Akamai

LIVRE NUMÉRIQUE


# État de la segmentation

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

**Secteur du commerce électronique**

# Table des matières



# Introduction

Les équipes chargées de la sécurité informatique, en particulier celles qui défendent les entreprises de commerce électronique, n'ont jamais eu la tâche facile. Traditionnellement, les budgets plus serrés et les ressources limitées en matière de sécurité ont obligé les défenseurs de l'entreprise à faire plus avec moins. Mais aujourd'hui, des attaquants très motivés et sophistiqués, associés à la gestion d'une infrastructure de plus en plus complexe, soumettent les équipes de sécurité à une pression plus forte que jamais pour atténuer les risques. Pour fonctionner, les entreprises de commerce électronique ont besoin d'une présence en ligne performante. De ce fait, une violation réussie, comme une attaque par ransomware, pourrait causer des dommages importants, voire irréparables, à la réputation de la marque et au chiffre d'affaires. Imaginez les conséquences négatives si les opérations en ligne, l'exécution des commandes ou les chaînes de production s'arrêtaient parce que les serveurs et les systèmes essentiels devenaient indisponibles en raison d'un chiffrement massif, et éventuellement d'une double extorsion du fait d'une exfiltration de données.

Comme le montrent les conclusions de ce rapport sur l'état de la segmentation pour le commerce électronique, ces attaques ont également des conséquences plus importantes, ce qui oblige les dirigeants à choisir les bons outils et les bonnes solutions pour assurer la sécurité des données critiques, sans sacrifier les performances ni alourdir les coûts d'exploitation. Selon le rapport, le commerce électronique est le secteur d'activité le plus ciblé parmi tous les participants à l'enquête, ce qui souligne l'urgence de prévenir, de détecter et de répondre aussi rapidement que possible à une attaque par ransomware afin d'en limiter les répercussions.

Les personnes interrogées dans les entreprises du secteur du commerce électronique (représentant toutes les régions, y compris les États-Unis, l'Amérique latine, EMEA et Asie-Pacifique) s'accordent en grande majorité sur l'efficacité de la segmentation pour assurer la protection des actifs informatiques, mais les progrès mondiaux dans le déploiement de la segmentation autour des applications, serveurs et systèmes critiques de l'entreprise sont plus faibles que prévu. Les principaux obstacles auxquels se heurtent les entreprises de commerce électronique sont le manque de connaissances pour déployer la segmentation de manière efficace, ainsi que les lourdes exigences en matière de conformité des données. Cela montre que non seulement les équipes luttent pour recruter ou retenir les talents nécessaires à leur secteur, mais qu'elles peuvent également constater qu'un temps précieux est consacré à essayer de garantir la conformité avec la législation, ce qui consomme encore plus de ressources déjà limitées.

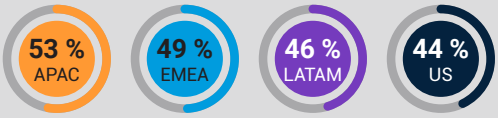
La bonne nouvelle ? Persévérer et choisir la bonne solution porte ses fruits. Pour ceux qui avaient réussi à segmenter la plupart de leurs actifs essentiels dans six domaines clés, la segmentation s'est avérée avoir un effet transformateur sur les capacités défensives, leur permettant d'atténuer et de contenir les ransomwares 11 heures plus rapidement que ceux qui n'avaient segmenté qu'un seul actif. Imaginez la différence que ces 11 heures peuvent faire non seulement pour vos intervenants, mais aussi pour vos clients et la réputation de votre marque.

# Dans l'ensemble, la segmentation a progressé lentement, 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 la sécurité et de réduire les risques associés aux réseaux plats. Elle a également été utilisée pour réduire la portée, le coût et la difficulté d'atteindre et de maintenir la conformité PCI pour les entreprises axées sur le commerce électronique.

La microsegmentation est une technique de sécurité définie par logiciel qui divise logiquement un réseau en segments de sécurité distincts jusqu'au niveau de la charge de travail ou du processus individuel (couche 7). Les contrôles de sécurité et la fourniture de services peuvent alors être définis pour chaque segment unique à un niveau plus granulaire par rapport aux méthodes de segmentation traditionnelles telles que les VLAN, les ACL et les pare-feux internes qui n'offrent qu'un contrôle de couche 4. C'est pourquoi 94 % des personnes interrogées sur le commerce électronique préfèrent les solutions de segmentation basées sur des logiciels aux méthodes traditionnelles.




Les décideurs en matière de sécurité de la région Asie-Pacifique sont plus enclins à dire que la segmentation du réseau est extrêmement importante pour garantir la sécurité de leur organisation que ceux de l'EMEA, d'Amérique latine ou des États-Unis. Les décideurs de la région Amérique latine sont plus enclins à dire que la microsegmentation est la priorité absolue (42 %) que leurs homologues de la région Asie-Pacifique (35 %), des États-Unis (34 %) et de la région EMEA (26 %).

## Le commerce électronique est le secteur le plus ciblé et les attaques par ransomware continuent d'augmenter

Le nombre d'attaques par ransomware dans les entreprises de commerce électronique (qu'elles aient réussi ou non) est en moyenne de 167 au cours des 12 derniers mois. Non seulement le commerce électronique se place en haut de la liste pour le nombre moyen d'attaques par ransomware, mais ce nombre est aussi deux fois plus important que le secteur qui le suit de près (89 attaques en moyenne).

Les pirates sont plus susceptibles de cibler les entreprises de commerce électronique aux États-Unis : le nombre d'attaques par ransomware aux États-Unis est le plus élevé de toutes les régions, avec 312 attaques en moyenne au cours des 12 derniers mois, contre 119 dans la région Asie-Pacifique, 91 dans la région EMEA et 68 dans la région Amérique latine (figure 1).

## Nombre moyen d'attaques par ransomware dans les entreprises de commerce électronique au cours des 12 derniers mois, par région

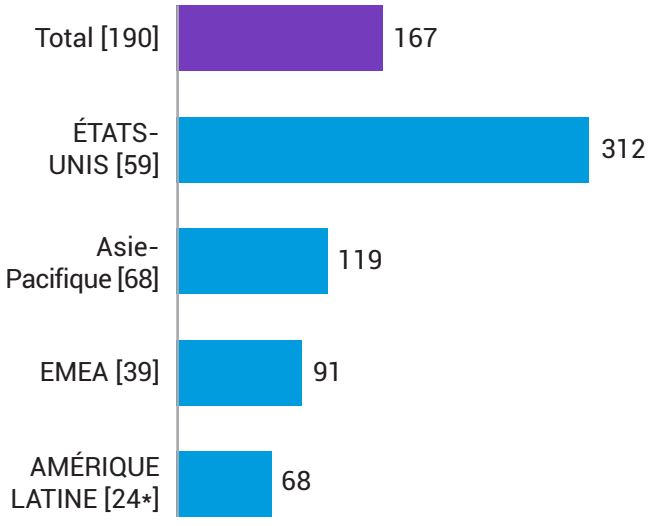



Figure 1 : Combien d'attaques par ransomware votre entreprise a-t-elle subi au cours des 12 derniers mois (qu'elles aient abouti ou non) ? Le graphique montre le nombre moyen d'attaques au cours des 12 derniers mois, par région, uniquement pour le secteur du commerce électronique.

* Attention – taille de base basse inférieure à 30

Bien que les moyennes dans les régions en dehors des États-Unis ne puissent pas être qualifiées de faibles, elles sont éclipsées par le nombre d'attaques qui se concentrent sur les États-Unis. Les États-Unis, dont l'économie est la plus importante au monde, sont le pays le plus ciblé par les ransomwares, et les pirates s'attaquent souvent à d'autres pays anglophones et occidentaux. Les motivations géopolitiques jouent également un rôle dans le choix des pays et des secteurs les plus durement touchés. Les entreprises de commerce électronique sont souvent dans le collimateur, car elles sont traditionnellement moins matures en matière de sécurité que d'autres secteurs comme les services financiers, ce qui en font des cibles plus faciles. Pour ajouter à la pression, une attaque par ransomware réussie peut être très médiatisée, en particulier si les entreprises sont touchées pendant des périodes clés génératrices de revenus telles que les vacances, les festivals, les événements sportifs, la rentrée scolaire ou d'autres périodes de forte affluence, ce qui rend le paiement plus probable, dans l'esprit de l'attaquant, si les opérations sont interrompues.

Malgré le nombre élevé d'attaques par ransomware dont les entreprises de commerce électronique sont la cible, le niveau de segmentation mis en œuvre est décevant. Seules 11 % de ces entreprises ont segmenté plus de deux domaines, un chiffre globalement cohérent dans toutes les régions. Cela indique que beaucoup de ces entreprises peuvent avoir des ressources limitées au-delà de ce qui est nécessaire pour faire face aux problèmes et aux attaques au fur et à mesure qu'ils surviennent.

Les attaques par ransomware dans le secteur du commerce électronique peuvent avoir des conséquences énormes et immédiates sur l'entreprise (figure 2) : les personnes interrogées parlent des pertes financières et des atteintes à la réputation, deux facteurs qui augmentent considérablement les enjeux pour les équipes de sécurité dans les entreprises de commerce électronique. La proportion de personnes interrogées signalant des primes d'assurance plus élevées a également augmenté. Cela démontre le niveau de risque que les entreprises de commerce électronique peuvent comporter, puisqu'elles détiennent souvent des données personnelles sur les individus et leurs habitudes d'achat, en plus des risques liés aux problèmes logistiques de stock ou d'entreposage.

Les conséquences peuvent varier selon les régions : les personnes interrogées dans la région Asie-Pacifique sont particulièrement susceptibles de mettre en avant les pertes financières, plus de la moitié d'entre elles (51 %) le faisant, alors que la moyenne générale est de 42 %. Les personnes interrogées aux États-Unis sont toutefois les plus susceptibles de signaler des interruptions de réseau, près de la moitié d'entre elles (49 %) le faisant, alors que la moyenne générale est de 39 %. Les personnes interrogées dans l'UE sont plus susceptibles de signaler une baisse du moral des salariés parmi les conséquences (41 %, contre 36 % pour l'ensemble des personnes interrogées).

L'effet de cette pression se fait également sentir en termes de stratégie : le nombre d'entreprises de commerce électronique qui mettent continuellement à jour leurs stratégies ou politiques de cybersécurité est passé de 3 % en 2021 à 13 % en 2023, non seulement en réponse aux ransomwares mais aussi à une surface d'attaque en constante évolution. La complexité croissante de l'infrastructure à mesure que les charges de travail migrent vers le cloud ne sont que quelques-uns des facteurs de risque qui affectent les stratégies de sécurité et les équipes chargées de la sécurité au quotidien.

## Impact des ransomwares/ cyberattaques sur les entreprises de commerce électronique

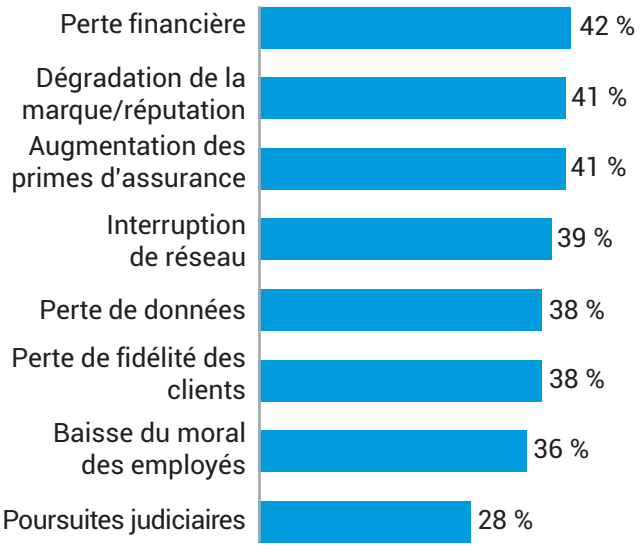



Figure 2 : Lorsque votre entreprise a déjà détecté un ransomware ou une autre cyberattaque, quelles conséquences cela a-t-il eu sur votre entreprise ? Le graphique ne montre pas toutes les options de réponse, les données du secteur du commerce électronique seulement.

# 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.


Près de la moitié (48 %) déclarent que la segmentation est extrêmement importante et 89 % pensent qu'elle est essentielle pour déjouer les attaques préjudiciables.

La segmentation est également reconnue comme la pierre angulaire d'un cadre de sécurité Zero Trust, et la bonne nouvelle pour les entreprises de commerce électronique est que des progrès ont déjà été réalisés dans ce domaine. Toutes déploient ou ont déjà déployé un cadre de sécurité Zero Trust (100 %), bien que seulement un peu plus de deux sur cinq (42 %) déclarent que leur cadre Zero Trust est totalement complet et défini, et qu'il est considéré comme mature. Il s'agit donc d'un domaine où la segmentation peut aider les entreprises de commerce électronique à progresser sur la voie du Zero Trust. D'après ces données, les entreprises américaines sont beaucoup plus matures en ce qui concerne le déploiement de leur cadre de sécurité Zero Trust : elles sont beaucoup plus nombreuses à affirmer que leur déploiement Zero Trust est totalement achevé et défini (63 %), par rapport à l'Amérique latine (46 %), l'Asie-Pacifique (32 %), et EMEA (23 %).

Les raisons qui motivent le lancement d'un projet de segmentation du réseau varient considérablement d'une région à l'autre, l'accent mis par les pouvoirs publics sur la cybersécurité arrivant en tête (41 %). La région Amérique latine et les pays de l'UE ont tous deux cité les vulnérabilités Zero Day très médiatisées comme les principales raisons de poursuivre une initiative de segmentation (par 44 % et 42 %, respectivement). Toutefois, les personnes interrogées de l'UE sont beaucoup plus nombreuses à déclarer que les projets ont été lancés parce qu'il s'agit d'une bonne pratique (41 %, contre 22 % pour l'ensemble des personnes interrogées). Les personnes interrogées des États-Unis et de la région APJ sont toutefois plus enclines à dire qu'elles ont commencé à travailler sur la cybersécurité en raison de l'importance accordée par leur gouvernement à cette question (41 % et 39 % respectivement, contre 35 % pour l'ensemble des personnes interrogées). Les personnes interrogées de la région APJ sont également plus enclines à dire que c'est le transfert d'applications critiques vers le cloud qui les a incitées à lancer un projet (39 %, contre 32 % pour l'ensemble des personnes interrogées).

La majorité des personnes interrogées dans les entreprises de commerce électronique souhaite aller plus loin et mettre en œuvre la microsegmentation, qui protège les charges de travail des applications à un niveau granulaire : 92 % déclarent que la microsegmentation est au moins une priorité élevée, 34 % la désignant comme leur priorité absolue. En outre, tous (100 %) les décideurs en matière d'informatique et de sécurité de ce secteur indiquent qu'elle a été adoptée par au moins une minorité de leur industrie, ce qui souligne qu'il s'agit d'une solution à laquelle tous sont au moins largement sensibilisés, même si les progrès ont été limités jusqu'à présent.

Les personnes interrogées ont également indiqué qu'il était nécessaire d'obtenir une meilleure visibilité de l'environnement informatique de l'entreprise. Les entreprises de la région Amérique latine déclarent avoir besoin de « beaucoup plus » de visibilité (63 %), suivies par celles de la région Asie-Pacifique (56 %), des États-Unis (46 %) et de la région EMEA (44 %), sur les communications réseau, l'emplacement des actifs, etc. pour réduire les risques.

# Les déploiements sont lents, mais la persévérance permet d'atteindre 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 en protégeant les actifs informatiques, le déploiement de la segmentation a été lent, et même plus lent que ce que l'on pouvait attendre.

Seules 11 % des entreprises de commerce électronique ont segmenté plus de deux domaines d'activité essentiels, et 48 % ont lancé un projet de segmentation du réseau il y a deux ans ou plus, ce qui laisse supposer que les efforts sont au point mort.

**Zones essentielles**

- Applications critiques
- Applications destinées au public
- Contrôleurs de domaine
- Points de terminaison
- Serveurs
- Ressources/données commerciales critiques

Cette lenteur s'explique le plus clairement par les principaux obstacles rencontrés par les personnes interrogées : le manque de compétences/connaissances en matière de segmentation (40 %), les exigences de conformité (40 %) et l'augmentation des goulots d'étranglement en matière de performances (38 %), tous associés aux méthodes de segmentation traditionnelles. Il est intéressant de noter que si le manque de ressources/connaissances 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.

Dans toutes les régions, les entreprises de commerce électronique sont confrontées à des défis : 100 % des entreprises des États-Unis et d'Amérique latine déclarent rencontrer des problèmes lors de la segmentation de leur réseau. Elles sont presque aussi nombreuses à dire la même chose dans la région Asie-Pacifique (99 %) et dans la région EMEA (97 %).

Toutefois, la répartition par région (figure 3) fait apparaître des différences dans les obstacles les plus susceptibles d'être rencontrés. Cela montre que certains problèmes (par exemple, le manque de compétences, le respect des règles) peuvent être autant, voire plus, liés à des problèmes locaux qu'à des problèmes mondiaux.

Les entreprises des régions EMEA et Amérique latine citent le manque de compétences/connaissances (54 % pour les deux) comme étant leur principal obstacle à la segmentation. Aux États-Unis, le plus grand défi est l'augmentation des goulots d'étranglement en matière de performances (44 %), et dans la région Asie-Pacifique, ce sont les exigences de conformité (43 %) qui sont les plus susceptibles de poser problème.

| | Ont très probablement rencontré un problème | Deuxième et troisième problème le plus probable | |
|---|---|---|---|
| **ÉTATS-UNIS [59]** | Augmentation des goulots d'étranglement (44 %) | Exigences de conformité/Disponibilité limitée d'outils appropriés (41 % chacun) | |
| **AMÉRIQUE LATINE [24*]** | Manque de compétences/expertise pour la segmentation (54 %) | C'est très complexe (46 %) | Une partie/tout le matériel utilisé est propriétaire / Une partie/tout le matériel utilisé est hérité (38 % dans les deux cas) |
| **EMEA [39]** | Manque de compétences/expertise pour la segmentation (54 %) | Disponibilité limitée des outils appropriés (41 %) | Exigences de conformité/Une partie ou la totalité de l'équipement utilisé est obsolète/C'est très cher (tous 36 %) |
| **ASIE-PACIFIQUE [67]** | Exigences de conformité (43 %) | Disponibilité limitée des outils appropriés/Une partie ou la totalité de l'équipement utilisé est propriétaire/Augmentation des goulots d'étranglement au niveau des performances (37 % pour tous) | |

Figure 3 : Quels problèmes, le cas échéant, votre entreprise a-t-elle rencontrés/prévoit-elle lors de la segmentation du réseau ? Le graphique montre les entreprises ayant segmenté leur réseau à un moment ou à un autre, avec les trois premières réponses sélectionnées par région, données du secteur du commerce électronique uniquement.

* Attention – taille de base basse inférieure à 30

# Points à retenir : les entreprises qui ont segmenté six secteurs d'activité critiques ont considérablement réduit leurs risques

La protection et la segmentation d'un plus grand nombre d'actifs dans l'environnement du commerce électronique renforcent immédiatement la sécurité des entreprises. Avec la bonne solution, les équipes de sécurité sont en mesure d'identifier les attaques plus rapidement, améliorant ainsi le temps moyen de détection (MTTD) et le temps moyen de réponse (MTTR) à un incident. Cependant, une segmentation insuffisante des actifs, qui résulte généralement de l'utilisation de technologies de segmentation héritées, peut créer des failles de sécurité et des angles morts, laissant l'entreprise dans une position plus vulnérable. Mais lorsqu'elle est bien réalisée, la segmentation via une approche définie par logiciel peut aider les entreprises à mieux gérer leurs surfaces d'attaque afin de protéger les actifs critiques de manière plus efficace et plus rentable.

**Nos résultats montrent qu'après une violation, la récupération prend 11 heures de moins avec la segmentation.** Faisons le calcul : pour les entreprises de commerce électronique 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 14 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.

**Imaginez la différence que cela représente pour votre équipe, les dommages à la marque et les coûts encourus pendant ces 11 heures, dans l'un ou l'autre 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 : **14 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

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 comme la solution ne repose pas sur le système d'exploitation sous-jacent 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 et Windows XP aux systèmes POS les plus récents en passant par les derniers terminaux IoT/OT et 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

Akamai Guardicore Segmentation 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 en matière de 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. Le temps et les efforts consacrés à la segmentation manuelle des domaines d'activité, puis au dépannage manuel de ces domaines en cas de panne, peuvent être considérables. Akamai s'efforce de résoudre ce problème, ainsi que le principal obstacle au déploiement, le manque de connaissances, en réduisant le temps consacré à la segmentation manuelle, et en proposant une assistance technique et des services professionnels de premier ordre. 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 et son étiquetage basées sur l'IA, ainsi que 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 des règles et d'éviter les erreurs de configuration d'origine 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 segmentation rationalise la conformité

Nombre de nos clients déploient notre solution pour garantir et attester la conformité à un certain nombre de directives nationales et internationales sur la conformité, comme la norme PCI-DSS, la SWIFT, la loi Sarbanes-Oxley, la norme HIPAA, le RGPD et bien plus encore. Ces directives relatives à la conformité exigent généralement que les données du champ d'application, comme l'environnement des données des titulaires de cartes (CDE) pour PCI DSS, soient séparées et protégées 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 la conformité aux directives en montrant physiquement que les données dans le champ d'application ne sont pas accessibles par des utilisateurs, des systèmes et des machines non autorisés.

# Persévérez avec la bonne solution et le bon support pour transformer votre posture 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 les mouvements latéraux et permet aux intervenants de réagir plus rapidement en cas d'attaque active. Et après une violation, les efforts de récupération sont sécurisés et prennent moins de temps.

Le choix d'une solution définie par logiciel conçue pour surmonter les défis courants associés à un déploiement traditionnel 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 domaines d'activité, plus vous faites progresser votre architecture Zero Trust en réduisant les risques actuels.

# Notre panel

Pour les besoins de ce rapport, nous avons analysé les réponses de 190 personnes travaillant dans le secteur du commerce électronique (59 aux États-Unis, 39 dans la région EMEA, 68 dans la région Asie-Pacifique et 24 dans la région Amérique latine).

Pour l'étude totale, 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'une gamme 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, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. 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 de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com 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.