CSO

Microsoft Security

CONTENU SPONSORISÉ

Sécurité Zero Trust : **Les conseils de nos premiers utilisateurs**

CSO Microsoft Security

Table des matières

CSO Microsoft Security

Introduction

Les perturbations de ces deux dernières années ont ébranlé les modèles traditionnels d'informatique et de sécurité. En conséquence, la sécurité Zero Trust est rapidement passée du statut de concept intéressant à celui d'élément indispensable dans la sécurité des entreprises modernes.

Une nouvelle étude de Foundry révèle que 52 % des entreprises testent actuellement ou ont déjà déployé une architecture Zero Trust, et que 15 % d'entre elles effectuent des recherches sur les modèles Zero Trust. Ces adoptants font état de nombreux avantages découlant de leurs déploiements, notamment une meilleure protection des données des clients, une réduction de la complexité, ainsi qu'un accès sécurisé et fiable aux ressources de l'entreprise.

Cet Ebook explorera les résultats de la recherche de Foundry, qui souligne l'importance d'une stratégie Zero Trust pour aider les DSI à protéger leurs entreprises contre une multitude de risques provenant de nombreux vecteurs d'attaque. Il comprend également des conseils sur la mise en œuvre de Zero Trust pour ceux qui entament leur parcours.

À propos de l'enquête

Foundry a interrogé des entreprises américaines en février et mars 2022 pour étudier l'état actuel de l'adoption de Zero Trust. Les personnes interrogées devaient être des responsables informatiques ou poste supérieur dans une entreprise de plus de 500 collaborateurs et avoir un rôle dans l'achat de produits et de services de cybersécurité.

Il y a eu 250 répondants au total pour cette enquête comprenant 23 questions.

CSO Microsoft Security

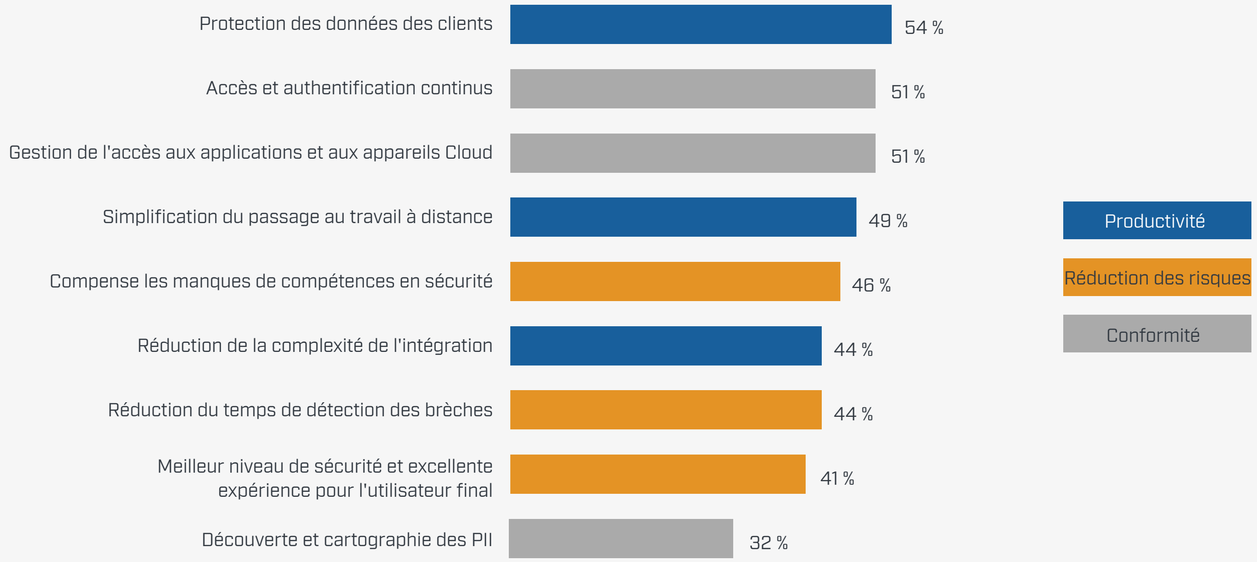
Zero Trust est là pour apporter de la valeur

Il ressort clairement des résultats de l'enquête, ainsi que des entretiens approfondis avec des responsables de l'informatique et de la sécurité, que Zero Trust est une priorité pour la plupart des entreprises. Ceux qui ont déployé différents composants Zero Trust en voient déjà les avantages.

La plupart des répondants ayant mis en œuvre Zero Trust (87 %) affirment que l'architecture atteint ou dépasse leurs objectifs initiaux en matière de mise en œuvre, d'adoption et d'intégration.

« [Zero Trust] est devenu une procédure d'exploitation standard pour nous. Je ne nous vois pas revenir un jour à nos anciennes procédures », déclare un directeur informatique d'une entreprise internationale de la distribution. (Les répondants ont pu parler librement de leurs plans de sécurité en ayant la garantie que leur anonymat serait conservé).

Avantages obtenus depuis la mise en œuvre de Zero Trust



12 % des répondants ont déclaré avoir obtenu *tous* ces avantages

Source : enquête sur l'adoption de Zero Trust, mars 2022, Foundry. Base :250

CSO Microsoft Security

Quelque 44 % des répondants ont également indiqué que Zero Trust réduisait la complexité inhérente à la mise en œuvre d'une architecture de sécurité intégrée. « Travailler avec un cadre facilite grandement les choses », déclare le DSI d'une société de centre d'appels comptant 3 500 collaborateurs.

Un vice-président et DSI d'une société de services financiers comptant 17 000 collaborateurs affirme que l'authentification multifactorielle mise en place par son entreprise dans le cadre de l'architecture Zero Trust a été un succès auprès des collaborateurs. « La satisfaction des collaborateurs a augmenté, car ils n'ont plus besoin d'utiliser un client VPN sur la machine fournie par l'entreprise ; ils peuvent accéder aux ressources de n'importe où », explique-t-il.

Le concept d'accès basé sur les privilèges minimum a également porté ses fruits, note le DSI. « Nous avons eu moins d'erreurs catastrophiques de la part des administrateurs système grâce à la mise en place de ce système d'accès aux privilèges », dit-il. « Les privilèges leur sont donnés dans un cadre spécifique et dans des délais précis, ils sont ainsi moins susceptibles de faire une erreur. »

Compte tenu de la prévalence accrue du hameçonnage et de divers autres cyberattaques, le directeur informatique de l'entreprise de distribution résume ainsi les avantages de Zero Trust : « Si nous n'avions pas ce type d'outils, nous serions probablement dans une bien mauvaise posture, peut-être en train de verser des bitcoins à quelqu'un en ce moment même. »

CSO Microsoft Security

Moteurs du déploiement de Zero Trust

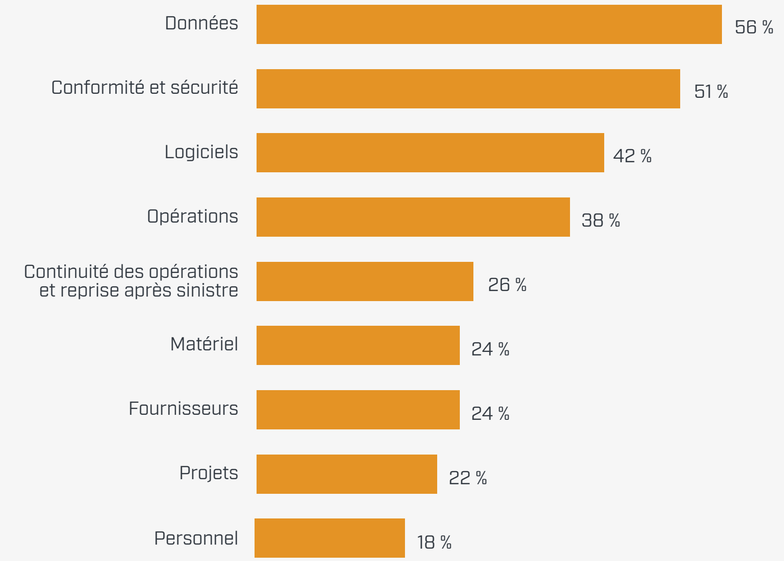
Un ensemble de facteurs pousse les entreprises à au moins envisager une architecture Zero Trust. En tête de liste, il y a la nécessité de gérer les risques de menaces sur les nombreuses ressources de chaque entreprise. Les répondants ont attribué les incidents de sécurité survenus au cours des dernières années à différentes causes, les principales étant les vulnérabilités de sécurité provenant de personnes ou d'entreprises tierces. Parmi les autres causes, se trouvaient les suivantes :

- Risques opérationnels imprévus
- Mauvaise configuration des services ou des systèmes
- Attaques internes malveillantes et intentionnelles
- Erreur d'utilisateur non malveillant, y compris des victimes de hameçonnage
- Identités compromises
- Logiciels non corrigés
- Identifiants volés

Ces incidents représentent un grand nombre de risques, principalement vis-à-vis des données.

Pour de nombreuses entreprises, le passage soudain au travail à distance provoqué par la pandémie a accéléré les plans d'adoption de Zero Trust, les modèles de sécurité traditionnels basés sur le périmètre étant devenus obsolètes. De nombreuses entreprises s'étaient déjà engagées dans cette voie en transférant davantage d'applications et d'infrastructures informatiques vers le Cloud, mais la pandémie a été un coup de pouce supplémentaire.

Principales catégories exposées aux menaces de cybersécurité



Source : enquête sur l'adoption de Zero Trust, mars 2022, Foundry. Base :250

CSO Microsoft Security

Par exemple, le DSI d'une entreprise de technologie médicale comptant 1 700 collaborateurs affirme que le Cloud et la pandémie ont été les moteurs de son adoption de Zero Trust, qui constitue désormais une base sûre pour tout modèle de lieu de travail à venir.

« Les moteurs de l'entreprise étaient le fait que nous sommes une société basée sur le Cloud et que nous devions être en mesure de sécuriser notre environnement », explique-t-il. « Nous devions également fournir une main-d'œuvre à distance compétente pendant la pandémie. [Zero Trust] nous a permis de réduire considérablement notre empreinte immobilière. Nous allons probablement rester une entreprise virtuelle à distance à hauteur de 60 % au minimum. »

CSO Microsoft Security

Les menaces ne manquent pas

Les besoins de conformité ont également incité le développement de modèles de sécurité plus robustes. « Les régulateurs nous observent et attendent de nous que nous continuions à améliorer notre cadre de sécurité », déclare le vice-président sécurité mondiale des informations d'une société de services financiers comptant 290 000 collaborateurs.

Certaines entreprises ont pris des mesures proactives en faveur de Zero Trust afin d'éviter une violation très médiatisée qui les mettrait sous les feux des projecteurs pour de mauvaises raisons. « L'important était d'être proactifs et d'essayer de ne pas être trop présents dans les médias », explique le DSI d'un établissement d'enseignement supérieur comptant 3500 collaborateurs. « Nous avons eu vent de véritables histoires d'horreur concernant d'autres institutions locales d'à peu près notre taille qui ont été paralysées pendant une longue période. »

D'autres ont déjà connu un grave incident de cybersécurité, ce qui les a incités à revoir rapidement leur stratégie de sécurité. Après qu'une compagnie d'assurance de 6 000 collaborateurs a subi une attaque de ransomware qui a mis le réseau de l'entreprise hors service pendant deux semaines, le mandat réclamant l'adoption de Zero Trust est venu directement du PDG. « Nous avons accéléré la mise en œuvre », déclare le vice-président du développement informatique de l'entreprise. « Il s'agissait sans nul doute d'une bonne pratique au départ, puis le processus s'est réellement accéléré après notre attaque par ransomware. »

Un moteur basé sur le Cloud

Le vice-président et DSI d'une grande entreprise de services financiers explique que son équipe a reconnu la nécessité d'une nouvelle architecture de sécurité il y a plusieurs années, alors qu'elle commençait à adopter davantage de ressources basées sur le Cloud et que les utilisateurs devenaient plus mobiles.

« Nous avons réalisé que l'architecture de sécurité traditionnelle de type "château et douve" sur laquelle nous nous étions appuyés dans le passé ne nous protégerait pas des attaquants à l'avenir », explique-t-il.

Cette réalité est devenue très claire au début de 2020, lorsque l'entreprise a découvert qu'à un moment donné au cours de l'année précédente, un attaquant avait pénétré dans son périmètre et s'était déplacé latéralement dans l'environnement sans être détecté. « Nous avions besoin d'une nouvelle architecture où nous pourrions protéger et authentifier l'utilisation de ces ressources où qu'elles se trouvent, et Zero Trust est une architecture conçue à cet effet. »

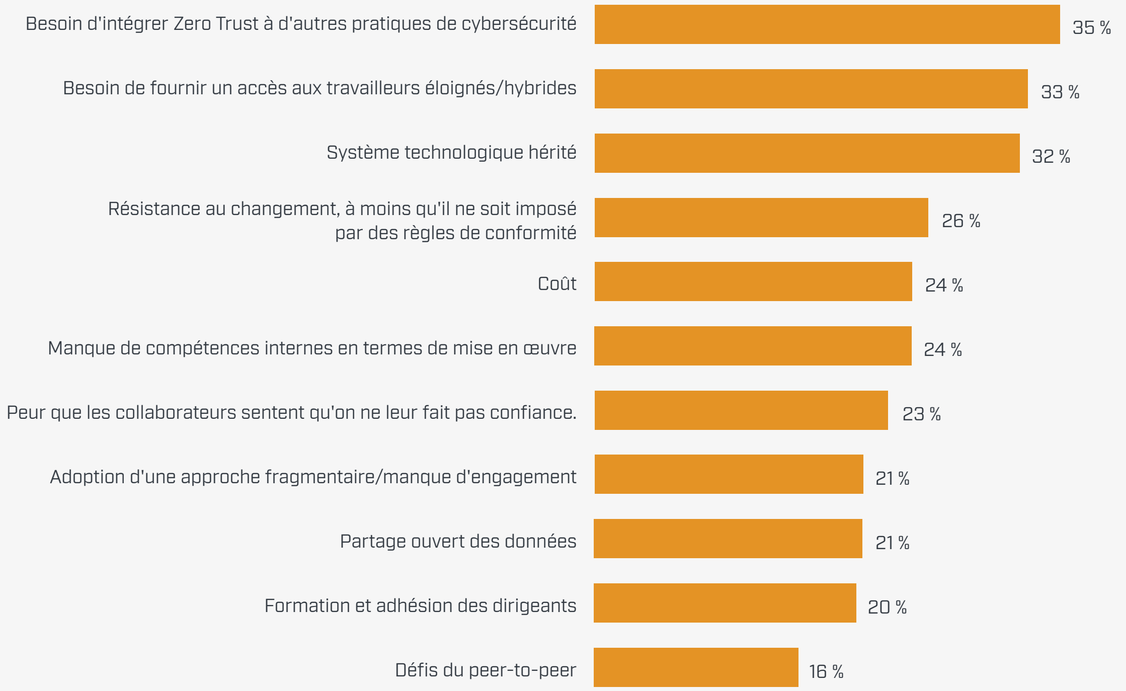
CSO Microsoft Security

Obstacles à l'adoption de Zero Trust

Pour de nombreuses entreprises, Zero Trust représente un changement fondamental de structure, de processus et de mentalité en matière de sécurité, ce qui explique certains des obstacles qu'elles doivent surmonter avant de l'adopter.

« Il y avait tellement de silos différents que nous avons commencé à nous heurter au sein de l'entreprise », a noté le DSI du centre d'appels, expliquant que les équipes chargées des serveurs, du réseau et des bases de données avaient chacune leur propre contingent de serveurs et d'outils Web. « Cela nous a ralentis, car chacun avait une idée différente de l'endroit où aller et de la manière de le faire. »

Qu'est-ce qui empêche l'adoption de Zero Trust ?



Source : enquête sur l'adoption de Zero Trust, mars 2022, Foundry. Base :250

CSO Microsoft Security

La mise au jour de ces problèmes peut en fait être un effet secondaire positif de Zero Trust, selon Anthony Mocny, responsable marketing produit senior pour Zero Trust chez Microsoft. « En tant qu'architecture, Zero Trust est conçu pour briser les silos des équipes de sécurité instaurés au sein des piliers technologiques et aider les équipes à travailler ensemble de manière cohérente », dit-il. « Cela peut également impliquer un changement culturel, en ce qui concerne la façon dont les équipes travaillent ensemble. »

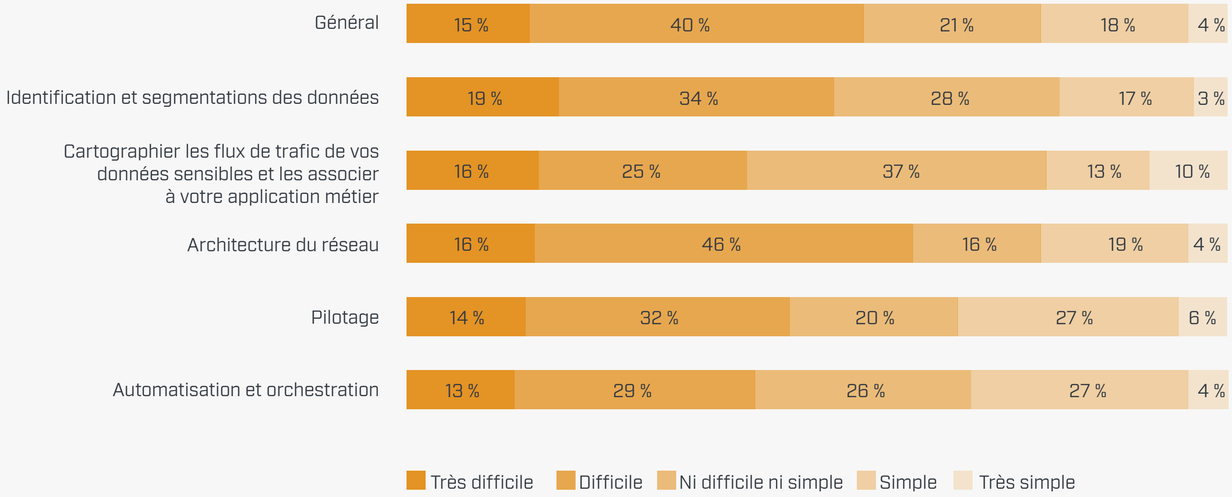
Pour le VP/CSI des services financiers, les applications patrimoniales constituaient un obstacle à surmonter sur le parcours Zero Trust de l'entreprise. « Elles doivent être équipées d'une technologie d'authentification moderne », explique-t-il. « En fonction de leur âge, cela n'est pas forcément facile à faire. »

CSO Microsoft Security

Défis liés au déploiement

Une fois que les entreprises s'engagent dans un parcours Zero Trust, un grand nombre de défis de mise en œuvre peuvent également apparaître. Plus de la moitié des répondants à l'enquête (56 %) ont reconnu que la mise en œuvre de Zero Trust était difficile, voire très difficile. En particulier :

À quel point la mise en œuvre de Zero Trust représente-t-elle un défi ?



Source : enquête sur l'adoption de Zero Trust, mars 2022, Foundry. Base :168

CSO Microsoft Security

Les défis liés à la segmentation et à la micro-segmentation sont revenus fréquemment dans les entretiens approfondis.

« Il faut segmenter son réseau à l'échelle de chaque hôte individuel », explique le VP/CSI des services financiers. « C'est comme mettre en place un petit pare-feu entre chaque hôte du réseau interne afin de pouvoir voir tout le trafic et le contrôler au niveau de chaque machine individuelle. Cela présente d'énormes avantages en matière de sécurité, mais c'est extrêmement difficile à mettre en œuvre, car il faut gérer des dizaines de milliers de pare-feu. »

La cartographie des flux de trafic peut être un autre processus de plusieurs mois. Le directeur technique d'une société d'édition et de médias comptant 5 000 collaborateurs explique qu'après avoir défini les données critiques, les applications et les services réseau qu'ils devaient protéger, « nous avons cartographié les flux de transactions le long du réseau et essayé de les considérer comme des groupes d'informations ». « [Nous avons ensuite] segmenté des portions de ces informations et la façon dont elles voyagent à travers le réseau, même à l'échelle de simples paquets d'informations. » À ce stade, l'entreprise a appliqué des politiques Zero Trust à chaque type de flux de trafic. « Nous nous sommes également appuyés sur de nouvelles capacités pour surveiller et entretenir notre réseau. »

Malgré les défis, de nombreuses personnes interrogées pensent que Zero Trust simplifie finalement les opérations quotidiennes. Avec les technologies traditionnelles, « il faut des jours pour apporter des changements ; il faut les diffuser à travers tous les composants matériels et logiciels, et cela demande beaucoup de ressources », déclare le vice-président exécutif des services financiers pour la sécurité globale de l'information. « Zero Trust minimise vraiment la complexité architecturale à long terme et réduit le nombre de collaborateurs nécessaires pour effectuer le même type de travail. »

CSO Microsoft Security

Meilleures pratiques pour la mise en œuvre de Zero Trust

Au fur et à mesure que de plus en plus d'entreprises mettent en œuvre une architecture Zero Trust, elles élaborent des feuilles de route et des bonnes pratiques que d'autres pourront suivre. Voici cinq éléments à prendre en compte lors de la planification d'un déploiement.

N'essayez pas de trop en faire au début

L'élaboration d'une stratégie Zero Trust peut être décourageante si on la considère uniquement dans le contexte général de la révision des politiques et des protections sur les réseaux, les données, les applications, les identités, les points de terminaison et l'infrastructure. « Au début, il s'agissait d'une énorme montagne à gravir et nous nous demandions si nous allions vraiment y arriver », explique le DSI d'un établissement d'enseignement supérieur. « Il faut juste faire un pas à la fois. »

Le DSI et son équipe ont finalement adopté une approche centrée sur l'argent, en donnant la priorité à la segmentation des applications financières et de paie sur un réseau distinct.

Identifier les biens les plus critiques à protéger est une approche judicieuse, selon Mocny. « Gardez toujours à l'esprit la raison première pour laquelle vous mettez en place Zero Trust », conseille-t-il.

En cas de doute, commencez par le multifacteur

Lors de la hiérarchisation de la pile de sécurité, de nombreux DSI et fournisseurs de sécurité recommandent de se concentrer initialement sur l'authentification et les autres protections basées sur l'identité. « Si vous n'avez pas de point de départ bien défini, il est peut être intéressant de commencer par l'authentification multifacteur », déclare Mocny. Microsoft estime que l'authentification multifacteur peut prévenir plus de 90 % des attaques basées sur l'identité.

Le VP/DSI des services financiers confirme cette thèse. « L'authentification est un élément fondamental de la mise en œuvre d'une architecture Zero Trust. Aucun autre composant ne fonctionne si l'on ne peut valider l'identité de l'utilisateur final, c'est pourquoi nous avons commencé par là. »

Ensuite, le VP/DSI des services financiers s'est attaqué à la composante réseau, qui a fourni des avantages immédiats pour la prise en charge des travailleurs à distance. L'équipe a gardé la micro-segmentation pour plus tard dans son parcours, car elle n'est pas facilement visible pour l'ensemble de l'entreprise. « Lorsque vous avez fini de gérer la micro-segmentation, votre niveau de sécurité est nettement plus élevé, mais personne ne remarque la différence », dit-il.

CSO Microsoft Security

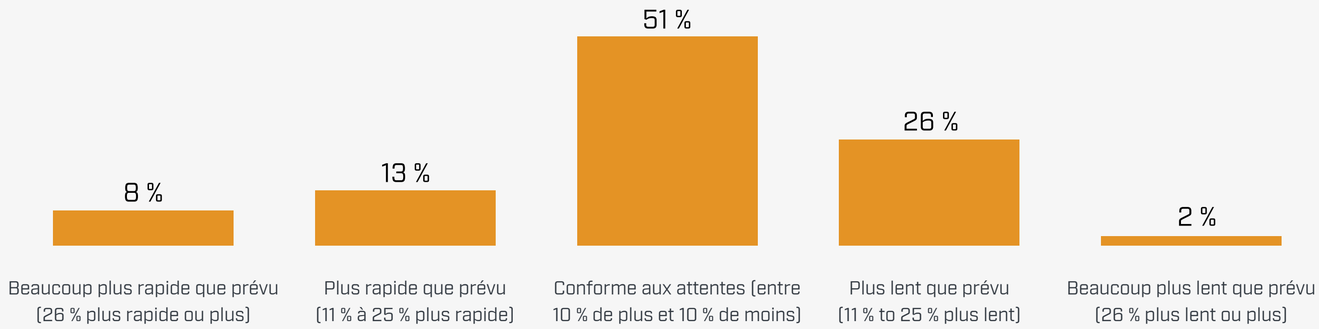
Soyez réaliste quant à vos délais

Il est important que les DSI aient des attentes réalistes quant aux déploiements de Zero Trust. « La mise en œuvre d'une architecture Zero Trust est un programme et non un projet », déclare le VP/DSI des services financiers. « C'est un changement majeur. La mise en œuvre d'une architecture Zero Trust ne se fait pas en un clin d'œil et sans encombre. »

Son collègue vice-président exécutif financier abonde en ce sens. « Je pense que nous n'en aurons jamais fini, car il y a toujours de nouvelles technologies, de nouveaux logiciels malveillants et de nouvelles menaces qui apparaissent », déclare-t-il.

La majorité des répondants de l'enquête (72 %) ont déclaré que leur déploiement était soit dans le délai, soit en avance sur le planning. Pour les autres, cette mise en œuvre prend plus de temps que prévu.

Zero Trust répond-il à vos objectifs en termes de délais ?



Source : enquête sur l'adoption de Zero Trust, mars 2022, Foundry. Base :168

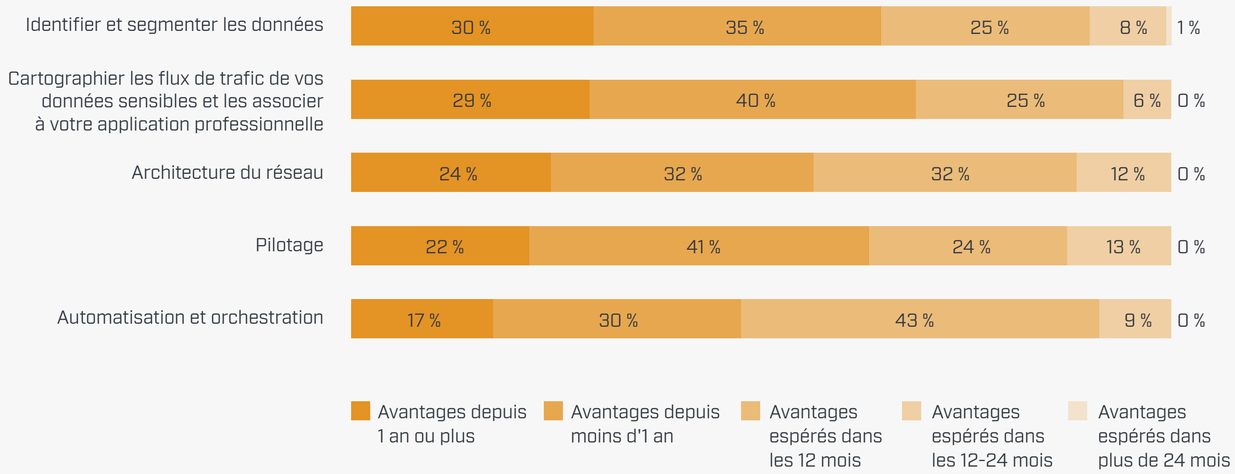
CSO Microsoft Security

Prenez des mesures au fil de votre parcours

Lorsqu'un déploiement de Zero Trust est en cours, les DSI peuvent et doivent créer des jalons en cours de route pour mesurer les progrès. Il est très positif de constater qu'environ deux tiers des répondants à l'enquête déclarent avoir tiré des bénéfices de la plupart des aspects de leurs projets dans un délai d'un an, et que, parmi les autres, environ un quart ou plus s'attendent à ce que ce soit le cas pour eux aussi dans un délai de 12 mois, pour des activités clés telles que l'identification et la segmentation des données, la cartographie des flux de trafic et l'architecture du réseau.

« Zero Trust est un parcours continu, car la nature changeante des attaques implique d'évoluer constamment », déclare Mocny. « Soyez toujours à l'affût d'améliorations. »

Délais avant les premiers avantages notables de Zero Trust



Source : enquête sur l'adoption de Zero Trust, mars 2022, Foundry. Base :103

Concentrez-vous sur les personnes, pas seulement sur les technologies

La portée étendue d'un modèle de sécurité Zero Trust a un impact sur chaque collaborateur, y compris sur les équipes informatiques et de sécurité chargées de le déployer. C'est pourquoi, comme pour tout grand projet technologique, il est important de s'assurer que les déploiements sont en phase avec les nouveaux processus et les pratiques de gestion du changement pour garantir un déploiement sans heurts et réussi.

« En plus d'un changement technologique, il y a aussi un changement culturel », déclare Mocny. « Si vous disposez de plusieurs équipes gérant la sécurité (comprenant des architectes de réseau ou des experts en identité), vous devez également changer la façon dont elles travaillent toutes ensemble. Vous devez abattre les silos pour que la technologie fonctionne de manière cohérente. »

Abattre les silos demande d'impliquer étroitement les équipes de toutes ces disciplines dans des projets d'expérimentation et de proof of concept (POC). Un directeur des systèmes informatiques d'une entreprise de télécommunications d'environ 2 000 collaborateurs a appris cette leçon après avoir lutté contre plusieurs points uniques de défaillance pendant le déploiement, notamment des services qui ne pouvaient pas s'authentifier et qui étaient soudainement « non fiables », ce qui les rendait indisponibles, au même titre que certains systèmes.

« Le déploiement d'un service peut causer un effet domino et faire tomber les autres », dit-il. À l'avenir, « nous serons beaucoup plus prudents : plus de temps de POC, plus d'évaluations et plus de révisions architecturales avec des experts en la matière avant de déployer ».

Retour sur investissement de Zero Trust

Une **étude Total Economic Impact™ commandée par Forrester Consulting en 2021** quantifie les économies de coûts et les avantages commerciaux des solutions Microsoft Zero Trust. Sur la base des cinq entreprises interrogées par Forrester, une entreprise composite a réalisé un retour sur investissement de 92 % sur trois ans en mettant en œuvre une architecture Zero Trust avec Microsoft.

Cette entreprise composite a également économisé en moyenne 20 dollars par collaborateur et par mois en supprimant les outils de sécurité devenus redondants avec Zero Trust, notamment les outils de gestion des points de terminaison, les antivirus et les solutions anti-logiciels malveillants.

CSO Microsoft Security

Où en êtes-vous dans votre parcours Zero Trust ?

Comme l'indique l'enquête, les avantages d'un modèle de sécurité Zero Trust l'emportent clairement sur certains des défis de déploiement auxquels sont confrontés les DSI et leurs équipes de sécurité. Relever ces défis avec un plan bien pensé peut aider votre entreprise à améliorer rapidement son niveau de protection, à réduire ses risques et à apporter de la valeur à toute son activité.

Pour évaluer le niveau de maturité Zero Trust de votre entreprise et découvrir des ressources de déploiement plus pratiques, réalisez **l'évaluation du modèle de maturité Zero Trust** de Microsoft.