Akamai

LIVRE BLANC

L'état de la segmentation en 2023

Pour surmonter les obstacles au déploiement, une transformation s'impose

Table des matières

Introduction

Le travail des services de sécurité informatique n'a jamais été facile. Mais aujourd'hui, des attaquants de plus en plus sophistiqués combinent des techniques pour générer des menaces plus importantes et plus fréquentes, ce qui met les équipes de sécurité sous une pression sans précédent. Aucune entreprise ne peut fonctionner sans une présence en ligne, et une seule violation réussie peut causer des dommages considérables, voire irréparables, à la réputation et au chiffre d'affaires.

Comme le montrent les conclusions de ce rapport, ces attaques ont également un effet plus important, ce qui accroît la pression sur les responsables de la sécurité pour choisir les bonnes solutions et assurer la sécurité de l'ensemble de l'environnement, sans sacrifier les performances globales ou l'innovation.

En actualisant les conclusions de ce rapport depuis 2021, nous avons cherché à savoir si la segmentation était la solution de choix et si elle était efficace. Les 1 200 personnes interrogées ont largement reconnu l'efficacité de la segmentation pour assurer la protection des actifs, mais leurs progrès globaux dans le déploiement de la segmentation au niveau des applications et des actifs critiques de l'entreprise ont été plus lents que prévu. Dans tous les pays, l'obstacle numéro un a été le manque d'expertise pour déployer la segmentation, ce qui suggère que les équipes pourraient hésiter à se lancer dans un projet susceptible de perturber les performances, en particulier compte tenu de la complexité croissante des environnements informatiques.

La bonne nouvelle ? La persévérance paie. Pour ceux qui avaient segmenté la plupart de leurs actifs critiques, la segmentation s'est avérée avoir un effet transformateur sur la défense, leur permettant d'atténuer et de contenir les ransomwares avec 11 heures d'avance par rapport à ceux qui n'avaient segmenté qu'un seul actif. Imaginez la différence que ces 11 heures représentent pour votre équipe, vos clients, la réputation de votre marque et votre chiffre d'affaires.

Les attaques par ransomware et leurs conséquences prennent de l'ampleur

Au cours des deux dernières années, le nombre d'attaques par ransomware (réussies et infructueuses) a doublé, passant de 43 en moyenne en 2021 à 86 en 2023. Une augmentation encore plus importante a été mesurée entre le premier trimestre 2022 et le premier trimestre 2023 par les données collectées à partir des sites de fuite d'environ 90 groupes de ransomware différents. Publié en août 2023, le rapport Les ransomwares évoluent : techniques d'exploitation évolutives et recherche active des vulnérabilités de type Zero Day indique que l'utilisation de vulnérabilités de type Zero Day et One Day a conduit à une augmentation de 143 % du nombre total de victimes de ransomwares dans le monde.

Sans surprise, les entreprises américaines sont toujours confrontées au plus grand nombre de menaces liées aux ransomwares (figure 1) : les équipes de sécurité informatique et les décideurs américains signalent en moyenne 115 attaques par ransomware au cours des 12 derniers mois, soit le nombre le plus élevé de tous les pays étudiés.

Nombre moyen d'attaques par ransomware au cours des 12 derniers mois par pays

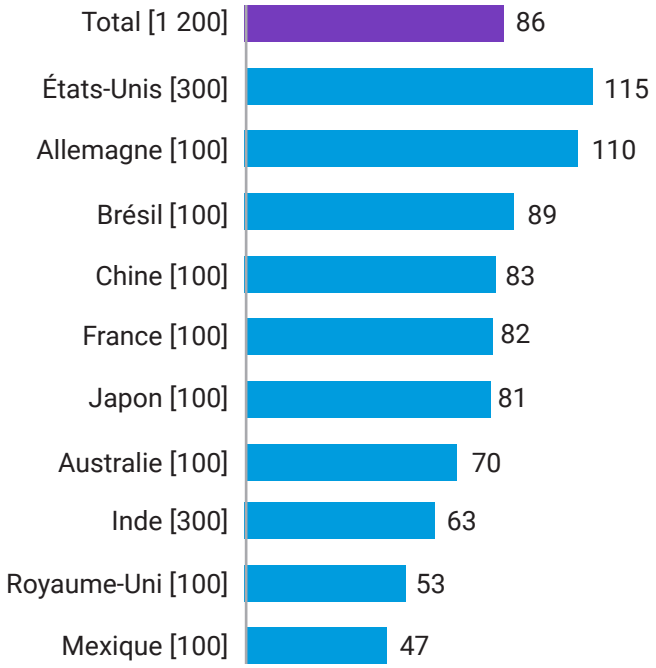

Figure 1 : Combien d'attaques par ransomware votre entreprise a-t-elle subi au cours des 12 derniers mois (qu'elles aient abouti ou non) ? [1 200], s'agissant uniquement du nombre moyen d'attaques au cours des 12 derniers mois, réparties par pays.

Étant donné que les États-Unis font partie des deux pays les moins susceptibles d'avoir mis en œuvre la segmentation dans plus de deux domaines d'activité critiques (figure 2), leur classement en tête des attaques par ransomware et leur faible classement en matière de déploiement de la segmentation pourraient être liés.

Bien entendu, le nombre élevé d'attaques par ransomware aux États-Unis est probablement imputable à une série de facteurs, notamment l'actualité de violations majeures telles que celle qu'un groupe cybercriminel russe a commise contre des agences fédérales en 2023 et la prolifération des terminaux IoT aux États-Unis (2 milliards de plus que la Chine, qui arrive en deuxième position). Le Ransomware for IoT (R4IoT) exploite les terminaux IoT vulnérables, tels que les caméras IP, pour s'implanter dans un premier temps, puis se déplace latéralement dans un réseau informatique, en profitant des mauvaises pratiques de sécurité pour prendre en otage les processus essentiels.

Les attaques par ransomware sont non seulement plus fréquentes au niveau mondial en 2023 par rapport à 2021, mais leurs conséquences sont plus importantes (figure 3). Les personnes interrogées indiquent en effet une augmentation des interruptions de réseau, des pertes de données et des atteintes à la réputation. Autant d'éléments qui augmentent considérablement les enjeux pour les équipes de sécurité. L'effet de cette pression se fait également sentir en termes de stratégie : le nombre d'entreprises qui mettent continuellement à jour leurs stratégies ou politiques de cybersécurité est passé de 5 % en 2021 à 13 % en 2023, non seulement en réponse aux ransomwares mais aussi à une surface d'attaque en constante évolution. La dispersion des collaborateurs et les applications et données qui migrent vers le cloud ne sont que deux facteurs parmi d'autres qui influent sur la stratégie de sécurité au quotidien.

Entreprises qui ont segmenté plus de deux actifs/domaines par pays

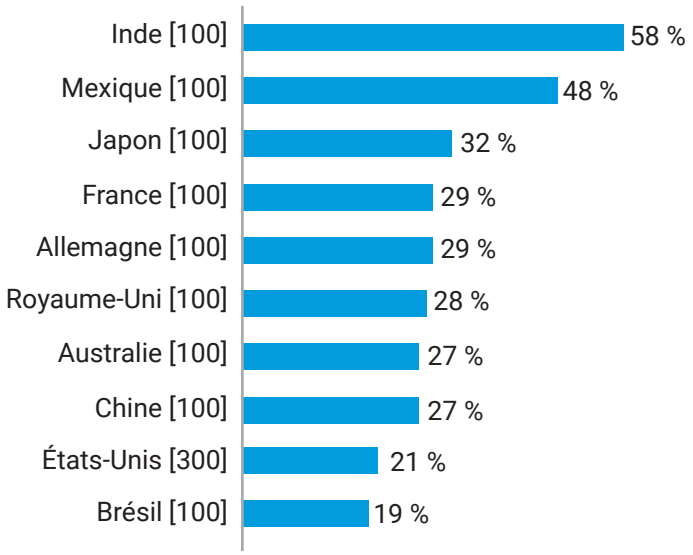

Figure 2 : Pour chacune des mesures de sécurité informatique suivantes, quels actifs couvrent-elles, le cas échéant ? [1 200], s'agissant des réponses pour la mesure de sécurité de la segmentation uniquement, et des pourcentages qui utilisent la segmentation pour protéger les actifs clés, répartis par pays.

Conséquences des ransomwares/cyberattaques

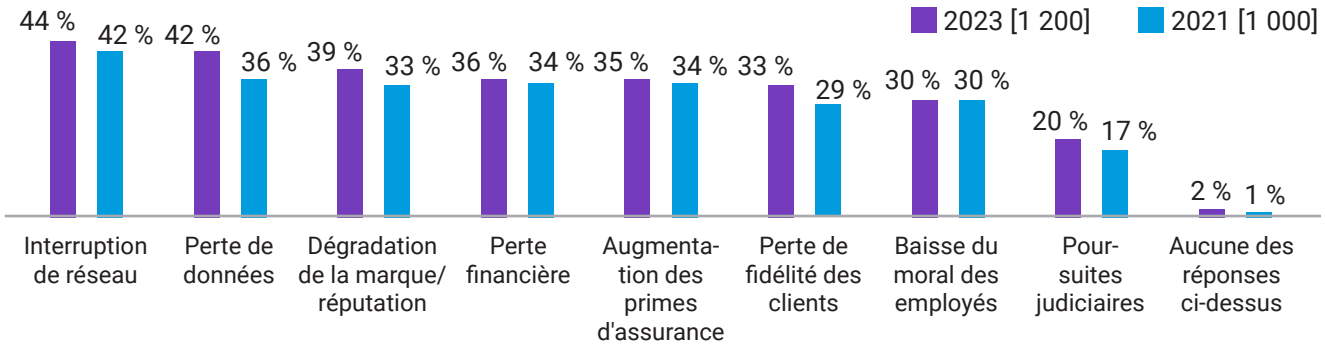

Figure 3 : Lorsque votre entreprise a déjà détecté un ransomware ou une autre cyberattaque, quelles conséquences cela a-t-il eu sur votre entreprise ? [Tailles de la base dans le graphique], seulement certaines options de réponse sont indiquées, en fonction des données historiques.

Points à retenir pour chaque région

Les cyberattaquants sont plus susceptibles de cibler les pays d'Amérique : le nombre total d'attaques par ransomware est le plus élevé dans les Amériques, avec 96 attaques en moyenne au cours des 12 derniers mois, contre 83 dans la région EMEA et 75 dans la région APAC.

La segmentation et la microsegmentation sont considérées comme plus importantes dans les régions APAC et Amériques que dans la région EMEA : les équipes de sécurité informatique et les décideurs de l'APAC (62 %) et des Amériques (60 %) sont plus susceptibles de dire que la segmentation du réseau est extrêmement importante pour assurer la sécurité de leur entreprise que ceux de l'EMEA (53 %).

Les décideurs des Amériques sont plus enclins à dire que la microsegmentation est la priorité absolue (41 %) que leurs homologues de l'APAC (35 %) ou de l'EMEA (23 %).

Les équipes de sécurité informatique et les décideurs de la région EMEA sont plus susceptibles de ne pas avoir segmenté du tout : les entreprises sont beaucoup plus susceptibles de dire qu'aucun actif critique n'a été segmenté dans la région EMEA (10 %) que dans la région APAC (4 %) ou dans la région Amériques (1 %).

Les taux de déploiement les plus faibles, c'est-à-dire ceux où aucun domaine n'a été segmenté, ont été observés au Royaume-Uni (23 %), l'équipement existant étant considéré comme le principal obstacle (46 %).

Les entreprises de l'APAC sont celles qui ont le plus segmenté : les entreprises de la région APAC sont plus susceptibles d'avoir segmenté plus de deux actifs critiques (36 %) que celles de la région EMEA (29 %) ou des Amériques (26 %).

Dans toutes les régions, les entreprises sont confrontées à des défis : 97 % des entreprises des Amériques déclarent rencontrer des problèmes lors de la segmentation de leur réseau. Le même pourcentage est observé dans les régions EMEA (94 %) et APAC (97 %).

Les entreprises des régions EMEA et APAC citent le manque de compétences/expertise (38 % et 43 %) comme étant leur principal obstacle à la segmentation. Pour celles des Amériques, le plus grand obstacle est l'augmentation des goulots d'étranglement en matière de performances (41 %).

Les entreprises des Amériques sont plus nombreuses à considérer que leurs cadres de sécurité Zero Trust sont matures : les entreprises des Amériques sont plus susceptibles de dire que leur déploiement Zero Trust est entièrement achevé et défini (49 %) que celles de l'APAC (35 %) ou de l'EMEA (33 %).

La segmentation largement reconnue comme une partie importante du Zero Trust

Les personnes interrogées s'accordent à dire que la segmentation est importante pour garantir la sécurité de leur entreprise, en particulier pour lutter contre les logiciels malveillants. Dans tous les secteurs d'activité, 93 % estiment que la segmentation est essentielle pour contrecarrer les attaques dévastatrices, un chiffre qui atteint 99 % dans les secteurs de la fabrication et de la production. Cela pourrait être dû au fait que ces secteurs dépendent fortement d'un certain nombre de tiers dans leur chaîne d'approvisionnement, de sorte qu'une perturbation peut avoir des effets en cascade considérables sur l'entreprise.

La segmentation contribue également de manière importante à une structure Zero Trust. Lors de l'évocation des raisons pour lesquelles leur entreprise a lancé un projet de segmentation, la troisième réponse la plus fréquente est la volonté de faire progresser le Zero Trust : la quasi-totalité des entreprises qui ont procédé à une segmentation déploie ou a déjà déployé un cadre de sécurité Zero Trust (99 %), même si seulement deux sur cinq (40 %) indiquent que leur structure Zero Trust est entièrement définie et achevée.

À l'échelle mondiale, la majorité des personnes interrogées souhaite aller plus loin et mettre en œuvre la microsegmentation, qui protège les charges de travail des applications à un niveau granulaire : 89 % déclarent que la microsegmentation est au moins une priorité élevée, 34 % la désignant comme leur priorité absolue.

En outre, 97 % des équipes de sécurité informatique et des décideurs déclarent qu'elle a été adoptée par au moins une minorité de leur secteur d'activité. Ce chiffre tombe à 80 % dans le secteur public (à l'exclusion des soins de santé), une différence qui peut s'expliquer par des budgets plus serrés et une infrastructure existante qui constituent des obstacles plus importants au déploiement de la protection au niveau de la charge de travail de la microsegmentation.

Microsegmentation

des équipes de sécurité informatique et des décideurs déclarent que la microsegmentation a été adoptée par au moins une minorité de leur secteur d'activité

Mais le secteur public a tout à gagner à mettre en œuvre des techniques de sécurité avancées telles que la microsegmentation. Comme les systèmes de ce secteur ne sont pas nécessairement conçus pour interagir les uns avec les autres, ils manquent d'interopérabilité, ce qui augmente à la fois le risque d'erreur humaine et la probabilité de réussite d'une cyberattaque.

Au niveau de la segmentation, 15 % des répondants du secteur public déclarent ne pas avoir de segmentation, même si 93 % reconnaissent son importance. Il s'agit du niveau de déploiement le plus faible par secteur, le principal obstacle étant les exigences de conformité (52 %).

La segmentation, c'est bien. La microsegmentation, c'est encore mieux.

La segmentation est une approche architecturale qui divise un réseau en segments plus petits dans le but d'améliorer les performances et la sécurité.

La microsegmentation divise un réseau en segments au niveau de la charge de travail individuelle, de sorte que les contrôles de sécurité et la prestation de services peuvent ensuite être définis pour chaque segment unique.

Les déploiements sont lents, mais persévérer donne des résultats transformateurs

La dure réalité, c'est que même si l'on s'accorde largement à dire que la segmentation est la clé pour stopper les attaques, le déploiement de la segmentation a été lent, et même plus lent que ce que l'on pouvait attendre. Seulement 30 % des entreprises ont segmenté plus de deux secteurs d'activité critiques en 2023 (contre 25 % en 2021), et 44 % ont lancé un projet de segmentation du réseau il y a deux ans ou plus, ce qui suggère que les efforts en la matière ont stagné.

La lenteur des déploiements s'explique le plus clairement par les principaux obstacles rencontrés par les personnes interrogées : le manque de compétences/expertise en matière de segmentation (39 %), l'augmentation des goulots d'étranglement au niveau des performances (39 %) et les exigences en matière de conformité (38 % ; figure 4). Presque toutes les personnes interrogées, quel que soit le secteur, l'industrie ou le pays, ont signalé les mêmes obstacles à des degrés légèrement différents. Il est intéressant de noter que si le manque de compétences/expertise est la première cause de retard dans les projets de segmentation, une pénurie de talents est présente dans l'ensemble de la cybersécurité, et à l'allure à laquelle les changements dans ce domaine se produisent, les lacunes en matière de compétences ne peuvent qu'être présentes.

Malgré la lenteur des progrès, les taux de segmentation augmentent progressivement dans l'ensemble. Le pourcentage d'entreprises ayant des applications/données critiques segmentées a augmenté de 12 % et les serveurs segmentés ont augmenté de 8 % entre 2021 et 2023.

Obstacles rencontrés lors de la segmentation du réseau

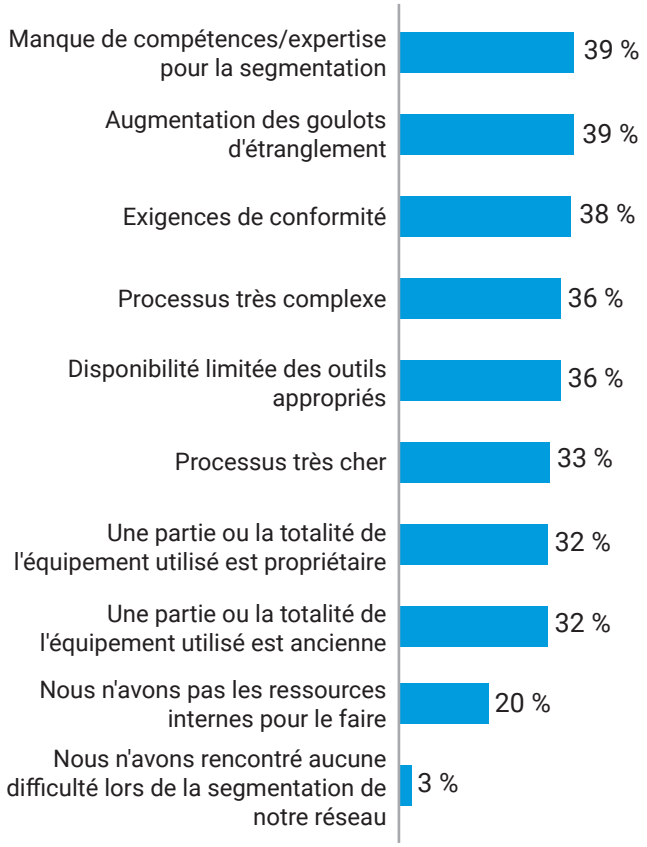

Figure 4 : Quels problèmes, le cas échéant, votre entreprise a-t-elle rencontrés/prévoit-elle lors de la segmentation du réseau ? [1187], s'agissant uniquement de celles qui ont segmenté leur réseau à un moment donné, avec seulement certaines options de réponse.

Conclusion : segmenter six secteurs d'activité critiques réduit considérablement les risques

La protection et la segmentation d'un plus grand nombre d'actifs renforcent immédiatement la sécurité des entreprises. Les équipes de sécurité sont plus à même d'identifier les attaques et d'y réagir beaucoup plus efficacement. La mise en œuvre de stratégies de segmentation immatures ou mal définies ne fait qu'augmenter le risque pour une entreprise. Mais lorsqu'elle est bien faite, la segmentation vaut clairement la peine de surmonter les obstacles et d'être mise en œuvre.

Nos résultats montrent qu'après une violation, la récupération prend 11 heures de moins avec la segmentation. Faisons le calcul : pour les entreprises qui ont mis en place une segmentation dans six secteurs critiques, il faut en moyenne quatre heures pour stopper complètement une attaque par ransomware ; pour celles qui ont mis en place une segmentation sur un seul actif, il faut 15 heures.

De même, la segmentation permet de gagner 11 heures en limitant les mouvements latéraux. Pour les entreprises qui ont mis en place une segmentation dans les six secteurs critiques, il faut en moyenne trois heures pour limiter de manière significative le mouvement latéral d'une attaque par ransomware. Pour celles n'ayant segmenté qu'un seul actif, cela prend en moyenne 14 heures.

Réfléchissez à ce que représentent ces 11 heures pour votre équipe et pour contenir les coûts et les dommages causés à la marque dans ces deux scénarios.

Pour arrêter une attaque

4 heures

Le temps qu'il faut, en moyenne, pour arrêter complètement une attaque par ransomware, lorsque les six actifs de l'entreprise ont été segmentés

Lorsqu'un seul actif a été segmenté : **15 heures**

Pour limiter les mouvements

3 heures

Le temps qu'il faut, en moyenne, pour limiter de manière significative le mouvement latéral d'une attaque par ransomware, lorsque les six actifs de l'entreprise ont été segmentés

Lorsqu'un seul actif a été segmenté : **14 heures**

Comment une solution de microsegmentation logicielle aide à relever les défis

La microsegmentation permet non seulement une segmentation plus avancée et plus granulaire, mais elle est également plus facile à mettre en œuvre.

Les solutions logicielles, comme Akamai Guardicore Segmentation, peuvent être déployées rapidement sans apporter de modifications physiques au réseau. Il n'est pas nécessaire d'attribuer une nouvelle plage IP à vos nouveaux segments ou de vous préoccuper de l'emplacement physique de vos serveurs et de vos terminaux. Cette solution est donc beaucoup plus rapide et facile à déployer que les approches basées sur l'infrastructure telles que les pare-feu et les VLAN. Et puisque la solution utilise son propre pilote propriétaire pour l'application des règles, elle fonctionne de manière fluide sur toutes les machines et tous les systèmes d'exploitation : des serveurs bare metal aux déploiements multicloud, des technologies héritées comme Windows Server 2003 aux derniers terminaux IoT/OT et à la technologie conteneurisée. Cela signifie que vous ne gérez qu'une seule solution avec une seule interface pour visualiser et contrôler les connexions établies par différents systèmes d'exploitation et terminaux dans l'ensemble de votre environnement, quel que soit leur emplacement physique.

Comment elle facilite le déploiement

La microsegmentation génère d'abord un visuel interactif de toutes les connexions établies dans votre environnement, ce qui est un composant essentiel pour surmonter les principaux obstacles au déploiement. En outre, Akamai a intégré dans sa solution des moyens actifs de remédier aux goulots d'étranglement des performances et de respecter les exigences de conformité.

Les goulots d'étranglement des performances ne résultent pas nécessairement d'une contrainte technique exercée sur un système par une solution de segmentation, mais de goulots d'étranglement au niveau de la main-d'œuvre, causés par la nécessité de segmenter manuellement les secteurs d'activité, puis de dépanner manuellement ces secteurs en cas de dysfonctionnement. Akamai s'efforce de résoudre ce problème, ainsi que le principal obstacle au déploiement, le manque d'expertise, en réduisant la nécessité de segmenter manuellement et en offrant un support technique et des services professionnels de premier plan. Nos experts en segmentation vous accompagnent tout au long du processus de déploiement pour vous permettre d'atteindre vos objectifs de segmentation dans l'environnement informatique qui vous est propre.

La prise en charge du déploiement provient également de la solution elle-même : ses recommandations de règles basées sur l'IA et ses modèles de règle prêts à l'emploi pour les scénarios d'utilisation courants permettent d'économiser du temps et des clics, de simplifier le flux de travail, de réduire le temps global de mise en œuvre de la règle et d'éviter les erreurs de configuration dues à l'erreur humaine. Pour l'un de nos clients, nous avons pu livrer un projet de segmentation granulaire estimé à deux ans et à plus de 1 million de dollars de coûts totaux en seulement six semaines avec un seul ingénieur, réduisant ainsi le coût global du projet de 85 %, ce qui prouve que la segmentation granulaire peut être déployée rapidement et facilement, sans souffrir de goulots d'étranglement.

Comment elle facilite la conformité

Nombre de nos clients déploient notre solution pour garantir et attester la conformité à un certain nombre de mandats de conformité nationaux et internationaux, tels que la norme PCI-DSS, la SWIFT, la loi Sarbanes-Oxley, la norme HIPAA, le RGPD et bien plus encore. Ces mandats de conformité exigent généralement que les données du champ d'application soient séparées des autres systèmes de votre environnement. Si l'utilisation de pare-feu et de VLAN peut s'avérer prohibitive, notre solution logicielle vous permet de créer des segments spécifiques pour les données du champ d'application et d'appliquer des règles de communication sur ce qui peut ou ne peut pas accéder à ces données. En utilisant notre carte visuelle avec des vues historiques et en temps quasi réel, vous pouvez attester de votre conformité à ces mandats en montrant physiquement que les données dans le champ d'application ne sont pas accessibles par des utilisateurs et des machines non autorisés.

Persévérez avec la bonne solution et le bon support pour transformer votre approche en matière de sécurité

La segmentation peut être extrêmement difficile à mettre en œuvre. Mais comme le montre ce rapport, ceux qui parviennent à la mettre en œuvre efficacement constatent une réduction massive de leurs cyberrisques. La mise en place d'une segmentation adéquate limite le déplacement latéral des menaces et vous permet de réagir plus rapidement en cas de violation active. Et après une violation, les efforts de récupération sont sécurisés et prennent moins de temps.

Le choix d'une solution conçue pour surmonter les défis courants liés au déploiement de la segmentation, et le partenariat avec des experts fournis au cours de ce parcours, vous place dans la meilleure position possible pour transformer votre posture de sécurité. En outre, plus vous segmentez de secteurs d'activité, plus vous faites progresser votre architecture Zero Trust, en réduisant les risques actuels et en assurant une défense de première ligne contre les futurs vecteurs de menace.

Notre panel

Nous avons interrogé 1 200 décideurs informatiques et de sécurité dans 10 pays, afin de mesurer les progrès réalisés par les entreprises dans la sécurisation de leurs environnements, en mettant l'accent sur le rôle de la segmentation.

Ils ont été interrogés sur leurs approches de la sécurité informatique, leurs stratégies de segmentation et sur les menaces auxquelles leur entreprise sera confrontée en 2023. Ces résultats nous donnent un aperçu de la manière dont les stratégies de sécurité ont évolué depuis 2021 et des domaines dans lesquels des progrès restent à faire.

Nous avons interrogé du personnel de sécurité et des décideurs des États-Unis, du Mexique, du Brésil, du Royaume-Uni, de la France, de l'Allemagne, de la Chine, de l'Inde, du Japon et de l'Australie. Tous travaillaient pour des entreprises de plus de 1000 employés et représentaient un éventail équilibré d'industries et de secteurs.

Remarque : cet échantillon différait légèrement de celui de 2021. Tailles des échantillons — 2023 : 1 200 personnes interrogées, 2021 : 1 000 personnes interrogées. En 2023, nous avons également interrogé des personnes en Australie, au Japon et en Chine. Les secteurs différaient légèrement de ceux de 2021. En 2023, nous nous sommes particulièrement concentrés sur le commerce digital comme secteur à part entière.

En savoir plus sur Akamai Guardicore Segmentation

Akamai protège votre expérience client, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous concevez, quel que soit l'endroit où vous le développez et où vous le diffusez. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre posture de sécurité, pour activer le Zero Trust, protéger les applications et les API, et sécuriser votre infrastructure, en vous donnant la confiance nécessaire pour innover, vous développer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de sécurité, de traitement et de diffusion d'Akamai, consultez les sites akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 10/23.

VansonBourne

Vanson Bourne est un spécialiste indépendant des études de marché pour le secteur technologique. Sa réputation d'analyse rigoureuse et fiable est fondée sur des principes de recherche stricts et sur sa capacité à recueillir l'avis de cadres dirigeants dans toutes les fonctions techniques et commerciales, dans tous les secteurs d'activité et sur tous les grands marchés. Pour plus d'informations, rendez-vous sur www.vansonbourne.com.