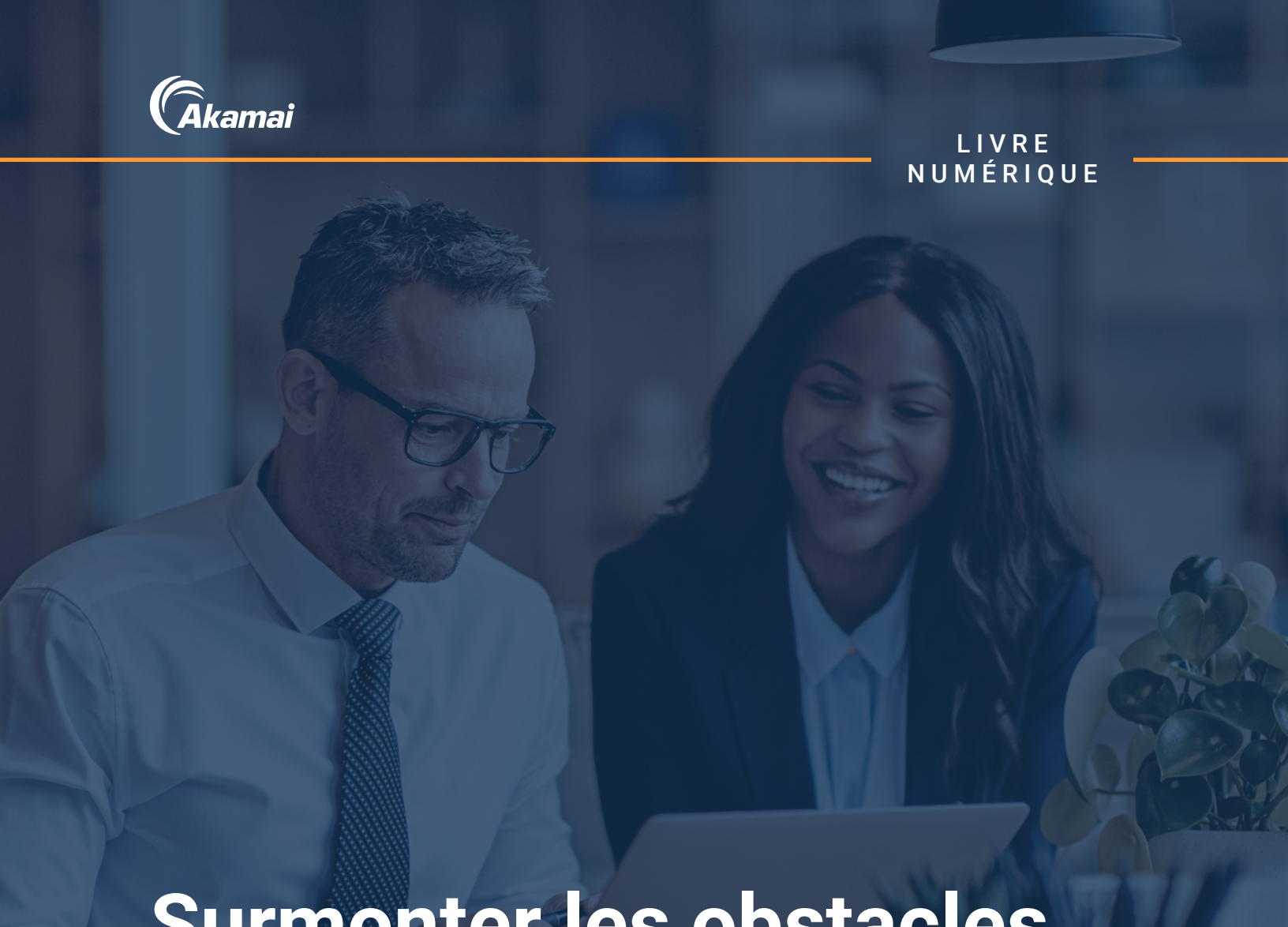
Akamai

LIVRE NUMÉRIQUE



Surmonter les obstacles au déploiement pour protéger les systèmes bancaires critiques

Rapport global sur l'état de la segmentation

Table des matières

Introduction

La protection du secteur des services financiers a toujours posé des défis importants et uniques aux équipes chargées de la sécurité informatique. Toutefois, des attaquants de plus en plus sophistiqués combinent maintenant des techniques pour générer des menaces plus importantes et plus fréquentes, ce qui met les équipes responsable de la sécurité des institutions de services financiers sous une pression sans précédent. Les institutions de services financiers s'appuient sur une présence digitale pour fonctionner 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 des conséquences plus importantes, 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, ou risquer d'exposer de grandes quantités de données sensibles.

Les personnes interrogées dans les institutions de services financiers (représentées dans toutes les régions, y compris les États-Unis, l'Amérique latine, la région EMEA et la région Asie-Pacifique) s'accordent majoritairement sur l'efficacité de la segmentation pour assurer la protection des actifs, mais les progrès globaux dans le déploiement de la segmentation autour des applications et des actifs critiques de l'entreprise sont plus faibles que prévu. L'obstacle numéro un pour les institutions de services financiers a été l'augmentation des goulots d'étranglement, ce qui suggère que les équipes ont peut-être réagi aux menaces sans avoir le temps ou le soutien nécessaire pour bien comprendre et atténuer les conséquences sur les performances résultant des changements.

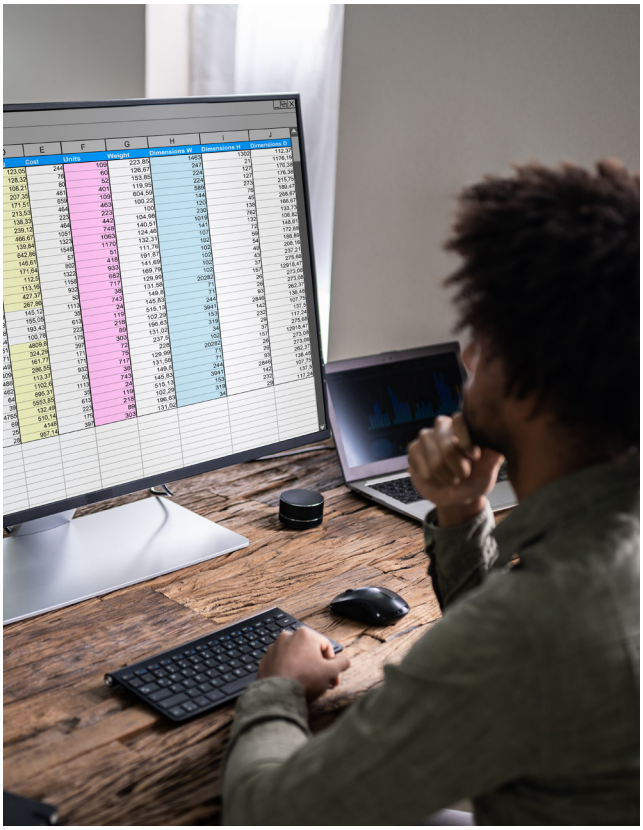
La bonne nouvelle ? La persévérance paie. Pour ceux qui avaient segmenté la plupart de leurs actifs critiques, la segmentation s'est avérée avoir un effet transformateur sur la défense, leur permettant d'atténuer et de contenir les ransomwares avec 13 heures d'avance par rapport à ceux qui n'avaient segmenté qu'un seul actif. Imaginez la ifférence que ces 13 heures représentent pour votre équipe, vos clients et la réputation de votre marque.

Résultat : la segmentation a progressé lentement dans l'ensemble, mais ceux qui ont persévéré ont considérablement réduit leur risque.

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 est une technique de sécurité qui permet de diviser logiquement un réseau en segments de sécurité distincts, jusqu'au niveau de la charge de travail individuelle. Les contrôles de sécurité et la prestation de services peuvent alors être définis pour chaque segment unique.



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

Le nombre d'attaques par ransomware dans les institutions de services financiers (qu'elles soient réussies ou non) a augmenté de près de 50 % au cours des deux dernières années, passant de 43 en moyenne en 2021 à 62 en 2023. Malgré la réputation du secteur pour ses mesures de sécurité robustes, ces chiffres soulignent une vulnérabilité critique qui ne peut être négligée. Il est évident que le secteur des services financiers n'est pas à l'abri de la menace des ransomwares, et il n'est pas envisageable de faire preuve de complaisance.

Les institutions de services financiers de la région Asie-Pacifique ont été la cible du plus grand nombre d'attaques par ransomware en moyenne (73), et celles de la région Amérique latine du plus petit nombre (48, figure 1).

Nombre moyen d'attaques par ransomware dans le secteur des services financiers au cours des 12 derniers mois par région

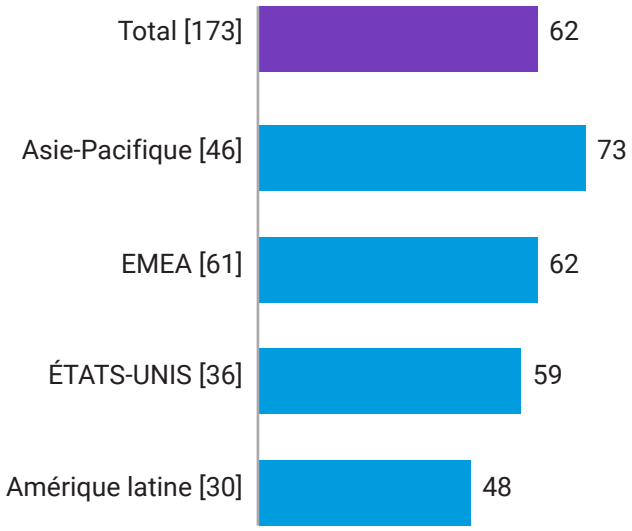


Figure 1 : Combien d'attaques par ransomware votre entreprise a-t-elle subi au cours des 12 derniers mois (qu'elles aient abouti ou non) ? Le graphique montre le nombre moyen d'attaques au cours des 12 derniers mois, réparties par région (chiffres de base indiqués), données relatives au secteur des services financiers uniquement.

Étant donné que la plupart des institutions de services financiers opèrent à l'échelle mondiale, l'augmentation du nombre d'attaques ciblées en Asie-Pacifique pourrait s'expliquer par le fait que les pirates pensent que les cibles de la région Asie-Pacifique offrent des rendements plus élevés. Toutefois, cela ne signifie pas que les institutions financières situées dans d'autres régions sont plus sûres, mais simplement qu'elles sont plus susceptibles de subir des attaques latérales provenant d'ailleurs.

En outre, les personnes interrogées dans la région Amérique latine sont les plus susceptibles de déclarer que leur institution financière a segmenté plus de deux actifs, suivies par la région Asie-Pacifique. Cela montre que les institutions financières de la région Asie-Pacifique pourraient tenter d'accroître leur segmentation à la lumière du nombre d'attaques par ransomware dont elles sont la cible.

Ceux qui ont segmenté plus de deux actifs/domaines par région dans le secteur des services financiers

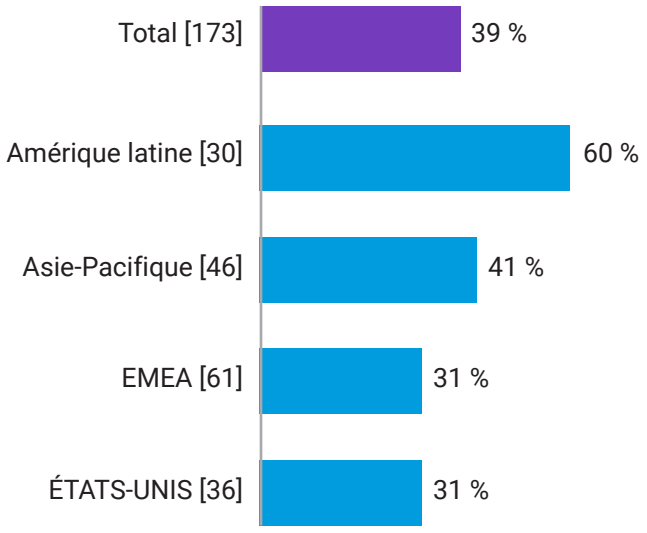


Figure 2 : Pour chacune des mesures de sécurité informatique suivantes, quels actifs couvrent-elles, le cas échéant ? Le graphique montre les réponses pour la mesure de sécurité de la segmentation uniquement, et les pourcentages qui utilisent la segmentation pour protéger les actifs clés, répartis par région (chiffres de base indiqués), données du secteur des services financiers uniquement.

Les attaques par ransomware sont non seulement plus fréquentes 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 et des pertes de données. Autant d'éléments qui augmentent considérablement les enjeux pour les équipes de sécurité. La proportion de personnes interrogées déclarant des primes d'assurance plus élevées a également augmenté, en particulier aux États-Unis (56 %). Cela démontre le niveau de risque que peuvent présenter les institutions financières, qui détiennent souvent des données non seulement sur des particuliers, mais aussi sur des entreprises.

L'effet de cette pression se fait également sentir en termes de stratégie : le nombre d'institutions de services financiers qui mettent continuellement à jour leurs stratégies ou politiques de cybersécurité est passé de 3 % en 2021 à 18 % 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.

Conséquences des ransomwares/ cyberattaques sur les institutions de services financiers

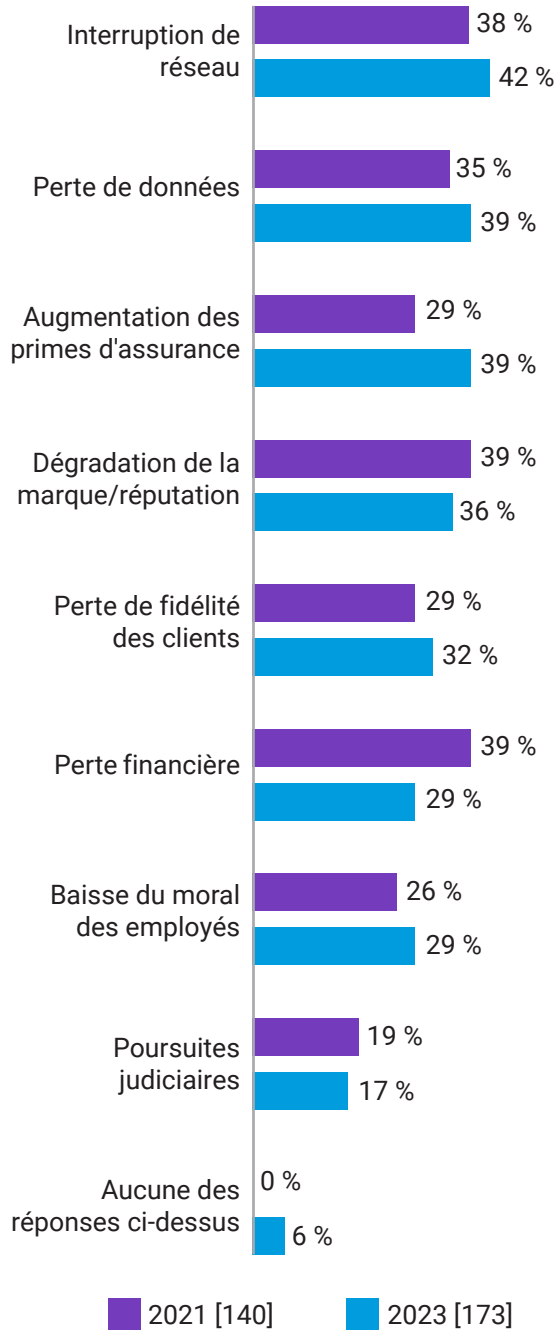


Figure 3 : Lorsque votre entreprise a déjà détecté un ransomware ou une autre cyberattaque, quelles conséquences cela a-t-il eu sur votre entreprise ? Le graphique montre les tailles de base par année, réparties selon les données historiques, données du secteur des services financiers uniquement, toutes les options de réponse ne sont pas présentées.

La segmentation est la pierre angulaire de l'approche Zero Trust

Les personnes interrogées dans le secteur des services financiers s'accordent à dire que la segmentation est importante pour garantir la sécurité de leur entreprise, en particulier pour lutter contre les logiciels malveillants : 66 % déclarent qu'elle extrêmement importante, et 92 % pensent qu'elle est essentielle pour aider à contrecarrer les attaques préjudiciables.

La segmentation contribue également de manière importante à une structure Zero Trust. Lorsqu'elles citent les raisons pour lesquelles leur entreprise a lancé un projet de segmentation, la réponse la plus fréquente de ces personnes est qu'il s'agit de faire progresser le modèle Zero Trust : la quasi-totalité des entreprises qui ont procédé à une segmentation déploient ou ont déjà déployé un cadre de sécurité Zero Trust (99 %), bien que moins de la moitié d'entre elles (47 %) déclarent que leur cadre Zero Trust est totalement complet et défini, et donc mature.

La majorité des personnes interrogées dans les institutions de services financiers aspirent à aller plus loin et à mettre en œuvre la microsegmentation, qui protège les charges de travail des applications à un niveau granulaire : 88 % déclarent que la microsegmentation est au moins une priorité élevée, 39 % la désignant comme leur priorité absolue. Les personnes interrogées dans la région Amérique latine sont les plus susceptibles de la considérer comme une priorité absolue (50 %), tandis que celles de la région EMEA sont les moins susceptibles de la considérer comme telle (31 %). Le fait que les personnes interrogées de la région Amérique latine soient plus nombreuses à déclarer qu'il s'agit d'une priorité absolue se reflète dans leurs performances (figure 1), ce qui montre que les entreprises qui accordent la priorité à la microsegmentation peuvent s'attendre à en récolter les fruits.

En outre, 99 % des décideurs informatiques de ce secteur déclarent que la microsegmentation a été adoptée par au moins une minorité de leur secteur, ce qui souligne qu'il s'agit d'une solution à laquelle presque tous sont sensibilisés.

La persévérance produit 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 39 % des institutions de services financiers ont segmenté plus de deux secteurs d'activité critiques en 2023 (contre 26 % en 2021), et 45 % 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.

Cette lenteur s'explique le plus clairement par les principaux obstacles rencontrés par les personnes interrogées : goulots d'étranglement accrus au niveau des performances (41 %), manque de compétences/connaissances en matière de segmentation (39 %) et exigences en matière de conformité (35 %). Il est intéressant de noter que si le manque de ressources ou de connaissances est l'une des principales raisons du retard des projets de segmentation, la 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.

Toutefois, lorsqu'on les répartit par région (voir fig. 4), on observe des variations dans les obstacles les plus susceptibles d'être rencontrés. Cela montre que certaines questions peuvent être motivées autant, sinon plus, par des conditions locales (par ex. le manque de compétences aux États-Unis, les problèmes de conformité dans la région Asie-Pacifique) que par des questions globales.

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 17 % et les serveurs segmentés ont également augmenté de 17 % entre 2021 et 2023. Ces augmentations dépassent les moyennes globales observées dans tous les secteurs (12 % et 8 %, respectivement), ce qui montre que les départements informatiques des institutions de services financiers sont un peu plus aptes que la plupart des autres à surmonter les obstacles rencontrés. Cela peut s'expliquer par le fait que les exigences de conformité généralement strictes mentionnées ci-dessus requièrent un niveau de sécurité de plus en plus élevé. Cela pourrait également être lié à l'augmentation des primes d'assurance à laquelle les institutions de services financiers ont été confrontées. Les assureurs pourraient exiger de leurs clients qu'ils soient en mesure de résoudre certains problèmes le plus rapidement possible.

Obstacles rencontrés lors de la segmentation du réseau dans le secteur des services financiers.- les trois principaux obstacles par région

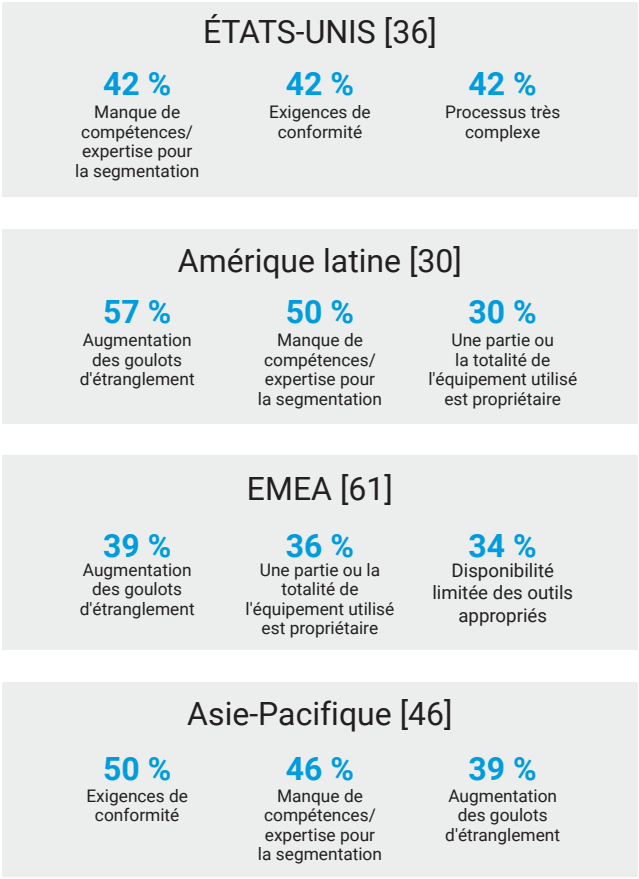


Figure 4 : Quels problèmes, le cas échéant, votre entreprise a-t-elle rencontrés/prévoit-elle lors de la segmentation du réseau ? Le graphique montre la taille des bases par région, la question n'est posée qu'à ceux qui ont segmenté leur réseau à un moment ou à un autre. Seules les trois premières réponses sélectionnées par région sont présentées et seules les données du secteur des services financiers sont prises en compte.

Les entreprises qui ont segmenté six secteurs d'activité critiques ont énormément réduit leurs risques

La protection et la segmentation d'un plus grand nombre d'actifs renforcent immédiatement la sécurité des institutions financières. 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 non matures ou mal définies ne fait qu'accroître la vulnérabilité, mais lorsqu'elle est bien exécutée, la segmentation améliore la cyber-résilience et empêche les cyberattaques de provoquer des échecs commerciaux majeurs en bloquant la propagation des ransomwares et des violations aux systèmes et aux données essentielles.

Nos résultats montrent qu'après une violation, la récupération prend 13 heures de moins avec la segmentation. Faisons le calcul : pour les institutions de services financiers qui ont mis en place une segmentation dans six domaines critiques, il faut en moyenne trois heures pour stopper complètement une attaque par ransomware. Pour celles n'ayant segmenté qu'un seul actif, cela prend 16 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.

Pensez à la différence que cela représente pour votre équipe, les dommages causés à la marque et les coûts encourus pendant ces 11 à 13 heures, selon le scénario.

Pour arrêter une attaque

3 heures

C'est 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 : **16 heures**

Pour limiter les mouvements

3 heures

C'est 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

Les institutions financières cherchent à améliorer l'évolutivité, à tirer parti des investissements existants, à optimiser les coûts et à améliorer l'agilité et la flexibilité en migrant les charges de travail vers le cloud, souvent en intégrant des centres de données sur site avec des clouds privés ou publics. Les solutions de segmentation définies par logiciel, telles que Akamai Guardicore Segmentation, se sont imposées comme une approche flexible, rationalisée et rentable de la sécurité au niveau des applications, accélérant considérablement la mise en œuvre, simplifiant la maintenance et atténuant efficacement les menaces. Parce qu'elle est plus rapide et plus facile à déployer que les approches basées sur l'infrastructure telles que les pare-feux et les VLAN, elle permet aux institutions financières d'assurer une sécurité à grande échelle tout en répondant aux exigences croissantes de leur activité et en offrant des expériences innovantes à leurs clients grâce à des technologies de pointe. En outre, elle fonctionne de manière transparente sur divers systèmes et environnements, offrant une gestion et un contrôle centralisés, des serveurs dédiés physiques (bare-metal) aux déploiements multicloud en passant par les systèmes hérités. Elle offre donc une solution unifiée pour visualiser et contrôler les connexions dans l'ensemble de l'environnement, quel que soit l'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 la microsegmentation facilite la conformité

Nombre de nos clients déploient notre solution pour garantir et attester la conformité à un certain nombre de directives relatives à la conformité, comme la norme PCI-DSS, la SWIFT, la loi Sarbanes-Oxley, le RGPD, DORA et bien plus encore. Ces directives réglementaires exigent généralement que les données du champ d'application soient séparées des autres systèmes de votre environnement. Si l'utilisation de pare-feux 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 directives 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 posture de sécurité

La segmentation peut être complexe. Mais comme le montre ce rapport, ceux qui parviennent à la mettre en œuvre efficacement constatent une amélioration de la sécurité et des performances du réseau, une meilleure conformité et une simplification de la gestion du réseau. 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.

Points à retenir pour chaque région

La segmentation et la microsegmentation sont plus importantes dans la zone EMEA et aux États-Unis qu'en Amérique latine : les décideurs en matière de sécurité informatique de l'EMEA (70 %) et des États-Unis (60 %) sont plus susceptibles de dire que la segmentation du réseau est extrêmement importante pour assurer la sécurité de leur entreprise que ceux d'Amérique latine (57 %).

Ceux de la région Amérique latine sont plus enclins à dire que la microsegmentation est la première priorité (50 %) que leurs homologues aux États-Unis (42 %), dans la région Asie-Pacifique (41 %) et dans la région EMEA (31 %).

Les décideurs de la région EMEA sont plus susceptibles de ne pas avoir segmenté du tout : les décideurs de la zone EMEA sont plus susceptibles de dire qu'aucun actif stratégique n'a été segmenté (7 %), alors que toutes les autres régions l'ont fait dans une certaine mesure.

Les décideurs d'Amérique latine sont les plus susceptibles d'avoir fait le plus de progrès en matière de segmentation : les entreprises de services financiers de la région Amérique latine sont plus susceptibles d'avoir segmenté plus de deux actifs critiques (60 %) que ceux de la région Asie-Pacifique(41 %), de la région EMEA (31 %) et des États-Unis (31 %).

Dans toutes les régions, les entreprises sont confrontées à des défis : 98 % des personnes interrogées dans la région Asie-Pacifique déclarent rencontrer des problèmes lors de la segmentation de leur réseau. Le pourcentage est similaire aux États-Unis (97 %), mais un peu moins élevé dans la région EMEA (89 %) et dans la région Amérique latine (87 %).

Les institutions de services financiers de la région Amérique latine sont beaucoup plus matures en ce qui concerne le déploiement de leur cadre de sécurité Zero Trust : les entreprises d'Amérique latine sont plus susceptibles de dire que leur déploiement Zero Trust est entièrement achevé et défini (57 %) que celles de l'EMEA (48 %), des États-Unis (47 %) ou d'Asie-Pacifique (41 %).

Notre panel

Pour l'étude globale, 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 informations et 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.

Les personnes interrogées proviennent du monde entier, notamment des États-Unis, de l'Inde, du Mexique, du Brésil, du Royaume-Uni, de la France, de l'Allemagne, de la Chine, du Japon et de l'Australie. Elles provenaient d'entreprises comptant plus de 1 000 employés, ainsi que d'un éventail de secteurs et d'industries.

Pour les besoins de ce rapport, nous avons analysé les réponses de 173 (2023) et 140 (2021) personnes travaillant dans le secteur des services financiers.

En savoir plus sur Akamai Guardicore Segmentation

Akamai soutient et protège la vie en ligne. Les entreprises leaders du monde entier choisissent Akamai pour concevoir, diffuser et sécuriser leurs expériences digitales, et aident des milliards de personnes à vivre, travailler et jouer chaque jour. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions Akamai pour les institutions financières, rendez-vous sur akamai.com/finserv et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 05/24.

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.