. Parmi les entreprises qui considèrent que leur stratégie Confiance Zéro doit être pleinement mise en œuvre, par exemple, près de la moitié n'ont pas encore effectué la mise en œuvre dans les domaines présentant un risque de sécurité, et cette mise en œuvre est encore moins susceptible d'être effectuée dans l'infrastructure et les identités.

Figure 9. Comparaison de la mise en œuvre de la stratégie Confiance Zéro



	États-Unis	Allemagne	Japon	Australie/Nouvelle Zélande
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 stratégie Confiance Zéro restera une priorité absolue en matière de sécurité

Les entreprises adhèrent totalement à la stratégie Confiance Zéro et les décisionnaires déclarent qu'elle sera la priorité maximale en matière de sécurité au cours des deux prochaines années. L'importance relative de la stratégie Confiance Zéro en tant qu'initiative de sécurité devrait augmenter (passer de 53 % à 58 %) d'ici 2023, tandis que les décisionnaires anticipent que cette stratégie restera essentielle à la réussite globale (96 %). (Voir la Figure 10)

La prévision de l'importance de la mise en œuvre est particulièrement élevée dans les entreprises japonaises. En effet 70 %, déclarent que la stratégie Confiance Zéro sera très importante au cours des deux prochaines années, par rapport à la moyenne globale de 56 %. Les budgets de stratégie Confiance Zéro devraient également croître avec 73 % des entreprises qui s'attendent à augmenter leurs budgets. Bien que ce chiffre soit légèrement inférieur en Allemagne (67 %), où 31 % anticipent que leurs budgets resteront les mêmes. (Voir la Figure 11.)

Figure 10. Prévision de l'importance de la mise en œuvre de la stratégie Confiance Zéro au cours des deux prochaines années

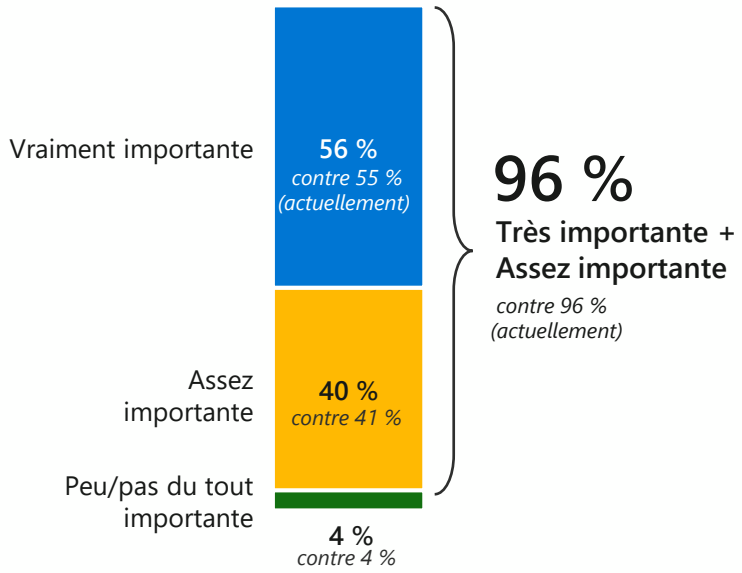
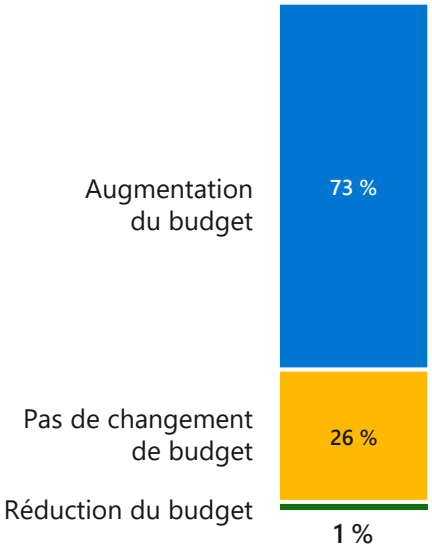
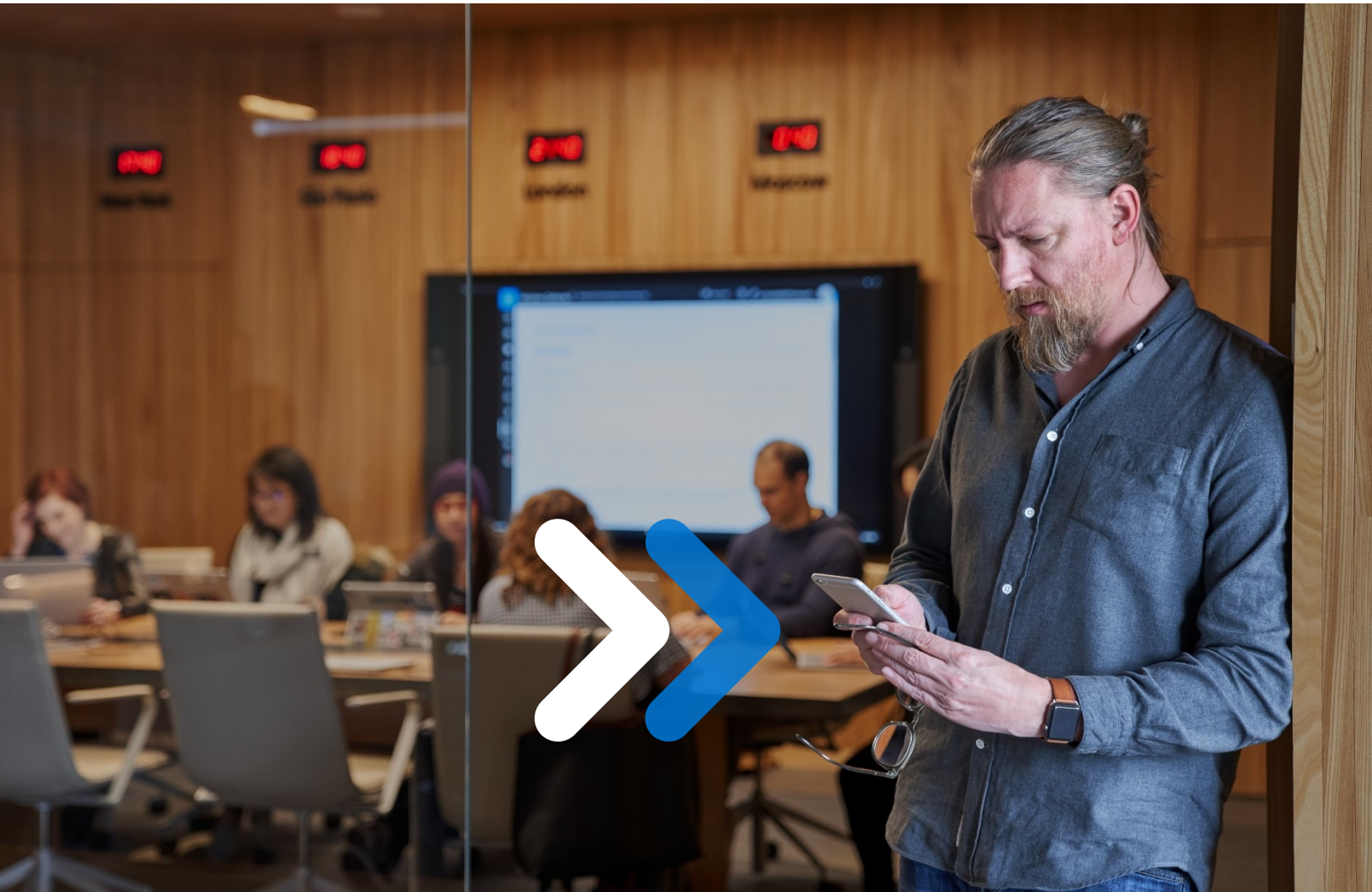


Figure 11. Prévision du budget consacré à la stratégie Confiance Zéro au cours des deux prochaines années



La preuve de la réussite de la stratégie Confiance Zéro pourrait engendrer davantage d'investissements

Les entreprises qui ont résolument adopté la stratégie Confiance Zéro s'attendent à doubler leurs investissements au cours des deux prochaines années, et celles qui n'ont pas encore commencé à adopter risquent d'être en retard. Ces entreprises ne se contentent pas de suivre leurs homologues qui ont entièrement effectué la mise en œuvre lorsqu'il s'agit de prioriser la stratégie Confiance Zéro dans leurs plans de sécurité (42 % contre 66 %) et d'anticiper les augmentations budgétaires (66 % contre 72 %), mais elles se sentent également nettement moins confiantes dans la gestion de la sécurité de l'IoT et de l'OT à l'avenir (40 % contre 53 %).



Surmonter les défis avec les collaborateurs sera essentiel pour doubler les investissements en matière de stratégie Confiance Zéro

Malgré les progrès rapides de l'adoption de la stratégie Confiance Zéro, les entreprises doivent surmonter une multitude de défis s'ils veulent avancer davantage dans la mise en œuvre. (Voir la Figure 12) Les défis liés aux ressources et à la direction sont les plus répandus dans ces catégories. Le temps nécessaire pour mettre en œuvre la stratégie Confiance Zéro et un manque de soutien de la part de la direction arrivent en tête dans la liste des obstacles, ces derniers étant particulièrement importants en Australie/Nouvelle-Zélande (65 %).

En outre, les contraintes budgétaires (que 45 % des entreprises identifient comme un obstacle), sont susceptibles de jouer un rôle dans les défis liés aux ressources et à la direction.

Par exemple, 21 % des décisionnaires citent des difficultés à prouver le retour sur investissement d'un investissement dans la stratégie Confiance Zéro comme un obstacle à la mise en œuvre, un défi qui peut entraîner un manque d'adhésion de la part de la direction. Étant donné que les marchés autres que les 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/Nouvelle-Zélande), il est possible que cela ait un effet d'entraînement, ce qui conduit à une mise en œuvre plus lente et moins efficace de la stratégie Confiance Zéro au Japon, en Allemagne et en Australie/Nouvelle-Zélande qu'aux États-Unis.

Figure 12. Obstacles à la stratégie Confiance Zéro

Défis liés aux ressources 60 %	Direction 53 %	Technologie 46 %	Fournisseur 46 %	Contraintes budgétaires 45 %
20 % Temps de mise en œuvre trop long	**20** % Manque de soutien de la part de la direction	**21** % Difficulté d'intégration des solutions de sécurité	**21** % Besoin d'une prise en charge dans la mise en œuvre de la part des fournisseurs	**21** % Coût de la mise en œuvre d'une stratégie Confiance Zéro
19 % Manque de gestion des changements internes	**19** % Manque de soutien de la part des parties prenantes	**19** % Incompatibilité avec les systèmes hérités	**21** % Difficulté à identifier les bons fournisseurs	**21** % Difficulté à prouver le retour sur investissement
18 % Supports de formations supplémentaires nécessaires	**19** % Besoin d'aide pour effectuer une analyse de rentabilité convaincante	**19** % Difficulté de mise à l'échelle dans l'ensemble de l'entreprise	**17** % Incapacité à trouver des partenaires innovants	**14** % Budget insuffisant
17 % Mise en œuvre inutile vue la taille de l'entreprise	**18** % Manque d'adhésion institutionnelle			
16 % Absence de talents appropriés pour mettre en œuvre correctement				

« L'adhésion initiale était difficile, mais une fois que nous nous sommes mis d'accord pour investir dans ce projet, nous avons pu obtenir l'assentiment de tout le monde. »

Décisionnaire en sécurité
FinTech

Les décisionnaires de sécurité ont un légère préférence pour les fournisseurs globaux

Quand il s'agit de la stratégie Confiance Zéro pour les fournisseurs, les entreprises doivent faire le choix entre adopter une approche Best-in-suite ou Best-in-Breed. L'ancienne stratégie implique l'achat d'une suite de produits pour l'ensemble de l'architecture Confiance Zéro auprès d'un fournisseur global, une solution qui selon les décisionnaires offre davantage d'expertise, de ressources et de simplicité pour ceux qui sont attachés à des ressources en interne. Toutefois, les préoccupations liées à cette approche incluent une vulnérabilité accrue et un manque de souplesse. (Voir la Figure 13)

Cette dernière stratégie, Best-in-Breed, consiste à obtenir des composants de technologie Confiance Zéro individuels auprès de fournisseurs spécialisés. Contrairement au Best-in-suite, cette stratégie s'appuie sur les fournisseurs qui se spécialisent dans différents domaines et offrent donc une plus grande flexibilité et peuvent s'aligner plus étroitement sur la stratégie de l'entreprise. Cela dit, les professionnels de la sécurité considèrent que la stratégie Best-in-Breed est plus coûteuse et nécessite davantage de ressources et inhibe la visibilité, des inconvénients qui conduisent finalement à des défis de fournisseur et de budget. (Voir la Figure 14.)

Bien que les entreprises soient largement scindées, une petite majorité des décisionnaires (55 %) préfèrent travailler avec des fournisseurs globaux (Best-in-suite). (Les entreprises en Australie/Nouvelle-Zélande, cependant, penchent dans la direction opposée, en effet 52 % préfèrent la stratégie Best-in-Breed).

Figure 13. Avantages et inconvénients de la stratégie Best-in-Suite – Classés dans l'ordre

⊕ Avantages du Best-in-suite	
Le fournisseur a une expertise spécifique au secteur dans les solutions	24 %
Plus de ressources disponibles pour aider à planifier la stratégie Confiance Zéro	23 %
Pile de sécurité simplifiée	22 %

⊖ Inconvénients du Best-in-suite	
Plus grande vulnérabilité en raison de la dépendance à l'égard d'un fournisseur unique	34 %
Nécessite une intégration plus complexe avec l'architecture héritée	33 %
Moins de souplesse pour un fonctionnement spécialisé	29 %

Figure 14. Avantages et inconvénients de la stratégie Best-in-Breed – Classés dans l'ordre

⊕ Avantages du Best-in-Breed	
Flexibilité pour rechercher les meilleures solutions pour n'importe quel composant de la stratégie Confiance Zéro	33 %
Possibilité d'aligner plus étroitement la solution avec l'architecture ou la stratégie de l'entreprise	30 %
Opportunités accrues en matière d'innovation avec divers fournisseurs	26 %

⊖ Inconvénients du Best-in-Breed	
Augmentation des coûts	29 %
Incapacité à partager des données entre différentes solutions	26 %
Adoption et gestion d'un volume élevé de solutions pour les équipes internes	26 %

Dernières considérations

À mesure que les risques de sécurité deviennent non seulement plus fréquents, mais plus néfastes, les entreprises de différents marchés et secteurs optent pour une stratégie Confiance Zéro qui incite à une approche de type « Aucune confiance, vérification continue ». La stratégie Confiance Zéro est la priorité absolue pour les entreprises qui cherchent à améliorer la sécurité globale, l'expérience des utilisateurs finaux et la productivité, à simplifier les procédures de sécurité pour les collaborateurs et à réduire les coûts. Toutefois, bien que les avantages d'une stratégie Confiance Zéro soient bien établis, les ressources limitées et le scepticisme parmi les dirigeants font obstacle à une mise en œuvre universelle.

L'adoption de la stratégie Confiance Zéro s'est accélérée au cours des trois dernières années, en partie en raison de la pandémie de COVID-19. Bien entendu, la transition vers les lieux de travail éloignés et hybrides entraîne une adoption plus large des approches de type Confiance Zéro, avec la promesse de protéger les systèmes et les données, même lorsque les employés y accèdent, parfois sur des appareils personnels. L'adoption accélérée due à l'épidémie de COVID est un bon indicateur de l'état de préparation globale pour la stratégie Confiance Zéro. En effet, les entreprises qui ont adopté cette stratégie pendant la pandémie l'ont mise en œuvre dans plus de domaines présentant un risque de sécurité que leurs homologues.

Cela dit, même les adoptants de la stratégie Confiance Zéro les plus avancés ont encore du travail à faire, et en raison des idées fausses autour de leur propre maturité dans ce domaine, ils risquent de laisser passer certaines vulnérabilités.

Une majorité d'entreprises sur l'ensemble des marchés estiment que l'importance d'une stratégie Confiance Zéro ne fera que croître avec le temps et s'attendent à ce que leurs budgets augmentent à leur rythme. Cette évolution anticipée de la hiérarchisation est particulièrement cruciale pour les marchés autres que les États-Unis, où les préoccupations budgétaires sont des obstacles importants à l'adoption. Appliquer une mise en œuvre complète peut être très lourd financièrement et logistiquement. Néanmoins, les avantages d'une approche de type Confiance Zéro sont indéniables, et Microsoft sera là pour guider et soutenir les entreprises au fur et à mesure qu'elles se dirigent vers ce domaine en plein essor.

Pour en savoir plus sur la stratégie Confiance Zéro et effectuer une évaluation de la maturité de votre entreprise en la matière, visitez

aka.ms/zerotrust

Objectifs de recherche détaillés et public visé

Les objectifs de cette étude étaient les suivants :

Comprendre l'état actuel des approches de Confiance Zéro

Découvrir les états d'esprit, les bonnes pratiques, les avantages et les défis liés à l'adoption d'une stratégie Confiance Zéro

Explorer l'avenir des approches Confiance Zéro

Contextualiser les innovations et les tendances dans les approches Confiance Zéro

Pour répondre aux critères de sélection, les décisionnaires de sécurité devaient être :

Responsable de la sécurité dans leur entreprise, y compris la cybersécurité, les opérations de sécurité, la protection contre les menaces, la gestion des identités, la gestion des risques, la sécurité des applications, la criminalistique numérique et la réponse aux incidents

Employés à plein temps dans une entreprise de taille intermédiaire (plus de 1 000 collaborateurs aux États-Unis ; plus de 500 collaborateurs en Allemagne, au Japon, en Australie/Nouvelle-Zélande)

Âgés de 25 à 75 ans

connaissent la stratégie Confiance Zéro

Impliqués dans la prise de décision concernant le développement ou la mise en œuvre d'une stratégie Confiance Zéro

Sur les 911 décisionnaires de sécurité interrogés pour la vague de recherche d'avril 2021 :

477 ont été interrogés aux États-Unis

201 ont été interrogés en Allemagne

126 ont été interrogés en Australie/Nouvelle Zélande

107 ont été interrogés au Japon

Remarque : les recherches ont été menées pendant la pandémie de COVID-19, alors à différents stades d'intensification et de maîtrise dans le monde

Microsoft Security hypothesis